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

бакалавр
(назва освітнього ступеня)

на тему: Інформаційні технології штучного інтелекту та блокчейн для убезпечення розумних міст

Виконав: студент IV курсу, групи СТ-41
спеціальності 126 Інформаційні системи та технології
(шифр і назва спеціальності)

_____ Крамар В.В.
(підпис) (прізвище та ініціали)

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

Нормоконтроль _____ Шимчук Г.В.
(підпис) (прізвище та ініціали)

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

Рецензент _____ _____
(підпис) (прізвище та ініціали)

Тернопіль
2026

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)
«_8_» _червня_ 2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)
за спеціальністю 126 Інформаційні системи та технології
(шифр і назва спеціальності)
Студенту Крамару Владиславу Володимировичу
(прізвище, ім'я, по батькові)
1. Тема роботи Інформаційні технології штучного інтелекту та блокчейн для убезпечення розумних міст

Керівник роботи Пасічник Володимир Володимирович, д.т.н., професор кафедри КН
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
Затверджені наказом ректора від «*30*» *березня* 2026 року № *4/7-162*
2. Термін подання студентом завершеної роботи 22 червня 2026 р.
3. Вихідні дані до роботи Наукові публікації щодо розумних міст, інформаційних технологій штучного інтелекту та блокчейн, методів та засобів забезпечення беспеки обчислювальних середовищ
4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1. Теоретичні основи побудови «розумних міст» та застосування штучного інтелекту і блокчейну для їх убезпечення. 2. Сучасні технології та кібербезпека «розумних міст». 3. Практичні аспекти застосування штучного інтелекту та блокчейну для кібербезпеки «розумних міст». 4. Безпека життєдіяльності, основи охорони праці. Висновки. Перелік джерел.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Титульна сторінка. 2. Тема та мета дослідження. 3. Завдання дослідження. 4. Актуальність дослідження. 5. Структура «розумного міста». 6. Еволюція «розумного міста». 7. Характеристики «розумного міста». 8. Інформаційно-технологічна архітектура «розумного міста». 9. Аналіз публікацій про інформаційні технології штучного інтелекту та блокчейн для убезпечення розумних міст. 10. Структура послуг кібербезпеки в «розумних містах». 11. Застосування штучного інтелекту в кібербезпеці «розумних міст». 12. Застосування блокчейну в кібербезпеці «розумних міст». 13. Інтеграція штучного інтелекту та блокчейну для кібербезпеки в «розумних містах». 12 Висновки. 13 Завершальний слайд.

6. Консультанти розділів роботи

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

7. Дата видачі завдання 26 січня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	26.01.2026	
2.	Підбір та опрацювання літературних джерел по темі	27.01.2026-16.01.2026	
	кваліфікаційної роботи		
3.	Виконання дослідження щодо застосування	17.01.2026-10.05.2026	
	інформаційних технологій штучного інтелекту та		
	блокчейн для убезпечення «розумних міст»		
4.	Оформлення розділу «Теоретичні основи побудови	11.05.2026-17.05.2026	
	«розумних міст» та застосування штучного інтелекту		
	і блокчейну для їх убезпечення»		
5.	Оформлення розділу «Сучасні технології та	18.05.2026-24.05.2026	
	кібербезпека «розумних міст»»		
6.	Оформлення розділу «Практичні аспекти	25.05.2026-31.05.2026	
	застосування штучного інтелекту та блокчейну для		
	кібербезпеки «розумних міст»»		
7.	Виконання завдання до підрозділу «Безпека	01.06.2026-08.06.2026	
	життєдіяльності»		
8.	Виконання завдання до підрозділу «Основи охорони	01.06.2026-08.06.2026	
	праці»		
9.	Оформлення кваліфікаційної роботи	09.06.2026-11.06.2026	
10.	Нормоконтроль	12.06.2026-15.06.2026	
11.	Перевірка на плагіат	16.06.2026	
12.	Попередній захист кваліфікаційної роботи	18.06.2026	
13.	Захист кваліфікаційної роботи	22.06.2026	

Студент _____ Крамар В.В.
(підпис) (прізвище та ініціали)

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

АНОТАЦІЯ

Інформаційні технології штучного інтелекту та блокчейн для убезпечення розумних міст // Кваліфікаційна робота освітнього рівня «Бакалавр» // Крамар Владислав Володимирович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група СТ-41 // Тернопіль, 2026 // С. 67, рис. – 11, табл. – 4, кресл. – 15, додат. – 0, бібліогр. – 51.

Ключові слова: блокчейн, безпека даних, інформаційна інфраструктура, кібербезпека, розумні міста, системи штучного інтелекту, технології захисту інформації, цифрова трансформація.

Кваліфікаційна робота присвячена дослідженню інформаційних технологій штучного інтелекту та блокчейн для убезпечення розумних міст. В першому розділі кваліфікаційної роботи подано передумови використання штучного інтелекту та блокчейну для забезпечення безпеки розумних міст. Висвітлена методика систематичного аналізу наукових джерел щодо кіберзахисту «розумних міст». Розглянуто концептуальні основи побудови та функціонування «розумних міст». Описана еволюція «розумних міст». Подано характеристики «розумних міст». Проаналізовано ключові компоненти «розумних міст». Сформовано інформаційно-технологічну архітектуру «розумного міста». В другому розділі кваліфікаційної роботи описано кібератаки, загрози та безпекові виклики в «розумних містах». Розглянута кібербезпека в «розумних містах». Сформовано принципи кібербезпеки в «розумних містах». Описано послуги кібербезпеки в «розумних містах». Досліджено важливість кібербезпеки в «розумних містах». Проаналізовано технологічний прогрес у кібербезпеці «розумних міст». В третьому розділі кваліфікаційної роботи розглянуто застосування штучного інтелекту в кібербезпеці «розумних міст». Проаналізовано застосування блокчейну в кібербезпеці «розумних міст». Досліджено інтеграцію штучного інтелекту та блокчейну для кібербезпеки в «розумних містах».

ANNOTATION

Information Technologies of Artificial Intelligence and Blockchain for Securing Smart Cities // Qualification work of the educational level «Bachelor» // Vladyslav Kramar // Ternopil Ivan Pulyu National Technical University, Computer and Information Systems and Software Engineering Faculty, Computer Sciences Department, group ST-41 // Ternopil, 2026 // P. 67, fig. – 1, tabl. – 4, chair. – 15, annexes. – 0, references – 51.

Keywords: blockchain, data security, information infrastructure, cybersecurity, smart cities, artificial intelligence systems, information protection technologies, digital transformation.

The qualification work is devoted to the study of information technologies of artificial intelligence and blockchain for securing smart cities. The first chapter of the qualification work presents the prerequisites for the use of artificial intelligence and blockchain to ensure the security of smart cities. The methodology of systematic analysis of scientific sources on cybersecurity of “smart cities” is highlighted. The conceptual foundations of the construction and functioning of “smart cities” are considered. The evolution of “smart cities” is described. The characteristics of “smart cities” are presented. The key components of “smart cities” are analyzed. The information and technological architecture of a “smart city” is formed. The second chapter of the qualification work describes cyberattacks, threats, and security challenges in “smart cities.” Cybersecurity in “smart cities” is considered. The principles of cybersecurity in “smart cities” are formulated. Cybersecurity services in “smart cities” are described. The importance of cybersecurity in “smart cities” is investigated. Technological progress in cybersecurity of “smart cities” is analyzed. The third chapter of the qualification work examines the application of artificial intelligence in cybersecurity of “smart cities”. The use of blockchain in cybersecurity of “smart cities” is analyzed. The integration of artificial intelligence and blockchain for cybersecurity in “smart cities” is investigated.

ПЕРЕЛІК СКОРОЧЕНЬ І ТЕРМІНІВ

ШІ – штучний інтелект.

AES (Advanced Encryption Standard) — це сучасний симетричний алгоритм шифрування, який використовується для захисту даних у критичних системах «розумного міста».

CPS (англ. Cyber-Physical Systems) – кіберфізичні системи, що інтегрують фізичні процеси з цифровими технологіями управління.

DL (англ. Deep Learning) – глибинне навчання, метод машинного навчання на основі багатошарових нейронних мереж.

IDS (Intrusion Detection System) — це система виявлення вторгнень.

IoT (англ. Internet of Things) – Інтернет речей, мережа взаємопов’язаних пристроїв і сенсорів для збору та обміну даними.

ML (англ. Machine Learning) – машинне навчання, підгалузь ШІ для навчання систем на основі даних.

NLP (англ. Natural Language Processing) – обробка природної мови, технологія ШІ для аналізу та інтерпретації текстів і мовлення.

ЗМІСТ

ВСТУП

Актуальність теми. Розвиток «розумних міст» зумовлює формування складних інформаційно-технологічних екосистем, у яких цифрові сервіси забезпечують ефективне управління міською інфраструктурою та реагування на урбаністичні виклики [1]. Водночас зростання кількості підключених пристроїв, обсягів даних і взаємозв'язків між системами призводить до суттєвого підвищення рівня кіберзагроз і вразливостей [2]. У цьому контексті особливої актуальності набуває застосування технологій штучного інтелекту та блокчейну як інструментів підвищення стійкості та захищеності міських цифрових систем.

Аналіз наукових джерел за 2021–2024 роки, представлених у провідних наукових базах даних, свідчить про активний розвиток підходів до використання штучного інтелекту та блокчейну в системах кіберзахисту «розумних міст» [1]. Штучний інтелект забезпечує можливість виявлення аномальних поведінкових моделей, прогнозування потенційних атак та оперативного реагування на інциденти за рахунок методів машинного навчання та глибокого навчання [3]. У свою чергу, блокчейн-технологія гарантує цілісність, незмінність та прозорість даних завдяки децентралізованій структурі зберігання інформації, а також розширює можливості керування ідентифікацією, транзакціями та обміном даними через використання смарт-контрактів [4].

Поєднання цих технологій формує нові підходи до побудови багаторівневих моделей кіберзахисту, що підвищують надійність та стійкість цифрової інфраструктури «розумних міст» до сучасних кіберризиків [1]. Подальші дослідження доцільно спрямовувати на розробку інтегрованих архітектур безпеки міських інформаційних систем та формування практичних рекомендацій для фахівців у сфері кібербезпеки та міського управління [5].

Таким чином, дослідження можливостей інтеграції технологій штучного інтелекту та блокчейну для підвищення рівня безпеки «розумних міст» є

актуальним і перспективним напрямом наукових досліджень у сфері інформаційних технологій.

Мета і задачі дослідження. Мета даної кваліфікаційної роботи освітнього рівня «Бакалавр» полягає у теоретичному обґрунтуванні та аналізі можливостей застосування технологій штучного інтелекту та блокчейну для підвищення рівня кібербезпеки та забезпечення захищеності інформаційно-технологічної інфраструктури «розумних міст». Для досягнення поставленої мети потрібно виконати ряд завдань, зокрема:

– Проаналізувати теоретичні засади функціонування «розумних міст» та їх інформаційно-технологічної інфраструктури.

– Дослідити основні загрози та виклики кібербезпеки в умовах розвитку міських цифрових систем.

– Обґрунтувати можливості застосування технологій штучного інтелекту для виявлення та запобігання кіберзагрозам у «розумних містах».

– Визначити роль блокчейн-технологій у забезпеченні цілісності, прозорості та захищеності міських інформаційних даних.

– Розробити підходи до інтеграції штучного інтелекту та блокчейну для підвищення рівня кібербезпеки «розумних міст».

Практичне значення одержаних результатів полягає у можливості їх використання для підвищення рівня кібербезпеки інформаційно-технологічної інфраструктури «розумних міст» шляхом удосконалення методів виявлення та запобігання кіберзагрозам, а також забезпечення цілісності та надійності міських цифрових сервісів на основі технологій штучного інтелекту та блокчейну.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ «РОЗУМНИХ МІСТ» ТА ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ І БЛОКЧЕЙНУ ДЛЯ ЇХ УБЕЗПЕЧЕННЯ

1.1 Передумови використання штучного інтелекту та блокчейну для забезпечення безпеки розумних міст

За даними ООН, процес урбанізації призведе до того, що до 2050 року у містах проживатиме понад 68% населення світу [1]. Це зумовлює значні виклики:

– перевантаження інфраструктури;
– забруднення;
– дефіцит ресурсів;
– енергетичні проблеми;
– соціальні проблеми [3].

У відповідь на це формується концепція «розумного міста», що базується на використанні:

– сенсорних систем;
– IoT-пристроїв та систем;
– 5G;
– цифрових двійників;
– великих за обсягом наборів і колекцій даних;

ШІ-інструментів [6]. Інтеграція транспортної, енергетичної, медичної та управлінської сфер у єдину систему забезпечує ефективне планування та стійкий розвиток [1].

Проте впровадження таких технологій супроводжується зростанням кіберзагроз від атак на IoT-пристрої до складних APT-кампаній [7]. Відомі випадки втручання у «розумні» системи водопостачання та транспортні сигнали демонструють потенційні ризики для безпеки та довіри громадян [1].

Традиційні методи захисту, як-от шифрування чи біометрія, виявляються недостатніми [1].

Поєднання ШІ та блокчейну пропонує нові підходи до кіберзахисту «розумних міст». ШІ забезпечує виявлення аномалій та прогнозування атак за допомогою ML і DL [1], тоді як блокчейн гарантує цілісність даних, децентралізований контроль та безпечну ідентифікацію [8]. Синергія цих технологій формує стійкі моделі кібербезпеки «розумних міст», здатні протидіяти сучасним загрозам [1].

Огляд літератури [1] показує, що інтеграція ШІ та блокчейну у сфері кіберзахисту «розумних міст» перебуває на етапі становлення. Подальші дослідження мають зосередитися на розробці комплексних рішень, які враховують специфіку урбаністичних систем та забезпечують баланс між технологічним розвитком і захистом даних [9].

1.2 Методика систематичного аналізу наукових джерел щодо кіберзахисту «розумних міст»

Дослідження [1] спрямоване на аналіз застосування технологій ШІ та блокчейну для посилення кіберзахисту «розумних міст». Використано систематичний огляд літератури за 2021–2024 рр., що охоплює наукові статті, матеріали конференцій, монографії та інші джерела. Пошук здійснювався у провідних базах даних, зокрема «ACM Digital Library», «Wiley Online Library», «Springer», «ScienceDirect», «MDPI», «IEEE Xplore» та «Google Scholar» (див. рисунок 1.1), із застосуванням ключових слів та логічних операторів для відбору релевантних праць [2].

Відбір матеріалів проводився за чіткими критеріями: відповідність тематиці ШІ, блокчейну та кібербезпеки «розумних міст», наявність прозорої методології та достовірних результатів.

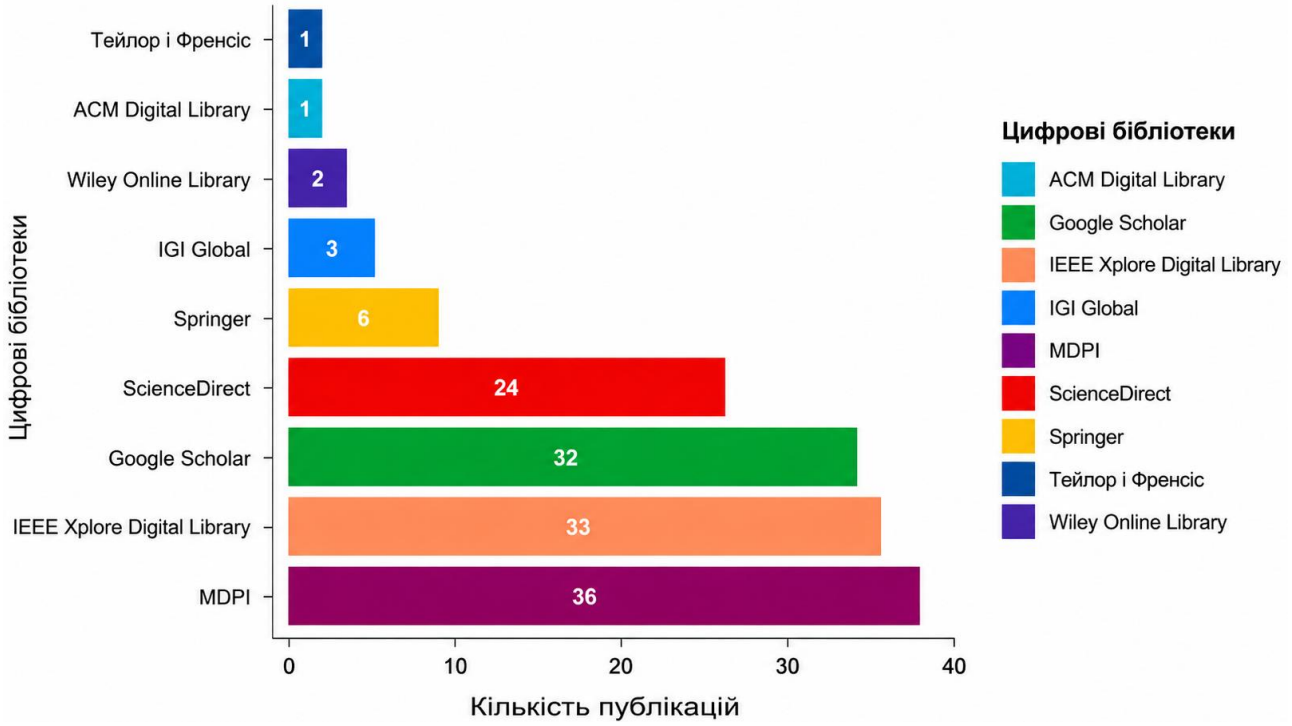

Рисунок 1.1 – Цифрові бази даних, що використовуються для пошуку вибраних дослідницьких робіт [1]

Виключалися публікації, що не відповідали темі або мали нечіткі висновки [1]. У процесі аналізу було розглянуто майже сто сорок публікацій, які систематизовано за напрямами [3]:

– інформаційно-технологічна архітектура «розумних міст»;
– новітні технології;
– кіберзагрози;
– принципи захисту.

Особливу увагу приділено застосуванню ШІ для виявлення аномалій та прогнозування атак за допомогою ML та DL, а також використанню блокчейну для забезпечення цілісності даних «розумних міст», децентралізованого управління та безпечної комунікації [4]. Синергія цих технологій розглядається як перспективний напрям формування стійких моделей кіберзахисту «розумних міст», що відповідають потребам сучасних урбаністичних систем [1]. На рисунку 1.2 показано розподіл вибраних статей за цифровими бібліотеками залежно від типу статті.

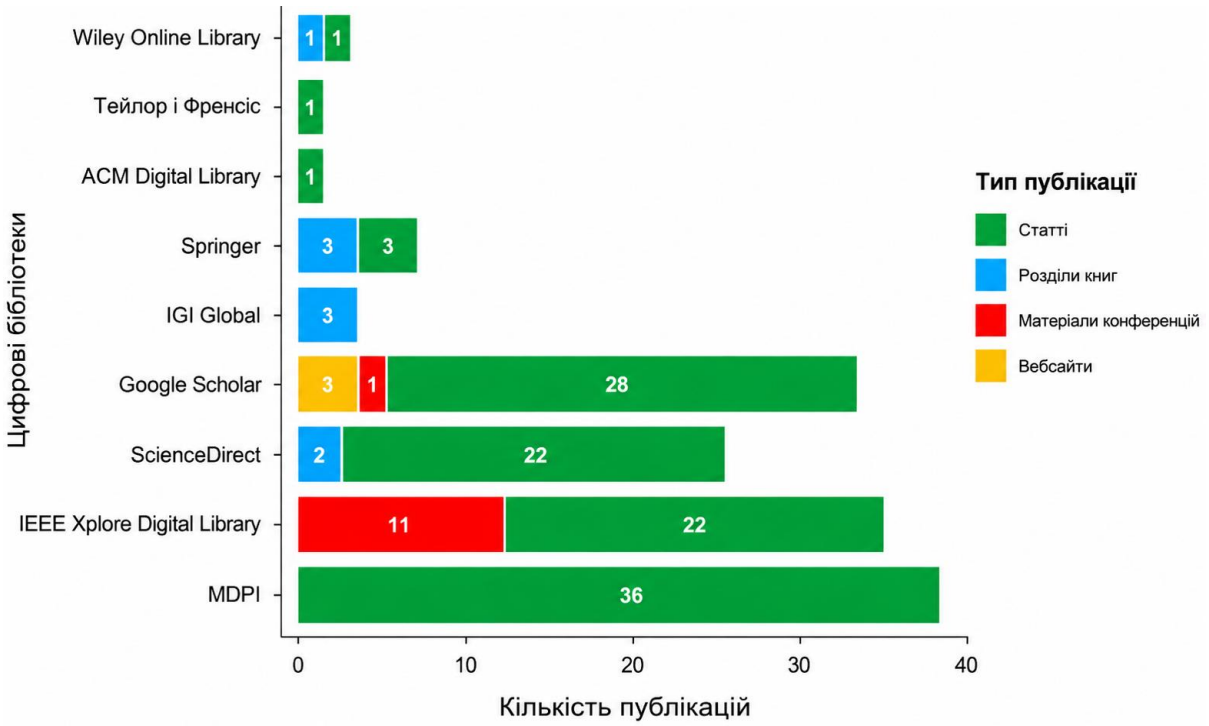

Рисунок 1.2 – Розподіл вибраних статей за цифровими бібліотеками залежно від типу статті [1]

На рисунку 1.3 зображено розподіл вибраних статей за цифровими бібліотеками залежно від року публікацій.

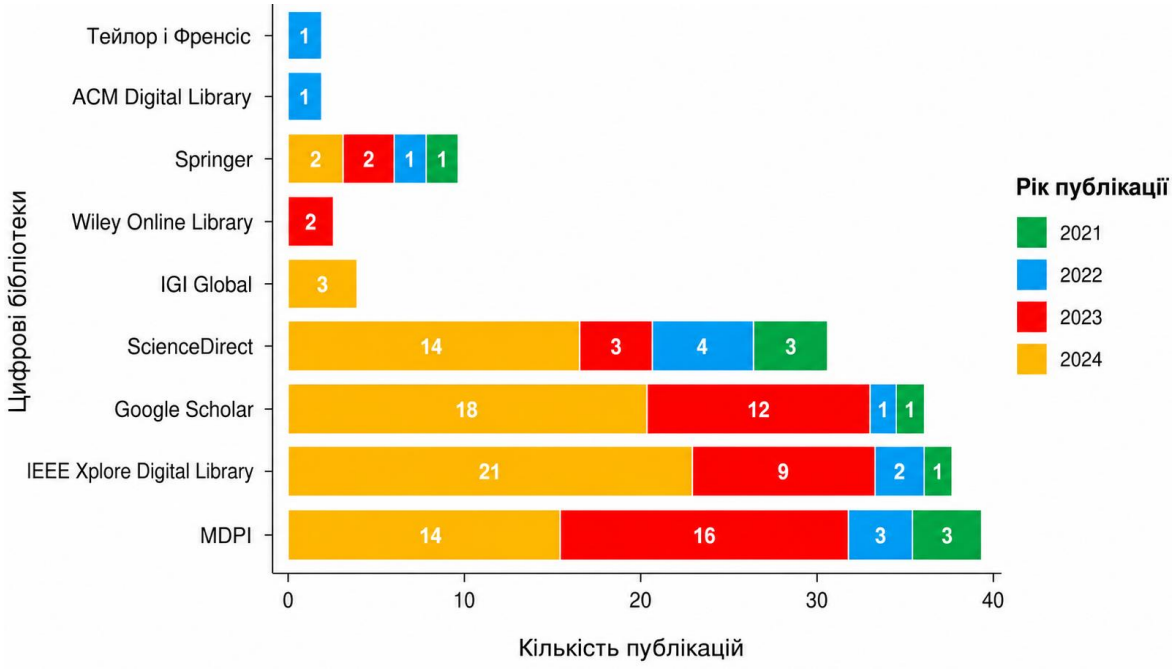

Рисунок 1.3 – Розподіл вибраних статей за цифровими бібліотеками залежно від року публікацій [1]

У дослідженні [1] здійснено систематичний аналіз літератури щодо застосування ШІ та блокчейну для кіберзахисту «розумних міст». Зібрані дані охоплювали публікаційні відомості, напрями досліджень, технології та методології, що дало можливість здійснити тематичний синтез. Використано якісний підхід, який застосовував класифікацію результатів за ключовими темами:

– виявлення аномалій у IoT-системах за допомогою ШІ;

– забезпечення цілісності даних та контролю доступу через блокчейн;

– інтеграцію цих технологій для автоматизованого реагування на загрози [2].

Оцінювалася ефективність ШІ та блокчейну окремо й у поєднанні, з урахуванням масштабованості, споживання ресурсів, рівня безпеки та продуктивності у реальних умовах «розумних міст» [1]. Виявлено прогалини у наявних дослідженнях, що визначають напрями подальших робіт, зокрема розвиток методів інтеграції та оптимізації систем кіберзахисту «розумних міст» [3]. Аналіз [1] показав, що успішність застосування ШІ та блокчейну у «розумних містах» залежить від здатності:

– зменшувати кількість кіберінцидентів;

– забезпечувати масштабованість інфраструктури;

– оптимізувати використання обчислювальних ресурсів;

– інтегруватися без значних порушень у вже існуючі системи.

Водночас відзначено обмеження, пов’язані з швидким розвитком технологій та мовними бар’єрами у доступі до досліджень [5].

1.3 Концептуальні основи побудови та функціонування «розумних міст»

Концепція «розумного міста» виникла у США на початку 1990-х років, зокрема під час Міжнародного конгресу «Smart Cities, Global Networks» у Сан-Франциско (1990 р.) [10]. Відтоді визначення цього явища зазнало еволюції

та потребує міждисциплінарного підходу для повного розуміння його складових. У науковій літературі «розумне місто» трактується з двох позицій: функціональної та технологічної. На рисунку 1.4 подана концептуальна структура «розумного міста».

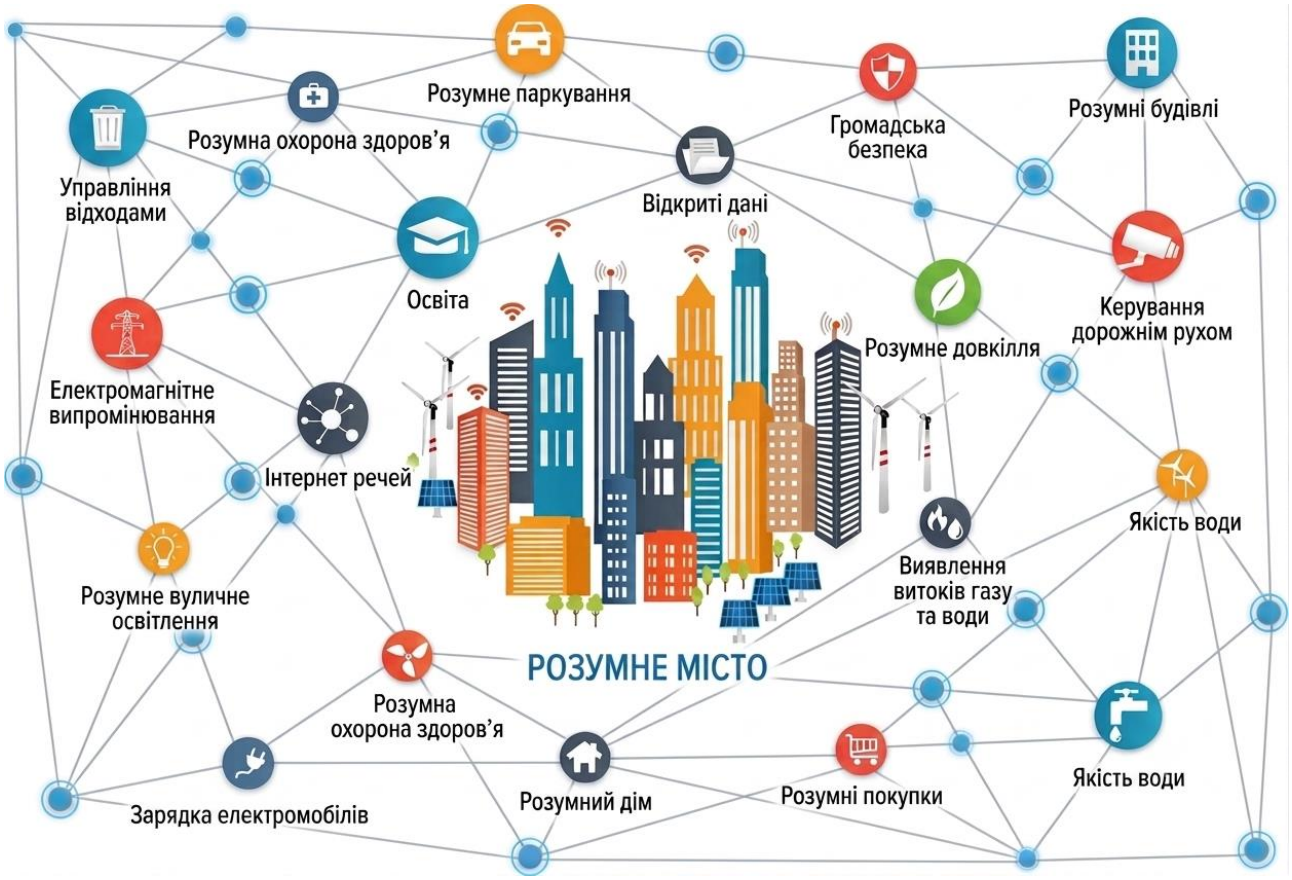

Рисунок 1.4 – Концептуальна структура «розумного міста» [1]

Концепція «розумного міста» потребує використання технологічних інновацій, сучасної інфраструктури та ефективного управління для трансформації урбаністичних просторів у стійкі та інклюзивні середовища [1]. Поєднання технологій та аналітичного опрацювання даних забезпечує підвищення якості життя мешканців, оптимізацію міських процесів та розвиток сталого управління.

Удосконаленню «розумних» транспортних систем, «розумних» комунальних послуг та «розумних» екологічних програм сприяє [1] застосування:

– IoT-пристроїв та систем;

– великих за обсягом наборів і колекцій даних;

– аналітичних методів.

Ефективний обмін даними між економічними, управлінськими та екологічними секторами формує інтегровану систему «розумного міста», що забезпечує оперативне реагування та підвищує рівень зручності й безпеки для мешканців [10]. Таким чином, «розумні міста» створюють адаптивні урбаністичні моделі, орієнтовані на стійкий розвиток та потреби суспільства.

1.4 Еволюція «розумних міст»

Еволюція «розумних міст» розгортається впродовж п’яти окремих фаз, від «розумного міста 1.0» до «розумного міста 5.0». Кожна фаза знаменує собою значний стрибок у технологіях, управлінні та залученні громади. Ці фази підкреслюють, як міське середовище трансформується, щоб краще служити своїм мешканцям [11].

Етап «розумного міста 1.0» визначає початкову фазу розвитку «розумного міста», коли впроваджуються цифрові технології та інноваційні стратегії для вирішення урбаністичних проблем і підвищення якості життя населення [11]. Основна увага приділяється запуску пілотних проєктів та перевірці життєздатності нових рішень у реальних умовах.

На цьому етапі реалізуються ініціативи у сферах транспорту, енергетики, управління відходами, безпеки та охорони здоров’я, що демонструють потенціал масштабування [12]. Формується базова інфраструктура, зокрема:

– високошвидкісний інтернет;

– «розумне» освітлення;

– системи збору даних.

Водночас здійснюється цифровізація комунальних послуг. Головна мета полягає у створенні інтегрованої інфраструктури, яка стане основою для подальшого розвитку «розумних міст» [11].

Етап «розумного міста 2.0» є наступною фазою розвитку «розумного міста», що базується на досягненнях «розумного міста 1.0» [11]. Він орієнтований на використання аналітичного опрацювання даних, ML та ШІ для оптимізації процесів, стратегічного управління та підвищення стійкості міських систем. Основні пріоритети [12] цього етапу:

– інтеграція;
– масштабованість;
– інклюзивність;
– орієнтація на потреби громадян.

«Розумне місто 2.0» потребує створення єдиних інформаційно-технологічних платформ для обміну даними та взаємодії між секторами «розумної» економіки, «розумного» управління, «розумного» транспорту й «розумної» безпеки. Централізовані системи збору та аналізу інформації забезпечують узгоджене прийняття рішень, а використання режимів реального часу у «розумних» транспортних та «розумних» безпекових системах підвищує ефективність і рівень захисту населення [11]. Таким чином, «розумне місто» переходить від базової цифровізації до комплексного управління, де ШІ та блокчейн стають ключовими інструментами забезпечення кіберзахисту та сталого розвитку.

У відповідь на нові виклики та можливості етап «розумного міста 3.0» характеризується:

– інноваційністю;
– стійкістю
– адаптивністю.

Для формування надійніших «розумних» міських середовищ [11] його розвиток базується на використанні:

– блокчейну;
– IoT-пристроїв;
– автономних систем.

«Розумна» інфраструктура, зокрема самовідновлювані «розумні» енергомережі та автоматизовані «розумні» системи управління водними ресурсами, підвищують надійність критичних міських послуг [12].

Важливу роль відіграють інноваційні інформаційно-технологічні системи та цифрові хаби, що підтримують стартапи, малий бізнес та інтегрують університети й наукові установи у міський простір. «Розумне місто 3.0» використовує гіперзв'язану інфраструктуру, де технології 5G/6G, квантові та периферійні обчислення забезпечують інтеграцію й обмін даними у режимі реального часу [11]. Особливий акцент робиться на залученні громадян через цифрові платформи, що сприяє прозорості, довірі та узгодженню розвитку «розумного міста» з потребами суспільства [12].

Етап «розумного міста 4.0» є наступною фазою міського розвитку, що ґрунтується на попередніх етапах та інтегрує новітні технології, зокрема ШІ, мережі 5G та периферійні обчислення [11]. Його мета полягає у створенні інтелектуальніших, адаптивних та взаємопов'язаних урбаністичних систем, здатних забезпечувати персоналізовані послуги для мешканців і відвідувачів.

Особливу роль відіграють VR та AR-технології, що формують «розумні» простори відповідно до індивідуальних потреб. «Розумне місто 4.0» використовує розширену співпрацю між містами та приватним сектором, використання децентралізованих моделей управління та інтеграцію цифрових двійників і кіберфізичних систем [12]. Це забезпечує узгоджене функціонування «розумних» транспортних мереж, «розумних» енергетичних систем та галузі «розумної» охорони здоров'я. Застосування ШІ та великих за обсягом наборів та колекцій даних надає можливість:

– прогнозувати інфраструктурні проблеми;
– оптимізувати розподіл енергії;
– підвищувати ефективність «розумних» медичних послуг [13];
– підвищувати ефективність транспортних послуг [11].

Етап «розумного міста 5.0» визначає нову фазу розвитку «розумного міста», орієнтовану на:

– технологічну досконаліть;

– стійкість;

– гуманітарну спрямованість.

Основна увага приділяється екологічній сталості через принципи циркулярної економіки, зменшення відходів та використання відновлюваних джерел енергії [11]. Важливим аспектом є підвищення здатності міських систем швидко відновлюватися після криз та природних катастроф, що забезпечує надійність інфраструктури [12].

«Розумне місто 5.0» також акцентує увагу на:

– добробуті населення;

– соціальній інклюзії;

– збереженні природних ресурсів.

Еволюція від «розумного міста 1.0» до «розумного міста 5.0» (див. рисунок 1.5) демонструє поступовий перехід до інтелектуальніших, адаптивних та стійких урбаністичних моделей, де кожен етап базується на попередньому, інтегруючи новітні технології та залучаючи громаду до управління [11].

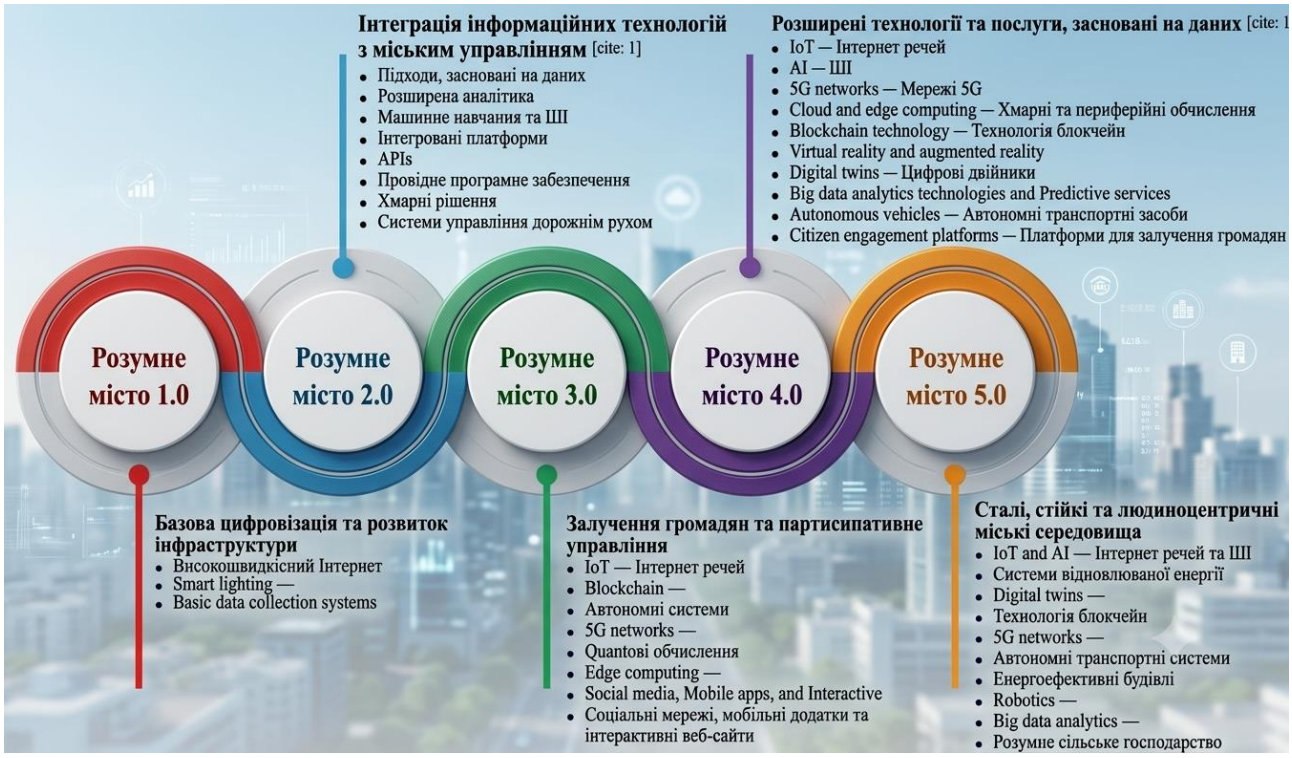

Рисунок 1.5 – Еволюція від «розумного міста 1.0» до «розумного міста 5.0» [1]

1.5 Характеристики «розумних міст»

«Розумні міста» активно використовують технології та дані для покращення якості життя, стимулювання сталого розвитку та стимулювання економічного розвитку. Розвиток «розумного міста» базується на використанні Інтернету речей (IoT), що визначає його гетерогенність [14]. Системи характеризуються автономністю, розподіленим розгортанням та різноманітністю користувачів. Інформаційно-технологічні архітектури «розумних міст» інтегрують:

– IoT-вузли;
– технології підключення;
– мобільність;
– апаратні можливості;
– інформаційно-технологічні платформи [15].

IoT-пристрої нерідко мають обмежені ресурси – невелику пам’ять, 8- або 16-бітні мікроконтролери та низьку швидкість передачі даних (20–250 кбіт/с). Міська мобільність інтегрує інтелектуальні транспортні системи, електромобілі та автономні засоби, що зменшує затори та викиди, підвищуючи ефективність перевезень. Підключення формує основу інформаційно-технологічної системи [16], використовуючи для збору й обміну даними:

– IoT-пристрої та системи;
– 5G;
– смарт-сенсори.

Обмеженість ресурсів у «розумному місті» вимагає оптимізації енергоспоживання та використання відновлюваних джерел. Давачі збирають дані про транспорт, якість повітря, енергетику та відходи, що дає містам можливість приймати обґрунтовані рішення. Аналітичне опрацювання даних, ML та ШІ виявляють закономірності й аномалії, прогнозують сценарії та оптимізують послуги. Сталий розвиток потребує економічного процвітання, соціальної інклюзивності та екологічної стійкості. Використання цифрових

технологій сприяє прозорості, електронному управлінню та залученню громадян [6].

Зв’язок та масштабованість є критичними для розширення від невеликих проєктів до великих міських середовищ. Зростання обсягів даних потребує масштабованих систем. Інфраструктура та підключення дають «розумним містам» змогу збирати й аналізувати інформацію для підвищення якості життя та сталого розвитку. Важливим є залучення громад, що забезпечує ефективність та безпеку застосунків [6].

Залучення користувачів у «розумному місті» реалізується через електронне управління, цифрові послуги, портали відкритих даних та системи охорони здоров’я. Це сприяє прозорості, активності громадян та спрощенню бюрократичних процесів. Використання ML та ШІ дає містам можливість проактивно управляти ресурсами та формувати адаптивні стратегії розвитку [6].

Рисунок 1.6 – Характеристики «розумного міста»

Інтернет речей та сенсори забезпечують інтеграцію технологій у міське середовище. Використання IoT, 5G та «розумних» сенсорних систем надає

можливість ефективно збирати дані, що стимулює інновації та підвищує ефективність управління [17]. Це створює технологічну основу для сталого розвитку «розумних міст» [11].

Аналітичне опрацювання даних та ШІ дає містам змогу прогнозувати майбутні сценарії, оптимізувати послуги та управляти ресурсами. Використання ML та алгоритмів ШІ забезпечує виявлення тенденцій та аномалій, що підвищує якість управління та сприяє екологічній стійкості «розумних міст» [11].

Таким чином, розвиток «розумного міста» базується на:

– гетерогенності IoT-систем [18];
– обмежених ресурсах;
– масштабованості;
– залученні громадян;
– використанні ШІ;
– використанні блокчейну.

Це забезпечує прозорість, ефективність та сталий розвиток «розумного міста» [11].

1.6 Ключові компоненти «розумних міст»

Інтеграція ключових компонентів у «розумному місті» спрямована на підвищення ефективності управління ресурсами та забезпечення сталого розвитку. Інтелектуальна інфраструктура використовує IoT-сенсори для моніторингу «розумного» транспорту та «розумних» споруд [19], а ШІ прогнозує потреби у ремонті та оптимізує графіки обслуговування. Блокчейн забезпечує прозорість та захист даних, що підвищує довіру між учасниками [20].

«Розумні» енергомережі оптимізують розподіл енергії з відновлюваних джерел, використовуючи сенсори та алгоритми ШІ для балансування попиту й запобігання аваріям. Блокчейн підтримує безпечні енергетичні транзакції та

розвиток peer-to-peer моделей [21]. У сфері «розумного» транспорту застосовуються IoT-пристрої та аналітичне опрацювання для прогнозування заторів, а блокчейн гарантує безпечний обмін даними між транспортними агентствами [22].

Система «розумної» охорони здоров’я у «розумному місті» інтегрує IoT-пристрої, телемедицину та ШІ для діагностики й прогнозування епідемій, тоді як блокчейн забезпечує захист медичних даних [23]. Аналогічно, у сфері управління відходами сенсори та алгоритми ШІ оптимізують маршрути збору, а блокчейн гарантує прозорість процесів [23].

«Розумне» управління водними ресурсами здійснюється через IoT-сенсори та ML-алгоритми, що прогнозують витоки та оптимізують розподіл води, а блокчейн забезпечує достовірність даних [20]. «Розумне» освітлення, енергетика та будівлі використовують сенсори й ШІ для зниження споживання ресурсів, а блокчейн забезпечує прозорість витрат [24].

Управління містом базується на цифрових платформах, що підвищують прозорість, залучають громадян та забезпечують ефективність адміністративних процесів [1]. «Розумні» громади активно використовують цифрові інструменти, ШІ та блокчейн для участі в управлінні та формування політик [22]. Таким чином, поєднання ШІ, ML та блокчейну у різних сферах «розумного міста» створює комплексну систему кіберзахисту, оптимізації ресурсів та забезпечення сталого розвитку [25].

1.7 Інформаційно-технологічна архітектура «розумного міста»

Інформаційно-технологічна архітектура «розумного міста» (див. рисунок 1.7) функціонує як багаторівнева система, що забезпечує ефективне управління ресурсами, підвищення якості життя населення та підтримку сталого розвитку. Вона інтегрує різні технології та компоненти у взаємопов’язані рівні, які оптимізують потоки даних та сприяють удосконаленню міських сервісів [26].

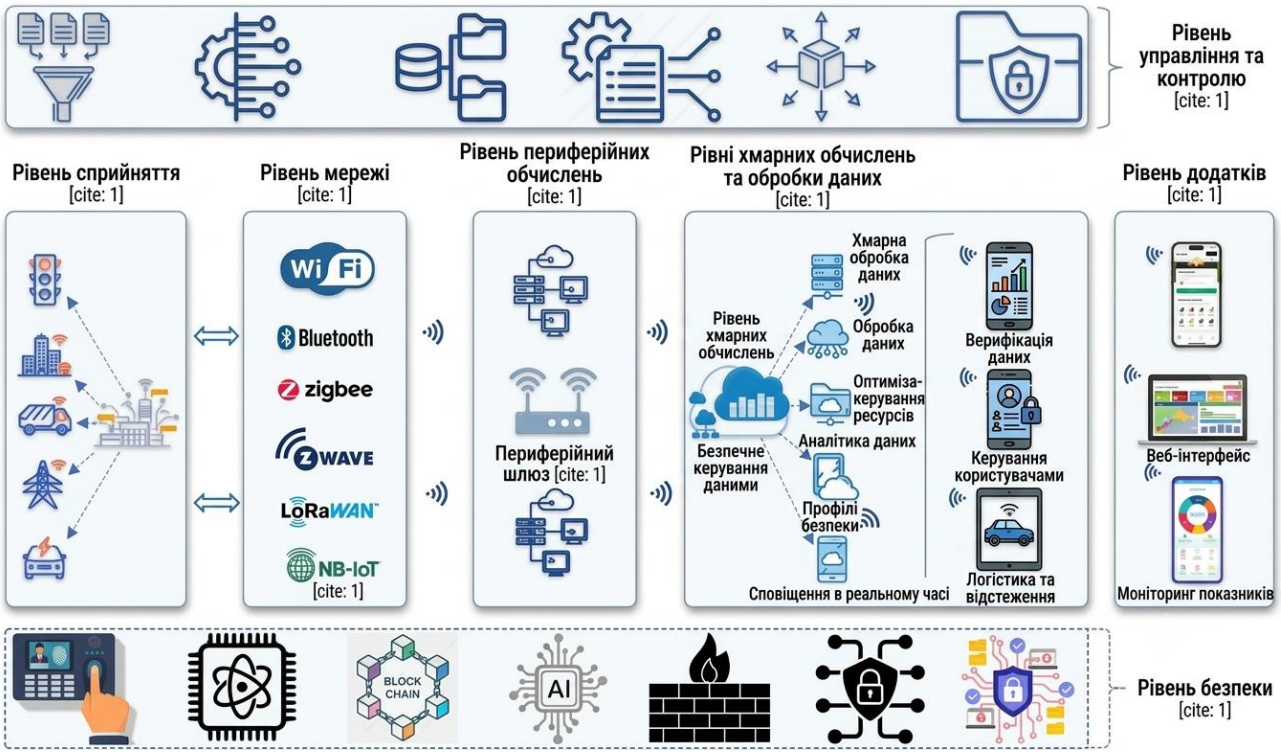

Рисунок 1.7 – Основні рівні інформаційно-технологічної архітектури «розумного міста»

Дизайн такої інформаційно-технологічної архітектури є масштабованим і динамічним, що дає можливість адаптуватися до змінних функціональних та якісних вимог. Завдяки безперервній інтеграції рівнів система стає чутливішою до потреб громадян, забезпечуючи ефективне «розумне» управління та надання послуг у мінливому середовищі «розумних міст» [27]. Шар сприйняття в інформаційно-технологічній архітектурі «розумного міста» виконує ключову роль у зборі даних у режимі реального часу для підтримки управління та прийняття рішень. Інформацію для «розумного» підвищення безпеки, «розумної» оптимізації ресурсів та «розумного» транспорту [27] забезпечують:

– IoT-сенсори та пристрої;
– Інтелектуальні екологічні давачі;
– смарт-лічильники;
– RFID-мітки;
– GPS-системи.

Обробка даних на периферійних пристроях зменшує затримки та надає можливість швидко реагувати на зміни міського середовища, наприклад, регулювати світлофори чи активувати аварійні сигнали. Актуатори перетворюють дані на дії, керуючи освітленням, транспортними потоками та системами енергоспоживання. У результаті формується адаптивна "інформаційно-технологічна система, що підвищує стійкість, ефективність та якість управління «розумним містом» [28].

Мережевий шар є комунікаційною основою інформаційно-технологічної архітектури «розумного міста», що забезпечує безперервну передачу даних та з'єднання між пристроями й системами. Він гарантує стабільний потік інформації від збору до обробки та зберігання [29].

Для короткодистанційної взаємодії застосовуються протоколи Wi-Fi, Bluetooth, Zigbee, Z-Wave, а для високошвидкісної передачі даних у режимі реального часу – технології 4G LTE та 5G. LPWAN-рішення (LoRaWAN, NB-IoT) забезпечують енергоефективний зв'язок на значні відстані для IoT-пристроїв [8]. Цей шар підтримує масштабованість, безпеку та інтероперабельність «розумного міста», що дає змогу здійснювати аналіз у режимі реального часу та приймати управлінські рішення, водночас захищаючи дані від кіберзагроз [30].

Периферійні обчислення доповнюють хмарні технології, забезпечуючи локальну обробку даних та зменшення затримок, що є критично важливим для систем управління транспортом та екстрених служб. Локальна фільтрація даних знижує навантаження на канали зв'язку та витрати, підвищуючи ефективність і надійність «розумних» міських сервісів навіть за обмеженого доступу до хмар [1].

Хмарні платформи забезпечують масштабоване зберігання та обробку великих за обсягом наборів та колекцій даних, що генеруються IoT-пристроями «розумних міст». Вони підтримують аналітичне опрацювання у режимі реального часу, навчання ML-моделей та роботу ШІ-алгоритмів, що є основою для застосувань «розумного міста». Гнучкість хмарних рішень дає можливість

адаптувати ресурси до змінних умов, зокрема під час кризових ситуацій, забезпечуючи безпечне зберігання та доступність даних [29].

Шар обробки даних трансформує інформацію сенсорів у практичні рішення, використовуючи аналітичне опрацювання великих за обсягом наборів та колекцій даних та алгоритми ШІ для прогнозування та оптимізації міських процесів, зокрема, «розумного» транспорту та «розумного»розподілу ресурсів [20].

Застосунковий рівень безпосередньо орієнтований на мешканців, пропонуючи сервіси на основі ШІ:

– «розумне» управління транспортом;
– «розумну» оптимізацію енергоспоживання;
– «розумну» телемедицину;
– «розумне» водопостачання;
– «розумну» утилізацію відходів.

Інтерфейси у вигляді мобільних застосунків забезпечують участь громадян у прийнятті рішень [29].

Безпека «розумного міста» ґрунтується на шифруванні даних, багаторівневій автентифікації та блокчейні, що гарантує прозорий і незмінний обмін інформацією. Алгоритми ШІ підвищують ефективність виявлення загроз «розумним містам» у режимі реального часу [30].

Шар управління та контролю координує всі компоненти системи, забезпечуючи ефективність, адаптивність та стійкість міських сервісів. Використання аналітичних панелей та автоматизованих контролерів сприяє оптимізації енергоспоживання, транспорту та інших критичних сфер [31].

Таким чином, інформаційно-технологічна архітектура «розумного міста» інтегрує IoT, ШІ, хмарні та блокчейн-технології, формуючи стійку систему управління, що підвищує якість життя та забезпечує кіберзахист урбаністичних середовищ.

1.8 Висновок до першого розділу

В першому розділі кваліфікаційної роботи подано передумови використання штучного інтелекту та блокчейну для забезпечення безпеки розумних міст. Висвітлена методика систематичного аналізу наукових джерел щодо кіберзахисту «розумних міст». Розглянуто концептуальні основи побудови та функціонування «розумних міст». Описана еволюція «розумних міст». Подано характеристики «розумних міст». Проаналізовано ключові компоненти «розумних міст». Сформовано інформаційно-технологічну архітектуру «розумного міста».

РОЗДІЛ 2. СУЧАСНІ ТЕХНОЛОГІЇ ТА КІБЕРБЕЗПЕКА «РОЗУМНИХ МІСТ»

2.1 Новітні технології в «розумних містах»

Новітні технології трансформують «розумні міста», підвищуючи ефективність, сталий розвиток та орієнтований на громадян міський розвиток. У таблиці 2.1 подано огляд ключових нових технологій, які впливають на «розумні міста».

Таблиця 1 – Інфраструктурні технології «розумних міст»

Технологія	Опис
Інтернет речей (IoT)	Забезпечує інтеграцію сенсорів та пристроїв для збору даних у режимі реального часу, оптимізації ресурсів та розвитку «розумного міста». Використовується у «розумному» транспорті, «розумній» енергетиці, «розумній» охороні здоров'я, але створює нові кіберзагрози [22].
Кіберфізичні системи (CPS)	Інтегрують ІКТ з інфраструктурою, підтримують «розумні» енергомережі, транспорт та медичний моніторинг [32].
Сенсорні мережі	Формують основу «розумного міста», забезпечуючи моніторинг довкілля, безпеки та транспорту [6].
5G та бездротові мережі	Підвищують швидкість та щільність з'єднань, підтримують IoT, автономний транспорт та «розумну» телемедицину. Використовуються для відеоспостереження та «розумних» будівель [33].
Хмарні обчислення	Забезпечують масштабоване зберігання та аналітичне опрацювання даних, підтримують інтеграцію IoT та скорочують витрати «розумного міста» [21].
Туманні обчислення	Оптимізують локальну обробку даних, зменшують затримки та підтримують безпеку у «розумному місті» [21].
Edge-обчислення	Виконують аналіз даних біля джерела, зменшуючи навантаження на «розумну» мережу та забезпечуючи швидке реагування [21].

Ця таблиця систематизує ключові інформаційно-комунікаційні технології, які формують технологічну основу та інфраструктуру «розумного міста». У ній описано функціональну роль кожного рішення – від збору та швидкої передачі даних «розумного міста» за допомогою IoT-сенсорів і мереж 5G до їхнього масштабованого й оперативного аналізу через хмарні, туманні та периферійні обчислення. У таблиці 2.2 продовжено огляд ключових аналітичних та інтелектуальних технологій, які впливають на «розумні міста».

Таблиця 2.2 – Аналітичні та інтелектуальні технології «розумних міст»

Технологія	Опис
ШІ	Використовує ML, DL та NLP для прогнозування трафіку, енергоспоживання, управління відходами та безпеки «розумних міст». Підсилює аналітичне опрацювання та автоматизацію міських процесів [33].
Великі за обсягом набори та колекції даних та аналітичне опрацювання	Інтеграція даних із сенсорів, соцмереж та сервісів. Використання Hadoop, Spark, NoSQL для прогнозування заторів та «розумної» оптимізації транспортних маршрутів [33].
Семантичні технології	Використовують онтології та стандартизовані моделі для забезпечення інтероперабельності та аналітичне опрацювання даних «розумного міста» [32].
AR/VR	Використовуються для «розумного» планування міського простору, кризового управління та навчання. Підвищують залучення громадян [1].
Мобільне зондування (MCSC)	Використовує мобільні пристрої для збору даних про довкілля та транспорт, інтегрується з IoT для прийняття рішень в «розумному місті» [32].

Ця таблиця класифікує та описує передові аналітичні, візуалізаційні та інтеграційні технології, спрямовані на інтелектуальну обробку великих масивів інформації в концепції розумного міста. У ній висвітлено інструменти автоматизації, прогнозування міських процесів та залучення громадян — від штучного інтелекту й аналітики великих даних до семантичних моделей, мобільного зондування та віртуальної чи доповненої реальності.

У таблиці 2.3 доповнено огляд ключових нових технологій, які впливають на «розумні міста».

Таблиця 2.3 – Безпекові та енергетичні технології «розумних міст»

Технологія	Опис
Блокчейн	Забезпечує децентралізоване та захищене управління даними, підтримує смарт-контракти, цифрову ідентифікацію та енергетичні транзакції. Інтеграція з IoT та ШІ формує стійкі «розумні» інформаційно-технологічні системи [1].
Криптографія	Легкі алгоритми шифрування забезпечують захист даних у системах з обмеженими ресурсами, зокрема, «розумної» охорони здоров’я та хмарних сервісів [6].
Біометрія	Використовується для автентифікації у IoT-системах. Нові методи, як автентифікація за мозковими хвилями, підвищують надійність «розумних» систем [6].
Кібербезпека	Забезпечує захист цифрових систем «розумного міста» через ML, шифрування та блокчейн. Є критичною для довіри та стійкості «розумних» систем [32].
Відновлювана енергія	Використання сонячної, вітрової та біоенергії для зменшення викидів та підвищення енергетичної стійкості [1].
Інтелектуальні енергомережі	Інтегрують відновлювані джерела та системи зберігання, забезпечують ефективність та знижують ризики відключень «розумних» систем [33].

У табл. 2.3 систематизовано інструменти безпеки, конфіденційності та енергетичної стійкості, що гарантують надійну життєдіяльність урбаністичних екосистем. Текст акцентує увагу на двох критичних авангардах урбаністичної модернізації: технологіях комплексного кіберзахисту (блокчейн, криптографія, біометрія) та рішеннях для створення екологічної й автономної енергетичної інфраструктури (відновлювані джерела та інтелектуальні енергомережі). Носимі та транспортні технології «розумних міст» охарактеризовано в таблиці 2.4.

Таблиця 2.4 – Носимі та транспортні технології «розумних міст»

Технологія	Опис
ШІ	Використовує ML, DL та NLP для прогнозування трафіку, енергоспоживання, управління відходами та безпеки. Підсилює аналітичне опрацювання та автоматизацію «розумних» міських процесів [33].
БПЛА	Забезпечують моніторинг, картографію та підтримку екстрених служб. Використовуються у «розумних» транспорті, охороні довкілля та інфраструктурі [22].
Автономні системи	Роботи та дрони виконують завдання з транспорту, прибирання та моніторингу, підвищуючи ефективність «розумних» міських процесів [6].
Автономні транспортні засоби	Використовують сенсори та мережеві технології для оптимізації маршрутів, ride-sharing та безпілотного громадського транспорту «розумного міста» [1].
Носимі пристрої	Збирають біометричні дані для медицини та моніторингу здоров’я, інтегруються у системи «розумної» охорони здоров’я [6].

Цей перелік узагальнює технології інтелектуальної автоматизації та індивідуального моніторингу, які забезпечують перехід від статичного цифрового контролю до динамічного управління міським простором. Фокус уваги тут зміщено на роботизовані й безпілотні комплекси (ШІ, БПЛА, автономні системи та транспорт), що оптимізують логістику й інфраструктуру, а також на персоналізовані гаджети (носимі пристрої), які інтегрують потреби конкретного мешканця в загальну систему «розумної» охорони здоров'я.

2.2 Кібератаки, загрози та безпекові виклики в «розумних містах»

«Розумні міста» інтегрують IoT, ШІ і великі за обсягом набори та колекції даних для оптимізації сервісів, але водночас стають вразливими до кіберзагроз. Масове використання сенсорів, камер та мобільних застосунків створює ризики для приватності, зокрема через розпізнавання облич та непрозоре поширення даних [1]. Недостатній захист IoT-пристроїв спричинив атаки на критичну інфраструктуру, як у випадку «Oldsmar» в 2021р. чи «Mirai»-ботнету в 2016р., що доводить потребу у посиленні кіберзахисту [34].

Серед основних загроз – «ransomware» та «malware», які блокують або пошкоджують дані, як у Балтиморі в 2019р. та Атланті в 2018р. [24]. Важливими є також внутрішні загрози, коли співробітники навмисно чи випадково компрометують системи, як у випадку Tesla в 2018р. [25]. «Replay»-атаки та «MitM»-атаки надають можливість перехоплювати й змінювати дані у транспортних та енергетичних системах [35].

«DDoS»-атаки паралізують сервіси, як у Сан-Франциско в 2016р., де було зупинено роботу транспортної системи [34]. SQL-ін'єкції та «zero-day» експлойти відкривають доступ до баз даних і невідомих вразливостей [36]. Уразливості ланцюгів постачання, як у випадку «SolarWinds» в 2020р., демонструють небезпеку сторонніх компонентів [37].

Інші загрози – це «side-channel» атаки, що використовують фізичні характеристики пристроїв [1], APT-атаки, які забезпечують довготривалий

несанкціонований доступ, та «cryptojacking», що виснажує ресурси інфраструктури [7]. Також поширені «black hole», «gray hole», «sinkhole» та «wormhole» атаки, які порушують маршрутизацію даних [36].

Системи «розумного міста» вразливі до «Sybil»-атак, коли створюються фіктивні вузли [36], та «illusion»-атак, що вводять хибну інформацію [1]. «Sleep denial» та «fake node injection» виснажують IoT-сенсори й порушують роботу критичних сервісів [36]. «Buffer overflow» створює можливість виконання шкідливого коду [36].

Особливу небезпеку становлять атаки на смарт-мережі, «розумні» будівлі, «розумні» транспортні системи та хмарні платформи, які можуть призвести до відключень, витоку даних чи саботажу [6]. Навіть блокчейн не є повністю захищеним – прикладом є DAO-атака 2016 року [36].

Таким чином, кіберзагрози для «розумних міст» охоплюють широкий спектр – від технічних експлойтів до соціальної інженерії. Їхня спільна риса – здатність порушувати роботу критичних сервісів, підривати довіру та створювати ризики для безпеки громадян. Це вимагає комплексних рішень на основі ШІ, блокчейну та сучасних методів кіберзахисту.

2.3 Кібербезпека в «розумних містах»

Кібербезпека у «розумному місті» спрямована на захист цифрової інфраструктури, даних та систем від атак, що стають дедалі небезпечнішими через зростання використання IoT-пристроїв, сенсорів та систем на основі ШІ. Ці технології підвищують ефективність «розумного» транспорту, «розумної» енергетики, «розумної» охорони здоров’я та «розумного» управління відходами, але водночас створюють нові вразливості. Компрометація IoT-систем, як у випадку з атакою на Йоганнесбург у 2019 р., призводить до збоїв у постачанні електроенергії та води. Аналогічно, інцидент у Флориді (2020р.) показав, як хакери намагалися змінити хімічний склад води, що підкреслює потребу у надійних механізмах контролю доступу [1].

Хоча ШІ забезпечує прогнозну аналітику та підтримує прийняття рішень, він також може бути використаний для атак – від блокування систем відеоспостереження до внесення хибних даних у критичні сервіси. Тому «розумні міста» повинні впроваджувати багаторівневі стратегії захисту, що інтегрують моніторинг, шифрування та блокчейн-рішення для прозорого управління даними. Приклад Сінгапуру демонструє ефективність комплексних регуляторних рамок та суворих стандартів захисту даних [30].

Таким чином, кібербезпека у «розумному місті» є не лише технічним завданням, а й складовою міського управління, що потребує проактивних стратегій, оцінки ризиків та залучення громади для забезпечення безпечного використання новітніх технологій.

2.4 Принципи кібербезпеки в «розумних містах»

Захист «розумного міста» потребує дотримання базових принципів кібербезпеки:

– конфіденційності;
– цілісності;
– доступності;
– стійкості.

Вони гарантують надійність цифрової інфраструктури та безперервність «розумних» міських сервісів [36].

Конфіденційність забезпечує захист персональних і державних даних, що збираються сенсорами та смарт-лічильниками. Використання шифрування та багаторівневого контролю доступу запобігає порушенням приватності [38].

Цілісність даних є критичною для коректної роботи «розумних» енергомереж та «розумних» транспортних систем. Викривлення інформації може спричинити аварії чи перебої, тому застосовуються хешування та цифрові підписи для перевірки достовірності [36].

Доступність гарантує безперервну роботу критичних сервісів – від «розумної» медицини до «розумного» транспорту. Резервні системи та дублювання знижують ризики відмови, а регулярне тестування підвищує надійність [36].

Стійкість означає здатність швидко відновлювати функціонування після атак. Використання резервних протоколів та ручних механізмів дає можливість мінімізувати наслідки кіберінцидентів [1].

Таким чином, багаторівневі стратегії захисту, що інтегрують ШІ, блокчейн, шифрування та постійний моніторинг, є необхідними для безпечного функціонування «розумного міста» та збереження довіри громадян.

2.5 Послуги кібербезпеки в «розумних містах»

Кібербезпекові сервіси у «розумному місті» формують комплексну систему захисту, що охоплює три ключові напрями:

– превентивні заходи;

– захисні заходи;

– моніторингово-відповідні заходи.

Вони забезпечують стійкість цифрової інфраструктури та безперервність міських сервісів [28].

Превентивні сервіси використовують оцінку ризиків, тестування на проникнення та сканування вразливостей. Використання шифрування, контроль доступу та сучасні міжмережеві екрани з функціями IDS/IPS мінімізують площину атаки. Інтеграція ML-алгоритмів у системи виявлення загроз надає можливість ідентифікувати нові типи атак [28].

Захисні сервіси спрямовані на критичні системи – транспорт, енергетику, охорону здоров’я. Використовуються багатофакторна автентифікація, антивірусні рішення та системне оновлення. Ефективність забезпечує багаторівневий підхід, що гарантує цілісність і безпеку даних [38] використовує:

– антивіруси;

– міжмережеві екрани;

– IDS;

– шифрування (AES, end-to-end).

Таким чином, багаторівневі кіберзахисні стратегії, що поєднують ШІ, блокчейн, IDS/IPS та шифрування (див. рисунок 2.1), є основою безпечного функціонування «розумного міста» та підтримки довіри громадян [30].

Рисунок 2.1 – Структура послуг кібербезпеки в «розумних містах» [1]

Моніторинг та реагування базуються на реальному аналізі трафіку через SIEM-платформи та IDS. ШІ-моделі виявляють аномалії у поведінці користувачів, а безперервне сканування вразливостей знижує ризики атак. Важливими є плани реагування на інциденти, обмін загрозовою інформацією та відновлення сервісів після атак, що забезпечує стійкість критичної інфраструктури [38].

2.6 Важливість кібербезпеки в «розумних містах»

Інтеграція новітніх технологій у «розумному місті» потребує розвинених механізмів кіберзахисту, що гарантують безпеку даних, інфраструктури та сервісів. Захист персональної та операційної інформації запобігає фінансовим втратам і порушенню приватності, а використання шифрування та контролю доступу забезпечує конфіденційність і цілісність даних [38]. Регулярні аудити та оновлення систем знижують ризики атак [1].

Кібербезпека підтримує безперервність бізнес-процесів і функціонування критичних сервісів:

– «розумного» транспорту;

– «розумної» енергетики;

– «розумної» охорони здоров’я.

Дотримання міжнародних стандартів (GDPR, NIST, ISO/IEC 27001) зміцнює довіру та зменшує юридичні ризики [1]. Прозора політика використання даних підвищує залучення громадян до цифрових сервісів [38].

Захист інфраструктури – енергомереж, водопостачання, транспорту – базується на багаторівневих інформаційно-технологічних архітектурах, моніторингу та блокчейн-рішеннях, що забезпечують прозорість і стійкість [1]. Використання ШІ та ML дає змогу виявляти аномалії та прогнозувати загрози, а блокчейн мінімізує ризики маніпуляцій [1].

Особливу увагу приділяють IoT-пристроям, які розширюють площину атак. Їхній захист потребує:

– регулярних оновлень;

– автентифікації;

– безпечних протоколів [39].

Важливими є також плани реагування на інциденти, автоматизовані системи відновлення та співпраця державного й приватного секторів [40].

Захист цифрових ідентичностей громадян забезпечується блокчейн-технологіями, багатофакторною автентифікацією та біометрією, що

підвищує довіру до міських сервісів. У сфері «розумної» охорони здоров'я застосовуються наскрізне шифрування та аудит IoT-пристроїв для захисту медичних даних [38].

Таким чином, кібербезпека у «розумному місті» є фундаментом сталого розвитку, що поєднує ШІ, ML та блокчейн для захисту критичних систем, підтримки інновацій та формування довіри громадян [1].

2.7 Технологічний прогрес у кібербезпеці «розумних міст»

Технологічні досягнення у сфері кібербезпеки відіграють ключову роль у захисті «розумного міста», що функціонує на основі взаємопов'язаних пристроїв та систем. Захист великих за обсягом наборів та колекцій даних є необхідним для запобігання атакам, які можуть порушити роботу «розумного» транспорту, «розумної» енергетики чи «розумної» охорони здоров'я [35].

Шифрування (AES, RSA) забезпечує конфіденційність даних, а дослідження спрямовані на вдосконалення управління ключами та створення гібридних моделей. Розвиток квантових технологій актуалізує пост-квантову криптографію та квантовий розподіл ключів, що гарантує довгострокову стійкість систем [1].

IDPS здійснюють моніторинг мережевого трафіку у режимі реального часу, використовуючи сигнатурні та аномальні методи для виявлення атак. Інтеграція ML підвищує здатність систем адаптуватися до нових загроз [41].

SIEM-системи збирають дані з різних джерел, забезпечують відповідність стандартам (GDPR, HIPAA) та підвищують довіру громадян. Використання ML дає можливість швидше виявляти аномалії та реагувати на інциденти [20].

Захист кінцевих пристроїв (ноутбуки, смартфони, IoT-пристрої) базується на багаторівневих стратегіях, що застосовують поведінковий аналіз та моніторинг мереж [1]. Міжмережеві екрани нового покоління поєднують фільтрацію пакетів із виявленням вторгнень, блокуючи несанкціонований доступ та забезпечуючи безпеку критичних сервісів [38].

«Honeypot»-системи створюють пастки для атакувальників, надаючи можливість аналізувати їхні методи та підвищувати рівень захисту у сферах «розумної» енергетики, «розумної» охорони здоров’я та «розумної» індустрії [42]. Багатофакторна автентифікація (MFA) зміцнює захист цифрових сервісів «розумного міста», знижуючи ризик несанкціонованого доступу та підвищуючи довіру громадян [39].

Зростання використання хмарних рішень у «розумному місті» потребує розвинених механізмів захисту. Cloud-брокери доступу реалізують політики безпеки, а шифрування даних у стані зберігання та передачі гарантує їхню конфіденційність. Формування комплексних хмарних стратегій убезпечення «розумних міст» забезпечує відповідність регуляторним стандартам [43].

Інтеграція ШІ та ML у кіберзахист дає змогу здійснювати проактивне виявлення загроз та автоматизацію реагування. Поведінкові шаблони аналізують та підвищують точність прогнозування атак [40], зокрема алгоритми класифікації:

– K-найближчих сусідів;
– дерева рішень;
– випадкові ліси;
– екстремальне градієнтне бустування.

Квантовий розподіл ключів (QKD) забезпечує захищену комунікацію, виявляючи спроби перехоплення. Попри високу вартість обладнання, ця технологія є перспективною для «розумного» транспорту, «розумної» медицини та «розумної» громадської безпеки [26].

Блокчейн застосовується для децентралізованого управління ідентичностями та безпечних транзакцій, знижуючи ризики централізованого зберігання даних [24]. DMZ-мережі ізолюють внутрішні системи від зовнішніх загроз, як у проєкті Aspern, забезпечуючи захист критичних ресурсів [42].

Платформи кіберрозвідки інтегруються з IDS, міжмережевими екранами та системами кінцевого захисту, автоматично оновлюючи політики безпеки та

допомагаючи у пріоритизації патчів. Обмін даними між «розумними містами» посилює колективний захист [44].

Таким чином, сучасні технології – ШІ, ML, блокчейн, квантове шифрування та хмарні рішення – формують основу кіберзахисту «розумного міста», забезпечуючи його стійкість та безпечний розвиток.

2.8 Висновок до другого розділу

В другому розділі кваліфікаційної роботи досліджено новітні технології в «розумних містах». Описано кібератаки, загрози та безпекові виклики в «розумних містах». Розглянута кібербезпека в «розумних містах». Сформовано принципи кібербезпеки в «розумних містах». Описано послуги кібербезпеки в «розумних містах». Досліджено важливість кібербезпеки в «розумних містах». Проаналізовано технологічний прогрес у кібербезпеці «розумних міст».

РОЗДІЛ 3. ПРАКТИЧНІ АСПЕКТИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ТА БЛОКЧЕЙНУ ДЛЯ КІБЕРБЕЗПЕКИ «РОЗУМНИХ МІСТ»

3.1 Застосування штучного інтелекту в кібербезпеці «розумних міст»

ШІ відіграє ключову роль у кіберзахисті «розумного міста», забезпечуючи захист критичної інформації та інфраструктури. Інтеграція ШІ дає можливість аналізувати мережеву активність у режимі реального часу, швидко виявляти аномалії та реагувати на інциденти, що підвищує стійкість «розумного» транспорту, «розумної» енергетики та «розумної» медицини [37].

Автоматизовані системи реагування (SOAR) ізолюють уражені пристрої, блокують несанкціонований доступ та відновлюють сервіси, зменшуючи час реагування та навантаження на персонал. Алгоритми ШІ також оптимізують системи відеоспостереження, використовуючи розпізнавання облич та поведінковий аналіз для підвищення громадської безпеки.

У сфері управління доступом ШІ інтегрує біометричну автентифікацію (відбитки, обличчя, голос), адаптивний контроль прав та моніторинг логів, що забезпечує відповідність регуляторним вимогам і довіру громадян [1].

Точність виявлення шкідливого ПЗ та фішингових атак підвищують ML-алгоритми:

– дерева рішень;
– випадкові ліси;
– KNN;
– XGBoost.

NLP аналізує електронні повідомлення для блокування небезпечних листів [37]. Для захисту персональних даних ШІ також:

– оптимізує криптографічні протоколи;
– автоматизує управління ключами;

– застосовує методи диференційної приватності.

У фінансових системах ШІ виявляє шахрайські транзакції в режимі реального часу, а у сфері критичної інфраструктури – моніторить «розумні» сенсори та системи управління, прогнозуючи ризики DDoS-атак і шкідливих програм [1]. Таким чином, застосування ШІ у кіберзахисті «розумного міста» забезпечує проактивне виявлення загроз, автоматизацію реагування та захист даних, формуючи основу безпечного й стійкого розвитку урбаністичних систем (див. рисунок 3.1).

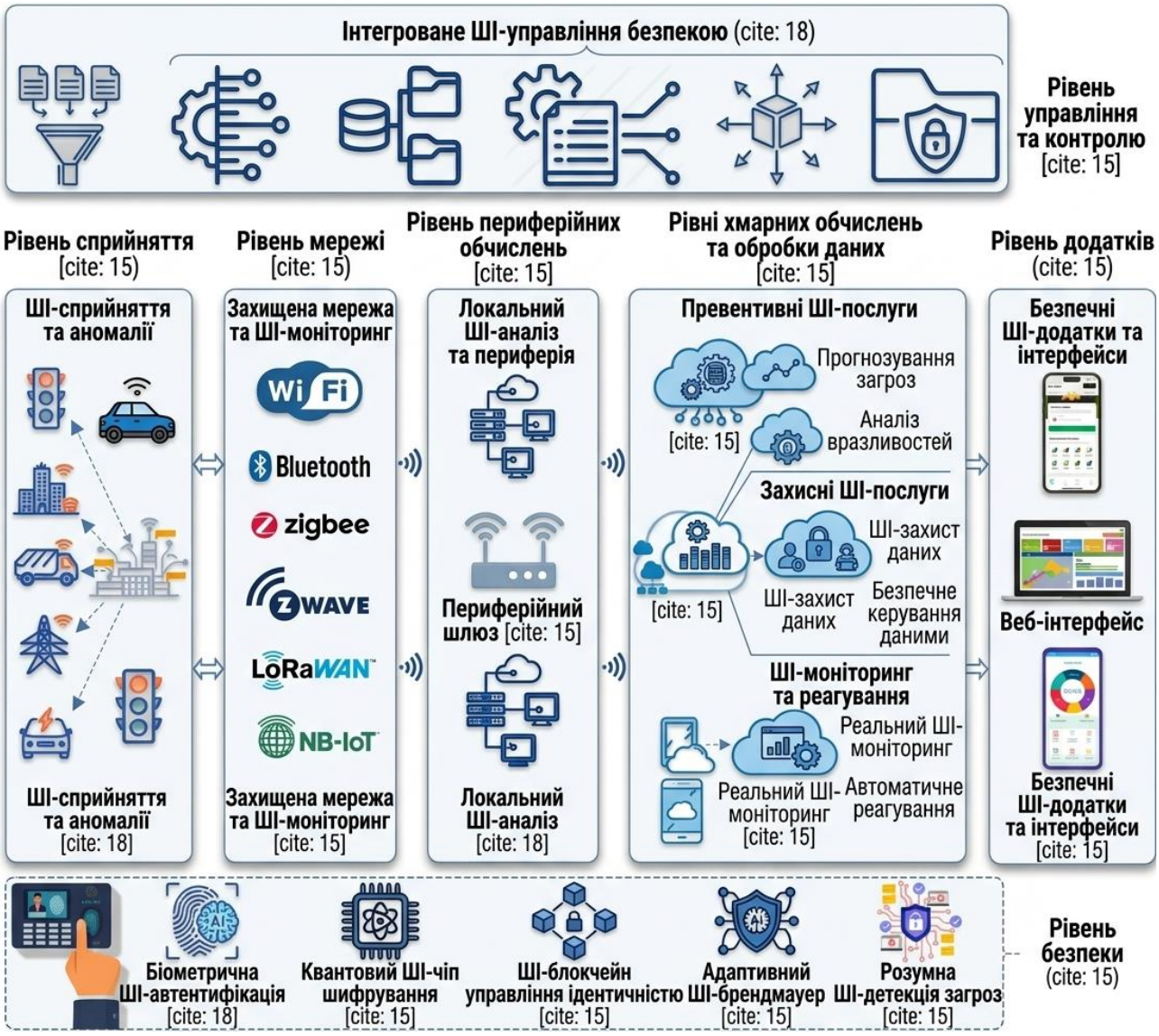

Рисунок 3.1 – Застосування штучного інтелекту в кібербезпеці «розумних міст»

ШІ суттєво трансформує кіберзахист «розумного міста», забезпечуючи проактивне виявлення вразливостей та автоматизацію тестування. Інструменти на основі ШІ виконують сканування, моделюють атаки та формують рекомендації для усунення ризиків, що підвищує стійкість міських систем [37]. Важливим напрямом є навчання персоналу, де ШІ-платформи моделюють реалістичні інциденти, наприклад, фішинг, атаки на сервіси, надаючи можливість відпрацьовувати реакції та підвищувати компетентність співробітників. Це формує підготовленішу команду кіберзахисту.

Захист кінцевих пристроїв (ноутбуки, смартфони, IoT-пристрої) здійснюється через поведінковий аналіз застосунків та процесів. Системи блокують несанкціонований доступ чи шкідливі дії у режимі реального часу [37]. ШІ також удосконалює автентифікацію, використовуючи поведінкову біометрію – швидкість набору, рухи миші, взаємодію з сенсором. Це забезпечує адаптивний контроль доступу та підвищує точність перевірки користувачів [37].

У сфері IoT ШІ моніторить пристрої, виявляє аномальні комунікації та ізолює скомпрометовані вузли, що знижує ризики атак. Він також виявляє APT-атаки, які залишаються непомітними тривалий час, аналізуючи відхилення у доступі до даних [37]. Інтеграція ШІ у SIEM-системи підвищує ефективність пошуку прихованих загроз, корелюючи події у великих за обсягом наборах та колекціях даних. Це дає аналітикам змогу діяти проактивно та скорочує час реагування [37].

Таким чином, ШІ забезпечує багаторівневий захист «розумного міста» – від виявлення вразливостей до автоматизації реагування, що формує основу його безпечного та стійкого розвитку.

3.2 Застосування блокчейну в кібербезпеці «розумних міст»

Блокчейн є ключовим інструментом кіберзахисту «розумного міста» завдяки децентралізованій та незмінній інформаційно-технологічній

архітектурі, що забезпечує цілісність даних, прозорість транзакцій та захист від несанкціонованих змін [8]. Його інтеграція у міську інфраструктуру підвищує довіру та відповідальність у сфері управління інформацією (див. рисунок 3.2).

Рисунок 3.2 – Застосування блокчейну в кібербезпеці «розумних міст»

Технологія зміцнює цілісність даних, даючи можливість безпечний обмін між сервісами, правоохоронними органами та медициною. Вона захищає медичні записи й фінансові транзакції, а також підвищує прозорість ланцюгів постачання, зменшуючи ризики підробок [7].

Децентралізовані цифрові ідентичності забезпечують контроль користувачів над власними даними, знижуючи ризик крадіжки та усуваючи єдині точки відмови. Це формує безпечну інформаційно-технологічну систему автентифікації у «розумному місті».

У сфері IoT блокчейн автентифікує пристрої, шифрує канали зв’язку та блокує несанкціонований доступ, що підвищує стійкість «розумної» інфраструктури [1].

Смарт-контракти автоматизують процеси – від комунальних платежів до управління транспортом, зменшуючи ризики шахрайства та забезпечуючи прозорість. Вони можуть виконувати протоколи безпеки, наприклад, блокування несанкціонованого доступу.

Захист критичної «розумної» інфраструктури посилюється завдяки децентралізації та моніторингу у режимі реального часу, що надає можливість швидко реагувати на загрози [1].

Блокчейн також забезпечує безпечні цифрові платежі, токенізацію активів та прозорість у фінансових операціях, сприяючи економічному розвитку. У сфері електронного голосування він гарантує незмінність результатів та прозорість виборчого процесу [31].

«Розумне» управління ланцюгами постачання та логістикою стає ефективнішим завдяки відстеженню походження та маршруту товарів у режимі реального часу, що знижує ризики шахрайства та підвищує довіру до міських сервісів. У «розумному місті» питання володіння даними та захисту інтелектуальної власності набувають особливої ваги. Блокчейн забезпечує контроль доступу до інформації, створює незмінні записи власності та запобігає несанкціонованому використанню, формуючи безпечне середовище для інновацій [8].

У сфері охорони здоров’я технологія гарантує захищене управління електронними медичними записами (EHR), доступ лише для авторизованих користувачів та безпечну взаємодію між медичними пристроями, що підвищує якість лікування та довіру пацієнтів [45].

Блокчейн зміцнює комунікаційну безпеку, використовуючи криптографію з відкритим ключем для захисту повідомлень від атак типу MitM, забезпечуючи конфіденційність обміну [46]. У протидії DDoS-атакам децентралізований розподіл трафіку між вузлами ускладнює перевантаження системи, блокуючи шкідливі запити [46]. Технологія створює прозорий журнал подій, що дає змогу швидше проводити розслідування інцидентів та відновлювати хронологію атак [1]. У хмарних сервісах блокчейн забезпечує контроль доступу до даних,

зберігаючи їхню конфіденційність та запобігаючи несанкціонованому використанню [46].

Таким чином, блокчейн підвищує рівень кіберзахисту «розумного міста», вирішуючи проблеми витоків даних, слабкої автентифікації, шахрайства та вразливостей IoT-пристроїв, формуючи надійну цифрову інфраструктуру.

3.3 Інтеграція штучного інтелекту та блокчейну для кібербезпеки в «розумних містах»

Інтеграція ШІ та блокчейну посилює кіберзахист «розумного міста», що функціонує на основі взаємопов'язаних систем. Ці технології протидіють витокам даних, шахрайству та атакам на критичну інфраструктуру. ШІ аналізує великі за обсягом масиви інформації для виявлення аномалій, а блокчейн забезпечує прозору та незмінну інформаційно-технологічну архітектуру захисту [8].

ШІ та блокчейн у виявленні загроз – алгоритми моніторять трафік IoT-пристроїв, а дані про інциденти фіксуються у блокчейні, що гарантує їхню цілісність та доступ лише для авторизованих користувачів [1].

Смарт-контракти автоматизують протоколи безпеки, ізолюючи скомпрометовані мережі чи блокуючи доступ. Інтеграція ШІ дає можливість динамічно оновлювати контракти відповідно до нових загроз [25]. Управління ідентичностями базується на децентралізованих цифрових профілях у блокчейні, що знижує ризик крадіжки даних (див. рисунок 3.3). ШІ застосовує біометричну автентифікацію та поведінковий аналіз для виявлення аномальних дій [1].

Захист даних та інфраструктури забезпечується записом сенсорної інформації у блокчейні та її аналізом ШІ. Це мінімізує ризики підробки та підвищує довіру до рішень міського управління [40].

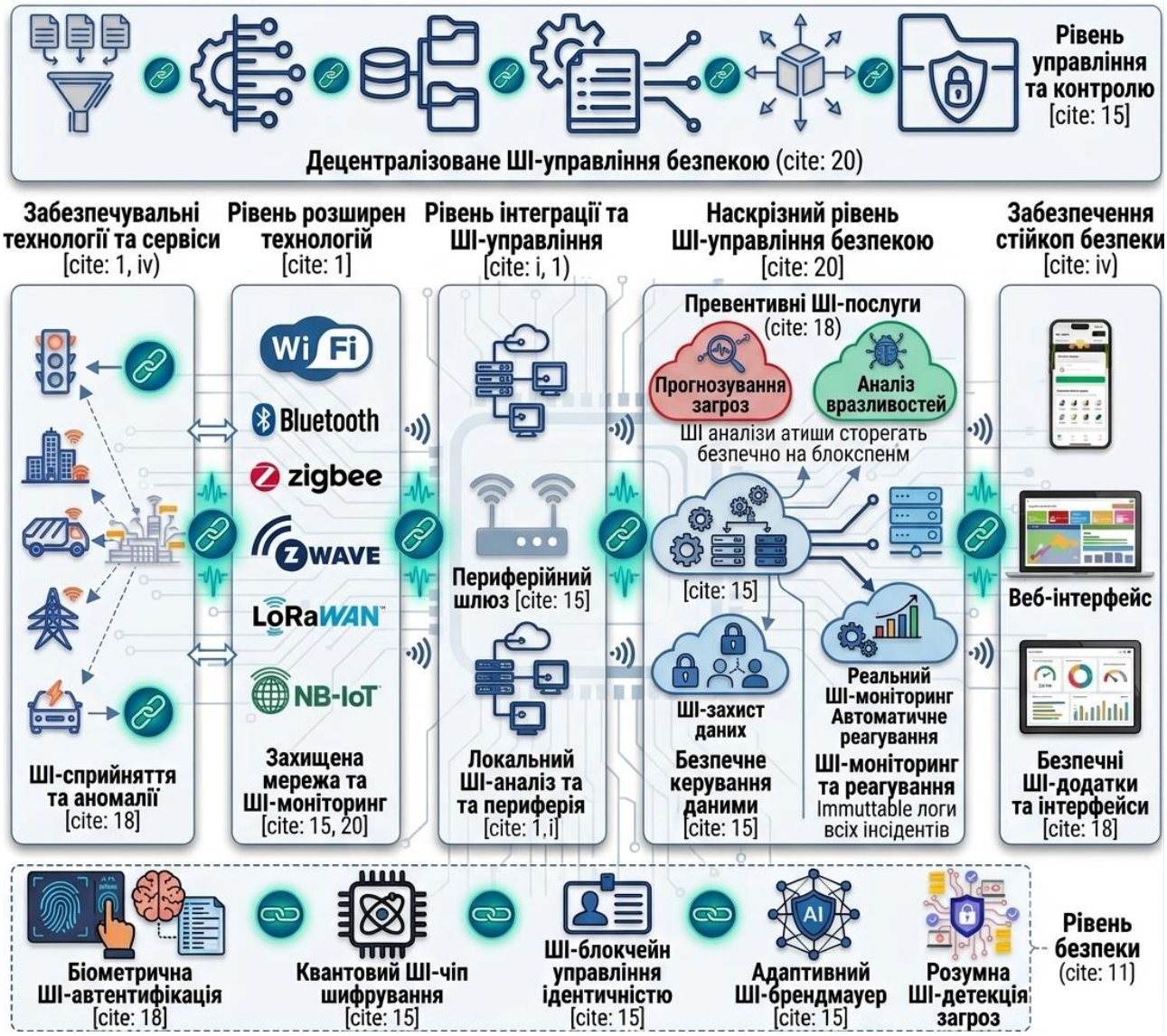

Рисунок 3.3 – Інтеграція штучного інтелекту та блокчейну для кібербезпеки в «розумних містах»

IoT-мережі отримують додатковий рівень захисту завдяки блокчейн-шифруванню та автентифікації пристроїв, тоді як ШІ виявляє аномальні комунікації та потенційні атаки [30].

Таким чином, поєднання ШІ та блокчейну формує багаторівневу систему кіберзахисту «розумного міста», що забезпечує стійкість, прозорість та довіру громадян до цифрових сервісів.

Інтеграція ШІ та блокчейну посилює кіберзахист «розумного міста», забезпечуючи ефективність, прозорість та стійкість цифрових систем. ШІ оптимізує методи консенсусу, підвищує швидкість транзакцій, знижує

енергоспоживання та виявляє шахрайські дії, тоді як блокчейн гарантує незмінність даних і довіру користувачів [26].

У сфері захисту даних ШІ анонімізує конфіденційну інформацію перед її збереженням у блокчейні, забезпечуючи безпечний обмін та відповідність регуляторним вимогам. Смарт-контракти надають можливість здійснювати контрольований обмін даними у сфері «розумної» медицини чи «розумного» транспорту, а ШІ моніторить політики доступу [38].

Виявлення шахрайства здійснюється ML-алгоритмами, що аналізують транзакції, тоді як блокчейн зберігає результати у незмінному реєстрі, забезпечуючи прозорість та доказовість [25].

Прогнозна аналітика на основі ШІ дає змогу передбачати кіберзагрози, а блокчейн забезпечує швидке реагування та захист критичних сервісів. Це формує довіру громадян до цифрових систем [38].

З огляду на розвиток квантових технологій, ШІ бере участь у створенні пост-квантових криптографічних алгоритмів, сумісних із блокчейном, що гарантує стійкість у майбутньому [35]. У режимі реального часу ШІ аналізує дані «розумних» транспортних систем, «розумних» енергомереж та комунікацій, виявляючи аномалії, тоді як блокчейн зберігає результати у незмінному вигляді, забезпечуючи прозорість та відповідальність [30].

У протидії DDoS-атакам блокчейн розподіляє навантаження між вузлами, а ШІ визначає джерело атаки та перенаправляє трафік на безпечні канали [46].

Таким чином, поєднання ШІ та блокчейну створює багаторівневу систему захисту «розумного міста», що забезпечує стійкість критичної інфраструктури та довіру громадян до цифрових сервісів.

Поєднання ШІ та блокчейну посилює кіберзахист «розумного міста», забезпечуючи прозорість, відповідальність та ефективність управління. ШІ здійснює моніторинг міських операцій для дотримання регуляторних вимог, тоді як блокчейн формує незмінний журнал дій, що спрощує аудит та знижує ризики корупції у централізованих системах [38]. Це поєднання зміцнює довіру

громадян та узгоджує цифрове управління з правовими й етичними стандартами [43].

ШІ підвищує швидкість виявлення загроз, адаптує заходи захисту та автоматизує реагування, тоді як блокчейн забезпечує безпечне управління даними та захист ідентичностей через децентралізовану інформаційно-технологічну архітектуру. Разом вони формують стійку систему кіберзахисту, що охоплює публічні сервіси, інфраструктуру та приватність громадян, протидіючи сучасним кіберзагрозам.

Таким чином, інтеграція ШІ та блокчейну створює багаторівневий захисний каркас «розумного міста», який забезпечує його безпечний розвиток та довіру суспільства.

3.4 Перспективи майбутніх досліджень для убезпечення «розумних міст»

Сучасні дослідження демонструють перспективність інтеграції ШІ та блокчейну у кіберзахист «розумного міста». Ці технології забезпечують підвищення рівня приватності, цілісності даних та стійкості інфраструктури.

Приватність та захист даних: застосування федеративного навчання, диференційної приватності та «zero-knowledge» доказів у поєднанні з блокчейном дає можливість здійснювати безпечний обмін інформацією без розкриття деталей. Це створює прозоре середовище для міських сервісів [44].

Персоналізовані моделі безпеки: ШІ адаптує протоколи до поведінки користувачів, а блокчейн забезпечує контроль доступу через незмінні записи, що підвищує довіру громадян [44].

Масштабованість та енергоефективність: майбутні дослідження мають зосередитися на легких блокчейн-архітектурах, консенсус-алгоритмах (Proof-of-Stake, DAG), шарових рішеннях та шардінгу для зниження витрат і підвищення швидкості транзакцій.

Правові та етичні аспекти – необхідно створювати стандартизовані рамки для сумісності та захисту даних, враховуючи регуляції на кшталт Європейського AI Act, що забезпечить прозорість та відповідальність [1].

Аналіз поведінки та виявлення шахрайства: ШІ формує динамічні профілі безпеки, виявляє аномалії та шахрайські дії, а блокчейн гарантує незмінність даних, підвищуючи довіру до цифрових сервісів.

Енергоефективні протоколи – інтеграція відновлюваних джерел енергії для роботи ШІ-вузлів та блокчейну сприятиме сталому розвитку міських систем.

Хмарні середовища – гібридні моделі ШІ-блокчейн забезпечують захист даних у мультихмарних інфраструктурах, створюючи єдиний рівень безпеки.

Пост-квантова криптографія та QKD – розвиток квантостійких алгоритмів та інтеграція протоколів квантового розподілу ключів є критично важливими для захисту IoT-пристроїв та чутливих даних [26].

Легкі криптографічні рішення та гомоморфне шифрування – дослідження спрямовані на оптимізацію захисту IoT-пристроїв та безпечну обробку зашифрованих даних у режимі реального часу [26].

Таким чином, інтеграція ШІ та блокчейну формує основу кіберзахисту «розумного міста», забезпечуючи масштабованість, приватність та стійкість до новітніх загроз. Подальші дослідження мають зосередитися на енергоефективності, правових стандартах та квантостійких рішеннях для довготривалої безпеки.

У сучасних умовах «розумне місто» стає центром урбаністичного розвитку, використовуючи цифрові технології для підвищення якості життя та ефективності управління. Проте зростаюча взаємозалежність систем створює нові кіберзагрози, що ставить під сумнів захист даних, приватності та цілісності критичних сервісів.

ШІ забезпечує оперативну обробку великих за обсягом масивів інформації, виявлення аномалій та прогнозування ризиків, що підвищує ефективність реагування на атаки. Блокчейн гарантує децентралізоване та

незмінне збереження транзакцій і даних, забезпечуючи прозорість та стійкість до маніпуляцій. Їхня інтеграція формує багаторівневу систему захисту, яка поєднує прогнозні можливості ШІ з надійністю блокчейн-реєстру, зменшуючи вразливості та зміцнюючи довіру громадян [38].

Водночас існують виклики, пов’язані з масштабованістю, сумісністю та етичними аспектами використання цих технологій. Питання ресурсомісткості, приватності та регуляторних вимог потребують подальших досліджень і співпраці між урядами, бізнесом та науковцями.

Отже, інтеграція ШІ та блокчейну пропонує перспективні рішення для кіберзахисту «розумного міста», забезпечуючи інноваційні та стійкі підходи до захисту цифрової трансформації урбаністичних систем. Їхнє подальше вдосконалення та регульоване впровадження є критично важливими для формування безпечних і інтелектуальних міських інформаційно-технологічних систем.

3.5 Висновок до третього розділу

В третьому розділі кваліфікаційної роботи розглянуто застосування штучного інтелекту в кібербезпеці «розумних міст». Проаналізовано застосування блокчейну в кібербезпеці «розумних міст». Досліджено інтеграцію штучного інтелекту та блокчейну для кібербезпеки в «розумних містах». Описано перспективи майбутніх досліджень для убезпечення «розумних міст».

РОЗДІЛ 4. БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Організація оповіщення і зв'язку у надзвичайних ситуаціях техногенного та природного характеру

Автоматизовані «розумні» інженерні мережі, попри високу ефективність, підвладні впливу зовнішніх чинників: пошкодженням магістралей, знеструмленням, природним катаклізмам чи промисловим катастрофам. За таких умов оперативне сповіщення жителів та профільних підрозділів дозволяє запобігти критичним наслідкам, як-от критичному зниженню температури у приміщеннях або загрозі здоров'ю людей через витоки теплоносія чи газу. За відсутності відпрацьованих каналів комунікації навіть найбільш технологічна інфраструктура не здатна гарантувати захист і належні умови для населення у кризовий період. Нормативно-правове підґрунтя для розгортання інформаційних систем у разі загрози або розгортання небезпечних подій базується на вітчизняному законодавстві. Сюди належать Основний Закон України, Кодекс цивільного захисту України, урядові постанови, які регулюють положення про організацію сповіщення та функціонування єдиної державної системи цивільного захисту, а також розпорядження профільних міністерств, відомств та обласних органів влади.

До першочергових завдань державної системи цивільного захисту, що об'єднує органи управління та відповідні ресурси, належить негайне доведення до відома громадян інформації про небезпеку як у мирний час, так і в умовах воєнного стану, разом із безперервним висвітленням поточних умов життєдіяльності.

Комплекс централізованого інформування становить собою сукупність організаційних заходів, апаратно-технічних інструментів, каналів передачі даних, а також мереж дротового, радіо- та телевізійного мовлення. Головною метою цієї структури є своєчасне розповсюдження сигналів цивільного захисту серед органів влади, підприємств, організацій та безпосередньо населення [47].

Для привернення уваги суспільства перед трансляцією повідомлень застосовуються акустичні сирени, звук яких є загальноприйнятим попередженням «УВАГА ВСІМ».

Загальна архітектура обміну даними охоплює загальнодержавний, обласний та об’єктовий рівні, а також системи групового виклику, які забезпечують зв’язок із:

– черговими підрозділами міністерств та відомств через службові телефонні лінії;

– диспетчерськими службами місцевих органів самоврядування;

– оперативними рятувальними загонами.

Ключові орієнтири інформаційної взаємодії полягають у забезпеченні швидкого обміну даними між інституціями управління, попередженні про загрозу радіоактивного, хімічного чи біологічного зараження, а також у постійному супроводі актуальними відомостями про стан середовища.

Робота механізму базується на використанні виділених каналів загальнонаціональної мережі зв’язку. Спеціальне обладнання розгортається на об’єктах телекомунікацій, у чергових частинах правоохоронних органів, на радіо- та телепередавальних станціях. Для швидкого зв’язку з керівництвом застосовуються блоки групового з’єднання та пристрої автоматичного багатоканального зв’язку.

Трансляція сигналу «УВАГА ВСІМ» реалізується через мережу електричних сирен, які можуть запускатися як централізовано, так і в автономному режимі. Подальші деталі надсилаються громадянам через вузли дротового мовлення, вуличні гучномовці, а також визначені телевізійні та радіомовні канали.

На об’єктах із підвищеним рівнем небезпеки створюються локальні та об’єктові системи за рахунок коштів самих підприємств, якщо зона ймовірного ураження від аварії здатна досягти житлових секторів чи суміжних організацій. До структури таких локальних вузлів входять гучномовці, блоки дистанційного

пуску сирен, пристрої колективного виклику та заздалегідь підготовлені аудіозаписи зі зверненнями до громадян.

Постійна працездатність зазначених систем досягається шляхом реалізації таких кроків:

– організації цілодобового моніторингу та чергування персоналу;

– створення прямих ліній зв’язку між диспетчерами підприємств та обласними пунктами управління цивільного захисту чи підрозділами внутрішніх справ;

– регулярного навчання та підготовки персоналу до дій у кризових умовах;

– інтеграції автоматизованих комплексів на основі новітніх технологічних рішень;

– проведення планового технічного обслуговування комунікаційного устаткування.

Суворо заборонено проводити відключення ліній зв’язку, що забезпечують запуск засобів оповіщення, або демонтувати вуличні гучномовці без узгодження з відповідальними структурами.

Надійна координація дозволяє оперативно надавати населенню інструкції щодо необхідних дій (наприклад, перекриття інженерних комунікацій, знеструмлення приладів, евакуаційні заходи) та інформувати про терміни проведення ремонтних робіт в «розумних» мережах постачання ресурсів [48]. Стабільна взаємодія між комунальними службами та аварійними підрозділами гарантує швидке виявлення дефектів та усунення несправностей. Це знижує тривалість простою обладнання, нівелює матеріальні втрати та запобігає загрозам для життєдіяльності міста. З огляду на це, впровадження таких інструментів у структуру сучасного житлового сектора є фундаментом його стійкості та безпеки.

Без належної побудови інформаційних каналів навіть найновіші системи теплопостачання стають незахищеними перед раптовими технічними чи природними викликами.

4.2 Професійне вигорання фахівців у сфері інформаційних технологій

Професійне вигорання фахівців у сфері інформаційних технологій є важливим фактором, який може негативно впливати на ефективність та надійність систем, що забезпечують функціонування «розумних міст». Створення, впровадження та супровід технологій штучного інтелекту і блокчейну потребують високого рівня професійної підготовки, значної концентрації уваги та постійного оновлення знань. Тривале розумове навантаження, робота в умовах жорстких термінів і відповідальність за безперервне функціонування критично важливих інформаційних систем часто стають причинами накопичення стресу та виснаження працівників.

У результаті тривалого впливу несприятливих чинників у спеціалістів може спостерігатися зниження мотивації, погіршення здатності до аналізу інформації та прийняття рішень. У такому стані зростає ймовірність виникнення помилок під час розроблення програмного забезпечення, налаштування цифрових платформ та аналізу даних. Це може призвести до зниження рівня інформаційної безпеки, порушення стабільності роботи систем штучного інтелекту та втрати ефективності механізмів захисту, які використовуються в інфраструктурі «розумного міста».

Наслідки професійного вигорання позначаються не лише на роботі окремого працівника, а й на діяльності всього колективу. Виснажені співробітники менш ефективно взаємодіють між собою, що ускладнює спільне вирішення складних завдань та уповільнює процеси впровадження нових технологічних рішень. Крім того, зростає ризик виникнення конфліктних ситуацій та знижується загальна продуктивність команди. За таких умов можуть виникати труднощі під час модернізації цифрових систем, усунення несправностей та забезпечення належного рівня кіберзахисту міської інфраструктури.

Синдром професійного вигорання являє собою стан фізичного, психологічного та емоційного виснаження, який формується внаслідок

тривалого впливу стресових чинників у професійній діяльності. У сфері інформаційних технологій ця проблема є особливо актуальною через швидкий розвиток технологій, необхідність постійного навчання та високий рівень відповідальності за результати роботи.

До основних причин виникнення професійного вигорання серед фахівців інформаційної галузі належать:

– надмірне робоче навантаження та систематична понаднормова зайнятість;

– високі вимоги до якості виконання завдань і необхідність підтримувати безперервну роботу інформаційних систем;

– тривале виконання однотипних функцій, що знижує зацікавленість у роботі;

– недостатній баланс між професійною діяльністю та особистим життям;

– обмежені можливості для живого спілкування та соціальна ізоляція під час дистанційної роботи [49].

Найбільш поширеними наслідками професійного вигорання є:

– зниження продуктивності праці та творчої активності працівників;

– збільшення кількості помилок під час виконання професійних обов’язків;

– погіршення фізичного та психоемоційного стану;

– втрата інтересу до професійного розвитку та вдосконалення навичок;

– підвищення рівня плинності кадрів у організаціях;

– розвиток безсоння, депресивних станів та серцево-судинних порушень [50].

Для запобігання професійному вигоранню доцільно впроваджувати комплекс організаційних та психологічних заходів, серед яких:

– раціональне планування робочого часу та недопущення надмірних навантажень;

– проведення навчальних заходів, спрямованих на підвищення стійкості до стресу;

– створення сприятливої атмосфери в колективі та підтримка командної взаємодії;

– заохочення працівників до ведення здорового способу життя;

– забезпечення належного балансу між роботою та відпочинком шляхом використання гнучких режимів праці.

Професійне вигорання є серйозною проблемою для сфери інформаційних технологій, оскільки воно негативно впливає як на працівників, так і на діяльність організацій загалом [51]. Зниження працездатності персоналу, погіршення якості виконання завдань та збільшення кількості помилок можуть створювати додаткові ризики для інформаційної безпеки та стабільності функціонування цифрових систем.

У контексті використання технологій штучного інтелекту та блокчейну для убезпечення «розумних міст» особливого значення набуває підтримка належного психологічного стану фахівців. Саме від їхньої компетентності, уважності та професійної відповідальності залежить ефективність роботи систем аналізу даних, виявлення загроз, захисту інформації та забезпечення цілісності цифрових записів. Тому створення комфортних умов праці, підтримка професійного розвитку та впровадження програм психологічної допомоги є важливими складовими забезпечення надійності міської цифрової інфраструктури.

Крім того, професійне вигорання може спричинити втрату досвідчених працівників, що негативно впливає на збереження накопичених знань і практичного досвіду в організації. Заміна таких спеціалістів потребує додаткових витрат часу та ресурсів на підготовку нових кадрів, що уповільнює розвиток і вдосконалення технологічних рішень. Таким чином, запобігання професійному вигоранню слід розглядати як один із важливих напрямів забезпечення довгострокової стабільності, безпеки та ефективності систем штучного інтелекту і блокчейну, які використовуються для захисту та розвитку «розумних міст».

4.3 Висновок до четвертого розділу

В четвертому розділі кваліфікаційної роботи описано організацію оповіщення і зв’язку у надзвичайних ситуаціях техногенного та природного характеру. Розглянуто професійне вигорання фахівців у сфері інформаційних технологій.

ВИСНОВКИ

Комплексне застосування технологій штучного інтелекту та блокчейну сприяє підвищенню рівня кібербезпеки «розумних міст» завдяки своєчасному виявленню загроз, забезпеченню цілісності даних, підвищенню прозорості інформаційних процесів і стійкості міської цифрової інфраструктури до сучасних кіберризиків.

В першому розділі кваліфікаційної роботи освітнього рівня «Бакалавр»:

– Подано передумови використання штучного інтелекту та блокчейну для забезпечення безпеки розумних міст.

– Висвітлена методика систематичного аналізу наукових джерел щодо кіберзахисту «розумних міст».

– Розглянуто концептуальні основи побудови та функціонування «розумних міст».

– Описана еволюція «розумних міст».

– Подано характеристики «розумних міст».

– Проаналізовано ключові компоненти «розумних міст».

– Сформовано інформаційно-технологічну архітектуру «розумного міста».

В другому розділі кваліфікаційної роботи:

– Досліджено новітні технології в «розумних містах».

– Описано кібератаки, загрози та безпекові виклики в «розумних містах».

– Розглянута кібербезпека в «розумних містах».

– Сформовано принципи кібербезпеки в «розумних містах».

– Описано послуги кібербезпеки в «розумних містах».

– Досліджено важливість кібербезпеки в «розумних містах».

– Проаналізовано технологічний прогрес у кібербезпеці «розумних міст».

В третьому розділі кваліфікаційної роботи:

– Розглянуто застосування штучного інтелекту в кібербезпеці «розумних міст».

– Проаналізовано застосування блокчейну в кібербезпеці «розумних міст».

– Досліджено інтеграцію штучного інтелекту та блокчейну для кібербезпеки в «розумних містах».

– Описано перспективи майбутніх досліджень для убезпечення «розумних міст».

У розділі «Безпека життєдіяльності, основи охорони праці» описано організацію оповіщення і зв’язку у надзвичайних ситуаціях техногенного та природного характеру. Розглянуто професійне вигорання фахівців у сфері інформаційних технологій.

ПЕРЕЛІК ДЖЕРЕЛ

1 Denis, Asiku, et al. "A survey on artificial intelligence and blockchain applications in cybersecurity for smart cities." SHIFRA 2025 (2025): 1-45.

2 H. Omrany, K. M. Al-Obaidi, M. Hossain, N. a. M. Alduais, H. S. Al-Duais, and A. Ghaffarianhoseini, “IoT-enabled smart cities: a hybrid systematic analysis of key research areas, challenges, and recommendations for future direction,” Discover Cities, vol. 1, no. 2, pp. 1–35, 2024. https://doi.org/10.1007/s44327-024-00002-w

3 Á. Veloso, F. Fonseca, and R. Ramos, “Insights from Smart City Initiatives for Urban Sustainability and Contemporary Urbanism,” Smart Cities, vol. 7, no. 6, pp. 3188–3209, 2024. https://doi.org/10.3390/smartcities7060124

4 J. Liu, X. Liu, and J. Yang, “TOE Configuration analysis of smart city construction in China under the concept of sustainable Development,” Sustainability, vol. 16, no. 23, pp. 1–15, 2024. https://doi.org/10.3390/su162310708

5 V. S. Barletta, D. Caivano, M. De Vincentiis, A. Pal, and M. Scalera, “Hybrid quantum architecture for smart city security,” Journal of Systems and Software, vol. 217, pp. 1–15, 2024. https://doi.org/10.1016/j.jss.2024.112161

6 M. Houichi, F. Jaidi, and A. Bouhoula, “Cyber Security within Smart Cities: A Comprehensive Study and a Novel Intrusion Detection-Based Approach,” Computers, Materials & Continua, vol. 81, no. 1, pp. 393–441, 2024. https://doi.org/10.32604/cmc.2024.054007

7 G. Ali, M. M. Mijwil, B. A. Buruga, and M. Abotaleb, “A Comprehensive Review on Cybersecurity Issues and Their Mitigation Measures in FinTech,” Iraqi Journal For Computer Science and Mathematics, vol. 5, no. 3, pp. 45–91, 2024. https://doi.org/10.52866/ijcsm.2024.05.03.004

8 K. S. Kumar, J. A. Alzubi, N. Sarhan, E. M. Awwad, V. Kandasamy, and G. Ali, “A secure and efficient BlockChain and distributed Ledger technology-based optimal resource management in digital twin beyond 5G networks using hybrid

energy valley and levy Flight Distributer Optimization algorithm," IEEE Access, vol. 12, pp. 110331–110352, 2024. https://doi.org/10.1109/access.2024.3435847

9 M. Alaeddini, M. Hajizadeh, and P. Reaidy, "A Bibliometric Analysis of Research on the Convergence of Artificial Intelligence and Blockchain in Smart Cities," Smart Cities, vol. 6, no. 2, pp. 764–795, 2023. https://www.mdpi.com/2624-6511/6/2/37#

10 Y. Zhuang, J. Cenci, and J. Zhang, "Review of big data implementation and expectations in smart cities," Buildings, vol. 14, no. 12, pp. 1–27, 2024. https://doi.org/10.3390/buildings14123717

11 A. Hassebo, M. Tealab, and M. Hamouda, "From a traditional city to a Smart City: The Measurement of Cities' Readiness for Transition, Egypt as a case study," Urban Science, vol. 8, no. 4, pp. 1–38, 2024. https://doi.org/10.3390/urbansci8040212

12 D. E. Okonta, and V. Vukovic, "Smart cities software applications for sustainability and resilience," Heliyon, vol. 10, no. 12, pp. 1–20, 2024. https://doi.org/10.1016/j.heliyon.2024.e32654

13 Duda O., Kunanets N., Matsiuk O., Pasichnyk V., Rzheuskyi A. Aggregation, Storing, Multidimensional Representation and Processing of COVID-19 Data // Advances in Intelligent Systems and Computing V. CSIT 2020. Springer, Cham, 2021. Vol. 1293. DOI: 10.1007/978-3-030-63270-0_60. ISSN 2194-5357, EISSN 2194-5365.

14 Duda O., Matsiuk O., Kunanets N., Pasichnyk V., Rzheuskyi A., Bilak Y. Formation of hypercubes based on data obtained from IoT devices // International Journal of Sensors, Wireless Communications and Control. 2021. Vol. 11(5). P. 498–504. DOI: 10.2174/2210327910999201210145151.

15 Duda O., Stanko A. Architecture of monitoring platform in smart cities // Вісник ХНУ. 2023. No. 4. P. 10–19. DOI: 10.31891/2307-5732.

16 Zhovnir Y., Kunanets N., Burov Y., Duda O., Pasichnyk V. Situation-aware security systems design // Eastern-European Journal of Enterprise Technologies. 2025. Vol. 1/9(133). P. 6–23. DOI: 10.15587/1729-4061.2025.315248.

17 Orlov M. V., Duda O. M., Zhovnir Y. I., Hrybovskyi O. M. DevOps tools in IoT systems // Комп'ютерно-інтегровані технології. 2024. Vol. 57. P. 128–138. DOI: 10.36910/6775-2524-0560-2024-57-15.

18 Orlov M. V., Hrybovskyi O. M., Zhovnir Y. I., Duda O. M. DevOps methodology in IoT ecosystems // Вчені записки ТНУ. 2024. Vol. 35(6). P. 163–170. DOI: 10.32782/2663-5941/2024.6.2/22.

19 Zhovnir Y. I., Hrybovskyi O. M., Orlov M. V., Duda O. M., Kunanets N. E. IoT information systems methodology // Управління розвитком складних систем. 2024. Vol. 60. P. 56–71. DOI: 10.32347/2412-9933.2024.60.56-70.

20 D. Bastos, N. Costa, N. P. Rocha, A. Fernández-Caballero, and A. Pereira, "A comprehensive survey on the societal aspects of smart cities," Applied Sciences, vol. 14, no. 17, pp. 1-39, 2024. https://doi.org/10.3390/app14177823

21 S. A. Ali, S. A. Elsaid, A. A. Ateya, M. ElAffendi, and A. a. A. El-Latif, "Enabling Technologies for Next-Generation Smart Cities: A Comprehensive Review and research Directions," Future Internet, vol. 15, no. 12, pp. 1–43, 2023. https://doi.org/10.3390/fi15120398

22 E. H. Houssein, M. A. Othman, W. M. Mohamed, and M. Younan, "Internet of Things in Smart Cities: Comprehensive review, open issues and challenges. IEEE Internet of Things Journal, vol. 11, no. 21, pp. 34941–34952, 2024. https://doi.org/10.1109/jiot.2024.3449753

23 A. Gelbukh, M. T. Zamir, F. Ullah, M. Ali, T. Taiba, M. Usman, N. Hafeez, L. Dudaeva, and C. Fasoldt, "State-ofthe-Art Review in Explainable Machine Learning for Smart-Cities Applications," In Studies in Big Data (Vol. 148, pp. 67–76). Springer, 2024. https://doi.org/10.1007/978-3-031-54277-0_3

24 H. N. Fakhouri, S. Alawadi, F. M. Awaysheh, I. Bani Hani, M. Alkhalaileh, and F. Hamad, "A comprehensive study on the role of machine learning in 5G security: Challenges, technologies, and solutions," Electronics, vol. 12, no. 22, pp. 1-44, 2023. https://doi.org/10.3390/electronics12224604

25 L. Chen, Z. Chen, Y. Zhang, Y. Liu, A. I. Osman, M. Farghali, J. Hua, A. Al–Fatesh, I. Ihara, D. W. Rooney, and P.-S. Yap, "Artificial intelligence-based

solutions for climate change: a review," Environmental Chemistry Letters, vol. 21, no. 5, pp. 2525-2557, 2023. https://doi.org/10.1007/s10311-023-01617-y

26 Z. Zhang, H. A. Hamadi, E. Damiani, C. Y. Yeun, and F. Taher, "Explainable artificial intelligence applications in cyber security: State-of-the-art in research," IEEE Access, vol. 10, pp. 93104–93139, 2022. https://doi.org/10.1109/ACCESS.2022.3204051

27 M. M. Alshahrani, "A secure and intelligent Software-Defined networking Framework for future smart cities to prevent DDOS attack," Applied Sciences, vol. 13, no. 17, pp. 1–16, 2023. https://doi.org/10.3390/app13179822

28 R. K. Mahmood, A. I. Mahameed, N. Q. Lateef, H. M. Jasim, A. D. Radhi, S. R. Ahmed, and P. Tupe-Waghmare, "Optimizing network security with machine learning and multi-factor authentication for enhanced intrusion detection," Journal of Robotics and Control, vol. 5, no. 5, pp. 1502-1524, 2024. https://doi.org/10.18196/jrc.v5i5.22508

29 H. Li, D. He, P. Vijayakumar, F. Alqahtani, and A. Tolba, "A certificateless and KGA-secure searchable encryption scheme with constant trapdoors in smart city," Digital Communications and Networks, pp. 1–13, 2024. https://doi.org/10.1016/j.dcan.2024.08.005

30 M. H. B. Ibrahim, Y. Al Moaiad, W. Abu-Ulbeh, H. Al-Wahshat, W. A. H. M. Ghanem, and R. R. Mohamed, "Security frameworks for IoT devices in smart cities," Journal of Jilin University (Engineering and Technology Edition), vol. 43, no. 6, pp. 206-230, 2024. https://doi.org/10.5281/zenodo.12529126

31 R. Fatih, S. Arezki, and T. Gadi, "A review of blockchain-based e-voting systems: Comparative analysis and findings," International Journal of Interactive Mobile Technologies, vol. 17, no. 23, pp. 49–67, 2023. https://doi.org/10.3991/ijim.v17i23.45257

32 C. Goumopoulos, "Smart City Middleware: A survey and a Conceptual framework," IEEE Access, vol. 12, pp. 4015– 4047, 2024. https://doi.org/10.1109/access.2023.3349376

33 M. Ryalat, N. Almtireen, H. Elmoaqet, and M. Almohammedi, “The Integration of Two Smarts in the Era of Industry 4.0: Smart Factory and Smart City,” 2024 IEEE Smart Cities Futures Summit (SCFC), Marrakech, Morocco, Marrakech, Morocco, pp. 9–12. https://doi.org/10.1109/scfc62024.2024.10698351

34 R. Salama, S. Al-Turjman, C. Altrjman, F. Al-Turjman, O. Vikash, S. P. Yadav, and S. Vats, “The Main Threat to Computer Network Security in Smart Cities. 2023 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE), Ghaziabad, India, 23-24 November 2023, pp. 419–425. https://doi.org/10.1109/aece59614.2023.10428154

35 A. Algarni, Z. Ahmad, and M. A. Ala’Anzy, “An edge computing-based and threat behavior-aware smart prioritization framework for cybersecurity intrusion detection and prevention of IEDs in smart grids, integrating modified LGBM and one class-SVM models,” IEEE Access, vol. 12, pp. 104948-104963, 2024. https://doi.org/10.1109/ACCESS.2024.3435564

36 G. Ali, M. M. Mijwil, A. B. Bosco, M. Abotaleb, and I. Adamopoulos, “A Survey on Artificial Intelligence in Cybersecurity for Smart Agriculture: State-of-the-Art, Cyber Threats, Artificial Intelligence Applications, and Ethical Concerns,” Mesopotamian Journal of Computer Science, vol. 2024, pp. 71–121, 2024. https://doi.org/10.58496/MJCSC/2024/007

37 M. Ozkan-Okay, E. Akin, Ö. Aslan, S. Koşunalp, T. Iliev, I. Stoyanov, and I. Beloev, “A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions,” IEEE Access, vol. 12, pp. 12229–12256, 2024. https://doi.org/10.1109/access.2024.3355547

38 K. Kim, I. M. Alshenaifi, S. Ramachandran, J. Kim, T. Zia, and A. Almorjan, “Cybersecurity and Cyber Forensics for Smart Cities: A Comprehensive literature review and survey,” Sensors, vol. 23, no. 7, pp. 1–25, 2023. https://doi.org/10.3390/s23073681

39 L. Ismail, and R. Buyya, “Artificial intelligence applications and self-learning 6G networks for smart cities digital ecosystems: Taxonomy, challenges, and

future directions," Sensors, vol. 22, no. 15, pp. 1-30, 2022. https://doi.org/10.3390/s22155750

40 M. M. Rashid, J. Kamruzzaman, M. M. Hassan, T. Imam, S. Wibowo, S. Gordon, and G. Fortino, "Adversarial training for deep learning-based cyberattack detection in IoT-based smart city applications," Computers & Security, vol. 120, pp. 102783, 2022. https://doi.org/10.1016/j.cose.2022.102783

41 Y. Djenouri, and A. N. Belbachir, "Empowering Urban Connectivity in Smart Cities using Federated Intrusion Detection," 2022 IEEE 9th International Conference on Data Science and Advanced Analytics (DSAA), Thessaloniki, Greece, 09-13 October 2023, pp. 1-9. https://doi.org/10.1109/dsaa60987.2023.10302528

42 K. Kalinaki, N. N. Thilakarathne, H. R. Mubarak, O. A. Malik, and M. Abdullatif, "Cybersafe capabilities and utilities for smart cities," In Advanced sciences and technologies for security applications (pp. 71–86). Springer, 2023. https://doi.org/10.1007/978-3-031-24946-4_6

43 U. Majeed, L. U. Khan, I. Yaqoob, S. M. A. Kazmi, K. Salah, and C. S. Hong, "Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges," Journal of Network and Computer Applications, vol. 181, pp. 103007, 2021. https://doi.org/10.1016/j.jnca.2021.103007

44 M. A. Mansoor, M. Ali, A. Mateen, M. Kaleem, and S. Nazir, "Blockchain technology for land registry management in developing countries," 2023 2nd International Conference on Emerging Trends in Electrical, Control, and Telecommunication Engineering (ETECTE), Lahore, Pakistan, 27-29 November 2023, pp. 1–6. https://doi.org/10.1109/ETECTE51838.2023.1005678

45 R. Wolniak, and K. Stecuła, "Artificial intelligence in smart cities Applications, barriers, and future directions: A review," Smart Cities, vol. 7, no. 3, pp. 1346–1389, 2024. https://doi.org/10.3390/smartcities7030057

46 C. Kontos, T. Panagiotakopoulos, and A. Kameas, "Applications of blockchain and smart contracts to address challenges of cooperative, connected, and automated mobility," Sensors, vol. 24, no. 19, pp. 1–30, 2024. https://doi.org/10.3390/s24196273

47 Організація оповіщення і зв’язку. https://czndep.zht.gov.ua/SOZ.html.

48 Організація оповіщення та зв’язку. https://nmc.dsns.gov.ua/zk/news/ostanni-novini/164.

49 Gartner. Risk Management in Cyber-Physical Systems: IoT Security. – Аналітичний звіт, 2023. – https://www.gartner.com/

50 Бакшаєва О. В., Ковальчук І. М. Психоемоційний стан працівників ІТ-сфери в умовах сучасного робочого середовища. Науковий журнал «Психологія праці». – 2020. – № 4 (15). – С. 45 – 48.

51 Воронова Н. Професійне вигорання: причини, наслідки, шляхи подолання Журнал «Охорона праці». – 2019. – № 2 (8). – С. 32 – 37.