Хмельницький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

Галузь знань 12 - Інформаційні технології

Спеціальність 123 -Комп'ютерна інженерія

на тему «Метод та система управління безпекою на основі смарт-контрактів для взаємодії служб "Розумного міста"»

КвРКІП. 302174.23.02.14 ПЗ

Виконав: студент 2 курсу, група КІ2м-23-2 _____ Андрій ВОЙТКОВ
Підпис Ім'я, прізвище

Керівник д-р. техн. наук, професор _____ Сергій ЛИСЕНКО
Науковий ступінь, вчене звання Підпис Ім'я, прізвище

До захисту допускаю:
Зав. кафедри КІІС, доктор філософії, доцент
Ольга ПАВЛОВА
06 05 2025 р.

Хмельницький, 2025

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Освітній рівень МАГІСТР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 123 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Освітня програма ОСВІТНЬО-НАУКОВА ПРОГРАМА «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ ТА ПРОГРАМУВАННЯ»

ЗАТВЕРДЖУЮ

Зав. кафедри Ольга ПАВЛОВА

" 01 " 09 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА

Андрію ВОЙТКОВУ
Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Метод та система управління безпекою на основі смарт-контрактів для взаємодії служб "Розумного міста"

Керівник проекту (роботи) Сергій ЛИСЕНКО, д.т.н., професор
Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 08.01.2025 №8

2. Строк подання студентом проекту (роботи) на кафедру 01.05.2025 р.

3. Вихідні дані до проекту (роботи) Завдання на дипломне проектування

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Аналіз відомих методів управління безпекою у розподілених смарт-сервісах розумного міста

Модель процесу управління безпекою на основі смарт-контрактів для взаємодії служб "розумного міста"

Метод управління безпекою на основі смарт-контрактів для взаємодії служб "розумного міста"

Система управління безпекою на основі смарт-контрактів для взаємодії служб "розумного міста"

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

6. Консультанти розділів кваліфікаційної роботи магістра

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Сергій ЛИСЕНКО, професор кафедри КІС		
Антиплагіат	Андрій НІЧЕПОРУК, доцент кафедри КІС		

7. Дата видачі завдання «_01_»_____09_____2024р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи магістра	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір напряму дослідження та узгодження тематики КвРМ з керівником	01.09.2024	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	01.10.2024	виконано
3	Робота над розділом 1 - аналіз відомих моделей, методів за темою; постановка задачі	01.11.2024	виконано
4	Робота над розділом 2 - розробка моделей для вирішення поставленої задачі	01.12.2024	виконано
5	Робота над науковою статтею	01.02.2025	виконано
6	Робота над розділом 3 - розробка методів для вирішення поставленої задачі	15.02.2025	виконано
7	Робота над розділом 4 - проектування та розробка ПЗ для вирішення поставленої задачі, експериментальна частина	01.04.2025	виконано
8	Оформлення пояснювальної записки згідно вимог	18.04.2025	виконано
9	Попередній захист ДРМ	29.04.2025	виконано
10	Захист ДРМ на засіданні ЕК	До 15.05.2025	

Студент _____ Андрій ВОЙТКОВ
Підпис Ім'я, прізвище

Керівник роботи _____ Сергій ЛИСЕНКО
Підпис Ім'я, прізвище

РЕФЕРАТ

Тема кваліфікаційної роботи магістра: Метод та система управління безпекою на основі смарт-контрактів для взаємодії служб “Розумного міста”

Автор роботи: Войтков Андрій Олексійович

Керівник роботи: Лисенко Сергій Миколайович

Пояснювальна записка: 81 с., 17 рис., 6 табл., 3 дод., 87 джерел.

РОЗУМНЕ МІСТО, СМАРТ-КОНТРАКТ, УПРАВЛІННЯ БЕЗПЕКОЮ, БЛОКЧЕЙН, SDIOT, СМАРТ-СЕРВІС

Об’єктом дослідження є процес управління безпекою в умовах розподіленої взаємодії між сервісами розумного міста.

Предметом дослідження є метод управління безпекою на основі смарт-контрактів у гетерогенному середовищі SDIoT з багаторівневою оцінкою довіри.

Метою кваліфікаційної роботи магістра підвищення ефективності з взаємодії смарт-сервісів у розумному місті на основі смарт-контрактів.

Для розв’язання поставлених задач використовувалися методи теорії комп’ютерних систем, блокчейн-технологій, криптографії на основі еліптичних кривих, теорії довіри та програмно-керованих мереж (SDN).

Наукова новизна отриманих результатів:

− удосконалено метод управління безпекою на основі смарт-контрактів для взаємодії служб “Розумного міста”, який на відміну від відомих використовує смарт-контрактти та багатоланцюгової блокчейн-інфраструктури що дозволяє здійснювати децентралізовану, адаптивну взаємодію смарт-сервісів у цифровій інфраструктурі інтелектуального міста;

− удосконалено систему управління безпекою на основі смарт-контрактів для взаємодії служб “Розумного міста”

Практична значимість отриманих результатів полягає у можливості впровадження запропонованого методу у системи управління безпекою смарт-міст, що дозволяє підвищити стійкість до атак, забезпечити прозорість угод між

сервісами та мінімізувати ручне адміністрування завдяки автоматизованим контрактам.

У першому розділі було розглянуто сучасні виклики кібербезпеки в інтелектуальних міських середовищах, особливості взаємодії смарт-сервісів, а також технології SDIoT, блокчейн та смарт-контрактів, які забезпечують основу для розробки безпечних децентралізованих систем.

У другому розділі було запропоновано формальну модель методу управління безпекою, визначено ключові суб’єкти, описано життєвий цикл смарт-контрактів, структуру довіри та контекстного управління доступом. Також представлено логіку взаємодії між сервісами через блокчейн-інфраструктуру.

У третьому розділі сформовано повну архітектуру системи, що реалізує запропонований метод, включаючи адаптивні рушії політик, криптографічне управління ключами, контракти доступу та виконання завдань. Показано побудову безпечного середовища обміну даними у смарт-місті.

У четвертому розділі змодельовано ключові сценарії обміну повідомленнями між сервісами, проведено експерименти з вимірюванням пропускної здатності, затримок та навантаження при масштабуванні, що підтвердило ефективність методу.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

IoT - інтернет речей

SDIoT - програмно-визначений Інтернет речей

SDN - програмно-визначене мережеве управління сенсорних мереж

API - інтерфейс прикладного програмування

GPS - глобальна система позиціонування

JSON - текстовий формат обміну даними

TCP/IP - протокол керування передачею / Інтернет-протокол

IP - інтернет-протокол

ECC - криптографія на еліптичних кривих

MFA - багатофакторна автентифікація

IDS - система виявлення вторгнень

IPS – система запобігання вторгненням

IDS/IPS – Комплекс систем виявлення та запобігання вторгненням

PBFT - практична візантійська стійкість до відмов

SDN-WISE - програмно-визначені мережі для бездротових

SLA - угода про рівень обслуговування між постачальником та споживачем послуг

ВСТУП

У сучасному цифровому середовищі інфраструктура розумного міста все більше інтегрує смарт-сервіси, IoT-пристрої та автономні агенти, що функціонують у гетерогенному та динамічному середовищі. У таких умовах виникає критична потреба у забезпеченні надійної, гнучкої та масштабованої системи управління безпекою, яка б могла адаптуватись до змін середовища, гарантувати довіру між суб'єктами взаємодії та забезпечувати цілісність даних при спільному виконанні завдань.

Актуальність роботи полягає у розробці методу управління безпекою на основі смарт-контрактів, що функціонує в інфраструктурі програмно-керованого Інтернету речей (SDIoT), підтримує багаторівневу взаємодію між сервісами та дозволяє формалізувати правила доступу, аутентифікації та довіри в умовах розподіленої архітектури інтелектуального міста.

Метою кваліфікаційної роботи магістра є підвищення ефективності з взаємодії смарт-сервісів у розумному місті на основі смарт-контрактів.

Поставлена мета досягається розв'язанням таких основних завдань:

- проаналізувати принципи реалізації смарт-контрактів у блокчейн-середовищі для організації міжсервісної взаємодії;
- сформувати модель управління довірою, яка базується на історії взаємодій та динамічних параметрах;
- розробити метод управління безпекою на основі смарт-контрактів для взаємодії служб "Розумного міста";
- реалізувати процес аутентифікації, авторизації та обміну повідомленнями між службами з використанням криптографії ECC;
- створити алгоритми генерації та оновлення політик безпеки на основі контексту та сервісних угод;
- здійснити перевірку ефективності розробленого методу за допомогою критеріїв продуктивності, затримки та масштабованості.

Об’єктом дослідження є процес управління безпекою в умовах розподіленої взаємодії між сервісами розумного міста.

Предметом дослідження є метод управління безпекою на основі смарт-контрактів у гетерогенному середовищі SDIoT з багаторівневою оцінкою довіри.

Наукова новизна отриманих результатів:

− удосконалено метод управління безпекою на основі смарт-контрактів для взаємодії служб “Розумного міста”, який на відміну від відомих використовує смарт-контрактти та багатоланцюгової блокчейн-інфраструктури що дозволяє здійснювати децентралізовану, адаптивну взаємодію смарт-сервісів у цифровій інфраструктурі інтелектуального міста;

− удосконалено систему управління безпекою на основі смарт-контрактів для взаємодії служб “Розумного міста”

Практична значимість отриманих результатів полягає у можливості впровадження запропонованого методу у системи управління безпекою смарт-міст, що дозволяє підвищити стійкість до атак, забезпечити прозорість угод між сервісами та мінімізувати ручне адміністрування завдяки автоматизованим контрактам.

Для розв’язання поставлених задач використовувалися методи теорії комп’ютерних систем, блокчейн-технологій, криптографії на основі еліптичних кривих, теорії довіри та програмно-керованих мереж (SDN).

За темою кваліфікаційної роботи опубліковано тези у матеріалах конференції "Актуальні проблеми комп’ютерних наук АПКН-2024"

1 АНАЛІЗ ВІДОМИХ МЕТОДІВ УПРАВЛІННЯ БЕЗПЕКОЮ НА ОСНОВІ СМАРТ-КОНТРАКТІВ ДЛЯ ВЗАЄМОДІЇ СЛУЖБ “РОЗУМНОГО МІСТА”

1.1 Розуміння концепції розумного міста

Сучасний світ розвивається стрімкими темпами, що створює умови для миттєвої адаптації технологічних нововведень.

Такий прогрес вважається невід’ємною складовою еволюційного розвитку, який має як позитивні, так і негативні наслідки.

До основних викликів сучасності належать економічні та соціальні труднощі, швидке зростання населення, активне споживання природних ресурсів, значне використання енергії, екологічне забруднення та кліматичні зміни[24,25].

Світ є не лише мінливим, а й відкритим до технологічних змін. Він являє собою єдину інтегровану систему, що поєднує фізичну, цифрову та соціальну складові.

Окрім цього, інформаційна революція, активний розвиток інновацій та підприємницької діяльності значно вплинули на урбаністичні процеси, так само як і на інші сфери суспільного життя.[26]

Одним із перспективних підходів до вирішення проблем урбанізації є концепція інтелектуального міста. Вона має різні визначення та моделі, що розроблялися науковцями та практиками у різні періоди. Уперше ця ідея з’явилася ще у 1990-х роках, а з початку 2000-х років почала активно поширюватися та набувати популярності[27].

Інтелектуальні міста покликані відповідати на виклики швидкої урбанізації та містять у собі комплекс взаємопов’язаних компонентів.

Їх розвитком займаються численні міжнародні організації, наукові установи та компанії.

Завдяки цим дослідженням з’явилися численні економічні програми та ініціативи, спрямовані на підтримку і впровадження концепції інтелектуального містах[28,29].

1.1.1 Визначення інтелектуального міста

Сучасні підходи до розумного міста визначають його як територію, що активно використовує цифрові та телекомунікаційні технології для оптимізації інфраструктури, підвищення ефективності послуг та створення комфортного середовища для мешканців і підприємств[30].

Однак розумне місто - це не лише набір технологій, а передусім бачення майбутнього, де цифровізація та інновації сприяють загальному покращенню міського середовища та сталому розвитку суспільства. Технології нового покоління відіграють у цьому процесі ключову роль, оскільки, подібно до нервової системи людини, дозволяють містам гнучко реагувати на зміни та ефективно керувати міськими процесами[31].

1.1.2 Використання технологій у містах нового покоління

Застосування сучасних технологій для збору та аналізу інформації, включно з даними в реальному часі, є ключовим чинником розвитку інтелектуальних міст[32]. Використання отриманих аналітичних висновків дає можливість міським адміністраціям покращувати управління інфраструктурою та якість наданих послуг - від поводження з відходами до ефективності громадського транспорту. Такі зміни сприяють підвищенню рівня комфорту для жителів міста[33].

Удосконалення міських сервісів також допомагає зменшити рівень викидів парникових газів, підтримуючи глобальні ініціативи щодо боротьби зі змінами клімату, а також покращуючи якість повітря в межах населених пунктів[34]. Крім того, технологічні рішення для інтелектуальних міст можуть стати потужним рушієм економічного розвитку, оскільки модернізована інфраструктура та впровадження новітніх технологій створюють передумови для появи нових робочих місць і відкривають нові можливості для бізнесу[35].

1.1.3 Інтелектуальна інфраструктура міського простору

Однією з ключових складових концепції інтелектуального міста є його технологічно вдосконалена інфраструктура. Її основне завдання - інтеграція передових розробок у фізичну структуру населеного пункту з метою оптимізації використання ресурсів і підвищення ефективності наданих послуг[36].

Основні елементи міської інфраструктури нового покоління:

1) розумні енергетичні мережі (Smart Grids),

2) системи, що застосовують цифрові технології для контролю процесів генерації, розподілу та споживання електроенергії,

3) зменшують втрати енергетичних ресурсів, скорочують витрати та забезпечують стабільність електропостачання завдяки адаптації до змін попиту,

4) інтелектуальна транспортна система (Smart Transportation),

5) використання датчиків, супутникового позиціонування та алгоритмів аналізу даних для оптимізації руху транспорту, мінімізації заторів і підвищення ефективності громадського транспорту,

6) включає адаптивні світлофори, автономні транспортні засоби та цифрові рішення для організації паркування,

7) сталий розвиток будівель (Sustainable Buildings).

Використання технологій Інтернету речей (IoT) для автоматизованого контролю над мікрокліматом будівель (опалення, кондиціонування, вентиляція), освітленням та системами безпеки.

Проєктування будівель із фокусом на енергоефективність та екологічну безпеку, що сприяє зниженню загального рівня забруднення та оптимізації ресурсів[40].

1.1.4. Висновок.

Концепція інтелектуального міста є однією з найперспективніших стратегій розвитку сучасних мегаполісів[41]. Вона дозволяє не лише підвищити

ефективність управління міськими ресурсами, але й значно покращити якість життя мешканців завдяки впровадженню інноваційних технологій у всі сфери урбаністичного управління[42]. Використання Інтернету речей (IoT), штучного інтелекту (AI), великих даних (Big Data) та автоматизованих систем адміністрування сприяє створенню ефективного, безпечного та екологічно збалансованого середовища.

Для ефективного впровадження інтелектуальних міст необхідна тісна співпраця державного та приватного секторів. Притягнення міжнародних інвестицій, впровадження інноваційних рішень та створення сприятливого правового середовища дозволять містам швидше адаптуватися до сучасних викликів. Важливим аспектом також є залучення громади до процесу цифрової трансформації, що сприятиме підвищенню рівня довіри та ефективності впроваджених технологічних рішень.

Перспективи подальшого розвитку інтелектуальних міст охоплюють використання екологічно чистих джерел енергії, автономного транспорту, інноваційних систем управління водними та енергетичними ресурсами. Усе це сприятиме зниженню екологічного навантаження та підвищенню рівня комфорту міського життя[46]. Отже, концепція Smart City - це не просто тренд, а стратегічний напрямок розвитку майбутнього, що дозволить зробити міста більш зручними, безпечними та сталими для всіх мешканців[47].

1.2 Впровадження концепції інтелектуального міста

Одним із ключових завдань місцевих органів самоврядування є ефективне впровадження концепції інтелектуального міста. Ця ідея залишається відносно новою, однак інтерес до неї зростає, оскільки прогнозується, що до 2050 року більшість населення планети-приблизно 70%-буде проживати у міських районах.

За даними досліджень, якщо процес урбанізації контролюватиметься належним чином, він може стати рушієм стійкого розвитку, підвищуючи рівень продуктивності та стимулюючи інноваційні процеси. Це особливо важливо,

враховуючи, що саме міста формують понад 80% загального світового валового внутрішнього продукту[50].

Ще одним вагомим чинником, що вплинув на активне впровадження елементів розумного міста, стала швидка цифровізація, яка посилилася внаслідок пандемії. Багато сфер діяльності, зокрема міські сервіси, потребували швидкої адаптації до нових реалій, що спричинило активний розвиток цифрових технологій і закріплення цього тренду в міському управлінні.

На думку експертів, концепція інтелектуального міста базується на інтеграції цифрових технологій у міські системи з метою покращення інфраструктури, підвищення ефективності послуг та створення сприятливих умов для жителів та підприємств[52].

Деякі дослідники розглядають розумне місто як потужний інтелектуальний потенціал, що охоплює технологічні, соціальні, економічні та інноваційні аспекти розвитку міського простору[53]. Інші науковці визначають інтелектуальне місто як високотехнологічний мегаполіс, спроєктований для задоволення потреб громадян, державних установ та бізнесу.

Такі підходи також спрямовані на розв’язання широкого спектра проблем, пов’язаних із сталим розвитком та ефективним управлінням міським простором[55]. Незважаючи на їхню амбітність, ці стратегії є необхідними для успішної урбанізації та вимагають значних фінансових вкладень. Вони мають довгострокові наслідки, тому їх впровадження потребує детального аналізу як на етапі формування політики, так і в процесі її реалізації.

Будівництво розумних міст повинне відбуватися на стратегічних засадах з метою досягнення конкретних економічних, соціальних та урбаністичних результатів. Це підтверджує важливість подальших досліджень у цій сфері для вдосконалення існуючих підходів і розробки ефективних рішень.

1.2 Ключові елементи інтелектуального міста.

Численні дослідники розділили концепцію інтелектуального міста на кілька ключових аспектів і вимірів, оскільки його управління є багаторівневим та складним процесом. На основі аналізу наукових праць було визначено основні складові, що формують розумне місто[60].

Було ідентифіковано шість основних напрямів, що забезпечують функціонування розумного міста[61]. Для досягнення високої ефективності урбаністичного середовища необхідно приділяти увагу цим сферам, розвивати їх та використовувати як основу для міської взаємодії.

Деякі аспекти є більш значущими для громадян, ніж інші. Наприклад, жителі сучасних міст найчастіше зосереджують увагу на питаннях мобільності та інфраструктури, оскільки вони безпосередньо впливають на повсякденне життя. Водночас екологічна стійкість та ефективне міське управління займають проміжне місце за рівнем важливості серед мешканців.

Інтелектуальна економіка - даний компонент включає розвиток інноваційного підприємництва, цифрової комерції та технологічних рішень, що підвищують продуктивність та оптимізують використання ресурсів.

Основними характеристиками інтелектуальної економіки є розширення ділових можливостей, створення нових робочих місць та розвиток технологічних галузей.

Цифровізація промислових процесів, впровадження штучного інтелекту, інноваційні методи виробництва та інтеграція у світову економіку сприяють залученню інвестицій, туристичного потоку та висококваліфікованих фахівців, що стимулює загальний економічний ріст міста.

Проте, активний розвиток економіки може супроводжуватися виснаженням природних ресурсів, що вимагає впровадження механізмів екологічного управління та раціонального використання ресурсів

Інноваційне управління - інтелектуальне управління міськими процесами передбачає поєднання технологічних рішень, законодавчих ініціатив та громадської участі для підвищення ефективності муніципального адміністрування.

Застосування інформаційних технологій забезпечує прозорість державних процесів, підвищує якість наданих послуг та сприяє активному залученню громадян до ухвалення управлінських рішень.

Інтеграція цифрових платформ дозволяє централізувати надання муніципальних послуг та мінімізувати бюрократичні бар'єри. Використання концепцій електронного уряду (e-Government) та цифрової демократії (e-Democracy) сприяє відкритості влади, доступності адміністративних сервісів та зростанню довіри з боку населення.

Ключові аспекти інноваційного управління включають:

1) цифрову комунікацію між владою та мешканцями,

2) відкритий доступ до державних послуг та інформації,

3) застосування великих даних (Big Data) та штучного інтелекту для ухвалення рішень,

4) автоматизацію процесів з метою мінімізації бюрократичного навантаження.

Однією з важливих складових є забезпечення рівного доступу всіх громадян до цифрових послуг, що підвищує соціальну інклюзивність та сприяє ефективному використанню міських ресурсів.

Інтелектуальна мобільність та транспорт - розвиток сучасних транспортних систем є критичним для зниження рівня заторів, підвищення якості перевезень та зменшення екологічного навантаження на міське середовище.

Технологічні рішення, зокрема інтелектуальні транспортні системи (ITS) та Інтернет речей (IoT), дозволяють ефективно управляти потоками транспорту, оптимізувати дорожній рух та покращувати функціонування громадського транспорту.

Основні підходи до розвитку розумного транспорту включають:

1) використання адаптивних світлофорів та датчиків трафіку для оптимізації дорожнього руху,

2) інтеграцію цифрових транспортних систем та мобільних додатків,

3) створення екологічно чистого громадського транспорту,

4) розширення велосипедної та пішохідної інфраструктури.

Партнерство між державним та приватним секторами дозволяє реалізовувати комплексні рішення для модернізації інфраструктури, що сприяє зменшенню використання приватного автотранспорту, підвищенню ефективності перевезень та покращенню екологічного стану міст.

Сталий розвиток та екологічна безпека - екологічний аспект інтелектуальних міст передбачає ефективне використання природних ресурсів, зменшення рівня забруднення та впровадження екологічно безпечних технологій.

Використання Інтернету речей (IoT), штучного інтелекту та блокчейну сприяє контролю якості повітря, управлінню відходами та оптимізації енергоспоживання.

Основні екологічні ініціативи включають:

1) використання альтернативних джерел енергії для зменшення викидів парникових газів,

2) інтелектуальне управління відходами через сенсорні системи та автоматизовані сміттєві контейнери,

3) моніторинг екологічного стану для зменшення негативного впливу на здоров’я мешканців.

Майбутнє екологічно сталих міст залежить від впровадження дієвої екологічної політики, що сприятиме покращенню умов життя населення. Баланс між економічним розвитком та екологічною безпекою дозволяє створювати стійке та гармонійне міське середовище без необхідності жертвувати жодним із цих факторів[77].

1.3 Блокчейн-технології в розумних містах

Протягом останнього десятиліття блокчейн зарекомендував себе як ефективна децентралізована система. Він являє собою розподілену базу даних, що фіксує транзакції в одноранговій (peer-to-peer) мережі. Такий метод забезпечує децентралізацію обчислень і дозволяє усунути необхідність довіри до централізованих установ[29]. Завдяки синхронній взаємодії численних вузлів мережі всі транзакційні записи зберігаються у розподіленому середовищі, виключаючи потребу у посереднику.

Блокчейн є відносно новою технологією, що має потенціал стати революційною інновацією на рівні Інтернету або протоколу TCP/IP. Одним із ключових понять цієї технології є розподілений реєстр (DLT), що означає безпечне збереження та обробку цифрових транзакцій у децентралізованій системі[31].

Використання блокчейну в розумних містах дозволяє обробляти, аналізувати та контролювати дані в реальному часі, що значно покращує якість міського життя[32]. Інтелектуальні міста передбачають активну взаємодію громадян із міськими системами за допомогою мобільних пристроїв, транспортних засобів та побутових об'єктів. Взаємозв'язок цифрових і фізичних структур допомагає оптимізувати використання ресурсів, знизити витрати та підвищити стійкість міських екосистем.

Впровадження блокчейн-рішень сприяє екологічній та економічній стабільності міста. Завдяки інтеграції з Інтернетом речей (IoT) громади отримують такі переваги:

1) покращена якість повітря через оптимізацію транспортних потоків,
2) раціональне використання енергетичних ресурсів,
3) скорочення заторів за рахунок інтелектуального управління дорожнім рухом,
4) ефективне управління збором та переробкою відходів,
5) блокчейн у фінансовій системі

Окрему роль блокчейн відіграє у фінансовій сфері, оскільки забезпечує прозорість цифрових платежів і усуває посередників, таких як банки чи державні установи. Спочатку ця технологія застосовувалася переважно у фінансовому секторі, однак згодом її почали використовувати для розв’язання ширшого спектра соціально-економічних та екологічних проблем.

Серед ключових переваг блокчейну у фінансових операціях можна виокремити:

1) скорочення фінансових бар'єрів між учасниками ринку,
2) відсутність посередників у централізованих фінансових структурах,
3) збільшення прозорості в логістичних і постачальницьких мережах.

Ця технологія сприяє розвитку економіки, підвищенню рівня довіри між учасниками ринку та зменшенню фінансових витрат завдяки автоматизованим і безпечним транзакціям.

1.3.1. Смарт-контракти та їх структура

Смарт-контракт - це цифровий договір, який має вбудовані механізми автоматичного виконання без необхідності втручання регулятора чи центрального органу[34]. Його умови закладені у програмному коді, що дозволяє взаємодіяти сторонам без посередників.

Кожен смарт-контракт складається з таких ключових елементів:

1) змінні стану (Status variables) - параметри, що зберігаються в контракті протягом усього періоду його функціонування,
2) функції (Functions) - окремі блоки коду, що визначають логіку роботи контракту[35],
3) модифікатори функцій (Function modifiers) - механізми, які дозволяють змінювати поведінку контракту без переписування основного коду,
4) події (Events) - інструменти, що забезпечують комунікацію з віртуальною машиною Ethereum (EVM) та надсилають сповіщення про зміни в контракті.

5) структура - користувацькі типи даних, що можуть містити кілька змінних,

6) перерахування (Enumerations) - набір можливих значень змінної, що дозволяє встановити обмежений список станів контракту.

Смарт-контракти значно спрощують взаємодію між сторонами та забезпечують автоматизацію багатьох фінансових і логістичних процесів. Їх використання у розумних містах сприяє підвищенню прозорості угод, зниженню ризиків шахрайства та мінімізації витрат на адміністрування[36].

Швидке поширення блокчейн-технологій призводить до труднощів у виборі відповідної платформи, оскільки на сьогодні не існує універсальної методики оцінювання різних варіантів. Важливо створювати систематизовані підходи до збереження, управління та доступу до інформації про блокчейн-мережі.

Різні дослідники пропонували підходи до вирішення питань безпеки в блокчейні та смарт-контрактах, застосовуючи методи багатокритеріального аналізу. Наприклад, у сфері медицини та ювелірної справи були розроблені аналітичні моделі, засновані на теорії нечітких множин, для підвищення безпеки транзакцій.

Блокчейн уже зарекомендував себе як перспективна технологія, що активно трансформує фінансовий сектор, бізнес-процеси та інфраструктуру розумних міст. Його ключові переваги включають:

1) децентралізацію, що усуває необхідність у посередниках,

2) прозорість, яка забезпечує відкритий доступ до всіх записів у мережі,

3) автоматизацію, що дозволяє смарт-контрактам виконувати операції без втручання третьої сторони,

4) посилену безпеку, яка ускладнює шахрайство або маніпуляції з даними.

Попри численні переваги, впровадження блокчейн-рішень супроводжується певними викликами. Зокрема, складність у створенні безпечних смарт-контрактів, а також вибір оптимальної платформи для конкретних потреб залишається важливим завданням. Подальші дослідження спрямовані на розробку ефективних

методів оцінювання рівня безпеки та продуктивності блокчейн-систем для забезпечення їх надійності в майбутньому.

1.3.2. Багатоакторна та однофакторна аутентифікація.

Багатофакторна аутентифікація - є першою лінією захисту від несанкціонованого доступу та ключовим елементом у забезпеченні безпеки інформаційних систем[37]. Цей процес передбачає перевірку особи користувача, який намагається отримати доступ до пристрою чи онлайн-сервісу. Перший етап аутентифікації - це реєстрація, під час якої користувач вводить свої дані, такі як логін, пароль та електронну пошту. Ця інформація зберігається на сервері та використовується для подальшої ідентифікації під час входу в систему.

Процедура перевірки особи складається з кількох послідовних кроків:

1) реєстрація - введення персональних даних користувача (логін, пароль, електронна пошта або інші ідентифікатори),

2) передача облікових даних - відправлення введеної інформації на сервер для обробки,

3) зіставлення даних - система перевіряє відповідність отриманої інформації з тією, що збережена у базі даних,

4) авторизація - у разі успішного проходження перевірки користувач отримує доступ до системи, а в разі помилки може знадобитися додаткова перевірка або блокування входу.

Багатофакторна аутентифікація (MFA) - це механізм, що вимагає від користувача проходження перевірки за допомогою двох або більше факторів, таких як пароль у комбінації з біометричними даними або апаратним ключем. Це значно підвищує рівень безпеки, оскільки для злому зловмисник має подолати декілька рівнів захисту одночасно.

Попри високу ефективність, MFA також має свої слабкі місця:

1) фішингові атаки[39] - користувачів можуть обманом змусити надати всі необхідні фактори аутентифікації,

2) перехоплення OTP-кодів[40] - якщо використовується одноразовий пароль (OTP), його можна перехопити за допомогою шкідливого програмного забезпечення,

3) соціальна інженерія[41] - зловмисники можуть маніпулювати користувачами, змушуючи їх розголошувати конфіденційну інформацію,

4) залежність від пристроїв - використання апаратних токенів або смартфонів для аутентифікації може ускладнити доступ у разі їх втрати або крадіжки.

Попри ці ризики, багатофакторна аутентифікація залишається найефективнішим способом захисту облікових записів і персональних даних.

Хоча існує багато різних моделей багатофакторної аутентифікації, жодна з них не є універсальною. Це створює труднощі як для розробників, так і для кінцевих користувачів, адже кожна система потребує індивідуального підходу для досягнення оптимального рівня безпеки.

Саме тому подальші дослідження у сфері кібербезпеки спрямовані на розробку гнучких рішень, здатних адаптуватися до різних технологічних середовищ та типів загроз, забезпечуючи баланс між зручністю користування та рівнем захисту.

1.3.3. Система виявлення та запобігання вторгненням

Система виявлення вторгнень (IDS, Intrusion Detection System) - це технологія, що дозволяє виявляти загрози та спроби несанкціонованого доступу шляхом аналізу мережевого трафіку[43]. IDS працює в режимі 24/7, контролюючи активність у мережі, відстежуючи поведінку користувачів та створюючи звіти для адміністраторів безпеки.

Головна мета системи IDS - виявлення підозрілих дій та загроз, зокрема:

1) атаки на мережеві сервіси, що містять вразливості,

2) спроби отримання підвищених привілеїв у системі,

3) несанкціоновані дії з конфіденційними файлами,

4) виявлення активності шкідливого програмного забезпечення (вірусів, троянів, черв’яків тощо).

IPS працює в режимі реального часу, аналізуючи мережевий трафік на предмет небезпечної активності та порівнюючи його зі встановленими профілями загроз. Якщо система визначає відповідність певному патерну атак, вона може:

1) створити попередження для адміністратора,

2) блокувати або відхиляти шкідливий трафік ще до його потрапляння в мережу.

Основна мета IPS - зупинити атаку ще на етапі її виконання, запобігаючи потенційному збитку.

Для забезпечення комплексного захисту мережі компанії використовують IDS/IPS у поєднанні з брандмауерами (файрволами) та маршрутизаторами. Головна відмінність між цими системами полягає в наступному брандмауери (файрволи) контролюють трафік за IP-адресами та номерами портів, приймаючи або блокуючи його відповідно до заданих правил.

Файрволи аналізують пакети за сигнатурами загроз:

1) якщо пакет відповідає дозволеним правилам, він проходить далі,

2) якщо ні - трафік блокується.

Файрвол слугує першою лінією захисту, яка запобігає проникненню загроз у мережу. Однак його функціонал є обмеженим, оскільки він може виявляти лише певні типи атак. Саме тому IDS/IPS розміщують між зовнішнім і внутрішнім брандмауером для детального аналізу мережевого трафіку.

IDS/IPS часто встановлюється між мережевим портом і веб-сервером, що дозволяє аналізувати всі вхідні пакети та порівнювати їх із базою відомих загроз. Таким чином, інтеграція цих систем забезпечує додатковий рівень безпеки для веб-ресурсів, доступних через Інтернет, і мінімізує ризики вторгнень.

1.3.4 Інтеграція Інтернету речей у міське середовище

Впровадження технологій Інтернету речей (IoT, Internet of Things) у міську інфраструктуру знаменує новий етап у розвитку сучасних міст, змінюючи підходи до їх проєктування, управління та функціонування. У міру зростання урбаністичних територій міста стикаються з низкою викликів, зокрема транспортними перевантаженнями, екологічними проблемами, високим рівнем енергоспоживання та питаннями громадської безпеки. IoT відкриває нові можливості для вирішення цих питань, пропонуючи технологічні рішення, що не лише оптимізують міські процеси, а й адаптують міське життя до вимог XXI століття[24,26].

Використання IoT у міському просторі

Технології Інтернету речей застосовуються в різних сферах міського господарства, зокрема:

1) транспорт - інтелектуальні системи управління дорожнім рухом допомагають мінімізувати затори, зменшити рівень викидів CO_2 та підвищити комфорт пересування для мешканців,

2) енергетика - розумні електромережі (smart grids) дозволяють оптимізувати енергоспоживання, інтегрувати відновлювані джерела енергії та підвищити стабільність та екологічність енергосистем,

3) комунальне господарство - використання IoT у сферах управління відходами, постачання води та екологічного моніторингу сприяє підвищенню ефективності міських сервісів та покращенню рівня життя населення,

4) вплив IoT на міську екосистему,

5) аналіз даних, отриманих від мережі підключених пристроїв, дає змогу міським адміністраціям ухвалювати обґрунтовані рішення, що балансують між економічними, соціальними та екологічними потребами. Це сприяє створенню більш витривалого та стійкого міського середовища.

Сучасні технології формують фундамент розумних міст, які стають більш ефективними, екологічно свідомими та комфортними для мешканців. Інтернет

речей відіграє ключову роль у цій трансформації, об’єднуючи фізичні пристрої та інформаційні системи для збору, аналізу та оптимізації міської інфраструктури[31].

Впровадження IoT у процеси управління міськими ресурсами дозволяє містам бути більш адаптивними до змін, підвищує їхню стійкість до зовнішніх викликів та сприяє сталому розвитку, що є критично важливим у сучасних умовах урбанізації.

1.4 Формулювання завдання

Ефективний розвиток концепції «Розумного міста» (Smart City) потребує впровадження надійних механізмів управління безпекою, які забезпечать безпечну та ефективну взаємодію між міськими структурами, громадянами та міською інфраструктурою. У сучасних міських системах безпеки спостерігаються наступні проблеми:

Підвищена вразливість до кібератак, що спрямовані на централізовані системи управління.

Складнощі з ідентифікацією та контролем доступу до критично важливих міських об’єктів.

1) відсутність прозорих механізмів аудиту дій службових осіб та користувачів,
2) високі корупційні ризики, пов’язані з розподілом прав доступу,
3) недостатній рівень автоматизації у системах реагування на потенційні загрози.

Традиційні централізовані підходи до управління безпекою міської інфраструктури не гарантують належного рівня захисту, що вимагає розробки нових, більш ефективних рішень. Інноваційні блокчейн-технології та смарт-контракти дають змогу реалізувати автоматизовану, децентралізовану та прозору систему управління безпекою у «Розумному місті», що дозволяє знизити ризики атак на централізовані системи та уникнути можливих маніпуляцій із даними.

Основні завдання дослідження:

1) провести аналіз сучасних підходів до управління безпекою у «Розумному місті» та визначити їхні обмеження.

2) дослідити потенціал використання блокчейн-технологій і смарт-контрактів для оптимізації безпекових процесів,

3) розробити та протестувати прототип системи управління безпекою, оцінити її ефективність та можливість практичного застосування.

1.5 Висновки

Здійснено огляд сучасного стану досліджень у сфері управління безпекою смарт-сервісів в умовах розумного міста. Проаналізовано існуючі підходи до забезпечення безпеки в IoT-інфраструктурах, досліджено архітектури та принципи функціонування програмно-визначених мереж (SDN), особливості використання блокчейн-технологій, зокрема смарт-контрактів, у контексті захисту даних і контролю доступу. Розглянуто переваги й обмеження централізованих та децентралізованих систем безпеки, що дозволило виявити основні недоліки сучасних рішень - обмежена гнучкість, відсутність механізмів адаптації до контексту середовища та ускладнене масштабування.

У результаті аналізу сформульовано базові вимоги до майбутнього методу управління безпекою, який має поєднувати переваги SDIoT та блокчейн-технологій, забезпечуючи динамічне прийняття рішень щодо автентифікації, авторизації та контролю доступу в умовах взаємодії великої кількості гетерогенних смарт-сервісів. Отримані висновки стали основою для побудови концептуальної моделі управління безпекою, що представлена в наступному розділі.

2 МОДЕЛЬ ПРОЦЕСУ УПРАВЛІННЯ БЕЗПЕКОЮ НА ОСНОВІ СМАРТ-КОНТРАКТІВ ДЛЯ ВЗАЄМОДІЇ СЛУЖБ “РОЗУМНОГО МІСТА”

2.1 Функціональні суб’єкти моделі керування безпекою смарт-сервісів

Вирішення поставленої задачі керування безпекою у середовищі смарт-міста ґрунтується на взаємодії низки функціональних суб’єктів, кожен із яких відіграє визначену роль у контексті ініціювання, маршрутизації, перевірки, підтвердження автентичності, динамічного оцінювання довіри та реалізації сервісних транзакцій. У моделі методологічного підходу особливу увагу приділено координації між смарт-сервісами, контролерами програмно-визначеної мережі (SDN), агентами взаємодії та механізмами, які реалізують інтеграцію з блокчейн-інфраструктурою. Така побудова забезпечує гнучкість, адаптивність і відповідність динамічним вимогам безпеки в реальному часі.

Умовно, модель взаємодії складається з чотирьох ключових суб’єктів.

Сервіс А - ініціатор транзакції. Цей смарт-сервіс виступає як відправник інформаційного запиту або ініціатор початкової взаємодії. У типових сценаріях це можуть бути сервіси моніторингу навколишнього середовища, системи відеоспостереження, енергетичні датчики або сервіси збору телеметрії. Сервіс А генерує повідомлення у форматі, що включає мета-дані, цифрові ідентифікатори, хеш-підпис, відкритий ключ, позначки часу, контекстні атрибути (наприклад, тип запиту, рівень критичності) та криптографічну інформацію. Повідомлення передається до SDN-контролера через локального агента, де попередньо шифрується з використанням ECC і підписується приватним ключем сервісу.

Сервіс В - приймальний оброблювач. Цей смарт-сервіс виступає як виконавець, надавач або приймач даних у відповідь на запит сервісу А. Його завдання полягає у верифікації автентичності запиту, оцінці рівня довіри до сервісу А, перевірці відповідності наданим політикам доступу та прийнятті рішення щодо виконання дії. Сервіс В може представляти критичні інфраструктури: наприклад, медичні системи, аварійні служби, логістичні центри або електромережі. Якщо всі

перевірки пройдено успішно, сервіс B генерує відповідь у форматі узгодженого смарт-контракту, який також підписується і реєструється в блокчейн-мережі

SDN-контролер - логічне ядро керування. Центральний елемент архітектури SDIoT, який забезпечує керування потоками даних, маршрутизацію запитів, а також ініціацію локальних механізмів безпеки. Контролер реалізує базову автентифікацію, виконує оцінку довіри на початкових етапах взаємодії та передає транзакції до агентів для подальшої обробки. Він формує вузол взаємодії між фізичним рівнем (IoT-вузли) та логічними елементами (блокчейн, адаптивні рушії, API інтерфейси).

Агенти взаємодії - універсальні компоненти забезпечення комунікацій. Агенти реалізують проміжну логіку між SDN-контролером, смарт-сервісами, адаптивними рушіями безпеки та блокчейн-середовищем. У моделі виділено кілька типів агентів:

1) агенти локальної безпеки - забезпечують комунікацію між SDN-контролером та локальним блокчейн-ланцюгом;

2) агенти глобального управління політиками - працюють з глобальним блокчейн-середовищем, передаючи транзакції для перевірки та інтеграції політик;

3) агенти сервісів - керують запитами від прикладних служб, інтегруючи їх з контекстними модулями та механізмами безпеки.

Узгоджена взаємодія між цими суб’єктами забезпечує дотримання основних принципів безпеки (конфіденційність, цілісність, доступність), адаптивне оновлення політик на основі контексту, забезпечення перевірки автентичності на всіх етапах транзакцій та мінімізацію людського втручання. Також важливо зазначити, що кожен із суб’єктів функціонує в межах строго регламентованої взаємодії, яка реалізується через багаторівневу блокчейн-архітектуру, смарт-контракти безпеки та механізми динамічної довіри [45], [70], [91].

Візуальна модель взаємодії функціональних суб’єктів представлена на рисунку 2.1.

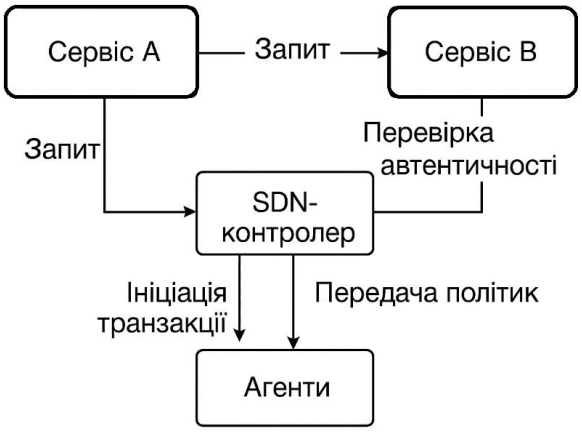

Рисунок 2.1 - Функціональна модель взаємодії суб’єктів методу управління безпекою.

У представленій моделі (рис. 2.1) чітко окреслено логіку послідовної передачі інформації, валідації повідомлень, застосування смарт-контрактів, а також участь кожного з елементів у повному циклі управління безпекою - від ініціації до завершення транзакції. Такий підхід дозволяє масштабувати запропоновану одель у рамках великих інфраструктурних рішень для інтелектуальних міст, підвищуючи загальний рівень захисту цифрових сервісів.

2.2 Взаємодія суб’єктів та логіка реалізації моделі керування безпекою

Ефективність функціонування системи управління безпекою у середовищі смарт-міста значною мірою визначається логікою та стабільністю взаємодії між її основними компонентами. Вся система побудована на принципах взаємозалежності між сервісами, контролерами, агентами та блокчейн-інфраструктурою, що забезпечує цілісність, адаптивність і захищеність процесів обміну даними.

Взаємодія між компонентами починається на прикладному рівні, де сервіс А формує структурований запит. Цей запит містить всі необхідні мета-дані, ідентифікаційні ключі та атрибути доступу, після чого він передається SDN-контролеру. Саме на цьому етапі SDN-контролер визначає маршрут проходження

запиту, застосовує політики фільтрації та виконує перевірку автентичності IoT-вузла. Крім того, контролер взаємодіє з локальним агентом безпеки для ініціалізації відповідного запису у локальному блокчейні.

Після верифікації запит надходить до локального рушія безпеки, де відбувається формування локального контракту, який описує права доступу до сервісу B. Контракт створюється у форматі JSON, зберігається в локальному каналі MultiChain і дублюється через агента політик до глобального блокчейну. Тут запускається механізм глобального узгодження - об’єднання локальних політик із загальними адміністративними правилами безпеки.

Далі контекстний рушій виконує контекстну обробку: визначається актуальний рівень довіри, перевіряється статус учасників, зчитуються обмеження, пов’язані з типом події. Результати цього аналізу передаються до рушія виконання, який ініціює запуск транзакції - наприклад, надсилання сигналу про тривогу, передача GPS-координат або активація зовнішнього API.

Комунікація між компонентами забезпечується за допомогою криптографічного захисту та синхронізації з блокчейн-каналами. Кожен обмін повідомленнями між сервісами супроводжується хешуванням, шифруванням публічними ключами та верифікацією цифрових підписів. Такий рівень зв’язків гарантує, що система залишається стійкою до зовнішніх загроз навіть при високому навантаженні або збільшенні кількості взаємодіючих учасників.

На рисунку 2.2 представлено логіку взаємозв’язків між основними компонентами системи. Візуалізація ілюструє повний цикл: від надходження запиту до виконання дії - з виділенням ключових точок взаємодії, ролей агентів та блоків обміну політиками. Цей рисунок дозволяє краще зрозуміти внутрішню узгодженість архітектури та її здатність динамічно адаптуватися до змін у середовищі смарт-міста.

Ефективність функціонування моделі управління безпекою у середовищі смарт-міста визначається логікою та узгодженістю взаємодії між його ключовими суб’єктами. Цей процес базується на обміні даними між сервісами, контролерами,

агентами та блокчейн-компонентами, що забезпечує цілісність, адаптивність та динамічну реакцію на загрози.

Початковий етап взаємодії розпочинається з того, що сервіс A формує запит у вигляді структурованого повідомлення:

$$M = \{ i, t, m, k, h \}, \tag{2.1}$$

де:

1) i - ідентифікатор запиту;
2) t - мітка часу;
3) m - текст повідомлення;
4) k - публічний ключ відправника;
5) h = H(m) - хеш повідомлення.

Перед відправленням запит шифрується за допомогою публічного ключа отримувача r:

$$c = E(m, r), \tag{2.2}$$

Після шифрування повідомлення надходить до SDN-контролера, який проводить автентифікацію та перевіряє достовірність структури. Перевірка цифрового підпису виконується наступним чином:

$$v = V(m, s, k), \tag{2.3}$$

де:

1) v - результат перевірки,
2) s - цифровий підпис,
3) k - ключ перевірки.

У разі успішної перевірки SDN-контролер формує запис у локальному реєстрі блокчейну та передає запит до локального адаптивного рушія, який генерує політичний контракт:

$$p = \{ a, r, p, t \}, \tag{2.4}$$

де:

1) a - автентифікаційні параметри,
2) r - ролі,
3) p - правила доступу,
4) t - довірчий рівень.

Контракт дублюється через агента політик до глобального адаптивного рушія, де здійснюється об’єднання локального та глобального рівнів:

$$p' = p \cup q, \tag{2.5}$$

де:

1) q - набір адміністративних політик.

Контекстний рушій виконує оцінку довіри d, яка обчислюється за формулою:

$$d = w \cdot c + (1 - w) \cdot p, \tag{2.6}$$

де:

1) w - ваговий коефіцієнт,
2) c - поточна довіра,
3) p - попередня довіра.

Далі перевіряється, чи перевищує значення d поріг t

$$d \geq t, \tag{2.7}$$

Якщо умова дотримана, запускається механізм виконання транзакції:

$$t = f(m), \tag{2.8}$$

якщо d ≥ t

Результатом є виконання необхідної дії, такої як передача координат або виклик API, з обов'язковою реєстрацією у глобальному блокчейні.

На рисунку 2.2 ілюстровано весь процес - від формування запиту до виконання дії, із деталізацією ключових етапів: криптографічного захисту, узгодження політик, динамічного обчислення довіри та реалізації транзакцій.

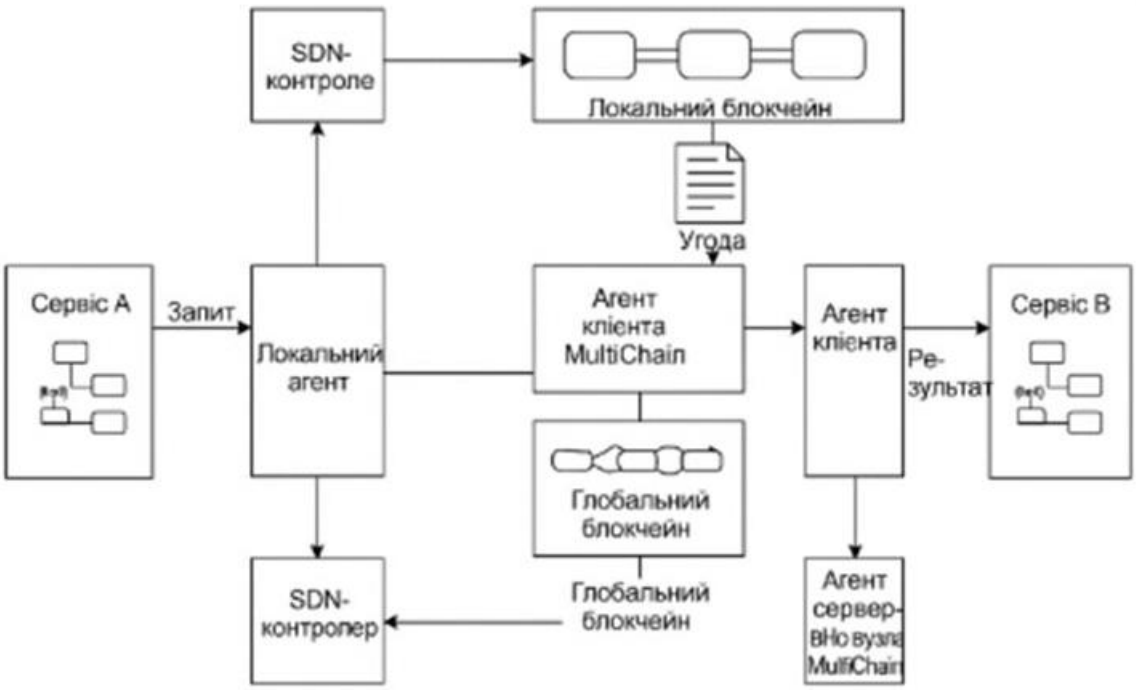

Рисунок 2.2 - Архітектурна модель управління безпекою розумного міста

2.3 Модель життєвого циклу смарт-контрактів у системі

У межах запропонованої моделі керування безпекою смарт-сервісів важливою складовою є життєвий цикл смарт-контракту. Цей цикл охоплює всі фази функціонування контракту - від моменту його створення до завершення

взаємодії, включно з перевірками, узгодженням, активацією та виконанням. Його реалізація базується на інтеграції сервісів, SDN-контролерів, агентів політик та розподіленої блокчейн-системи MultiChain. Завдяки послідовності операцій забезпечується цілісність логіки безпеки, простежуваність транзакцій і гнучкість у реалізації сценаріїв взаємодії.

Початковою фазою для життєвого циклу смарт-контракту є ініціювання взаємодії, ця інформація відображена на рисунку 2.3. Сервіс A формує запит до сервісу B, створюючи структуру, що включає унікальний ідентифікатор i, відкритий ключ k, опис дії s та параметри сесії a. Для збереження конфіденційності запит шифрується за публічним ключем адресата r за формулою:

$$c = E(r, i, k, s, a), \tag{2.9}$$

де

1) E - криптографічна функція шифрування.

Отриманий пакет передається SDN-контролеру, який проводить первинну перевірку достовірності та ініціює комунікацію з локальним агентом безпеки.

Далі відбувається генерація локального контракту безпеки. Агент формує політичний шаблон контракту у вигляді множини параметрів:

$$p = \{a, r, p, t\}, \tag{2.10}$$

де

1) a - автентифікаційні дані,
2) r - ролі учасників,
3) p - набір правил доступу,
4) t - первинна довірча оцінка.

Згенерований контракт фіксується у локальному блокчейні у форматі JSON, отримуючи статус чернетки.

Після цього відбувається узгодження на глобальному рівні. Локальний агент передає контракт через MultiChain до глобального рушія політик, який порівнює надані параметри з адміністративними правилами q. Формується узагальнена політика:

$$p' = p \cup q, \tag{2.11}$$

і контракт переходить у статус «узгоджений», якщо перевірка пройдена успішно.

На етапі активації контекстний рушій проводить динамічну перевірку актуальності параметрів і виконує оцінку довіри між учасниками:

$$d = \omega \cdot c + (1 - \omega) \cdot p, \tag{2.12}$$

де

1) d - нова довірча оцінка,
2) ω - ваговий коефіцієнт ($0 < \omega < 1$),
3) c - поточна оцінка довіри,
4) p - попереднє значення.

Контракт активується, якщо d перевищує порогове значення τ.

Активація контракту відкриває доступ до сервісних функцій. Під час виконання відбувається обмін зашифрованими повідомленнями, активація зовнішніх API або інших сервісів. Усі дії логуються у журналі MultiChain із цифровими підписами та хеш-функціями, що унеможливлює підміну або несанкціоновані зміни.

На завершальному етапі контракт переводиться у стан «виконано» або «відкликано» залежно від результатів взаємодії. Контракт переноситься до архіву для майбутнього аудиту, повторного використання чи аналітики.

2.4 Формалізація моделі

Формалізація моделі управління безпекою в інфраструктурі смарт-міста є необхідною умовою для забезпечення узгодженої, прозорої та захищеної взаємодії між смарт-сервісами. Вона охоплює опис основних процесів - від ініціації запиту до його виконання - і включає логіку перевірки достовірності, авторизації, генерації смарт-контрактів, оцінки довіри та фіксації результатів транзакцій у блокчейн-середовищі. Такий формалізований підхід дозволяє зменшити ймовірність помилок, підвищити ступінь захищеності та забезпечити масштабованість запропонованої системи.

Рисунок 2.3 - Модель життєвого циклу смарт-контрактів у системі

У межах запропонованої моделі кожен смарт-сервіс оперує через відкриті точки взаємодії у вигляді API-інтерфейсів, які забезпечують доступ до функціоналу, зокрема - ініціацію колаборативних запитів, передачу атрибутів доступу та метаданих. Ініціатива запиту належить сервісу A, який формує повідомлення, що включає унікальний ідентифікатор, часову мітку, цифровий підпис та параметри сесії. Це повідомлення надсилається до SDN-контролера, який виконує верифікацію підпису, перевіряє цілісність пакету та порівнює вхідні параметри з локальними політиками доступу, визначеними в межах політичного контракту.

У випадку успішної верифікації SDN-контролер ініціює створення локального смарт-контракту. Формується набір правил безпеки, що регламентує доступ, автентифікацію, дозволені дії та допустимі сценарії взаємодії. Цей контракт зберігається у форматі JSON у відповідному локальному каналі MultiChain. Застосування саме формату JSON зумовлене необхідністю універсальної інтерпретації даних між компонентами системи. Наступним кроком є передача цього контракту на глобальний рівень через агента політик, що координує обмін між локальними та глобальними компонентами.

Глобальний рушій аналізує наданий контракт на предмет відповідності адміністративним політикам міської інфраструктури. У результаті формується об’єднаний набір правил, що враховує як локальні обмеження, так і загальноміські нормативи. Якщо умови узгоджені, контракт передається до контекстного рушія, який виконує оцінку довіри, базуючись на історії взаємодій, репутаційних записах та контекстуальній інформації.

Оцінювання довіри виконується на основі кумулятивної моделі. Поточна довірча оцінка d розраховується як зважене середнє між новою (c) та попередньою (p) оцінками:

$$d = w \cdot c + (1 - w) \cdot p, \tag{2.13}$$

де

1) d - агрегована довіра,
2) w - ваговий коефіцієнт, що задається адміністративно;
3) c - поточна оцінка довіри,
4) p - попередня довіра.

Контракт активується, якщо $d \geq \tau$, де τ - порогове значення довіри. Таким чином, забезпечується елемент адаптивності: лише сервіси з достатнім рівнем довіри можуть активувати взаємодію.

Після активації контракту виконується передбачене дією: обмін повідомленнями, доступ до даних, ініціація зовнішніх API або інших сервісів. Усі

події фіксуються у MultiChain у вигляді транзакцій із цифровими підписами та гешами, що гарантує незмінність та прозорість взаємодії. Цей підхід дозволяє реалізувати аудиторський слід, що є важливим для оцінки безпеки після завершення транзакцій.

Таким чином, формалізована модель дає змогу чітко структурувати процеси, визначити учасників, атрибути, правила доступу та механізми перевірки на всіх рівнях взаємодії. Вона є основою для подальшої автоматизації, інтелектуального аналізу політик та динамічного налаштування безпеки в умовах змінного середовища смарт-міста. Створена структура підтримує принцип мінімальних привілеїв, розмежування доступу, контекстної адаптації та репутаційного зважування, що відповідає сучасним вимогам до систем розподіленої безпеки.

2.5 Модель довіри та контролю доступу

Ефективне управління доступом у розподіленому середовищі смарт-міста потребує гнучкої, контекстно-орієнтованої та адаптивної моделі оцінювання довіри. На відміну від традиційних підходів, що базуються виключно на попередньо визначених правилах авторизації, запропонована модель передбачає постійне динамічне оновлення довіри між учасниками взаємодії, враховуючи історичні, поведінкові та контекстні фактори. Це дозволяє системі адаптуватися до змінного середовища, знижувати ризики зловживань та підтримувати високий рівень безпеки без зменшення гнучкості процесів.

У розробленій архітектурі процес довіри починається з побудови профілю кожного сервісу. Цей профіль формується на основі даних із локального та глобального блокчейн-реєстрів, де зберігається інформація про попередні транзакції, кількість успішних та невдалих взаємодій, частоту звернень, час відповіді, відповідність політикам доступу та результати автентифікації. Кожен новий запит супроводжується оцінкою поточного значення довіри, що агрегується за допомогою зваженої формули:

$$d = w \cdot c + (1 - w) \cdot p, \quad (2.14)$$

де

1) d - поточна довіра,

2) w - ваговий коефіцієнт, що визначає вплив останньої взаємодії ($0 < w < 1$),

3) c - нова оцінка на основі поточної транзакції, p - попереднє значення довіри.

Цей підхід дозволяє точно регулювати чутливість моделі: для критичних сервісів (напр., медичних або аварійних) встановлюється нижчий w, що забезпечує стабільність; для динамічних або експериментальних сервісів - вищий, що гарантує швидке реагування на зміну поведінки.

Контекст взаємодії також враховується при обчисленні довіри. Модель аналізує тип запиту, роль ініціатора, рівень доступу, навантаження на мережу, час доби, політики, що діють у поточному контексті. Усі ці параметри впливають на вагу оцінки або порогове значення довіри τ. Якщо обчислене значення d перевищує τ, запит дозволяється; у протилежному випадку - блокується або передається на повторну перевірку вручну або за допомогою контекстного рушія.

Порогове значення довіри τ може змінюватись динамічно. Його значення коригується на основі статистики системи, історії взаємодій, середнього рівня довіри в мережі або поведінкових шаблонів сервісу. Це запобігає хибним блокуванням через короткострокові збої та дозволяє вчасно виявляти потенційно шкідливу поведінку. Наприклад, у разі різкого зниження стабільності сервісу значення τ може автоматично підвищитись.

Модель підтримує двосторонній зворотний зв’язок між рушієм довіри та механізмом політик доступу. Отримані значення d використовуються для прийняття рішень щодо доступу, а також можуть ініціювати зміни у політиках - наприклад, обмежити доступ до окремих функцій або змінити вимоги до автентифікації. Таким чином, модель не лише фільтрує небажані запити, а й

активно впливає на поведінку системи, забезпечуючи динамічну перебудову взаємодій.

У рамках моделі було запропоновано використання смарт-контрактів для фіксації та перевірки результатів обчислення довіри. Контракт містить усі атрибути: ідентифікатор транзакції, значення довіри d, ваговий коефіцієнт w, порогове значення τ та результат прийняття рішення. Це дозволяє забезпечити прозорість і простежуваність кожного рішення, а також використовувати ці дані для подальшого машинного аналізу, аудиту або самонавчання системи.

На рисунку 2.4 представлено узагальнений механізм оцінювання довіри між сервісами, що включає етапи автентифікації, оновлення профілю довіри, порівняння з порогом, прийняття рішення та фіксацію результату у блокчейні. Це візуалізує взаємозв'язок між логікою доступу, політиками безпеки та механізмами динамічного регулювання взаємодії в системі смарт-міста.

У доповнення до класичної моделі обчислення довіри в рамках моделі управління доступом у смарт-місті запропоновано вдосконалений підхід, що враховує стабільність поведінки учасників. Такий механізм дає змогу зменшити ймовірність хибнопозитивних або хибнонегативних рішень у випадках, коли довіра змінюється нестабільно або носить маніпулятивний характер.

Запропонована модель базується на концепції варіативності - показника σ, який описує дисперсію довіри для певного сервісу протягом обраного вікна часу або транзакцій. Таким чином, оцінка довіри доповнюється новим параметром - стабільністю довірчого профілю. Сервіси з низьким рівнем варіативності отримують пріоритет у доступі, оскільки вважаються більш передбачуваними та надійними.

2.6 Адаптивна модель довіри з урахуванням стабільності поведінки

Оновлена функція обчислення довіри формалізується наступним чином:

$$d = \alpha \cdot c + \beta \cdot p + \gamma \cdot (1 - \sigma'), \tag{2.15}$$

де:

1) d - скориговане значення довіри;

2) c - останнє зафіксоване значення довіри на основі поточної взаємодії;

3) p - попереднє усереднене значення довіри;

4) σ' - нормалізоване стандартне відхилення за останні n транзакцій ($0 \leq \sigma' \leq 1$);

α, β, γ - вагові коефіцієнти, що регулюють вплив відповідного параметра, де $\alpha + \beta + \gamma = 1$.

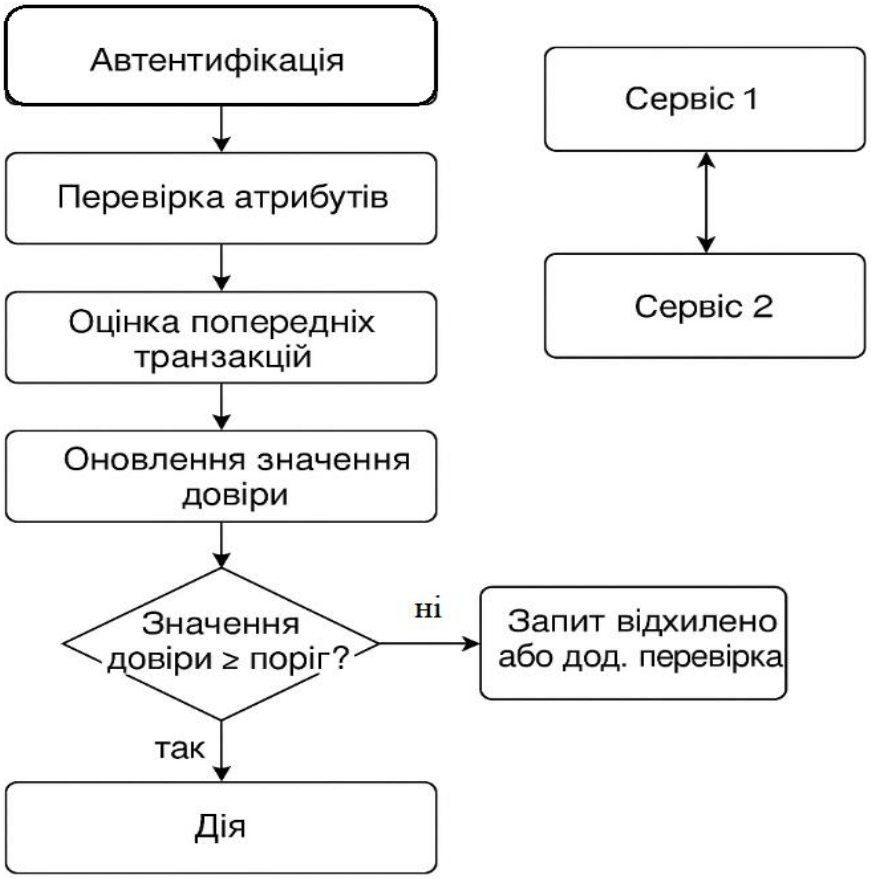

Рисунок 2.4 - Модель оцінювання довіри та контролю доступу між сервісами у смарт-місті

Використання нормалізованого значення $(1 - \sigma')$ гарантує, що менша варіативність довіри має більший позитивний внесок у фінальне значення d. Це дозволяє адаптувати модель до різних сценаріїв: підвищити обережність у

взаємодії з нестабільними вузлами, одночасно стимулюючи тривалу надійну поведінку з боку сервісів.

Такий підхід також дозволяє модифікувати політики контролю доступу динамічно - залежно від змін у стабільності поведінки сервісу. Наприклад, навіть при високому середньому значенні довіри, різка нестабільність у поведінці викликає зниження оцінки й відповідне коригування дозволених дій. Навпаки, сервіси зі стабільною взаємодією отримують полегшений доступ, знижуючи навантаження на механізми додаткової перевірки.

Таким чином, запропонована модель забезпечує не лише точніше оцінювання довіри, але й підвищує загальну резистентність системи до поведінкових аномалій і динамічних загроз у середовищі смарт-міста.

2.7 Висновки

Було розроблено цілісну модель процесу управління безпекою на основі смарт-контрактів для взаємодії служб розумного міста. Побудовано базову архітектуру з інтеграцією SDIoT, блокчейн-технологій і платформи MultiChain, що формує основу для децентралізованого й прозорого середовища керування безпекою.

У межах моделі розглянуто ключові суб’єкти системи та типи їхньої взаємодії, а також сформульовано життєвий цикл смарт-контрактів - від ініціації до реалізації політик доступу. Проведено формалізацію взаємозв’язків між компонентами системи, включно з алгоритмами обміну даними, побудовою ключових структур і криптографічною аутентифікацією. Особливу увагу приділено побудові моделі довіри, яка адаптивно змінюється на основі історії взаємодій, порогових значень і контексту сервісу.

Представлена модель формує теоретичну основу для подальшої реалізації практичної системи, здатної до автоматизованого управління політиками безпеки в умовах смарт-міст. Її реалізацію та тестування буде докладно розглянуто у наступному розділі.

3 МЕТОД УПРАВЛІННЯ БЕЗПЕКОЮ НА ОСНОВІ СМАРТ-КОНТРАКТІВ ДЛЯ ВЗАЄМОДІЇ СЛУЖБ “РОЗУМНОГО МІСТА”

3.1 Основи методу управління безпекою на основі смарт-контрактів для взаємодії служб “Розумного міста”

У даному методі управління безпекою, який орієнтований на децентралізовану, адаптивну взаємодію смарт-сервісів у цифровій інфраструктурі інтелектуального міста. Метод базується на інтеграції трьох ключових технологічних складових: програмно-керованого Інтернету речей (SDIoT), багаторівневої блокчейн-архітектури та механізмів смарт-контрактів, що забезпечують гнучке і масштабоване середовище безпеки.

Особливість методу полягає в тому, що він забезпечує динамічне формування політик безпеки у реальному часі - в залежності від контексту взаємодії, рівня довіри між сервісами та оцінки поточних ризиків. Запропонований підхід дозволяє не лише автоматизувати контроль доступу, автентифікацію та авторизацію учасників цифрової екосистеми, а й забезпечити адаптацію до змін у загрозовому ландшафті, що є критично важливим у високодинамічному середовищі смарт-міста.

На базі розробленого методу сформовано адаптивний рушій політик безпеки, функціонування якого забезпечується через смарт-контракти. Ці контракти виконують роль керованих політик - вони зберігаються у блокчейн-реєстрах, автоматично активуються в залежності від тригерних умов і забезпечують відтворюваність, прозорість та дотримання правил взаємодії між сервісами [70, 91].

Ключовими елементами запропонованого методу є:

1) модуль управління ключами та цифровими ідентифікаторами;
2) контекстно-орієнтоване прийняття рішень;
3) механізм оцінювання довіри;
4) життєвий цикл смарт-контрактів, що охоплює генерацію, публікацію, виконання та оновлення політик.

Таким чином, запропонований метод не є лише сукупністю функціональних модулів, а цілісною моделлю поведінки компонентів безпеки, яка реалізується через взаємодію окремих агентів, служб і інфраструктурних елементів. Завдяки використанню блокчейн-технологій метод забезпечує незмінність даних та доказову перевірку відповідності діям, що значно підвищує рівень довіри у середовищі смарт-міста [76, 78].

Запропонований метод управління безпекою було перевірено на практичну реалізованість шляхом моделювання прикладного сценарію, який демонструє децентралізовану взаємодію смарт-сервісів у контексті інфраструктури інтелектуального міста. Представлений сценарій взаємодії підтверджує доцільність впровадження методу в реальних умовах функціонування міських цифрових платформ.

Для оцінювання ефективності методу було використано низку технічних метрик, серед яких: пропускна здатність каналу безпеки, затримка доступу та обчислювальна складність виконання смарт-контрактів. Особливу увагу приділено дослідженню впливу різних довжин криптографічних ключів, зокрема еліптичної криптографії (ECC), на продуктивність та адаптивність безпекових процедур [3].

Проведено адаптивне тестування, що дозволило виявити здатність запропонованого методу своєчасно розпізнавати та локалізовувати загрози, динамічно адаптувати політики безпеки до змін середовища та підтримувати стійкість до потенційних атак. Це дозволяє реалізувати постійно самонавчальну архітектуру захисту, що еволюціонує разом із зростанням складності кіберзагроз.

Основою методу є інтеграція трьох провідних технологічних напрямів: програмно-визначеного Інтернету речей (SDIoT), багатоланцюгової блокчейн-інфраструктури та механізмів смарт-контрактів, які разом створюють синергетичну основу для побудови надійного середовища цифрової взаємодії [70], [91]. Метод дозволяє гнучко формувати правила взаємодії між сервісами, особливо у випадках виконання колаборативних завдань, де узгодженість і захищеність є критично важливими [76].

Особливу роль у реалізації методу відіграють механізми аутентифікації та авторизації доступу, які не є окремими функціями, а вбудовані безпосередньо у логіку смарт-контрактів, що виконуються у межах запропонованої архітектури. Це гарантує, що доступ до сервісних ресурсів отримують виключно довірені та перевірені суб'єкти, що унеможливлює несанкціоновані дії та підвищує загальний рівень безпеки в екосистемі смарт-міста [10], [13].

Описані конфігурації та параметри реалізації методу управління безпекою подано у вигляді програмованих скриптів, що відкрито опубліковані на платформах GitHub та Code Ocean. Це забезпечує прозорість підходу, можливість перевірки та відтворення результатів, а також дає змогу зацікавленим сторонам адаптувати запропоновану модель до власних умов.

У подальшому розділі докладно розглянуто технології та ключові складові, які лежать в основі розробленого методу, спрямованого на забезпечення безпечної взаємодії між смарт-сервісами. Як продемонстровано на рисунку 3.1, метод ґрунтується на тісній інтеграції трьох провідних технологічних напрямів: програмно-визначеного Інтернету речей (SDIoT), багатоланцюгової блокчейн-інфраструктури та смарт-контрактів. Ретельно вибудувана архітектура взаємодії цих компонентів створює передумови для впровадження гнучкого та масштабованого механізму безпеки, що здатен адаптуватися до різних сценаріїв цифрової взаємодії у смарт-місті.

3.2 Програмно-керований Інтернет речей (SDIoT) як складова методу управління безпекою

У межах запропонованого методу управління безпекою смарт-сервісів у середовищі інтелектуального міста ключовою складовою виступає концепція програмно-керованого Інтернету речей (SDIoT - Software-Defined Internet of Things). На відміну від класичних централізованих архітектур, метод SDIoT дозволяє створити гнучку, масштабовану та адаптивну модель взаємодії між IoT-

пристроями, сенсорними вузлами та сервісними компонентами, що функціонують у межах міської цифрової екосистеми [49].

Метод засновано на принципах програмно-визначених мереж, що забезпечує логічне розділення функцій управління та переспрямування трафіку. Завдяки цьому можлива централізована конфігурація політик безпеки, динамічна маршрутизація запитів та адаптивне реагування на зміни в середовищі. Такий підхід значно спрощує реалізацію колаборативних сценаріїв між смарт-сервісами, оскільки дозволяє узгоджено керувати доступом, автентифікацією та довірою на основі єдиної мережевої моделі.

У структурі методу передбачено три рівні SDIoT: прикладний, рівень контролера та рівень сприйняття. Ці рівні реалізують послідовну модель розподілу функціональних обов’язків, забезпечуючи прозору комунікацію між компонентами та підтримку механізмів безпеки. На рисунку 3.1 зображено загальну структуру безпекового середовища з урахуванням локальних та глобальних адаптивних рушіїв.

Прикладний рівень є ключовою частиною методу, що відповідає за об’єднання функціоналу різних смарт-сервісів. Саме тут реалізується логіка інтеграції API сервісів, безпечного зберігання ключів, взаємодії між компонентами та координації обміну повідомленнями в реальному часі. Такий підхід дозволяє досягти високого рівня взаємодії між учасниками цифрової інфраструктури розумного міста [46].

Рівень контролера виконує роль центрального модуля прийняття рішень. Тут розміщуються компоненти управління ключами, довірою та контрактами. Завдяки централізації логіки прийняття рішень забезпечується узгоджена реакція системи на запити сервісів, контроль за виконанням політик доступу та своєчасне оновлення довірчих параметрів.

На рівні сприйняття знаходяться IoT-вузли та сенсори, що забезпечують збір первинних даних із фізичного середовища. Цей рівень взаємодіє з контролером через протоколи SDN, надаючи інформацію для обробки й прийняття рішень у колаборативному середовищі.

Завдяки застосуванню методу SDIoT у поєднанні з блокчейн-технологіями та смарт-контрактами досягається високий рівень прозорості, захищеності й масштабованості інфраструктури безпеки. Це дозволяє ефективно реалізовувати адаптивні політики доступу та забезпечити стійкість до атак у складних мережевих сценаріях [70]. На рисунку 3.2 зображено типову архітектуру SDIoT, як основа методу управління безпекою

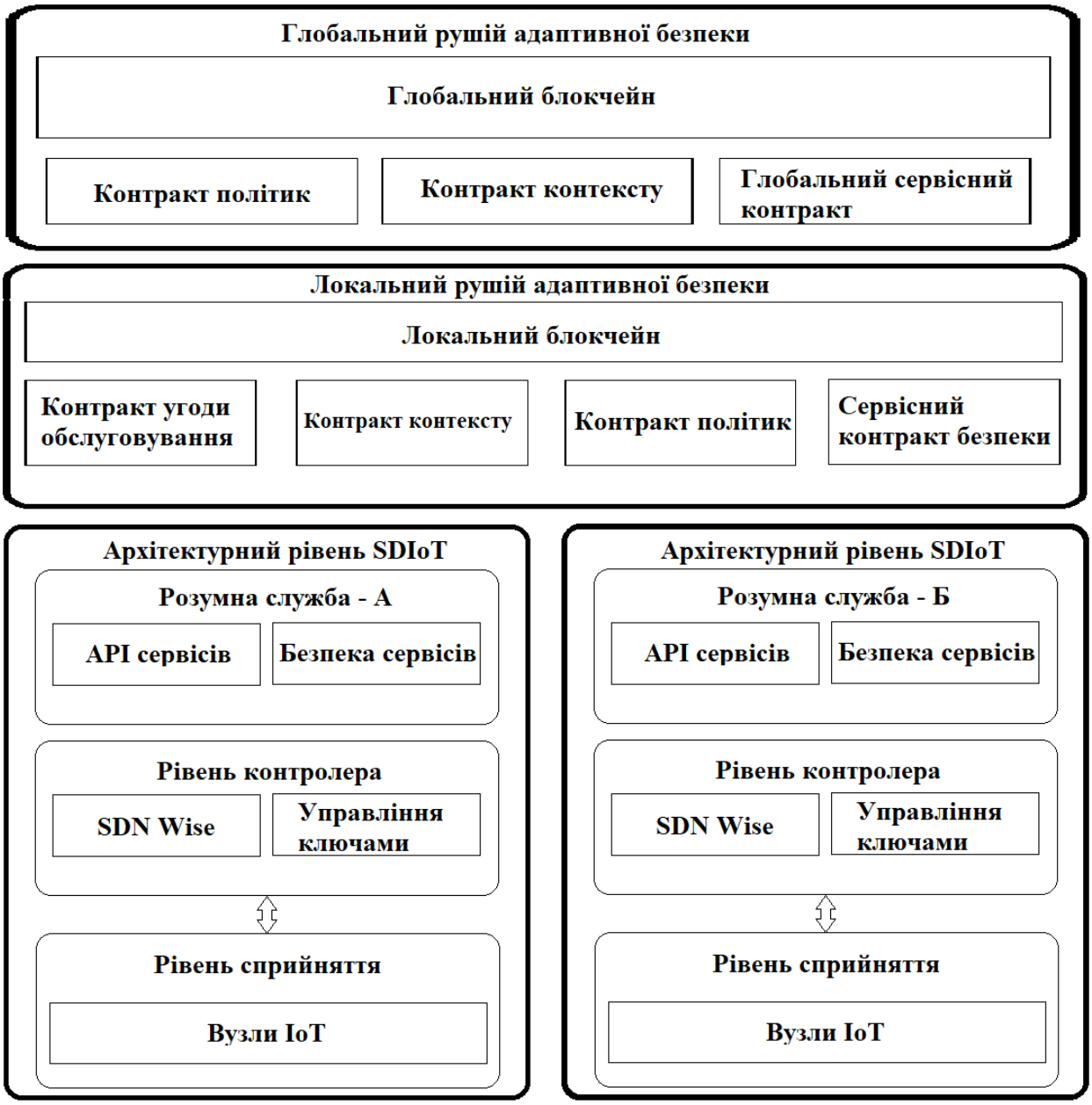

Рисунок 3.1 - Структура безпеки для спільних служб

3.3. Метод адаптивного управління безпекою на основі SDN-WISE та багатоланцюгового блокчейну

Метод управління безпекою смарт-сервісів, запропонований у цьому дослідженні, базується на застосуванні концепції SDN-WISE як архітектурної платформи, що дозволяє реалізувати динамічну маршрутизацію, керування потоками, а також підтримку гнучкої мережевої взаємодії між сервісами в межах інтелектуального міста.

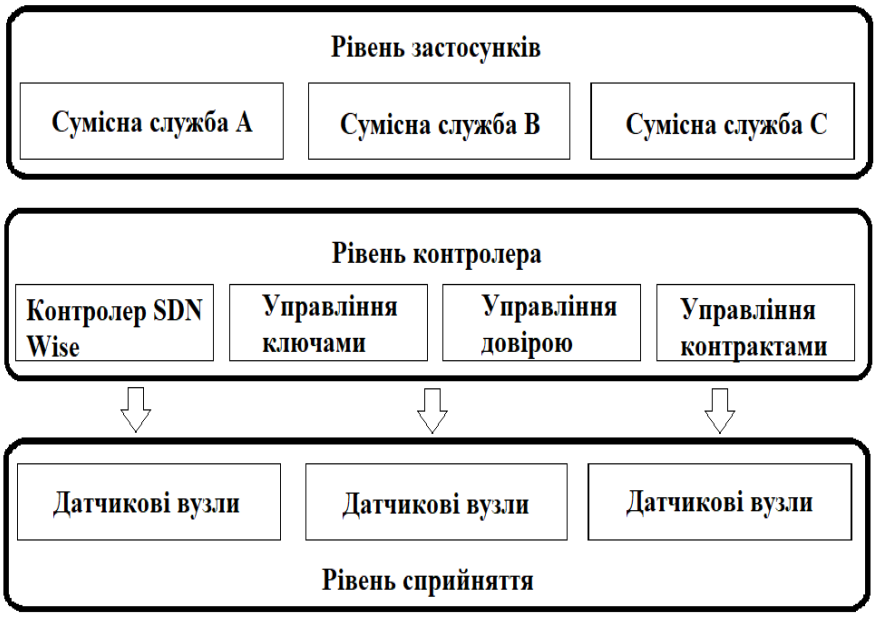

Рисунок 3.2 - Типова архітектура SDIoT, як основа методу управління безпекою..

Поверх базової SDIoT-інфраструктури метод передбачає реалізацію двох рівнів адаптивного керування безпекою - глобального та локального, кожен із яких побудований з використанням технологій багатоланцюгового блокчейну. Ключова роль цих рівнів полягає у забезпеченні виконання правил доступу, контролю автентичності та довіри на основі смарт-контрактів, розподіленої валідації та контекстно-орієнтованих політик.

Для формалізації децентралізованої взаємодії метод використовує платформу Multichain 2.0 як основу блокчейн-комунікації між компонентами.

Multichain забезпечує створення незалежних ланцюгів транзакцій, які верифікують політики безпеки в контексті розподілених мереж. Її гнучкість дозволяє розгортати ланцюги відповідно до специфіки функціоналу - наприклад, для реєстрації автентифікаційних атрибутів, обміну контекстом або збереження угод обслуговування.

Запропонований метод поєднує ці інструменти з концепцією Web3, яка передбачає усунення посередників у процесах цифрової взаємодії. Такий підхід дозволяє не лише мінімізувати ризики компрометації даних, а й сприяє створенню масштабованих рішень для забезпечення безпеки без необхідності централізованої авторизації.

Багатоланцюгова архітектура в межах методу реалізує ізольовані канали валідації, серед яких:

1) ланцюг автентифікації користувачів та вузлів, що забезпечує контроль доступу на основі перевірки відкритих ключів і цифрових підписів;

2) ланцюг перевірки безпекових політик, що виконує роль фільтра при впровадженні нових правил доступу;

3) контракт контексту, який дозволяє враховувати змінні зовнішні фактори під час ухвалення рішень щодо взаємодії між сервісами.

На рисунку 3.3 наведено узагальнену архітектуру взаємодії компонентів у межах запропонованого методу, що базується на клієнт-серверній логіці, де обидві сторони функціонують у децентралізованому середовищі. Клієнтські компоненти відповідають за генерацію запитів, а серверні - за обробку політик та їхню перевірку на відповідність визначеним нормам.

Таким чином, представлений метод є не просто інструментом контролю доступу, а комплексною концепцією, що об’єднує IoT-інфраструктуру, політики безпеки, логіку взаємодії смарт-сервісів та блокчейн-валидацію в єдиний адаптивний простір забезпечення безпеки розумного міста.

3.4 Метод організації глобальних угод і смарт-контрактів у розподіленому середовищі

У межах запропонованого методу управління безпекою особливу роль відіграє механізм реалізації глобальної сервісної угоди, яка базується на впровадженні ланцюга валідації сервісних угод. Цей ланцюг виконує функції збереження, перевірки та координації транзакцій, пов'язаних із домовленостями між смарт-сервісами. Така структура дозволяє організовувати безпечну й скоординовану взаємодію між сервісами, що співпрацюють у межах інтелектуального міста.

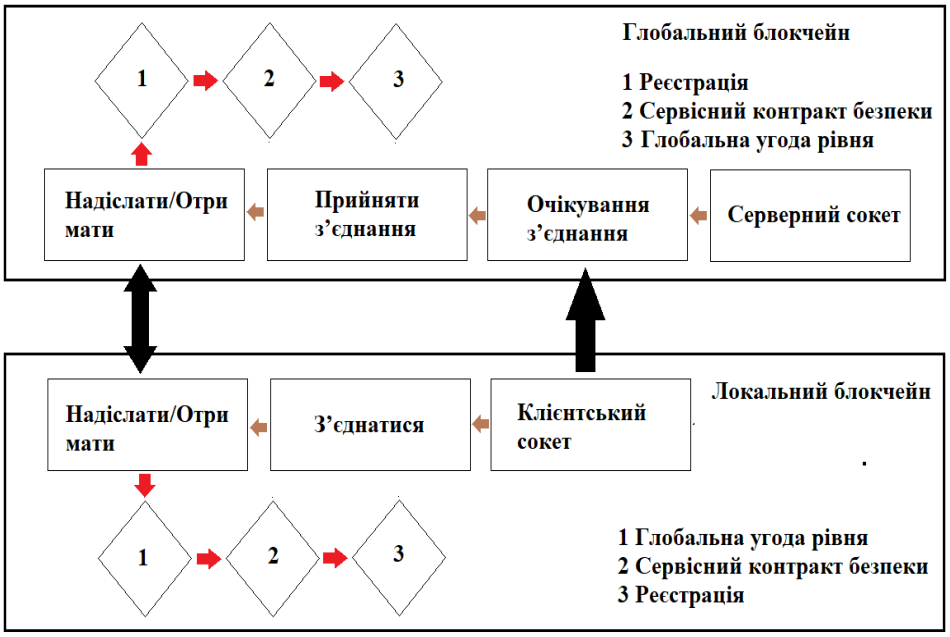

Рисунок 3.3 - Архітектура взаємодії у межах методу управління безпекою, реалізованого на основі SDN-WISE та блокчейн-середовища.

Глобальна угода рівня є формалізованим представленням домовленостей між смарт-сервісами, що досягається шляхом послідовної реєстрації транзакцій у багатоланцюговій блокчейн-мережі. Використання смарт-контрактів як інструменту автоматизованої координації забезпечує безперервність і цілісність взаємодії, оскільки всі умови, строки та обмеження фіксуються незмінно в ланцюгу

блоків. Це дозволяє гарантувати стабільність механізмів спільного реагування, оперативну синхронізацію даних та послідовність дій навіть за умов зростання навантаження на систему.

В основі реалізації методу лежить використання смарт-контрактів, які визначають правила взаємодії між суб'єктами цифрової інфраструктури. Смарт-контракт у цьому контексті - це формалізована програма, що розгортається у блокчейн-середовищі, забезпечуючи автоматичне виконання умов домовленостей без участі сторонніх контролерів. Саме така автоматизація дозволяє досягти нової якості у розробці безпечних протоколів обміну даними.

Запропонований метод передбачає реалізацію чотирьох ключових типів смарт-контрактів, які реалізуються в локальних і глобальних компонентах адаптивного рушія. Їх роль полягає не лише в описі умов доступу, але й у керуванні динамікою колаборативних завдань між службами, адаптацією до середовища та підтримці розмежування рівнів довіри.

Зокрема:

1) контракт угоди між сервісами регламентує узгодження умов взаємодії між конкретним сервісом і локальним або глобальним рушієм безпеки. Це дозволяє верифікувати відповідність дій поточному контексту, політикам і рівню критичності;

2) контракт безпеки сервісу відіграє центральну роль у формуванні вимог до захисту під час виконання спільних завдань. До нього включаються специфікації механізмів автентифікації, авторизації, довірчих перевірок та обмежень доступу до критичних даних, що дозволяє підтримувати цілісність і стабільність у взаємодії.

Таким чином, метод організації управління безпекою, запропонований у дослідженні, ґрунтується на послідовному впровадженні блокчейн-смарт-контрактів як основи для гнучкого, захищеного та автоматизованого керування міжсервісними угодами, що особливо актуально для динамічного середовища інтелектуального міста [3, 76, 91].

3.5 Реалізація політик та контекстної взаємодії між смарт-сервісами

У рамках запропонованого методу управління безпекою ключову роль відіграють контракт політик безпеки та контракт контекстного рушія, які забезпечують формалізацію та автоматизоване застосування правил взаємодії між смарт-сервісами у межах цифрової інфраструктури інтелектуального міста.

Контракт політик безпеки слугує основою для створення, підтримки та впровадження політик на локальному та глобальному рівнях. Політики, які генеруються за допомогою цього типу контракту, визначають допустимі умови взаємодії, рівні доступу, пріоритети обробки запитів та обмеження щодо обміну даними. Наприклад, окрема політика може регламентувати допустимі часові інтервали обміну повідомленнями між службами охорони здоров’я та рятувальними службами під час надзвичайної події. Завдяки смарт-контрактному механізму, зазначені умови виконуються автоматично, без потреби у ручному нагляді або централізованому контролі.

Контракт контекстного рушія реалізує логіку застосування політик у контексті взаємодії. Саме цей елемент методу визначає, які саме умови повинні бути враховані в момент взаємодії - зокрема, поточний стан сервісів, рівень довіри, тип запиту, критичність ситуації тощо. Контекстуальна логіка дозволяє системі адаптуватися до динамічних змін, роблячи рішення про доступ не лише залежними від історичних даних, але й від поточної обстановки.

Запропонований метод ґрунтується на багаторівневій взаємодії компонентів, до якої входять: програмно-кероване середовище SDIoT, локальні та глобальні адаптивні рушії безпеки, побудовані на блокчейн-технологіях. Усі ці компоненти функціонують як цілісний механізм - метод гнучкого управління безпекою смарт-взаємодій. Архітектура SDIoT забезпечує зв’язність і адаптивність між фізичними IoT-вузлами та логікою сервісної взаємодії, тоді як адаптивні рушії гарантують застосування захисних сценаріїв відповідно до ситуації.

Особливість методу полягає у використанні багатоланцюгової структури, що забезпечує одночасне застосування локальних та глобальних угод. Відповідні смарт-контракти гарантують, що дані залишаються достовірними, непідробними та доступними лише авторизованим сторонам. Інтеграція таких принципів дозволяє

досягти узгодженого впровадження політик по всій системі - від сенсора до сервісу - що, у свою чергу, знижує вірогідність несанкціонованого доступу та покращує реактивність на загрози [45], [70].

Ключовим доповненням до методу стало розширення можливостей SDN-контролера WISE, у якому реалізовано нові модулі:

1) модуль керування криптографічними ідентифікаторами;
2) модуль управління сесіями;
3) внутрішнє захищене сховище ідентичностей.

Ці модулі забезпечують генерацію цифрових пар ключів для IoT-вузлів, а також прив'язку сесій до відповідних політик безпеки. Це дозволяє системі не лише перевіряти атрибути автентичності, але й забезпечувати зв'язність між контекстом запиту та застосованими політиками.

Таким чином, метод формалізованого управління політиками та контекстною взаємодією дозволяє автоматизувати як перевірку, так і виконання правил, зменшуючи ризики людського фактору та забезпечуючи високий ступінь узгодженості між учасниками цифрової взаємодії в умовах смарт-міста.

3.6 Метод криптографічного управління ідентичностями в SDIoT

У запропонованому методі реалізації безпеки в середовищі інтелектуального міста, особлива увага приділяється механізму керування криптографічними ідентичностями, який забезпечує захищену взаємодію між смарт-сервісами, IoT-вузлами та SDN-контролерами. Метод орієнтований на використання еліптичної криптографії (ECC) з ключами змінної довжини - 128, 192 та 256 біт - що дозволяє адаптувати рівень безпеки до ресурсних можливостей учасників мережі.

В основі методу - структурований підхід до генерації та розповсюдження ключів, що починається із формування трійки ECC-ключів для кожного елемента системи:

1) ключ θ - ідентифікатор для смарт-сервісу;
2) ключ λ - криптографічний ідентифікатор клієнтського вузла;

3) ключ μ - ідентифікатор, закріплений за SDN-контролером.

Ці ключі формуються за допомогою модуля $L\theta$, який виконує функцію ϕ формування криптографічної трійки для кожного вузла. Згенеровані значення структуруються у множину:

$$L(\tau) = \{(\theta, \lambda, \mu) \mid k \in R, \exists n \in D\}, \quad (3.1)$$

де R і D - множини смарт-сервісів та клієнтських вузлів відповідно.

Алгоритм керування ключами, який реалізує запропонований метод, включає наступні кроки:

1) обрати рівень безпеки шляхом вибору довжини ключа із множини {128, 192, 256};

2) виконати генерацію пари ключів K, C за допомогою ECC;

3) зберегти ключову пару у захищеному сховищі;

4) ініціалізувати структуру метаданих сервісу у форматі JSON;

5) створити JSON-запис, який включає ідентифікатор session_ref, сформований через хешування структури метаданих.

6) повернути session_ref як унікальний ідентифікатор сесії.

На цьому етапі формується база для автентифікації, яка використовується на всіх рівнях SDIoT-інфраструктури.

Метод підтримує захищений обмін сесійними ключами за допомогою алгоритму ECDH (Elliptic Curve Diffie-Hellman), що забезпечує високий рівень стійкості до атак типу "man-in-the-middle".

На початку взаємодії:

1) IoT-вузли ініціюють запит до SDN-контролера, використовуючи його публічний ключ, та підписують повідомлення власним приватним ключем.

2) Контролер виконує розшифрування повідомлення, перевіряє автентичність, після чого генерує сесійний ключ.

Цей ключ:

1) шифрується публічним ключем IoT-вузла;

2) підписується приватним ключем SDN-контролера;

3) надсилається назад до вузла.

Після успішного прийому та дешифрування, IoT-вузли отримують сесійні ключі, які надалі використовуються для захищеного обміну даними в рамках колаборативної роботи смарт-сервісів (див. також [3], [70]).

3.7 Метод адміністрування смарт-сервісів на основі SDIoT

У межах запропонованого методу управління безпекою смарт-інфраструктури інтелектуального міста ключовою функціональною ланкою виступає метод динамічного адміністрування смарт-сервісів, який базується на архітектурі SDIoT.

Цей метод передбачає адаптивне керування наборами API сервісів, оцінюванням довіри та генерацією криптографічних ідентичностей, що забезпечує гнучке, масштабоване та безпечне середовище взаємодії між цифровими службами.

Основна мета методу - забезпечити ефективну інтеграцію неоднорідних смарт-сервісів, які функціонують у розподіленому середовищі. Для цього використовується адаптивний прикладний рівень, який обробляє API кількох сервісів через відповідну функцію керування $\boldsymbol{F}$. Ця функція автоматично прив'язує до кожного сервісу параметри криптографічної ідентифікації та довіри:

$$F(IntelligentServicea..z) = \{ServiceAPIs, Trust = 0\}, \quad (3.2)$$

Таким чином, кожен смарт-сервіс під час реєстрації отримує нульовий рівень довіри, який оновлюється в процесі подальшої взаємодії відповідно до поведінки сервісу.

Алгоритм обробки API-сервісів

Метод містить алгоритмічну процедуру формування сервісного реєстру, яка виконує наступні дії:

1) ініціалізація порожнього списку сервісів;

2) поетапне додавання кожного API;

3) генерація ключів сервісу через вбудовану криптографічну функцію generate_keys();

4) призначення базового рівня довіри (0);

5) формування структури сервісу й включення до загального реєстру.

Адаптивні рушії, формалізація взаємодії в даному методі передбачає використання адаптивних рушіїв безпеки - rule engine та execution engine, які вбудовано у блокчейн-інфраструктуру. Вони забезпечують динамічне формування політик і виконання безпекових операцій шляхом виклику смарт-контрактів. Взаємодія між цими рушіями здійснюється через валідаційний ланцюг, що гарантує узгодженість рішень у глобальному та локальному контекстах.

У межах rule engine реалізовано функцію Y, яка трансформує безпекові параметри сервісів у формалізовані контракти. Ці контракти є представленням правил для локального (LocalServiceContract) та глобального (GlobalServiceContract) рівнів:

$$Y(IntelligentServicea..z) = (LocalServiceContract, GlobalServiceContract), \quad (3.3)$$

де контракти визначаються як множини 5-кортежів:

1) θ - пара ключів ECC для смарт-сервісу;

2) λ - пара ключів для клієнтських вузлів;

3) μ - ключова пара SDN-контролера;

4) APIs - інтерфейси, якими оперує сервіс;

5) Trust - накопичене значення довіри.

Інтеграція з криптографічною моделлю є ключовим елементом методу є механізм генерації цифрових ідентичностей, які створюються в межах обох ланцюгів (локального та глобального) на базі ECC.

Це дозволяє кожному сервісу отримати унікальні атрибути, необхідні для захищеного обміну даними. Кожна операція з API сервісу супроводжується

верифікацією довіри, що знижує ризики компрометації на етапі виконання колаборативних завдань.

Таким чином, метод адміністрування смарт-сервісів у середовищі SDIoT реалізує поетапну ідентифікацію, оцінювання довіри, захист API та автоматизацію правил взаємодії. Він є фундаментом для забезпечення безперервної, динамічно контрольованої і безпечної взаємодії між службами розумного міста в умовах зростаючого навантаження та високої варіативності сценаріїв застосування.

Важливою складовою методу управління безпекою смарт-сервісів є механізм трансляції політик безпеки, який забезпечує формалізацію умов доступу, автентифікації та авторизації у вигляді придатних до виконання смарт-контрактів.

Цей процес є критичним етапом у реалізації захищеної взаємодії між сервісами в інфраструктурі інтелектуального міста, оскільки він визначає, як саме логіка безпеки інтегрується у поведінку системи.

На вхід модулю трансляції подаються параметри автентифікації, набір авторизаційних правил і профілі доступу до сервісів. У процесі обробки цих вхідних даних формуються три основні логічні блоки, що лягають в основу структури політики: блок автентифікації (authBlock), блок авторизації (authzBlock) та блок доступу (accessBlock). В authBlock заносяться ключі SDN-контролера, а також ініціалізується ключова пара для локального ланцюга; додатково зчитуються глобальні відкриті ключі, що дозволяє досягти наскрізної криптографічної сумісності.

У блоці authzBlock визначається рівень довіри до сервісу (TrustScore), який буде використовуватися при прийнятті рішень щодо дозволу чи заборони доступу, та виконується прив’язка політик до конкретного сервісу або API. У свою чергу, блок accessBlock структурує перелік сервісів, із якими може бути здійснена взаємодія, та описує набір дозволених дій, які можуть бути виконані в межах конкретного колаборативного завдання.

Усі три блоки інкапсулюються в єдиний політичний об’єкт (GeneratedPolicy), який передається до глобального блокчейну через MultiChainAPI. Цей політичний об’єкт реалізовано у форматі JSON, що забезпечує гнучкість і масштабованість у

процесі впровадження нових параметрів безпеки. Політика безпеки у представленому методі описується як структура PolicyObject, яка включає параметри SecureMeta (ідентифікатори, підписи, мітки ключів), authBlock (ключові дані для автентифікації), CredScore (рейтингову оцінку довіри) та TaskMap (опис взаємодії в межах спільного процесу).

Після формування політики рушій правил ініціює передачу сформованого контракту до рушія виконання. У межах даного методу реалізовано два типи смарт-контрактів: глобальний контракт безпеки (Global Security Contract), який активується в локальному рушії, та сервісний контракт безпеки (Service Security Contract), який виконується глобальним рушієм. Обидва контракти створюються на основі структурованих конфігурацій безпеки, зокрема файлу ServiceSecurity.json, і використовуються для ініціалізації логіки перевірки атрибутів автентичності, прав доступу та рівнів довіри.

Контекстний рушій забезпечує гнучку обробку отриманих політик, адаптуючи їх до поточного контексту сервісної взаємодії. Він приймає політики з обох рівнів - локального та глобального - і на їх основі ухвалює рішення про надання доступу. Відповідно до запропонованого методу, весь процес - від трансляції політик до їх реалізації у вигляді смарт-контрактів - формує ядро механізму адаптивного управління безпекою, що відображає сучасні вимоги до захисту у високодинамічному середовищі інтелектуального міста.

У межах запропонованої архітектури управління безпекою ключову роль відіграє локальний адаптивний рушій, який здійснює оцінювання автентичності, обробку авторизаційних правил та прийняття рішень про надання доступу на основі поточного рівня довіри. На вхід рушія надходять результати автентифікаційної перевірки, набір авторизаційних умов та визначені політики доступу, після чого запускається процес обчислення рейтингу довіри - credScore. Початкове значення цього рейтингу дорівнює нулю і поступово змінюється в залежності від результатів перевірки. Якщо автентичність підтверджена, обчислюється нове значення рейтингу довіри за формулою оновлення: з урахуванням коефіцієнта впливу α і коригувального параметра delta, що дорівнює

1 − α. Після оновлення значення записується у блокчейн, а якщо воно перевищує наперед визначене порогове значення, система дозволяє виконання відповідної дії - наприклад, запуску спільного завдання.

Паралельно з цим, у межах інфраструктури передбачено механізм агрегації політик безпеки, що здійснюється за допомогою функції Ψ, яка об'єднує локальні й глобальні контракти безпеки у єдину узгоджену політику. Для цього використовуються відповідні контракти, витягнуті з блокчейн-реєстрів обох рівнів. Зокрема, локальний контракт (Q) містить специфічні умови взаємодії в межах SDIoT, тоді як глобальний (R) регламентує міжсервісну координацію. Результат об’єднання формується у вигляді структури політики, яка передається рушію виконання для подальшого застосування в контексті безпечної взаємодії.

Передача політики безпеки відбувається шляхом звернення до сховища смарт-контрактів у блокчейні, звідки витягується остання версія політичного контракту. Отримані дані перетворюються у формат JSON і збагачуються додатковими фрагментами, отриманими через API платформи MultiChain. Об'єднана політика у JSON-форматі передається до модуля виконання, який ініціює відповідні механізми реалізації безпекових сценаріїв.

Механізм динамічного оновлення довіри ґрунтується на безперервному перерахунку значення довіри між сервісами. Припускаючи наявність двох сервісів u та v, кожне нове оновлення оцінки довіри здійснюється із врахуванням часової дельти Δζ, що пройшла з моменту останньої взаємодії. Поточна оцінка позначається як $\psi_{u,v}(\zeta)$ і належить до інтервалу від 0 до 1. Значення агрегованої довіри $V_{u,v}(\zeta)$ визначається як вагоме середнє між останньою оцінкою й попереднім значенням, що зберігається в системі. Коефіцієнт ω вказує на рівень значущості останньої взаємодії: чим більшим є його значення, тим більше ваги матиме поточна поведінка сервісу. Таким чином, якщо $V_{u,v}(\zeta)$ прямує до 1 - система розглядає взаємодію як високодостовірну; якщо до 0 - як ризиковану або недостовірну.

Інфраструктура смарт-міста вимагає, щоб взаємодія між сервісами відбувалась лише за умови укладеної угоди щодо рівня обслуговування, яка також фіксується у вигляді смарт-контракту. У рамках запропонованого методу така

угода слугує основою для фіксації нових вимог до безпеки, які можуть бути динамічно додані до системи. Саме смарт-контракт, що репрезентує угоду між сервісами, забезпечує підтримку адаптивного рівня безпеки у процесі масштабованої взаємодії. У такий спосіб реалізується безперервне вдосконалення системи безпеки на основі аналізу поточних ризиків, історії взаємодій та параметрів довіри.

Для отримання доступу до спільних завдань усі сервіси, що беруть участь у взаємодії, повинні підтвердити свою згоду з умовами відповідної угоди. Цей процес реалізується шляхом багатоступеневої криптографічної процедури, яка гарантує безпеку та цілісність переданих даних у межах смарт-інфраструктури міста. Візуальне представлення етапів реалізації цього механізму наведено на рисунку 3.4..

Крок №1. На першому етапі агент прикладного рівня формує запит до SDN-контролера. Запит супроводжується тегом безпеки (session-id) і підлягає шифруванню за допомогою криптографічних механізмів на основі еліптичних кривих (ECC). Для забезпечення конфіденційності та автентичності, запит шифрується публічним ключем локального блокчейну, а підписується - приватним ключем відповідного IoT-вузла. Перед відправкою передбачається, що між агентом та локальним блокчейн-середовищем уже було здійснено обмін хешами публічних ключів, що дозволяє верифікувати джерело запиту.

Крок №2. Другий крок передбачає обробку отриманого повідомлення локальним адаптивним рушієм. За допомогою свого приватного ключа в поєднанні з публічним ключем вузла-ініціатора, рушій розшифровує вхідне повідомлення. Це дозволяє витягти інформацію про сам запит і сесійний ключ, необхідний для подальшого встановлення безпечного каналу зв’язку.

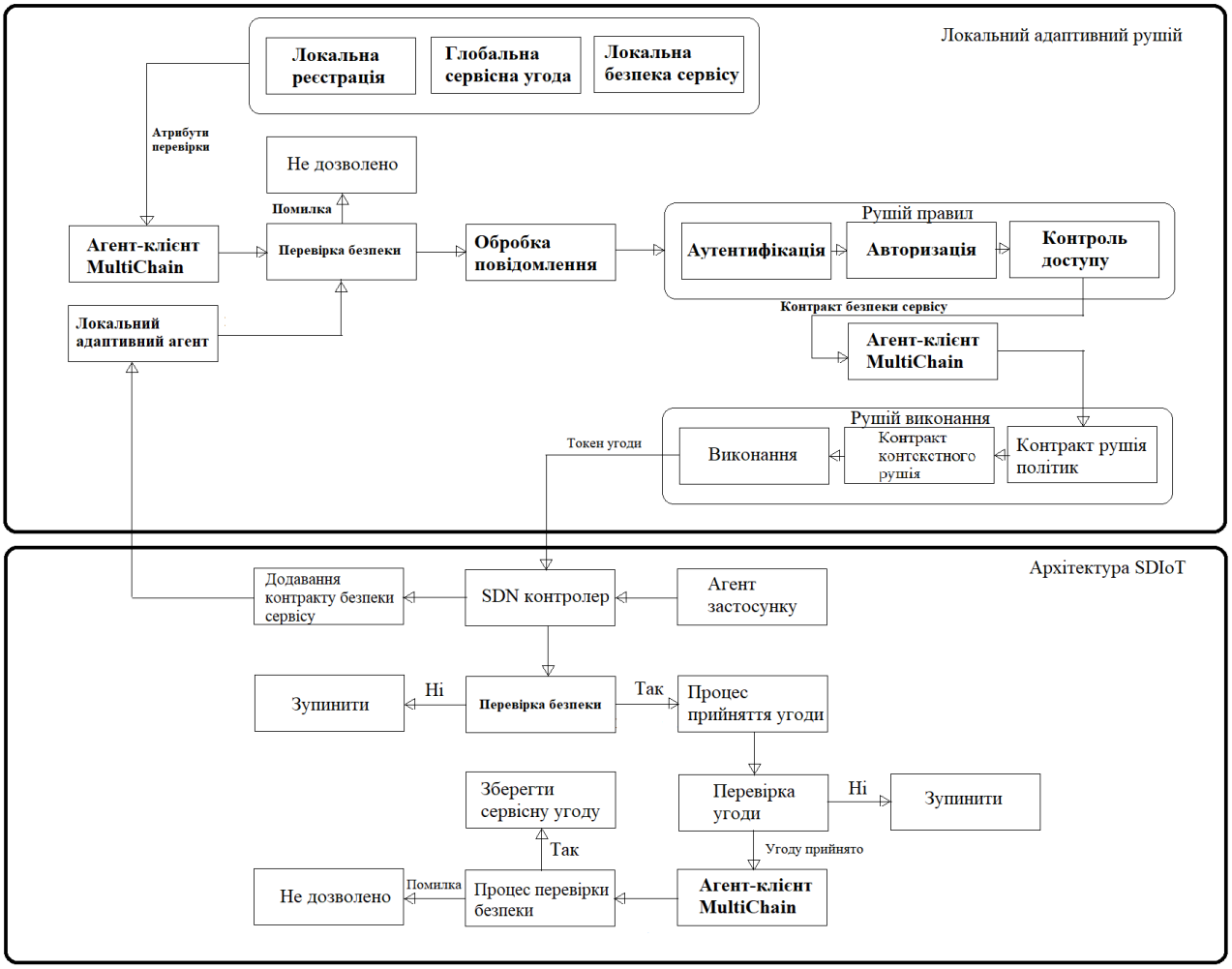

Рисунок 3.4 - Робочий процес додавання безпеки локальної служби

Розшифроване повідомлення має формат:

$$M = [\Psi \parallel Hash(\kappa)], \tag{3.4}$$

де

1) M - декодоване повідомлення;

2) Ψ - власне запит (Request), к - сеансовий ключ (SessionKey), а Hash(·) - хеш-функція, яка забезпечує перевірку цілісності ключа.

Продовження криптографічного протоколу взаємодії смарт-сервісів ілюструє подальші етапи обробки повідомлення після успішного його розшифрування локальним адаптивним рушієм.

Крок №3. Після дешифрування повідомлення модуль валідації здійснює витяг очікуваного сесійного ключа з локального блокчейн-реєстру. Далі виконується обчислення хеш-функції від цього ключа та її порівняння з хешем, переданим у повідомленні. У разі збігу система підтверджує цілісність і справжність отриманих даних, відкриваючи можливість подальшої обробки запиту.

Крок №4. Після перевірки автентичності запиту активується механізм розширення локальних вимог безпеки. Відповідні дані щодо ідентифікації, авторизації та прав доступу консолідуються в об’єкт смарт-контракту, який фіксується у вигляді транзакції в локальному ланцюгу MultiChain. Після цього транзакція передається глобальному адаптивному рушію для накладення адміністративних параметрів безпеки.

Крок №5. Глобальний рушій політик приймає сформований смарт-контракт та відповідний ідентифікатор транзакції. Ідентифікатор виступає як токен угоди - Service Agreement Token. Цей токен передається контекстному модулю, який забезпечує захищений обмін повідомленнями. У контекстному рушії вміст повідомлення шифрується із використанням публічного ключа SDN-контролера, а хеш від Session ID додається як додатковий маркер автентичності.

Формат зашифрованого контрактного повідомлення подається у вигляді:

$$C = [(\Gamma \parallel Hash(\kappa))\hat{}\xi]\hat{}\rho, \tag{3.5}$$

де:

1) C - зашифроване контрактне повідомлення (ContractEnc);
2) Γ - контракт безпеки (Contract);
3) κ - сеансовий ключ (SessionKey);
4) ξ - секретний ключ відправника (sk);
5) ρ - відкритий ключ отримувача (pk);
6) Hash(·) - геш-функція, що підтверджує достовірність ключа.

Крок №6. Сторона застосунку, отримавши повідомлення, розшифровує його за допомогою власної пари криптографічних ключів, отримуючи доступ до вмісту контрактної угоди.

Крок №7. Витягнутий контракт передається до внутрішнього модуля прийняття рішень, який виконує підтвердження укладення угоди між сервісами.

Крок №8. На етапі затвердження ініціюється повторна перевірка токена угоди (Service Agreement Token). Цей процес забезпечується функціоналом блокчейн-системи MultiChain, що гарантує достовірність і цілісність токена.

Крок №9. Після завершення перевірки токен угоди зберігається у локальному захищеному сховищі. У подальшому цей токен використовується для підтвердження авторизації доступу до сервісів, а також для обліку взаємодій у межах інфраструктури смарт-міста.

Загалом описаний механізм формує основу для безпечного, узгодженого та підтвердженого виконання спільних задач у середовищі інтелектуального міста з високими вимогами до довіри та безпеки.

3.8 Глобальні вимоги безпеки для смарт-сервісів

У системі розумного міста з високим ступенем децентралізації та динамічної взаємодії між численними смарт-сервісами, забезпечення єдиних глобальних вимог безпеки є критично важливим завданням. Запропонований метод управління безпекою передбачає узгодження індивідуальних (локальних) політик кожного сервісу з централізованими адміністративними політиками, що формуються відповідно до загальноміських нормативів і стандартів взаємодії.

Глобальні вимоги безпеки формуються на основі аналізу сценаріїв колаборативної взаємодії, де необхідна координація дій між різними службами - наприклад, між медичною службою, транспортною мережею та аналітичними платформами. У таких умовах стандартні політики одного окремого сервісу виявляються недостатніми для забезпечення цілісної безпеки в рамках усього міського середовища.

Метод, запропонований у цій роботі, реалізує багаторівневу перевірку відповідності політик, в якій глобальний адаптивний рушій виконує інтегруючу роль. Цей рушій створює адміністративні смарт-контракти безпеки, які доповнюють локальні політики і формують єдиний набір вимог для всіх учасників взаємодії. Контракти генеруються з урахуванням поточних параметрів сеансу, типу сервісу, рівня довіри та пріоритетності запиту.

Технічна реалізація даного підходу базується на механізмі агентної взаємодії між клієнтським модулем multi-chain та глобальним агентом, який забезпечує доставку повідомлень і запуск глобальних процедур перевірки. Усі події реєструються в розподіленій системі зберігання на основі блокчейну, що гарантує прозорість і недоступність до зміни історії транзакцій.

Процес формування глобального контракту безпеки починається з того, що локальний рушій передає підтверджений контракт до глобального модуля. Далі глобальний агент перевіряє сумісність з поточними адміністративними політиками та накладає відповідні обмеження або дозвіл на взаємодію. Це дозволяє гарантувати, що навіть у складних сценаріях багатоетапної співпраці між сервісами дотримуються стандарти безпеки.

Схематичне представлення цього процесу ілюструє рисунок 3.5 - Робочий процес глобального контракту безпеки служби, де відображено логіку обміну між агентами, механізм перевірки контрактів, обробку через multi-chain API та затвердження глобального рівня політики.

Завдяки такому підходу метод управління безпекою забезпечує:

1) зниження ризику несанкціонованого доступу;
2) дотримання контекстних та адміністративних правил;
3) забезпечення єдиного інформаційного простору між сервісами;
4) підвищення надійності взаємодії у середовищі smart city.

Інтеграція локальних смарт-контрактів безпеки у глобальне блокчейн-середовище забезпечується через послідовність криптографічних і логічних дій, які реалізують об’єднання політик безпеки на всіх рівнях архітектури.

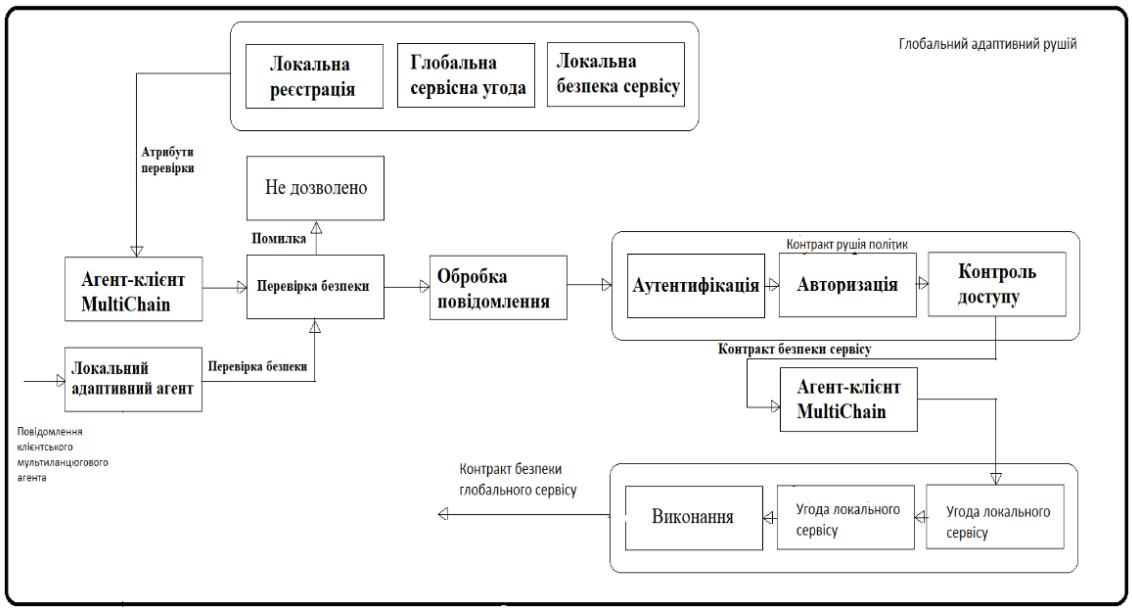

Рисунок 3.5 - Робочий процес глобального контракту безпеки служби

Крок №1. Ініціалізація транзакцій безпеки відтворює компонент локального адаптивного рушія формує локальний смарт-контракт безпеки, який реєструється одночасно у двох реєстрах: локальному та глобальному. Повідомлення перед передачею шифрується публічним ключем глобального реєстру, підписується приватним ключем IoT-вузла, та до нього додається хеш від сесійного параметра.

Формула шифрування повідомлення:

$$M = \tau \parallel Hash(\varsigma), \tag{3.6}$$

де:

1) M - зашифроване повідомлення, яке надсилається до глобального адаптивного рушія;

2) τ- унікальний ідентифікатор транзакції (відповідає певному локальному контракту безпеки);

3) ς- session ID, тобто унікальний ідентифікатор поточної взаємодії (сеансу);

4) Hash(ς) - хеш-функція від session ID, що використовується для перевірки цілісності запиту;

5) ‖ - оператор конкатенації, що поєднує ідентифікатор транзакції з хешем.

Крок №2: Дешифрування на глобальному рівні розшифровує повідомлення, використовуючи свій приватний ключ та публічний ключ IoT-вузла, що ініціював транзакцію.

Формула розшифрування:

$$M = \tau \parallel Hash(\varsigma), \tag{3.7}$$

де:

1) M - повідомлення, отримане після розшифрування глобальним адаптивним рушієм;

2) Параметри аналогічні попередній формулі.

Крок 3: Перевірка сесійної ідентичності відбувається після розшифрування повідомлення, здійснюється порівняння хешу сесійного ключа з відповідним записом у глобальному блокчейн-реєстрі. Успішна перевірка гарантує достовірність даних.

Крок 4: Формування глобального контракту безпеки витягує локальний контракт за ідентифікатором τid та доповнює його адміністративними політиками, після чого створюється єдиний контракт.

Формула глобального контракту:

$$C = K \parallel A, \tag{3.8}$$

1) C - глобальний контракт безпеки, який включає всі вимоги взаємодії;

2) K - локальний контракт безпеки, сформований на рівні смарт-сервісу;

3) A - адміністративна політика безпеки, задана на рівні інфраструктури міста;

4) ‖ - об’єднання в єдину структуру.

Крок 5: Завершення протоколу та передача результату

Контекстний рушій створює нову транзакцію, яка фіксує об’єднаний контракт у локальному та глобальному блокчейнах. Потім надсилається повідомлення назад до локального адаптивного рушія, шифроване публічним ключем локального реєстру та підписане приватним ключем IoT-вузла.

Контекстний рушій активується після верифікації, та відповідає за виконання контракту контекстного виконання. У межах цього контракту реалізовано два підконтракти:

1) Service Agreement Contract - обробляє запити щодо формування угод між сервісами;

2) Message Execution Contract - виконує обробку запитів після укладання угоди та ініціює спільні дії.

Такий поетапний механізм дозволяє підтримувати гнучке, перевірене та криптографічно захищене середовище для взаємодії смарт-сервісів, забезпечуючи цілісність, достовірність і контроль виконання угод у межах інтелектуального міста.

У межах реалізації методу управління безпекою смарт-сервісів контекстний рушій виконує одну з ключових функцій - забезпечення перевірки автентичності запитів, оцінювання довіри до ініціаторів взаємодії та прийняття рішень щодо доступу до виконання спільних завдань у міському цифровому середовищі [27].

Крок 1: Початковий контроль автентичності.

Після проходження базових процедур перевірки безпеки на рівні локального блокчейну, запит передається до контекстного рушія. Першим етапом цього процесу є верифікація джерела запиту, яка охоплює перевірку цифрового підпису, структури повідомлення та його відповідності до стандартів безпеки. Це гарантує, що повідомлення дійсно сформоване авторизованим смарт-сервісом (див. рис. 3.5).

Крок 2: Динамічне оцінювання довіри.

У разі підтвердження автентичності активується механізм динамічної оцінки довіри. Поточне значення довіри формується на основі попередніх транзакцій, контексту запиту та поведінкової історії взаємодії [91]. Це значення оновлюється за допомогою вагової формули, що враховує поточну оцінку та попередню довіру:

$$V(\zeta) = \omega \cdot \psi(\zeta) + (1 - \omega) \cdot V(\zeta - \Delta\zeta), \quad (3.9)$$

де

1) $\omega \in [0,1]$ - коефіцієнт впливу останньої оцінки;
2) $\psi(\zeta)$ - поточна довіра;
3) $\Delta\zeta$ - часовий зсув.

Крок №3: Генерація відповіді системи.

Якщо накопичене значення довіри перевищує встановлений поріг, контекстний рушій формує відповідь системи. У залежності від результату вона може містити або підтвердження угоди у вигляді токена (Agreement Token Payload), або результат - дозволити чи заборонити доступ до ресурсів чи дій. Такий підхід забезпечує гнучке управління доступом, адаптоване до поведінки конкретного сервісу [3], [90].

Представлений механізм дозволяє реалізувати контекстно-орієнтовану перевірку політик безпеки, яка включає етапи автентифікації, оцінки довіри, валідації угод та захищеної генерації відповіді. Це значно підвищує стійкість до атак на рівні міжсервісної взаємодії та гарантує достовірність виконання спільних завдань у смарт-інфраструктурі [27].

Увесь описаний процес ілюструється на рисунку 3.6 - «Робочий процес контекстного механізму».

На рисунку представлено узагальнену схему функціонування контекстного механізму у процесі перевірки та обробки запиту на доступ до глобального сервісу безпеки. Процес розпочинається з аналізу вхідного повідомлення, що надходить як запит на укладення угоди або перевірку глобального рівня безпеки сервісу.

Далі здійснюється класифікація запиту та визначення його типу: запит на участь у кооперативному завданні чи ініціація перевірки автентичності. У відповідь на це формуються відповідні смарт-контракти: глобальний сервісний контракт або контракт безпеки. Після цього запит направляється до локального або глобального контекстного рушія (в залежності від рівня взаємодії), де відбувається серія перевірок.

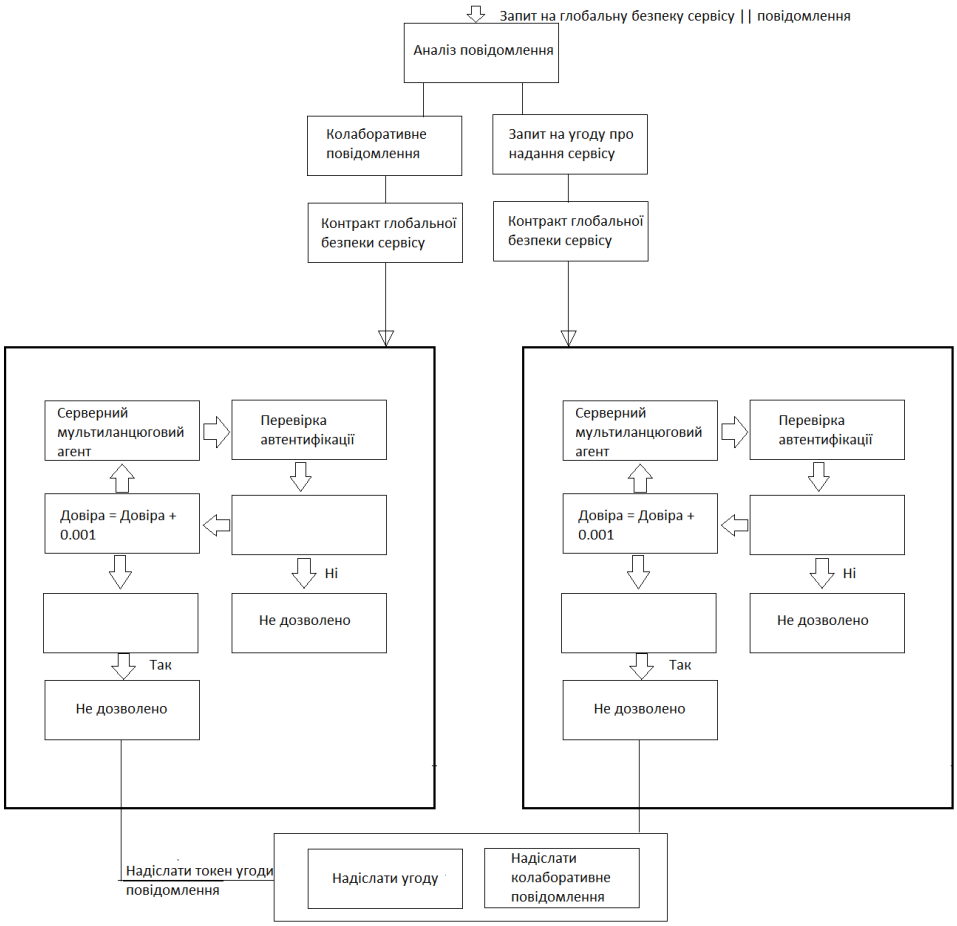

Рисунок 3.6 - Робочий процес контекстного механізму

3.9 Висновки

У межах цього розділу було розроблено комплексну архітектуру системи управління безпекою смарт-сервісів для умов розумного міста, яка поєднує в собі динамічність, масштабованість і децентралізований метод до забезпечення захисту даних та взаємодії між сервісами. Основними технологічними засадами архітектури стали програмно-визначений Інтернет речей (SDIoT), багатоланцюгова блокчейн-інфраструктура та механізми смарт-контрактів.

Розроблена система враховує специфіку виконання колаборативних завдань у середовищі з високим рівнем динаміки та взаємозалежності, де критично важливим є забезпечення довіри, контроль автентичності та захист каналу обміну. Архітектура включає локальні та глобальні адаптивні рушії, які взаємодіють між собою через мультиблокчейн-клієнт, забезпечуючи погодження політик безпеки та

підтримку різнорівневого контролю доступу. Було також запропоновано формальну модель управління криптографічними ідентифікаторами та генерації сесійних ключів, що забезпечує стійкість до атак і гарантує конфіденційність взаємодії.

У розділі детально описано процеси формування, передачі та верифікації політик безпеки, включно з реалізацією смарт-контрактів безпеки для управління сервісними угодами, контекстними запитами та динамічними політиками доступу. Контекстний рушій відіграє ключову роль у перевірці автентичності, обчисленні довіри, виконанні колаборативних дій, а також в управлінні реакцією системи на запити, що надходять від сервісів.

Окремо було приділено увагу реалізації механізмів динамічного оновлення довіри між сервісами, формуванню глобального контракту безпеки з урахуванням адміністративних політик смарт-міста, а також описано повний цикл криптографічного захисту повідомлень - від ініціації транзакцій до архівації токенів угод.

Запропонований метод враховує можливість гнучкої інтеграції нових смарт-сервісів через динамічне оновлення політик безпеки, з урахуванням поточних контекстуальних умов, оцінки довіри та результатів попередньої взаємодії. Така адаптивність дозволяє забезпечити безпеку навіть у розподілених та гетерогенних середовищах, характерних для міської інфраструктури.

Крім технічної реалізації, архітектура орієнтована на практичну масштабованість та подальше розширення функціоналу. Застосування багатоцільових смарт-контрактів та політик дозволяє централізовано або децентралізовано керувати сервісами з мінімальною участю користувача, що значно підвищує ефективність управління безпекою в умовах реального часу.

Загалом, запропонована архітектура становить фундаментальну основу для впровадження інтелектуальних систем захисту в розумних містах, відповідає сучасним вимогам до кібербезпеки, та має значний потенціал для подальшого науково-практичного дослідження та розвитку в сфері розподілених систем, сервісно-орієнтованих платформ та IoT-інфраструктур.

4 СИСТЕМА УПРАВЛІННЯ БЕЗПЕКОЮ НА ОСНОВІ СМАРТ-КОНТРАКТІВ ДЛЯ ВЗАЄМОДІЇ СЛУЖБ “РОЗУМНОГО МІСТА”

4.1 Побудова механізму взаємодії служб реагування в умовах смарт-міста

Останніми роками в умовах інтенсивної урбанізації та зростання кількості надзвичайних подій спостерігається суттєве зростання запиту на системи оперативного реагування у середовищі розумних міст. Разом із поступальним розвитком смарт-технологій критичним чинником стає ефективне поєднання сервісів та їхня взаємодія, особливо в кризових ситуаціях. Від злагодженості роботи між сервісами залежить здатність системи оперативно відповідати як на реальні, так і на потенційні загрози.

Оперативність реалізації заходів у випадку надзвичайних подій є базовим чинником для збереження життя громадян і зменшення шкоди, завданої міській інфраструктурі. Швидкість реагування має вирішальне значення у контексті збору, аналізу та інтерпретації актуальної інформації, оцінки рівня небезпеки, а також координації дій між задіяними сервісами та організаціями. Забезпечення оперативного реагування сприяє підвищенню адаптивності смарт-міста до надзвичайних викликів і, як наслідок, допомагає запобігти втратам серед населення та зберегти майно.

З метою перевірки життєздатності запропонованої архітектури безпеки було змодельовано сценарій взаємодії між сервісами швидкого реагування у рамках інфраструктури розумного міста. Як представлено на рисунку 10, у системі беруть участь три ключові сервіси, які діють у тісній координації з метою реалізації механізмів реагування на надзвичайні події. У подальшому розділі надається детальна характеристика цих сервісів та їхнього функціонального призначення в загальній системі реагування.

У межах цього дослідження було створено систему для управління кризовими ситуаціями, реалізовану на основі клієнт-серверної архітектури із застосуванням сокет-програмування мовою Python. Ця система виконує роль центрального серверного вузла, який підтримує взаємодію з іншими

функціональними модулями в екосистемі розумного міста. Для забезпечення злагодженої координації між сервісами було впроваджено дві основні дії: отримання та відправлення повідомлень.

Функція отримання відповідає за збір критично важливих даних у контексті надзвичайних ситуацій. Система отримує актуальні метеодані від сервісу погоди, що дозволяє відстежувати кліматичну обстановку в режимі реального часу. Крім того, надходить інформація про GPS-координати користувачів служби швидкої допомоги, що забезпечує оперативну ідентифікацію місця розташування осіб, які можуть потребувати допомоги.

У свою чергу, функція відправлення ініціює надсилання попереджувальних сигналів до служби швидкої допомоги, орієнтуючись на погодні умови, отримані раніше. Це дозволяє екстреним службам вживати превентивних заходів. Також передається поточне розташування серверного вузла до метеосервісу, що підтримує синхронізацію й координацію між усіма задіяними компонентами.

Поєднання цих функціональних можливостей дозволяє побудувати ефективну модель обміну інформацією між смарт-сервісами та забезпечити узгоджене прийняття рішень у критичних ситуаціях. Використання такої архітектури є актуальним для побудови гнучких і надійних систем реагування в умовах розумного міста.

Окрім самої інтеграції з метео-API, у межах функціонування сервісу були реалізовані дві ключові дії - отримання та відправлення. Функція отримання забезпечує доступ до актуальної інформації про погоду з OpenWeather API, а також приймає координати користувачів служби швидкої допомоги у режимі реального часу. Це дозволяє системі відстежувати їхнє переміщення та швидко реагувати на можливі загрози.

Водночас функція відправлення відповідає за поширення сповіщень про потенційні загрози, пов’язані з погодними умовами (дощ, зливи, повінь), до служб екстреного реагування.

До сервісу інтелектуальної швидкої допомоги входить модуль системи який виконує критичну функцію - швидке реагування на надзвичайні події та

налагодження ефективної взаємодії між сервісами. Завдяки постійному обміну інформацією з іншими ключовими компонентами - зокрема службою реагування на надзвичайні ситуації та погодним сервісом - розумна швидка допомога забезпечує вчасне реагування на критичні події, підвищуючи безпеку населення міста.

Сервіс реалізовано на основі клієнт-серверної моделі із застосуванням сокет-програмування мовою Python. Як клієнтський вузол, він підтримує зв'язок із іншими сервісами для узгодженого виконання задач, що дозволяє організувати комплексну відповідь на надзвичайні події у межах інфраструктури розумного міста.

Для реалізації механізму взаємодії в рамках смарт-інфраструктури було запроваджено дві ключові функції: відправлення та отримання.

Функція отримання виконує критичну роль, оскільки забезпечує прийом повідомлень про тривожні події, що надходять від служб управління надзвичайними ситуаціями та погодного сервісу. Такі сповіщення містять оперативну інформацію про можливі загрози або несприятливі погодні явища, які можуть вимагати негайного медичного реагування. Швидке опрацювання вхідних повідомлень дає змогу сервісу швидкої допомоги оперативно реагувати на надзвичайні події.

У свою чергу, функція відправлення відповідає за передачу сигнальних повідомлень до інших взаємодіючих сервісів. Ці повідомлення містять дані про поточний стан та доступність сервісу, слугуючи індикаторами активності для інших елементів системи. Такий механізм дозволяє досягти безперервної комунікації та узгодженості між модулями під час реагування.

У таблиці В.1 Додотку В представлено приклади політик безпеки, що реалізовані кожним із сервісів, залучених до структури екстреного реагування в смарт-місті. У наступному розділі буде докладно проаналізовано модель тестового середовища, розроблену для перевірки ефективності архітектури безпеки. Основна увага приділяється параметрам оцінювання та метрикам продуктивності, що використовуються для аналізу поведінки системи за різних сценаріїв надзвичайних

ситуацій, а комунікаційну модель суміжних служб розумного реагування на надзвичані ситуації можна ереглянути на рисунку 4.1.

Модель мережі розумного міста реалізовано з використанням мережевого симулятора COOJA, що є відкритим інструментом, розробленим на основі операційної системи Contiki. У рамках нашої конфігурації система Contiki інтегрується з SDN-Wise контролером, що забезпечує впровадження архітектури SDIoT.

Рисунок 4.1 - Комунікаційний процес сумісних служб для розумного реагування на надзвичайні ситуації

SDN-Wise виступає як проміжне програмне забезпечення (middleware), яке надає інтерфейс високого рівня для розробки IoT-додатків і сервісів, усуваючи потребу у взаємодії з низькорівневою інфраструктурою мережі.

У такій конфігурації пристрої Інтернету речей (IoT) виступають у ролі клієнтських вузлів, що взаємодіють з різними смарт-сервісами. Для забезпечення обміну даними між ними використовуються контролери SDN-Wise. Кожен вузол клієнта має модуль керування ключами, який забезпечує зберігання безпечних ідентифікаційних даних у вигляді публічних і приватних ключів. Крім того, модулі керування смарт-сервісами, розміщені в контролері SDN, гарантують безперешкодний доступ клієнтських вузлів до функціоналу взаємодіючих сервісів.

У межах розробленого програмного середовища була реалізована децентралізована клієнт-серверна модель взаємодії, де сервіс управління надзвичайними ситуаціями виступає як центральний сервер, тоді як інші сервіси виконують функції клієнтів. Для забезпечення безпеки та надійності транзакцій кожен із сервісів інтегрується з блокчейн-платформою MultiChain, що забезпечує розподілене та захищене зберігання усіх транзакцій. Такий підхід дозволяє гарантувати незмінність записів і прозорість усередині всієї мережі, що позитивно впливає на рівень довіри до системи та її загальну стійкість.

У системі реалізовано основний алгоритм консенсусу, що застосовується в MultiChain - Practical Byzantine Fault Tolerance (PBFT). Цей механізм забезпечує досягнення згоди між усіма вузлами мережі щодо достовірності транзакцій та порядку їх включення до ланцюга блоків. PBFT характеризується високою продуктивністю та надійністю, особливо у контексті дозволених блокчейн-мереж (permissioned networks), до яких належить і MultiChain.

Кожен сервіс, що функціонує у даному середовищі, додатково використовує підсистеми управління логікою - а саме рушій правил, рушій політик та контекстний рушій. Взаємодіючи між собою, ці модулі підтримують координоване функціонування інфраструктури смарт-сервісів. У поєднанні зі смарт-контрактами, вищезазначені компоненти дозволяють досягти автоматизованої, надійної та

скоординованої взаємодії між сервісами, забезпечуючи при цьому збереження конфіденційності та цілісності даних.

Для оцінювання ефективності розробленої архітектури безпеки, проводиться аналіз загальної продуктивності системи, а також швидкості виконання смарт-контрактів, які реалізовані в адаптивних модулях на основі блокчейн-технологій. Ефективність системи значною мірою залежить від пропускної здатності пулу пам’яті multi-chain, а також від ресурсів оперативної пам’яті SDN-контролера, що відіграє ключову роль у маршрутизації потоків даних між сервісами під час обробки запитів та відповідей.

Пул пам’яті MultiChain виконує функцію буфера для транзакцій, які ще не були підтверджені та не внесені до основного ланцюга блоків. Проте зі зростанням кількості запитів і відповідей, що надходять між SDN-WISE та блокчейн-системою MultiChain, навантаження на цей буферний простір збільшується. Унаслідок цього можуть виникати затримки в обробці транзакцій, що негативно впливає на загальну швидкодію системи. Додатково варто враховувати обмеженість пам’яті SDN-контролера, яка необхідна для підтримки актуальної інформації про топологію мережі та маршрутизацію трафіку, що також є важливим фактором загальної ефективності роботи системи.

З метою емпіричної перевірки розробленої архітектури було створено тестове середовище, що орієнтується на чотири базові процеси обміну повідомленнями, які забезпечують взаємодію між сервісами у рамках інфраструктури розумного міста. Щоб оцінити поведінку системи під різним навантаженням, поступово змінювалася кількість активних смарт-сервісів та IoT-вузлів.

Імітовані потоки повідомлень варіювались у межах від 100 до 5000, із затримками в обробці, які поступово зменшувалися: 600 мс, 120 мс, 60 мс, 30 мс, 15 мс та 5 мс. Такий підхід дозволяє точно вимірювати продуктивність системи в умовах різної інтенсивності навантажень.

У рамках моделювання особлива увага приділялася трьом ключовим сценаріям взаємодії між сервісами в контексті спільного реагування на надзвичайні події:

1) укладання угоди про рівень сервісу (SLA) між смарт-сервісами;

2) обробка запитів, що стосуються надзвичайних ситуацій, у процесі міжсервісної координації;

3) повний цикл обміну повідомленнями: від ініціації запиту до його обробки та зворотного зв’язку.

Тестова інфраструктура була реалізована на чотирьох окремих фізичних пристроях. З них три виступають як децентралізовані клієнтські вузли, пов’язані з окремими смарт-сервісами, а четвертий - як центральний блокчейн-вузол (глобальний сервер).

Технічні характеристики використаного обладнання наведено в таблиці 4.2, а структурну схему мережевої архітектури представлено у таблиці В.2 Додотку В.

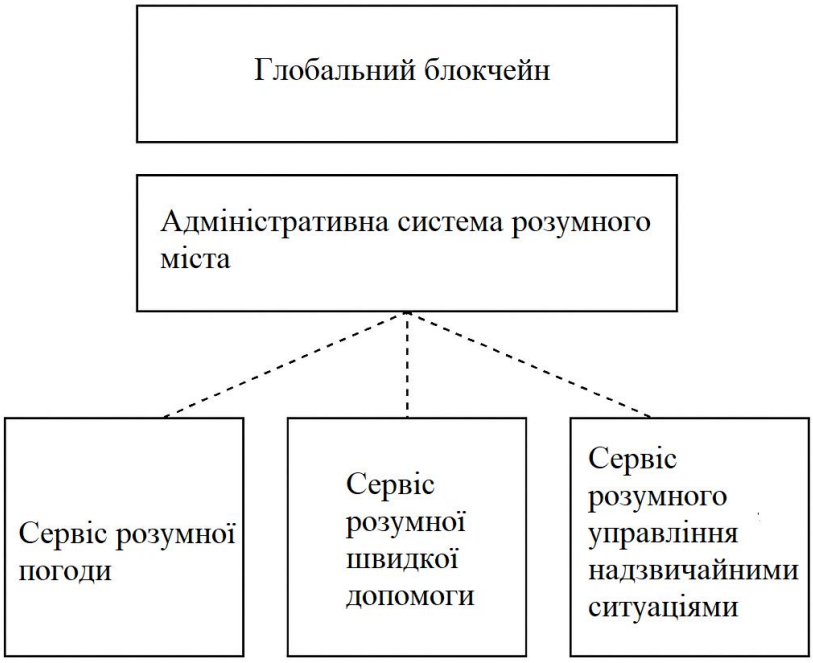

Рисунок 4.2 - Схематичне зображення мережевої архітектури запропонованого сценарію використання

Запит на укладення угоди про рівень обслуговування між взаємодіючими сервісами діє для досягнення інтероперабельності між смарт-сервісами необхідно встановити угоди про рівень обслуговування (SLA), які регламентують правила взаємодії між ними. Першим кроком до забезпечення такої взаємодії є створення глобальної угоди між усіма відповідними сервісами.

На рисунку 4.3 зображено послідовність етапів, що ілюструють процес створення та прийняття такої угоди.

сервіс A надсилає запит на встановлення угоди через агент застосунку до SDN-контролера в архітектурі SDIoT. Структура повідомлення запиту описується формулою , де символ X позначає назву сумісного сервісу :

$$M=(\text{Request}\|X\|\text{Hash}(\text{SessionKey})), \quad (4.1)$$

локальний адаптивний агент отримує зашифроване повідомлення із запитом з SDIoT-архітектури. Після цього він проводить перевірку автентичності як самого повідомлення, так і відповідних IoT-вузлів, використовуючи механізми локального блокчейн-ланцюга;

У разі успішної перевірки автентичності повідомлення та вузлів, запит перенаправляється до рушія правил;

Рушій правил створює локальне правило безпеки у форматі JSON, після чого передає його агенту клієнта “multi-chain” для збереження нової транзакції локальної угоди безпеки у локальному блокчейні;

Оскільки в рамках запропонованої моделі безпеки система multi-chain реалізована як клієнтські й серверні вузли, після запису транзакції в локальний блокчейн її копія перенаправляється до глобального блокчейну через глобальний адаптивний агент. Структура переданого повідомлення описується рівнянням, де AgreementTxid - це унікальний ідентифікатор транзакції локального сервісу безпеки.

$$M = (AgreementTxid \parallel Hash(SessionKey)), \quad (4.2)$$

Після успішної перевірки ідентифікатора сесії (Session ID) у глобальному блокчейні, запит перенаправляється до глобального рушія правил. Цей модуль відповідає за формування та застосування адміністративних політик безпеки, які регламентують взаємодію локальних сервісів у межах смарт-міста.

Після створення глобального правила безпеки у форматі JSON, відповідна транзакція формується за допомогою агента серверного вузла MultiChain і передається до рушія виконання в структурі глобального адаптивного модуля безпеки.

Далі рушій виконання здійснює пошук локального контракту безпеки сервісу, використовуючи ідентифікатор транзакції. Після цього він об’єднує локальний та глобальний контракти безпеки у модулі контексту, формуючи єдину політику, яка передається для подальшого виконання;

Під час процесу виконання транзакція глобального контракту безпеки надсилається агенту клієнтського вузла MultiChain через глобальний адаптивний агент;

На цьому етапі глобальний контракт безпеки витягується з локального блокчейну. Після цього локальний рушій виконання комбінує локальні вимоги безпеки з адміністративними та формує їх у форматі JSON, який передається до локального контекстного рушія.

Локальний рушій контексту виконує перевірку чинності глобального контракту безпеки. Як зображено на рисунку 4.3, цей етап завершується передачею перевіреного контракту до локального процесу виконання.

Локальний процес виконання пересилає запит до запрошеного сервісу.

Сервіс В, отримавши запит, виконує аналогічні дії, що були описані у кроках 2-14 для Сервісу А.

Після завершення перевірки безпеки, локальний адаптивний агент надсилає відповідь до агента застосунку Сервісу А;

Агент застосунку передає отримане повідомлення до SDN-контролера для повторної перевірки безпеки;.

У разі підтвердження автентичності повідомлення, ініціюється процедура прийняття угоди про рівень обслуговування (SLA).

Після згоди з умовами, валідність атрибутів безпеки SLA повторно перевіряється через клієнтського агента MultiChain.

Угода про рівень обслуговування, що пройшла всі етапи перевірки, зберігається у локальному репозиторії для подальшого використання.

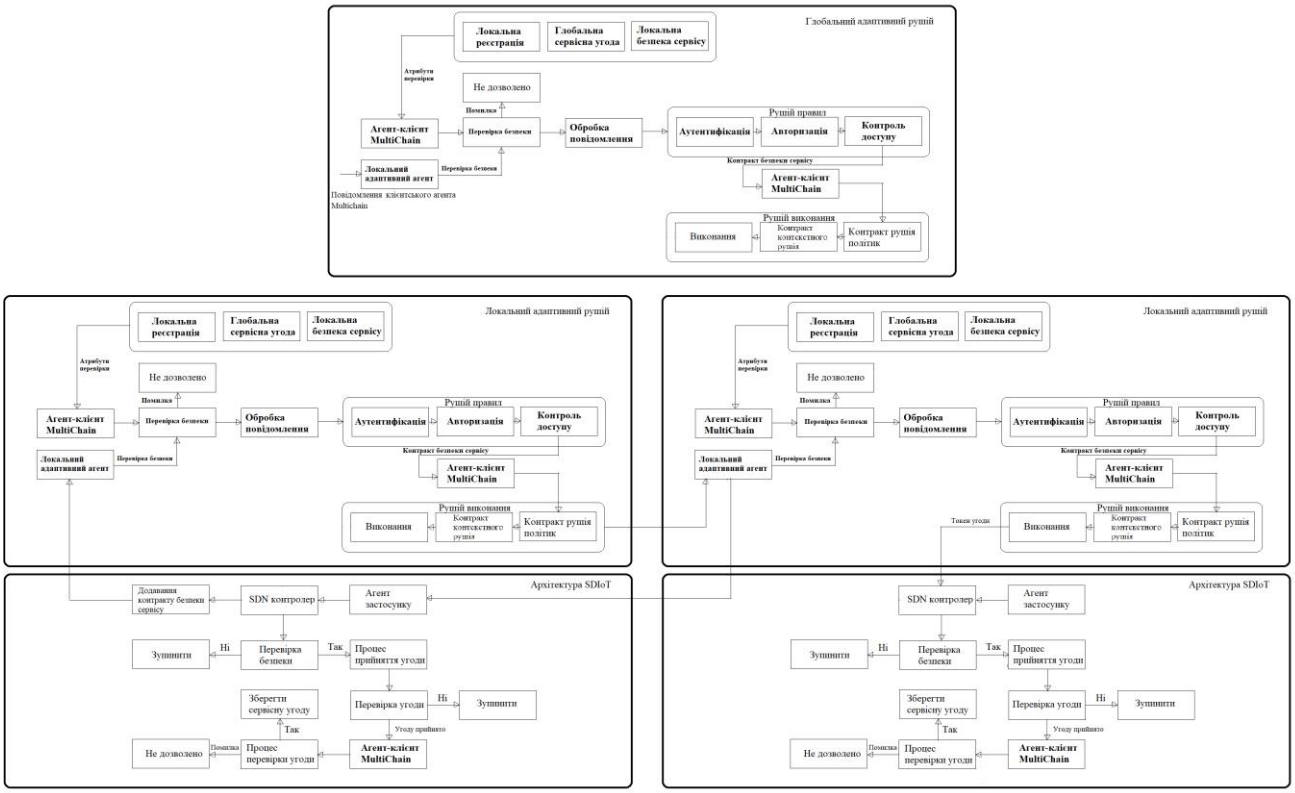

Рисунок 4.3 - Угода про рівень обслуговування між взаємодіючими сервісами.

Аналізуючи дані, представлені в таблиці 4.3, було виявлено суттєве підвищення пропускної здатності системи під час взаємодії трьох смарт-сервісів із метою формування угоди про рівень обслуговування. Особливо це проявилося у випадках, коли кожен сервіс мав у своєму розпорядженні по 50 сенсорних вузлів. Такий результат свідчить про здатність системи ефективно обробляти більший обсяг транзакцій у заданих умовах.

Зростання пропускної здатності прямо вплинуло на скорочення часу виконання смарт-контрактів у відповідних рушіях виконання. Помітне покращення

часу обробки демонструє, що механізми виконання контрактів стали працювати значно ефективніше, навіть у ситуаціях з високою щільністю запитів. Також зафіксовано, що затримка отримання запитів між глобальним адаптивним рушієм та сумісними сервісами зменшилася, що вказує на зростання чутливості й швидкодії запропонованої архітектури безпеки.

Разом із тим, при досягненні максимальної кількості одночасних запитів, показники ефективності системи починають знижуватися, що також відображено на рисунку 4.4, де представлено графічне відображення даних таблиці.

У межах другого експерименту було проведено оцінювання динаміки продуктивності системи за умови поступового збільшення кількості сенсорних пристроїв у сценарії безперервної взаємодії смарт-сервісів для формування SLA-запитів. Як показано у таблиці В.3 Додотку В, при зростанні кількості IoT-вузлів загальний рівень продуктивності погіршується у порівнянні з попередніми результатами.

Цей результат демонструє, що архітектура SDIoT відіграє ключову роль у стабільності та масштабованості безпекової моделі. Відповідні тенденції деградації продуктивності за зростання навантаження також візуалізовано на рисунку 4.5. Показники цієї матриці ефективності надають важливу інформацію про стійкість системи, її поведінку при змінних навантаженнях і здатність підтримувати узгоджену взаємодію між сервісами.

Рисунок 4.4 - Аналіз продуктивності при збільшенні числа запитів

Таблиця В.4 Додатку В ілюструє поведінку системи у відповідь на збільшення кількості IoT-вузлів. При зростанні числа вузлів від 100 до 2000 throughput зростає з 0.21 до 6.95 транзакцій на секунду, проте вже при 5000 вузлах він знижується до 3.2. Водночас час виконання контрактів та затримка отримання запиту коливаються, демонструючи, що надмірне збільшення кількості пристроїв погіршує узгодженість та швидкодію системи (див. рис. 4.4).

Ці результати демонструють, що архітектура SDIoT є ефективною за помірного навантаження, однак її масштабованість обмежена - надмірна кількість запитів або пристроїв призводить до зниження стабільності. Таким чином, подальша оптимізація має зосереджуватися на балансуванні навантажень та покращенні обробки транзакцій у розподіленому середовищі.

У контексті двосторонньої взаємодії смарт-сервісів було досліджено сценарій повного обміну повідомленнями - від початкової ініціації до фінального отримання відповіді.

Цей кейс підкреслює важливість запропонованої моделі безпеки для забезпечення надійності обміну даними в умовах інтенсивного міжсервісного трафіку. Відповідну схему взаємодії відправки та отримання повідомлень наведено на рисунку 4.5.

У цьому процесі смарт-сервіс А ініціює надсилання повідомлення про аварійну подію, яке формується агентом застосунку. Повідомлення передається до інших сервісів через SDN-контролер із зазначенням відповідних вимог безпеки. Після цього локальний адаптивний агент приймає повідомлення і здійснює перевірку автентичності за допомогою локального блокчейну. Він витягує атрибути валідації з реєстру і порівнює їх із вмістом повідомлення.

У разі успішного проходження перевірки повідомлення дешифрується та передається до рушія виконання. На цьому етапі рушій політик звертається до локального блокчейну, щоб отримати глобальний контракт безпеки за ідентифікатором транзакції. Контракт конвертується у формат JSON та передається

до контекстного рушія для виконання відповідної політики. У контекстному рушії перевіряється достовірність глобального контракту безпеки, після чого до повідомлення додається значення довіри, і воно надсилається на етап виконання.

Під час виконання перевіряється порогове значення довіри у повідомленні, і, якщо воно відповідає заданим критеріям, повідомлення пересилається до сервісу B. Своєю чергою, сервіс

B повторює описану послідовність дій у відповідь на запит, забезпечуючи повноцінний цикл двостороннього обміну повідомленнями.

Згідно з результатами, наведеною у таблиці В.5 Додатку В, було зафіксоване зниження продуктивності цього процесу у порівнянні з попередніми експериментами.

Основною причиною є зростання обчислювального навантаження, пов’язаного з криптографічними операціями шифрування і розшифрування в процесі повного обміну. Це погіршення відображено на рисунку 4.6, де представлено графічну залежність продуктивності від кількості запитів.

Також аналіз таблиці В.6 Додатку В вказує на зниження пропускної здатності системи при збільшенні кількості вузлів у сервісах, що підтверджує важливість врахування масштабованості при побудові архітектури безпеки. На рисунку 4.7 візуалізовано зміну ефективності системи в умовах поступового зростання кількості запитів.

Представлені результати підтверджують, що ефективність SDIoT-архітектури залежить як від обчислювального навантаження, так і від кількості учасників взаємодії у системі.

Таким чином, у межах дослідження було реалізовано повноцінну модель взаємодії смарт-сервісів у середовищі SDIoT із підтримкою механізмів безпеки на основі блокчейн-технологій. Було розроблено сценарії для моделювання основних процесів міжсервісної комунікації: від укладення угод про рівень обслуговування до повного циклу обміну повідомленнями між сервісами. Результати експериментів підтверджують, що запропонована архітектура здатна ефективно масштабуватись у середовищі з помірним навантаженням, забезпечуючи високу

пропускну здатність, зменшення часу виконання смарт-контрактів та зниження затримки отримання повідомлень.

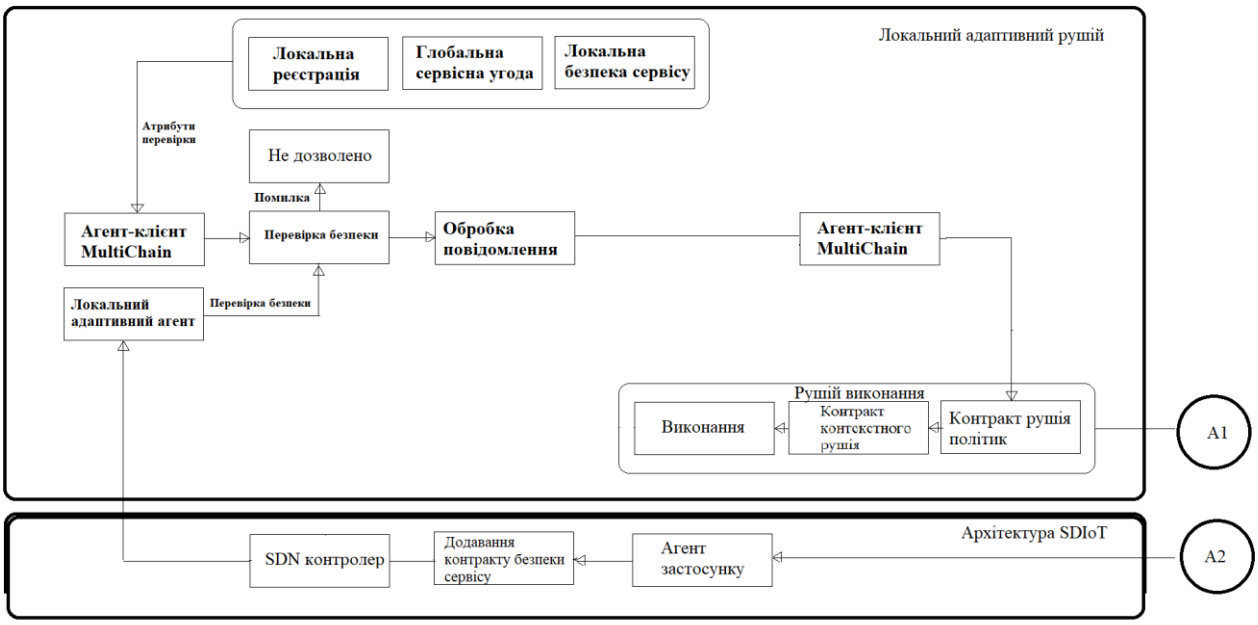

Рисунок 4.5 - Механізм обміну тривожними повідомленнями між взаємодіючими сервісами(частина 1).

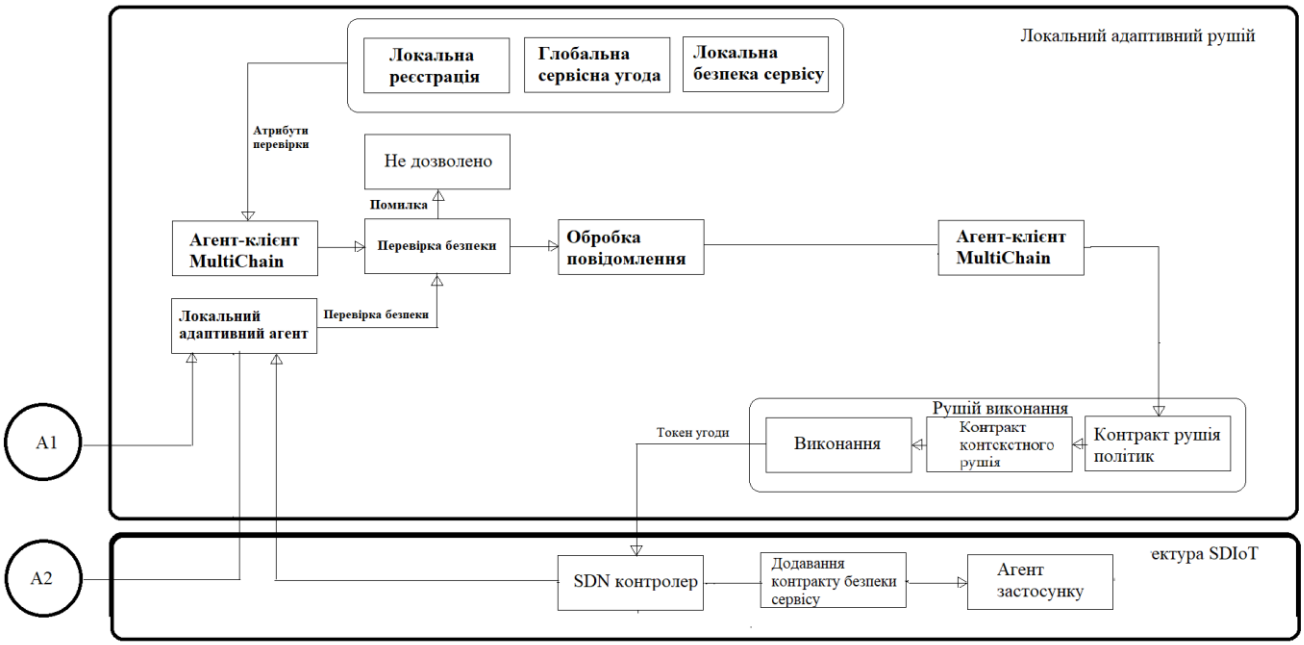

Рисунок 4.6 - Механізм обміну тривожними повідомленнями між взаємодіючими сервісами(частина 2).

Водночас було виявлено критичні межі продуктивності, пов’язані зі зростанням кількості одночасних запитів та вузлів, що актуалізує питання подальшої оптимізації обчислювальних ресурсів та механізмів розподілу навантаження.

Запропоноване рішення демонструє потенціал для впровадження в умовах реального функціонування розумного міста, сприяючи підвищенню рівня адаптивності, безпеки й надійності у сфері критично важливих сервісів.

Рисунок 4.7 - Оцінка ефективності процесу end-to-end передавання та отримання повідомлень при збільшенні запитів

4.2 Висновки

У даному розділі було представлено результати експериментальної реалізації запропонованого методу управління безпекою смарт-сервісів у середовищі розумного міста. Запропонований підхід базується на поєднанні технологій програмно-визначеного Інтернету речей (SDIoT), багатоланцюгової блокчейн-архітектури та смарт-контрактів, що разом забезпечують децентралізоване й адаптивне середовище для безпечної взаємодії між сервісами.

Результати моделювання демонструють, що метод ефективно масштабується в умовах помірного навантаження, забезпечуючи високу пропускну здатність, низький час виконання смарт-контрактів та зниження затримки обробки запитів. Було досліджено поведінку системи в умовах збільшення кількості запитів і IoT-вузлів, а також під час повного циклу двостороннього обміну повідомленнями між смарт-сервісами. Усі експерименти підтвердили, що ключовою перевагою методу є його здатність адаптивно реагувати на зміну середовища та підтримувати баланс між ефективністю, довірою та безпекою.

Окрему увагу приділено механізмам динамічного оновлення довіри, оцінці контексту запитів, формуванню сервісних угод (Service Agreement Tokens) та забезпеченню криптографічного захисту переданих повідомлень. Впровадження зазначених механізмів доводить життєздатність методу для умов реального розгортання в інфраструктурі інтелектуального міста.

Таким чином, проведене експериментальне дослідження підтверджує доцільність застосування розробленого методу для реалізації ефективного, стійкого та масштабованого підходу до управління безпекою в умовах багатокомпонентної взаємодії між цифровими сервісами смарт-міста.

ВИСНОВКИ

У роботі за результатами виконаних теоретичних та практичних досліджень розроблено метод управління безпекою для смарт-сервісів у середовищі розумного міста, що базується на використанні смарт-контрактів, багатоланцюгової блокчейн-інфраструктури та технологій SDIoT. Запропонований метод забезпечує адаптивне, децентралізоване й контекстно-залежне прийняття рішень щодо контролю доступу, взаємодії сервісів та виконання колаборативних завдань з урахуванням оцінки довіри й криптографічного захисту.

У першому розділі проведено аналіз існуючих підходів до управління безпекою в розумних містах, досліджено специфіку архітектур смарт-сервісів, розглянуто сучасні рішення на основі блокчейну та смарт-контрактів, а також обґрунтовано вибір інструментів і підходів для подальшої розробки методу.

У другому розділі побудовано концептуальну модель управління безпекою смарт-сервісів, що включає формальні вимоги до функціональних і нефункціональних властивостей, структуру взаємодії між суб’єктами системи, життєвий цикл смарт-контрактів, модель довіри та політики доступу, а також реалізовано її формалізацію у вигляді архітектурної та поведінкової специфікації.

У третьому розділі здійснено деталізацію архітектури методу, включно з модулями локального й глобального адаптивного управління, механізмами генерації та розподілу криптографічних ключів, описом політик безпеки, принципами роботи смарт-контрактів у мультиблокчейн-середовищі, а також впроваджено алгоритми обробки довіри й контролю доступу в умовах динамічної міжсервісної взаємодії.

У четвертому розділі проведено експериментальну перевірку працездатності та ефективності запропонованого методу шляхом моделювання сценаріїв взаємодії між сервісами. Отримано числові характеристики, що демонструють масштабованість, зниження затримки та стабільну продуктивність за умов різного навантаження. Досліджено поведінку системи в умовах зростання кількості вузлів і запитів, а також при виконанні повного циклу обміну повідомленнями.

Набула подальшого розвитку інформаційна технологія управління безпекою у середовищах із підвищеним рівнем взаємозалежності компонентів, що діють на основі смарт-контрактів, із підтримкою контекстного прийняття рішень та механізмів динамічної довіри у децентралізованих IoT-системах.

Впровадження результатів роботи дозволило підвищити рівень автоматизації прийняття безпекових рішень, знизити ризики несанкціонованого доступу, забезпечити прозорість взаємодії між сервісами та надати платформу для масштабованого використання смарт-сервісів у міській інфраструктурі.

За темою кваліфікаційної роботи магістра опублікована одна стаття у фаховому науковому виданні, а також підготовлено тези для участі в конференції Академії прикладних наук (АПКН).

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Yadav J., Misra M., Singh K. Sensitizing netizen's behavior through influencer intervention enabled by crowdsourcing-a case of reddit. Behaviour & Information Technology. 2022. Том. 41, № 6. С 1286–1297.

2. Koul B., Yadav D., Singh S., Kumar M., Song M. Insights into the domestic wastewater treatment (DWWT) regimes: a review. *Water*. 2022. № 14(21). С. 3542.

3. Wang H., Liu Z., Ge C., Sakurai K., Su C. A privacy-preserving data feed scheme for smart contracts. *IEICE Transactions on Information and Systems*. 2022. № E105D(2). С. 195–204.

4. Meijin L., Zhiyang F., Junfeng W., Luyu C., Qi Z., Tao Y. та ін. A systematic overview of android malware detection. *Applied Artificial Intelligence*. 2022. № 36(1). С. 2007327.

5. Biswas A., Roy A. Blockchain and IPFS based secure cloud banking system using smart card. *Research Square Preprint*. 2022. С. 1–34.

6. Kumar A., Kumar K.S., Sharma M., Menaka C., Naaz R., Vekriya V. Machine learning in molecular communication and applications for health monitoring networks. *Software Computing*. 2023.

7. Goscinski A., Delicato F.C., Fortino G., Kobusińska A., Srivastava G. Special issue on distributed intelligence at the edge for the future internet of things. *Journal of Parallel and Distributed Computing*. 2023. № 171. С. 157–162.

8. Bouchaala M., Ghazel C., Saidane L.A. Enhancing security and efficiency in cloud computing authentication and key agreement scheme based on smart card. *Journal of Supercomputing*. Springer, 2022. № 78(1). С. 497–522.

9. Sarna S., Czerwinski R. Small prime divisors attack and countermeasure against the RSA-OTP algorithm. *Electronics (Switzerland)*. MDPI AG, 2022. № 11(1).

10. Li S., Xu C., Zhang Y., Zhou J. A secure two-factor authentication scheme from password-protected hardware tokens. *IEEE Transactions on Information Forensics and Security*. 2022. № 17. С. 3525–3538.

11. Prabhu D., Vijay Bhanu S., Suthir S. Privacy preserving steganography based biometric authentication system for cloud computing environment. *Measurement: Sensors*. 2022. № 24. С. 100511.

12. Hafiza Razami H., Ibrahim R. Models and constructs to predict students' digital educational games acceptance: A systematic literature review. *Telematics and Informatics*. Elsevier Ltd., 2022. № 73.

13. Yang Y., Huang X., Li J., Sun J.S. BubbleMap: Privilege Mapping for Behavior-Based Implicit Authentication Systems. *IEEE Transactions on Mobile Computing*. 2023. № 22(8). С. 4548–4562.

14. Lone S.A., Mir A.H. A novel OTP based tripartite authentication scheme. *International Journal of Pervasive Computing and Communications*. 2022. № 18(4). С. 437–459.

15. Kaur S., Kaur G., Shabaz M. A secure two-factor authentication framework in cloud computing. *Security and Communication Networks*. 2022. С. 1–9.

16. Shakil K.A., Zareen F.J., Alam M., Jabin S. BAMCloud: a cloud based Mobile biometric authentication framework. *Multimedia Tools and Applications*. 2023. № 82(25). С. 39571–39600.

17. Robles-González P., Arias-Cabarcos P., Parra-Arnau J. Privacy-centered authentication: A new framework and analysis. *Computer Security*. 2023. № 132. С. 103353.

18. Mane J.S., Bhosale S. Advancements in biometric authentication systems: A comprehensive survey on internal traits, multimodal systems, and vein pattern biometrics. *Revue d'Intelligence Artificielle*. 2023. № 37(3). С. 709–718.

19. Chenchev I. Framework for Multi-factor Authentication with Dynamically Generated Passwords. *Future of Information and Communication Conference*. Cham: Springer Nature Switzerland, 2023. С. 563–576.

20. Berrios J., Mosher E., Benzo S., Grajeda C., Baggili I. Factorizing 2FA: Forensic analysis of two-factor authentication applications. *Forensic Science International: Digital Investigation*. 2023. № 45. С. 301569.

21. Binbeshr F., Por L.Y., Kiah M.M., Zaidan A.A., Imam M. Secure PIN-entry method using one-time PIN (OTP). *IEEE Access*. 2023. № 11. С. 18121–18133.

22. Correia D., Teixeira L., Marques J.L. Reviewing the State-of-the-Art of Smart Cities in Portugal: Evidence Based on Content Analysis of a Portuguese Magazine. *Publications*. 2022. № 9. С. 49.

23. Correia D., Vagos C., Marques J.L., Teixeira L. Fulfilment of last-mile urban logistics for sustainable and inclusive smart cities: A case study conducted in Portugal. *International Journal of Logistics Research and Applications*. 2022. С. 1–28.

24. Correia D., Teixeira L., Marques J.L. Study and analysis of the relationship between smart cities and Industry 4.0: A systematic literature review. *International Journal of Technology Management and Sustainable Development*. 2022. № 21. С. 37–66.

25. Madanchian M., Taherdoost H. The Impact of Digital Transformation Development on Organizational Change. In: *Driving Transformative Change in E-Business through Applied Intelligence and Emerging Technologies*. Hershey, PA: IGI Global, 2022. С. 1–24.

26. Taherdoost H. An Overview of Trends in Information Systems: Emerging Technologies that Transform the Information Technology Industry. *Cloud Computing and Data Science*. 2023. № 4. С. 1–16.

27. Correia D., Teixeira L., Marques J.L. Investigating Smart City Barriers: Contribution of Experts based on a Delphi Analysis. *Spatial Planning and Sustainable Development.* 2022. № 10. С. 179–199.

28. Correia D., Teixeira L., Marques J.L. Reviewing the State-of-the-Art of Smart Cities in Portugal: Evidence Based on Content Analysis of a Portuguese Magazine. *Publications*. 2022. № 9. С. 49.

29. Correia D., Vagos C., Marques J.L., Teixeira L. Fulfilment of last-mile urban logistics for sustainable and inclusive smart cities: A case study conducted in Portugal. International Journal of Logistics *Research and Applications*. 2022. С. 1–28.

30. Correia D., Teixeira L., Marques J.L. Study and analysis of the relationship between smart cities and Industry 4.0: *A systematic literature review. International*

Journal of Technology Management and Sustainable Development. 2022. № 21. С. 37–66.

31. Correia D., Teixeira L. From Smart City 1.0 to Smart City 3.0: Deep Understanding of the Smart City Concept and Evolution. Smart Cities and Tourism: Co-Creating Experiences, Challenges and Opportunities. London, UK: Goodfellow Publishers Ltd, 2023. С. 43.

32. Taherdoost H.A. Critical Review of Blockchain Acceptance Models-Blockchain Technology Adoption *Frameworks and Applications. Computers*. 2022. № 11. С. 24.

33. Madanchian M., Taherdoost H. The Impact of Digital Transformation Development on Organizational Change. Driving Transformative Change in E-Business through Applied Intelligence and Emerging Technologies. Hershey, PA, USA: IGI Global, 2022. С. 1–24.

34. Lai C.S., Jia Y., Lai L.L., Collinson A., McCulloch M.D., Wong K.P. A review of technical standards for smart cities. *Clean Technologies*. 2020. № 2(3). С. 290–310.

35. Ismagilova E., Hughes L., Rana N.P., Dwivedi Y.K. Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. *Information Systems Frontiers*. 2020. № 24. С. 393–414.

36. Ahad M.A., Paiva S., Tripathi G., Feroz N. Enabling technologies and sustainable smart cities. *Sustainable Cities and Society*. 2020. № 61. С. 102301.

37. Ross A., Banerjee S., Chowdhury A. Security in smart cities: A brief review of digital forensic schemes for biometric data. Pattern Recognition Letters. 2020. № 138. С. 346–354.

38. Sikder A.K., Petracca G., Aksu H., Jaeger T., Uluagac A.S. A survey on sensor-based threats and attacks to smart devices and applications. IEEE Communications Surveys & Tutorials. 2021. № 23(2). С. 1125–1159.

39. Lv Z., Qiao L., Singh A.K., Wang Q. AI-empowered IoT security for smart cities. *ACM Transactions on Internet Technology*. 2021. № 21(4). С. 1–21.

40. Chen D., Wawrzynski P., Lv Z. Cyber security in smart cities: A review of deep learning-based applications and case studies. *Sustainable Cities and Society*. 2021. № 66. С. 102655.

41. Ahad M.A., Paiva S., Tripathi G., Feroz N. Enabling technologies and sustainable smart cities. *Sustainable Cities and Society*. 2020. № 61. С. 102301.

42. Ross A., Banerjee S., Chowdhury A. Security in smart cities: A brief review of digital forensic schemes for biometric data. *Pattern Recognition Letters*. 2020. № 138. С. 346–354.

43. Sikder A.K., Petracca G., Aksu H., Jaeger T., Uluagac A.S. A survey on sensor-based threats and attacks to smart devices and applications. IEEE Communications Surveys & Tutorials. 2021. № 23(2). С. 1125–1159.

44. Lv Z., Qiao L., Singh A.K., Wang Q. AI-empowered IoT security for smart cities. *ACM Transactions on Internet Technology*. 2021. № 21(4). С. 1–21.

45. Chen D., Wawrzynski P., Lv Z. Cyber security in smart cities: A review of deep learning-based applications and case studies. *Sustainable Cities and Society*. 2021. № 66. С. 102655.

46. Al Harbi S., Halabi T., Bellaiche M. Fog computing security assessment for device authentication in the Internet of Things. IEEE 22nd International Conference on High Performance Computing and Communications. 2020.

47. Guerar M., Migliardi M., Palmieri F., Verderame L., Merlo A. Securing PIN-based authentication in smartwatches with just two gestures. *Concurrency and Computation: Practice and Experience*. 2020. № 32(18).

48. Alizadeh M., Dowlatshah K., Ahmadzadeh Raji M., Nabiel Alkhanak E. A secure and robust smart card-based remote user authentication scheme. *International Journal of Internet Technology and Secured Transactions*. 2020. № 10(3). С. 255–267.

49. Prabhanjan Yadav B., Shiva Sai Prasad C., Padmaja C., Naik Korra S., Sudarshan E. A coherent and privacy-protecting biometric authentication strategy in cloud computing. IOP Conference Series: Materials Science and Engineering. 2020. № 981.

50. Karie N.M., Kebande V.R., Ikuesan R.A., Sookhak M., Venter H.S. Hardening SAML by integrating SSO and multi-factor authentication (MFA) in the cloud. *Pervasive Computing Technologies for Healthcare*. 2020.

51. Karie N.M., Kebande V.R., Ikuesan R.A., Sookhak M., Venter H.S. Hardening SAML by Integrating SSO and Multi-Factor Authentication (MFA) in the Cloud. Pervasive Computing Technologies for Healthcare. 2020.

52. Gosavi S.S., Shyam G.K. A novel approach of OTP generation using time-based OTP and randomization techniques. Data Science and Security: Proceedings of IDSCS 2020. Springer, 2021. С. 159–167.

53. Hassan M.A., Shukur Z., Hasan M.K. An improved time-based one time password authentication framework for electronic payments. *International Journal of Advanced Computer Science and Applications*. 2020. № 11(11). С. 359–366.

54. Megouache L., Zitouni A., Djoudi M. Ensuring user authentication and data integrity in multi-cloud environment. Human-centric *Computing and Information Sciences*. 2020. № 10. С. 1–20.

55. Yellamma P., Rajesh P.S.S., Pradeep V.V.S.M., Manishankar Y.B. Privacy preserving biometric authentication and identification in cloud computing. *International Journal of Advanced Science and Technology*. 2020. № 29(6). С. 3087–3096.

56. Nalajala S., Moukthika B., Kaivalya M., Samyuktha K., Pratap N.L. Data security in cloud computing using three-factor authentication. International Conference on Communication, Computing and Electronics Systems: Proceedings of ICCCES 2019. Springer, 2020. С. 343–354.

57. Velásquez I. Framework for the Comparison and Selection of Schemes for Multi-Factor Authentication. *CLEI Electronic Journal*. 2021.

58. Rajasekar V., Jayapaul P., Krishnamoorthi S., Saračević M. Secure Remote User Authentication Scheme on Health Care, IoT and Cloud Applications: A Multi-layer Systematic Survey. *Acta Polytechnica Hungarica*. 2021.

59. Gosavi S.S., Shyam G.K. A novel approach of OTP generation using time-based OTP and randomization techniques. Data Science and Security: Proceedings of IDSCS 2020. Springer, 2021. С. 159–167.

60. Cunha V.A., Corujo D., Barraca J.P., Aguiar R.L. TOTP Moving Target Defense for sensitive network services. *Pervasive Mobile Computing*. 2021. № 74. С. 0–18.

61. Zheng Z., Xie S., Dai H.-N., Chen W., Chen X., Weng J., Imran M. An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems*. 2020. № 105. С. 475–491.

62. Marchesi L., Marchesi M., Destefanis G., Barabino G., Tigano D. Design patterns for gas optimization in ethereum. IEEE International *Workshop on Blockchain Oriented Software Engineering (IWBOSE)*. 2020. С. 9–15.

63. Chen Y., Zhang Y., Zhou B. Research on the risk of blockchain technology in Internet finance supported by wireless network. *EURASIP Journal on Wireless Communications and Networking*. 2020. № 71.

64. Perera S., Nanayakkara S., Rodrigo M., Senaratne S., Weinand R. Blockchain technology: Is it hype or real in the construction industry? *Journal of Industrial Information Integration*. 2020. № 17. С. 100125.

65. Dolgui A., Ivanov D., Potryasaev S., Sokolov B., Ivanova M., Werner F. Blockchain-oriented dynamic modelling of smart contract design and execution in the supply chain. International *Journal of Production Research*. 2020. № 58. С. 2184–2199.

66. Dolgui A., Ivanov D., Potryasaev S., Sokolov B., Ivanova M., Werner F. Blockchain-oriented dynamic modelling of smart contract design and execution in the supply chain. *International Journal of Production Research*. 2020. № 58. С. 2184–2199.

67. Sultana T., Almogren A., Akbar M., Zuair M., Ullah I., Javaid N. Data sharing system integrating access control mechanism using blockchain-based smart contracts for IoT devices. Applied Sciences. 2020. № 10. С. 488.

68. Wang H., Qin H., Zhao M., Wei X., Shen H., Susilo W. Blockchain-based fair payment smart contract for public cloud storage auditing. Information Sciences. 2020. № 519. С. 348–362.

69. De Giovanni P. Blockchain and smart contracts in supply chain management: *A game theoretic model. International Journal of Production Economics*. 2020. № 228. С. 107855.

70. Sharma A., Tomar R., Chilamkurti N., Kim B.-G. Blockchain based smart contracts for internet of medical things in e-healthcare. *Electronics*. 2020. № 9. С. 1609.

71. Huang X., Ye D., Yu R., Shu L. Securing parked vehicle assisted fog computing with blockchain and optimal smart contract design. *IEEE/CAA Journal of Automatica Sinica*. 2020. № 7. С. 426–441.

72. Oliva G.A., Hassan A.E., Jiang Z.M.J. An exploratory study of smart contracts in the Ethereum blockchain platform. Empirical Software Engineering. 2020. № 25. С. 1864–1904.

73. Seven S., Yao G., Soran A., Onen A., Muyeen S. Peer-to-peer energy trading in virtual power plant based on blockchain smart contracts. *IEEE Access*. 2020. № 8. С. 175713–175726.

74. Xuan S., Zheng L., Chung I., Wang W., Man D., Du X., Yang W., Guizani M. An incentive mechanism for data sharing based on blockchain with smart contracts. Computers & Electrical Engineering. 2020. № 83. С. 106587.

75. Fan K., Bao Z., Liu M., Vasilakos A.V., Shi W. Dredas: Decentralized, reliable and efficient remote outsourced data auditing scheme with blockchain smart contract for industrial IoT. *Future Generation Computer Systems*. 2020. № 110. С. 665–674.

76. Unal D., Hammoudeh M., Kiraz M.S. Policy specification and verification for blockchain and smart contracts in 5G networks. ICT Express. 2020. № 6. С. 43–47.

77. Omar I.A., Jayaraman R., Salah K., Simsekler M.C.E., Yaqoob I., Ellahham S. Ensuring protocol compliance and data transparency in clinical trials using Blockchain smart contracts. BMC Medical Research Methodology. 2020. № 20. С. 224.

78. Patil A.S., Hamza R., Hassan A., Jiang N., Yan H., Li J. Efficient privacy-preserving authentication protocol using PUFs with blockchain smart contracts. Computers & Security. 2020. № 97. С. 101958.

79. Debe M., Salah K., Rehman M.H.U., Svetinovic D. Monetization of services provided by public fog nodes using blockchain and smart contracts. *IEEE Access*. 2020. № 8. С. 20118–20128.

80. Vieira G., Zhang J. Peer-to-peer energy trading in a microgrid leveraged by smart contracts. *Renewable and Sustainable Energy Reviews*. 2021. № 143. С. 110900.

81. Ante L. Smart contracts on the blockchain-A bibliometric analysis and review. *Telematics and Informatics*. 2021. № 57. С. 101519.

82. Hewa T., Ylianttila M., Liyanage M. Survey on blockchain based smart contracts: Applications, opportunities and challenges. *Journal of Network and Computer Applications*. 2021. № 177. С. 102857.

83. Khan S.N., Loukil F., Ghedira-Guegan C., Benkhelifa E., Bani-Hani A. Blockchain smart contracts: Applications, challenges, and future trends. Peer-to-Peer Networking and Applications. 2021. № 14. С. 2901–2925.

84. Sharma P., Jindal R., Borah M.D. Blockchain-based decentralized architecture for cloud storage system. *Journal of Information Security and Applications*. 2021. № 62. С. 102970.

85. Namasudra S., Deka G.C., Johri P., Hosseinpour M., Gandomi A.H. The revolution of blockchain: State-of-the-art and research challenges. Archives of Computational Methods in Engineering. 2021. № 28. С. 1497–1515.

86. Kumar P., Kumar R., Gupta G.P., Tripathi R. A Distributed framework for detecting DDoS attacks in smart contract-Based Blockchain-IoT Systems by leveraging Fog computing. Transactions on Emerging Telecommunications Technologies. 2021. № 32. С. e4112.

87. Zhang L., Zhang Z., Wang W., Jin Z., Su Y., Chen H. Research on a covert communication model realized by using smart contracts in blockchain environment. IEEE Systems Journal. 2021. № 16. С. 2822–2833.

ДОДАТОК А
(обов'язковий)

ПУБЛІКАЦІЯ ПО ТЕМІ РОБОТИ

Сертифікат № 2024-035-1

Міністерство освіти і науки України
Хмельницький національний університет

СЕРТИФІКАТ

Войтков Андрій Олексійович

учасник XVI Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2024»

24 години участі (0,8 ECTS credits)

Голова оргкомітету АПКН-2024

Олег СИНЮК
проректор Хмельницького національного університету з наукової роботи, доктор технічних наук, професор

м. Хмельницький
15-16 листопада 2024

E-mail: apkt.khnu@gmail.com

ДОДАТОК Б
(обов'язковий)

ПРЕЗЕНТАЦІЯ

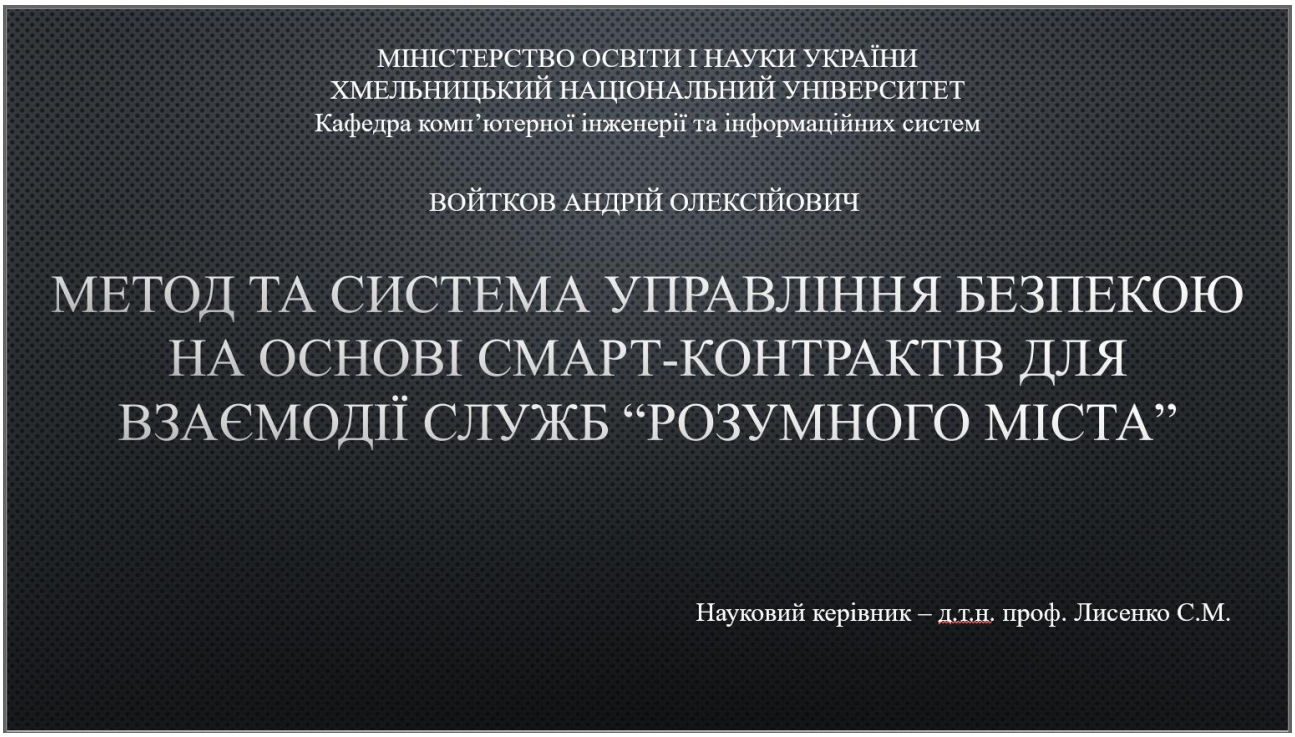

Рисунок Б.1 – слайд 1

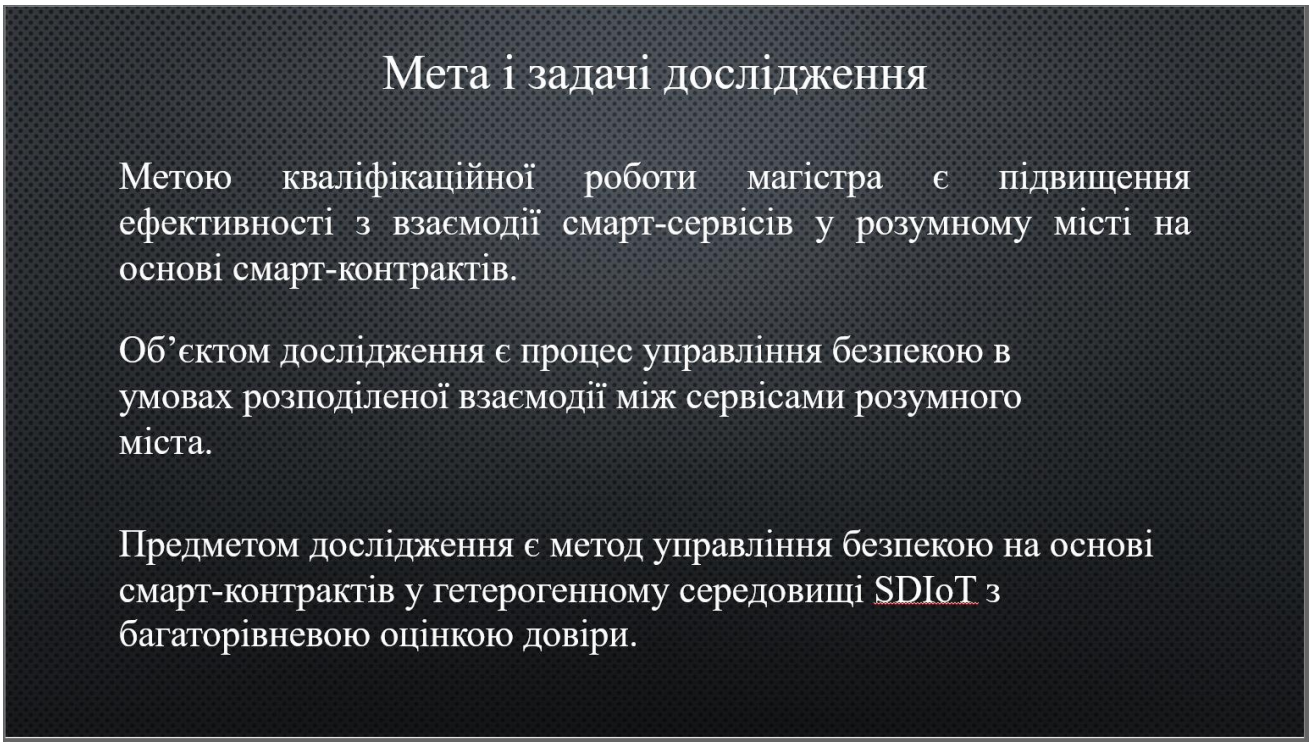

Рисунок Б.2 – слайд 2

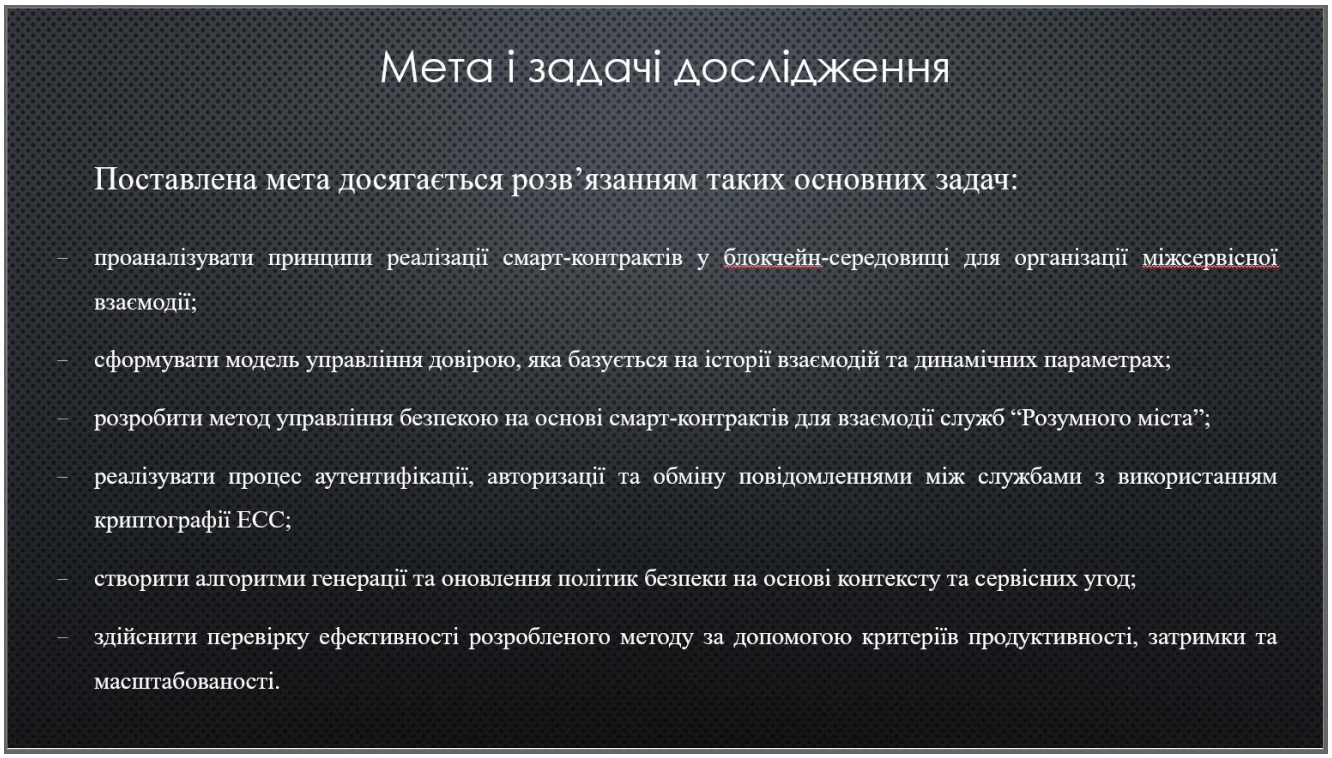

Рисунок Б.3 – слайд 3

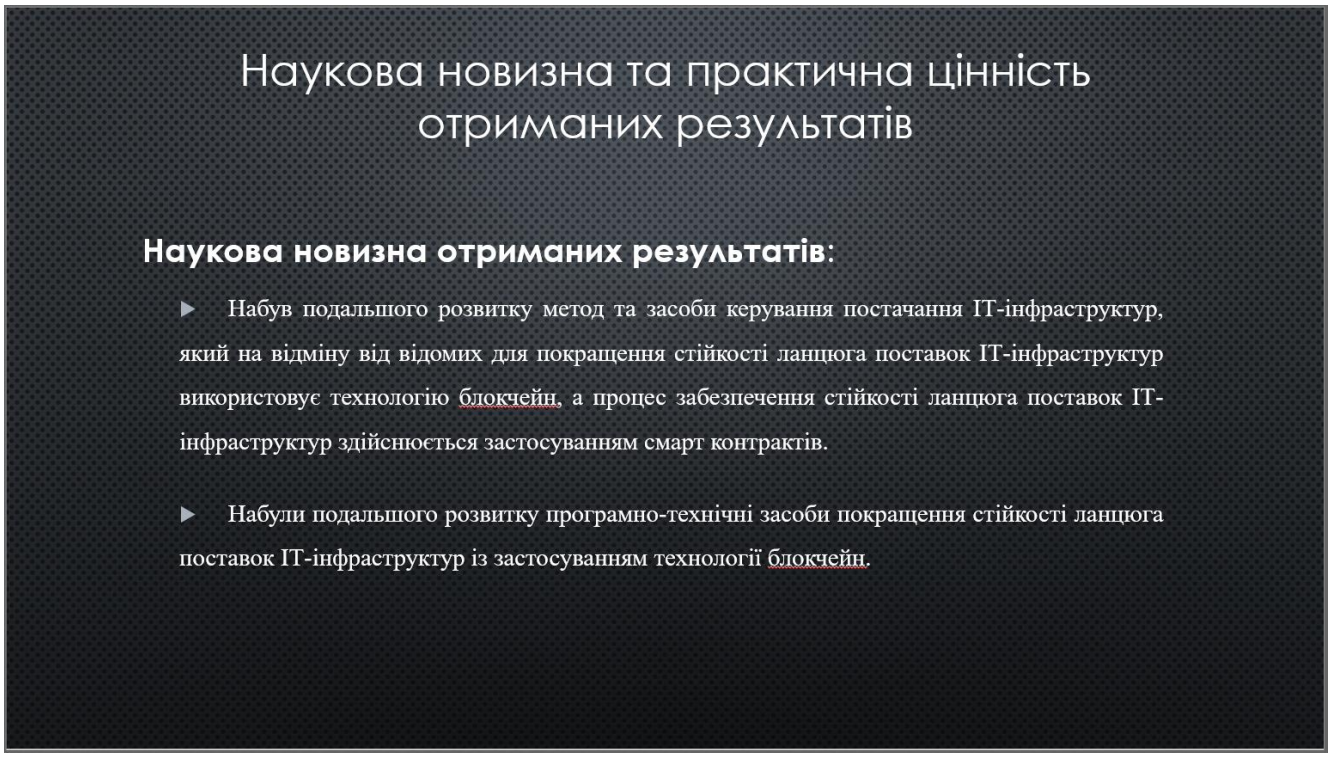

Рисунок Б.4 – слайд 4

Актуальність дослідження

Актуальність роботи полягає у розробці методу управління безпекою на основі смарт-контрактів, присутні наспуний функціонал:

- функціонує в інфраструктурі програмно-керованого Інтернету речей (SDIoT);
- підтримує багаторівневу взаємодію між сервісами та дозволяє формалізувати правила доступу;
- аутентифікація та довіра в умовах розподіленої архітектури інтелектуального міста.

Рисунок Б.5 – слайд 5

Удосконалений метод керування постачання IT-інфраструктур згідно з технологією блокчейн

Ключові аспекти методу:

1. Запропонований метод використовує децентралізований підхід до управління безпекою взаємодії між службами розумного міста..

2. Кожен учасник (сервіс, пристрій) діє як незалежний агент, що взаємодіє через смарт-контракти з чітко визначеними правилами.

3. Смарт-контракти використовуються для формалізації угод між сервісами, що дозволяє автоматизувати прийняття рішень та перевірку дотримання умов доступу.

4. Архітектура методу враховує контекст середовища та довіру між учасниками при прийнятті рішень.

Рисунок Б.6 – слайд 6

Етапи функціонування методу управління безпекою смарт-сервісів на основі смарт-контрактів

Кроки методу:
Крок №1 – відповідає за ініціацію безпечного запиту: формування запиту агентом, шифрування з використанням ECC та накладення цифрового підпису для автентифікації джерела.
Крок №2 – забезпечує дешифрування запиту локальним рушієм, витяг сесійного ключа та підготовку до створення захищеного каналу зв'язку.
Крок №3 – реалізує перевірку цілісності повідомлення шляхом порівняння хешів очікуваного та переданого сесійного ключа.
Крок №4 – виконує формування смарт-контракту локального рівня з даними автентифікації та авторизації; передає його до глобального рівня для затвердження.
Крок №5 – активує глобальний рівень управління безпекою, де створюється Service Agreement Token і зашифроване повідомлення передається далі.
Крок №6 – сторона одержувача розшифровує повідомлення та отримує доступ до контракту угоди.
Крок №7 – виконується логіка прийняття рішення, чи укладено угоду між сервісами на основі отриманого контракту.
Крок №8 – повторно верифікується Service Agreement Token через блокчейн, що підтверджує легітимність угоди.
Крок №9 – відбувається збереження токена в захищеному сховищі та його подальше використання для контролю доступу і ведення журналу взаємодій.

Рисунок Б.7 – слайд 7

Результат методу.

Показники ефективності угоди про рівень обслуговування між постачальником та споживачем послуг при зростанні кількості запитів

Без використання методу

Результати	Кількість запитів	Пропускна здатність (запитів/сек)	Час виконання контракту (мс)	Затримка отримання запиту (мс)
Низьке навантаження, низька продуктивність	100	0.24	2.48	3.72
Суттєве зростання пропускної здатності	500	2.17	2.32	3.26
Оптимальна швидкодія при зростаючому навантаження	1000	3.15	1.93	2.33
Найкраща продуктивність системи	2000	4.97	1.81	1.86
Ознаки перевантаження, зниження ефективності	5000	3.76	4.02	3.72

З використанням методу

Результати	Кількість запитів	Пропускна здатність (запитів/сек)	Час виконання контракту (мс)	Затримка отримання запиту (мс)
Низьке навантаження, низька продуктивність	100	0.41	1.66	2.66
Суттєве зростання пропускної здатності	500	3.63	1.55	2.33
Оптимальна швидкодія при зростаючому навантаження	1000	5.25	1.29	1.67
Найкраща продуктивність системи	2000	8.29	1.21	1.33
Ознаки перевантаження, зниження ефективності	5000	6.27	2.68	2.66

Рисунок Б.8 – слайд 8

Рисунок Б.9 – слайд 9

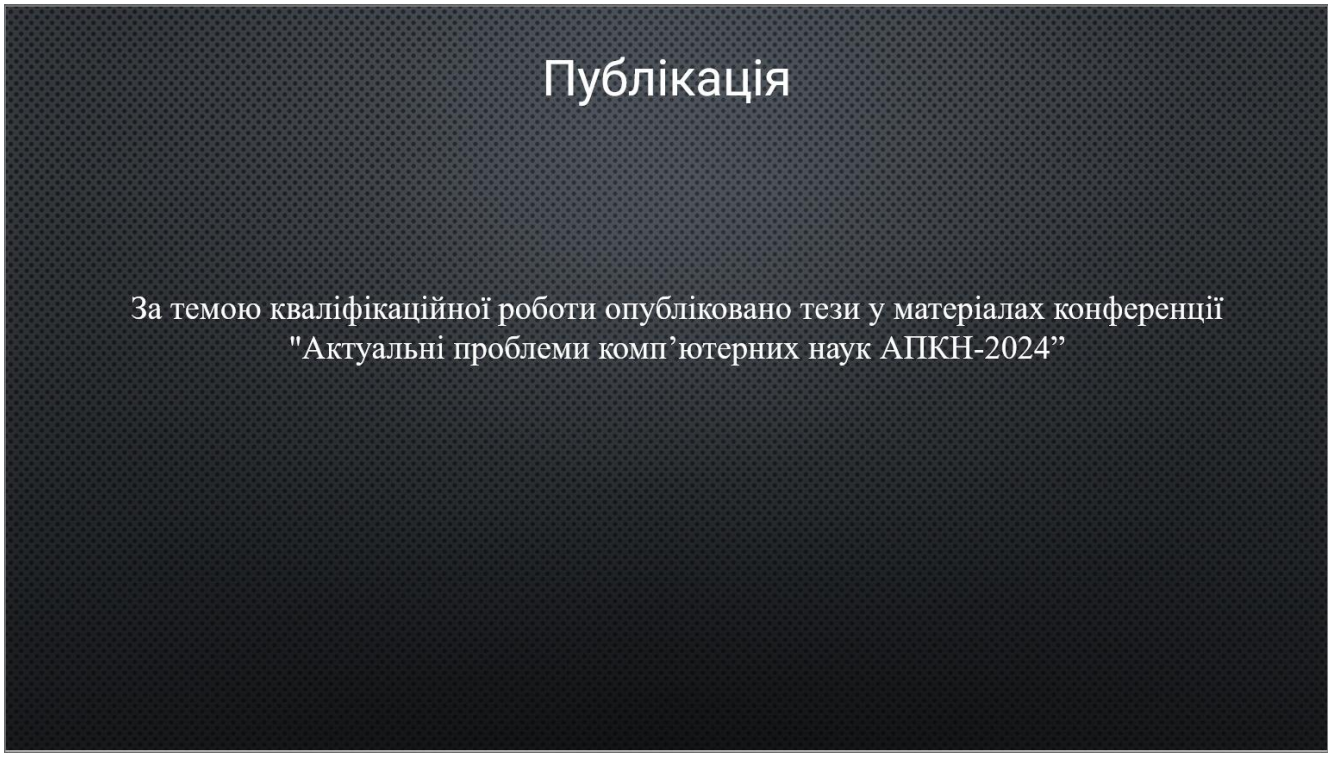

Рисунок Б.10 – слайд 10

Висновки

У роботі за результатами виконаних теоретичних та практичних досліджень розроблено метод управління безпекою для смарт-сервісів у середовищі розумного міста, що базується на використанні смарт-контрактів, багатоланцюгової блокчейн-інфраструктури та технологій SDIoT. Запропонований метод забезпечує адаптивне, децентралізоване й контекстно-залежне прийняття рішень щодо контролю доступу, взаємодії сервісів та виконання колаборативних завдань з урахуванням оцінки довіри й криптографічного захисту.

У першому розділі проведено аналіз існуючих підходів до управління безпекою в розумних містах, досліджено специфіку архітектур смарт-сервісів, розглянуто сучасні рішення на основі блокчейну та смарт-контрактів, а також обґрунтовано вибір інструментів і підходів для подальшої розробки методу.

У другому розділі побудовано концептуальну модель управління безпекою смарт-сервісів, що включає формальні вимоги до функціональних і нефункціональних властивостей, структуру взаємодії між суб'єктами системи, життєвий цикл смарт-контрактів, модель довіри та політики доступу, а також реалізовано її формалізацію у вигляді архітектурної та поведінкової специфікації.

Рисунок Б.11 – слайд 11

Висновки

У третьому розділі здійснено деталізацію архітектури методу, включно з модулями локального й глобального адаптивного управління, механізмами генерації та розподілу криптографічних ключів, описом політик безпеки, принципами роботи смарт-контрактів у мультиблокчейн-середовищі, а також впроваджено алгоритми обробки довіри й контролю доступу в умовах динамічної міжсервісної взаємодії.

У четвертому розділі проведено експериментальну перевірку працездатності та ефективності запропонованого методу шляхом моделювання сценаріїв взаємодії між сервісами. Отримано числові характеристики, що демонструють масштабованість, зниження затримки та стабільну продуктивність за умов різного навантаження. Досліджено поведінку системи в умовах зростання кількості вузлів і запитів, а також при виконанні повного циклу обміну повідомленнями.

Набула подальшого розвитку інформаційна технологія управління безпекою у середовищах із підвищеним рівнем взаємозалежності компонентів, що діють на основі смарт-контрактів, із підтримкою контекстного прийняття рішень та механізмів динамічної довіри у децентралізованих IoT-системах.

Впровадження результатів роботи дозволило підвищити рівень автоматизації прийняття безпекових рішень, знизити ризики несанкціонованого доступу, забезпечити прозорість взаємодії між сервісами та надати платформу для масштабованого використання смарт-сервісів у міській інфраструктурі.

Рисунок Б.12 – слайд 12

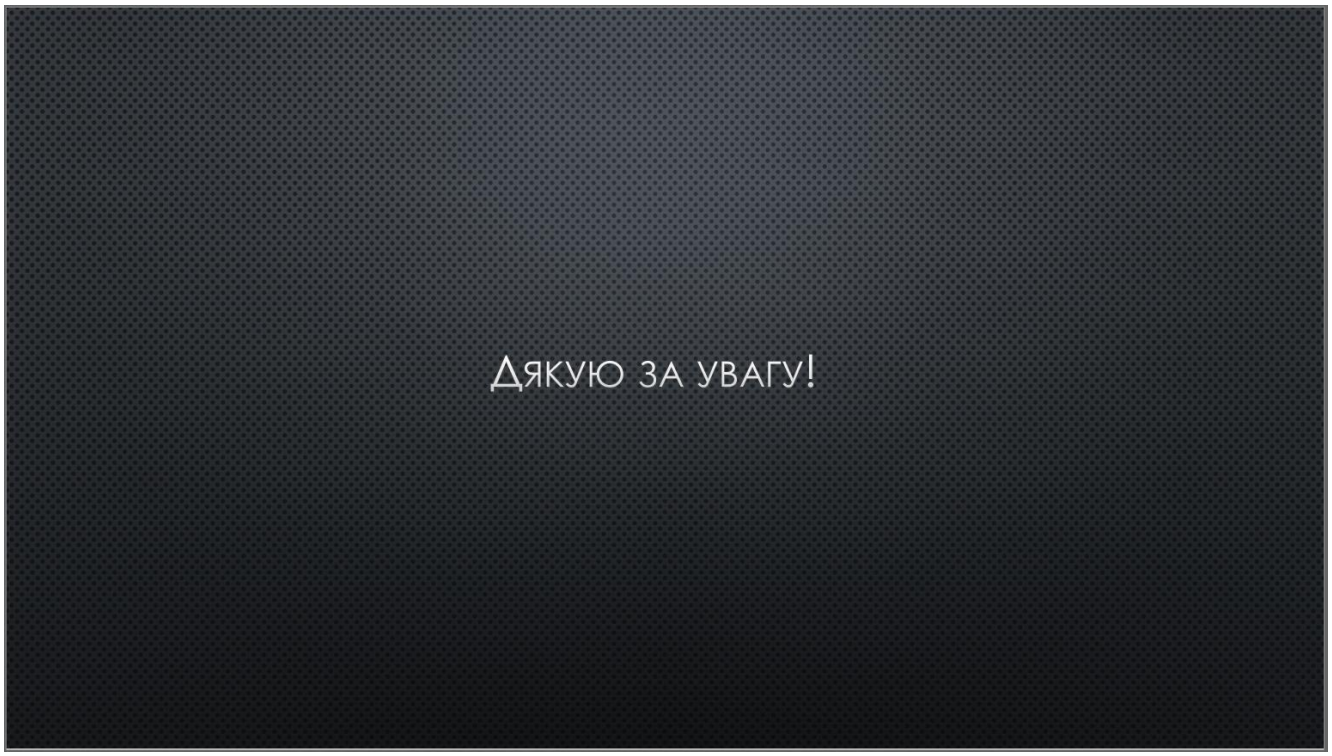

Рисунок Б.13 – слайд 13

ДОДАТОК В
(обов’язковий)

ТАБЛИЧНІ ДАНІ ДОСЛІДЖЕННЯ

Таблиця В.1 – Синтаксично сумісні правила безпеки для спільної роботи між розумними службами

Сервіс реагування на надзвичайні ситуації	Ідентифікація виконується за допомогою ECC-ключів розміром 128 біт	Встановлений рівень довіри: 0.003	Застосовується протокол IEEE 802.15.4
Сервіс прогнозування погодних умов	Аутентифікація реалізована за допомогою ECC-ключів на 192 біти	Рівень довіри складає 0.0033	Сумісність зі стандартом IEEE 802.15.4
Сервіс екстреної медичної допомоги	Аутентифікація базується на ECC-ключах довжиною 256 біт	Рівень довіри: 0.003	IEEE 802.15.4

Таблиця В.2 - Конфігурація обладнання чотирьох фізичних машин.

Процесор	Intel® 6-го покоління, Intel® Core™ i7 (6700)
Оперативна пам’ять	16 ГБ DDR
Чипсет	H110
Накопичувач	256 ГБ твердотільний диск (SSD) SATA

Таблиця В.3 - Показники ефективності SLA при зростанні кількості запитів

Результати	Кількість запитів	Пропускна здатність (запитів/сек)	Час виконання контракту (мс)	Затримка отримання запиту (мс)
Низьке навантаження, низька продуктивність	100	0.41	1.66	2.66
Суттєве зростання пропускної здатності	500	3.63	1.55	2.33
Оптимальна швидкодія при зростаючому навантаження	1000	5.25	1.29	1.67
Найкраща продуктивність системи	2000	8.29	1.21	1.33
Ознаки перевантаження, зниження ефективності	5000	6.27	2.68	2.66

Таблиця В.4 - Показники ефективності SLA при збільшенні кількості вузлів

Результати	Кількість вузлів	Пропускна здатність (запитів/сек)	Час виконання контракту (мс)	Затримка отримання запиту (мс)
Низька продуктивність при мінімальній кількості вузлів	100	0.21	1.82	2.98
Зростання ефективності, але ще із затримками	500	1.63	1.68	2.5
Оптимальна продуктивність за кількістю вузлів	1000	3.65	1.32	2.0
Найвищий показник throughput, але збільшується час виконання	2000	6.95	2.10	2.2
Падіння ефективності системи через надмірне навантаження	5000	3.20	2.30	2.8

Таблиця В.5 - Оцінка ефективності процесу повної передачі та прийому повідомлень при збільшенні кількості запитів

Результати	Кількість запитів	Пропускна здатність (запитів/сек)	Час виконання контракту (мс)	Затримка відповіді на запит (мс)
Базова ефективність, мінімальне навантаження	100	1.35	1.28	1.91
Покращення throughput при прийнятному часі затримки	500	5.12	1.12	2.12
Найкращий результат виконання контракту	1000	7.23	0.86	1.62
Максимальна продуктивність, але стабільна затримка	2000	13.53	1.26	2.12
Невелике падіння продуктивності через збільшене навантаження	5000	11.77	1.40	2.30

Таблиця В.6 - Оцінка ефективності двостороннього обміну повідомленнями залежно від кількості IoT-пристроїв

Результати	Кількість вузлів	Пропускна здатність (запитів/сек)	Час виконання контракту (мс)	Затримка відповіді (мс)
Мінімальне навантаження, низька продуктивність	100	0.21	1.72	2.5
Помірне покращення ефективності	500	3.12	1.52	2.3
Оптимальні показники швидкодії	1000	5.21	1.13	1.8
Найвища продуктивність, проте зростає затримка	2000	7.53	1.53	2.3
Перевантаження системи, зниження ефективності	5000	4.77	1.92	2.5

Tue May 06 19:12:17 EEST 2025, Медзатий Дмитро Миколайович, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.274 Educational

The maximum coincidence with one document 0.0%

Dictionaries check: en_US, ru_RU, ua_UA. **Errors in the documents: 12%**

	Document		Sum coincidence on the DB	
ID: 240917 Title: МКР Метод та система управління безпекою на основі смарт-контрактів для взаємодії служб “Розумного міста” Added in a DB: 2025-05-06 Authors: Андрій ВОЙТКОВ Heads: Сергій ЛИСЕНКО Consultants: Opponents:	Symbols	Lexemes	Symbols	Lexemes
	130881	1003	2239 (2%)	38 (4%)

Plagiarism sources

ID	Description	Plagiarism presence in the document	
		Symbols	Lexemes

Протокол аналізу звіту подібності експертом

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Андрій ВОЙТКОВ

Співавтор:

Назва: Войтков_Метод та система управління безпекою на основі смарт-контрактів для взаємодії служб "Розумного міста"

Експерт:

Підрозділ: Кафедра комп'ютерної інженерії та інформаційних систем

Коефіцієнт подібності 1:7.1%

Коефіцієнт подібності 2:3.6%

Мікропробіли: 0

Заміна букв: 3

Інтервали: 0

Білі знаки: 1

Дата створення звіту: 2025-05-06 21:11:53.0

Після аналізу Звіту подібності констатую наступне:

☒ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

2025-05-07 Доцент Андрій Нічепорук

Дата експерт

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА

Здобувач: Андрій ВОЙТКОВ

Тема: Метод та система управління безпекою на основі смарт-контрактів для взаємодії служб "Розумного міста"

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи магістра:

Кількість листів креслень – ; кількість сторінок записки 81

1. Короткий зміст роботи та прийнятих рішень у роботі запропоновано метод та система управління безпекою на основі смарт-контрактів для взаємодії служб "Розумного міста"

2. Висновок про відповідність роботи дипломному завданню Кваліфікаційна робота магістра відповідає виданому завданню

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі проведено відомих методів управління безпекою у розподілених смарт-сервісах розумного міста. Досліджено відомі рішення та засоби в цій сфері. У другому розділі запропоновано модель процесу управління безпекою на основі смарт-контрактів для взаємодії служб "розумного міста" У третьому розділі запропоновано метод управління безпекою на основі смарт-контрактів для взаємодії служб "розумного міста". У четвертому розділі запропоновано систему управління безпекою на основі смарт-контрактів для взаємодії служб "розумного міста".

4. Позитивні сторони роботи: Запропоновано метод управління безпекою для смарт-сервісів у середовищі розумного міста, що базується на використанні смарт-контрактів, багатоланцюгової блокчейн-інфраструктури та технологій SDIoT

5. Негативні сторони роботи: В роботі присутні певні логічні помилки щодо опису взаємодії суб'єктів моделі та механізмів узгодження політик безпеки. Деякі етапи методів недостатньо формалізовані, що ускладнює їхню відтворюваність.

6. Оцінка графічного оформлення та пояснювальної записки роботи: –

7. Відгук про роботу в цілому: В загальному робота виконана на невисокому рівні.

8. Інші зауваження: –

9. Оцінка кваліфікаційної роботи магістра:

Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи магістра вважаю, що робота заслуговує оцінки «задовільно» 3.00 (E)

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) д.т.н., професор, Мартинюк В.В., завідувач кафедри автоматизації, комп'ютерно-інтегрованих технологій та робототехніки

" 5 травня " 2025р.

Завідувачу кафедри КІІС
доктору філософії, доценту
Ользі ПАВЛОВІЙ

Войтова Андрія Олексійовича
ПІБ здобувача вищої освіти

ФІТ, 2 курсу, групи КІ2м-23-2

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 01.07.2022, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений(а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (StrikePlagiarism та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

6 травня 2025 року

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ
КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ
ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Метод та система управління безпекою на основі смарт-контрактів для взаємодії служб "Розумного міста"

Автор: Андрій ВОЙТКОВ

Спеціальність: 123 – Комп'ютерна інженерія

Освітня програма: освітньо-наукова

Науковий керівник: Сергій ЛИСЕНКО, д-р. техн. наук, професор

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи. Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з джерелами на один фрагмент речення;
2) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості StrikePlagiarism, складає :7.1% і адресується до 39 першоджерела; та системою Anti-Plagiarism складає 0%, що, з урахуванням наведених обгрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ Сергій ЛИСЕНКО

Гарант ОП _____ Олег САВЕНКО

Завідувач кафедри КІС _____ Ольга ПАВЛОВА