МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ, ОБЛІКУ ТА ФІНАНСІВ
Кафедра комп'ютерних технологій і моделювання систем

Кваліфікаційна робота
на правах рукопису

Пожарко Антон Русланович
(прізвище, ім’я, по батькові здобувача освіти)

УДК 004.7:004.056.5

КВАЛІФІКАЦІЙНА РОБОТА

Моделювання системи безпеки IoT-пристроїв на основі блокчейн-технологій
(тема роботи)
122 Комп’ютерні науки
(шифр і назва спеціальності)

Подається на здобуття освітнього ступеня магістр

кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
Пожарко А. Р.
(підпис, ініціали та прізвище здобувача вищої освіти)

Керівник роботи
Лапін А.В..
(прізвище, ім’я, по батькові)
к.т.н.
(науковий ступінь, вчене звання)

Житомир – 2025

Висновок кафедри комп'ютерних технологій і моделювання систем:
за результатами попереднього захисту: _____

Протокол засідання кафедри комп'ютерних технологій і моделювання систем
№ ____ від «_____» _____ 20__ р.

Завідувач кафедри комп'ютерних технологій і моделювання систем
к.п.н., доцент _____ М. О. Ковальчук
(науковий ступінь, вчене звання) (підпис)
(прізвище, ім'я, по батькові)
«_____» _____ 20___ р.

Результати захисту кваліфікаційної роботи

Здобувач вищої освіти Пожарко Антон Русланович захистив (ла)
(прізвище ,ім'я, по батькові)
кваліфікаційну роботу з оцінкою:

сума балів за 100-бальною шкалою _____
за шкалою ECTS _____
за національною шкалою _____

Секретар ЕК
лаборант кафедри _____ В. В. Корольчук
(науковий ступінь, вчене звання) (підпис)
(прізвище, ім'я, по батькові)

АНОТАЦІЯ

Пожарко А. Р. *Моделювання системи безпеки IoT-пристроїв на основі блокчейн-технологій.* – *Кваліфікаційна робота на правах рукопису.*

Кваліфікаційна робота на здобуття освітнього ступеня магістр за спеціальністю **122 – Комп'ютерні науки**. – Поліський національний університет, Житомир, 2025.

Обсяг кваліфікаційної роботи: **32 сторінки** (кількість рисунків – ___, таблиць – ___, додатків – ___, використаних джерел – 45).

Ключові слова: Internet of Things, IoT, кібербезпека, блокчейн, Hyperledger Fabric, контроль доступу, аномалії, математичне моделювання.

Кваліфікаційна робота присвячена розробленню та дослідженню системи безпеки IoT-пристроїв на основі блокчейн-технологій. У роботі проаналізовано архітектуру IoT-систем та основні загрози їх інформаційній безпеці. Обґрунтовано доцільність використання дозвільної блокчейн-платформи Hyperledger Fabric для забезпечення автентифікації, контролю доступу та цілісності даних.

Запропоновано архітектурну та математичну модель системи захисту IoT-пристроїв, яка формалізує процеси обробки подій, оцінювання аномальної поведінки та динаміку ризику. Для наочного подання роботи системи використано UML-діаграми. Запропонований підхід забезпечує адаптивне реагування на порушення безпеки та може бути застосований у корпоративних і промислових IoT-інфраструктурах.

SUMMARY

Pozharko A. R. *Modeling a security system for IoT devices based on blockchain technologies.* – *Qualification work in the form of a manuscript.*

Qualification work for obtaining the Master's degree in specialty **122 – Computer Science**. – Polesie National University, Zhytomyr, 2025.

The volume of the work: **32 pages** (number of figures – ___, tables – ___, appendices – ___, references – 45).

Key words: Internet of Things, IoT, cybersecurity, blockchain, Hyperledger Fabric, access control, anomaly detection, mathematical modeling.

The qualification work focuses on the development and study of an IoT device security system based on blockchain technologies. The architecture of IoT systems and key security threats are analyzed, and the feasibility of using the permissioned Hyperledger Fabric platform for authentication, access control, and data integrity is substantiated.

An architectural and mathematical model of the IoT security system is proposed, formalizing event processing, anomaly detection, and risk dynamics. UML diagrams are used to illustrate system operation. The proposed approach provides adaptive security response and can be applied in corporate and industrial IoT infrastructures.

Зміст

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IoT – Інтернет речей

MSP – служба керування ідентичністю в Hyperledger Fabric

ACL – список контролю доступу

ABAC – атрибутивна модель контролю доступу

PKI – інфраструктура відкритих ключів

CA – центр сертифікації

Tx – транзакція

T – транзакція, сформована пристроєм/шлюзом

Sig_g – цифровий підпис шлюзу

Sig_peer – цифровий підпис вузла-валідатора

E(t) – множина обов'язкових підтверджень для транзакції

Sig(t) – множина отриманих підписів

R_max – граничний допустимий рівень ризику

A(x) – функція виявлення аномалій

StateDB – база станів у Hyperledger Fabric

Ledger – незмінний журнал блокчейна

Chaincode – смартконтракт у середовищі Hyperledger Fabric

Orderer – сервіс формування та впорядкування блоків у Fabric

Peer – вузол-учасник, що виконує симуляцію та валідацію транзакцій

Gateway – шлюз, через який IoT-пристрої взаємодіють із блокчейном

Device – IoT-пристрій (сенсор, контролер, виконавчий модуль)

TLS – протокол безпечної передачі даних

API – Application Programming Interface

JSON – формат обміну даними

CPU/RAM – апаратні ресурси пристрою

DoS/DDoS – атаки типу відмови в обслуговуванні

gRPC – протокол взаємодії у Fabric

SDK – Software Development Kit

ВСТУП

У сучасних інформаційних системах спостерігається стрімке зростання кількості IoT-пристроїв, які використовуються у промисловості, транспорті, енергетиці, медичних системах та розумній інфраструктурі. Такі пристрої функціонують у гетерогенних мережевих середовищах, часто мають обмежені обчислювальні ресурси та працюють без постійного контролю з боку користувача. У поєднанні з централізованими моделями управління це створює підвищений рівень вразливості, що робить IoT-системи привабливою ціллю для кібератак, зокрема підміни даних, несанкціонованого доступу та компрометації керуючих команд.

Традиційні підходи до забезпечення безпеки IoT-інфраструктур здебільшого базуються на централізованих серверах автентифікації та зберігання журналів подій. Такий підхід має суттєві недоліки, оскільки наявність єдиного центру довіри призводить до ризику повної компрометації системи у разі успішної атаки. Крім того, централізовані журнали подій не гарантують незмінності записів і можуть бути змінені або видалені без можливості подальшого виявлення таких дій.

Одним із перспективних напрямів вирішення зазначених проблем є використання блокчейн-технологій, які забезпечують розподілене зберігання даних, криптографічну цілісність транзакцій та прозорий механізм перевірки дій учасників системи. Особливий інтерес у контексті корпоративних та промислових IoT-рішень становлять дозволені (permissioned) блокчейн-платформи, зокрема Hyperledger Fabric, які поєднують децентралізований журнал подій із можливістю чіткого контролю ідентичності учасників та політик доступу.

Разом з тим, застосування блокчейн-технологій у сфері безпеки IoT потребує формального опису процесів взаємодії між пристроями, шлюзами та блокчейн-інфраструктурою. Без побудови математичної моделі неможливо забезпечити коректне визначення станів пристроїв, оцінку їх поведінки та формалізоване реагування на ризикові або аномальні дії. Саме тому актуальним є завдання моделювання системи безпеки IoT-пристроїв, яка поєднує архітектурні рішення Hyperledger Fabric з математичним апаратом аналізу транзакцій, станів та ризиків.

Мета дослідження

Метою магістерської роботи є розроблення та дослідження математичної та архітектурної моделі системи безпеки IoT-пристроїв на основі блокчейн-технологій, яка забезпечує автентифікацію учасників, незмінність журналів подій, контроль доступу та адаптивне реагування на аномальну поведінку пристроїв.

Завдання дослідження

Для досягнення поставленої мети у роботі необхідно розв’язати такі завдання: проаналізувати архітектуру та особливості функціонування IoT-систем з точки зору безпеки; дослідити основні загрози та обмеження традиційних підходів до захисту IoT-інфраструктур; проаналізувати можливості блокчейн-технологій та обґрунтувати вибір платформи Hyperledger Fabric; розробити формальну модель транзакцій та умов їх валідності; побудувати математичну модель переходу станів IoT-пристроїв у процесі взаємодії з системою; розробити модель оцінки ризику поведінки пристроїв та механізм реагування на аномалії; узгодити математичну модель з архітектурою системи захисту IoT-пристроїв.

Об’єкт дослідження

Об’єктом дослідження є процеси взаємодії IoT-пристроїв у розподілених мережевих середовищах.

Предмет дослідження

Предметом дослідження є математичні, алгоритмічні та архітектурні моделі забезпечення безпеки IoT-пристроїв на основі блокчейн-технологій.

Практичне значення роботи

Результати роботи можуть бути використані при проєктуванні та впровадженні корпоративних і промислових IoT-систем, де необхідні прозорий контроль дій пристроїв, захист від несанкціонованого доступу та можливість формалізованого реагування на інциденти безпеки.

1. Теоретичні засади функціонування IoT-систем та їх інформаційної безпеки

1.1. Аналіз предметної області IoT

Інтернет речей (Internet of Things, IoT) є класом розподілених кіберфізичних систем, у межах яких фізичні об’єкти, оснащені сенсорами, виконавчими модулями та мережевими інтерфейсами, здійснюють автоматизований збір, передачу й обробку даних без безпосередньої участі людини. IoT-системи широко застосовуються у промисловій автоматизації, енергетиці, транспорті, медицині, «розумних» будівлях та інфраструктурних об’єктах, де ключовими вимогами є автономність, масштабованість і безперервність функціонування.

Типова архітектура IoT має багаторівневу структуру, що включає рівень пристроїв (сенсори та актуатори), рівень шлюзів і рівень обробки та зберігання даних. Пристрої генерують телеметрію або виконують команди, шлюзи забезпечують агрегацію, попередню обробку та передачу даних, а серверний або хмарний рівень реалізує логіку керування та аналітичні функції. Така архітектура дозволяє масштабувати систему, проте одночасно ускладнює контроль взаємодій між її компонентами.

Однією з визначальних характеристик IoT є гетерогенність. У межах однієї системи можуть функціонувати пристрої з різними апаратними ресурсами, операційними середовищами та протоколами зв’язку. Це унеможливлює використання уніфікованих механізмів захисту та створює додаткові ризики, пов’язані з помилками конфігурації, несумісністю компонентів і різним рівнем захищеності вузлів.

Іншою суттєвою особливістю IoT-систем є обмежені обчислювальні ресурси більшості пристроїв. Мікроконтролери з низькою продуктивністю та мінімальним обсягом пам’яті не здатні виконувати складні криптографічні операції або зберігати великі обсяги службової інформації. Унаслідок цього значна частина

функцій безпеки переноситься на шлюзи або зовнішні обчислювальні вузли, що підвищує залежність системи від проміжних компонентів.

IoT-системи зазвичай функціонують у відкритому або напівконтрольованому середовищі. Пристрої можуть бути фізично доступними для сторонніх осіб та використовувати публічні канали зв’язку, що істотно підвищує ризик несанкціонованого доступу, підміни даних і втручання у процеси керування. У таких умовах особливо актуальними стають завдання забезпечення автентичності пристроїв, цілісності переданої інформації та трасованості дій у системі.

Масштабованість IoT-мереж створює додаткові виклики з точки зору безпеки. Зі зростанням кількості пристроїв централізовані механізми керування стають «вузьким місцем» і формують єдині точки відмови. Компрометація центрального сервера або служби автентифікації може призвести до порушення роботи всієї системи, що є критичним для промислових і інфраструктурних застосувань.

Таким чином, специфіка предметної області IoT визначається поєднанням гетерогенності, обмежених ресурсів, відкритого середовища функціонування та високої масштабованості. Ці фактори формують комплексні вимоги до систем безпеки, які мають забезпечувати контроль дій пристроїв, стійкість до компрометації окремих вузлів та можливість незалежної перевірки подій у розподіленому середовищі. Саме ці особливості обумовлюють доцільність застосування децентралізованих підходів до захисту IoT-систем, що розглядається у наступних підрозділах.

1.2. Теоретичні основи забезпечення безпеки IoT

Забезпечення інформаційної безпеки є базовою умовою стабільного функціонування IoT-систем, оскільки порушення захищеності навіть окремого пристрою може призвести до компрометації всієї мережі. На відміну від традиційних інформаційних систем, IoT характеризується високою децентралізацією, автономністю вузлів та відсутністю постійного

адміністративного контролю, що суттєво ускладнює реалізацію класичних механізмів захисту.

Теоретично безпека IoT ґрунтується на загальноприйнятих принципах конфіденційності, цілісності, доступності та автентичності. Проте специфіка IoT-середовищ зумовлює необхідність їх адаптації. Обмежені апаратні ресурси пристроїв не дозволяють повною мірою застосовувати традиційні криптографічні алгоритми, а динамічна топологія мережі ускладнює централізоване керування ідентичностями та політиками доступу.

Однією з ключових проблем безпеки IoT є автентифікація пристроїв. У багатьох реалізаціях використовуються спрощені механізми ідентифікації або спільні ключі, що створює ризики підміни пристроїв та клонування вузлів. У результаті система втрачає можливість достовірно визначити джерело даних або команд, що є критичним для автоматизованих середовищ керування.

Не менш важливим аспектом є забезпечення цілісності даних. Передавання телеметрії через публічні або бездротові канали зв’язку робить IoT-системи вразливими до атак типу «людина посередині», модифікації повідомлень та ін’єкцій хибних даних. Оскільки результати вимірювань часто використовуються для прийняття рішень у реальному часі, порушення цілісності інформації може мати безпосередні фізичні наслідки.

Проблема доступності також має особливе значення для IoT. Масові DDoS-атаки на слабозахищені пристрої або шлюзи здатні вивести з ладу критичні сервіси. Крім того, енергетичні обмеження сенсорів роблять їх чутливими до атак, спрямованих на виснаження ресурсів.

Окрему категорію загроз становить відсутність надійного журналювання подій. У централізованих архітектурах журнали можуть бути змінені або видалені у разі компрометації сервера. Це унеможливлює проведення повноцінного аудиту та встановлення причин інцидентів безпеки, що є критичним для промислових і регульованих середовищ.

Таблиця 1.1 – Класифікація основних загроз IoT

Категорія загрози	Опис
Порушення автентичності	Підміна або клонування IoT-пристроїв
Порушення цілісності	Модифікація даних під час передавання
Порушення доступності	DDoS-атаки, виснаження ресурсів
Порушення конфіденційності	Перехоплення та аналіз трафіку
Компрометація прошивки	Встановлення шкідливого програмного коду

Аналіз загроз свідчить, що традиційні централізовані механізми безпеки не забезпечують достатнього рівня стійкості в IoT-середовищах. Вони формують єдині точки відмови, не масштабуються пропорційно кількості пристроїв і не гарантують незмінність журналів подій. Унаслідок цього виникає потреба у децентралізованих моделях довіри, здатних забезпечити незалежну верифікацію дій кожного вузла системи.

Таким чином, теоретичні основи безпеки IoT визначають необхідність переходу від централізованих архітектур до розподілених підходів, що поєднують криптографічну ідентифікацію, контроль доступу та надійне журналювання подій.

1.3. Блокчейн-технології та їх застосування для забезпечення безпеки IoT-пристроїв

Сучасні вимоги до безпеки IoT-систем зумовлюють необхідність використання децентралізованих підходів, здатних усунути залежність від єдиного

центру керування та забезпечити незалежну перевірку дій усіх учасників системи. Однією з таких технологій є блокчейн, який реалізує розподілений незмінний реєстр подій із криптографічним захистом та механізмами колективної валідації.

Блокчейн представляє собою послідовність блоків, кожен з яких містить набір транзакцій і криптографічний хеш попереднього блоку. Така структура забезпечує незмінність історії подій, оскільки будь-яка спроба модифікації даних призводить до порушення цілісності всього ланцюга. Для IoT-систем це означає можливість надійного фіксування дій пристроїв, результатів вимірювань, команд керування та подій безпеки.

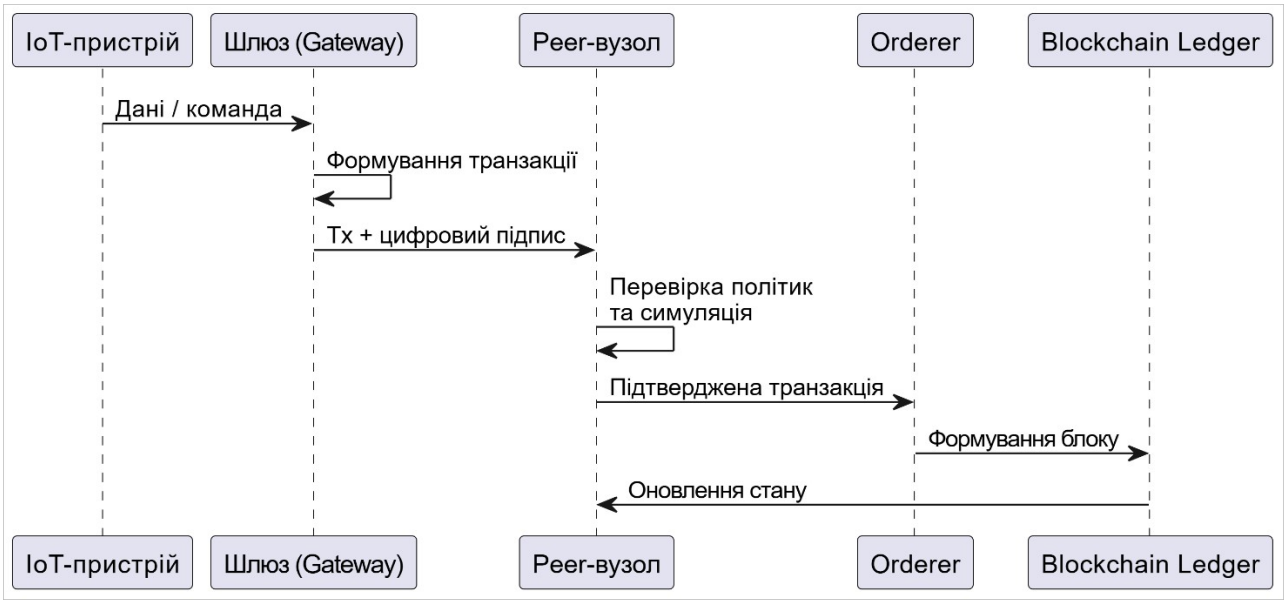

Рис 1.1 - Взаємодії IoT-пристрою з блокчейн-мережею

Незважаючи на очевидні переваги, публічні блокчейн-платформи (Bitcoin, Ethereum) мають суттєві обмеження щодо застосування в IoT-середовищах. Вони характеризуються високими затримками, значними витратами обчислювальних ресурсів та відсутністю контролю над учасниками мережі. Крім того, публічний характер таких мереж не дозволяє забезпечити конфіденційність даних, що є критичним для промислових та інфраструктурних IoT-систем.

У зв’язку з цим у практичних реалізаціях все частіше застосовуються **дозволені (permissioned) блокчейн-платформи**, у яких кожен учасник має підтверджену ідентичність, а правила доступу визначаються політиками мережі.

Hyperledger Fabric є корпоративною блокчейн-платформою, орієнтованою на побудову приватних та консорціумних мереж. Її архітектура базується на чіткому розмежуванні ролей учасників, гнучких політиках доступу та підтримці модульного консенсусу. Це робить Fabric придатною для інтеграції з IoT-системами, де необхідно забезпечити контроль доступу, масштабованість та високу продуктивність.

Ключовим елементом Fabric є **служба керування ідентичністю (MSP)**, яка реалізує автентифікацію учасників на основі цифрових сертифікатів. Для IoT це дозволяє кожному пристрою або шлюзу мати унікальну криптографічну ідентичність, що унеможливлює підміну або несанкціоновану реєстрацію вузлів.

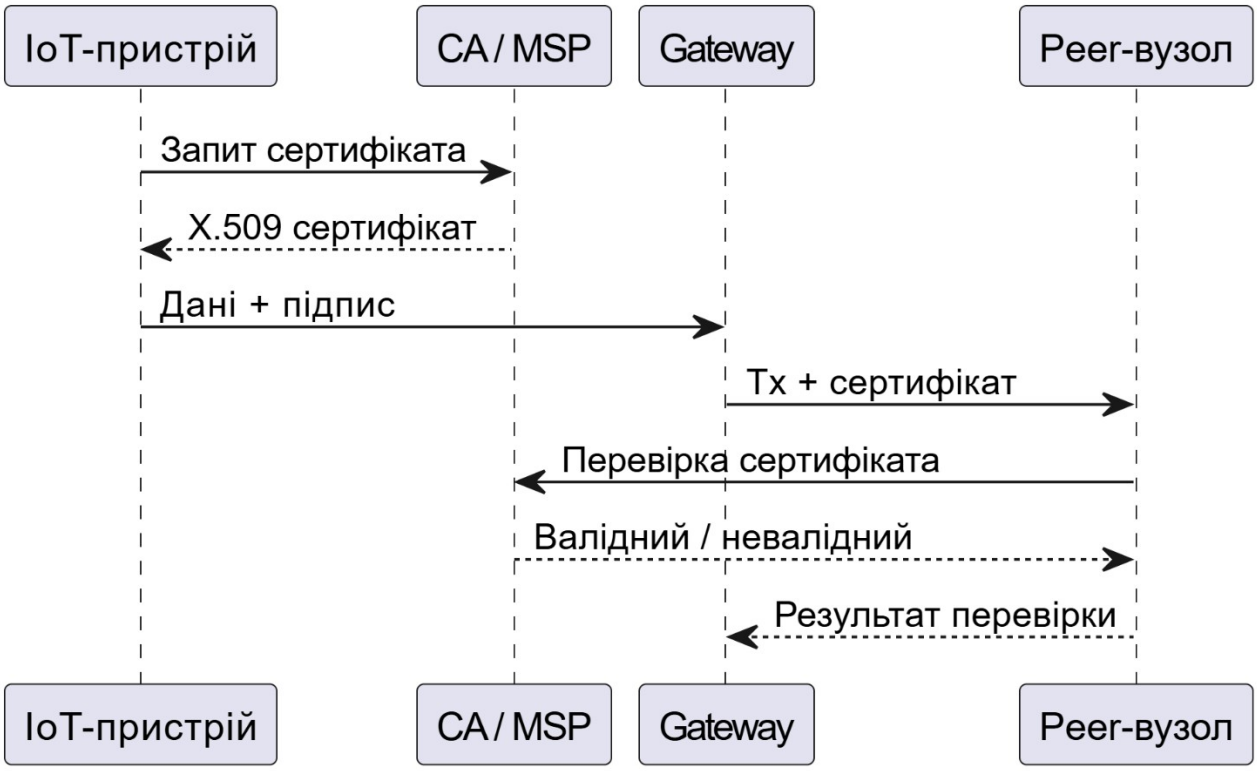

Рис 1.2 UML-діаграму автентифікації IoT-пристрою в Hyperledger Fabric

Однією з ключових переваг Hyperledger Fabric є підтримка гнучких механізмів контролю доступу, зокрема списків ACL та атрибутивної моделі доступу (ABAC). Це дозволяє визначати дозволені дії пристроїв залежно від їх ролі, контексту та стану системи. У результаті навіть скомпрометований пристрій не зможе виконати операції, що виходять за межі встановлених політик.

Фіксація подій у блокчейні забезпечує невідмовність та трасованість дій. Кожна транзакція підписується криптографічно та підтверджується визначеною множиною вузлів відповідно до політики ендорсменту. Формально умову коректності транзакції можна подати у вигляді:

$$Sig(t) \supseteq E(t)$$

де (E(t)) - множина обов'язкових підтверджень, а (Sig(t)) - множина отриманих цифрових підписів.

Таблиця 2.2 Переваги використання блокчейну в IoT

Характеристика	Значення для IoT
Децентралізація	Відсутність єдиної точки відмови
Незмінність даних	Захист журналів подій
Контроль доступу	Формалізовані політики дій
Трасованість	Аудит дій пристроїв
Масштабованість	Підтримка великих мереж

Таким чином, блокчейн-технології, а зокрема платформа Hyperledger Fabric, створюють надійне підґрунтя для побудови систем захисту IoT-пристроїв. Поєднання децентралізованої моделі довіри, криптографічної автентифікації та незмінного журналювання дозволяє усунути ключові недоліки традиційних підходів до безпеки IoT та забезпечити високий рівень стійкості системи до зовнішніх і внутрішніх загроз.

Висновки до розділу 1

У першому розділі було розглянуто фундаментальні поняття Інтернету речей, проаналізовано основні архітектури побудови IoT-систем та окреслено ключові загрози, притаманні таким середовищам. Показано, що децентралізований характер пристроїв, їх обмежені обчислювальні можливості та залежність від мережевої інфраструктури формують широкий спектр вразливостей - від несанкціонованого доступу й підміни пристроїв до порушення цілісності даних та маніпулювання потоками телеметрії. Проведений огляд моделей автентифікації, авторизації та контролю доступу свідчить, що традиційні засоби кіберзахисту не забезпечують належного рівня довіри у розподіленому середовищі.

У цьому контексті було обґрунтовано необхідність використання блокчейн-орієнтованих підходів для підвищення безпеки IoT-екосистем. Технології розподілених реєстрів забезпечують незмінність журналу подій, верифікованість кожної транзакції та можливість організувати децентралізоване управління довірою між пристроями та сервісами. Таким чином, результати першого розділу створюють концептуальне підґрунтя для подальшого аналізу блокчейн-платформ та розробки моделі системи захисту IoT-пристроїв, що реалізується у наступних розділах роботи.

2. Аналіз блокчейн-платформ та обґрунтування вибору Hyperledger Fabric для захисту IoT-пристроїв

2.1. Підходи до побудови системи захисту IoT-пристроїв: архітектурні та концептуальні основи

Проєктування системи захисту IoT-пристроїв вимагає комплексного архітектурного підходу, що враховує децентралізований характер взаємодії вузлів, автономність функціонування пристроїв та їхню апаратну й програмну різнорідність. На відміну від класичних інформаційних систем, де безпека здебільшого реалізується централізовано, IoT-середовище характеризується відсутністю єдиного контрольного центру та високою динамікою мережі, що унеможливлює застосування традиційних моделей управління доступом без істотної модифікації. У таких умовах ефективна система захисту повинна розподіляти функції безпеки між кількома рівнями архітектури, забезпечуючи баланс між обмеженими ресурсами пристроїв та вимогами до надійності й масштабованості.

Архітектурна модель захисту IoT зазвичай формується як багаторівнева структура, у якій кожен рівень виконує строго визначений набір функцій. На рівні IoT-пристроїв реалізуються лише базові механізми ідентифікації та захищеного обміну даними, оскільки обчислювальні та енергетичні ресурси таких вузлів є обмеженими. Пристрої формують підписані повідомлення та передають їх до шлюзів, не виконуючи складних операцій перевірки політик або аналізу ризиків. Це дозволяє мінімізувати навантаження на сенсори та виконавчі модулі, зберігаючи при цьому можливість однозначного встановлення джерела кожної дії.

Шлюзи та edge-вузли виконують роль проміжного рівня, на якому зосереджується значна частина логіки безпеки. Вони здійснюють агрегацію та попередню валідацію даних, фільтрацію аномальної активності, формування транзакцій та підготовку їх до подальшої обробки у розподіленій інфраструктурі

довіри. Завдяки вищій обчислювальній потужності шлюзи можуть виконувати статистичний аналіз поведінки пристроїв, оцінювати ризики та приймати попередні рішення щодо допустимості дій. Використання edge-обчислень знижує затримки обробки подій та зменшує навантаження на мережу, оскільки у блокчейн передаються лише ті події, які мають значення з точки зору безпеки або аудиту.

Ключовим елементом сучасної архітектури захисту IoT є рівень розподіленої інфраструктури довіри, який забезпечує незмінність журналів подій, колективну валідацію операцій та формалізований контроль доступу. Реалізація цього рівня на основі дозволених блокчейн-платформ дозволяє усунути єдині точки відмови та забезпечити стійкість системи навіть у разі компрометації окремих вузлів. Усі критичні дії пристроїв, включаючи передавання даних, виконання команд і зміни конфігурації, фіксуються у розподіленому реєстрі та підтверджуються відповідно до заздалегідь визначених політик. Такий підхід створює можливість незалежної перевірки кожної операції та значно підвищує прозорість функціонування системи.

Концептуально побудова системи захисту IoT ґрунтується на принципі мінімальної довіри, відповідно до якого жоден пристрій або компонент інфраструктури не вважається довіреним за замовчуванням. Кожна дія перевіряється з урахуванням ролі пристрою, контексту взаємодії та його попередньої поведінки. Такий підхід дозволяє обмежити наслідки компрометації окремих вузлів і запобігти поширенню атаки на всю систему. Додатково застосовується принцип розмежування відповідальності, за яким жоден окремий компонент не має повного контролю над усією інфраструктурою безпеки, що знижує ризики внутрішніх загроз.

Важливою складовою архітектурних підходів є забезпечення масштабованості системи захисту. IoT-мережі природно зростають з часом, тому система безпеки повинна підтримувати динамічне додавання нових пристроїв і організацій без необхідності повної реконфігурації. Розподілені моделі керування ідентичностями та політиками доступу дозволяють реєструвати, оновлювати або

відкликати пристрої незалежно від інших компонентів системи, зберігаючи цілісність і узгодженість глобального стану.

Таким чином, архітектурні та концептуальні підходи до побудови системи захисту IoT-пристроїв передбачають поєднання багаторівневої структури, розподіленої моделі довіри та принципів мінімальної довіри й масштабованості. Така інтегрована архітектура створює основу для впровадження блокчейн-орієнтованих механізмів безпеки, здатних забезпечити контроль дій пристроїв, стійкість до атак і можливість повноцінного аудиту, що є необхідним для функціонування сучасних IoT-систем у критичних та промислових середовищах.

2.2. Порівняльний аналіз блокчейн-платформ для забезпечення безпеки IoT-пристроїв

Застосування блокчейн-технологій для захисту IoT-пристроїв потребує обґрунтованого вибору платформи, оскільки різні блокчейн-рішення суттєво відрізняються за архітектурою, механізмами консенсусу, рівнем конфіденційності та вимогами до обчислювальних ресурсів. IoT-середовище висуває специфічні вимоги до блокчейн-платформи, зокрема високу пропускну здатність, низьку затримку обробки транзакцій, можливість контролю учасників мережі та підтримку гнучких політик доступу. Тому використання публічних блокчейнів загального призначення у більшості випадків є малопридатним для реальних IoT-систем.

Публічні блокчейн-платформи, такі як Bitcoin та Ethereum, орієнтовані на відкриті децентралізовані середовища з анонімними учасниками та не забезпечують механізмів керування ідентичностями на рівні протоколу. Консенсусні алгоритми, що застосовуються у таких мережах, характеризуються значними часовими затримками та високими обчислювальними витратами, що робить їх непридатними для IoT-систем із великою кількістю транзакцій та вимогами до обробки подій у майже реальному часі. Крім того, публічний характер

зберігання даних у таких мережах унеможливлює використання їх у промислових та інфраструктурних IoT-сценаріях, де конфіденційність інформації є критичною.

Альтернативою публічним блокчейнам є дозволені (permissioned) платформи, які передбачають наявність підтверджених учасників та контроль доступу до мережі. До таких рішень належать Hyperledger Fabric, Corda та Quorum. Їх спільною рисою є орієнтація на корпоративні та міжорганізаційні середовища, де важливими є не анонімність, а керованість, прозорість та відповідність вимогам безпеки. Саме ці характеристики роблять дозволені блокчейни більш придатними для інтеграції з IoT-системами.

Платформа Corda першопочатково орієнтована на фінансові застосування та моделювання двосторонніх транзакцій між учасниками. Вона не використовує класичний ланцюг блоків, а реалізує обмін станами між зацікавленими сторонами. Такий підхід зменшує обсяг переданих даних, однак ускладнює реалізацію глобального журналу подій, що є важливим для аудиту дій IoT-пристроїв. Крім того, модель Corda менш придатна для сценаріїв, у яких необхідно забезпечити колективну валідацію подій великою кількістю учасників.

Платформа Quorum є модифікацією Ethereum з підтримкою приватних транзакцій, однак зберігає значну частину архітектурних обмежень базового протоколу. Зокрема, вона використовує віртуальну машину Ethereum та модель смартконтрактів, що потребує більших обчислювальних ресурсів і не завжди відповідає вимогам IoT-середовищ. Крім того, механізми керування ідентичностями у Quorum не є настільки гнучкими, як у спеціалізованих корпоративних платформах.

Hyperledger Fabric відрізняється від інших рішень модульною архітектурою, яка дозволяє незалежно налаштовувати механізми консенсусу, керування ідентичностями та політики доступу. Fabric використовує детермінований консенсус, що забезпечує низькі затримки та високу пропускну здатність, критично важливі для IoT-систем. Наявність служби керування ідентичностями (MSP)

дозволяє кожному учаснику мережі мати перевірену криптографічну ідентичність, а підтримка атрибутивного контролю доступу забезпечує гнучке обмеження дій пристроїв залежно від їх ролі та контексту.

Особливою перевагою Hyperledger Fabric є підтримка приватних каналів та приватних даних, що дозволяє ізолювати інформацію між різними групами учасників у межах однієї мережі. Це є важливим для IoT-систем, у яких взаємодіють пристрої різних організацій або підсистем з різними рівнями доступу. Крім того, розмежування етапів симуляції, ендорсменту та впорядкування транзакцій дозволяє зменшити навантаження на мережу та оптимізувати процес обробки подій.

Таблиця 2.1 Порівняльні характеристики блокчейн-платформ для IoT

Платформа	Консенсус	Приватність	Підтримка смарт-контрактів
Hyperledger Fabric	RAFT / PBFT	✔ дозвільна мережа	✔ Chaincode
Ethereum	PoS	✘ публічна	✔ Solidity
IOTA	DAG (Tangle)	умовна	обмежена
Polygon	PoS	✘ публічна	✔ Solidity
Corda	Notary-based	✔ приватна	✔ (flows, contracts)

Таким чином, результати порівняльного аналізу свідчать, що Hyperledger Fabric найбільш повно відповідає вимогам IoT-систем з точки зору безпеки, масштабованості та керованості. Поєднання дозволеної моделі доступу, гнучких політик контролю, підтримки приватних каналів і високої продуктивності робить цю платформу оптимальною технологічною основою для побудови системи захисту IoT-пристроїв.

2.3. Концептуальна модель системи захисту IoT-пристроїв на основі Hyperledger Fabric

Концептуальна модель системи захисту IoT-пристроїв на основі Hyperledger Fabric формується з урахуванням архітектурних особливостей IoT-середовищ, вимог до децентралізованої довіри та необхідності забезпечення контролю дій пристроїв у розподіленій мережі. Основною ідеєю моделі є перенесення критичних функцій безпеки з централізованих компонентів у дозволену блокчейн-інфраструктуру, яка забезпечує незмінність журналів подій, формалізовану автентифікацію та колективну валідацію транзакцій.

Рис 2.3 Концептуальна модель системи захисту IoT-пристроїв на основі Hyperledger Fabric

У межах запропонованої концепції IoT-пристрої розглядаються як автономні джерела подій, які не взаємодіють із блокчейном безпосередньо, а передають дані через шлюзи. Такий підхід дозволяє врахувати обмежені обчислювальні ресурси пристроїв та зменшити накладні витрати на криптографічні операції. Кожен пристрій має унікальну криптографічну ідентичність, пов’язану з цифровим сертифікатом, що використовується для формування підписаних повідомлень. Шлюз виконує функції агрегатора, перевіряє коректність форматів даних, здійснює

попередню оцінку поведінки пристрою та формує транзакції для подальшої обробки у блокчейн-мережі.

Hyperledger Fabric у даній моделі виступає як розподілена інфраструктура довіри, у межах якої реалізується керування ідентичностями, контроль доступу та фіксація подій. Служба керування ідентичностями забезпечує перевірку сертифікатів учасників та однозначну прив'язку кожної транзакції до конкретного суб'єкта. Це дозволяє унеможливити анонімні дії в системі та створює основу для подальшого аудиту. Політики ендорсменту визначають, які вузли повинні підтвердити транзакцію, перш ніж вона буде зафіксована у розподіленому реєстрі, що забезпечує колективну відповідальність і знижує ризик маніпуляцій.

Центральним елементом концептуальної моделі є смартконтракти (chaincode), які інкапсулюють логіку безпеки системи. У межах chaincode визначаються правила допустимих дій пристроїв, умови доступу до ресурсів, а також механізми фіксації та перевірки подій. Завдяки розміщенню цих правил у блокчейні досягається їх незмінність і незалежність від окремих компонентів інфраструктури. Будь-яка спроба змінити логіку контролю доступу або обійти встановлені обмеження потребує узгоджених дій учасників мережі, що істотно підвищує рівень захищеності системи.

Запропонована модель також передбачає інтеграцію механізмів оцінки ризику та виявлення аномальної поведінки пристроїв. Дані про транзакційну активність, частоту звернень та типи виконуваних операцій накопичуються у розподіленому реєстрі та використовуються для формування поведінкових профілів. У разі виявлення відхилень від нормальної поведінки система може автоматично обмежувати доступ пристрою або переводити його у режим підвищеного контролю. Такий підхід дозволяє поєднати формальні криптографічні механізми з адаптивними методами реагування на загрози.

Важливою особливістю концептуальної моделі є підтримка масштабованості та міжорганізаційної взаємодії. Використання приватних каналів і механізмів

ізоляції даних дозволяє розмежовувати інформаційні потоки між різними групами учасників, не створюючи окремих блокчейн-мереж для кожного сценарію. Це є критичним для IoT-систем, у яких взаємодіють пристрої різних виробників, операторів або підсистем із різними рівнями довіри та відповідальності.

Таким чином, концептуальна модель системи захисту IoT-пристроїв на основі Hyperledger Fabric поєднує багаторівневу архітектуру, дозволену блокчейн-інфраструктуру та формалізовану логіку безпеки, реалізовану у смартконтрактах. Такий підхід забезпечує контроль дій пристроїв, незмінність журналів подій, можливість аудиту та адаптивне реагування на загрози. Сформована концепція створює логічну основу для подальшого проєктування та практичного моделювання системи захисту, що реалізується у третьому розділі роботи.

Висновки до розділу 2

У другому розділі було здійснено системний аналіз сучасних підходів до захисту IoT-систем та порівняно можливості різних блокчейн-платформ щодо їх застосування у сфері Інтернету речей. Показано, що традиційні централізовані моделі не забезпечують достатнього рівня стійкості до атак, масштабованості та прозорості, що є критично важливими характеристиками для середовищ із великою кількістю взаємодіючих пристроїв. Проведене порівняння технологій продемонструвало, що блокчейн-платформи з дозволеним доступом, зокрема Hyperledger Fabric, найбільш повно відповідають вимогам IoT завдяки гнучким механізмам управління доступом, розподіленій архітектурі та здатності забезпечувати цілісність і автентичність даних.

На основі отриманих результатів було обґрунтовано вибір Hyperledger Fabric як платформи для побудови системи захисту IoT-пристроїв. Сформована у підрозділі 2.3 концептуальна модель демонструє, що Fabric дозволяє інтегрувати криптографічні механізми, політики доступу, смартконтракти та сегментацію даних у єдину архітектуру безпеки. Це створює необхідне теоретичне підґрунтя для

розробки практичної реалізації системи, що буде детально представлено у наступному розділі.

3. Проєктування та моделювання системи захисту IoT-пристроїв на основі Hyperledger Fabric

3.1. Архітектура розробленої системи захисту IoT-пристроїв

Архітектура розробленої системи захисту IoT-пристроїв ґрунтується на концептуальній моделі, сформованій у попередньому розділі, та орієнтована на практичну реалізацію механізмів децентралізованої довіри, контролю доступу й незмінного журналювання подій. Основною метою архітектурного проєктування є створення такої структури системи, у межах якої забезпечується захищена взаємодія між IoT-пристроями, шлюзами та блокчейн-інфраструктурою без перевантаження малопотужних вузлів і без формування єдиних точок відмови.

Розроблена архітектура має багаторівневу організацію, у якій IoT-пристрої виконують роль джерел подій, шлюзи – роль посередників і агрегаторів, а блокчейн-мережа Hyperledger Fabric – роль розподіленої інфраструктури довіри. IoT-пристрої не взаємодіють із блокчейном безпосередньо, що зумовлено їх обмеженими обчислювальними ресурсами та енергетичними можливостями. Натомість кожен пристрій формує підписані повідомлення, які містять дані вимірювань або запити на виконання дій, і передає їх на шлюз через захищений канал зв’язку. Такий підхід дозволяє зберегти криптографічну прив’язку даних до конкретного пристрою, не ускладнюючи його внутрішню логіку.

Шлюз у розробленій архітектурі є ключовим елементом, що забезпечує перехід від фізичного рівня IoT до логічного рівня блокчейн-мережі. Він виконує попередню валідацію отриманих повідомлень, перевіряє коректність підписів, аналізує базові поведінкові характеристики пристроїв і формує транзакції для подальшої обробки у Hyperledger Fabric. Завдяки цьому зменшується кількість некоректних або повторюваних транзакцій, що передаються у блокчейн, а також знижується навантаження на мережу та вузли-валідатори. Крім того, шлюз може виконувати функції тимчасового буферування даних у разі нестабільного з’єднання з блокчейн-інфраструктурою, що підвищує загальну стійкість системи.

Блокчейн-мережа Hyperledger Fabric у межах архітектури реалізує функції автентифікації учасників, колективної валідації транзакцій та незмінного зберігання подій. Кожен компонент мережі, включаючи peer-вузли та сервіс упорядкування, має підтверджену ідентичність, що забезпечується службою керування ідентичностями. Це дозволяє однозначно встановити джерело кожної транзакції та виключити анонімні або неавторизовані дії. Процес обробки транзакцій у Fabric розділений на етапи симуляції, ендорсменту та фіксації у реєстрі, що забезпечує високу продуктивність і детермінованість виконання операцій.

Логіка безпеки системи реалізується у смартконтрактах, які визначають правила доступу пристроїв до функціональних можливостей системи, допустимі типи операцій та умови їх виконання. У межах розробленої архітектури смартконтракти відповідають не лише за фіксацію подій, але й за застосування політик контролю доступу та перевірку контексту виконання дій. Завдяки розміщенню цієї логіки у блокчейн-мережі досягається її незмінність і стійкість до несанкціонованих змін, що є критичним для систем безпеки.

Окрему роль в архітектурі відіграє база станів блокчейну, яка зберігає актуальну інформацію про пристрої, їхній статус, історію взаємодій та результати перевірок. Доступ до цих даних здійснюється відповідно до визначених політик, що дозволяє використовувати їх як для оперативного прийняття рішень, так і для подальшого аудиту. У разі виявлення аномальної активності або перевищення допустимого рівня ризику архітектура передбачає можливість автоматичного обмеження функціональних можливостей пристрою або блокування його взаємодії з системою.

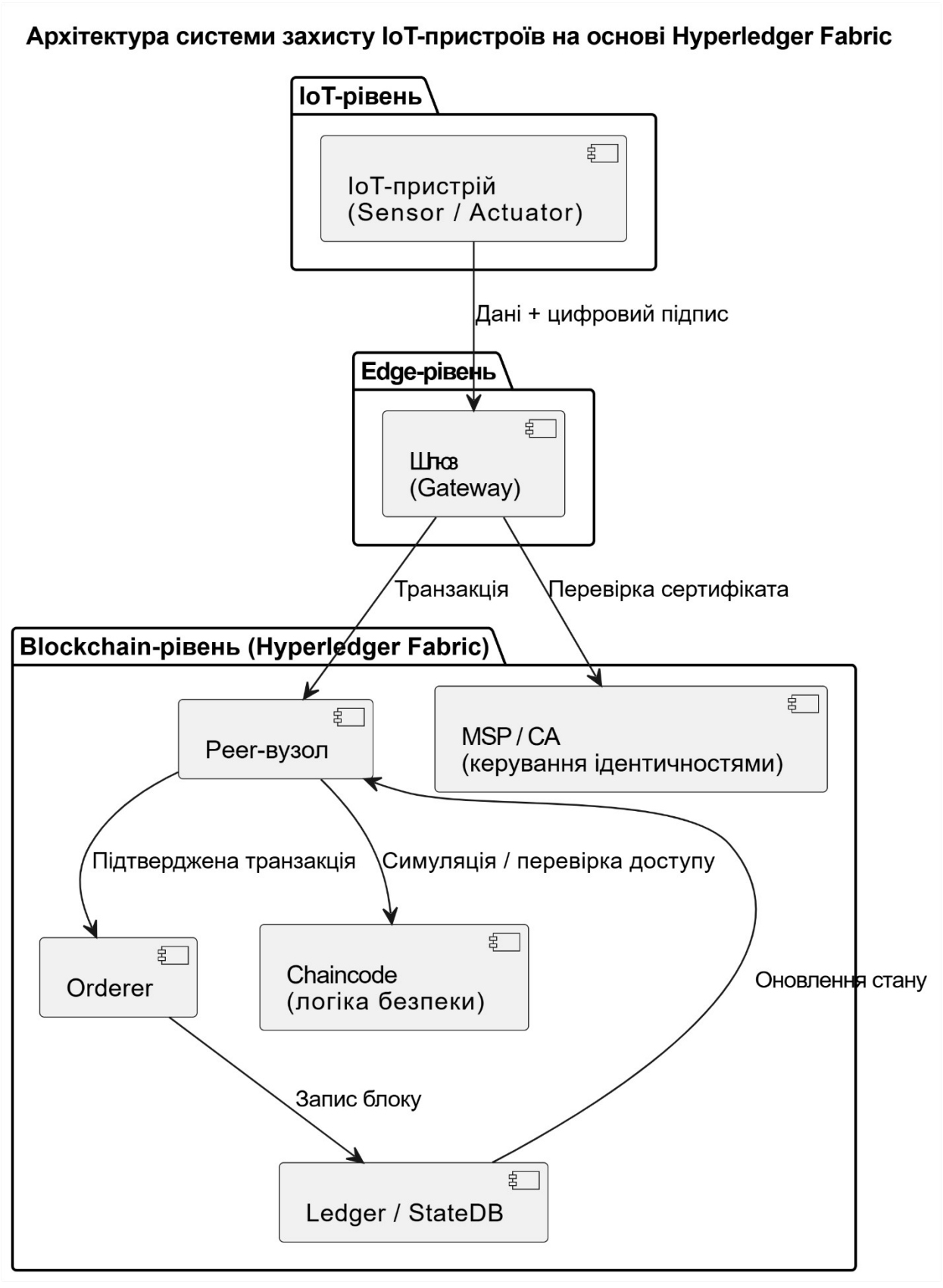

Рис 3.1 Архітектура розробленої системи захисту IoT-пристроїв на основі Hyperledger Fabric

3.2. Реалізація механізмів автентифікації, авторизації та контролю доступу в системі захисту IoT-пристроїв на основі Hyperledger Fabric

Реалізація механізмів автентифікації, авторизації та контролю доступу в розробленій системі захисту IoT-пристроїв базується на можливостях платформи Hyperledger Fabric та її моделі керування ідентичностями. Ключовою особливістю даного підходу є відмова від анонімних або спрощених схем доступу на користь формалізованої криптографічної ідентифікації кожного учасника системи. Це дозволяє забезпечити однозначну прив’язку будь-якої дії до конкретного пристрою або сервісу та створює основу для подальшого аудиту й аналізу безпеки.

Автентифікація у системі реалізується за допомогою інфраструктури відкритих ключів, інтегрованої в Hyperledger Fabric через службу керування ідентичностями. Кожному IoT-пристрою або шлюзу на етапі реєстрації видається цифровий сертифікат, який підтверджує його належність до певної організації та визначає базові атрибути доступу. Під час взаємодії з системою пристрій формує криптографічний підпис для кожного повідомлення, що дозволяє перевірити його автентичність ще до обробки даних у блокчейн-мережі. Завдяки цьому унеможливлюється підміна пристроїв та використання неавторизованих вузлів у системі.

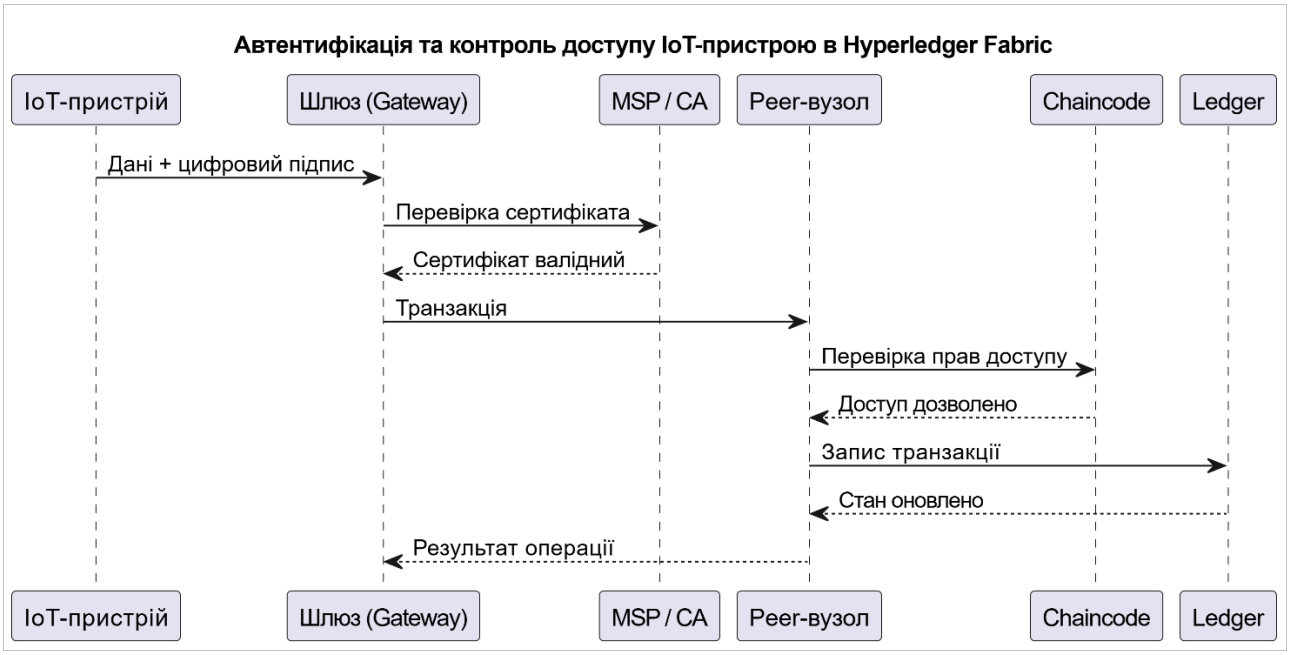

Рис 3.2 Процес автентифікації, авторизації та контролю доступу IoT-пристрою

Процес авторизації тісно пов’язаний з автентифікацією та реалізується на основі політик доступу, визначених у Fabric. На відміну від традиційних систем, де рішення про доступ приймається централізованим сервером, у даній архітектурі авторизація є частиною логіки блокчейн-мережі. Після перевірки сертифіката учасника система визначає, чи має він право ініціювати конкретний тип транзакції або виконувати певні дії. Це дозволяє гнучко обмежувати функціональні можливості пристроїв залежно від їх ролі, призначення та контексту взаємодії.

Контроль доступу у розробленій системі реалізується шляхом поєднання атрибутивної моделі доступу та політик ендорсменту. Атрибути, закладені у сертифікатах учасників, використовуються для визначення дозволених операцій на рівні смартконтрактів. Таким чином, логіка доступу переноситься безпосередньо у chaincode, де кожна транзакція перевіряється на відповідність встановленим правилам. Це дозволяє виключити можливість обходу політик доступу через зовнішні компоненти або помилки конфігурації окремих вузлів.

Політики ендорсменту доповнюють механізми контролю доступу, забезпечуючи колективну перевірку транзакцій. У межах системи визначається

множина вузлів, підтвердження яких є обов’язковим для визнання операції коректною. Такий підхід гарантує, що жоден окремий учасник мережі не може одноосібно схвалити або відхилити транзакцію, що є особливо важливим у міжорганізаційних IoT-системах. Навіть у разі компрометації одного з вузлів зловмисник не отримує можливості змінити стан системи без погодження з іншими учасниками.

Розроблена система також передбачає динамічний контроль доступу на основі поведінкових характеристик пристроїв. Інформація про транзакційну активність, частоту звернень та історію порушень накопичується у розподіленому реєстрі та використовується для оцінки поточного рівня ризику. У разі виявлення підозрілої або аномальної поведінки система може автоматично знизити рівень доступу пристрою або повністю заблокувати виконання критичних операцій. Такий механізм дозволяє адаптувати політики безпеки до поточного стану системи та реагувати на загрози в режимі, наближеному до реального часу.

Завдяки інтеграції механізмів автентифікації, авторизації та контролю доступу у блокчейн-інфраструктуру досягається високий рівень узгодженості та прозорості процесів безпеки. Усі рішення щодо доступу фіксуються у незмінному журналі подій, що дозволяє відстежувати еволюцію прав пристроїв та аналізувати причини обмежень або блокувань. Такий підхід не лише підвищує рівень захищеності IoT-системи, але й спрощує проведення аудиту та розслідування інцидентів.

Таким чином, реалізація механізмів автентифікації, авторизації та контролю доступу на основі Hyperledger Fabric забезпечує формалізований і стійкий до атак підхід до керування взаємодією IoT-пристроїв. Запропоноване рішення поєднує криптографічну ідентифікацію, політики доступу та колективну валідацію дій, створюючи надійну основу для практичної моделі роботи системи

3.3. Практична модель роботи системи захисту IoT-пристроїв на основі Hyperledger Fabric

Для формального опису функціонування розробленої системи захисту IoT-пристроїв побудуємо математичну модель, яка охоплює всі етапи життєвого циклу події - від її генерації пристроєм до прийняття рішення щодо зміни стану системи та статусу пристрою. Модель базується на поєднанні формалізованих політик доступу, механізмів ендорсменту Hyperledger Fabric та динамічної оцінки ризику поведінки пристроїв.

На початковому етапі визначимо множини базових об'єктів системи. Нехай $D=\{d_1, d_2, \ldots, d_n^D\}$ - множина IoT-пристроїв, що функціонують у системі, де кожен елемент d_i представляє окремий фізичний або віртуальний пристрій. Взаємодія пристроїв з блокчейн-мережею здійснюється через множину шлюзів $G=\{g_1, g_2, \ldots, g_n^G\}$, які виконують функції проміжної обробки, перевірки та формування транзакцій. Блокчейн-інфраструктура Hyperledger Fabric описується множиною peer-вузлів $P=\{p_1, p_2, \ldots, p_n^P\}$, які виконують смартконтракти, здійснюють ендорсмент транзакцій та зберігають розподілений реєстр.

Кожен IoT-пристрій має цифровий сертифікат cert(d_i), виданий службою керування ідентичностями, а також набір атрибутів $attr(d_i) \subseteq A$, де A - множина можливих атрибутів. Ці атрибути використовуються для реалізації атрибутивного контролю доступу та визначення дозволених операцій.

Подія, згенерована пристроєм, формалізується як кортеж

$$e=(d_i, op, data, t),$$

де d_i- джерело події, op - тип операції, data - корисні дані, t - момент часу. Подія не може бути безпосередньо оброблена блокчейн-мережею і тому на рівні шлюзу перетворюється у транзакцію

$$T=(e, meta, Sig_g)$$

де meta - службова інформація Fabric, а Sig_g - цифровий підпис шлюзу, що гарантує цілісність і автентичність сформованої транзакції.

Перед виконанням транзакції в мережі Fabric застосовується політика дозволу операції

$$Allow(d_i, op, attr(d_i), t) \in \{0,1\}$$

яка визначає, чи має пристрій право виконувати відповідну дію з урахуванням атрибутів і контексту. Паралельно перевіряється політика ендорсменту, яка задає множину обов'язкових вузлів-підтверджувачів $E(T) \subseteq P$ Транзакція вважається валідною лише за умови

$$Sig(T) \supseteq E(T)$$

де *Sig*(T)- множина фактичних ендорсерів транзакції.

Стан системи в момент часу (t) описується множиною станів усіх пристроїв

$$S(t)=\{s_{d_1}(t), s_{d_2}(t), \ldots, s_{d_{n_0}}(t)\}$$

де стан окремого пристрою задається трійкою

$$s_{d_i}(t) = (\ status_{d_i}(t),\ risk_{d_i}(t),\ last_{td_i}(t)\ )$$

Зміна стану системи описується функцією переходу

$$S(t+1)=\delta(S(t), T)$$

яка оновлює параметри пристрою у разі прийняття транзакції або коригує рівень ризику у випадку її відхилення.

Для оцінювання поведінки пристроїв вводиться поведінковий вектор

$$X_{d_i}(t)$$

що включає частоту операцій, типи команд, кількість відмов та інші характеристики. На його основі визначається функція виявлення аномалій

$$A_{d_i}(t) \in \{0,1\}$$

де значення 1 відповідає аномальній поведінці. Поточний рівень ризику визначається функцією

$$risk_{d_i}(t) \in [0,1]$$

а його динаміка описується співвідношенням

$$risk_{d_i}(t+1) = \{$$

$$risk_{d_i}(t) + \alpha, A_{d_i}(t) = 1$$

$$risk_{d_i}(t) - \beta, A_{d_i}(t) = 0$$

$$\}$$

де α та β - коефіцієнти зростання та згасання ризику.

Для визначення реакції системи вводяться порогові значення

$$\theta_1 < \theta_2 < \theta_3$$

які визначають рівні критичності поведінки IoT-пристрою залежно від поточного значення функції ризику $risk_{d_i}(t)$. На основі порівняння значення ризику з відповідними порогами формується рівень реагування системи $level_{d_i}(t)$, що відображає ступінь небезпеки поточної поведінки пристрою.

Зокрема, якщо $risk_{d_i}(t) < \theta_1$, рівень реагування вважається мінімальним, і пристрій функціонує у штатному режимі. У випадку, коли $\theta_{d_i} \leq risk_{d_i}(t) < \theta_2$, формується попереджувальний рівень реагування, що сигналізує про потенційні відхилення в роботі пристрою. При перевищенні порогу θ_2 система переходить до обмежувального рівня реагування, який передбачає часткове обмеження доступу пристрою до виконання операцій. Якщо ж значення ризику перевищує порогове значення θ_3, поведінка пристрою вважається критично небезпечною, і застосовується повне блокування його активності.

Зміна поточного статусу IoT-пристрою формалізується функцією

$$status_{d_i}(t+1) = g(status_{d_i}(t), level_{d_i}(t))$$

яка визначає правила переходу між станами active, warning, restricted та blocked. Функція g реалізує детермінований механізм зміни стану пристрою залежно від поточного статусу та сформованого рівня реагування. Таким чином, при зростанні рівня ризику відбувається послідовний перехід пристрою до більш обмежувальних станів, тоді як зниження ризику нижче відповідних порогових значень дозволяє повернення до менш критичних станів.

Графічною інтерпретацією функції g є діаграма станів UML, у якій кожен стан відповідає можливому значенню статусу IoT-пристрою, а переходи між станами визначаються умовами, що базуються на порівнянні значення ризику з пороговими величинами θ_1, θ_2, θ_3 Такий підхід забезпечує наочне відображення математичної моделі та підтверджує її узгодженість із реалізацією системи.

Таким чином, запропонована математична модель повністю описує процес функціонування системи захисту IoT-пристроїв: від генерації події та її формалізації у транзакцію до прийняття рішення щодо дозволу операції, оновлення глобального стану системи та зміни статусу пристрою. Поєднання механізмів Hyperledger Fabric із динамічною моделлю ризику забезпечує адаптивний, формалізований та стійкий до атак підхід до безпеки IoT-систем. Вся математична модель має ось такий вигляд:

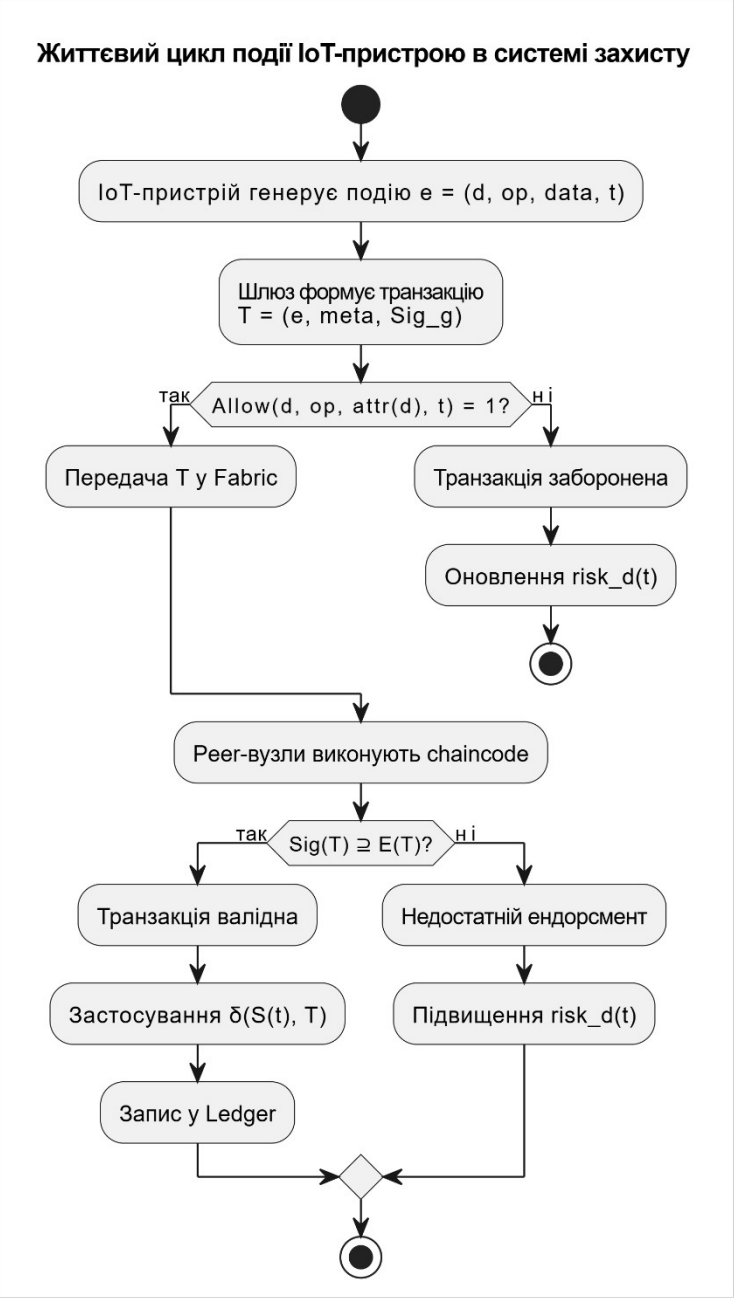

Рис 3.3 Життєвий цикл події IoT-пристрою в системі захисту

Висновок

У магістерській роботі було проведено комплексне дослідження проблем захисту IoT-пристроїв та розроблено модель системи безпеки, що базується на технології розподілених реєстрів Hyperledger Fabric. На основі аналізу сучасних загроз, вразливостей та недоліків централізованих моделей управління IoT було

доведено, що блокчейн-платформи надають низку унікальних переваг для побудови надійної, масштабованої та децентралізованої інфраструктури.

Здійснено аналіз існуючих платформ та протоколів, проведено порівняння Hyperledger Fabric з іншими блокчейн-рішеннями, визначено його технічні особливості, механізми безпеки та можливості застосування у контексті Інтернету речей. Це дозволило сформувати обґрунтований вибір технології та визначити її як оптимальну для реалізації вимог до захисту IoT-середовищ.

Було розроблено архітектуру системи, описано моделі взаємодії між пристроями, шлюзами та компонентами Fabric, створено математичні формалізації процесів авторизації, обробки транзакцій і виявлення аномалій. Запропонована система включає декілька рівнів захисту - криптографічний, логічний, поведінковий та організаційний, що значно підвищує загальну стійкість до атак та збоїв.

Особливу увагу приділено розробці алгоритмів реагування на інциденти, таблиць ризиків, формальних моделей доступу та механізмів сегментації даних, що забезпечує практичну реалізованість запропонованої моделі. У роботі також показано, що інтеграція IoT з Hyperledger Fabric дає змогу створити систему, у якій усі події верифікуються незалежними вузлами, а історія дій залишається незмінною та доступною для аудиту.

Узагальнюючи проведене дослідження, можна зробити висновок, що запропонована система є не лише теоретично обґрунтованою, а й придатною до реального впровадження. Вона забезпечує високий рівень безпеки, масштабованість і адаптивність, що робить її перспективним рішенням для захисту сучасних IoT-інфраструктур.

ПЕРЕЛІК ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1) Androulaki E., Barger A., Bortnikov V. та ін. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. – 2018. arXiv:1801.10228 [Електронний ресурс]. URL: https://arxiv.org/abs/1801.10228 (дата звернення: 05.12.2025).
2) Ali J., Ali T., Musa S., Zahrani A. Towards Secure IoT Communication with Smart Contracts in a Blockchain Infrastructure. – 2020. arXiv:2001.01837 [Електронний ресурс]. URL: https://arxiv.org/abs/2001.01837 (дата звернення: 05.12.2025).
3) Salimitari M., Chatterjee M., Fallah Y. AI-enabled Blockchain: An Outlier-aware Consensus Protocol for Blockchain-based IoT Networks. – 2019. arXiv:1906.08177 [Електронний ресурс]. URL: https://arxiv.org/abs/1906.08177 (дата звернення: 05.12.2025).
4) Saad M., et al. An Efficient Privacy and Anonymity Setup on Hyperledger Fabric for IoT Devices. *Electronics*. – 2024. – 13(13):2652 [Електронний ресурс]. URL: https://www.mdpi.com/2079-9292/13/13/2652 (дата звернення: 05.12.2025).
5) Chen C.L., et al. Secure State Sharing and Intelligent Reconfiguration for Edge-enabled IIoT: A Hyperledger Fabric Approach. – 2022. PMC8839262 [Електронний ресурс]. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC8839262/ (дата звернення: 05.12.2025).
6) Hyperledger Fabric – офіційна документація. ReadTheDocs [Електронний ресурс]. URL: https://hyperledger-fabric.readthedocs.io/ (дата звернення: 05.12.2025).
7) Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. – 2008 [Електронний ресурс]. URL: https://bitcoin.org/bitcoin.pdf (дата звернення: 05.12.2025).
8) Dorri A., Kanhere S., Jurdak R. Blockchain in Internet of Things: Challenges and Solutions. – 2017. arXiv:1608.05187 [Електронний ресурс]. URL: https://arxiv.org/abs/1608.05187 (дата звернення: 05.12.2025).

9) Christidis K., Devetsikiotis M. Blockchains and Smart Contracts for the Internet of Things. – 2016. IEEE Access [Електронний ресурс]. URL: https://arxiv.org/abs/1608.05187 (дата звернення: 05.12.2025).
10) Reyna A., Martín C., Chen J., Soler E., Díaz M. On blockchain and its integration with IoT. – 2018. *Future Generation Computer Systems* [Електронний ресурс]. URL: https://arxiv.org/abs/1802.04491 (дата звернення: 05.12.2025).
11) Khan M.A., Salah K. IoT security: Review, blockchain solutions. – 2018. *Future Generation Computer Systems* [Електронний ресурс]. URL: https://arxiv.org/abs/1806.08850 (дата звернення: 05.12.2025).
12) Ferrag M.A., et al. Security for IoT-based Smart Cities. – 2018. IEEE Surveys [Електронний ресурс]. URL: https://arxiv.org/abs/1802.04635 (дата звернення: 05.12.2025).
13) Chandola V., Banerjee A., Kumar V. Anomaly Detection: A Survey. – 2009. ACM Computing Surveys [Електронний ресурс]. URL: https://www.cs.umn.edu/~kumar001/dmbook/anomalydetection.pdf
14) Patcha A., Park J.M. An overview of anomaly detection techniques. – 2007. *Computer Networks* [Електронний ресурс]. URL: https://www.cs.ucf.edu/~jpark/papers/AnomalyDetection.pdf
15) Denning D. An Intrusion-Detection Model. – 1987. IEEE [Електронний ресурс]. URL: https://faculty.washington.edu/rjl/classes/cse590q/denning.pdf
16) Sommer R., Paxson V. Outside the Closed World. – 2010 [Електронний ресурс]. URL: https://www.icir.org/vern/papers/closedworld.pdf
17) Ongaro D., Ousterhout J. In Search of an Understandable Consensus Algorithm (Raft). – 2014 [Електронний ресурс]. URL: https://raft.github.io/raft.pdf
18) Castro M., Liskov B. Practical Byzantine Fault Tolerance. – 1999 [Електронний ресурс]. URL: https://pmg.csail.mit.edu/papers/osdi99.pdf

19) Sousa J., Bessani A., Vukolic M. A Byzantine Fault-Tolerant Ordering Service for Hyperledger Fabric. – 2018. arXiv:1709.06921 [Електронний ресурс]. URL: https://arxiv.org/abs/1709.06921

20) Cachin C. Architecture of the Hyperledger Blockchain Fabric. – 2016 [Електронний ресурс]. URL: https://www.zurich.ibm.com/dccl/papers/cachin_dccl.pdf

21) Tanenbaum A., Van Steen M. Distributed Systems: Principles and Paradigms. – 2007 [Електронний ресурс]. URL: https://www.distributed-systems.net/

22) Coulouris G., Dollimore J., Kindberg T., Blair G. Distributed Systems: Concepts and Design. – 2012 [Електронний ресурс]. URL: https://www.distributed-systems.net/index.php/books/

23) Stallings W. Cryptography and Network Security. – 2017 [Електронний ресурс]. URL: https://williamstallings.com/Cryptography/

24) Menezes A., Van Oorschot P., Vanstone S. Handbook of Applied Cryptography. – 1996 [Електронний ресурс]. URL: https://cacr.uwaterloo.ca/hac/

25) Atzori L., Iera A., Morabito G. The Internet of Things: A survey. – 2010. *Computer Networks* [Електронний ресурс]. URL: https://arxiv.org/abs/1006.3231

26) Sicari S., et al. Security, privacy and trust in IoT. – 2015. *Computer Networks* [Електронний ресурс]. URL: https://arxiv.org/abs/1501.04105

27) Roman R., Zhou J., Lopez J. Security challenges in IoT. – 2013 [Електронний ресурс]. URL: https://arxiv.org/abs/1304.0444

28) NIST SP 800-213. Security and Privacy in IoT. – 2021 [Електронний ресурс]. URL: https://csrc.nist.gov/publications/detail/sp/800-213/final

29) NIST SP 800-162. Guide to Attribute Based Access Control. – 2014 [Електронний ресурс].
URL: https://csrc.nist.gov/publications/detail/sp/800-162/final
30) ETSI TS 103 645. Cyber Security for Consumer IoT. – 2020 [Електронний ресурс].
URL: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/
31) ENISA. Baseline Security Recommendations for IoT. – 2017 [Електронний ресурс].
URL: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
32) ISO/IEC 27001:2022 Information Security Management Systems. – 2022 [Електронний ресурс].
URL: https://www.iso.org/standard/82875.html
33) ISO/IEC 27002:2022 Information Security Controls. – 2022 [Електронний ресурс].
URL: https://www.iso.org/standard/75652.html
34) ISO/IEC 29100 Privacy Framework. – 2011 [Електронний ресурс].
URL: https://www.iso.org/standard/45123.html
35) ISO/IEC 15408 Common Criteria. – 2017 [Електронний ресурс].
URL: https://www.commoncriteriaportal.org/
36) OWASP. IoT Top 10 Security Risks. – 2023 [Електронний ресурс].
URL: https://owasp.org/www-project-internet-of-things/
37) Hyperledger Caliper. Blockchain Performance Benchmarking.
URL: https://www.hyperledger.org/use/caliper
38) IBM. Blockchain Security Architecture.
URL: https://www.ibm.com/docs/en/blockchain-platform
39) AWS. Blockchain and IoT Security Documentation.
URL: https://docs.aws.amazon.com/blockchain/
40) Microsoft. Azure Blockchain and IoT Security.
URL: https://learn.microsoft.com/azure/blockchain/

41) World Economic Forum. Blockchain Beyond the Hype. – 2018 [Електронний ресурс].
URL: https://www.weforum.org/reports/blockchain-beyond-the-hype
42) IEEE Internet of Things Journal.
URL: https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6488907
43) IEEE Security & Privacy Magazine.
URL: https://www.computer.org/csdl/magazine/sp
44) Axelsson S. Intrusion Detection Systems: A Survey. – 2000 [Електронний ресурс].
URL: https://www.cse.chalmers.se/~axelsson/publications/axelsson00.pdf
45) National Institute of Standards and Technology. Risk Management Framework.
URL: https://csrc.nist.gov/projects/risk-management-framework

ДОДАТКИ