УДК 004.056 DOI https://doi.org/10.35546/kntu2078-4481.2025.4.3.17

Д. М. НЕХОРОШИХ
асистент кафедри безпеки інформаційних технологій
Харківський національний університет радіоелектроніки
ORCID: 0000-0002-6455-2221

П. В. БУСЛОВ
старший викладач кафедри безпеки інформаційних технологій
Харківський національний університет радіоелектроніки
ORCID: 0000-0002-2558-4984

А. М. ЄВГЕНЬЄВ
старший викладач кафедри безпеки інформаційних технологій
Харківський національний університет радіоелектроніки
ORCID: 0000-0003-4365-5675

М. С. СКИБЕНКО
старший викладач кафедри безпеки інформаційних технологій
Харківський національний університет радіоелектроніки
ORCID: 0009-0002-4838-9329

АНАЛІЗ ФРЕЙМВОРКІВ ТА ТЕХНІЧНИХ ЗАСОБІВ ЗАХИСТУ ДЛЯ ІНФРАСТРУКТУРИ ІНТЕРНЕТУ РОБОТИЗОВАНИХ РЕЧЕЙ

У статті проведено комплексний аналіз архітектурних, організаційних та технологічних засад формування системи управління інформаційною безпекою (СУІБ) для інфраструктури Інтернету роботизованих речей (IoRT) що поєднує можливості IoT та робототехніки й характеризується високим рівнем автономності, масштабованості та критичністю функцій. Розглянуто класифікацію сфер застосування IoRT за суб'єктами використання та галузевими напрямами. На основі вимог стратегічного та оперативного рівнів управління окреслено ключові складові СУІБ для IoRT.

Особливу увагу приділено аналізу адміністративних, фізичних і технічних заходів безпеки, що охоплюють управління ідентифікацією й автентифікацією пристроїв, контроль доступу, безпечну взаємодію з постачальниками, захист апаратури, мережеву сегментацію, криптографічні механізми та безпечний життєвий цикл програмного забезпечення. У контексті впровадження європейської директиви NIS2 наголошено на необхідності інтеграції міжнародних стандартів ISMS (ISO, NIST, ISA) на всіх рівнях архітектури IoRT.

Проведено аналіз сучасних тенденцій розгортання СУІБ, виявлені основні сценарії ризиків, типові загрози та вразливості, які характерні як для IoT, IoRT технологій зокрема так і комплексної інраструктури, що використовує IoT, IoRT кластер, вцілому.

Запропанований підхід застосування декількох фреймворків управління безпекою в рамках однієї разголуженої інфраструктури у відповіднсті з виявленим конеткстом та результатами процеса упроавління ризиками.

Присвячено увагу можливостям і обмеженням використання технології блокчейн для підвищення рівня безпеки IoRT. Проаналізовано етапи інтеграції блокчейну. Водночас підкреслено проблеми масштабованості, затримок обробки та енергоспоживання, що обмежують застосування блокчейну у сценаріях реального часу. Запропоновано гібридний підхід, що передбачає поєднання блокчейну з децентралізованими базами даних для досягнення балансу між продуктивністю та безпекою.

Ключові слова: *IoRT, СУІБ, управління ризиками, загрози, вразливості, інфорамційні активи, блокчейн, децентралізовані системи, інтелектуальні пристрої, екосистема IoT, критична інфраструктура, цифрова безпека.*

D. M. NEKHOROSHYKH
Assistent Professor at the Department of Information Technology Security
Kharkiv National University of Radio Electronics
ORCID: 0000-0002-6455-2221

P. V. BUSLOV
Senior Instructor at the Department of Information Technology Security
Kharkiv National University of Radio Electronics
ORCID: 0000-0002-2558-4984

A. M. YEVHENIEV
Senior Instructor at the Department of Information Technology Security
Kharkiv National University of Radio Electronics
ORCID: 0000-0003-4365-5675

M. S. SKYBENKO
Senior Instructor at the Department of Information Technology Security
Kharkiv National University of Radio Electronics
ORCID: 0009-0002-4838-9329

ANALYSIS OF FRAMEWORKS AND TECHNICAL SECURITY MEASURES FOR THE INFRASTRUCTURE OF THE INTERNET OF ROBOTIC THINGS

The article provides a comprehensive analysis of the architectural, organizational, and technological foundations for the formation of an information security management system (ISMS) for the Internet of Things (IoRT) infrastructure, which combines the capabilities of IoT and robotics and is characterized by a high level of autonomy, scalability, and criticality of functions. The classification of IoRT application areas by user entities and industry areas is considered. Based on the requirements of the strategic and operational levels of management, the key components of the ISMS for IoRT are outlined.

Particular attention is paid to the analysis of administrative, physical, and technical security measures, covering device identification and authentication management, access control, secure interaction with suppliers, hardware protection, network segmentation, cryptographic mechanisms, and a secure software lifecycle. In the context of the implementation of the European NIS2 directive, the need to integrate international ISMS standards (ISO, NIST, ISA) at all levels of the IoRT architecture is emphasized.

An analysis of current trends in the deployment of ISMS was conducted, the main risk scenarios, typical threats and vulnerabilities that are characteristic of both IoT, IoRT technologies in particular and complex infrastructure using IoT, IoRT cluster, as a whole were identified.

An approach is proposed to use several security management frameworks within one branched infrastructure in accordance with the identified context and results of the risk management process.

Attention is paid to the possibilities and limitations of using blockchain technology to increase the level of IoRT security. The stages of blockchain integration are analyzed. At the same time, the problems of scalability, processing delays and energy consumption that limit the use of blockchain in real-time scenarios are emphasized. A hybrid approach is proposed that involves combining blockchain with decentralized databases to achieve a balance between performance and security.

Key words: *IoRT, ISMS, risk management, threats, vulnerabilities, information assets, blockchain, decentralized systems, intelligent devices, IoT ecosystem, critical infrastructure, digital security.*

Постановка проблеми

Сучасні інформаційні системи функціонують у середовищах, що характеризуються високою мінливістю, динамікою взаємодій та зростаючим обсягом поведінкових даних про діяльність користувачів і сервісів. Швидкий розвиток технологій створив з'єднаний світ, де різні системи та пристрої легко інтегруються в усі аспекти нашого життя. Інтернет роботизованих речей (IoRT) з'єднує роботи та автономні пристрої з Інтернетом, щоб вони могли спілкуватися, співпрацювати над даними та виконувати завдання більш ефективно. IoRT має потенціал повністю трансформувати різні галузі, включаючи виробництво, охорону здоров'я та транспорт. Однак проблеми безпеки можуть призвести до збою систем IoRT, роблячи їх вразливими, що є правдою для будь-якого пристрою, підключеного до Інтернету [3].

З урахуванням сучасних підходів до інформаційної та кібербезпеки, жодний інформаційний актив не можно розглядити у відриві його існування, як частини СУІБ. Тому таку інфраструктуру, як IoRT треба розглядати виключно с точки зору оцінки інформаційної безпеки в рамках міжнародних фреймворков ISO, NIST, ISA, стандартів захисту персональних даних, таких як GDPR [13].

З урахуванням оцінки ризиків, як невід'ємного компонента та заходу безпеки, були виділені головні потенційні загрози у даному сегменті та вразивості інфраструктури IoRT [3]. На підставі цього, існує необхідність приділити увагу аналізу безпеки функціонування як окремих компонентів інфраструктури IoRT (речі, блок інтелектуального прийняття рішень, датчики та механізми виконання, вбудовані системи, комунікація), так і надійну роботу взаємопов'язаних роботизованих систем, безпеку інфраструктури IoRT в цілому. Зважаючи на численні

переваги, які пропонує IoRT, особливу увагу слід приділити заходам безпеки для захисту чутливих даних від зловмисних атак, контролюванням пристроєм, чи зловживання повноваженнями операційної системи, які керують пристроями [6].

Аналіз останніх досліджень і публікацій

Опрацювання доробків наукового кола з досліджуваної тематики дозволяють констатувати відсутність детальної уваги до питань безпеки, що стосуються програмного забезпечення, повідомлень, які потрібно транспортувати, та даних [7]. Слід відзначити важливість наукових пошуків з використання безпечних методів обміну повідомленнями, таких як HTTPS, тим не менш, концепція безпеки не була суттєво добре висвітлена.Вермесан, Овідіу та інші науковці презентували нову стратегію забезпечення безпеки IoRT шляхом поєднання технології блокчейн з методами шифрування.

Автори пропонують безпечну рамку, яка використовує властивості безпеки цих технологій для створення потужної системи безпеки для IoRT. Корисність їхньої запропонованої рамки демонструється в дослідженні шляхом використання її в симульованому середовищі. Об'єднуючи передові технології, це нове рішення для безпеки IoRT долає труднощі захисту щільно взаємопов'язаних мереж роботизованих пристроїв [1]. Блокчейн також відомий своєю здатністю забезпечувати безпеку в системі IoRT [2]. У наукових колах пропонується безпечна система обміну даними для IoRT. Ця система використовує технологію блокчейн для гарантії цілісності та конфіденційності обміну даними.

Рішення використовує технологію розподіленого реєстру з блокчейну для створення незмінного запису передачі даних, створюючи прозоре та надійне середовище для обміну даними між роботизованим обладнання. Одна з основних проблем у IoRT вирішується стратегією авторів, яка підкреслює важливість підтримки цілісності та автентичності даних. Андроніє, Міхай та інші дослідники запропонували механізм обміну даними на основі блокчейн для IoRT, який є безпечним і масштабованим [1][2]. Автори створюють безпечне середовище для обміну даними між роботизованими пристроями, використовуючи блокчейн, одночасно забезпечуючи масштабованість та ефективне використання ресурсів.

Формулювання мети дослідження

Метою дослідження є комплексний аналіз архітектурних фреймворків і технічних механізмів захисту в системах Інтернету роботизованих речей (IoRT) у контексті управління інформаційною безпекою, а також виявлення ключових прогалин та формування напрямів подальших досліджень для підвищення надійності та стійкості IoRT-інфраструктур.

Викладення основного матеріалу дослідження

Сучасна технологія, відома як Інтернет роботизованих речей поєднує IoT з робототехнікою, щоб забезпечити її автономність. Сфери застосування IoRT є досить масштабним, їх можна класифікувати за декількома ознаками:

1. За суб’єктом застосування. Технології IoT охоплюють широкий спектр застосувань, включаючи медичний моніторинг, інфраструктуру «розумного дому» та офісу, промислові підприємства й ресурсодобувні об’єкти, міські системи управління та міжміські транспортно-логістичні платформи, забезпечуючи підвищення якості життя, операційної ефективності, безпеки та керованості в усіх відповідних середовищах.

2. За галузями впровадження можна виділити наступні сфери застосування.IoT-технології демонструють широку міжгалузеву застосовність – від масмедіа, де вони забезпечують персоналізовану взаємодію з користувачами, та екологічного моніторингу, що підвищує безпеку й оперативність реагування, до інтелектуального виробництва й цифрових систем керування, які оптимізують процеси, енергоспоживання та надійність інфраструктури, а також транспортної сфери, де IoT формує інтегровані високоефективні системи керування трафіком, логістикою та дорожньою безпекою.

Стратегічний рівень управління інформаційною безпекою формується такими заходами безпеки, як:

– Контекст середовища, сфера застосування. Для ефективного функціонування СУІБ в інфраструктурі IoRT необхідно визначити зовнішні та внутрішні фактори, врахувати потреби й вимоги зацікавлених сторін та встановити вимірювані, узгоджені з політикою й ризиками цілі інформаційної безпеки, забезпечуючи їх документування, комунікацію та постійне оновлення [13].

– Лідерство. Найвище керівництво повинне демонструвати лідерство у розбудові СУІБ для інфраструктури IoRT, установлюючи й документуючи політику інформаційної безпеки, що відповідає цілям організації, містить зобов’язання щодо дотримання вимог і постійного вдосконалення, доводиться до всіх рівнів персоналу та супроводжується чітким призначенням відповідальності й повноважень за ключові функції безпеки.

– Планування. Організація повинна, з урахуванням контексту застосування, визначати ризики та можливості для СУІБ інфраструктури IoRT і планувати дії, що забезпечать досягнення очікуваних результатів, зменшення небажаних ефектів та постійне вдосконалення, інтегруючи ці заходи у процеси системи управління інформаційною безпекою та регулярно оцінюючи їхню ефективність.

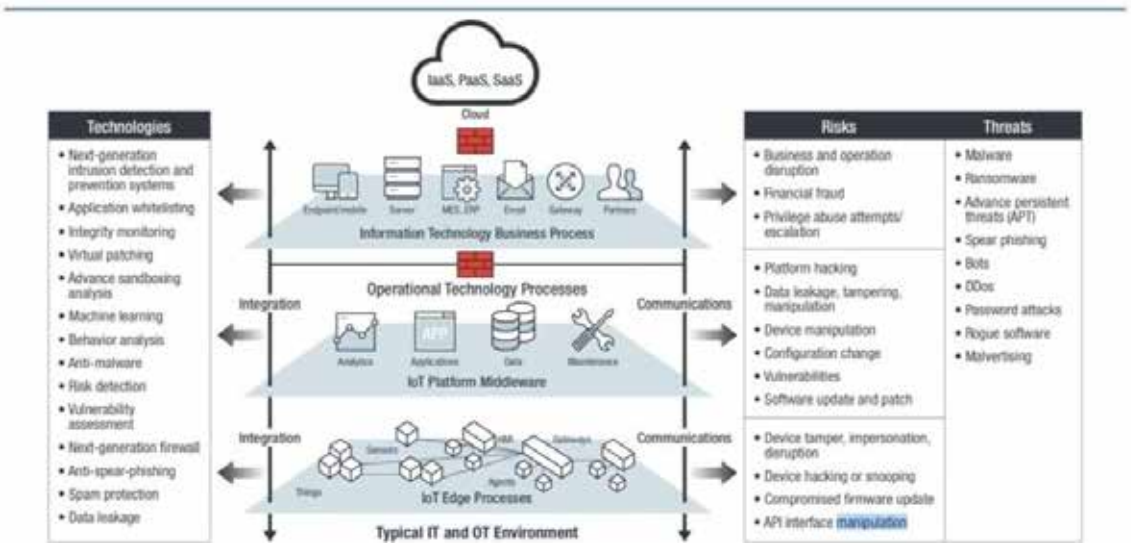

Рис. 1. Розгортання спеціальної рамки управління ІБ для IoT, IoRT за ISA IEC 62442

– Забезпечення. Інфраструктура IoRT повинна забезпечити необхідні ресурси, компетентність і поінформованість персоналу, організувати ефективні внутрішні та зовнішні комунікації та підтримувати належний рівень документованої інформації, охоплюючи її створення, оновлення, зберігання й вилучення, щоб гарантувати результативне функціонування та постійне вдосконалення системи менеджменту інформаційної безпеки.

– Управління ризиками. Оперативне планування та управління в інфраструктурі IoRT вимагає встановлення критеріїв процесів, керування ними відповідно до міжнародних стандартів (зокрема ISO/TR 22100-4:2018 та ISA/IEC 62443), а також впровадження систематичного процесу оцінки ризиків, що забезпечує їх ідентифікацію, аналіз, пріоритизацію та документування. Регулярна оцінка та обробка ризиків є необхідною для підтримання безпеки, цілісності й доступності IoRT-систем та гарантує, що можливості технології реалізуються без зростання загроз.

– Оцінка результатів функціонування, моніторинг аудит. Ефективне функціонування IoRT вимагає чітко визначених процедур моніторингу та вимірювання, які охоплюють об’єкти контролю, методи збору даних, відповідальних осіб і регулярний аналіз результатів, забезпечуючи своєчасне виявлення відхилень, вразливостей та інцидентів безпеки. Постійний моніторинг, внутрішні аудити та періодичний аналіз з боку керівництва гарантують адаптивність, відповідність вимогам і безперервну результативність системи менеджменту інформаційної безпеки IoRT [13].

Для підтримання ефективності та актуальності СУІБ організація повинна забезпечувати її постійне вдосконалення, системно реагуючи на невідповідності, усуваючи їхні причини, оцінюючи результативність коригувальних дій і вносячи необхідні зміни. Рішення керівництва за результатами аналізу мають бути спрямовані на розвиток можливостей постійного поліпшення та вдосконалення системи управління інформаційною безпекою в інфраструктурі IoRT [14].

З урахуванням впровадження загальноєвропейської директиви NIS2 особливо важливо забезпечити імплементацію базових світових стандартів управління інформаційною безпекою ISMS, таких як ISO, NIST та ISA, на всіх рівнях архітектур IoRT, оскільки створення пов’язаної екосистеми передбачає інтеграцію роботизованого обладнання, інструментів та IoT-технологій у рамках IoRT. У цьому контексті особливого значення набувають інноваційні технології підсилення безпеки, зокрема блокчейн – децентралізований і незмінний цифровий реєстр, який забезпечує прозоре, захищене та стійке до маніпуляцій зберігання даних і транзакцій, усуваючи потребу в посередниках та підвищуючи ефективність і довіру в різних сферах – від фінансів і логістики до цифрової ідентифікації та смарт-контрактів. До етапів впровадження блокчейну IoRT слід відносити:

1. Визначення випадку використання. Критично важливим першим кроком у впровадженні IoRT є визначення випадку використання. Це передбачає визначення операційних труднощів та оцінку можливостей роботизованої автоматизації. Один з факторів, який слід врахувати, це вивчення завдань, які є повторюваними, небезпечними, трудомісткими або потребують високої точності. Також важливо врахувати, чи підходить IoRT для таких завдань, як управління матеріалами, складання, інспекція або спостереження. Визначення випадку використання вимагає глибокого розуміння специфічних вимог галузі або організації. Організації можуть визначити найбільш ефективний випадок використання для використання роботизованих технологій з метою підвищення продуктивності, ефективності, безпеки та загальної продуктивності, співвідносячи можливості IoRT з визначеними труднощами та завданнями [1].

2. Вибір відповідної платформи блокчейн – передбачає порівняння характеристик різних платформ блокчейн, їх масштабованості, безпеки, взаємодії та процедур консенсусу. Ще одним фактором, який слід врахувати, є здатність платформи управляти величезною кількістю та швидкістю інформації, що виробляється пристроями IoRT. Важливо оцінити потенціал інтеграції та сумісність з існуючими системами. Для довгострокового успіху також критично важливо оцінити екосистему розробників платформи, документацію та підтримку спільноти. Організації можуть забезпечити безперебійну інтеграцію, точність даних та надійність серед пристроїв IoRT, ретельно оцінюючи та вибираючи правильну платформу блокчейн, що дозволяє безпечну та прозору комунікацію, обмін даними та автоматизовані транзакції в екосистемі IoRT [8].

3. Визначити схему даних. Це передбачає визначення організації та структури даних, які генерують пристрої IoRT. Серед факторів, які слід враховувати, є види даних, що підлягають збору, включаючи показання датчиків, статус обладнання, дані про місцезнаходження або експлуатаційні метрики. Визначення властивостей даних, методів вимірювання в порядку та будь-яких інших метаданих також є важливим. Схема повинна відповідати конкретному випадку використання та необхідній аналітиці або обробці. Необхідно забезпечити сумісність та взаємодію даних між різними системами та пристроями IoRT. Організації можуть ефективно захищати, аналізувати та отримувати цінні інсайти з даних, що генеруються пристроями IoRT, визначивши встановлену схему даних, що дозволяє приймати обґрунтовані рішення та оптимізувати систему в цілом.

4. Інтеграція пристроїв IoRT з блокчейном. Це передбачає налаштування апаратури для того, щоб вона могла спілкуватися з платформою технології блокчейн за допомогою протоколів та API. Окрім забезпечення процедур валідації даних та консенсусу, важливими аспектами є підтримка безпеки пристрою, обмеження доступу та конфіденційність даних. Щоб забезпечити безперешкодний обмін даними та комунікацію, процес об'єднання також має гарантувати взаємодію між різними апаратними та програмними платформами. Організації можуть забезпечити незмінність даних, прозорість та довіру в екосистемах IoRT, поєднуючи блокчейн з пристроями IoRT, що дозволяє безпечні та систематичні транзакції та взаємодії між пристроями [2]. Це з'єднання також може зробити можливим розвиток децентралізованих додатків та послуг, які використовують обидві технології IoRT та на основі блокчейн.

5. Розгортання розумних контрактів. Процес впровадження IoRT повинен включати розгортання розумних контрактів. На платформі блокчейн повинні бути запрограмовані та розгорнуті самовиконувані контракти. Логіка контракту, обставини та поведінка, які пристрої IoRT повинні виконувати самостійно, повинні бути враховані. У IoRT розумні контракти можуть спростити процеси, такі як координація пристроїв, розподіл ресурсів або врегулювання платежів. Щоб уникнути незаконного доступу або зловмисної діяльності, безпека та надійність розумних контрактів повинні бути гарантовані. Організації можуть автоматизувати взаємодії пристроїв, створити довіру та забезпечити безперешкодне прозоре виконання контрактних зобов'язань, впроваджуючи розумні контракти в IoRT [2]. Як наслідок, діяльність екосистеми IoRT може стати більш ефективною, точною та продуктивною, що призведе до підвищення автономії та загальної ефективності підключених пристроїв.

6. Моніторинг та підтримка мережі блокчейн. Для успішної реалізації IoRT важливо моніторити та управляти мережею блокчейн. Для забезпечення надійності, безпеки та ефективності мережі необхідно постійне моніторинг мережі. Стан вузлів блокчейн відстежується разом із швидкістю оброблюваних транзакцій та дійсністю механізму консенсусу. Крім того, слід вжити проактивних заходів, таких як періодичні оновлення, модифікації та аудити безпеки, щоб усунути вразливості та гарантувати надійність мережі. Щоб підтримувати зростаючу кількість пристроїв IoRT, організаціям також потрібно стежити за тим, як ефективно мережа використовує свої ресурси та наскільки легко вона може розширюватися. Організації можуть забезпечити безперебійну роботу, точність інформації та надійність серед пристроїв IoRT, ретельно відстежуючи та підтримуючи мережу блокчейн. Це допоможе створити надійне та безпечне середовище для автономних операцій, обміну інформацією та взаємодій.

7. Протоколи консенсусу блокчейн. Технологія блокчейн використовує різноманітні механізми консенсусу, кожен з яких має свої переваги та недолік.

8. Критична оцінка життєздатності блокчейн у IoRT. Децентралізовані бази даних, такі як InterPlanetary File System (IPFS) та Apache Cassandra, пропонують надійні рішення для зберігання та отримання даних у розподілених системах. Ці бази даних відзначаються в середовищах, де критично важливими є висока доступність, стійкість до збоїв та горизонтальна масштабованість. Вони розроблені для ефективної обробки великих обсягів даних та забезпечення узгодженості даних між розподіленими вузлам [4].

Безпека IoRT значною мірою залежить від шифрування даних та безпечної комунікації, оскільки вони забезпечують конфіденційність, цілісність та автентичність інформації, що обмінюється між пристроями, захищаючи її від несанкціонованого доступу або підробки. Шифруючи відкритий текст за допомогою методів шифрування та секретних ключів, дані стають недоступними для несанкціонованих осіб, які не мають ключа дешифрування. Основними для систем IoRT є шифрувальні протоколи, такі як Безпека транспортного рівня (TLS) або Протокол захищених сокетів (SSL), які автентифікують та шифрують дані під час передачі, забезпечуючи безпеку з кінця в кінець. Щоб захистити ключі шифрування від зловживання або розголошення, надійні системи управління ключами є обов'язковими в системах IoRT. Це передбачає безпечне генерування, розподіл та управління ключами,

а також своєчасне відкликання та заміну скомпрометованих ключів. Шифрування в реальному часі повинно виконуватись безперешкодно без компрометації продуктивності системи. Це вимагає вдосконалень апаратного або програмного забезпечення для забезпечення високошвидкісних процесів шифрування та дешифрування. Крім того, стратегії шифрування даних IoRT повинні враховувати безпечні методи зберігання та відновлення, щоб забезпечити захист даних навіть під час періодів бездіяльності [3].

Для безпечної комунікації можна використовувати алгоритми шифрування, такі як криптографія на основі еліптичних кривих (ECC) та RSA, щоб захистити з'єднання. Ці алгоритми гарантують конфіденційність і безпеку переданих даних. Крім того, зашифровані методи обміну повідомленнями, такі як MQTT-SN або CoAP, можуть бути використані для встановлення безпечної комунікації в IoRT[12]. Навіть у контекстах з обмеженими ресурсами використання легковагових технік повідомлень цими протоколами забезпечує безпечну та надійну комунікацію. В загальному, безпечна комунікація є необхідною для забезпечення надійності та безпеки додатків IoRT [9]. Завдяки впровадженню надійного шифрування та механізмів безпечної комунікації дані залишаються недоступними для несанкціонованих осіб, що зміцнює загальну безпеку системи IoRT. Ці заходи слугують основою в системах IoRT, гарантуючи безпеку переданих і збережених даних та встановлюючи фундамент для надійної та стійкої екосистеми IoRT.

Адміністративний рівень безпеки IoRT охоплює управління ідентифікацією та автентифікацією пристроїв, контроль прав доступу та взаємодію з постачальниками. Ідентифікація й автентифікація мають забезпечувати надійне підтвердження пристроїв і користувачів за допомогою криптографічних механізмів та керування всім життєвим циклом ідентифікаторів. Права доступу повинні призначатися, переглядатися та скасовуватися відповідно до політик, включаючи контроль привілейованих доступів та застосування безпечної аутентифікації.

Взаємодія з постачальниками та хмарними сервісами потребує процесів управління ризиками, встановлення вимог до безпеки та регулярного моніторингу діяльності постачальників. Крім того, організація повинна мати сформований процес реагування на інциденти та відновлення після катастроф, включаючи регулярне тестування планів реагування.

Безпека IoRT залежить від поінформованості персоналу: працівники мають бути навчени, підписувати угоди про конфіденційність та розуміти свою роль у збереженні безпеки [13]. На фізичному рівні необхідно захищати периметри, приміщення, обладнання та кабельні мережі, а також впроваджувати механізми захисту від стихійних, навмисних і випадкових фізичних загроз. Безпечне апаратне забезпечення – TPM, HSM, біометричні засоби – є ключовим для протидії маніпуляціям та фізичному доступу. Технічні засоби охоплюють увесь життєвий цикл програмного забезпечення та інфраструктури. Необхідно керувати технічними вразливостями, конфігураціями, оновленнями, маскуванням та видаленням даних. Системи повинні мати резервування, логування, контроль привілейованих утиліт, веб-фільтрацію, криптографічний захист та синхронізацію часу. Мережі мають бути сегментовані, захищені та керовані відповідно до політик безпеки.

Окрему увагу слід приділяти безпечній розробці програмного забезпечення: перевірка коду, тестування на проникнення, керування змінами та врахування вимог безпеки є обов’язковими елементами для підтримання цілісності та стійкості IoRT.

Хоча блокчейн пропонує значні переваги в певних сценаріях, це не універсальне рішення. Вибір між блокчейном та іншими децентралізованими рішеннями має базуватися на конкретних вимогах застосування. Наприклад, якщо основна потреба полягає у швидкісній обробці даних з складними запитами, децентралізовані бази даних можуть бути більш підходящими. Навпаки, якщо акцент робиться на забезпеченні цілісності даних, прозорості та функціонуванні в середовищі без довіри, блокчейн є переважним вибором.

Інтеграція блокчейну в IoRT надає унікальні переваги, які доповнюють можливості децентралізованих баз даних. Гібридний підхід, що використовує обидві технології на основі їхніх сильних сторін, може запропонувати найбільш комплексне рішення для забезпечення безпеки та оптимізації мереж IoRT. Однією з основних проблем, пов'язаних із використанням технології блокчейн в IoRT, є її ефективність. Мережі блокчейн, особливо ті, що використовують механізми консенсусу proof-of-work (PoW), можуть бути ресурсомісткими, що викликає занепокоєння щодо масштабованості та споживання енергії. Ці проблеми ефективності є критично важливими в додатках IoRT, де часто потрібна обробка даних у реальному часі та мінімальна затримка.

Традиційні блокчейни, такі як Біткойн та Ефіріум, мають обмежені можливості пропускної здатності, обробляючи відносно невелику кількість транзакцій на секунду [1]. Це обмеження може бути проблематичним для додатків IoRT, які вимагають високих обсягів транзакцій та низької затримки. Час, необхідний для підтвердження транзакцій у мережі блокчейн, може бути значним. В IoRT, де негайна обробка даних та реакція є критично важливими, такі затримки можуть вплинути на продуктивність та надійність системи.

Блокчейни на основі PoW відомі своїм високим споживанням енергії, що є неприйнятним для багатьох додатків IoRT, особливо тих, що залучають обмежені ресурси. Суттєві енергетичні вимоги блокчейнів на основі PoW викликають занепокоєння щодо їхнього впливу на навколишнє середовище. Оскільки системи IoRT часто прагнуть бути сталими та ефективними, альтернативні механізми консенсусу або рішення можуть бути переважними.

Висновки

Таким чином, формування надійної моделі безпеки IoRT є стратегічним завданням, що потребує інновацій, міждисциплінарної співпраці та глибокої адаптації існуючих фреймворків до специфіки роботизованих кіберфізичних систем. Безпека інфраструктури Інтернету роботизованих речей (IoRT) вимагає комплексного, багаторівневого та системного підходу, заснованого на принципах ISMS ISO 27001 і доповненого сучасними галузевими стандартами та технологіями. Проведений аналіз демонструє, що попри наявність базових вимог у міжнародних фреймворках, профілі безпеки для IoRT залишаються недостатньо формалізованими, що створює численні ризики та вразливості – від технічних до організаційних.

З метою подальших досліджень і практики в безпеці IoRT запропоновано впровадження інформації про загрози та аналітику, процес інтеграції принципів безпеки за дизайном, використання потенціалу блокчейн-технологій, які здатні суттєво підвищити прозорість, довіру та цілісність даних та аудиту у розподілених системах IoRT, а також реалізацію механізмів багатофакторної автентифікації для зміцнення контролю доступу.

Список використаної літератури

1. H. Yin, D. Guo, K. Wang, Z. Jiang, Y. Lyu, and J. Xing, ‘‘Hyperconnected network: A decentralized trusted computing and networking paradigm’’ IEEE Netw., vol. 32, no. 1, pp. 112–117, Jan./Feb. 2018.

2. Q. Lu and X. Xu, ‘‘Adaptable blockchain-based systems: A case study for product traceability’’ IEEE Softw., vol. 34, no. 6, pp. 21–27, Nov./Dec. 2017.

3.Y. Liang, Z. Cai, J. Yu, Q. Han, and Y. Li, ‘‘Deep learning based inference of private information using embedded sensors in smart devices’’ IEEE Netw. Mag., vol. 32, no. 4, pp. 8–14, Jul./Aug. 2018.

4. A. Halevy, P. Norvig, and F. Pereira, ‘‘The unreasonable effectiveness of data,’’ IEEE Intell. Syst., vol. 24, no. 2, pp. 8–12, Mar. 2009.

5. D. E. O’Leary, ‘‘Artificial intelligence and big data,’’ IEEE Intell. Syst., vol. 28, no. 2, pp. 96–99, Mar. 2013

6. T. Chajed, J. Gjengset, J. Van Den Hooff, M. F. Kaashoek, J. Mickens, R. Morris, and N. Zeldovich, ‘‘Amber: Decoupling user data from Web applications,’’ in Proc. 15th Workshop Hot Topics Oper. Syst. (HotOS XV), Warth-Weiningen, Switzerland, 2015, pp. 1–6.

7. Y.-A. de Montjoye, E. Shmueli, S. S. Wang, and A. S. Pentland, ‘‘openPDS: Protecting the privacy of metadata through SafeAnswers,’’ PLoS ONE, vol. 9, no. 7, 2014, Art. no. e98790

8. Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, ‘‘MeDShare: Trust-less medical data sharing among cloud service providers via blockchain,’’ IEEE Access, vol. 5, pp. 14757–14767, 2017.

9. W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, ‘‘When intrusion detection meets blockchain technology: A review,’’ IEEE Access, vol. 6, pp. 10179–10188, 2018.

10. J. Wang, M. Li, Y. He, H. Li, K. Xiao, and C. Wang, ‘‘A blockchain based privacy-preserving incentive mechanism in crowdsensing applications,’’ IEEE Access, vol. 6, pp. 17545–17556, 2018.

11. I. J. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, ‘‘Generative adversarial networks,’’ 2014, arXiv:1406.2661. [Online]. Available: https://arxiv.org/abs/1406.2661

12. A. Praseed and P. S. Thilagam, ‘‘DDoS attacks at the application layer: Challenges and research perspectives for safeguarding Web applications,’’ IEEE Commun. Surveys Tuts., vol. 21, no. 1, pp. 661–685, 1st Quart., 2019

13. Stain A.J. Mollerhaug, “Harmonizing Standards for Digital Trust: Bridging IEC 62443, ISO/IEC 42001, and ISO/IEC 27001”, https://pecb.com/en/past-webinars/harmonizing-standards-for-digital-trust-bridging-iec-62443-iso-iec-42001-and-iso-iec-27001#:~:text=Webinar-,Harmonizing%20Standards%20for%20Digital%20Trust:%20Bridging%20IEC%2062443%2C%20ISO/,and%20ISO/IEC%2027001%20auditing, 2025

14. George Usi, CMMC 2.0 vs. ISO/IEC 27001 vs. NIST 800-171: What You Need to Know, https://pecb.com/en/past-webinars/cmmc-2-0-vs-iso-iec-27001-vs-nist-800-171-what-you-need-to-know#:~:text=IEC%2027001%20vs. -,NIST%20800%2D171:%20What%20You%20Need%20to%20Know,to%20measure%20and%20implement%20compliance, 2021

References

1.H. Yin, D. Guo, K. Wang, Z. Jiang, Y. Lyu, and J. Xing, ‘‘Hyperconnected network: A decentralized trusted computing and networking paradigm’’ IEEE Netw., vol. 32, no. 1, pp. 112–117, Jan./Feb. 2018.

2. Q. Lu and X. Xu, ‘‘Adaptable blockchain-based systems: A case study for product traceability’’ IEEE Softw., vol. 34, no. 6, pp. 21–27, Nov./Dec. 2017.

3. Y. Liang, Z. Cai, J. Yu, Q. Han, and Y. Li, ‘‘Deep learning based inference of private information using embedded sensors in smart devices’’ IEEE Netw. Mag., vol. 32, no. 4, pp. 8–14, Jul./Aug. 2018.

4. A. Halevy, P. Norvig, and F. Pereira, ‘‘The unreasonable effectiveness of data,’’ IEEE Intell. Syst., vol. 24, no. 2, pp. 8–12, Mar. 2009.

5 D. E. O'Leary, ''Artificial intelligence and big data,'' IEEE Intell. Syst., vol. 28, no. 2, pp. 96–99, Mar. 2013

6. T. Chajed, J. Gjengset, J. Van Den Hooff, M. F. Kaashoek, J. Mickens, R. Morris, and N. Zeldovich, ''Amber: Decoupling user data from Web applications,'' in Proc. 15th Workshop Hot Topics Oper. Syst. (HotOS XV), Warth-Weiningen, Switzerland, 2015, pp. 1–6.

7. Y.-A. de Montjoye, E. Shmueli, S. S. Wang, and A. S. Pentland, ''openPDS: Protecting the privacy of metadata through SafeAnswers,'' PLoS ONE, vol. 9, no. 7, 2014, Art. no. e98790

8.Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, ''MeDShare: Trust-less medical data sharing among cloud service providers via blockchain,'' IEEE Access, vol. 5, pp. 14757–14767, 2017.

9. W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, ''When intrusion detection meets blockchain technology: A review,'' IEEE Access, vol. 6, pp. 10179–10188, 2018.

10. J. Wang, M. Li, Y. He, H. Li, K. Xiao, and C. Wang, ''A blockchain based privacy-preserving incentive mechanism in crowdsensing applications,'' IEEE Access, vol. 6, pp. 17545–17556, 2018.

11. I. J. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, ''Generative adversarial networks,'' 2014, arXiv:1406.2661. [Online]. Available: https://arxiv.org/abs/1406.2661

12. A. Praseed and P. S. Thilagam, ''DDoS attacks at the application layer: Challenges and research perspectives for safeguarding Web applications,'' IEEE Commun. Surveys Tuts., vol. 21, no. 1, pp. 661–685, 1st Quart., 2019

13. Stain A.J. Mollerhaug, "Harmonizing Standards for Digital Trust: Bridging IEC 62443, ISO/IEC 42001, and ISO/IEC 27001", https://pecb.com/en/past-webinars/harmonizing-standards-for-digital-trust-bridging-iec-62443-iso-iec-42001-and-iso-iec-27001#:~:text=Webinar-,Harmonizing%20Standards%20for%20Digital%20Trust:%20Bridging%20IEC%2062443%2C%20ISO/,and%20ISO/IEC%2027001%20auditing, 2025

14. George Usi, CMMC 2.0 vs. ISO/IEC 27001 vs. NIST 800-171: What You Need to Know, https://pecb.com/en/past-webinars/cmmc-2-0-vs-iso-iec-27001-vs-nist-800-171-what-you-need-to-know#:~:text=IEC%2027001%20vs. -,NIST%20800%2D171:%20What%20You%20Need%20to%20Know,to%20measure%20and%20implement%20compliance, 2021

Дата першого надходження рукопису до видання: 20.11.2025
Дата прийнятого до друку рукопису після рецензування: 17.12.2025
Дата публікації: 31.12.2025