https://doi.org/10.31891/2219-9365-2026-86-55
УДК 004.056

БАСИСТИЙ Віталій
Хмельницький національний університет
https://orcid.org/0009-0009-1978-614X
e-mail: basistavitalij@gmail.com
СТЕЦЮК Микола
Хмельницький національний університет
https://orcid.org/0000-0003-3875-0416
e-mail: mykola.stetsiuk@khmnu.edu.ua
ЧЕШУН Віктор
Хмельницький національний університет
https://orcid.org/0000-0002-3935-2068
e-mail: cheshunvn@khmnu.edu.ua
ЧЕШУН Дмитро
Хмельницький фаховий економіко-технологічний коледж УЕП
https://orcid.org/0009-0007-9937-9450
e-mail: dmitry_95@ukr.net

РЕГУЛЮВАННЯ ПИТАНЬ БЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ В ФРЕЙВОРКАХ ЄВРОПЕЙСЬКОГО СОЮЗУ, ВЕЛИКОБРИТАНІЇ І США

У сучасних умовах стрімкого розвитку цифрових технологій та глобального поширення Інтернету речей (IoT) питання безпеки таких систем набуває ключового значення для захисту критичної інформаційної інфраструктури, конфіденційності користувачів і безперебійності бізнес-процесів. У цій статті проведено комплексний огляд міжнародних стандартів, рекомендацій і нормативних актів, спрямованих на підвищення рівня кіберзахисту IoT-пристроїв та середовищ, зокрема проаналізовано положення NISTIR 8259, IoT Cybersecurity Improvement Act of 2020, ETSI EN 303 645, UK Code of Practice, CSA IoT Security Controls Framework, а також рамку відповідності IoT Security Foundation (IoTSF). Особливу увагу приділено аналізу призначення, структури та основних вимог до безпеки, які охоплюють ідентифікацію пристроїв, захист конфіденційності, управління оновленнями, контроль доступу, моніторинг подій, реагування на інциденти та зниження ризиків, пов'язаних із вразливостями в IoT-інфраструктурі.

Ключові слова: захист інформації, інтернет речей, нормативно-правове регулювання.

BASYSTYI Vitalii, STETSIUK Mykola, CHESHUN Viktor
Khmelnytsky National University
CHESHUN Dmytro
Khmelnytskyi Vocational Economic and Technological College of the UEE

REGULATION OF INTERNET OF THINGS SECURITY ISSUES IN THE FRAMEWORKS OF THE EUROPEAN UNION, THE UNITED KINGDOM, AND THE USA

In the context of rapid technological progress and the global expansion of the Internet of Things (IoT), ensuring the cybersecurity of IoT systems has become a crucial challenge for protecting critical infrastructure, safeguarding user privacy, and maintaining operational continuity. This article provides a comprehensive analysis of international standards, frameworks, and legislative acts aimed at enhancing IoT security. Specifically, it examines the core provisions, structures, and objectives of documents such as NISTIR 8259, the IoT Cybersecurity Improvement Act of 2020, ETSI EN 303 645, the UK's Secure by Design Code of Practice, the CSA IoT Security Controls Framework, and the IoT Security Foundation Compliance Framework. The article highlights the key requirements for IoT cybersecurity, including device identification, privacy protection, secure update management, access control, event monitoring, incident response, and the mitigation of vulnerabilities within diverse IoT environments. The analysis emphasizes the importance of aligning technical security measures with enterprise risk management. In addition, the article discusses practical tools and techniques relevant to modern IoT defense strategies: unified asset discovery tools that support real-time detection of managed and unmanaged devices, intrusion detection systems (IDS) adapted for industrial and embedded IoT contexts, and the role of virtual patching as a mitigation technique for legacy or unpatchable devices using network-level controls.

The findings conclude that a holistic combination of regulatory compliance, technical innovation, and risk-based governance is essential for building a resilient IoT security architecture. At the same time, the article outlines persistent challenges such as standard fragmentation, varying policy maturity across jurisdictions, and the limited capabilities of low-resource IoT devices.

Keywords: information protection, Internet of Things, regulatory framework.

Стаття надійшла до редакції / Received 10.03.2026
Прийнята до друку / Accepted 16.04.2026
Опубліковано / Published 31.05.2026

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

У сучасну епоху стрімкої цифровізації Інтернет речей (IoT) перетворився з перспективної концепції на один із ключових технологічних чинників розвитку промисловості, міської інфраструктури та побутового середовища. IoT-технології, що об'єднують фізичні об'єкти в єдину мережу через сенсори, мережеві протоколи та аналітичні платформи, створюють принципово нові можливості для збору, обробки й використання даних у реальному часі. Швидке зростання кількості підключених пристроїв, розширення можливостей обробки даних у реальному часі та інтеграція IoT з технологіями штучного інтелекту створюють передумови для глибоких трансформацій у багатьох галузях економіки й суспільного життя.

В економічних реаліях підприємства все частіше впроваджують IoT для оптимізації витрат, покращення контролю якості продукції, віддаленого моніторингу стану обладнання та прогнозного технічного обслуговування [1]. Це дозволяє зменшувати простої, запобігати аваріям і будувати більш гнучкі бізнес-моделі, що відповідають динаміці ринку. IoT виступає ключовим елементом розвитку індустрії 4.0, де виробничі процеси інтегруються з інформаційними технологіями для створення автоматизованих та адаптивних систем [2]. Не менш важливим напрямом залишається впровадження IoT у побутовій сфері. Смарт-пристрої для будинків, такі як інтелектуальні термостати, освітлення, охоронні системи чи побутова техніка, підвищують комфорт і енергоефективність житла. У містах IoT-технології застосовуються для організації інтелектуального управління транспортом, енергомережами, екологічним моніторингом і безпекою, що стає дедалі актуальнішим у контексті сталого розвитку [3]. Значну роль IoT відіграє у сфері охорони здоров'я, де дистанційний моніторинг пацієнтів, носимі медичні пристрої та автоматизовані системи збору даних допомагають оперативно реагувати на зміни стану здоров'я, що особливо важливо в умовах глобальних викликів, таких як пандемії чи демографічне старіння населення [4,5].

Водночас із зростанням значення IoT зростає й кількість викликів. Зокрема, це складнощі управління мережею великої кількості пристроїв, проблеми кібербезпеки та конфіденційності даних. Чисельність підключених пристроїв IoT постійно зростає і прогнозується, що найближчими роками їх будуть десятки мільярдів [6]. Ці пристрої генерують величезні обсяги даних. Саме тому актуальність IoT тісно пов'язана з розвитком нових стандартів безпеки і нормативних підходів, які повинні забезпечувати захищене та відповідальне використання цієї технології.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Для підвищення безпеки та надійності IoT застосовуються різноманітні рішення.

Виявляти та контролювати керовані та некеровані пристрої системи IoT в режимі реального часу допомагають інструменти уніфікованого виявлення активів [7]. Їхня основна функція полягає у тому, щоб автоматично ідентифікувати всі підключені пристрої в мережі, незалежно від типу, виробника чи операційної системи, та надати IT- і безпековим командам повну та актуальну інформацію про стан цих активів у режимі реального часу. Такі інструменти зазвичай поєднують кілька технологій виявлення – активне сканування, пасивний моніторинг мережевого трафіку, аналіз протоколів та інтеграцію з іншими системами управління активами. Це дозволяє створювати детальні профілі пристроїв: визначати їхній тип, модель, версію прошивки, відкриті порти, підключені сервіси та рівень ризику тощо.

Системи виявлення вторгнень (Intrusion Detection Systems – IDS) для IoT-середовищ забезпечують моніторинг, адаптований до промислових систем [7,8]. Такі IDS орієнтовані на специфіку промислових протоколів (Modbus, DNP3, OPC UA, BACnet та інші протоколи управління промисловим обладнанням і автоматизованими системами керування ICS/SCADA). На відміну від традиційних IT IDS, які зазвичай фокусуються на загальних IP-протоколах і мережевих аномаліях, IoT-IDS враховують особливості форматів команд, дозволених операцій і типових сценаріїв взаємодії пристроїв у виробничих мережах. Ці IDS мають підтримувати пасивний моніторинг, щоб уникнути порушення технологічних процесів. У промислових середовищах дуже важливо не створювати додаткового навантаження або затримок у роботі критичного обладнання. Тому більшість промислових IDS використовують дзеркальне копіювання трафіку (port mirroring) або TAP-пристрої для непомітного спостереження за мережею.

Віртуальне патчування у сфері IoT – ще один із практичних методів захисту середовищ, де велика кількість пристроїв часто не підтримує регулярних оновлень програмного забезпечення або взагалі не має технічної можливості для їх впровадження. Це характерна проблема для промислового IoT, медичних приладів, розумних побутових систем та вбудованих сенсорів, де будь-яке втручання в роботу пристрою може порушити його функції або суперечити вимогам сертифікації [7]. Рішення для віддаленого управління та моніторингу (Remote Management and Monitoring – RMM) полегшують управління патчами та моніторинг пристроїв [5].

Платформи безпеки IoT надають комплексний захист для пристроїв та систем IoT, а шлюзи безпеки IoT забезпечують безпечне підключення та обробку даних [9]. Апаратні модулі безпеки (Hardware Security Modules – HSM) забезпечують надійну криптографічну обробку та захист ключів [9]. Технологія блокчейн пропонує децентралізований та захищений від підробок спосіб управління даними IoT та підвищення безпеки

[10]. Багатооператорські eSIM підвищують надійність та гнучкість підключення пристроїв IoT, дозволяючи автоматичне перемикання між операторами [11]. Штучний інтелект та машинне навчання використовуються для виявлення шаблонів атак та захисту пристроїв IoT. Безпечні елементи та довірені середовища виконання (Trusted Execution Environments – TEEs) забезпечують захищені області на процесорах для виконання чутливих операцій [9].

Поряд із великим різноманіттям технологічних рішень для забезпечення безпеки IoT характерною рисою сучасного етапу їх розвитку є відсутність єдиних підходів в їх реалізації. Для вирішення існуючих проблем та недоліків необхідні комплексні рішення, які враховують аспекти безпеки, конфіденційності та операційної ефективності систем IoT і базуються на міжнародних нормативно-регулюючих документах.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою роботи є: аналіз міжнародних і національних фреймворків, що безпосередньо або опосередковано регулюють питання безпеки пристроїв, систем і технологій Інтернету речей.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Хоча безпека IoT є однією із найактуальніших задач сьогодення, рішенню цієї проблеми на рівні законів і стандартів увагу почали придідяти не так давно. На сьогодні існує сукупність фреймворків та нормативних документів, які допомагають забезпечити безпеку пристроїв та систем IoT.

Однією з перших спроб у світі стимулювати ринок масового IoT до самоорганізації у сфері кібербезпеки і сформулювати на рівні національного уряду загальнодержавні мінімальні вимоги до безпеки споживчих IoT-пристроїв в формі практичних рекомендацій для виробників, імпортерів, розробників та дистриб'юторів стали Рекомендації щодо безпеки споживчих IoT-пристроїв (Code of Practice for Consumer IoT Security) [12] – політичний документ, опублікований Міністерством цифрових технологій, культури, медіа та спорту Великої Британії (UK DCMS) у 2018 році.

У початковій редакції Code of Practice визначено 13 принципів безпеки, що покривають повний життєвий цикл IoT-пристрою від розробки і виробництва до утилізації, серед яких:

– паролі мають бути унікальними для кожного примірника пристроїв IoT або змінюватися під час першого налаштування;

– виробник має впровадити політику управління уразливостями і призначити контактну точку для повідомлення про знайдені вразливості;

– пристрої повинні мати зрозумілі механізми оновлення прошивки і програмного забезпечення (ПЗ) протягом погодженого строку підтримки, а виробник має чітко інформувати користувача про те, як довго пристрій буде підтримуватися оновленнями безпеки;

– пристрої мають обробляти особисті дані відповідно до принципів GDPR (мінімізувати обсяг зібраних даних, обґрунтовувати мету збирання, захищати дані шифруванням);

– функціонал і доступ мають ґрунтуватися на принципі мінімальних привілеїв, забезпечуючи мінімальні права доступу;

– реалізація захисту цілісності через впровадження механізмів виявлення несанкціонованих змін конфігурації, контролю цілісності ПЗ та прошивки;

– дані, що передаються між пристроями, мають бути захищені сучасними протоколами шифрування (захист каналу зв'язку);

– пристрої повинні мати функціонал для безпечного стирання (знеособлення) персональних даних при перепродажі чи утилізації;

– рекомендується забезпечити механізми журналювання безпечної діяльності пристрою, щоб вчасно виявляти інциденти;

– пристрої мають бути стійкими до збоїв, зокрема, здатними відновлюватися після аварійного оновлення;

– виробники мають чітко інформувати користувачів про налаштування безпеки, політики конфіденційності та терміни підтримки.

Завдяки цьому документу Велика Британія стала одним із лідерів формування практики «безпечного дизайну» для IoT у Європі та вплинула на глобальні рекомендації.

Базисом для розвитку системи стандартизації питань безпеки IoT в США став федеральний закон США «IoT Cybersecurity Improvement Act of 2020» [13], ухвалений Конгресом і підписаний у грудні 2020 року. Він став першим системним нормативним документом на федеральному рівні, що безпосередньо регулює вимоги до кібербезпеки IoT у державному секторі. Його головна мета – підвищити безпеку федеральних інформаційних систем за рахунок встановлення мінімальних стандартів кіберзахисту для IoT-пристроїв, які закуповуються та експлуатуються урядовими структурами. Цей закон покликаний усунути ризики, пов'язані з тим, що IoT-пристрої (від окремих датчиків та камер і до медичних пристроїв та розумних будівельних систем тощо) часто не мають належних механізмів автентифікації, оновлення або контролю доступу, що робить їх уразливими до атак. Закон зобов'язує Національний інститут стандартів і технологій США (NIST)

розробляти та публікувати рекомендації й технічні стандарти для безпечного проєктування, ідентифікації, конфігурації, оновлення й управління IoT-пристроями. Ці керівництва мають ґрунтуватися на передових практиках кібербезпеки. Федеральні агентства зобов'язані закуповувати лише ті IoT-пристрої та послуги, які відповідають стандартам і рекомендаціям NIST. Це означає, що будь-який постачальник, який хоче співпрацювати з урядом США, має гарантувати, що його пристрої відповідають базовим вимогам щодо конфіденційності, цілісності, доступності та можливості управління уразливостями.

На вимогу розглянутого закону Національним інститутом стандартів і технологій США розроблено серію спеціальних публікацій SP 800-213 [14], які надають керівництво для федеральних установ щодо використання пристроїв IoT у їхніх системах. Зокрема, SP 800-213 визначає вимоги до кібербезпеки пристроїв IoT та пояснює їх роль у федеральних системах, а також розглядає ризики, які вони можуть становити. Серія SP 800-213 пропонує комплексний підхід до управління ризиками, пов'язаними з використанням пристроїв IoT, враховуючи їхню роль у федеральних системах та їхні специфічні загрози. Документи серії розглядають пристрої IoT як невід'ємну частину федеральних систем та підкреслюють їх унікальні ризики для кібербезпеки, які необхідно враховувати.

Фреймворк кібербезпеки IoT Device Cybersecurity Guidance for the Federal Government [15], опублікований NIST у рамках серії SP 800-213 та суміжних документів, є одним із ключових нормативних орієнтирів для забезпечення безпеки IoT у державному секторі США. Його поява зумовлена швидким зростанням використання IoT-пристроїв у федеральних установах, що створює суттєві ризики для національної кібербезпеки через специфічні вразливості цих технологій. Головна мета керівництва – надати федеральним органам виконавчої влади чіткі рекомендації щодо того, як безпечно впроваджувати, експлуатувати й управляти IoT-пристроями протягом усього їхнього життєвого циклу. Фреймворк містить рекомендації щодо розгляду безпеки системи IoT з точки зору окремих пристроїв. Це дозволяє визначити вимоги до кібербезпеки пристроїв – можливості та дії, яких організація очікує від пристрою IoT, його виробника та третіх сторін. Документ допомагає замовникам і керівникам IT-проєктів враховувати ризики кібербезпеки вже на етапі закупівель і визначає вимоги до виробників і постачальників IoT-рішень, які мають відповідати мінімальним критеріям безпеки.

Для реалізації комплексного підходу у забезпеченні безпеки IoT Національним інститутом стандартів і технологій США також розроблено серію публікацій NISTIR 8259 [16], яка спрямована на формування уніфікованого підходу до забезпечення кібербезпеки IoT-пристроїв у контексті їхнього життєвого циклу: проєктування, виробництво, впровадження, експлуатація та виведення з експлуатації. Головна мета NISTIR 8259 – допомогти виробникам розуміти мінімальні обов'язкові характеристики безпеки IoT-пристроїв, які очікують замовники у федеральному секторі, і забезпечити прозорість у спілкуванні між постачальниками і користувачами.

Серія складається з трьох ключових документів:

– NISTIR 8259: Foundational Cybersecurity Activities for IoT Device Manufacturers [17] – основоположний документ, який описує базові заходи з кібербезпеки, що мають бути виконані виробниками IoT-пристроїв;

– NISTIR 8259A: IoT Device Cybersecurity Capability Core Baseline [18] – містить перелік мінімальних технічних можливостей безпеки, які мають бути вбудовані у будь-який IoT-пристрій;

– NISTIR 8259B (Draft): IoT Non-Technical Supporting Capability Core Baseline [19] – описує нефункціональні вимоги (політики, документи, інформаційна підтримка та супровід), що мають забезпечувати безпечну експлуатацію IoT.

Таким чином, NISTIR 8259 задає загальну рамку, NISTIR 8259A деталізує технічний мінімум, а NISTIR 8259B фокусується на нефункціональних та організаційних аспектах експлуатації IoT.

Рамковий документ CSA IoT Security Controls Framework [20] створено Cloud Security Alliance (CSA) для організацій, які проєктують, розробляють або впроваджують IoT-системи. Фреймворк є актуальним для корпоративних систем IoT, що включають різні типи підключених пристроїв, хмарних сервісів та мережевих технологій. Його головна мета – надати структуровану систему заходів контролю безпеки, що дозволяє виробникам, операторам і інтеграторам IoT зменшувати ризики вразливостей та забезпечувати безпечне функціонування IoT-рішень протягом життєвого циклу.

CSA структурувала фреймворк за принципом розподілу контролів безпеки на ключові домени відповідно до компонентів типової IoT-архітектури:

– пристрої (Device/Thing Security);
– мережевий рівень (Network Security);
– шлюзи (Gateway Security);
– IoT-платформи / хмара (Cloud/Platform Security);
– додатки (Application Security);
– операційні процеси та управління (Operations and Lifecycle Security).

Ключові принципи та групи контролів, на яких зосереджується CSA IoT Security Controls Framework:

– ідентифікація та автентифікація: усі IoT-пристрої мають бути однозначно ідентифіковані, має

бути впроваджена багатофакторна автентифікація для пристроїв і користувачів у всіх можливих випадках, уникнення «загальних» облікових даних за замовчуванням;

– управління конфігурацією та цілісністю: захист конфігурацій від несанкціонованої зміни, механізми перевірки цілісності ПЗ/прошивки, контроль і моніторинг змін конфігурації;

– захищені оновлення: можливість безпечного оновлення прошивки та ПЗ, підпис цифрових оновлень для перевірки автентичності, політика своєчасного усунення відомих уразливостей;

– захист даних: шифрування даних «у спокої» та «у русі», управління ключами шифрування, мінімізація збирання персональних даних;

– безпека комунікацій: захищені протоколи (TLS, VPN), сегментація мережевих зон для IoT, засоби запобігання атакам «людина посередині»;

– моніторинг та реагування: постійний моніторинг подій безпеки, інтеграція з SIEM/IDS/IPS, журналювання активності пристроїв;

– управління доступом: принцип мінімальних привілеїв, рольовий або атрибутивний контроль доступу (RBAC/ABAC), регулярна ревізія прав доступу;

– безпечний життєвий цикл: урахування безпеки ще на стадії проєктування (security by design), політика безпечної утилізації або перепродажу пристроїв, управління інцидентами й оновлення планів реагування.

Цей фреймворк не є обов'язковим стандартом або законом, а радше практичним методичним посібником, що допомагає врахувати різні аспекти безпеки IoT від пристроїв до хмарних платформ і мережевої інфраструктури. CSA Framework часто використовується як відправна точка для аудиту IoT-середовищ, розробки політик безпеки та планування відповідності вимогам регуляторів. Він особливо актуальний для організацій, які поєднують IoT із хмарними сервісами, промисловими мережами або великими екосистемами IoT.

Рамка відповідності (Compliance Framework) Фонду безпеки IoT (IoT Security Foundation – IoTSF) [21] розроблена як комплексна система відповідності, яка цілісно вирішує питання безпеки IoT. Фреймворк є практичним, добровільним методичним документом, який допомагає виробникам, постачальникам і операторам IoT-систем розробляти, впроваджувати та перевіряти безпечні IoT-продукти і сервіси. Головна мета Рамки відповідності – уніфікувати мінімальні вимоги до безпеки IoT, забезпечити їх перевірку й стимулювати ринок виробників і постачальників гарантувати споживачам і бізнесу належний рівень кіберстійкості.

Рамка відповідності IoTSF організована в чотири основні розділи, які визначають конкретні міркування безпеки, які повинні бути адресовані для забезпечення надійності систем IoT:

– розділ «Процес» фокусується на загальному управлінні та процесах, які повинні бути введені для ефективного управління безпекою IoT;

– розділ «Програмне забезпечення» охоплює конкретні міркування програмного забезпечення, які мають вирішальне значення для підтримки безпеки та цілісності систем IoT;

– розділ «Фізичний» охоплює фізичні аспекти пристроїв IoT, включаючи аспекти апаратного забезпечення;

– розділ «Зв'язок» окреслює міркування безпеки для зв'язку між пристроями та системами IoT.

Рамка відповідності IoTSF – це гнучкий інструмент для організацій, які прагнуть реалізувати принципи «безпечного IoT за замовчуванням» на практиці. Вона виступає містком між високорівневими політичними вимогами, технічними стандартами і реальними практиками розробки IoT-продуктів.

Стандарт кібербезпеки ЄС для споживчих пристроїв IoT ETSI EN 303 645 [22] охоплює широкий спектр споживчих пристроїв IoT, включаючи підключені дитячі іграшки, пристрої безпеки, розумні камери, телевізори, колонки, системи домашньої автоматизації та побутову техніку. ETSI EN 303 645 передбачає відсутність паролів за замовчуванням, впровадження політики розкриття уразливостей, забезпечення актуальності програмного забезпечення, захист даних споживачів. Стандарт спрямований на запобігання великомасштабним атакам на підключені споживчі пристрої, встановлюючи базовий рівень безпеки, і допомагає виробникам IoT-пристроїв вбудувати безпеку в продукти на етапі проєктування, що підвищує довіру споживачів та знижує ризики, пов'язані з вразливостями. Стандарт ETSI EN 303 645 не є обов'язковим згідно із законом, але його дотримання вважається важливим для виробників, що працюють на європейському ринку. Потенційно, ETSI EN 303 645 може бути основою для майбутніх схем сертифікації IoT, що підтверджують відповідність пристроїв вимогам безпеки.

Комплексну методологічну основу для побудови надійної системи управління інформаційною безпекою та конфіденційністю в IoT-середовищах забезпечують міжнародні стандарти ISO/IEC 27001 і ISO/IEC 27701.

Стандарт ISO/IEC 27001 [23] визначає вимоги до побудови, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою. Він встановлює рамкові умови для управління ризиками безпеки інформації незалежно від сфери застосуванняі може бути адаптований до IoT-середовищ. У цьому контексті ключову роль відіграє проведення комплексної оцінки ризиків, ідентифікація активів IoT

як об'єктів захисту та впровадження відповідних політик контролю доступу, шифрування, а також моніторингу та реагування на інциденти. Особливої уваги набувають питання захисту мережевої інфраструктури, автентифікації пристроїв і забезпечення цілісності даних, що передаються в IoT-середовищі.

Доповненням до ISO/IEC 27001 є стандарт ISO/IEC 27701 [24], який фокусується на управлінні конфіденційністю інформації та персональних даних. Цей стандарт розширює вимоги системи управління інформаційною безпекою до системи управління конфіденційністю інформації та пропонує конкретні механізми для дотримання законодавства у сфері захисту даних, таких як Загальний регламент ЄС про захист даних (GDPR). У випадку IoT це має критичне значення, оскільки такі системи часто обробляють великі обсяги даних про користувачів, їхню поведінку та фізичне середовище. Стандарт ISO/IEC 27701 передбачає запровадження процедур інформованої згоди, обмеження цілей обробки даних, мінімізації обсягів збору інформації та управління доступом до персональних даних.

Застосування цих стандартів у сфері IoT сприяє формуванню структурованих та прозорих процесів управління безпекою й конфіденційністю. Це особливо актуально для критичних галузей, таких як охорона здоров'я, транспорт, енергетика, де компрометація IoT-пристроїв може мати серйозні наслідки не лише для бізнесу, а й для безпеки людей. Імплементація ISO/IEC 27001 та ISO/IEC 27701 дозволяє організаціям формалізувати підходи до оцінки ризиків, впроваджувати технічні та організаційні заходи захисту, а також документувати відповідність нормативним вимогам.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Швидке поширення Інтернету речей відкриває значні можливості, але також створює серйозні проблеми, особливо у сферах безпеки, конфіденційності та операційної надійності. Існує широкий спектр проблем, починаючи від економічних бар'єрів та технічних складнощів, закінчуючи соціальними та регуляторними викликами. Для ефективного вирішення цих проблем необхідний комплексний підхід, що включає впровадження передових технологічних рішень, дотримання найкращих практик безпеки, використання існуючих фреймворків та стандартів, а також постійне навчання користувачів. Надійні механізми автентифікації, наскрізне шифрування даних, безпечні оновлення програмного забезпечення та сегментація мережі є критично важливими для забезпечення безпеки екосистеми IoT. Захист конфіденційності користувачів вимагає мінімізації даних, анонімізації та прозорого управління згодою відповідно до чинних правил. Забезпечення операційної ефективності та надійності передбачає стандартизацію, масштабованість, ефективне управління даними та надійне підключення.

Майбутнє безпеки та надійності IoT залежить від безперервних інновацій, тісної співпраці між галузевими гравцями та розробки глобальних стандартів. Лише спільними зусиллями в правовому полі можливо створити безпечну та надійну екосистему IoT, яка повністю реалізує свій трансформаційний потенціал.

Література

1. Франів І.А. Переваги впровадження IoT для автоматизації процесів у продуктовому ритейлі / І.А. Франів, П.П. Єременко // Вісник ЛТЕУ. Економічні науки. – 2024. – № 80. – С. 49–55.
2. Назаренко Н. Співпраця індустрії 4.0 та інтернету речей IoT / Н. Назаренко, С. Заєць, Ю. Киричук // Вісник Хмельницького національного університету. Технічні науки. – 2024. – № 5(*341*). – С. 74–79.
3. Шпак О. Розумні міста та Інтернет речей: вплив розробок у сфері IT на розвиток міст і покращення якості життя / О. Шпак, П. Федорка, М. Пригара // Сучасний стан наукових досліджень та технологій в промисловості. – 2023. – №3 (25). – С. 114–128.
4. Макаренко М.В. Особливості впровадження технологій інтернету речей у сфері охорони здоров'я / М.В. Макаренко // Вчені записки ТНУ імені В.І. Вернадського. Серія: Державне управління. – 2021. – № 2. – С. 64-68.
5. IoT в охороні здоров'я: Застосування, переваги та виклики у 2023 році [Електронний ресурс] // Stfalcon.com. – Режим доступу: https://stfalcon.com/uk/blog/post/iot-in-healthcare-benefits-challenges (Дата звернення: 13.06.2025). – Назва з екрана.
6. What are the emerging threats and challenges in securing Internet of Things (IoT) devices and networks? [Electronic resource] // ResearchGate. – Access mode: https://surl.li/rzzluj (Accessed: 13.06.2025). – Screen Title.
7. Top IoT security issues and solutions for low-power devices [Electronic resource] // Onomondo. – Access mode: https://onomondo.com/blog/iot-security-issues-and-solutions-low-power-devices/ (Accessed: 13.06.2025). – Screen Title.
8. Очеретний С.О. Системи виявлення та запобігання вторгнень, найбільш успішні практики / С.О. Очеретний, В.Г. Крижановський // Прикладні аспекти сучасних міждисциплінарних досліджень. – 2024. – С. 236-238.
9. Журило О. Огляд рішень з апаратної безпеки кінцевих пристроїв туманних обчислень у інтернеті речей / О. Журило, О. Ляшенко, К. Аветісова // Сучасний стан наукових досліджень та технологій в

промисловості. – 2023. – № 1 (23). – С. 57-81.

10. Serebriakov R. Integration of blockchain technology into the Internet of Things (overview) / R. Serebriakov, V. Tkachenko, I. Klymenko // Information, Computing and Intelligent systems. – 2024. – № 4. – P. 99-113.

11. Делембовський М.М. Аналіз сучасних наукових публікацій за напрямком тематики кібербезпеки IoT технологій / М.М. Делембовський, Б.В. Корнійчук // Грааль науки. – 2023. – № 25. – С. 203-206.

12. Code of Practice for Consumer IoT Security. – Government of the United Kingdom: Department for Digital, Culture, Media & Sport, 2018. – 20 p.

13. IoT Cybersecurity Improvement Act of 2020 [Electronic resource] // CONGRESS.GOV. – Access mode: https://www.congress.gov/bill/116th-congress/house-bill/1668/text (Accessed: 13.06.2025). – Screen Title.

14. SP 800-213 Series [Electronic resource] // NIST. – Access mode: https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/sp-800-213-series (Accessed: 13.06.2025). – Screen Title.

15. NIST SP 800-213: IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements [Electronic resource] // NIST. – Access mode: https://csrc.nist.rip/Pubs/sp/800/213/Final (Accessed: 13.06.2025). – Screen Title.

16. NISTIR 8259 Series [Electronic resource] // NIST. – Access mode: https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/nistir-8259-series (Accessed: 13.06.2025). – Screen Title.

17. NISTIR 8259: Foundational Cybersecurity Activities for IoT Device Manufacturers. National Institute of Standards and Technology Interagency or Internal Report 8259. – U.S. Department of Commerce: National Institute of Standards and Technology (NIST). – 2020. – 36 p.

18. NISTIR 8259A: IoT Device Cybersecurity Capability Core Baseline. National Institute of Standards and Technology Interagency or Internal Report 8259A. – U.S. Department of Commerce: National Institute of Standards and Technology (NIST). – 2020. – 23 p.

19. Draft NISTIR 8259B: IoT Non-Technical Supporting Capability Core Baseline. National Institute of Standards and Technology Interagency or Internal Report 8259B. – U.S. Department of Commerce: National Institute of Standards and Technology (NIST). – 2020. – 20 p.

20. CSA IoT Security Controls Framework v2 [Electronic resource] // Cloud Security Alliance. – Access mode: https://cloudsecurityalliance.org/artifacts/csa-iot-security-controls-framework-v2 (Accessed: 13.06.2025). – Screen Title.

21. Understanding IoT Security: Threats, Standards & Best Practices [Electronic resource] – Access mode: https://sternumiot.com/iot-blog/understanding-iot-security-challenges-standards-and-best-practices/ (Accessed: 13.06.2025). – Screen Title.

22. ETSI EN 303 645. Cyber Security for Consumer Internet of Things: Baseline Requirements. – ETSI. – 2024. – 41 p.

23. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements [Electronic resource] // ISO. – Access mode: https://www.iso.org/standard/27001 (Accessed: 13.06.2025). – Screen Title.

24. ISO/IEC 27701:2019 Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines [Electronic resource] // ISO. – Access mode: https://www.iso.org/standard/71670.html (Accessed: 13.06.2025). – Screen Title.

References

1. Franiv I.A. Perevahy vprovadzhennia IoT dlia avtomatyzatsii protsesiv u produktovomu ryteili / I.A. Franiv, P.P. Yeremenko // Visnyk LTEU. Ekonomichni nauky. – 2024. – № 80. – S. 49–55.

2. Nazarenko N. Spivpratsia industrii 4.0 ta internetu rechei IoT / N. Nazarenko, S. Zaiets, Yu. Kyrychuk // Herald of Khmelnytskyi National University. Technical Sciences. – 2024. – № 5(341). – S. 74–79.

3. Shpak O. Rozumni mista ta Internet rechei: vplyv rozrobok u sferi IT na rozvytok mist i pokrashchennia yakosti zhyttia / O. Shpak, P. Fedorka, M. Pryhara // Suchasnyi stan naukovykh doslidzhen ta tekhnolohii v promyslovosti. – 2023. – №3 (25). – S. 114–128.

4. Makarenko M.V. Osoblyvosti vprovadzhennia tekhnolohii internetu rechei u sferi okhorony zdorovia / M.V. Makarenko // Vcheni zapysky TNU imeni V.I. Vernadskoho. Seriia: Derzhavne upravlinnia. – 2021. – № 2. – S. 64-68.

5. IoT v okhoroni zdorovia: Zastosuvannia, perevahy ta vyklyky u 2023 rotsi [Elektronnyi resurs] // Stfalcon.com. – Rezhym dostupu: https://stfalcon.com/uk/blog/post/iot-in-healthcare-benefits-challenges (Data zvernennia: 13.06.2025). – Nazva z ekrana.

6. What are the emerging threats and challenges in securing Internet of Things (IoT) devices and networks? [Electronic resource] // ResearchGate. – Access mode: https://surl.li/rzzluj (Accessed: 13.06.2025). – Screen Title.

7. Top IoT security issues and solutions for low-power devices [Electronic resource] // Onomondo. – Access mode: https://onomondo.com/blog/iot-security-issues-and-solutions-low-power-devices/ (Accessed: 13.06.2025). – Screen Title.

8. Ocheretnyi S.O. Systemy vyiavlennia ta zapobihannia vtorhnen, naibilsh uspishni praktyky / S.O. Ocheretnyi, V.H. Kryzhanovskyi // Prykladni aspekty suchasnykh mizhdystsyplinarnykh doslidzhen. – 2024. – C. 236-238.

9. Zhurylo O. Ohliad rishen z aparatnoi bezpeky kintsevykh prystroiv tumannykh obchyslen u interneti rechei / O. Zhurylo, O. Liashenko, K. Avetisova // Suchasnyi stan naukovykh doslidzhen ta tekhnolohii v promyslovosti. – 2023. – № 1 (23). – S. 57-81.

10. Serebriakov R. Integration of blockchain technology into the Internet of Things (overview) / R. Serebriakov, V. Tkachenko, I. Klymenko // Information, Computing and Intelligent systems. – 2024. – № 4. – P. 99-113.

11. Delembovskyi M.M. Analiz suchasnykh naukovykh publikatsii za napriamkom tematyky kiberbezpeky IoT tekhnolohii / M.M. Delembovskyi, B.V. Korniichuk // Hraal nauky. – 2023. – № 25. – S. 203-206.

12. Code of Practice for Consumer IoT Security. – Government of the United Kingdom: Department for Digital, Culture, Media &

Sport, 2018. – 20 p.

13. IoT Cybersecurity Improvement Act of 2020 [Electronic resource] // CONGRESS.GOV. – Access mode: https://www.congress.gov/bill/116th-congress/house-bill/1668/text (Accessed: 13.06.2025). – Screen Title.

14. SP 800-213 Series [Electronic resource] // NIST. – Access mode: https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/sp-800-213-series (Accessed: 13.06.2025). – Screen Title.

15. NIST SP 800-213: IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements [Electronic resource] // NIST. – Access mode: https://csrc.nist.rip/Pubs/sp/800/213/Final (Accessed: 13.06.2025). – Screen Title.

16. NISTIR 8259 Series [Electronic resource] // NIST. – Access mode: https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/nistir-8259-series (Accessed: 13.06.2025). – Screen Title.

17. NISTIR 8259: Foundational Cybersecurity Activities for IoT Device Manufacturers. National Institute of Standards and Technology Interagency or Internal Report 8259. – U.S. Department of Commerce: National Institute of Standards and Technology (NIST). – 2020. – 36 p.

18. NISTIR 8259A: IoT Device Cybersecurity Capability Core Baseline. National Institute of Standards and Technology Interagency or Internal Report 8259A. – U.S. Department of Commerce: National Institute of Standards and Technology (NIST). – 2020. – 23 p.

19. Draft NISTIR 8259B: IoT Non-Technical Supporting Capability Core Baseline. National Institute of Standards and Technology Interagency or Internal Report 8259B. – U.S. Department of Commerce: National Institute of Standards and Technology (NIST). – 2020. – 20 p.

20. CSA IoT Security Controls Framework v2 [Electronic resource] // Cloud Security Alliance. – Access mode: https://cloudsecurityalliance.org/artifacts/csa-iot-security-controls-framework-v2 (Accessed: 13.06.2025). – Screen Title.

21. Understanding IoT Security: Threats, Standards & Best Practices [Electronic resource] – Access mode: https://sternumiot.com/iot-blog/understanding-iot-security-challenges-standards-and-best-practices/ (Accessed: 13.06.2025). – Screen Title.

22. ETSI EN 303 645. Cyber Security for Consumer Internet of Things: Baseline Requirements. – ETSI. – 2024. – 41 p.

23. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements [Electronic resource] // ISO. – Access mode: https://www.iso.org/standard/27001 (Accessed: 13.06.2025). – Screen Title.

24. ISO/IEC 27701:2019 Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines [Electronic resource] // ISO. – Access mode: https://www.iso.org/standard/71670.html (Accessed: 13.06.2025). – Screen Title.