УДК 342.9:5.08 DOI: https://doi.org/10.32631/pb.2025.1.05

ПЕТРО СЕРГІЙОВИЧ КЛІМУШИН,
Харківський національний університет внутрішніх справ,
навчально-науковий інститут № 4,
кафедра протидії кіберзлочинності;
https://orcid.org/0000-0002-1020-9399,
e-mail: klimushyn@ukr.net

ПРОБЛЕМНІ АСПЕКТИ СТАНДАРТИЗАЦІЇ КІБЕРБЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ

Популярність пристроїв Інтернету речей набуває інтересу серед споживачів. Зростання кількості користувачів, які отримують користь від пристроїв, а також активне використання технологій середовищ Інтернету речей підвищують ризик кібератак. Інтернет речей є важливим перехрестям для різних технологій. Це дозволяє підключати розумні фізичні пристрої та забезпечити розумне ухвалення рішень у широкому діапазоні програм. Різні пристрої – від комп'ютерів до виконавчих механізмів і датчиків – можуть з'єднуватися між собою та обмінюватися даними в мережевому середовищі. Оскільки пропозиція розумних об'єктів на ринку зростає, питання їхньої безпеки набуває дедалі більшого значення.

Основна проблема пристроїв Інтернету речей пов'язана з конфіденційністю та безпекою. Адміністрування великої кількості даних для надійної та безпечної обробки є справжнім викликом. Крім того, постають питання захисту, безпеки та конфіденційності користувачів.

Кібербезпека та конфіденційність користувачів Інтернету речей можуть негативно вплинути на розвиток цих технологій у разі використання вразливих пристроїв та їхніх середовищ. Отже, постає проблема інформаційного захисту пристроїв Інтернету речей. Для її вирішення розроблено велику кількість технологій та стандартів кібербезпеки. Крім того, існує значний перелік важливих вимог для захисту пристроїв Інтернету речей від кібератак. Усе це зумовлює потребу в аналізі ефективності цих програм і сфер їхнього застосування для забезпечення кібербезпеки середовищ Інтернету речей.

Для успішної роботи таких програм необхідно визначити характеристики середовищ Інтернету речей. Стандарти безпеки, передові технології вирішення проблем безпеки, застосунки з аналізу поточної структури безпеки формують дослідницьку таксономію Інтернету речей.

Стаття є більш комплексним дослідженням порівняно з багатьма попередніми роботами, присвяченими кібербезпеці Інтернету речей. У ній проаналізовано проблемні аспекти стандартизації, пов'язані з кібербезпекою Інтернету речей, а також досліджено діяльність міжнародних організацій у цій сфері.

Ключові слова: *технології Інтернету речей, виклики безпеки, організації стандартизації, стандарти безпеки, сертифікати безпеки, керування доступом до Інтернету речей.*

Оглядова стаття

ВСТУП. З розвитком технологій Інтернету речей (*Internet of Things*, далі – IoT), де розумні пристрої, які збирають дані, передають інформацію один одному, спільно її обробляють та виконують дії автоматично (AboBakr, Azer, 2018), виникає нова парадигма забезпечення їхнього безпечного функціонування. Широкий спектр технологій працює спільно, щоб об'єднувати речі чи пристрої в програмах IoT. Інтернет речей здійснює трансформаційний контроль над тим, як люди живуть у світі та працюють у багатьох сферах, зокрема у сфері підключеного транспорту, розумних міст, електронної охорони здоров'я, енергетичного менеджменту, домашньої автоматизації, управління промисловими процесами та громадської безпеки. Ця парадигма стала головною проблемою та найскладнішим завданням для протистояння зростанню IoT (Belkeziz, Jarir, 2020). Проблеми безпеки та конфіденційності (Virat et al., 2018; Bhardwaj, Kumar, 2021) пов'язані з процесами адаптації стандартизації та регулювання до потреб IoT. Деякі з них охоплюють складність створення безпечного та захищеного зв'язку (Alhalafi, Veeraraghavan, 2019).

Отже, дослідження, пов'язані з аналізом технологій та стандартів безпеки IoT, є дуже важливими для вирішення цих проблем, особливо на глобальному рівні (Brass et al., 2018).

Стандарти технологій та платформи, орієнтовані на екосистему IoT, розробляються стрімкими темпами й охоплюють широкий спектр застосувань. Проте нинішній стан стандартизації IoT свідчить про відсутність універсального стандарту безпеки.

У цій статті представлено комплексний аналіз технологій і сучасних стандартів безпеки, що розробляються для різних рівнів архітектури IoT, зокрема рівня керування доступом до середовища, мережевого рівня та рівня сеансу.

МЕТА І ЗАВДАННЯ ДОСЛІДЖЕННЯ. *Метою* статті є визначення перспективних захищених технологій середовищ IoT та стандартів кібербезпеки в багаторівневій системі взаємодії пристроїв IoT на основі позитивного світового досвіду.

Для досягнення вказаної мети були поставлені такі *завдання*:

– розглянути особливості використання безпечних технологій у середовищах IoT;

– визначити безпечні технології системи для підтримки IoT на основі туманних та хмарних обчислень;

– окреслити проблеми стандартизації кібербезпеки середовищ IoT, а також провідні міжнародні інституції, консорціуми, глобальні системи, фонди, проєкти та альянси, що займаються розробленням і впровадженням стандартів безпеки;

– надати класифікацію вимог безпеки IoT за п’ятьма категоріями: безпека мережі, керування ідентифікацією, конфіденційність, довіра та стійкість;

– надати потенційні рішення захисту інтелектуальних середовищ на основі IoT для забезпечення безперервності та стабільності послуг у майбутньому розгортанні.

ОГЛЯД ЛІТЕРАТУРИ. Усю сукупність наукових досліджень зі стандартизації кібербезпеки IoT можна розділити на три групи (Tournier et al., 2021): зосереджені на унікальному стандарті, зосереджені на безпеці конкретного рівня архітектури IoT і ті, які охоплюють системи IoT у повному обсязі.

Перша група досліджень присвячена безпеці унікального стеку стандартів, наприклад малопотужних бездротових персональних мереж. Ці дослідження не дозволили читачеві порівняти стандарти або отримати абстрактне уявлення про фундаментальні характеристики IoT (Sain, Kang, Lee, 2017).

Друга група досліджень охоплює проблему порівняння стандартів, проте кожне з них зосереджувалося лише на окремому рівні архітектури, такому як канал передачі даних (MAC), мережевий або сеансовий рівень. Вони не досліджували й не давали читачеві змоги зрозуміти захищену взаємодію між рівнями. Отже, для забезпечення повного розуміння технологій і стандартів IoT необхідно описати та проаналізувати всі рівні архітектури (Lounis, Zulkernine, 2020).

Нарешті, третя група досліджень представила глобальний погляд на безпеку та пов’язані з нею проблеми в IoT. Нещодавно опублікований стандарт ETSI EN 303 645[1] кібербезпеки для споживчого Інтернету речей (*Cyber Security for Consumer Internet of Things*, далі – CSCIoT) є глобальним стандартом, який описує вимоги щодо впровадження мінімального рівня безпеки для пристроїв IoT (Ammar, Russello, Crispo, 2018).

Ознайомлення зі стандартом CSCIoT показує, що існує значна різниця між стандартами безпеки пристроїв IoT для споживачів і стандартами безпеки пристроїв IoT для підприємств. Ця різниця переважно полягає у відсутності градації та кількості вимог CSCIoT.

Наведені наукові дослідження безпеки IoT мають абстрактний характер і не повною мірою висвітлюють проблеми стандартизації кібербезпеки IoT. Крім того, існує деяка плутанина між технологіями та стандартами на фізичному рівні пристроїв IoT (Mendez, Papapanagiotou, Yang, 2018).

Кілька оглядових робіт, пов’язаних із безпекою IoT, досліджують традиційні методи безпеки мережі з урахуванням обмеженості ресурсів IoT-пристроїв та аналізують міжнародні стандарти й проблеми, пов’язані безпекою середовищ IoT (Lee et al., 2021; Karie et al., 2021); висвітлюють застосування технологій IoT та поглиблено аналізують комунікаційні протоколи IoT із детальною технічною інформацією про їхні стеки, обмеження та застосування (Choudhary, Meena, 2022; Mansour et al., 2023); аналізують вимоги безпеки для бездротових сенсорних мереж, які є основними елементами мереж IoT (Yu et al., 2020); проводять комплексний огляд IoT, включаючи архітектуру системи, передові технології, проблеми безпеки та конфіденційності, а також інтеграцію туманних обчислень та їхніх застосунків (Lin et al., 2017); надають теоретичні, методологічні та технічні рекомендації щодо контролю доступу до IoT (Qiu et al., 2020);

[1] ETSI EN 303 645 V2.1.1 (2020-06). Cyber Security for Consumer Internet of Things: Baseline Requirements // ETSI : сайт. URL: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf (дата звернення: 07.01.2025).

вивчають безпеку даних в IoT і запроваджують архітектурний підхід до аналізу його безпеки IoT (Hou, Qu, Shi, 2019); досліджують міжнародні організації стандартизації та надають стандарти безпеки IoT (Hwang, Kim, 2017).

Аналіз наведених оглядових робіт показує, що вони зосередженні на наявних технологіях безпеки, а опитувань щодо стандартів безпеки доволі мало. Крім того, питання технологій та стандартів безпеки повинні розглядаються у взаємозв'язку, а не окремо. У цьому дослідженні проведено огляд літератури та комплексно проаналізовано технології і стандарти для забезпечення кібербезпеки середовищ IoT, включаючи архітектуру системи, передові технології, проблеми безпеки та конфіденційності, а також інтеграцію хмарних і туманних обчислень та їхніх застосунків.

МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ. Методологія дослідження ґрунтується на основі аналізу значного обсягу літературних даних і класифікується за трьома етапами: планування, проведення аналізу та звітування (Клімушин, Рог, Колісник, 2023).

Етап планування описує критерії вибору матеріалу шляхом вивчення анотацій, вступів та висновків різних наукових статей. Відбираються лише ті дослідницькі статті, які відповідають таким критеріям: опис проблем безпеки пристроїв IoT, обговорення нових технологічних рішень щодо безпеки та конфіденційності пристроїв IoT, надання інформації про загрози IoT, презентація методів вирішення проблем кібербезпеки пристроїв IoT, провідні міжнародні системи та організації сертифікації середовищ IoT, стандарти безпеки в системі IoT, потенційні рішення захисту інтелектуальних середовищ на основі IoT для забезпечення безперервності та стабільності послуг у майбутньому розгортанні.

Основною метою цього етапу дослідження є планування відбору наявної літератури про конфіденційність даних, загрози системам IoT і технології та стандарти безпеки в них.

Критерії включення та виключення робіт визначаються на основі їхньої наукової значущості. Для пошуку необхідного матеріалу при формуванні бібліографічної бази даних використовувались цифрові бібліотеки: Academia, Science Direct, Google Scholar, Google Search, Springer, IEEE Xplore та Research Gate. Ці автоматизовані бібліотеки містять літературу, пов'язану з дисципліною кібербезпеки IoT.

Етап проведення аналізу включає три фази: 1) вибір дослідження; 2) вилучення даних та оцінювання якості; 3) вилучення та синтез даних.

Для проведення дослідження визначено такі загальні терміни, як «безпека», «конфіденційність», «стандарти безпеки», «системи сертифікації», які об'єднуються в різні ключові слова та створюють різні комбінації для пошукових термінів, пов'язаних із питаннями дослідження.

Для оцінювання якості отриманих даних використано як якісні, так і кількісні методи. Якість вибраних робіт оцінюється за переліком загальних запитань, що охоплюють: чіткість сформульованої мети та завдань дослідження; наявність авторського огляду попередніх досліджень; використання актуальних та інноваційних джерел; корисність робіт для дослідження; зрозумілість і легкість сприйняття тексту; ефективність візуальних матеріалів (таблиць, діаграм, карт, малюнків); якість процесу збору даних для підтвердження результатів та їх аналізу; детальність порівняння методик в експерименті.

Під час аналізу застосовували метод інтелектуального аналізу даних, що охоплює їхню класифікацію, кластеризацію та синтез висновків. Ще одним серйозним викликом у цій галузі є збір, зберігання та керування великою кількістю пристроїв IoT разом із пов'язаними з ними функціями.

На *етапі звітування* дається відповідь на ключові дослідницькі питання з урахуванням важливості дослідження. Стрімке зростання інтелектуальних пристроїв IoT робить технологію управління ними системним завданням внаслідок таких проблем, як-от: застаріле програмне та апаратне забезпечення, сумісність, безпека, атаки, модифікації, труднощі, пов'язані з паролями, хробаки низького рівня, факти, пов'язані з безпекою, конфіденційні провокації. Крім того, складнощі IoT також можуть виникати через ненадійний зв'язок, проблеми з визначенням ефективності пристрою, системи автоматизації для керування даними, обмежене керування пристроями IoT, підтримку мережі з низьким енергоспоживанням, операційні системи IoT і проблеми, пов'язані з процесором.

Запропонована методологія дослідження зосереджена на аналізі поведінки пристрою IoT на основі багаторівневої архітектури IoT. Цей підхід не залежить від характеристик програмного та апаратного забезпечення різних пристроїв IoT і дає змогу проводити систематизоване оцінювання наявних стандартів. Методологію можна застосовувати на будь-яких пристроях IoT, які використовують канал зв'язку для надсилання або отримання даних. Крім того, методологія особливо стосується пристроїв, які використовують IP-з'єднання і через це є вразливими до віддалених атак з інтернету.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ ТА ДИСКУСІЯ. *Безпечні технології для підтримки IoT на основі туманних та хмарних обчислень*. Інтернет речей - це остання парадигма, яка охоплює потенціал підключення фізичного об'єкта до мережі Інтернет, а потім використовує хмарні обчислення (*Cloud Computing*) для збору, зберігання та обробки даних, створених цими підключеними пристроями. Щоб зменшити затримку обслуговування обчислень, процесів і зберігання в центрах хмарних обчислень, була створена парадигма туманних обчислень (*Fog Computing*), яка наближає керування даними до кінцевого пристрою або до межі мережі постачальника. Вузли туманних обчислень можуть бути не лише географічно розподіленими, а й більш динамічними за своєю природою, ніж центри хмарних обчислень, тому це робить захист даних ще складнішим.

При спільному використанні середовищ Інтернет речей – туманні обчислення – хмарні обчислення виникають юридичні, технологічні й організаційні питання відповідальності за втрату даних або порушення безпеки та інші питання конфіденційності й безпеки.

Хмарні обчислення надають безпечну платформу для зберігання та обробки даних, створених пристроями IoT. Дані, що зберігаються в центрах хмарних обчислень, зазвичай більш безпечні, ніж дані, що зберігаються на локальних пристроях IoT. Безпеку хмарних обчислень як послугу можна класифікувати як:

1) керування ідентифікацією/автентифікацією та доступом, що включає IoT, процедури та механізми, які використовуються для нагляду за доступом до великих бізнес-активів, гарантуючи надання належного рівня доступу;

2) інформаційну безпеку, яка полягає в забезпеченні конфіденційності, цілісності й доступності інформації та охоплює організаційний, фізичний і технічний контроль;

3) безпеку мережі, яка стосується технологій, політик, людей і процедур, які захищають будь-яку комунікаційну інфраструктуру від кібератак, несанкціонованого доступу та втрати даних. Крім самої мережі, вони також захищають трафік і доступні в мережі активи як на межі мережі, так і всередині периметра. Безпека мережі охоплює напади на систему, наприклад відмову в обслуговуванні, доступність підключення, уразливість;

4) контроль вторгнень. Це система, яка відстежує мережевий трафік і шукає відомі загрози та підозрілу або зловмисну активність, щоб виявити проникнення кіберзлочинців в інфраструктуру та сформувати оповіщення безпеки;

5) систему криптографічного захисту, яка запобігає несанкціонованому доступу до конфіденційної інформації. Будь-яка програма, що працює в хмарному середовищі, не повинна мати можливість безпосередньо розшифрувати інформацію, перш ніж отримати до неї доступ. Структури шифрування зазвичай складаються з перетворень інформації, які викликають труднощі розшифрування зловмисниками або які неможливо зламати, поряд із процедурами та методологією для нагляду за шифруванням і декодуванням, хешуванням і відновленням та управлінням ключами (Wang, Yongchareon, 2020).

Використовуючи можливості хмарних обчислень для економії коштів, безпеки та керування даними, компанії можуть максимізувати потенціал своїх мереж IoT і отримати конкурентну перевагу. Туманні обчислення слугують для швидкого оброблення даних на кордоні мережі, що зменшує затримку при передачі даних, а також можуть використовуватися для захисту даних через мережу взаємозв'язку середовищ Інтернет речей – туманні обчислення – хмарні обчислення (Aazam, Zeadally, Harras, 2018).

Туманні обчислення виконують функцію шлюзу між IoT і хмарними обчисленнями, реалізуючи концепцію ефективного обслуговування при наданні послуг з обробки та захисту даних IoT (Журило, Ляшенко, Аветісова, 2023).

Для визначення складності наявних технологій забезпечення кібербезпеки IoT пропонуємо безпечну архітектуру системи для підтримки IoT на основі туманних та хмарних обчислень (рис. 1).

Оскільки розрахунки проводяться біля пристроїв за допомогою туманних обчислень, то зменшується затримка при передачі даних порівняно з обробкою на хмарному рівні. Проте пристрої IoT здебільшого є малопродуктивними, тож лише незначна кількість з них може збирати статистичні дані та надсилати їх на проксі-сервери для подальшого аналізу. Тут пропонується механізм криптографічного захисту даних на сенсорному рівні з низьким енергоспоживанням, у якому h-проксі-сервер збирає дані з h-групи пристроїв IoT, проводить початкове шифрування і передає їх на проксі-сервери.

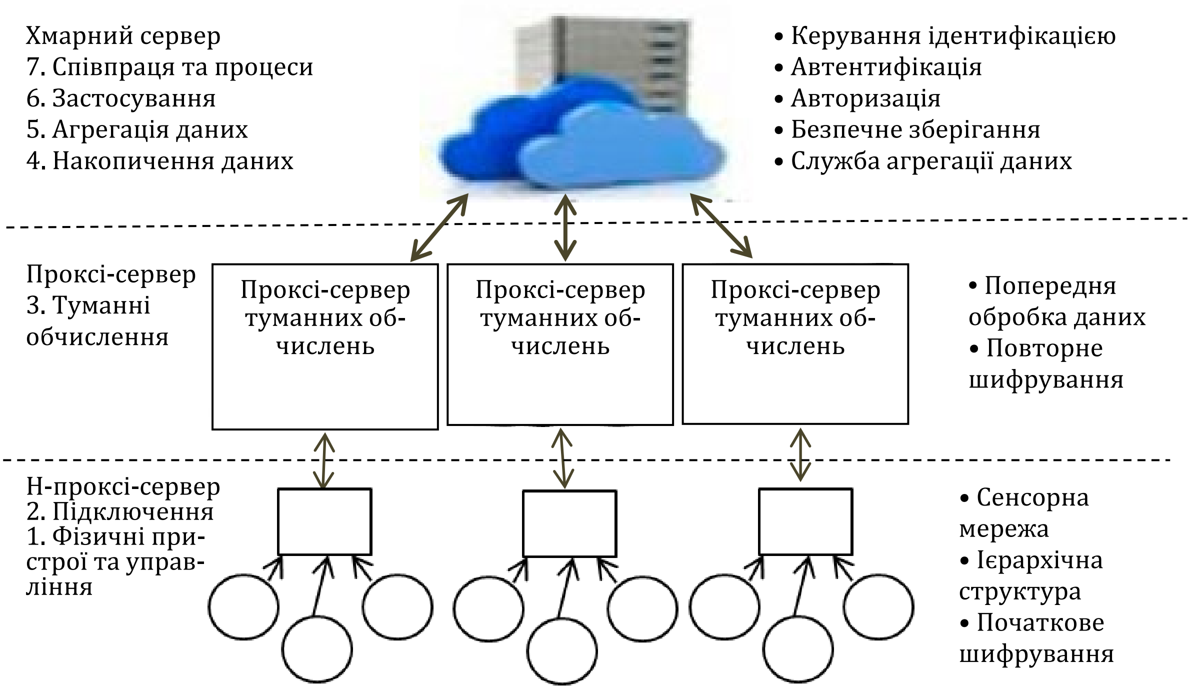

Рис. 1. Безпечна архітектура системи для підтримки IoT на основі туманних та хмарних обчислень

Архітектура туманних обчислень рухається зверху вниз, при цьому більша площа розподілу призводить до меншої затримки для кінцевих пристроїв при передачі даних (Khan at al., 2022). Тобто обчислювальні послуги на туманному рівні біля кінцевих пристроїв зменшують затримку, і сервери краще обробляють величезний трафік.

Мобільні пристрої (телефони, портативні комп'ютери, настільні комп'ютери) є переважно термінальними пристроями (Sabireen, Neelanarayanan, 2021). Сенсорні вузли також просуваються на рівнях кінцевих пристроїв. Вони можуть бути як стаціонарними, так і портативними пристроями. Сенсорні вузли на цьому рівні відчувають навколишнє середовище та створюють вміст. Ці створені дані надсилаються на базову станцію, а оброблений результат знову надсилається на цей рівень. Рівень туманних обчислень також потребує ідентифікації/автентифікації пристроїв IoT для пересилання даних.

Розроблено різні заходи безпеки для захисту мереж туманних обчислень від несприятливих впливів. Для забезпечення цілісності даних слід застосовувати систему захисту від клонування на фізичному рівні. Для підтримки надійності необхідно використовувати апаратні лічильники продуктивності. Щоб підвищити конфіденційність, варто застосовувати полегшені методи шифрування з функцією хешування.

Використання різних заходів безпеки та криптографічних алгоритмів у різних місцях споживає багато енергії. Отже, щоб зменшити енергію на різних рівнях, необхідно вибрати відповідні криптографічні алгоритми у відповідних місцях. Якщо даних небагато, їх можна обробити на рівні вузла, датчика або шлюза. Для ефективного функціонування системи необхідним є повне використання компонентів і локалізація даних, що зменшить затримки при передачі даних.

Модель контролю за допомогою доступу використовує безпечний зв'язок шляхом застосування криптографічного алгоритму. Проксі-сервер, який бажає надіслати дані іншим проксі-серверам, запитує ключові пари для безпечного обміну даними. Довірена сторона видає майстер-ключ, відкритий ключ і закритий ключ для обох сторін.

Таким чином, уся передача даних від туманних проксі-серверів до хмарного сервера зашифрована. По-перше, цільові дані шифруються майстер-ключем в одноразовому значенні. По-друге, у сеансі зв'язку між пристроями використовуються пари відкритих і закритих ключів, а алгоритми шифрування та дешифрування також безпечно розподіляються між сторонами.

За допомогою туманних обчислень можна ефективно використовувати енергію джерел розумної мережі за рахунок впровадження механізму відбору найкращих енергетичних ресурсів. Розумні мережі у пристроях IoT зазвичай фільтрують дані.

Безпечні туманні обчислення дуже важливі в галузі медицини, оскільки дані безпосередньо стосуються здоров'я людей. У цій галузі розроблено багато застосунків. Наприклад, створено програму з використанням датчиків параметрів пацієнта, які фіксують його дані та пересилають їх на сервер туманних обчислень, де вони аналізуються. Потім інформація про стан пацієнта надсилається до лікарні, у яку він був госпіталізований. При цьому дані пацієнта залишаються конфіденційними.

Загалом хмарні обчислення надають послуги для пристроїв на основі централізованого доступу до даних та інформації. У хмарних обчисленнях великий обсяг даних обробляється та передається між пристроями. У цій передачі та обробці є деякі проблеми із затримкою, неможливістю обробки в режимі реального часу та безпекою.

Туманні обчислення зменшують ці проблеми, обробляючи дані на своєму рівні та обмежуючи обсяг передачі даних до хмарних обчислень. Тобто невелика кількість даних передається на рівень хмарних обчислень, де додатково обробляється. Таким чином, затримка зменшується завдяки використанню рівня туманних обчислень. Крім того, зі збільшенням кількості кампаній для зв'язку зростає споживання енергії через збільшення обсягу передавання повідомлень між датчиками в середовищі туманних обчислень.

Відповідно до наукових прогнозів, очікується, що туманні обчислення стануть однією з основ IoT у найближчому майбутньому, трансформуючи IoT на базі хмарних обчислень у більш розподілену архітектуру (Butun, Sari, Österberg, 2020).

Водночас нові рішення проміжного програмного забезпечення на основі туманних обчислень можуть бути корисними й зручними, оскільки дозволяють обробляти термінові завдання на периферії мережі та розвантажувати вузли з обмеженими енергетичними ресурсами. Туманні обчислення можуть суттєво покращити якість обслуговування мереж IoT завдяки зменшенню затримки при передачі даних і перевантаженості мережі, одночасно збільшуючи виявлення збоїв і відновлення втрат.

Додаткові функції та компоненти іноді створюють єдину точку збою або ускладнюють роботу системи. Для покращення загальної продуктивності можна усунути єдину точку збою за рахунок перенавантаження на систему. Це стосується як апаратного, так і програмного забезпечення та функцій безпеки, пов'язаних із включенням додаткового компонента.

Таким чином, централізовані хмарні центри оброблення даних можуть виходити з ладу в процесі зберігання або оброблення запитів від мільйонів розподілених кінцевих пристроїв IoT через перевантажену мережу, високу затримку в службі, обмежену пропускну здатність тощо. Тому з метою вирішення цієї проблеми прогнозується, що дуже корисною буде концепція туманних обчислень, особливо для чутливих до затримки програм, таких як промислова автоматизація. Концепції підтримки мобільності, георозподілу, визначення місця розташування та низької затримки є важливими під час розгортання пристроїв IoT, і туманні обчислення є сильним кандидатом на допомогу в усіх цих питаннях. Запропонована безпечна архітектура системи для підтримки IoT на основі туманних та хмарних обчислень не схильна до кібератак, зламів, вторгнень, маніпуляцій за рахунок перенавантаження на систему та використання платформ безпеки IoT.

Сьогодні, за оцінкою ресурсу Глобальна мережа кібербезпеки (*Global Cyber Security Network*), серед найвідоміших платформ безпеки IoT виокремлюють такі:

– *Armis Security*. Відома тим, що забезпечує повну видимість активів і безпеку для пристроїв IoT, допомагає виявляти загрози та реагувати на них у реальному часі. Також пропонує моніторинг поведінки пристроїв у режимі реального часу, гарантуючи виявлення аномалій та їх оперативне усунення, щоб запобігти порушенням;

– *Azure Sphere (Microsoft)*. Пропонує високий рівень безпеки за допомогою наскрізного рішення, яке охоплює апаратне забезпечення та служби хмарних обчислень. *Azure Sphere* створено з кількома рівнями захисту – від захищених мікроконтролерів до спеціальної операційної системи на базі *Linux* і хмарних служб безпеки. Ця інтеграція пропонує комплексний механізм захисту, який усуває потенційні вразливості на кожному рівні стеку IoT;

– *IBM Watson IoT*. Інтегрує розширену аналітику з безпечним підключенням для забезпечення надійного захисту від кіберзагроз. Платформа може передбачати та запобігати загрозам ще до їх виникнення, а безпечна інтеграція з різними пристроями та протоколами IoT робить її універсальним рішенням для різноманітних застосувань;

– *Keyfactor*. Забезпечує безпечний зв'язок і автентифікацію пристроїв IoT за допомогою цифрових сертифікатів, пропонує автоматизоване, масштабоване рішення для керування життєвим циклом цифрових сертифікатів на мільйонах пристроїв IoT. Ця автоматизація зменшує ризик людської помилки та покращує загальну безпеку, гарантуючи, що сертифікати завжди актуальні та відповідають галузевим стандартам;

– *Symantec IoT Security*. Пропонує багаторівневий підхід до безпеки IoT із захистом на всіх пристроях, мережах і програмах. Рішення включає виявлення аномалій та безпечне оновлення мікропрограми. Аналітичні можливості *Symantec* допомагають організаціям швидко виявляти та зменшувати ризики, що робить його надійним вибором для захисту багатьох екосистем IoT від нових загроз;

– *Trustwave.* Відомий своїми комплексними заходами безпеки, допомагає компаніям зменшити ризики, пов'язані з розгортанням IoT. Послуги платформи включають виявлення загроз і реагування на них, керування вразливістю та підтримку відповідності, що забезпечує цілісний підхід до безпеки IoT.

Тенденція розвитку платформ безпеки IoT показує зростання попиту на спеціалізовані технології безпеки, які можуть гарантувати комплексний захист на кількох рівнях, включаючи пристрої, мережі, туманні та хмарні середовища. Важливим фактором, що сприяє розширенню сектору безпеки IoT, є зростання обізнаності компаній і споживачів про потенційні ризики, пов'язані з пристроями IoT. Крім того, розроблення нових застосунків IoT у різних галузях потребує індивідуальних рішень безпеки. Такі сектори, як охорона здоров'я, автомобілебудування та виробництво, інтегрують багато технологій, щоб покращити роботу та пропонувати нові послуги.

Вибір правильної платформи безпеки IoT передбачає оцінювання кількох аспектів, щоб переконатися, що вибір відповідає конкретним потребам організації. Ось деякі з них, які слід враховувати:

– функції безпеки. Шукайте платформи, які пропонують комплексні функції безпеки, зокрема шифрування, автентифікацію та виявлення загроз у реальному часі;

– масштабованість. Переконайтеся, що платформа може масштабуватися разом зі зростаючою мережею багатьох пристроїв;

– сумісність. Переконайтеся, що платформа підтримує різні пристрої та протоколи зв'язку відповідно до наявної інфраструктури;

– простота інтеграції. Рішення безпеки має легко інтегруватися в наявні системи та робочі процеси;

– підтримка постачальників. Обирайте постачальників, відомих чудовою підтримкою клієнтів і регулярними оновленнями для вирішення нових загроз.

Аналіз спеціалізованих стандартів та нормативних вимог щодо кібербезпеки IoT. Справжній потенціал ринку визначатиметься здатністю підприємств стимулювати інновації технології, які є безпечними, сумісними та захищають конфіденційність і права власності з визнаними бізнес-моделями. Для забезпечення такої безпеки на різних пристроях, що використовуються, необхідно розробити прийнятні стандарти IoT і дотримуватися їх (Клімушин, Рог, Колісник, 2023).

Стандарти є дуже важливими для забезпечення впевненості споживачів на противагу ризикам власних рішень. Вони також зменшують ризики для розробників через витрати на переробку. Поєднання ефекту мережі може значно збільшити розмір ринку послуг, програмного забезпечення та обладнання.

Важливі також стандарти для протоколів зв'язку, щоб використовувати звичайні процедури та інтерфейси кодування, а також платформи автоматизації, які зменшують перешкоди, пов'язані з різними обчислювальними платформами, операційними системами та пристроями. Багато встановлених стандартів безпеки для базових технологій також застосовуватимуться до IoT.

Водночас з'явилося багато нових спеціальних стандартів безпеки IoT як найкраща практика, що була застосована до простору. Спеціалізовані стандарти безпеки є доволі поширеними та різноманітними (Guerbouj, Gharsellaoui, Bouamama, 2019).

У розробленні ключових компонент стандартів безпеки IoT брали участь такі міжнародні організації (Lata, Kumar, 2021):

1) Європейський інститут телекомунікаційних стандартів (*European Telecommunications Standards Institute*, далі – ETSI), який став самоврядною некомерційною організацією. Інститут брав участь у розробленні стандартів, пов'язаних із такими ключовими компонентами IoT, як безпека та послідовність, інтероперабельність, масштабованість, підтримка державної політики та законодавства, прибуток від бізнесу, альтернатива, захист.

Багато стандартів, розроблених ETSI, важливі для домену IoT і орієнтовані на віртуалізацію мережевих функцій (*Network Functions Virtualization*, далі - NFV) і програмно-визначені мережі *(Software Defined Networking*, далі - SDN), які висвітлюють системні результати та ресурси;

2) Інститут інженерів з електротехніки та електроніки (*The Institute of Electrical and Electronics Engineers, IEEE*), який визначив стандарт IEEE P1915.1, що є спеціальним стандартом для підтримки безпеки для віртуалізованих середовищ. На підтримку SDN і NFV він надає структуру для створення та керування безпечними місцями SDN/NFV. Цей стандарт визначає безпечну модель прототипів, структуру, аналітику та основні елементи захисту SDN і NFV;

3) Консорціум із тестування вбудованих мікропроцесорів (*Embedded Microprocessor Benchmark Consortium, EEMBC*), що став галузевим альянсом, який покращує стандарти, щоб допомогти винахідникам систем, обираючи найкращі термінали та визначаючи характеристики енергоспоживання і продуктивності систем. Це дуже важливо для виробників IoT та всіх тих, хто залучений до обслуговування, розроблення та виробництва продуктів, пов'язаних з IoT. Він надає створений галуззю стандартизований інструмент для розробників застосунків та для аналізу впровадження безпеки IoT;

4) Глобальна система мобільного зв'язку (*Global System for Mobile Communications, GSMA*). Це дуже логічний і раціональний форум, який об'єднує все, щоб рухатися до бездротового світу. Працює на стандартах з підключенням до Wi-Fi, 3G/4G/5G і зараз працює над безпекою IoT, додатково оптимізує бездротові потоки. Глобальна система мобільного зв'язку запропонувала рекомендації щодо безпеки IoT, а також для самооцінювання безпеки IoT. Він пропонує інструкції з безпеки для підтримки екосистеми кінцевих точок, мережевих операторів і екосистеми послуг;

5) Фонд безпеки IoT, який був створений, щоб допомогти захистити IoT, прискорити впровадження та максимізувати потенційні вигоди, надаючи обізнаність і бездоганні методи безпеки для тих, хто визначає, створює та використовує системи та продукти IoT;

6) Проєкт безпеки відкритих вебзастосунків (*The Open Web Application Security Project, OWASP*), який був заснований для виявлення проблем безпеки, пов'язаних з IoT, а також для того, щоб зробити вибір найкращого рівня безпеки під час створення, вимірювання або розгортання інструментів і технологій IoT. Проєкт безпеки відкритих вебзастосунків має 10 проєктів безпеки IoT, які допоможуть в аналізі вбудованого програмного забезпечення, вразливостей IoT, зони поверхневих атак IoT, недоліків програмного забезпечення, посібників з тестування IoT, принципів безпеки IoT, інформації для спільноти, інструкцій з безпеки IoT, оцінювання інфраструктури IoT, принципів проєктування, стандартів споживача, виробників та розробників;

7) Альянс онлайн-довіри (*The Online Trust Alliance, OTA*), який був заснований у 2005 році з метою навчати користувачів, розробляти та вдосконалювати найкращі практики й інструменти для підвищення безпеки, конфіденційності та ідентифікації користувачів. Управління довірою та ідентифікацією є двома дуже важливими аспектами онлайн-середовища (Kumar, Pradhan, 2020). Альянс онлайн-довіри робить це завдяки обміну даними та співпраці через робочі групи, комітети і навчання. Альянс також є членом інших організацій, які займаються співробітництвом, правоохоронною діяльністю та обміном даними;

8) Альянс безпечних технологій, який став міжгалузевою асоціацією, що також називається Альянсом смарт-карток і була створена в березні 2017 року. Його зусилля спрямовані на впровадження, розуміння та поширення застосування для цілей безпеки з технологією вбудованих мікросхем, смарт-карт, а також підключення обладнання та програмного забезпечення. Він містить захищені інструменти і технології для підтримки верифікації й підтвердження, бізнесу та IoT для забезпечення конфіденційності даних;

9) Альянс хмарної безпеки (*Cloud Security Alliance, CSA*). Це провідна асоціація, яка займається описом і підвищенням обізнаності про максимальну кількість спостережень з метою безпеки хмарних обчислень. Безпека є загальновизнаною проблемою для середовища хмарних обчислень і вимагає регуляторного втручання (Singh, Kumar, 2021). Альянс пропонує спеціальні дослідження безпеки хмари, дій, сертифікації, освіти та продуктів з акцентом на IoT;

10) Я кавалерія (*I am the Cavalry*). Ця організація була створена в 2013 році з метою роботи над проблемами, пов'язаними з комп'ютерною та громадською безпекою. В основному це некомерційна освітня організація, яка може відігравати важливу роль у визначенні технологій IoT та їх можливого впливу на захист суспільства та життя людей. Це здійснюється кількома способами, включаючи освіту, поширення інформації та дослідження;

11) Національний інститут стандартів і технологій (*The National Institute of Standards and Technologies, NIST*), який є лабораторним агентством Міністерства торгівлі США. Громадська робоча група з кіберфізичних систем

(*Cyber-Physical Systems Public Working Group, CPS PWG*) Інституту зосереджується на кіберфізичних або інтелектуальних системах, що сприяють підвищенню ефективності та забезпечують зв'язок між фізичним світом і комп'ютерними мережами. Інститут прагне сприяти розробкам, які відновлюють якість життя, з тими, хто займається адаптованою охороною здоров'я, контролем потоку транспорту, відновленням і реагуванням на катастрофи, а також виробництвом і постачанням електроенергії. Це охоплює багато випадків використання IoT і включає мову згоди й еталонний структурний дизайн для підтримки сумісності систем і елементів, а також стимулювання взаємодії в масштабі кіберфізичних систем. Планування, надійність, безпека, сумісність даних обговорюються на основі пріоритетних принципів проєктування для підтримки кіберфізичних систем.

Інститут оприлюднив рекомендації NISTIR 7628 зі звітом у трьох томах. Це охопило стандарт і рекомендації щодо підтримки кібербезпеки інтелектуальної мережі, що пропонує аналітичний контекст, здатний покращити операційну політику кібербезпеки залежно від конкретних ризиків, характеристик і вразливостей. Тут пропонуються методи та допоміжна інформація, яка слугує керівництвом для вимірювання ризику та класифікації відповідних вимог безпеки. Ця техніка визначає, що електрична мережа рухається після відносно закритої системи до складної системи, добре пов'язаного середовища, яке включає елементи IoT, і підтримує використання вимог кібербезпеки, які також змінюються відповідно.

Крім того, публікація Інституту «SP 800-160 Інженерія безпеки систем» (*Systems Security Engineering*) розглядає IoT з інженерної точки зору та рукописів, необхідних для розроблення більш захищених і стійких систем, включаючи машинні, людські та фізичні компоненти;

12) Міжнародна електротехнічна комісія (*The International Electro-Technical Commission, IEC*), яка розробила стандарт IEC 62443 для забезпечення кібербезпеки промислових систем керування, який є найбільш поширеним стандартом промислової безпеки в усьому світі, він продовжує розвиватися, особливо в таких сферах, як IoT;

13) Північноамериканська корпорація електричної надійності (*The North American Electric Reliability Corporation, NERC*), яка запровадила правила захисту критичної інфраструктури для масової електроенергії в Північній Америці. Корпорація вимагає дотримання законодавства, зокрема щодо кібербезпеки;

14) Всесвітня рада IoT, яка є членською організацією для нових бізнес-лідерів галузі IoT. Її діяльність зосереджена на даних і безпеці IoT;

15) Цільова дослідницька група інтернету (*The Internet Research Task Force, IRTF*), яка розробила норми, пов'язані з автентифікацією та авторизацією для обмежених середовищ IoT;

16) Індустріальний інтернет-консорціум (*The Industrial Internet Consortium, IIC*), який розробив стандарт з фокусом на промисловість і створив спеціальну структуру кібербезпеки для IoT;

17) Фонд безпеки IoT, який був створений для підтримки безпеки IoT. Він допомагає стимулювати обізнаність та ідеальну підготовку відповідних механізмів безпеки для ідентифікації, створення й використання систем і продуктів IoT;

18) Федеральна торгова комісія США (*US Federal Trade Commission, FTC*), яка є головним регуляторним органом у Сполучених Штатах Америки, відповідальним за безпеку IoT. Комісія наголошує на проблемах безпеки IoT, які впливають на захист населення та критичної інфраструктури;

19) Міжнародна організація стандартів (*International Standards Organization, ISO*), яка розробила п'ять стандартів із кібербезпеки для забезпечення безпеки в кіберпросторі загалом (Brass et al., 2018), а саме:

– Стандарт ISO/IEC 27001, який визначає найкращий досвід підтримки систем управління інформаційною безпекою. Він пропонує точні та всеосяжні вимоги щодо підтримки захисту й збереження даних та інформації за стандартами конфіденційності, надійності й доступності. Стандарт визначає набір найкращих практичних засобів контролю для застосування та відповідає найголовнішим вимогам додаткових стандартів і нормативних актів, пов'язаних із кібербезпекою;

– Стандарт ISO/IEC 27032, який особливу увагу приділяє кібербезпеці і визначає вектори, від яких залежать кібератаки, включаючи ті, які створюють зовнішній кіберпростір або інтернет. Крім того, він містить правила щодо захисту інформації за межами асоціації, наприклад піклується про співпрацю або поширення інформації серед клієнтів і постачальників;

– Стандарт ISO/IEC 27035, який фокусується на управлінні подіями. Процедури управління подіями є першим ключовим етапом кібергнучкості. Схеми управління кібербезпекою вважаються безпечними за умови швидкого й ефективного реагування. Вони також передбачають поточний контроль під час розслідування інциденту та зменшують ризик його повторного виникнення;

– Стандарт ISO/IEC 27031, який зосереджений на готовності інформаційно-комунікаційних технологій до комерційної безперервності. Стандарт дозволяє уникнути перетворення нестримної події на ризик безперервності інформаційно-комунікаційних технологій. Він пропускає порушення між самою подією та загальною безперервністю бізнесу, а також обробляє життєву важливу ланку в серії кібернетичного опору;

– Стандарт ISO/IEC 22301 забезпечує підтримку систем управління безперервністю бізнесу і процедури кібервідмовостійкості. Цей стандарт зосереджується на виявленні загроз і підтримці доступу до засобів захисту інформації в разі критичних подій. Він також сприяє відновленню та завершенню захищених функцій.

Таким чином, з розвитком технологій IoT постійно прогресують стандарти безпеки. Багато організацій працюють по всьому світу, щоб розробити надійні стандарти та безпечні технології для роботи. Інтероперабельність між технологіями є ще однією проблемою, до якої потрібно підійти дуже серйозно. Станом на сьогодні стандарти та правила безпеки IoT встановлюються міжнародними організаціями стандартизації, а також міжнародними галузевими асоціаціями та альянсами. Крім того, багато країн визнали проблему інтероперабельності пріоритетною і повідомили про відповідність нормативним вимогам для постачальників і пристроїв IoT.

Запровадження IoT, підключених до хмарних і туманних середовищ, є важливим для України у створенні мінімальних стандартів кібербезпеки, особливо для тих, що перебувають у власності та під контролем уряду.

Ухвалений Закон України «Про хмарні послуги»[1] тільки визначає правові відносини, пов'язані з обробкою та захистом даних при використанні технології хмарних обчислень, наданні хмарних послуг та особливостей їхнього використання в публічному секторі. Однак проблеми правового регулювання хмарних технологій в економіці України наразі не отримали належного висвітлення.

Потрібно, щоб Україна розширила свою участь у глобальному процесі стандартизації у сфері мереж IoT, щоб врахувати варіанти використання та потреби українців. Участь у роботі міжнародних організацій зі стандартизації мереж IoT з боку українських наукових організацій сьогодні є незначною через відсутність фінансування міжнародних програм, що призводить до технологічного відставання у використанні мереж IoT, втрати компетенції та міжнародного статусу України як технологічного партнера.

ВИСНОВКИ. Представлено систематичний огляд літератури та надано комплексний аналіз технологій і стандартів для забезпечення кібербезпеки середовищ IoT, включаючи архітектуру системи, передові технології, проблеми безпеки та конфіденційності.

Запропонована безпечна архітектура системи для підтримки IoT на основі туманних та хмарних обчислень не схильна до кібератак, зломів, вторгнень, маніпуляцій за рахунок перенавантаження на систему та використання платформ безпеки IoT. Особливістю такої архітектури є визначення компромісних рішень щодо збору та обробки даних пристроїв IoT між розподіленими та централізованими серверами. Причому на рівні розподілених серверів визначено ієрархічну структуру у вигляді проксі-серверів туманних обчислень та h-проксі-серверів на рівні h-групи пристроїв IoT. Запропоновано безпечний механізм збору інформації з низьким енергоспоживанням, у якому h-проксі-сервер збирає дані з h-групи пристроїв і передає їх на проксі-сервери. Така організація захищає IoT на початковому фізичному рівні за допомогою криптографічного захисту інформації.

Туманні обчислення зменшують проблеми хмарних обчислень, обмежуючи обсяг передачі даних на хмарний рівень, зменшуючи затримку в їх обробці, та трансформують мережу IoT на основі хмарних обчислень у більш розподілену архітектуру. Тенденція розвитку платформ безпеки IoT показує зростання попиту на спеціалізовані технології безпеки IoT, які можуть забезпечити комплексний захист на кількох рівнях.

Аналіз сфери стандартизації IoT показав, що з'явилося багато нових спеціалізованих стандартів безпеки як найкраща практика. Сьогодні існує 80 стандартів безпеки ISO/IEC, 32 стандарти ETSI та 37 різних традиційних структур безпеки, які містять 7 спеціальних публікацій NIST про методи безпеки. Це дозволило класифікувати вимоги безпеки IoT за п'ятьма категоріями: безпека мережі, керування

[1] Про хмарні послуги : Закон України від 17.02.2022 № 2075-IX // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2075-20 (дата звернення: 07.01.2025).

ідентифікацією/автентифікацією, конфіденційність, довіра та стійкість.

Найкращими практиками безпеки IoT є впровадження безпечних механізмів завантаження та оновлення мікропрограми, надійних механізмів автентифікації, крипостійких алгоритмів шифрування, захищених протоколів зв'язку, інструментів контролю введення даних, надійних засобів ідентифікації пристроїв та керування доступом, комплексного та регулярного тестування та сканування вразливостей. Хмарні сервіси IoT є незамінними для будь-якої сучасної екосистеми IoT, оскільки вони охоплюють багато функцій: керування пристроєм, збір та аналіз даних, безпеку, інтеграцію, масштабованість, інтерфейс користувача.

Сьогодні основними проблемами безпеки використання пристроїв IoT в Україні є відсутність відповідальності за розроблення та використання незахищених IoT, фізичного захисту апаратного забезпечення IoT, шифрування при передачі даних між пристроями мережі IoT, єдиних стандартів передачі та збереження даних, автентифікації та ідентифікації, а також мінімальний доступ до вбудованого програмного забезпечення IoT та проблеми його оновлення.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Журило О. Д., Ляшенко О. С., Аветісова К. А. Огляд рішень з апаратної безпеки кінцевих пристроїв туманних обчислень у Інтернеті речей. *Інноваційні технології та наукові рішення для промисловості.* 2023. № 1 (23). С. 57–71. DOI: https://doi.org/10.30837/ITSSI.2023.23.057.

2. Клімушин П. С., Рог В. Є., Колісник Т. П. Правові аспекти стандартизації функціональної безпеки Інтернету речей. *Право і безпека.* 2023. № 3 (90). С. 200–213. DOI: https://doi.org/10.32631/pb.2023.3.17.

3. Aazam M., Zeadally S., Harras K. A. Fog computing architecture, evaluation, and future research directions. *Communications Magazine*. 2018. Vol. 56, Iss. 5. Pp. 46–52. DOI: https://doi.org/10.1109/MCOM.2018.1700707.

4. AboBakr A., Azer M. A. IoT Ethics Challenges and Legal Issues // 12th International Conference on Computer Engineering and Systems (Cairo, Egypt, 19–20 December 2017). Cairo, 2018. Pp. 233–237. DOI: https://doi.org/10.1109/ICCES.2017.8275309.

5. Alhalafi N., Veeraraghavan P. Privacy and Security Challenges and Solutions in IoT: A review // International Conference on Smart Power & Internet Energy Systems (Melbourne, Australia, 25–27 April 2019). Melbourne : Deakin University, 2019. DOI: https://doi.org/10.1088/1755-1315/322/1/012013.

6. Ammar M., Russello G., Crispo B. Internet of things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*. 2018. Vol. 38. Pp. 8–27. DOI: https://doi.org/10.1016/j.jisa.2017.11.002.

7. Belkeziz R., Jarir Z. An Overview of the IoT Coordination Challenge. *International Journal of Service Science, Management, Engineering, and Technology*. 2020. Vol. 11, Iss. 1. Pp. 99–115. DOI: https://doi.org/10.4018/IJSSMET.2020010107.

8. Bhardwaj A., Kumar V. Electronic Healthcare Records: Indian vs International Perspective on Standards and Privacy. *International Journal of Service Science, Management, Engineering, and Technology*. 2021. Vol. 12, Iss. 2. Pp. 44–58. DOI: https://doi.org/10.4018/IJSSMET.2021030103.

9. Brass I., Tanczer L., Carr M., Elsden M., Blackstock J. Standardizing A Moving Target: The Development and Evolution of IoT Security Standards // Proceedings of Living in the Internet of Things: Cybersecurity of the IoT (London, UK, 28–29 March 2018). London, 2018. DOI: https://doi.org/10.1049/cp.2018.0024.

10. Butun I, Sari A, Österberg P. Hardware Security of Fog End-Devices for the Internet of Things. *Sensors*. 2020. Vol. 20, No. 20. DOI: https://doi.org/10.3390/s20205729.

11. Choudhary S., Meena G. Internet of Things: Protocols, Applications and Security Issues. *Procedia Computer Science*. 2022. Vol. 215. Pp. 274–288. DOI: https://doi.org/10.1016/j.procs.2022.12.030.

12. Guerbouj S. S. E., Gharsellaoui H., Bouamama S. A Comprehensive Survey on Privacy and Security Issues in Cloud Computing, Internet of Things and Cloud of Things. *International Journal of Service Science, Management, Engineering, and Technology*. 2019. Vol. 10, Iss. 3. Pp. 32–44. DOI: https://doi.org/10.4018/IJSSMET.2019070103.

13. Hou J., Qu L., Shi W. A survey on Internet of Things security from data perspectives. *Computer Networks.* 2019. Vol. 148, No. 2. Pp. 295–306. DOI: https://doi.org/10.1016/j.comnet.2018.11.026.

14. Hwang I., Kim Y. G. Analysis of security standardization for the Internet of Things // International Conference on Platform Technology and Service (Busan, Korea (South), 13–15 February 2017). Busan, 2017. DOI: https://doi.org/10.1109/PlatCon.2017.7883687.

15. Karie N. M., Sahri N. M., Yang W., Valli C., Kebande V. R. Review of Security Standards and Frameworks for IoT-Based Smart Environments. *IEEE Access*. 2021. Vol. 9. Pp. 121975–121995. DOI: https://doi.org/10.1109/ACCESS.2021.3109886.

16. Khan G., Gola K. K., Kanauzia R., Kumar S. Secure Architecture to Support IoT based on Fog Computing. *Procedia Computer Science*. 2022. Vol. 215, No. 2. Pp. 608–617. DOI: https://doi.org/10.1016/j.procs.2022.12.063.

17. Kumar V., Pradhan P. Trust Management: Social vs Digital Identity. *International Journal of Service Science, Management, Engineering, and Technology*. 2020. Vol. 11, Iss. 4. Pp. 26–44. DOI: https://doi.org/10.4018/IJSSMET.2020100102.

18. Lata M., Kumar V. Standards and Regulatory Compliances for IoT Security. *International Journal of Service Science, Management, Engineering, and Technology*. 2021. Vol. 12, Iss. 5. Pp. 132–147. DOI: https://doi.org/10.4018/IJSSMET.2021090109.

19. Lee E., Seo Y. D., Oh S. R., Kim Y. G. A Survey on Standards for Interoperability and Security in the Internet of Things. *Communications Surveys and Tutorials*. 2021. Vol. 23, No. 2. Pp. 1020–1047. DOI: https://doi.org/10.1109/COMST.2021.3067354.

20. Lin J., Yu W., Zhang N., Yang X., Zhang H., Zhao W. A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications. *Internet of Things Journal*. 2017. Vol. 4, No. 5. Pp. 1125–1142. DOI: https://doi.org/10.1109/JIOT.2017.2683200.

21. Lounis K., Zulkernine M. Attacks and defenses in short-range wireless technologies for IoT. *IEEE Access*. 2020. Vol. 8. Pp. 88892–88932. DOI: https://doi.org/10.1109/ACCESS.2020.2993553.

22. Mansour M., Gamal A., Ahmed A. I., Said L. A., Elbaz A., Herencsar N., Soltan A. Internet of Things: A Comprehensive Overview on Protocols, Architectures, Technologies, Simulation Tools, and Future Directions. *Energies.* 2023. Vol. 16. Pp. 34–65. DOI: https://doi.org/10.3390/en16083465.

23. Mendez D. M., Papapanagiotou I., Yang B. Internet of Things: Survey on security and privacy. *Information Security Journal: A Global Perspective*. 2018. Vol. 27, No. 3. Pp. 162–182. DOI: https://doi.org/10.1080/19393555.2018.1458258.

24. Qiu J., Tian Z., Du C., Zuo Q., Su S., Fang B. A survey on access control in the age of Internet of Things. *Internet of Things Journal*. 2020. Vol. 7, No. 6. Pp. 4682–4696. DOI: https://doi.org/10.1109/JIOT.2020.2969326.

25. Sabireen H., Neelanarayanan V. A Review on Fog Computing: Architecture, Fog with IoT, Algorithms and Research Challenges. *ICT Express.* 2021. Vol. 7, No. 2. Pp. 162–176. DOI: https://doi.org/10.1016/j.icte.2021.05.004.

26. Sain M., Kang Y. J., Lee H. J. Survey on security in Internet of Things: State of the art and challenges // 19th International Conference on Advanced Communication Technology (PyeongChang, Korea (South), 19–22 February 2017). PyeongChang, 2017. Pp. 699–704. DOI: https://doi.org/10.23919/ICACT.2017.7890183.

27. Singh J., Kumar V. End User Driven Approach for Regulatory Compliance in Public Cloud. *International Journal of Service Science, Management, Engineering, and Technology*. 2021. Vol. 12, Iss. 3. DOI: https://doi.org/10.4018/IJSSMET.2021050101.

28. Tournier J., Lesueur F., Mouël F. L., Guyon L., Ben-Hassine H. A survey of IoT protocols and their security issues through the lens of a generic IoT stack. *Internet of Things*. 2021. Vol. 16. DOI: https://doi.org/10.1016/j.iot.2020.100264.

29. Virat M. S., Bindu S. M., Aishwarya B., Dhanush B. N., Kounte M. R. Security and Privacy Challenges in Internet of Things // 2nd International Conference on Trends in Electronics and Informatics (Tirunelveli, India, 11–12 May 2018). Tirunelveli, 2018. Pp. 454–460. DOI: https://doi.org/10.1109/ICOEI.2018.8553919.

30. Wang W., Yongchareon S. Security-as-a-service: a literature review. *International Journal of Web Information Systems*. 2020. Vol. 16, No. 5. Pp. 493–517. DOI: https://doi.org/10.1108/IJWIS-06-2020-0031.

31. Yu J. Y., Lee E., Oh S. R., Seo Y. D., Kim Y. G. A survey on security requirements for WSNs: Focusing on the characteristics related to security. *IEEE Access*. 2020. Vol. 8. Pp. 45304–45324. DOI: https://doi.org/10.1109/ACCESS.2020.2977778.

Надійшла до редакції: 10.01.2025

Прийнята до опублікування: 13.03.2025

REFERENCES

1. Aazam, M., Zeadally, S., & Harras, K. A. (2018). Fog computing architecture, evaluation, and future research directions. *Communications Magazine, 56*(5), 46–52. https://doi.org/10.1109/MCOM.2018.1700707.

2. AboBakr, A., & Azer, M. A. (2017, December 19–20). *IoT Ethics Challenges and Legal Issues* [Conference presentation abstract]. 12th International Conference on Computer Engineering and Systems, Cairo, Egypt. https://doi.org/10.1109/ICCES.2017.8275309.

3. Alhalafi, N., & Veeraraghavan, P. (2019, April 25–27). *Privacy and Security Challenges and Solutions in IoT: A review* [Conference presentation abstract]. International Conference on Smart Power & Internet Energy Systems, Melbourne, Australia. https://doi.org/10.1088/1755-1315/322/1/012013.

4. Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications, 38*, 8–27. https://doi.org/10.1016/j.jisa.2017.11.002.

5. Belkeziz, R., & Jarir, Z. (2020). An Overview of the IoT Coordination Challenge. *International Journal of Service Science, Management, Engineering, and Technology, 11*(1), 99–115. https://doi.org/10.4018/IJSSMET.2020010107.

6. Bhardwaj, A., & Kumar, V. (2021). Electronic Healthcare Records: Indian vs International Perspective on Standards and Privacy. *International Journal of Service Science, Management, Engineering, and Technology, 12*(2), 44–58. https://doi.org/10.4018/IJSSMET.2021030103.

7. Brass, I., Tanczer, L., Carr, M., Elsden, M., & Blackstock, J. (2018, March 28–29). *Standardising A Moving Target: The Development and Evolution of IoT Security Standards* [Conference presentation abstract]. Proceedings of Living in the Internet of Things: Cybersecurity of the IoT, London, United Kingdom. https://doi.org/10.1049/cp.2018.0024.

8. Butun, I, Sari, A, & Österberg, P. (2020). Hardware Security of Fog End-Devices for the Internet of Things. *Sensors, 20*(20). https://doi.org/10.3390/s20205729.

9. Choudhary, S., & Meena, G. (2022). Internet of Things: Protocols, Applications and Security Issues. *Procedia Computer Science, 215*, 274–288. https://doi.org/10.1016/j.procs.2022.12.030.

10. Guerbouj, S. S. E., Gharsellaoui, H., & Bouamama, S. (2019). A Comprehensive Survey on Privacy and Security Issues in Cloud Computing, Internet of Things and Cloud of Things. *International Journal of Service Science, Management, Engineering, and Technology, 10*(3), 32–44. https://doi.org/10.4018/IJSSMET.2019070103.

11. Hou, J., Qu, L., & Shi, W. (2019). A survey on Internet of Things security from data perspectives. *Computer Networks, 148*(2), 295–306. https://doi.org/10.1016/j.comnet.2018.11.026.

12. Hwang, I., & Kim, Y. G. (2017, February 13–15). *Analysis of security standardization for the Internet of Things* [Conference presentation abstract]. International Conference on Platform Technology and Service, Busan, Korea (South). https://doi.org/10.1109/PlatCon.2017.7883687.

13. Karie, N. M., Sahri, N. M., Yang, W., Valli, C., & Kebande, V. R. (2021). A Review of Security Standards and Frameworks for IoT-Based Smart Environments. *IEEE Access, 9*, 121975–121995. https://doi.org/10.1109/ACCESS.2021.3109886.

14. Khan, G., Gola, K. K., Kanauzia, R., & Kumar, S. (2022). Secure Architecture to Support IoT based on Fog Computing. *Procedia Computer Science, 215*(2), 608–617. https://doi.org/10.1016/j.procs.2022.12.063.

15. Klimushyn, P. S., Roh, V. Ye., & Kolisnyk, T. P. (2023). Legal aspects of functional security standardisation of the Internet of Things. *Law and Safety, 3*(90), 200–213. https://doi.org/10.32631/pb.2023.3.17.

16. Kumar, V., & Pradhan, P. (2020). Trust Management: Social vs Digital Identity. *International Journal of Service Science, Management, Engineering, and Technology, 11*(4), 26–44. https://doi.org/10.4018/IJSSMET.2020100102.

17. Lata, M, & Kumar, V. (2021). Standards and Regulatory Compliances for IoT Security. *International Journal of Service Science, Management, Engineering, and Technology, 12*(5), 132–147. https://doi.org/10.4018/IJSSMET.2021090109.

18. Lee, E., Seo, Y. D., Oh, S. R., & Kim, Y. G. (2021). A Survey on Standards for Interoperability and Security in the Internet of Things. *Communications Surveys and Tutorials, 23*(2), 1020–1047. https://doi.org/10.1109/COMST.2021.3067354.

19. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications. *Internet of Things Journal, 4*(5), 1125–1142. https://doi.org/10.1109/JIOT.2017.2683200.

20. Lounis, K., & Zulkernine, M. (2020). Attacks and defenses in short-range wireless technologies for IoT. *IEEE Access, 8*, 88892–88932. https://doi.org/10.1109/ACCESS.2020.2993553.

21. Mansour, M., Gamal, A., Ahmed, A. I., Said, L. A., Elbaz, A., Herencsar, N., & Soltan, A. (2023). Internet of Things: A Comprehensive Overview on Protocols, Architectures, Technologies, Simulation Tools, and Future Directions. *Energies, 16*, 34–65. https://doi.org/10.3390/en16083465.

22. Mendez, D. M., Papapanagiotou, I., & Yang, B. (2018). Internet of Things: Survey on security and privacy. *Information Security Journal: A Global Perspective, 27*(3), 162–182. https://doi.org/10.1080/19393555.2018.1458258.

23. Qiu, J., Tian, Z., Du, C., Zuo, Q., Su, S., & Fang, B. (2020). A survey on access control in the age of Internet of Things. *Internet of Things Journal, 7*(6), 4682–4696. https://doi.org/10.1109/JIOT.2020.2969326.

24. Sabireen, H., & Neelanarayanan, V. (2021). A Review on Fog Computing: Architecture, Fog with IoT, Algorithms and Research Challenges. *ICT Express, 7*(2), 162–176. https://doi.org/10.1016/j.icte.2021.05.004.

25. Sain, M., Kang, Y. J., & Lee, H. J. (2017, February 19–22). *Survey on security in Internet of Things: state of the art and challenges* [Conference presentation abstract]. International Conference on Advanced Communication Technology, PyeongChang, Korea (South). https://doi.org/10.23919/ICACT.2017.7890183.

26. Singh, J., & Kumar, V. (2021). End User Driven Approach for Regulatory Compliance in Public Cloud. *International Journal of Service Science, Management, Engineering, and Technology, 12*(3). https://doi.org/10.4018/IJSSMET.2021050101.

27. Tournier, J., Lesueur, F., Mouël, F. L., Guyon, L., & Ben-Hassine, H. (2021). A survey of IoT protocols and their security issues through the lens of a generic IoT stack. *Internet of Things, 16*. https://doi.org/10.1016/j.iot.2020.100264.

28. Virat, M. S., Bindu, S. M., Aishwarya, B., Dhanush, B. N., & Kounte, M. R. (2018, May 11–12). *Security and Privacy Challenges in Internet of Things* [Conference presentation abstract]. 2nd International Conference on Trends in Electronics and Informatics, Tirunelveli, India. https://doi.org/10.1109/ICOEI.2018.8553919.

29. Wang, W., & Yongchareon, S. (2020). Security-as-a-service: a literature review. *International Journal of Web Information Systems, 16*(5), 493–517. https://doi.org/10.1108/IJWIS-06-2020-0031.

30. Yu, J. Y., Lee, E., Oh, S. R., Seo, Y. D., & Kim, Y. G. (2020). A survey on security requirements for WSNs: Focusing on the characteristics related to security. *IEEE Access, 8*, 45304–45324. https://doi.org/10.1109/ACCESS.2020.2977778.

31. Zhurylo, O. D., Liashenko, O. S., & Avetisova, K. A. (2023). Hardware security overview of fog computing end devices in the Internet of Things. *Innovative Technologies and Scientific Solutions for Industries, 1*(23), 57–71. https://doi.org/10.30837/ITSSI.2023.23.057.

Received the editorial office: 10 January 2025

Accepted for publication: 13 March 2025

PETRO SERHIIOVYCH KLIMUSHYN,
Kharkiv National University of Internal Affairs,
Educational and Scientific Institute No. 4,
Department of Combating Cybercrime;
ORCID: https://orcid.org/0000-0002-1020-9399,
e-mail: klimushyn@ukr.net;

PROBLEMATIC ASPECTS OF IOT CYBERSECURITY STANDARDISATION

The popularity of IoT devices is gaining interest among consumers. The growing number of consumers benefiting from IoT devices and the use of IoT technologies has increased the risk of cyberattacks. The Internet of Things is an important “crossroads” for several technologies. As a result, it is possible to connect smart physical goods and enable smart decision-making in a wide range of applications. Different devices, including computers, actuators and sensors, can connect to each other and exchange data in a networked environment. The supply of smart objects on the market is growing, so ensuring their security is becoming increasingly important.

The main problem with IoT devices is related to privacy and security. The administration of large amounts of data for reliable and secure processing is a real challenge. There are also issues of user protection, security and privacy. The cybersecurity and privacy of IoT consumers can be negatively affected by the development of these technologies if vulnerable devices and their environments are used. Therefore, there is a problem of information protection of IoT devices. To address this problem, a large number of technologies and standards have been created to ensure cybersecurity of the Internet of Things. In addition, there are a large number of necessary and important requirements to ensure protection against cyber attacks on IoT devices. All of this necessitates an analysis of the effectiveness of all these programmes and their scope for ensuring the cybersecurity of IoT environments.

To be successful, these programmes need to define the characteristics of IoT environments. The security standards, advanced technologies for solving security problems, and applications for analysing the current security structure make up the research taxonomy of the Internet of Things.

The article is a more comprehensive study than many previous ones on the topic of cybersecurity of the Internet of Things. It analyses the problematic aspects of standardisation related to the cybersecurity of the Internet of Things and examines the activities of international organisations for the standardisation of the Internet of Things.

Keywords: *Internet of Things technologies, security challenges, standardisation organisations, security standards, security certificates, access control to the Internet of Things.*

Цитування (ДСТУ 8302:2015): Клімушин П. С. Проблемні аспекти стандартизації кібербезпеки Інтернету речей. *Право і безпека*. 2025. № 1 (96). С. 53–66. DOI: https://doi.org/10.32631/pb.2025.1.05.

Citation (APA): Klimushyn, P. S. (2025). Problematic aspects of IoT cybersecurity standardisation. *Law and Safety, 1*(96), 53–66. https://doi.org/10.32631/pb.2025.1.05.