КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.33.1035
УДК 342.9:5.08

Клімушин Петро Сергійович
кандидат технічних наук, доцент,
доцент кафедра комп'ютерних систем та робототехніки
Харківський національний університет імені В. Н. Каразіна
ORCID: 0000-0002-1020-9399
klimushyn@karazin.ua

Хруслов Максим Михайлович
кандидат фізико-математичних наук, старший дослідник,
доцент, завідувач кафедри комп'ютерних систем та робототехніки
Харківський національний університет імені В. Н. Каразіна
ORCID: 0000-0001-9639-9340
maksym.khruslov@karazin.ua

Колісник Тетяна Петрівна
кандидат педагогічних наук, доцент,
доцент, кафедра кібербезпеки та DATA-технологій
Харківський національний університет внутрішніх справ
ORCID:0000-0002-7442-8136
ktp201505@gmail.com

Хавіна Інна Петрівна
кандидат технічних наук, доцент,
доцент, кафедра кібербезпеки та DATA-технологій
Харківський національний університет внутрішніх справ
ORCID: 0000-0002-1856-1186
inna.khavina25@gmail.com

Тулупов Володимир Володимирович
кандидат технічних наук, доцент,
доцент, кафедра кібербезпеки та DATA-технологій
Харківський національний університет внутрішніх справ
ORCID: 0000-0003-4794-743X
madey1969@gmail.com

ІНТЕГРАЦІЯ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ У СИСТЕМИ КІБЕРЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. Проблема вивчення можливостей та ризиків інтеграції Інтернет речей у системи безпеки критичної інфраструктури є надзвичайно актуальною, оскільки вона передбачає комплексний аналіз переваг та викликів, що виникають під час впровадження інноваційних технологій у секторі безпеки. З одного боку, Інтернет речи відкриває великі можливості для автоматизації процесів безпеки, підвищення ефективності моніторингу та реагування на загрози в режимі реального часу, а з іншого боку, ця технологія несе з собою нові ризики, пов'язані з вразливістю пристроїв до кіберзагроз, етичними питаннями використання автономних систем та проблемами інтеграції різних технологій в єдину безпечну екосистему. Для вирішення цієї проблеми в статті достигнути наступні результати Проаналізовано існуючі дослідження в сфері кібербезпеки критичної інфраструктури та Інтернет речей як спільної безпечної екосистеми. Літературні джерела класифіковано за трьома напрямами: кібербезпека критичної інфраструктури, кібербезпека середовищ Інтернет речей та дослідження за спільними напрямами. Визначено відсутність цілісного підходу в спільних дослідженнях взаємопов’язаних середовищ критичної інфраструктури та Інтернет речей. Доведено фундаментальні цілі та їх пріоритетність для кібербезпеки критичної інфраструктури та Інтернет речей як єдиної системи, що базуються на класичній тріаді CIA (конфіденційність, цілісність, доступність), однак пріоритетність фундаментальних цілей кіберрбезпеки в процесах інтеграції технологій Інтернет речей до критичних структур повинна виконуватися в наступної черги: безпека людей та довкілля,

доступність, цілісність, стійкість і відновлення, конфіденційність. Досліджено основні технології Інтернет речей, що використовуються в критичної інфраструктурі та надано структурована системи безпеки в вигляди взаємопов'язаних компонент, яка дозволяє створити інтегровані системи безпеки, зменшити вплив людського фактору, забезпечити швидке реагування на інциденти, оптимізувати витрати на безпеку, підвищити загальний рівень безпеки об'єктів. Обґрунтовано інноваційні рішення кібербезпеки в секторі критичної інфраструктури: системи на основі штучного інтелекту та машинного навчання (аналіз поведінки мереж і пристроїв, автоматичне реагування на інциденти); децентралізоване управління безпекою для забезпечення конфіденційності та цілісності даних на основі блокчейн технології; квантові методи шифрування даних та розподілу ключів в безпечні мережі зв'язку; архітектура нульової довіри та хмарні системи безпеки (конфіденційні обчислення, безпечний доступ до сервісу, хмарні платформи захисту застосунків). Інновації у кібербезпеці критичної інфраструктури дозволяють: зменшити час виявлення та реагування на атаки; підвищити стійкість до цілеспрямованих атак; інтегрувати захист середовищ у єдину стратегію. Проаналізовано існуючі системи стандартизації інформаційної безпеки з захисту критичної інфраструктури за технічним рівнем та наявністю схем сертифікації. Стандарти для Інтернет речей та розподілених систем критичної інфраструктури стають обов'язковим елементом кіберзахисту. Вони забезпечують уніфіковані вимоги до безпеки пристроїв, мереж та процесів. Забезпечують інтеграцію пристроїв та систем, підвищуючи стійкість критичної інфраструктури до сучасних кіберзагроз.

Ключові слова: критична інфраструктура, Інтернет речей, інтеграція технологій, кібербезпека, системи стандартизації, штучний інтелект, машинне навчання, блокчейн, квантові технології.

ВСТУП

Постановка проблеми. Критична інфраструктура (КІ) – це сукупність стратегічно важливих об'єктів, необхідних для підтримки суспільства та економіки, включаючи електромережі, водопостачання, транспортні мережі, телекомунікації та охорону здоров'я. Зростаюча інтеграція технологій Інтернету речей (Internet of Things – IoT) у системи КІ революціонізувала різні галузі, полегшуючи досягнення кращої ефективності, автоматизації та моніторингу в реальному часі. Але це масштабне розгортання становить величезні загрози безпеці, які підривають надійність, безпеку та цілісність критичної інфраструктури. Хоча дослідження безпеки IoT досягли неймовірних успіхів, все ще є слабкі місця у вирішенні динамічної та складної природи вимог до КІ.

З IoT ці системи стають все більш інтегрованими, з більшою гнучкістю та ефективністю. Пристрої IoT, такі як датчики, виконавчі механізми та інтелектуальні контролери, встановлюються в середовищах КІ для полегшення збору даних у режимі реального часу, дистанційного моніторингу та автоматизації.

Пристрої IoT з низькою обчислювальною потужністю та пам'яттю надзвичайно вразливі до кібератак. Ці вразливості можуть зробити КІ вразливою до атак з потенційно серйозними наслідками, такими як перебої в обслуговуванні, витік даних та катастрофічний збій. Крім того, більшість пристроїв IoT не мають вбудованих функцій безпеки і, отже, стають вразливими цілями для кібератак. Широкомасштабне розгортання IoT у КІ збільшує поверхню атаки, з численними точками входу для хакерів.

Незважаючи на те, що ці технології забезпечують широкий спектр переваг, вони створюють нові загрози безпеці, які підривають стабільність та стійкість цих критично важливих галузей. Пристрої IoT часто вразливі до кібератак через притаманні недоліки конструкції, обмежені можливості обробки та відсутність ефективних засобів контролю безпеки. Як наслідок, ці вразливості роблять КІ вразливою до таких атак, як витік даних, несанкціонований доступ та порушення функціональності системи.

Сучасні системи безпеки мають труднощі з надання комплексних рішень, адаптованих до конкретних потреб таких оточень. Існує нагальна потреба у сильних, масштабованих та адаптивних механізмах безпеки, які можуть вирішувати такі виклики, як конфіденційність даних, автентифікація пристроїв, виявлення загроз і стійкість систем до загроз. Наукова новизна роботи полягає в систематичному аналізі потенціалу технологій IoT в системі кіберзахисту КІ, обґрунтуванні комплексного підходу щодо інтеграції цілій кібербезпеки, IoT технологій, рішень кібербезпеки КІ, систем стандартизації та кращих практик в систему захисту КІ.

Мета і завдання дослідження. Метою цього дослідження є аналіз поточних проблем безпеки IoT у контексті критичної інфраструктури, визначення прогалин у попередніх дослідженнях та комплексне

вирішення проблем запровадження технологій IoT, інноваційних рішень кібербезпеки на основі інноваційних механізмів виявлення та реагування на загрози, стандартизованих інструментах безпеки та кращих практик кіберзахисту КІ, життєво важливих послуг та ланцюгів постачання.

Для досягнення зазначеної мети поставлені такі завдання:

– провести огляд літературних джерел за трьома напрямами: кібербезпека КІ, технології для безпеки систем IoT, рішення безпеки IoT для сектора КІ;

– визначити фундаментальні цілі та їх пріоритетність для кібербезпеки КІ, що базуються на класичній тріаді CIA (конфіденційність, цілісність, доступність);

– дослідити основні технології IoT, що використовуються КІ, та надати узагальнену структуру системи безпеки IoT;

– оцінити переваги інтегрованих систем безпеки IoT у системі КІ з дистанційним моніторингом, автоматизованим реагуванням та розширеними аналітичними можливостями;

– встановити перспективи розвитку систем IoT у секторі безпеки КІ шляхом інтеграції штучного інтелекту, технологій 5G та впровадження децентралізованих підходів до інформаційної безпеки, здатних до незалежного аналізу даних та прогнозування загроз;

– проаналізувати інноваційні рішення кібербезпеки в секторі КІ такі як: штучний інтелект, блокчейн, квантова криптографія, архітектура нульової довіри та хмарні системи безпеки;

– проаналізувати існуючі системи стандартизації інформаційної безпеки з захисту КІ за технічним рівнем та наявністю схем сертифікації;

– визначити кращі практики кіберзахисту КІ, життєво важливих послуг та ланцюгів постачання.

Аналіз останніх досліджень і публікацій. Однією з основних тем, що була встановлена в літературі, є відсутність належного розгортання стандартизованих процесів безпеки для КІ на базі IoT. Відсутність єдиної системи безпеки призвела до різних практик безпеки в різних галузях, що ускладнює інтеграцію систем IoT. Розробка універсальних стандартів безпеки IoT необхідна для забезпечення як взаємодії, так і безпеки пристроїв IoT у системах КІ.

Обговоримо деяку доступну літературу, пов'язану з областю цього дослідження. Схема огляду літератури поділена на три перспективи: по-перше, проблеми кібербезпеки КІ; по-друге, технології безпеки систем IoT; і по-третє, рішення безпеки IoT для сектора КІ [18].

Рішення проблеми кібербезпеки КІ. Оцінка вразливостей та пов'язаних з ними загроз є основним викликом для кібербезпеки КІ. Q. Qassim та ін. [19] описують потенційні вразливості та загрози на основі системи контролю та збору даних (SCADA) електромережі.

Одним із викликів кібербезпеці є виявлення кіберінцидентів P. Haller, B. Genge та A-V. Duka [10] представляють корисний механізм моніторингу для виявлення вторгнень у промислові системи керування на основі відхилення швидкості планування завдань від нормальної швидкості через порушення мережевого трафіку.

Проблеми безпеки, пов'язані з виявленням аномалій у величезних технологічних даних промислових систем керування, обговорювали X. Clotet, J. Moyano, G. Leon [4]. У роботі пропонується алгоритм для системи виявлення вторгнень (IDS), заснований на вивченні атрибутів звичайних технологічних даних та використанні цього як основи для розділення аномалій.

Рішення безпеки систем IoT. I. Farris та ін. [9] представляють аналіз сфери застосування технологій програмно-визначених мереж (SDN) та віртуалізації мережевих функцій (NFV) як доповнення до традиційних рішень безпеки IoT. NFV дозволяє відокремити програмне забезпечення від апаратного забезпечення, налаштовуючи вимоги безпеки до пристроїв за допомогою брандмауерів та інспекторів глибоких пакетів. Роль контролера SDN полягає в управлінні потоком трафіку.

S. Yu та ін. [24] запропонували платформу блокчейн, яка може забезпечити ефективну передачу даних з інтелектуальних пристроїв в IoT. K. Elbehiery та H. Elbehiery [8] запропонували використовувати 5G як послугу для застосунків IoT. S. Paliwal та S. O. Hasan [17] визначили фактори, які роблять технологію 5G корисною для середовища IoT.

Важливо, що дослідники враховують різні проблеми та обмеження, пов'язані з впровадженням IoT, такі як затримка, управління живленням, масштабованість, продуктивність та пропускна здатність, сумісність, стандартизація, надійність та кібербезпека [27].

Рішення кібербезпеки КІ в середовищі IoT. Дослідження показали, що оцінка атак та вразливостей в архітектурі системи є ключем для ефективного управління кібербезпекою. N. R. Rodofile та ін. [21] представили повну структуру кібератак у всій архітектурі на основі SCADA для КІ. У роботі описано діапазон атак у чотирьох категоріях, пов'язаних з IT-системою, протоколом, конфігурацією та процесом управління.

Для демонстрації рішень безпеки IoT у КІ більшість досліджень базується на специфічних доменних областях використання, наприклад, інтелектуальних мережах. K. Kimani та ін. [12] визначили безпеку як критичний фактор, який слід враховувати перед прийняттям рішення про масштабне розгортання пристроїв IoT в інтелектуальних мережах. K. Demir та ін. [6] запропонували концепцію ієрархічного гібридного розширення хмари (HHCEC) для інтелектуальної мережі.

У деяких дослідницьких роботах запропоновано моделі відповідності для вирішення проблем стандартів безпеки. R. Leszczyna [13] обговорив різні галузеві стандарти та принципи стандартизації кібербезпеки для застосувань інтелектуальних мереж. Автор запропонував основу для вибору відповідних стандартів та критеріїв оцінки. D. Makupi та N. Masese [14] розробили модель для оцінки рівнів зрілості інформаційної безпеки організацій за рівнями.

Є також роботи, які досліджують конкретні аспекти інтеграції IoT у критичну інфраструктуру. Наприклад, в працях [1; 5;16] досліджують вплив IoT на системи енергопостачання, транспорт та охорону здоров'я, підкреслюючи як потенційні переваги, так і загрози, пов'язані з кібербезпекою. В роботі [7] запропоновано комплексний механізми для додаткового захисту технологій IoT в критичних системах на основі штучного інтелекту.

Таким чином, роботи кіберзахисту КІ орієнтовані на побудову систем контролю та збору даних електромережі, управління доступом до промислових систем, виявлення вторгнень та прогнозування зловмисної активності, управління кіберінцидентами. Рішення безпеки систем IoT пов’язані з аналізом програмно-визначених мереж та віртуалізацією мережевих функцій, використанням блокчейн технологій, 5G, дослідженням таких проблем як: затримка, управління живленням, масштабованість, продуктивність та пропускна здатність, сумісність, стандартизація, надійність та кібербезпека. Спільні дослідження зосереджується на вирішенні численних проблем, пов'язаних з архітектурою, технологіями, апаратним забезпеченням, стандартами, бізнесом, а також безпекою та конфіденційністю. Однак більшість досліджень зосереджена на окремих аспектах, відсутність цілісного підходу до інтеграції систем безпеки залишається проблемною. Зокрема, існує потреба вивчати взаємодію між технічними, організаційними та регуляторними факторами, та аспекти, що дозволять створити більш стійкі та ефективні системи. Огляд літератури вказує на необхідність подальших досліджень, спрямованих на розробку комплексних рішень для інтеграції IoT у системи безпеки КІ, враховуючи як можливості, так і ризики цієї технології. В статті було визначено п’ять аспектів інтеграції IoT у системи безпеки КІ, пов'язані з фундаментальними цілями кібербезпеки та їх пріоритетністю, технологіями IoT, рішеннями кібербезпеці КІ, стандартами та практиками захисту.

Методологія дослідження. У дослідженні розглядається інтеграція технологій IoT у системи кібербезпеки КІ. Під час проведення цього систематичного огляду застосовано методологічний підхід для: 1) розробки стратегії пошуку з використанням кількох баз даних, 2) визначення критеріїв включення та виключення публікацій – оцінки їхньої відповідності, 3) визначення схеми огляду та кодування, 4) аналізу та синтезу даних та 5) розробки опису. Це забезпечило прозорість та ретельність процесу відбору та аналізу публікацій. Розмежований пошук у базі даних проводився за ключовими словами, анотацією та назвою. Враховуючи обсяг літератури, застосовано ця стратегія, щоб зменшити кількість публікацій для огляду, одночасно підвищуючи точність пошуку інформації. Метою було визначити відповідні публікації, які чітко обговорювали концепцію викликів IoT в кібербезпеки КІ.

Критеріями включення були публікації з доповідями на конференціях та статті (концептуальні та емпіричні дослідження) у рецензованих журналах, написаних англійською мовою. Крім того, виключено з вибірки розділи книг, звіти, політичні документи, газети та огляди журналів.

Автори обмежили публікації періодом з 2017 по 2025 рік, включаючи важливі визначення, концепції та відповідну інформацію, що стосується предмета дослідження. Використана стратегія попереднього відбору забезпечила, щоб відповідні публікації зробили значний внесок у досліджуване явище, включене до процесу систематичного огляду літератури. Також перевірено анотації, ключові слова, вступ та висновок кожної статті, щоб зменшити помилки відбору. Оцінка відповідності включала ручну перевірку кожної публікації для підвищення ретельності, точності та надійності процесу відбору публікацій.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

1. Фундаментальні цілі кібербезпеки КІ: базуються на класичній тріаді CIA (Confidentiality, Integrity, Availability), але їх пріоритетність відрізняється від звичайних IT-систем через прямий вплив на життя людей, довкілля та національну безпеку.

Найвищий пріоритет для кібербезпеки КІ має ціль доступність (Availability) – забезпечення безперервної та стабільної роботи систем так як зупинка енергосистем, водопостачання, транспорту чи

лікарень може призвести до: загибелі людей; масштабних економічних втрат; соціальної дестабілізації. Тобто навіть короткочасна відмова сервісу життєво важливих послуг є неприпустимою.

Цілісність (Integrity) – захист від несанкціонованої зміни даних або команд має другий за пріоритетом. Зміна параметрів керування може призвести до: фізичних аварій (перевантаження турбін, аварії на АЕС); некоректних рішень операторів; прихованих атак, що складно виявити.

Конфіденційність (Confidentiality) – захист чутливої інформації від витоку має третій пріоритет. Витік даних менш небезпечний, ніж відмова або аварія системи. Розголошення конфіденційності може: полегшити підготовку майбутніх атак, розкрити вразливості та архітектуру КІ, становити загрозу національній безпеці.

У кібербезпеці КІ безпеку людей та довкілля (Safety) часто ставлять вище за CIA. Тобто жодна кіберміра не повинна створювати ризик для: життя людей, здоров'я, навколишнього середовища. Ця ціль має надпріоритет і система безпеки не повинна блокувати аварійне ручне керування.

Для систем КІ характерна стратегічна ціль стійкість та відновлюваність (Resilience & Recovery) – здатність системи: витримувати атаки, працювати в деградованому режимі, швидко відновлюватися після інциденту. Ключові елементи досягнення цілі: резервування, сегментація мереж, плани реагування та відновлення.

Тобто пріоритетність фундаментальних цілей кіберрбезпеки в процесах інтеграції технологій IoT до КІ повинна виконуватися в наступної черги: безпека людей та довкілля, доступність, цілісність, стійкість і відновлення, конфіденційність (рис. 1).

2. Аналіз основних технологій IoT, що використовуються в системах безпеки КІ. Завдяки використанню інтелектуальних пристроїв, IoT дозволяє здійснювати безперервний моніторинг та збір даних, що допомагає виявляти потенційні загрози та швидко реагувати на надзвичайні ситуації. До складових структури системи безпеки IoT входять [**Помилка! Джерело посилання не знайдено.**]:

Рис. 1. Узагальнена ієрархія пріоритетів цілей кібербезпеки критичної інфраструктури

1. Пристрої збору даних: датчики руху, звуку, температури, сигналізації тощо; камери відеоспостереження.

2. Шлюзи та контролери: шлюзи – це інтерфейси між пристроями IoT та мережею; контролери визначають доступ до певних об'єктів або ресурсів.

3. Мережа передачі даних – це інфраструктура, яка дозволяє передавати дані від датчиків та пристроїв на центральний сервер або хмарне сховище. Вона може бути побудована на основі різних технологій, таких як Wi-Fi, Bluetooth, Zigbee, LoRaWAN або мобільні мережі (4G/5G) [26].

4. Центральний сервер або хмарна платформа: сервер збирає дані з усіх пристроїв та обробляє їх для виявлення аномалій або подій, які потребують уваги; хмарні платформи можуть забезпечувати централізоване зберігання даних та віддалений доступ для моніторингу та управління.

5. Програмне забезпечення для керування та моніторингу – це інтерфейс користувача (наприклад, мобільний додаток або веб-платформа), який дозволяє операторам системи контролювати та керувати різними аспектами безпеки: переглядати відео з камер, отримувати сповіщення про спрацьовування датчиків, переглядати історію подій тощо.

6. Система автоматичного реагування – на основі аналізу отриманих даних система може автоматично реагувати на певні події. Це може включати автоматичні сповіщення на мобільні пристрої, спрацьовування тривоги, повідомлення правоохоронних органів або запуск інших механізмів безпеки.

7. Аналітичні інструменти та штучний інтелект – машинне навчання та алгоритми штучного інтелекту використовуються для ефективного аналізу великих обсягів даних з пристроїв IoT. Вони

допомагають прогнозувати потенційні загрози на основі історичних даних, виявляти аномалії та оптимізувати безпеку.

Така інтеграція різних технологій IoT (рис. 2) дозволяє: створити інтегровані системи безпеки, зменшити вплив людського фактору, забезпечити швидке реагування на інциденти, оптимізувати витрати на безпеку, підвищити загальний рівень безпеки об'єктів.

Рис. 2. Основні компоненти IoT-системи безпеки критичної інфраструктури

Наведені технології дозволяють створювати інтегровані системи безпеки з дистанційним моніторингом, автоматизованим реагуванням та розширеними аналітичними можливостями. Ефективність системи досягається завдяки автоматизації процесів, що значно зменшує можливість людських помилок. Цілодобовий моніторинг з миттєвими сповіщеннями та безперервним збором даних забезпечує своєчасне реагування на будь-які події. Всі ці елементи працюють разом, щоб створити надійну та ефективну систему безпеки на основі технологій IoT.

IoT продовжує «трансформувати» індустрію безпеки, відкриваючи нові можливості для вдосконалення систем безпеки та адаптації до зростаючих викликів. Однією з ключових тенденцій є поєднання IoT зі штучним інтелектом для створення інтелектуальних систем безпеки, здатних до незалежного аналізу даних та прогнозування загроз. AI дозволить виявляти потенційні небезпеки в режимі реального часу, аналізувати складні моделі поведінки та автоматизувати реагування на інциденти.

Ще однією перспективою є впровадження технологій 5G, що значно збільшить швидкість передачі даних між пристроями IoT, забезпечуючи безперервний моніторинг та миттєве реагування. Це відкриє нові можливості для впровадження складних систем з великою кількістю взаємодіючих елементів.

Зростаючі ризики кіберзагроз стимулюють розробку більш надійних механізмів захисту пристроїв IoT, включаючи децентралізовані підходи, такі як блокчейн, для забезпечення конфіденційності та цілісності даних.

Важливим аспектом є підвищення рівня сумісності систем IoT. Розробка уніфікованих стандартів та протоколів зв'язку сприятиме кращій інтеграції пристроїв різних виробників, що дозволить створювати більш гнучкі системи безпеки [26, 27].

Крім того, розробка автономних пристроїв, таких як патрульні роботи або дрони на базі IoT, розширить можливості фізичної безпеки. Вони здатні забезпечувати моніторинг у важкодоступних або небезпечних зонах, значно підвищуючи ефективність захисту об'єктів.

Таким чином, розвиток IoT у сфері безпеки спрямований на створення інтелектуальних, масштабованих та надійних систем, які можуть адаптуватися до сучасних викликів та забезпечувати високий рівень захисту як у приватному, так і в державному секторах.

У дослідженні було проведено комплексний аналіз основних особливостей застосування IoT у сфері безпеки КІ, який виявив як значні можливості, так і потенційні ризики впровадження рішень IoT. Технології IoT можуть радикально трансформувати традиційні підходи до безпеки, пропонуючи автоматизовані, інтелектуальні та високоефективні системи безпеки.

Ключовим результатом дослідження стало формування цілісного погляду на архітектуру систем безпеки IoT, яка включає пристрої збору даних, протоколи зв'язку, хмарні платформи та системи автоматичного реагування. Було визначено, що інтеграція гетерогенних технологій дозволяє створювати інтегровані системи з можливістю цілодобового моніторингу, швидкого виявлення та реагування на потенційні загрози.

Практичне значення роботи полягає у виявленні перспектив розвитку IoT у секторі безпеки КІ, зокрема шляхом інтеграції штучного інтелекту, технологій 5G та впровадження децентралізованих підходів до інформаційної безпеки.

3. Інноваційні рішення кібербезпеки КІ. Оскільки кіберзагрози стають все більш складними, організації впроваджують передові технології для посилення своєї безпеки. Новітні рішення, такі як

штучний інтелект, блокчейн, квантова криптографія, архітектура нульової довіри та передові хмарні системи безпеки, трансформують кібербезпеку, забезпечуючи проактивне виявлення загроз, покращений захист даних та надійну мережеву безпеку. Ці технології формують майбутнє кібербезпеки [11].

Штучний інтелект (AI) та машинне навчання (ML) революціонізують кібербезпеку, забезпечуючи виявлення загроз у режимі реального часу, автоматизоване реагування та прогнозну аналітику. Традиційні інструменти безпеки покладаються на виявлення на основі сигнатур, яке може ідентифікувати лише відомі загрози. Рішення на основі AI можуть виявляти атаки нульового дня, внутрішні загрози та передові постійні загрози, аналізуючи закономірності та поведінку:

– Виявлення аномалій: AI контролює мережевий трафік, поведінку користувачів та діяльність системи, щоб виявляти відхилення від нормальних закономірностей. Наприклад, якщо працівник раптово отримує доступ до конфіденційних файлів поза своїм звичайним робочим часом, AI може позначити це як потенційну внутрішню загрозу.

– Прогнозний аналіз загроз: моделі AI аналізують історичні дані про атаки, щоб передбачити нові загрози до їх виникнення, допомагаючи організаціям вживати проактивні заходи безпеки.

– Автоматизоване реагування на загрози: інструменти безпеки на базі AI можуть миттєво ізолювати заражені пристрої, блокувати шкідливий трафік та виправляти вразливості без втручання людини.

Варіанти використання AI в кібербезпеці:

– антивірусні рішення на базі AI (наприклад, CrowdStrike, Cylance) виявляють та нейтралізують загрози до того, як вони завдадуть шкоди;

– системи управління інформацією та подіями безпеки (SIEM) використовують штучний інтелект для фільтрації та визначення пріоритетів сповіщень, зменшуючи кількість хибнопозитивних результатів;

– інструменти виявлення фішингу на базі штучного інтелекту аналізують вміст електронної пошти, поведінку відправника та метадані для виявлення фішингових атак.

Хоча штучний інтелект посилює захист від кібербезпеки, зловмисники також використовують штучний інтелект для розробки більш складних загроз, таких як фішинг, згенерований штучним інтелектом, та автоматизовані інструменти злому, що робить штучний інтелект палицею з двома кінцями в кібербезпеці.

Технологія блокчейн стає потужним інструментом для підвищення безпеки даних, управління ідентифікацією та безпечних транзакцій. На відміну від традиційних централізованих моделей безпеки, блокчейн забезпечує децентралізовані, незмінні та прозорі рішення безпеки, зменшуючи ризик витоків даних та кібершахрайства.

Автентифікація на основі блокчейну дозволяє користувачам контролювати власні цифрові ідентичності, запобігаючи крадіжці облікових даних та несанкціонованому доступу:

– безпека даних, захищена від несанкціонованого доступу, оскільки записи блокчейну незмінні, після запису даних у блокчейн їх не можна змінити або видалити, що запобігає маніпуляціям даними зловмисниками;

– безпечні транзакції: блокчейн дозволяє здійснювати наскрізне шифрування транзакцій, зменшуючи фінансове шахрайство, витік даних та несанкціонований доступ до конфіденційних даних.

Приклади використання блокчейну в кібербезпеці:

– децентралізована інфраструктура відкритих ключів (DPKI) підвищує безпеку цифрових сертифікатів;

– безпека ланцюга постачання на основі блокчейну запобігає шахрайським змінам у системах відстеження продукції;

– розумні контракти автоматизують та захищають цифрові транзакції без посередників, зменшуючи ризик шахрайства.

Незважаючи на свої переваги, блокчейн стикається з такими проблемами, як масштабованість, високе енергоспоживання та регуляторні проблеми, які необхідно вирішити для широкого впровадження.

Зі зростанням квантових обчислень традиційні методи шифрування, такі як RSA та ECC, стають вразливими. Квантові комп'ютери можуть зламати класичні алгоритми шифрування за частку часу, який потрібен традиційним комп'ютерам, що створює значну загрозу безпеці даних. Квантова криптографія - майбутнє безпечного зв'язку.

Квантова криптографія використовує принципи квантової механіки для створення незламних методів шифрування. Найбільш помітним застосуванням є квантовий розподіл ключів (QKD), який дозволяє двом сторонам безпечно обмінюватися ключами шифрування. Переваги квантової криптографії:

– незламне шифрування: будь-яка спроба перехопити квантово-зашифроване повідомлення змінює квантовий стан, попереджаючи обидві сторони про порушення;

– безпечні мережі зв'язку: уряди та підприємства впроваджують квантову криптографію для захисту національної безпеки, банківських транзакцій та обміну конфіденційними даними.

Проблеми квантової криптографії:

– дорога інфраструктура: квантовий зв'язок вимагає спеціалізованого обладнання, волоконної оптики та можливостей квантових обчислень;

– обмежене впровадження: хоча Китай та США є лідерами в дослідженнях квантової криптографії, комерційне впровадження залишається на ранніх стадіях;

– оскільки квантові комп'ютери стають потужнішими, організації повинні переходити на квантово-стійкі алгоритми шифрування, щоб забезпечити майбутнє системи безпеки.

Оскільки підприємства все частіше мігрують до хмарних середовищ, виникають нові проблеми безпеки, такі як неправильно налаштовані хмарні сховища, несанкціонований доступ та витоки даних. Для вирішення цих ризиків розробляються технології хмарної безпеки наступного покоління.

Передові технології хмарної безпеки:

– конфіденційні обчислення: ця нова технологія шифрує дані не лише під час зберігання та передачі, але й під час обробки, запобігаючи несанкціонованому доступу постачальників хмарних послуг або зловмисних інсайдерів;

– безпечний доступ до сервісу на межі (SASE): SASE інтегрує мережеву безпеку (брандмауери, VPN та Zero Trust) з хмарними рішеннями безпеки, щоб забезпечити безпечний віддалений доступ та виявлення загроз у кількох хмарних середовищах;

– хмарні платформи захисту застосунків (CNAPP): CNAPP забезпечують комплексну безпеку для хмарних додатків, виявляючи вразливості, забезпечуючи дотримання політик безпеки та запобігаючи неправильним конфігураціям, які можуть призвести до криптоатак.

Стратегії пом'якшення наслідків для хмарної безпеки:

– впровадження багатофакторної автентифікації (MFA) для запобігання несанкціонованому доступу;

– шифрування конфіденційних хмарних даних для захисту від порушень;

– використання інструментів хмарної безпеки на базі штучного інтелекту для виявлення аномальної активності.

З огляду на те, що підприємства все більше покладаються на хмарну інфраструктуру, посилення хмарної безпеки є головним пріоритетом для запобігання кіберзагрозам та забезпечення цілісності, доступності та конфіденційності даних.

Таким чином, кіберзагрози стають все більш складними, а атаки на базі штучного інтелекту, програми-вимагачі та вразливості ланцюга поставок створюють серйозні ризики. Хоча нові технології, такі як штучний інтелект, блокчейн та квантова криптографія, пропонують перспективні рішення, кібербезпека залишається предметом постійної боротьби. Організації повинні застосовувати проактивні стратегії безпеки, інвестувати в кваліфікованих фахівців та впроваджувати передові системи безпеки для захисту від кіберзагроз, що постійно змінюються.

4. Аналіз систем стандартизації інформаційної безпеки з кіберзахисту КІ. Стандарти, що застосовуються до інформаційної безпеки, надзвичайно численні, від суто технічних, низькорівневих специфікацій криптопротоколів до високорівневих структур організаційного управління [25]. Промислові системи управління, серед яких системи КІ, все ще мають свій власний набір проблем та особливостей, незважаючи на тенденцію конвергенції до основних інформаційних технологій та мереж. Проведемо аналіз застосування стандартів у сфері захисту КІ, їх вибір, впровадження та економічні витрати та вигоди в контексті існуючого правового ландшафту, зокрема в контексті міжнародного, Європейського Союзу та Рамкової програми кібербезпеки США.

У широкому сенсі стандарти можна класифікувати за двома змінними: технічний рівень та наявність схем сертифікації. У сфері інформаційної безпеки специфікації криптографічних алгоритмів є прикладами технічних стандартів, а схеми оцінки ризиків – прикладами організаційних стандартів. Деякі організаційні схеми є сертифікованими, що означає, що третя сторона незалежно оцінює організацію та заявляє, що вона відповідає вимогам стандарту.

Серед організацій, що розробляють стандарти, найбільш актуальними в європейському контексті є Європейський комітет зі стандартизації (CEN), Європейський комітет зі стандартизації в галузі електротехніки (CENELEC) та Європейський інститут телекомунікаційних стандартів (ETSI). Вони також офіційно визнані Європейською комісією та можуть законно бути одержувачами запитів на стандартизацію. Їхні сфери компетенції можуть перетинатися – наприклад, інформаційна безпека та

кібербезпека – але їхній вибірковий склад та діяльність досить різні. У той час як членство в CEN-CENELEC складається з національних органів стандартизації, що входять до системи ISO (міжнародної організації зі стандартизації) та IEC (міжнародна електротехнічна комісія), членство в ETSI переважно базується на галузевих організаціях, а також включає академічні установи та національні адміністрації. Усі вони працюють, намагаючись досягти консенсусу між членами. Процес та продукти ETSI, як правило, більш технічно орієнтовані, ринково орієнтовані та швидші.

Міжнародний стандарт ДСТУ ISO/IEC 27001:2023 – це структура управління, яка визначає вимоги до управління безпекою інформаційних систем. Вона базується на концепції управління ризиками та безперервному циклі оцінки ризиків. Основні вимоги та можливості стандарту 27001 зображені на рис. 3. Окремо варто розглянути та виділити важливі вимоги, серед них: контекст організації, лідерство, планування, підтримка, операційна діяльність, оцінка результативності та вдосконалення. Вони демонструють важливість комплексного підходу до управління інформаційної безпекою , що включає не лише технічні, але й організаційні та людські фактори.

Слід зазначити, що загальноприйнятої системи управління ризиками для систем захисту КІ від кіберзагроз та кіберінцидентів не існує, і що система ДСТУ ISO 31000:2014 для управління ризиками може вважатися доповненням до ДСТУ ISO/IEC 27001:2023.

Рис. 3. Вимоги та можливості стандарту ДСТУ ISO/IEC 27001

Актуальними для сфери захисту критичної інформаційної інфраструктури є інші рекомендації, які є частиною сімейства стандартів 27xxx, наприклад, ДСТУ ISO/IEC 27032:2024 з кібербезпеки, ДСТУ ISO/IEC 27033-5:2016 з мережевої безпеки ДСТУ ISO/IEC 27037:2017, ДСТУ ISO/IEC 27041:2022 та ДСТУ ISO/IEC 27042:2016, що стосуються реагування на кіберінциденти.

Директива NIS2 2024 – це посилення протидії кіберзлочинності Європейського Союзу: розширення сфери застосування; уніфікація вимог безпеки; підвищення відповідальності (рис. 4). Це означає, що відтепер більше компаній і державних установ зобов'язані дотримуватися жорстких стандартів кібербезпеки. Директивою запропоновано: вимоги до безпеки, звітування про інциденти, контроль і забезпечення виконання вимог, безпека ланцюга постачання. Імплементація Директиви NIS2 є важливим кроком для інтеграції України у цифровий ринок ЄС.

Рис. 4. Сфера застосування директиви NIS2 ЄС

Кібербезпека та захист КІ від кібератак добре розвинені у США і навіть вважаються урядом пріоритетом національної безпеки. Стандартні рамки є більш розвиненими та зрілими та спрямовані на

прямі політичні внески виконавчої гілки влади до розробки добровільної Рамкової програми кібербезпеки «Покращення кібербезпеки критичної інфраструктури».

Стандарт Національного інституту стандартів і технологій (NIST) 800 53 – це система оцінки ризиків, орієнтований на федеральні урядові установи США та їхніх підрядників. Стандарт отримав широке визнання також за межами США завдяки власним заслугам та впливу її розробників.

NIST 800-53 можна розглядати як аналог ДСТУ ISO 31000:2014 – це дуже консолідована та зріла система, яка постійно оновлюється та підтримується в актуальному стані. Вона структурована на основі трирівневої базової безпеки та відповідного набору засобів контролю системного ризику: низький вплив, помірний вплив та високий вплив. Крім того, вона містить посібник з вибору засобів контролю на основі кількох прикладів та варіантів використання. Отже, надаються деякі деталі впровадження, на відміну від документів ISO.

Більш важливим для захисту критичної інфраструктури є фреймворк (NIST Framework) – це набір рекомендацій та вказівок для покращення кібербезпеки в організаціях та інших інфраструктурних системах. Основний принцип Framework визначає п'ять функцій кібербезпеки: ідентифікацію, захист, виявлення, реагування та відновлення (рис. 5).

Рис. 5. Функції кібербезпеки NIST Framework

Цей фреймворк дозволяє організаціям розробляти та впроваджувати стратегії кібербезпеки, враховуючи специфічні умови і виклики. Такий підхід стає особливо важливим в умовах мінливого кіберзлочинного середовища, де важливо постійно удосконалювати та підтримувати заходи забезпечення кібербезпеки.

Північноамериканська корпорація з надійності електроенергетики (NERC) – це корпорація з захисту критичної інфраструктури (CIP), що контролюється урядом і відповідає за ланцюг постачання електроенергетичної системи. Електромережа відіграє ключову роль серед критичних інфраструктур, оскільки вона є необхідним фактором для майже всіх інших.

З перших років існування стандартів CIP Міжнародне товариство автоматизації (ISA) через комітет ISA99 розробило серію галузевих стандартів для вирішення питань кібербезпеки операційних технологій електроенергетичної системи. ISA та IEC домовилися про співпрацю в розробці цих стандартів, які сьогодні визнані як стандарти ДСТУ ISA/IEC 62443:2022. Кілька з цих стандартів безпосередньо стосуються життєвого циклу розробки технічної безпеки продуктів.

Процес управління ризиками ланцюга поставок ідеально підходить для забезпечення того, щоб ключові можливості кібербезпеки були враховані постачальниками або виробниками оригінального обладнання. Визнаючи зв'язок між стандартами NERC CIP та стандартами ДСТУ ISA/IEC 62443:2022, галузь може використовувати сертифікації, що пропонуються для сімейства стандартів ДСТУ ISA/IEC 62443:2022, щоб допомогти забезпечити відповідність стандартам NERC CIP. Крім того, серія ДСТУ ISA/IEC 62443:2022 включає різноманітні міжнародно визнані вимоги, які оцінюються та перевіряються.

Керівні принципи безпеки та ресурси користувачів для систем промислової автоматизації та управління, розроблені Американським інститутом національних стандартів (ANSI) та пізніше були подані до IEC як стандарт ДСТУ ISA/IEC 62443:2022.

Захист безпеки КІ є важливим елементом державної політики стандартизації за моделлю аналізу витрат і вигод. Ця модель застосовується при виборі інвестиційних проєктів в інфраструктуру. Згідно з моделлю, вигоди повинні перевищувати витрати, щоб варіант політики був життєздатним, і, коли доступно кілька варіантів, обирається той, що тягне за собою найбільшу чисту вигоду. Питання, що стоїть перед регуляторами, полягає в тому, щоб зобов'язати операторів критичної інфраструктури приймати існуючі стандарти. На сьогоднішній день NERC CIP є єдиним прикладом обов'язкового стандарту.

Таким чином, у захисті КІ переваги обов'язкової технічної стандартизації досить очевидні. Однак забезпечення дотримання стандартів захисту КІ залишається значним викликом для багатьох комунальних підприємств, оскільки їм перешкоджають такі фактори, як обмеженість ресурсів, розвиток ландшафту загроз та складність регулювання.

5. Кращі практики кіберзахисту критичної інфраструктури, життєво важливих послуг та ланцюгів постачання. Поточний стан управління ризиками кіберланцюжка постачання у секторах КІ в усьому світі важко узагальнити.

З одного боку, можна стверджувати, що значна частина КІ на деяких ринках належить та управляється приватним сектором. У США, за офіційними оцінками, приватна власність на КІ становить 85%. У ЄС цей показник становить 80%. У Великій Британії приблизно 50% КІ належить та управляється приватним сектором, тоді як на багатьох інших ринках, таких як Китай, Близький Схід та інші, державна власність на КІ є поширеною моделлю.

З іншого боку, різні суб'єкти приватного сектору та державні структури, які складають глобальну спільноту власників та операторів КІ, є такими ж різноманітними, як і численними. Ці суб'єкти охоплюють спектр від великих багатонаціональних корпорацій до малих незалежних виробників, постачальників послуг, незалежних підрядників та субпідрядників.

Різниця в ключових визначеннях, серед іншого, може призвести до викликів у міжнародній політиці під час спроб розробити міжнародні найкращі практики та правила, спрямовані на посилення кібербезпеки та стійкості КІ на регіональному або глобальному рівні.

Існує широке визнання, що для досягнення більш ефективної безпеки ланцюгів поставок фахівці повинні вирішувати проблему комплексно. Наприклад, зменшення ризиків у ланцюжку поставок програмного забезпечення вимагає включення надійних практик безпеки у внутрішній процес кодування на початку циклу розробки продукту, захищаючи як комерційне програмне забезпечення сторонніх розробників, так і програмне забезпечення з відкритим кодом. Таким чином, у добре забезпечених організаціях із розвиненими програмами безпеки розробники запровадили такі практики, як послідовні перевірки коду, дисциплінований внутрішній управління вразливостями та протоколи [2].

Багато постачальників інформаційно-комунікаційних технологій та послуг використовують програмне забезпечення з відкритим вихідним кодом для своїх програмних проєктів та продуктів з метою надання постачальникам комунікаційних послуг можливості створювати відкриті, сумісні мережі за нижчою ціною.

Використання програмного забезпечення з відкритим вихідним кодом вимагає вищого рівня належної перевірки, який організації можуть впроваджувати, застосовуючи найкращі галузеві практики для управління ланцюгом постачання, безпечної розробки програмного забезпечення та безпечного обслуговування програмного забезпечення [3].

Глобалізація ланцюгів постачання підприємств ставить нові виклики для забезпечення ефективного управління ризиками відповідно до національних інтересів безпеки, що може вимагати додаткових вимог.

Схвалений Європою Регламент (ЄС) 2022/2554 про цифрову операційну стійкість фінансового сектору [20], який набув чинності з січня 2025 року, додатково перевірить захист ланцюгів постачання. Він включає, серед іншого, положення щодо контрактів, стандартів безпеки, управління ризиками, прав доступу, інспекції та аудиту постачальників, навчання з питань ризиків та стійкості, а також підвищення обізнаності персоналу та структур управління з питань управління безпекою.

Глобальна асоціація мобільних операторів (GSMA) та Національний інститут стандартів і технологій (NIST) США розробили рекомендації щодо безпеки IoT для виробників та їхніх третіх сторін, які надають підтримку, під час розробки, тестування, продажу та підтримки пристроїв IoT для всього спектру клієнтів.

Заходи безпеки IoT повинні бути адаптовані до клієнтів, програм та/або середовищ. Адаптація може бути спрямована на бізнес-сектори або вертикальні галузі та може додавати вимоги, редагувати конкретні вимоги, звужуючи або розширюючи способи їх застосування, або, в рідкісних випадках, видаляти вимоги.

Метою має бути досягнення гармонізованих вимог на всіх ринках на основі передового досвіду бізнесу та міжнародних стандартів. Багато попередніх зусиль щодо гармонізації вимог та оцінок не змогли досягти згоди та, на жаль, збільшили складність дотримання вимог, тим самим збільшуючи ризик. Як наслідок, генеральним підрядникам конкретних послуг стає важко та дорого розуміти ризики, пов'язані з кількома субпідрядниками, та управляти ними.

Таким чином, міжнародна співпраця щодо зобов'язань звітування про інциденти для операторів КІ є ще однією бажаною сферою співпраці, де міжнародне узгодження може зменшити складність та адміністративне навантаження, водночас забезпечуючи доступність відповідної та своєчасної інформації для підвищення ситуаційної обізнаності та з часом розширення сукупних знань. Для подальшого розвитку слід і надалі заохочувати кроки, вжиті між США та ЄС для впорядкування зобов'язань щодо звітування про інциденти, а також з часом розширювати географічно на відповідних міжнародних форумах.

Крім того, для підтримки стійкості, безпеки, довіри та конкурентоспроможності мереж і ланцюгів постачання ключовим фактором є диверсифікація. Рішення щодо національної безпеки, що обмежують критичні або чутливі компоненти від певних постачальників, повинні ґрунтуватися на об'єктивних критеріях, бути пропорційними та ефективно впроваджуватися. Виключення постачальників може мати значний вплив на витрати приватних операторів КІ, а також впливати на національну безпеку, стійкість та розвиток ринку. Отже, такі рішення також повинні враховувати, що приватні оператори КІ не несуть відповідальності за національну безпеку і не обов'язково враховують ризики національної безпеки у своїх бізнес-рішеннях.

Спільний та скоординований підхід усіх зацікавлених сторін – це найкращий засіб, за допомогою якого уряди підвищать базові стандарти кібербезпеки, уникаючи надмірної звітності, водночас створюючи ефективну спільну практику, засновану на довірі, особливо в ланцюжку постачання.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Зростаюче використання пристроїв IoT у КІ трансформувало такі галузі, як енергетика, охорона здоров'я, транспорт та фінанси, покращивши операційну ефективність та моніторинг у режимі реального часу. Однак безпрецедентне зростання впровадження технологій IoT принесло величезні загрози безпеці, які підривають стабільність, цілісність та захист таких критичних систем.

Проблема запровадження масштабованих та адаптивних рішень безпеки наражає КІ на ризик збоїв, витоків даних та системних збоїв, що може мати далекосяжні наслідки для національної безпеки, громадської безпеки та економічної стабільності. Тому існує потреба в проведенні систематичного аналізу потенціалу технологій IoT в системі кіберзахисту КІ, обґрунтуванні комплексного підходу щодо інтеграції цілій кібербезпеки, IoT технологій, рішень кібербезпеки КІ, систем стандартизації та кращих практик в систему кіберзахисту КІ.

Аналіз фундаментальних цілей кіберрбезпеки КІ визначає наступну ієрархію їх пріоритетності в процесах інтеграції технологій IoT до КІ: безпека людей та довкілля, доступність, цілісність, стійкість і відновлення, конфіденційність. Така ієрархія визначає, насамперед, певні вимоги до побудови інтегрованих систем контролю доступу на основі IoT за атрибутами: обчислення, зв'язок, сумісність, надійність та стійкість.

Аналіз основних технологій IoT, що використовуються в системах безпеки КІ, дозволів визначити структуру системи безпеки IoT до складових якої відносяться: пристрої збору даних, шлюзи та контролери, мережа передачі даних, центральний сервер або хмарна платформа, програмне забезпечення для керування та моніторингу, система автоматичного реагування та аналітичні інструменти та штучний інтелект. Інтеграція названих технологій IoT дозволяє: створити інтегровані системи безпеки, зменшити вплив людського фактору, забезпечити швидке реагування на інциденти, оптимізувати витрати на безпеку, підвищити загальний рівень безпеки об'єктів.

Практичне значення роботи полягає у виявленні перспектив розвитку IoT у секторі безпеки КІ, зокрема шляхом інтеграції штучного інтелекту, технологій 5G та впровадження децентралізованих підходів до інформаційної безпеки. Однією з ключових тенденцій є поєднання IoT зі штучним інтелектом для створення інтелектуальних систем безпеки, здатних до незалежного аналізу даних та прогнозування загроз. Штучний інтелект дозволить виявляти потенційні небезпеки в режимі реального часу, аналізувати складні моделі поведінки та автоматизувати реагування на інциденти.

В статті проаналізовано особливості застосування стандартів у сфері кіберзахисту КІ як з організаційної, так і з технічної точки зору, їх вибір, впровадження, економічні витрати та вигоди в контексті існуючого правового ландшафту. Серед організацій, що розробляють стандарти, найбільш актуальними є міжнародні організації, Європейського Союзу та Рамкової програми кібербезпеки США. Завданнями державної політики є забезпечення прийняття існуючих стандартів операторами КІ. Однак забезпечення дотримання стандартів захисту КІ залишається значним викликом для багатьох комунальних підприємств, оскільки їм перешкоджають такі фактори, як обмеженість ресурсів, розвиток ландшафту загроз та складність регулювання.

Ключовим фактором захисту кібербезпеки життєво важливих послуг та КІ є диверсифікація зобов’язань всіх постачальників послуг у поєднанні з відповідною національною та міжнародною нормативно-правовою базою. Міжнародна співпраця щодо зобов'язань звітування про інциденти для операторів КІ може зменшити складність та адміністративне навантаження, водночас забезпечуючи доступність відповідної та своєчасної інформації для підвищення ситуаційної обізнаності та з часом розширення сукупних знань.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ahmad, T., & Zhang, D. (2021). Using the Internet of Things in smart energy systems and networks. *Sustainable Cities and Society*, 68, 102783. https://doi.org/10.1016/j.scs.2021.102783
2. Tech Accord. (2023). *Best practice alignment for supply chain security across standards and regulatory frameworks*. https://cybertechaccord.org/best-practice-alignment-for-supply-chain-security-across-standards-and-regulatory-frameworks/
3. Cybersecurity and Infrastructure Security Agency. (2023). *Open source software security roadmap*. https://www.cisa.gov/sites/default/files/2024-02/CISA-Open-Source-Software-Security-Roadmap-508c.pdf
4. Clotet, X., Moyano, J., & Leon, G. (2018). A real-time anomaly-based IDS for cyber-attack detection at the industrial process level of critical infrastructures. *International Journal of Critical Infrastructure Protection*, 23, 11-20. https://doi.org/10.1016/j.ijcip.2018.08.002
5. Dede, G., Petsa, A. M., Kavalaris, S., Serrelis, E., Evangelatos, S., Oikonomidis, I., & Kamalakis, T. (2024). Cybersecurity as a contributor toward resilient Internet of Things (IoT) infrastructure and sustainable economic growth. *Information*, 15(12), 798. https://doi.org/10.3390/info15120798
6. Demir, K., Ismail, H., Vateva-Gurova, T., & Suri, N. (2018). Securing the cloud-assisted smart grid. *International Journal of Critical Infrastructure Protection*, 23, 100-111. https://doi.org/10.1016/j.ijcip.2018.08.004
7. Dommari, S., & Jain, A. (2022). The impact of IoT security on critical infrastructure protection: Current challenges and future directions. *International Journal of Research in Modern Engineering and Emerging Technology*, 10(1). https://doi.org/10.63345/ijrmeet.org.v10.i1.6
8. Elbehiery, K., & Elbehiery, H. (2019). 5G as a service (5GaaS). *SSRG International Journal of Electronics and Communication Engineering*, 6(8), 22-30. https://doi.org/10.14445/23488549/IJECE-V6I8P104
9. Farris, I., Taleb, T., Khettab, Y., & Song, J. (2019). A survey on emerging SDN and NFV security mechanisms for IoT systems. *IEEE Communications Surveys & Tutorials*, 21(1), 812-837.
10. Haller, P., Genge, B., & Duka, A.-V. (2019). On the practical integration of anomaly detection techniques in industrial control applications. *International Journal of Critical Infrastructure Protection*, 24, 48-68. https://doi.org/10.1016/j.ijcip.2018.10.008
11. Jha, M. K. (2025). From IoT to critical infrastructure battling next-gen cyber threats. *International Journal of Engineering Trends and Applications*, 12(5), 48-57.
12. Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection*, 25, 36-49. https://doi.org/10.1016/j.ijcip.2019.01.001
13. Leszczyna, R. (2019). Standards with cybersecurity controls for smart grid: A systematic analysis. *International Journal of Communication Systems*, 32(6), e3910. https://doi.org/10.1002/dac.3910
14. Makupi, D., & Masese, N. (2019). Determining information security maturity level of an organization based on ISO 27001. *SSRG International Journal of Computer Science and Engineering*, 6(7), 5-11. https://doi.org/10.14445/23488387/IJCSE-V6I7P102
15. Moore, S. J., Nugent, C. D., Zhang, S., et al. (2020). IoT reliability: A review leads to five key research directions. *CCF Transactions on Pervasive Computing and Interaction*, 2(3), 147-163. https://doi.org/10.1007/s42486-020-00037-z
16. Motlagh, H. N., et al. (2020). Internet of Things (IoT) and the energy sector. *Energies*, 13(2), 1-27. https://doi.org/10.3390/en13020494
17. Paliwal, S., & Hasan, S. O. (2017). 5G as the principal enabler towards the establishment of IoT society. In *Proceedings of the International Conference on I-SMAC (IoT in Social, Mobile, Analytics, and Cloud)* (pp. 16-21).
18. Priya, N. (2022). Cybersecurity considerations for industrial IoT in critical infrastructure sector. *International Journal of Computer and Organization Trends*, 12(1), 27-36. https://doi.org/10.14445/22492593/IJCOT-V12I1P306
19. Qassim, Q., Jamil, N., Daud, M., & Hasan, H. (2019). Towards implementing scalable and reconfigurable SCADA security testbed in the power system environment. *International Journal of Critical Infrastructures*, 15(2), 91-120. https://doi.org/10.1504/IJCIS.2019.098834
20. European Parliament and Council. (2022). *Regulation (EU) 2022/2554 on digital operational resilience for the financial sector*. https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

21. Rodofile, N. R., Radke, K., & Foo, E. (2019). Extending the cyber-attack landscape for SCADA-based critical infrastructure. *International Journal of Critical Infrastructure Protection*, 25, 14-35. https://doi.org/10.1016/j.ijcip.2019.01.002
22. Russell, L., Goubran, R., Kwamena, F., & Knoefel, F. (2018). Agile IoT for critical infrastructure resilience: Cross-modal sensing as part of a situational awareness approach. *IEEE Internet of Things Journal*, 5(6), 4454-4465.
23. Sotnik, S. (2024). Integration of IoT into security systems: Opportunities and risks. *International Journal of Academic Engineering Research*, 8(11), 56-61.
24. Yu, S., Lv, K., Shao, Z., Guo, Y., Zou, J., & Zhang, B. (2018). A high-performance blockchain platform for intelligent devices. In *2018 IEEE International Conference on Hot Information-Centric Networking (HotICN)* (pp. 260-261).
25. Klimushyn, P. S. (2025). Communication technologies and specialized protocols for ensuring cybersecurity of the Internet of Things. *Law and Security*, 2(97), 52-68. https://doi.org/10.32631/pb.2025.2.05
26. Klimushyn, P. S. (2025). Problematic aspects of cybersecurity standardization of the Internet of Things. *Law and Security*, 1(96), 53-66. https://doi.org/10.32631/pb.2025.1.05
27. Klimushyn, P. S., Roh, V. Y., & Kolisnyk, T. P. (2023). Legal aspects of standardization of functional safety of the Internet of Things. *Law and Security*, 3(90), 200-213. https://doi.org/10.32631/pb.2023.3.17

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023

Petro Klimushyn
PhD, Associate Professor of the Department of Computer Systems and Robotics
V. N. Karazin Kharkiv National University
ORCID: 0000-0002-1020-9399
klimushyn@karazin.ua

Maksym Khruslov
PhD, Senior Researcher, Associate Professor,
Head of the Department of Computer Systems and Robotics
V. N. Karazin Kharkiv National University
ORCID: 0000-0001-9639-9340
maksym.khruslov@karazin.ua

Tetyana Kolisnyk
PhD, Associate Professor of the Department of Cybersecurity and DATA-Technologies
Kharkiv National University of Internal Affairs
ORCID:0000-0002-7442-8136
ktp201505@gmail.com

Inna Khavina
PhD, Associate Professor of the Department of Cybersecurity and DATA-Technologies
Kharkiv National University of Internal Affairs
ORCID: 0000-0002-1856-1186
inna.khavina25@gmail.com

Volodymyr Tulupov
PhD, Associate Professor of the Department of Cybersecurity and DATA-Technologies
Kharkiv National University of Internal Affairs
ORCID: 0000-0003-4794-743X
madey1969@gmail.com

INTEGRATION OF INTERNET OF THINGS TECHNOLOGIES INTO CRITICAL INFRASTRUCTURE CYBERPROTECTION SYSTEMS

Abstract. The problem of studying the opportunities and risks of integrating the Internet of Things into critical infrastructure security systems is extremely relevant, as it involves a comprehensive analysis of the benefits and challenges that arise during the implementation of innovative technologies in the security sector. On the one hand, the Internet of Things opens up great opportunities for automating security processes, increasing the effectiveness of monitoring and responding to threats in real time, and on the other hand, this technology carries with it new risks associated with the vulnerability of devices to cyber threats, ethical issues of using autonomous systems and problems of integrating various technologies into a single secure ecosystem. To solve this problem, the article achieves the following results. Existing research in the field of critical infrastructure cybersecurity and the Internet of Things as a common secure ecosystem is analyzed. Literature sources are classified into three areas: cybersecurity of critical infrastructure, cybersecurity of Internet of Things environments and research in common areas. The lack of a holistic approach in joint research of interconnected critical infrastructure environments and the Internet of Things has been identified. The fundamental goals and their priority for cybersecurity of critical infrastructure and the Internet of Things as a single system have been proven, based on the classic CIA triad (confidentiality, integrity, availability), however, the priority of fundamental cybersecurity goals in the processes of integrating Internet of Things technologies into critical structures should be carried out in the following order: safety of people and the environment, availability, integrity, resilience and recovery, confidentiality. The main Internet of Things technologies used in critical infrastructure have been investigated and a structured security system in the form of interconnected components has been provided, which allows creating integrated security systems, reducing the impact of the human factor, ensuring rapid response to incidents, optimizing security costs, and increasing the overall level of security of facilities. Innovative cybersecurity solutions in the critical infrastructure sector are substantiated: systems based on

artificial intelligence and machine learning (analysis of network and device behavior, automatic response to incidents); decentralized security management to ensure confidentiality and data integrity based on blockchain technology; quantum methods for data encryption and key distribution in secure communication networks; zero-trust architecture and cloud security systems (confidential computing, secure access to the service, cloud application protection platforms). Innovations in critical infrastructure cybersecurity allow: to reduce the time to detect and respond to attacks; to increase resistance to targeted attacks; to integrate environment protection into a single strategy. Existing information security standardization systems for critical infrastructure protection are analyzed by technical level and availability of certification schemes. Standards for the Internet of Things and distributed critical infrastructure systems are becoming a mandatory element of cyber protection. They provide unified requirements for the security of devices, networks and processes. They ensure the integration of devices and systems, increasing the resilience of critical infrastructure to modern cyber threats.

Keywords: critical infrastructure, Internet of Things, technology integration, cybersecurity, standardization systems, artificial intelligence, machine learning, blockchain, quantum technologies.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Ahmad, T., & Zhang, D. (2021). Using the Internet of Things in smart energy systems and networks. *Sustainable Cities and Society*, 68, 102783. https://doi.org/10.1016/j.scs.2021.102783
2. Tech Accord. (2023). *Best practice alignment for supply chain security across standards and regulatory frameworks*. https://cybertechaccord.org/best-practice-alignment-for-supply-chain-security-across-standards-and-regulatory-frameworks/
3. Cybersecurity and Infrastructure Security Agency. (2023). *Open source software security roadmap*. https://www.cisa.gov/sites/default/files/2024-02/CISA-Open-Source-Software-Security-Roadmap-508c.pdf
4. Clotet, X., Moyano, J., & Leon, G. (2018). A real-time anomaly-based IDS for cyber-attack detection at the industrial process level of critical infrastructures. *International Journal of Critical Infrastructure Protection*, 23, 11-20. https://doi.org/10.1016/j.ijcip.2018.08.002
5. Dede, G., Petsa, A. M., Kavalaris, S., Serrelis, E., Evangelatos, S., Oikonomidis, I., & Kamalakis, T. (2024). Cybersecurity as a contributor toward resilient Internet of Things (IoT) infrastructure and sustainable economic growth. *Information*, 15(12), 798. https://doi.org/10.3390/info15120798
6. Demir, K., Ismail, H., Vateva-Gurova, T., & Suri, N. (2018). Securing the cloud-assisted smart grid. *International Journal of Critical Infrastructure Protection*, 23, 100-111. https://doi.org/10.1016/j.ijcip.2018.08.004
7. Dommari, S., & Jain, A. (2022). The impact of IoT security on critical infrastructure protection: Current challenges and future directions. *International Journal of Research in Modern Engineering and Emerging Technology*, 10(1). https://doi.org/10.63345/ijrmeet.org.v10.i1.6
8. Elbehiery, K., & Elbehiery, H. (2019). 5G as a service (5GaaS). *SSRG International Journal of Electronics and Communication Engineering*, 6(8), 22-30. https://doi.org/10.14445/23488549/IJECE-V6I8P104
9. Farris, I., Taleb, T., Khettab, Y., & Song, J. (2019). A survey on emerging SDN and NFV security mechanisms for IoT systems. *IEEE Communications Surveys & Tutorials*, 21(1), 812-837.
10. Haller, P., Genge, B., & Duka, A.-V. (2019). On the practical integration of anomaly detection techniques in industrial control applications. *International Journal of Critical Infrastructure Protection*, 24, 48-68. https://doi.org/10.1016/j.ijcip.2018.10.008
11. Jha, M. K. (2025). From IoT to critical infrastructure battling next-gen cyber threats. *International Journal of Engineering Trends and Applications*, 12(5), 48-57.
12. Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection*, 25, 36-49. https://doi.org/10.1016/j.ijcip.2019.01.001
13. Leszczyna, R. (2019). Standards with cybersecurity controls for smart grid: A systematic analysis. *International Journal of Communication Systems*, 32(6), e3910. https://doi.org/10.1002/dac.3910
14. Makupi, D., & Masese, N. (2019). Determining information security maturity level of an organization based on ISO 27001. *SSRG International Journal of Computer Science and Engineering*, 6(7), 5-11. https://doi.org/10.14445/23488387/IJCSE-V6I7P102

15. Moore, S. J., Nugent, C. D., Zhang, S., et al. (2020). IoT reliability: A review leads to five key research directions. *CCF Transactions on Pervasive Computing and Interaction*, 2(3), 147-163. https://doi.org/10.1007/s42486-020-00037-z
16. Motlagh, H. N., et al. (2020). Internet of Things (IoT) and the energy sector. *Energies*, 13(2), 1-27. https://doi.org/10.3390/en13020494
17. Paliwal, S., & Hasan, S. O. (2017). 5G as the principal enabler towards the establishment of IoT society. In *Proceedings of the International Conference on I-SMAC (IoT in Social, Mobile, Analytics, and Cloud)* (pp. 16-21).
18. Priya, N. (2022). Cybersecurity considerations for industrial IoT in critical infrastructure sector. *International Journal of Computer and Organization Trends*, 12(1), 27-36. https://doi.org/10.14445/22492593/IJCOT-V12I1P306
19. Qassim, Q., Jamil, N., Daud, M., & Hasan, H. (2019). Towards implementing scalable and reconfigurable SCADA security testbed in the power system environment. *International Journal of Critical Infrastructures*, 15(2), 91-120. https://doi.org/10.1504/IJCIS.2019.098834
20. European Parliament and Council. (2022). *Regulation (EU) 2022/2554 on digital operational resilience for the financial sector*. https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng
21. Rodofile, N. R., Radke, K., & Foo, E. (2019). Extending the cyber-attack landscape for SCADA-based critical infrastructure. *International Journal of Critical Infrastructure Protection*, 25, 14-35. https://doi.org/10.1016/j.ijcip.2019.01.002
22. Russell, L., Goubran, R., Kwamena, F., & Knoefel, F. (2018). Agile IoT for critical infrastructure resilience: Cross-modal sensing as part of a situational awareness approach. *IEEE Internet of Things Journal*, 5(6), 4454-4465.
23. Sotnik, S. (2024). Integration of IoT into security systems: Opportunities and risks. *International Journal of Academic Engineering Research*, 8(11), 56-61.
24. Yu, S., Lv, K., Shao, Z., Guo, Y., Zou, J., & Zhang, B. (2018). A high-performance blockchain platform for intelligent devices. In *2018 IEEE International Conference on Hot Information-Centric Networking (HotICN)* (pp. 260-261).
25. Klimushyn, P. S. (2025). Communication technologies and specialized protocols for ensuring cybersecurity of the Internet of Things. *Law and Security*, 2(97), 52-68. https://doi.org/10.32631/pb.2025.2.05
26. Klimushyn, P. S. (2025). Problematic aspects of cybersecurity standardization of the Internet of Things. *Law and Security*, 1(96), 53-66. https://doi.org/10.32631/pb.2025.1.05
27. Klimushyn, P. S., Roh, V. Y., & Kolisnyk, T. P. (2023). Legal aspects of standardization of functional safety of the Internet of Things. *Law and Security*, 3(90), 200-213. https://doi.org/10.32631/pb.2023.3.17

Отримано редакцією журналу / Received: 16.02.26
Прорецензовано / Revised: 28.02.26
Схвалено до друку / Accepted: 25.06.26