КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.34.1226
УДК 004.056:004.738.5

Вітів Назарій Андрійович
аспірант кафедри спеціалізованих комп'ютерних систем
Національний університет «Львівська політехніка», Львів, Україна
ORCID: 0009-0005-8225-9765
nazarii.vitiv.asp.2025@lpnu.ua

Гонсьор Оксана Йосипівна
к.т.н., доцент кафедри спеціалізованих комп'ютерних систем
Національний університет «Львівська політехніка», Львів, Україна
ORCID: 0000-0003-0895-5859
oksana.y.honsor@lpnu.ua

СИСТЕМАТИЧНИЙ АНАЛІЗ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В IOT-ПРИСТРОЯХ

Анотація. В даній роботі досліджено відомі методи забезпечення інформаційної безпеки, що є актуальними для IoT-пристроїв і враховують їх специфіку. Обґрунтовано актуальність проблеми захисту інформації в IoT, описано широкий діапазон існуючих підходів та необхідність їх комплексного застосування з урахуванням ресурсних обмежень пристроїв. Проаналізовано наукові праці дослідників, що охоплюють легковагову криптографію, системи виявлення вторгнень, апаратні методи захисту, блокчейн та методи штучного інтелекту. Розглянуто чотирирівневу архітектуру IoT-систем (рівень пристроїв, мережевий, платформний та рівень застосунків) з точки зору загроз і механізмів захисту, а також детально розглянуто концептуальні засади кожного методу: легковагова криптографія (алгоритми PRESENT, SPECK, SIMON, ASCON), системи виявлення вторгнень (IDS) на основі сигнатур, аномалій і машинного навчання, апаратні засоби захисту (TPM, Secure Boot, TEE, PUF), технологія блокчейн та методи з використанням штучного інтелекту. Для кожного методу систематизовано переваги та обмеження з урахуванням специфіки ресурсно-обмежених IoT-пристроїв. В заключному розділі проведено порівняльний аналіз зазначених методів за п'ятьма критеріями: ефективністю захисту даних, виявленням атак, адаптивністю, ресурсними витратами та оптимальним рівнем використання в архітектурі IoT. Наукова новизна роботи полягає в систематизації зазначених методів у єдиній порівняльній матриці з урахуванням оптимального рівня їх застосування в архітектурі IoT. На основі проведених досліджень обґрунтовано доцільність застосування комплексного підходу до забезпечення інформаційної безпеки, який передбачає інтеграцію різних механізмів захисту на всіх рівнях архітектури IoT.

Ключові слова: автентифікація; апаратні методи захисту; блокчейн; Інтернет речей; інформаційна безпека; криптографія; штучний інтелект.

ВСТУП

Інтернет речей (Internet of Things, IoT) це одна з ключових сучасних інформаційних технологій з великою перспективою подальшого розвитку. Інтернет речей – це така концепція, що складається із взаємозв'язаних пристроїв, які мають сенсори для збирання інформації про навколишній світ. Ці технології активно впроваджуються в промисловість, медицину, транспорт, енергетику і побут. IoT-системи базуються на використанні великої кількості пристроїв, які здатні комунікувати між собою, здійснювати збір, обробку і передачу даних.

Характерними особливостями IoT-пристроїв є обмеженість обчислювальних ресурсів і експлуатація їх в середовищах з низьким рівнем довіри. Ці особливості значно ускладнюють застосування традиційних механізмів захисту інформації в IoT і вимагають розробки спеціалізованих методів забезпечення конфіденційності, цілісності та доступності даних.

Існує широкий діапазон методів для забезпечення інформаційної безпеки в IoT-пристроях. Зокрема, криптографічні механізми захисту, методи автентифікації і контролю доступу, апаратні засоби захисту, системи виявлення вторгнень і виявлення аномалій, блокчейн, а також штучний інтелект. Проте жоден з перелічених методів не можна назвати «універсальним». Це обумовлює необхідність комплексного використання методів із урахуванням специфіки IoT.

Постановка проблеми. Інтенсивний розвиток Інтернету Речей останніми роками супроводжується зростанням кількості підключених пристроїв до мережі. Ці пристрої функціонують в різних критичних сферах – промисловості, енергетиці, медицині, транспорті, системах «розумного дому». Недоліки пристроїв IoT, такі як обмежені обчислювальні ресурси і низький рівень безпеки створюють передумови для виникнення широкого спектру кіберзагроз. Це зумовлює необхідність системного аналізу існуючих методів забезпечення інформаційної безпеки для IoT-пристроїв.

Незважаючи на значну кількість досліджень у сфері інформаційної безпеки в IoT, більшість із цих робіт зосереджені на окремих підходах до захисту інформації. В той же час, недостатньо уваги приділено комплексному аналізу і порівнянню цих методів між собою.

Аналіз останніх досліджень і публікацій. Питання інформаційної безпеки в Інтернеті речей активно піднімається і досліджується міжнародною науковою спільнотою. На сьогоднішній день для забезпечення захисту інформації пропонуються різні методи, а також поєднання різних методів захисту.

Одним із основних напрямків для забезпечення інформаційної безпеки із урахуванням специфіки IoT-пристроїв є легковагова криптографія (lightweight cryptography). В дослідженні [1] проведено огляд легковагових крипто-алгоритмів, порівняно ефективність та придатність їх для ресурсно-обмежених пристроїв. В [2] проведено аналіз конкретних алгоритмів і наведено рекомендації стосовно їх використання для IoT. Систематичний огляд 77 рецензованих праць за 2006–2025 рр. [3] охоплює легковагові схеми шифрування з урахуванням їх інтеграції з ШІ та блокчейном. В [4] здійснено порівняльний аналіз реалізацій алгоритмів ASCON і SPECK на мікроконтролерах ESP32 та MSP430.

Ще одним важливим напрямком і методом захисту інформації є використання методів виявлення вторгнень і аналізу підозрілої й аномальної активності. Так, в дослідженні [5] представлені IDS-підходи на основі аномалій і проведено оцінку точності виявлення загроз. Дослідження [6] пропонує нову систему виявлення вторгнень на основі аномалій для мереж IoT з використанням методу глибокого навчання, зокрема модель глибокої нейронної мережі (DNN) з фільтрацією ознак. В [7] порівняно різні техніки ШІ для покращення систем виявлення вторгнень. В [8] розглянуто підходи машинного навчання для захисту мереж IoT від атак та аномалій. Перспективним напрямком є також застосування TinyML для виявлення вторгнень безпосередньо на ресурсно-обмежених пристроях – відповідні моделі та їх ефективність досліджено в [9], [10].

Окрім програмних методів і засобів апаратний метод захисту є фундаментальним для забезпечення довіри до IoT-пристроїв. Так, в дослідженні [11] запропоновано апаратно-розширену систему безпеки, яка включає спеціалізовані чипи безпеки на всіх рівнях IoT. В роботі [12] проведено огляд апаратних засобів захисту для кінцевих пристроїв туманних обчислень в IoT. Питання автентифікації пристроїв на основі PUF без зберігання ключів у пам'яті розглядається в [13].

Ще одним методом, що набуває популярності є використання технології блокчейн як засобу захисту інформації в IoT-середовищі. Автори статті [14] досліджують потенціал технології блокчейн для вирішення критичних проблем безпеки в IoT. В [15] розглянуто поєднання методів криптографії і блокчейну, а також описуються проблеми інтеграції та перспективні напрями досліджень. В [16] здійснено аналіз комплексних підходів до безпеки IoT, в яких блокчейн використовується разом із криптографічними методами, а також автентифікацією та контролем доступу. В огляді [17] досліджено поєднання ШІ та блокчейну для побудови адаптивних систем захисту IoT. Дослідження [18] систематизує гібридні підходи, що включають ШІ, машинне навчання та блокчейн. Дослідження [19] розглядає інтеграцію блокчейну в IDS для безпеки IoT. Стаття [20] аналізує комплекс інтеграції IDS разом із блокчейном та криптографією. Федеративне навчання як метод збереження приватності при навчанні IDS-моделей розглядається в [21], [22].

Загальні огляди кіберзагроз, вразливостей та методів захисту IoT-систем, що формують контекст дослідження, представлені в [23], [24], [25].

Отже, як видно з проведеного огляду наукових досліджень, проблема захисту інформації в мережах IoT є важливою та актуальною в умовах сьогодення. Разом з тим, більшість існуючих робіт зосереджені на окремих підходах, і недостатньо уваги приділено їх комплексному порівняльному аналізу.

Мета статті. Метою даної статті є огляд і аналіз існуючих методів для захисту інформації з урахуванням специфіки IoT-пристроїв, порівняння цих методів і аналіз їхніх переваг і недоліків, придатності до використання в IoT-пристроях. На відміну від більшості існуючих оглядів, у дослідженні

вперше систематизовано зазначені методи у єдиній порівняльній матриці з урахуванням оптимального рівня їх застосування в архітектурі IoT, що формує наукову новизну даної роботи.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Рівні архітектури IoT з точки зору захисту інформації

Інтернет речей є багаторівневою системою, де кожен рівень має свої власні проблеми і механізми захисту для боротьби з ними. Загалом виділяють 4 рівні архітектури IoT-систем. Це рівень пристроїв, мережевий рівень, платформний рівень і рівень застосунків (рис.1).

Рівень пристроїв (Perception Layer) є найнижчим рівнем в цій архітектурі. Він відповідає за безпосередній збір інформації із навколишнього світу і обробку цієї інформації. Головними вразливостями цього рівня є фізичний доступ до пристрою, підміна прошивки й атака на інтерфейси (UART, I2C, SPI). Найкращими способами захисту буде застосовувати методи апаратного захисту інформації, такі як Secure Boot, TMP і інші.

Наступним в архітектурі йде мережевий рівень (Network Layer). Він відповідає за передачу даних і з'єднання із іншими пристроями через такі протоколи як Wi-Fi, LoRaWAN, Ethernet, тощо. Існує декілька векторів атак на даний рівень архітектури. Найвідоміші серед них це DDoS, Man-in-the-Middle і ризики перехоплення трафіку. Найкращими методами захисту цього рівня буде використання методів виявлення вторгнень і аналізу підозрілої й аномальної активності (IDS). Перспективним напрямком вважають поєднання IDS із блокчейном і ШІ для посилення захисту.

Третій згаданий рівень – платформний рівень (Platform Layer). Цей рівень складається із серверів, баз даних, API. Він відповідає за зберігання даних, аналітику цих даних, керування мережевими пристроями й інтеграцію із зовнішніми сервісами. Платформний рівень вразливий до витоку великих масивів даних, несанкціонованого доступу до баз даних, компрометації API. Для захисту цього рівня IoT використовуються такі механізми як автентифікація, шифрування даних у стані зберігання, RBAC (Role-Based Access Control) – обмеження доступу відповідно до ролей, використання API Gateway, токенів доступу.

Останнім згаданим рівнем є рівень застосунків (Application Layer). Цей рівень охоплює різні механізми для взаємодії із пристроєм і системою. Це є і веб-інтерфейси, і мобільні додатки, і системи керування IoT. Найбільшими загрозами на цьому рівні є ризики витоку персональних даних, атаки на веб-інтерфейси такі як XSS і CSRF. Для боротьби із даними загрозами впроваджують такі методи захисту, як багатофакторна автентифікація користувачів IoT-мережі, чи якогось конкретного пристрою. Для того, щоб уникати витоку персональних даних впроваджують шифрування даних користувача.

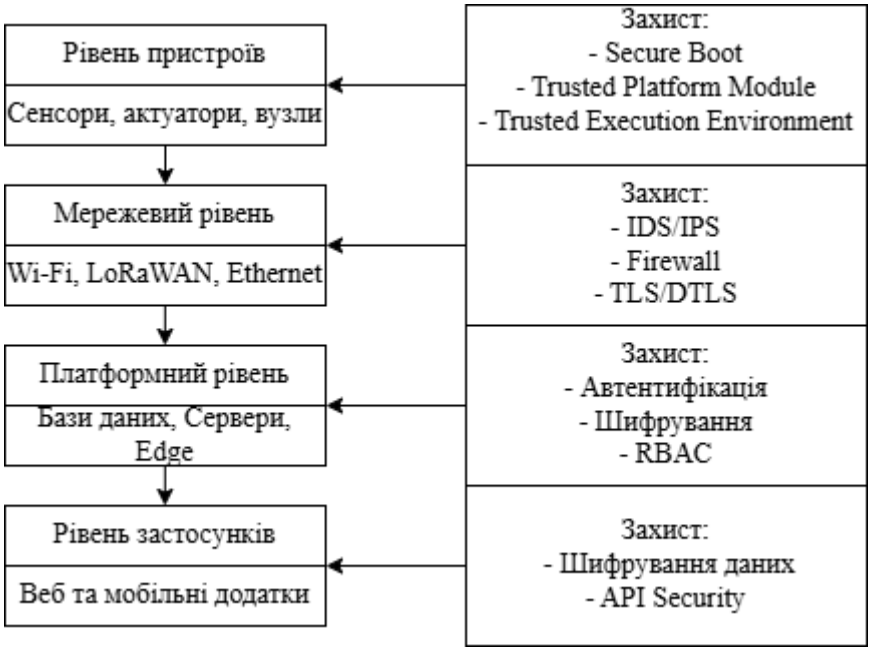

Рис. 1. Рівні архітектури IoT з точки зору захисту інформації

Легковагова криптографія

Легковагова криптографія (Lightweight cryptography) – це напрям сучасної криптографії, що орієнтований на розробку алгоритмів шифрування для пристроїв з обмеженими ресурсами, такими як мала обчислювальна потужність, обмежений обсяг пам'яті і низьке енергоспоживання. В контексті IoT-пристроїв застосування таких традиційних алгоритмів як RSA чи AES часто є надмірно ресурсоємним та знижує продуктивність пристроїв. Тому легковагова криптографія це вирішення для проблеми застосування криптографії в IoT-пристроях.

До найвідоміших прикладів легковагових алгоритмів шифрування можна віднести PRESENT, SPECK та SIMON, ASCON. PRESENT – це блочний шифр, з довжиною блоку 64 біти, оптимізований для апаратної реалізації. SPECK і SIMON – це сімейство шифрів, орієнтованих відповідно на програмну та апаратну реалізацію. ASCON – алгоритм автентифікованого шифрування, обраний американським Національним Інститутом Стандартів і Технологій для криптографії для пристроїв з обмеженими ресурсами. Усі ці алгоритми забезпечують баланс між крипостійкістю та ресурсною ефективністю, що є критичним для IoT-пристроїв.

Головними перевагами застосування методу легковагової криптографії є низьке енергоспоживання, мала вимога до пам'яті, висока швидкодія на слабких процесорах та можливість апаратної оптимізації. Низьке енергоспоживання при легковаговій криптографії гарантується тим, що зменшується кількість обчислювальних операцій, а це, в свою чергу, продовжує час автономної роботи пристрою. Легковагові криптографічні алгоритми оптимізовані для мікроконтролерів із лише десятками кілобайт пам'яті, і через цю оптимізацію вони використовують значно менше пам'яті аніж класичні криптографічні алгоритми. Структура операцій команд легковагових криптографічних алгоритмів є простою, за рахунок цього забезпечується вища швидкодія на слабких процесорах.

До недоліків і обмежень використання легковагових алгоритмів відносять потенційно нижчий запас криптостійкості, частина алгоритмів ще недостатньо добре перевірені часом (тобто деякі алгоритми ще не мають багаторічного практичного тестування), проблеми сумісності зі стандартними протоколами безпеки і складність управління ключами в великих IoT-мережах.

Легковагова криптографія є елементом забезпечення конфіденційності і цілісності даних IoT-пристроїв. Вона дозволяє реалізовувати криптографічний захист навіть в таких ресурсно-обмежених пристроях як IoT-пристрої. Але через її адаптованість до обмежених пристроїв знижується і її криптографічна стійкість в порівнянні з стандартними криптографічними алгоритмами. Через це використання лише легковагової криптографії не можна вважати достатнім методом захисту. Це підтверджує доцільність використання комбінованих методів захисту інформації, зокрема, поєднання легковагової криптографії з методами захисту іншого типу.

Методи виявлення вторгнень і аналізу підозрілої й аномальної активності

Впровадження механізмів виявлення вторгнень та аналізу аномальної активності є важливим методом для забезпечення інформаційної безпеки в IoT-пристроях. На відміну від криптографічних методів, які гарантують конфіденційність та цілісність даних, системи виявлення вторгнень (Intrusion Detection Systems, IDS) більш орієнтовані на ідентифікацію вже відомих атак. Через те, що кількість IoT-пристроїв зростає ускладняється і реалізація традиційних механізмів виявлення загроз.

Загалом методи IDS для IoT можна класифікувати за принципом функціонування на сигнатурні, методи на основі виявлення аномалій, та методи, що засновані на машинному навчанні. Сигнатурні методи базуються на порівнянні аналізованого трафіку з базою відомих типів атак. Такі методи забезпечують високу точність для відомих загроз і основною їх характеристикою є низький рівень хибних спрацювань. Але їх ефективність знижується у випадку нових або модифікованих типів атак. Методи на основі виявлення аномалій ґрунтуються на формуванні моделі поведінки пристрою за нормальних умов і подальшому виявленню значущих відхилень (аномальної поведінки пристрою). Такі методи уже дозволяють виявляти невідомі раніше загрози, однак також супроводжуються підвищеним рівнем хибних спрацювань. Це може бути особливо критично в IoT-мережах. Методи на основі машинного і глибокого навчання застосовуються для аналізу великих обсягів мережевого трафіку та виявлення складних типів атак. Проте впровадження моделей машинного навчання в ресурсно-обмежених IoT-пристроях є складною задачею, оскільки пов'язане з проблемами обчислювальної складності і потребою в значних обсягах навчальних даних.

До ключових проблем реалізації IDS в IoT-пристроях і мережах відносяться ресурсна обмеженість пристроїв, енергетичні обмеження і гетерогенність протоколів та архітектур. Так само як і в випадку впровадження криптографії, для провадження IDS потрібно застосовувати алгоритми, які будуть враховувати обмеженість пам'яті і обчислювальної здатності процесора. Оскільки IDS працює безперервно, то виникає питання як оптимізувати алгоритм таким чином, щоб зменшити його

електроспоживання. Гетерогенність протоколів спричинена тим, що середовища IoT дуже різноманітні, і різні пристрої використовують різні протоколи для комунікації. До цих протоколів належать MQTT, CoAP, Zigbee, LoRaWAN та інші. Наявність великої кількості протоколів значно ускладнює уніфікацію механізмів виявлення загроз.

Після аналізу даних методів стає зрозуміло, що найкращим рішенням буде застосування гібридних методів. Тобто доцільно поєднувати сигнатурні підходи і методи на основі виявлення аномалій, а також імплементувати методи блокчейн і машинного навчання.

Таблиця 1

Порівняння методів виявлення вторгнень

Критерій	Сигнатурні	На основі виявлення аномалій	Машинне навчання
Точність для відомих атак	Висока	Середня	Висока
Рівень хибних спрацювань (False Positive Rate)	Низький	Високий	Середній
Обчислювальна складність	Низька	Середня	Висока
Придатність для локального IoT	Висока	Обмежена	Низька

Методи виявлення вторгнень є невід'ємним компонентом архітектури системи захисту інформації для IoT-пристроїв. Сигнатурні методи є ефективнішими у порівнянні з методами на основі виявлення аномалій. Методи на основі виявлення аномалій більш ефективні проти нових загроз, але також мають високий шанс помилкового спрацювання, а методи машинного навчання вимагають значно більших ресурсів ніж попередні два. У табл.1 наведено порівняння методів виявлення вторгнень.

Апаратні методи захисту інформації

Апаратні методи захисту інформації це сукупність безпекових рішень, які інтегровані безпосередньо в апаратну платформу пристрою. Вони дозволяють забезпечувати цілісність, конфіденційність, автентичність і надійність виконання інструкцій. Для IoT-пристроїв апаратний захист є ключовим елементом для підвищення рівня безпеки. Апаратні засоби захисту дозволяють реалізовувати функції, які або складно, або неефективно реалізовувати лише програмними методами захисту. Наприклад, захищене зберігання криптографічних ключів, ізоляцію виконання критичних обчислень чи перевірка цілісності прошивок на етапі завантаження.

До найпопулярніших апаратних механізмів захисту належать: Trusted Platform Module (TPM), Secure Boot, Trusted Execution Environment (TEE), Physically Unclonable Function (PUF).

Trusted Platform Module (TPM) – це спеціалізований апаратний модуль безпеки, задача якого полягає в зберіганні криптографічних ключів в ізольованому апаратному середовищі. В IoT TPM можна використати для захищеного завантаження, автентифікації пристрою і забезпечення цілісності критичних даних. Завдяки тому, що ключі ізольовані апаратно, вони не є доступними для програмної частини IoT-пристрою, і це значно ускладнює їх компрометацію.

Призначення механізму Secure Boot полягає в тому, щоб гарантувати, що пристрій завантажує лише авторизоване програмне забезпечення. Коли пристрій стартує, прошивка перевіряється криптографічним підписом, і якщо відбувається невідповідність, то завантаження відхиляється. Такий підхід зменшує ризик підміни коду стороннім програмним забезпеченням.

Trusted Execution Environment (TEE) забезпечує ізоляцію виконання критично важливих обчислень у відокремленому апаратному середовищі. Такий вид ізоляції дозволяє захистити критичні операції, такі як криптографічні операції або перевірка автентичності від доступу із основної програми чи операційної системи, які можуть бути скомпрометовані.

Physically Unclonable Function (PUF) – це апаратна сутність, що використовує кремнієвий кристал для генерації унікальних і непередбачуваних відбитків (fingerprints) для кожного пристрою. PUF є ефективним механізмом, що дозволяє забезпечити однозначну ідентифікацію пристрою і генерацію криптографічних ключів, які не зберігаються явно в пам'яті.

До основних переваг застосування даних методів належить високий рівень безпеки, захист від атак нижнього рівня, апаратне прискорення криптографії і стійкість до фізичних атак. Завдяки апаратним механізмам захисту можна забезпечити фізичну ізоляцію критичних даних і операцій. Такий підхід значно ускладнює їх компрометацію навіть за наявності у зловмисника доступу до програмної частини коду. Такі технології як Secure Boot і TEE здатні протистояти атакам типу rootkits або ж bootkits. За допомогою апаратного прискорення криптографії можна виконувати складні обчислення з меншим навантаженням на

процесор і нижчим енергоспоживанням. Модулі з апаратним захистом складніше зламати ніж ті методи, що ґрунтуються на програмному коді.

Проте, ці методи також мають свої недоліки. Найперше – це вартість реалізації, оскільки додавання нових апаратних модулів, таких як TPM, збільшує собівартість пристрою. Це може бути критичним у масових і дешевих IoT-системах. Також розробка апаратних механізмів вимагає спеціалізованих знань. Це може уповільнити цикл розробки пристрою. Крім цього, на відміну від програмних рішень, апаратні механізми складно оновлювати і модифікувати після виробництва.

Інтеграція апаратних засобів безпеки в IoT-пристроях зіштовхується із рядом проблем. Багато з масово використовуваних мікроконтролерів не мають достатньої обчислювальної потужності для підтримки таких апаратних модулів як TPM і TEE. Також введення додаткових апаратних модулів спричиняє збільшення енергетичного навантаження.

В табл. 2 наведено порівняння апаратних методів захисту інформації, описано основну функцію цих методів, їх переваги і недоліки.

Таблиця 2

Порівняння апаратних методів захисту інформації

Механізм	Основна функція	Переваги	Недоліки
TPM	Захищене зберігання і обробка ключів	Фізична ізоляція ключів	Додаткові апаратні витрати
Secure Boot	Перевірка цілісності прошивки	Запобігає несанкціонованому завантаженню	Вимагає управління сертифікатами
TEE	Ізоляція середовища виконання програм	Захищені обчислення	Обмежена підтримка на низькорівневому обладнанні
PUF	Унікальна ідентифікація пристрою	Не потребує зберігання ключів	Механізм чутливий до температури і шумів

Блокчейн методи захисту інформації

Проаналізувавши сучасні дослідження стає зрозуміло, що використання блокчейну в IoT розглядається як перспективний напрям для забезпечення інформаційної безпеки. У контексті IoT блокчейн застосовується для автентифікації пристроїв, контролю доступу і безпечного обміну інформацією між пристроями в мережі.

Традиційні IoT-системи використовують централізовані сервери для автентифікації. Такий підхід створює ризик компрометації усієї системи в разі кібератаки на неї. Технологія блокчейн дозволяє формувати розподілений реєстр ідентифікаторів пристроїв і їхніх публічних ключів. Кожен пристрій реєструється в мережі й інформація про його автентичність зберігається в незмінному реєстрі. За допомогою такого підходу можна зменшити ризик підробки ідентифікаційних даних. А також відсутність центрального вузла підвищує відмовостійкість усієї IoT-системи.

Одним із найпоширеніших сценаріїв використання технології блокчейн в IoT є фіксація хешів даних, згенерованих пристроями. Самі дані можуть зберігатись поза блокчейном, тоді як в розподіленому реєстрі зберігається їхній цифровий відбиток. Якщо відбувається будь-яка зміна даних, що призводить до невідповідності хешу, то такий підхід дозволяє оперативно виявити несанкціоноване втручання.

Ще одним способом застосування блокчейн для захисту IoT-пристроїв є смарт-контракти. Смарт-контракти дозволяються реалізувати автоматизовані політики доступу до ресурсів IoT. Правила для доступу визначені у програмному коді, що виконується в блокчейн-мережі. Це забезпечує їхню прозорість і незмінність. Основна перевага такого підходу – це автоматизація прийняття рішень і виключення людського фактору.

Оскільки архітектура блокчейн розподілена, то такий підхід зменшує ризик атак типу DoS і DDoS на центральний сервер керування. Проте сама блокчейн-мережа може бути вразливою до атак на механізм консенсусу або до перевантаження транзакціями. Тому, у випадку впровадження блокчейн в IoT доцільно застосовувати permissioned-блокчейни, які краще відповідають ресурсним обмеженням пристроїв.

Основними перевагами застосування блокчейн у IoT є відсутність єдиної точки відмови, підвищена прозорість, незмінність даних, автоматизація політик доступу за допомогою смарт-контрактів і підвищення довіри між учасниками мережі. Завдяки своїй децентралізованій архітектурі блокчейн замінює традиційний центральний сервер. Це дозволяє забезпечити стійкість мережі навіть у разі виходу з ладу окремих вузлів системи. Підвищена прозорість це перевага блокчейну, оскільки кожна транзакція, що

відбувається у блокчейн-мережі, фіксується у незмінному реєстрі. Ця особливість забезпечує повну прозорість дій пристроїв і дозволяє відслідковувати історію мережі. Ще однією перевагою є незмінність даних. Якщо дані були хоча б раз зафіксовані в блокчейні, то їх уже неможливо змінити чи видалити без консенсусу мережі. Завдяки цьому можна ефективно протидіяти модифікації даних. Протидія модифікації даних є критично-важливою для таких IoT-систем як медичні пристрої, або ж системи розумного дому. За допомогою смарт-контрактів можна автоматично визначати які користувачі мають доступ і до яких ресурсів. Таким способом можна знизити ризик помилок через людський фактор. Оскільки всі транзакції перевіряються, блокчейн створює довірче середовище, навіть коли учасники мережі не знайомі між собою. В контексті IoT це важливо для розподілених систем.

Але, як і в інших методів, в блокчейну є й свої недоліки. Традиційні блокчейн-системи потребують значних обчислювальних ресурсів для транзакцій. Для IoT-пристроїв це проблема, бо не всі вони здатні виконувати повноцінний блокчейн-вузол без сторонніх хмарних сервісів. Також проблемою є затримка підтвердження транзакцій, оскільки у публічних блокчейнах підтвердження транзакцій займає певний час. Для IoT це може бути неприйнятним, оскільки тут потрібна оперативна обробка даних і миттєве прийняття рішень (наприклад в медичних пристроях або в промислових контролерах). Інша проблема – це масштабованість. Оскільки зростає кількість пристроїв, то буде зростати і кількість транзакцій. Велика кількість транзакцій призводить до більшого навантаження на мережу і збільшення кількості даних в реєстрі. Це ускладнює підтримку великих IoT-мереж. Стосовно смарт-контрактів – то будь-які помилки в їх реалізації або у механізмі виконання можуть бути використані зловмисниками. Це вимагає додаткового тестування коду перед його розгортанням в мережі.

Таким чином, блокчейн не є універсальним рішенням для безпеки IoT. Але в грамотному поєднанні із іншими методами він може суттєво покращити загальну безпеку пристроїв і систем загалом.

Використання штучного інтелекту як методу захисту інформації

Як вже зазначалося вище, кількість IoT-пристроїв у світі зростає. Відповідно, гетерогенність протоколів зв'язку для цих пристроїв зростає також. В поєднанні із обмеженістю ресурсів IoT-пристроїв це створює складне середовище для забезпечення інформаційної безпеки. Традиційні методи забезпечення безпеки інформації часто виявляються недостатніми для ефективного захисту від нових і складних атак. У цьому контексті методи ШІ, зокрема машинного навчання і глибокого навчання стають важливими інструментами для адаптивного захисту інформації. Із уже проаналізованих наукових праць очевидно, що ШІ у сфері IoT-безпеки застосовується для виявлення вторгнень, аналізу аномальної поведінки пристроїв і прогнозування атак.

Виявлення вторгнень на основі машинного навчання є найбільш досліджуваним методом застосування ШІ для забезпечення інформаційної безпеки на даний момент. Алгоритми машинного навчання дозволяють будувати моделі нормальної поведінки мережі і виявляти відхилення від цієї моделі. Такі моделі здатні виявляти як відомі атаки, так і виявляти нові аномалії. Вони здатні адаптуватися до змін у трафіку.

Глибокі нейронні мережі здатні виявляти складні часові та просторові закономірності в трафіку IoT мережі. Особливу увагу варто звернути на LSTM-моделі для аналізу часових рядів мережевого трафіку. Ці моделі дозволяють прогнозувати DDoS-атаки й виявляти активність ботнетів.

Через обмеженість ресурсів в IoT-пристроях моделі ШІ часто розміщуються не безпосередньо на цих пристроях, а на edge-вузлах або шлюзах. Таке розміщення дозволяє зменшити затримки реагування, мінімізувати передавання конфіденційних даних у хмару і знизити навантаження на центральні сервери. Edge ШІ – це компроміс між продуктивністю та ресурсними обмеженнями IoT-пристроїв.

Застосування ШІ в захисті IoT має свої переваги. ШІ-моделі здатні навчатися на нових даних. Завдяки цьому вони здатні виявляти невідомі раніше типи атак. Через глибоке навчання можна виявляти складні патерни атак, які важко формалізувати за допомогою традиційних правил. За допомогою ШІ можна налаштувати автоматизоване реагування на загрози. Також моделі ШІ можна адаптувати для великих розподілених мереж IoT.

Як і розглянуті вище методи, ШІ як метод захисту інформації має і свої недоліки. Першим обмеженням є висока обчислювальна потужність і необхідність великого обсягу пам'яті. Моделі глибокого навчання потребують значних ресурсів для їх роботи. Також, для того, щоб модель ШІ ефективно працювала її потрібно навчити на якісних датасетах, до яких може не бути широкого доступу. Проблемою також є те, що модель ШІ можна атакувати, якщо підмінити вхідні дані для неї.

Отже, основними проблемами впровадження ШІ в IoT є необхідність значних обчислювальних ресурсів, високе енергоспоживання і ризик компрометації моделі. Але існують підходи, за допомогою яких можна вирішувати ці проблеми. Наприклад, можна застосовувати легковагові моделі, такі як TinyML, по аналогії із легковаговою криптографією. Можна розміщувати моделі на edge-шлюзах. Також хорошим

рішенням буде поєднувати ШІ разом із криптографічними і апаратними методами захисту. Методи ШІ є одним із найбільш перспективних напрямів розвитку безпеки IoT і потребують подальшого дослідження.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Провівши аналіз наукових джерел і дослідивши різні методи для забезпечення інформаційної безпеки з урахуванням особливостей IoT-пристроїв стає зрозуміло, що кожен із методів має як свої переваги так і свої недоліки. Тому, забезпечення інформаційної безпеки в IoT-системах потребує більш комплексного підходу, аніж використання лише одного із розглянутих в цій статті методів. У попередніх розділах статті були розглянуті такі підходи як легковагова криптографія, методи виявлення вторгнень та аналізу аномалій, апаратні методи захисту, блокчейн-рішення і методи на основі ШІ. В цьому розділі проведемо порівняння цих методів між собою із урахуванням специфіки IoT-пристроїв.

Для того, щоб провести коректне зіставлення методів використано наступні критерії: захист даних, можливість виявлення атаки, адаптивність, ресурсні витрати. Також розглянуто, де в IoT найбільш доцільно використати той чи інший метод.

Перший розглянутий метод в цій статті – легковагова криптографія. Він забезпечує конфіденційність і цілісність даних при нижчих витратах ресурсів аніж звичайна криптографія. Проте цей метод не здатен виявляти атаки на мережу і не здатний захистити вже скомпрометований пристрій. Він грає роль фундаментального, але пасивного механізму.

Другим розглянутим методом були методи виявлення вторгнень і аналізу підозрілої й аномальної активності . Цей метод орієнтований на моніторинг трафіку в мережі. Він здатний активно виявляти загрози, але також у нього є висока кількість хибних спрацювань. Він вимагає постійного оновлення правил.

Третім методом дослідженим в цій роботі були апаратні методи захисту інформації. Ці методи забезпечують захист ключів і прошивки. Вони надають високий рівень довіри до пристрою, але в той же час збільшують вартість кінцевого пристрою і ускладнюють його архітектуру.

Наступним розглянутим методом був блокчейн. Він здатний забезпечити децентралізовану довіру і контроль доступу через смарт-контракти. За допомогою цього методу можна усунути єдину точку відмови, але це ресурсоємний метод, і його складно масштабувати.

І останнім розглянутим методом було використання ШІ для забезпечення безпеки інформації. ШІ є окремим класом методів. Багато сучасних досліджень захисту інформації для IoT розглядали поєднання методів ШІ і методів виявлення вторгнень, проте, це не є єдиним перспективним напрямком для застосування ШІ.

На основі досліджень основних викликів, які можуть виникати в сфері інформаційної безпеки IoT, визначено п’ять основних критеріїв, що формують ефективність методів захисту інформації. За цими критеріями проведено порівняльний аналіз вищезгаданих методів, результати якого наведено у табл. 3:

Таблиця 3

Порівняння методів захисту IoT-систем

Метод	Ефективність захисту даних	Виявлення атак	Адаптивність	Ресурсні витрати	Оптимальний рівень використання в IoT
Легковагова криптографія	Високий	Низький	Низька	Низькі	Пристрій
Апаратний захист	Високий	Низький	Низька	Середні	Пристрій
Методи виявлення вторгнень (IDS)	Середній	Високий		Середні-високі	Шлюз
Блокчейн	Високий	Низький	Низька	Високі	Edge/Cloud
Штучний інтелект	Середній	Дуже високий	Висока	Високі	Edge/Cloud

Порівняльний аналіз свідчить, що не існує універсального методу, який би повністю задовольняв усі вимоги безпеки IoT. За допомогою легковагої криптографії і апаратного захисту можна сформувати

базовий рівень захисту. За допомогою IDS і ШІ можна забезпечити активний моніторинг мережі. За допомогою блокчейну можна підвищити довіру та прозорість у розподілених системах. З врахуванням специфіки IoT, найбільш ефективною буде система багаторівневого захисту, тобто поєднання декількох існуючих методів між собою.

У ході дослідження методи захисту інформації були оцінені за такими критеріями, як ефективність захисту даних, ефективність виявлення атак, адаптивність, ресурсні витрати і оптимальний рівень використання в IoT. У результаті аналізу виявлено, що жоден із методів не забезпечує комплексного захисту IoT-системи самостійно. Найвищий рівень захисту можна досягти тільки у комплексній інтеграції методів у багаторівневу архітектуру IoT. Виявлено, що для ресурсно-обмежених IoT-пристроїв найкраще використовувати методи легковагової криптографії разом із апаратним захистом ключів, тому що вони вимагають найменших ресурсів і споживають менше енергії. Для мережевого рівня IoT найкраще використовувати IDS із елементами машинного навчання. Для критичних IoT-систем найкраще буде комбінування методів із апаратними засобами, блокчейном і адаптивними системами ШІ.

Результати дослідження показують, що перспективним напрямом для подальших робіт є розробка інтегрованих методів для забезпечення безпеки IoT. Також доцільно розробити алгоритм вибору методу забезпечення безпеки інформації залежно від специфіки конкретної IoT системи. Оскільки кожен із методів має свої недоліки, то також вартує досліджувати і покращувати кожен із методів окремо.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

В статті проведено огляд і аналіз методів захисту інформації для IoT-пристроїв. У розділі теоретичних основ систематизовано концептуальні засади кожного методу із урахуванням специфіки ресурсно-обмежених IoT-пристроїв. Проаналізовано переваги і недоліки застосування кожного із методів та здійснено їх порівняння за певними критеріями. Наукова новизна роботи полягає в тому, що вперше систематизовано зазначені методи у єдиній порівняльній матриці з урахуванням оптимального рівня їх застосування в архітектурі IoT, що дозволяє обирати стратегію захисту залежно від специфіки конкретної системи. В результаті аналізу доведено, що жоден із методів не являється універсальним. Найкращим і найефективнішим захистом буде поєднання декількох методів між собою. Запропоновано проводити подальші дослідження, які стосувались би інтеграції різних підходів залежно від специфіки конкретної IoT. Показано, що різні методи найкраще підходять для різних IoT-пристроїв. Зокрема, методи легковагової криптографії і апаратного захисту найкраще застосовувати до вбудованих пристроїв. Методи IDS найкраще використовувати для захисту шлюзів. Для великих IoT-систем найкраще буде використовувати поєднання блокчейн, штучного інтелекту і апаратних методів захисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Amrita, Ekwueme, C. P., Adam, I. H., & Dwivedi, A. (2024). Lightweight cryptography for Internet of Things: A review. *EAI Endorsed Transactions on Internet of Things, 10*. https://publications.eai.eu/index.php/IoT/article/view/5565
2. Suryateja, P. S., & Rao, K. V. (2024). A survey on lightweight cryptographic algorithms in IoT. *Cybernetics and Information Technologies, 24*(1), 21–34. https://doi.org/10.2478/cait-2024-0002
3. Alqahtani, H., & Sarker, I. H. (2025). A systematic review of lightweight cryptographic schemes for security and privacy in IoT. *Discover Computing*. https://doi.org/10.1007/s10791-025-09755-3
4. Santos-González, I., Rivero-García, A., González-Martín, C., & Caballero-Gil, P. (2025). A survey of efficient lightweight cryptography for power-constrained microcontrollers. *Technologies, 13*(1), 3. https://doi.org/10.3390/technologies13010003
5. Bhavsar, M., Roy, K., Kelly, J., & Odeyomi, O. (2023). Anomaly-based intrusion detection system for IoT application. *Discover Internet of Things, 3*, Article 5. https://doi.org/10.1007/s43926-023-00034-5
6. Sharma, B., Sharma, L., Lal, C., & Roy, S. (2023). Anomaly based network intrusion detection for IoT attacks using deep learning technique. *Computers and Electrical Engineering, 107*, Article 108626. https://doi.org/10.1016/j.compeleceng.2023.108626
7. Sabeena, S., & Chitra, S. (2024). Comparative study on anomaly based intrusion detection using deep learning techniques. *EAI Endorsed Transactions on Internet of Things, 11*(1). https://doi.org/10.4108/eetiot.7178

8. Seth, A. (2025). Attack and anomaly detection in IoT sensors using machine learning approaches. *Journal of Recent Innovations in Computer Science and Technology, 2*(1), 16–27. https://doi.org/10.70454/JRICST.2025.20108
9. Mohan, S., Jayakumar, V., & Selvaraj, R. (2025). TinyML-based intrusion detection systems for sustainable and energy-constrained IoT devices. *Results in Engineering, 24*, 103171. https://doi.org/10.1016/j.rineng.2025.108013
10. Velázquez-Rodríguez, A., Iglesias-Martínez, M. E., & Fernández-de-Vega, F. (2025). Lightweight signal processing and edge AI for real-time anomaly detection in IoT sensor networks. *Sensors, 25*(21), 6629. https://doi.org/10.3390/s25216629
11. Xia, Y., Zhou, Y., Liu, J. N., Liu, X., Chen, J., Xiao, F., & Zhu, H. (2025). Hardware-enhanced data security for Internet of Things. *Fundamental Research*. https://doi.org/10.1016/j.fmre.2025.09.025
12. Zhurylo, O., Liashenko, O., & Avetisova, K. (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
13. García-Teodoro, P., Camacho, J., Maciá-Fernández, G., & Díaz-Verdejo, J. E. (2024). Strengthening Internet of Things security: Surveying physical unclonable functions for authentication, communication protocols, challenges, and applications. *Applied Sciences, 14*(5), 1700. https://doi.org/10.3390/app14051700
14. Almarri, S., & Aljughaiman, A. (2024). Blockchain technology for IoT security and trust: A comprehensive SLR. *Sustainability, 16*(23), 10177. https://doi.org/10.3390/su162310177
15. Gugueoth, V., Safavat, S., Shetty, S., & Rawat, D. (2023). A review of IoT security and privacy using decentralized blockchain techniques. *Computer Science Review, 50*, 100585. https://doi.org/10.1016/j.cosrev.2023.100585
16. Obaidat, M. A., Rawashdeh, M., Alja'afreh, M., Abouali, M., Thakur, K., & Karime, A. (2024). Exploring IoT and blockchain: A comprehensive survey on security, integration strategies, applications and future research directions. *Big Data and Cognitive Computing, 8*(12), 174. https://doi.org/10.3390/bdcc8120174
17. Kaushik, D., Gulia, P., Gill, N. S., Mohammad, Y., Shukla, P. K., & Shreyas, J. (2026). Synergizing blockchain and AI to fortify IoT security: A comprehensive review. *Artificial Intelligence Review, 59*(2), Article 41. https://doi.org/10.1007/s10462-025-11434-0
18. Juber, A. H., & Farhan, B. I. (2026). Innovative strategies for IoT security using AI and blockchain: A comprehensive review. *Iraqi Journal for Computers and Informatics, 52*(1), 99–112. https://doi.org/10.25195/ijci.v52i1.656
19. Hassan, J., Abid, M. K., Ahmad, M., Ghulam, A., Fakhar, M. S., & Asif, M. (2023). A survey on blockchain based intrusion detection systems for IoT. *VAWKUM Transactions on Computer Sciences, 11*(1). https://doi.org/10.21015/vtcs.v11i1.1385
20. AlE'mari, S., Anbar, M., Sanjalawe, Y., Manickam, S., & Hasbullah, I. (2022). Intrusion detection systems using blockchain technology: A review, issues and challenges. *Computer Systems Science and Engineering, 40*(1), 87–112. https://doi.org/10.32604/csse.2022.017941
21. Khraisat, A., Alazab, A., & Alazab, M. (2025). Federated learning for intrusion detection in IoT environments: A privacy-preserving strategy. *Discover Internet of Things, 5*, 72. https://doi.org/10.1007/s43926-025-00169-7
22. Pagano, A., Ferraro, G., & Petralia, G. (2025). Federated learning-driven cybersecurity framework for IoT networks with privacy preserving and real-time threat detection capabilities. *Informatics, 12*(3), 62. https://doi.org/10.3390/informatics12030062
23. Al-Sarem, M., Al-Hagery, M., & Saeed, F. (2025). A survey on cybersecurity in IoT. *Future Internet, 17*(1), 30. https://doi.org/10.3390/fi17010030
24. Rivadeneira, J. E., Díaz-Verdejo, J. E., García-Teodoro, P., & González-Manzano, L. (2025). A literature review on security in the Internet of Things: Identifying and analysing critical categories. *Computers, 14*(2), 61. https://doi.org/10.3390/computers14020061
25. Tuptuk, N., Hazell, P., Watson, J., & Hailes, S. (2023). A survey on cyber risk management for the Internet of Things. *Applied Sciences, 13*(15), 9032. https://doi.org/10.3390/app13159032

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023

Nazarii A. Vitiv
Postgraduate student, Department of Specialized Computer Systems
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0009-0005-8225-9765
nazarii.vitiv.asp.2025@lpnu.ua

Oksana Y. Honsor
PhD, Associate Professor, Department of Specialized Computer Systems
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0000-0003-0895-5859
oksana.y.honsor@lpnu.ua

SYSTEMATIC ANALYSIS OF INFORMATION SECURITY PROVISION METHODS IN IOT DEVICES

Abstract. This study examines well-known methods of ensuring information security that are relevant for IoT devices and take into account their specifics. The relevance of the problem of information protection in IoT is substantiated, a wide range of existing approaches is described and the need for their comprehensive application, taking into account the resource limitations of devices, is analyzed. The scientific works of researchers covering lightweight cryptography, intrusion detection systems, hardware protection methods, blockchain and artificial intelligence methods are analyzed. The four-level architecture of IoT systems (device level, network, platform and application level) is considered from the point of view of threats and protection mechanisms, and the conceptual principles of each method are considered in detail: lightweight cryptography (PRESTENT, SPECK, SIMON, ASCON algorithms), intrusion detection systems (IDS) based on signatures, anomalies and machine learning, hardware protection means (TPM, Secure Boot, TEE, PUF), blockchain technology and methods using artificial intelligence. For each method, the advantages and limitations are systematized, taking into account the specifics of resource-limited IoT devices. In the final section, a comparative analysis of the specified methods is carried out according to five criteria: data protection efficiency, attack detection, adaptability, resource costs and optimal level of use in the IoT architecture. The scientific novelty of the work lies in the systematization of the specified methods in a single comparative matrix, taking into account the optimal level of their application in the IoT architecture. Based on the conducted research, the feasibility of using a comprehensive approach to ensuring information security, which involves the integration of various protection mechanisms at all levels of the IoT architecture, is substantiated.

Keywords: authentication; hardware protection methods; blockchain; Internet of Things; information security; cryptography; artificial intelligence.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Amrita, Ekwueme, C. P., Adam, I. H., & Dwivedi, A. (2024). Lightweight cryptography for Internet of Things: A review. *EAI Endorsed Transactions on Internet of Things, 10*. https://publications.eai.eu/index.php/IoT/article/view/5565
2. Suryateja, P. S., & Rao, K. V. (2024). A survey on lightweight cryptographic algorithms in IoT. *Cybernetics and Information Technologies, 24*(1), 21–34. https://doi.org/10.2478/cait-2024-0002
3. Alqahtani, H., & Sarker, I. H. (2025). A systematic review of lightweight cryptographic schemes for security and privacy in IoT. *Discover Computing*. https://doi.org/10.1007/s10791-025-09755-3
4. Santos-González, I., Rivero-García, A., González-Martín, C., & Caballero-Gil, P. (2025). A survey of efficient lightweight cryptography for power-constrained microcontrollers. *Technologies, 13*(1), 3. https://doi.org/10.3390/technologies13010003
5. Bhavsar, M., Roy, K., Kelly, J., & Odeyomi, O. (2023). Anomaly-based intrusion detection system for IoT application. *Discover Internet of Things, 3*, Article 5. https://doi.org/10.1007/s43926-023-00034-5
6. Sharma, B., Sharma, L., Lal, C., & Roy, S. (2023). Anomaly based network intrusion detection for IoT attacks using deep learning technique. *Computers and Electrical Engineering, 107*, Article 108626. https://doi.org/10.1016/j.compeleceng.2023.108626
7. Sabeena, S., & Chitra, S. (2024). Comparative study on anomaly based intrusion detection using deep learning techniques. *EAI Endorsed Transactions on Internet of Things, 11*(1). https://doi.org/10.4108/eetiot.7178

8. Seth, A. (2025). Attack and anomaly detection in IoT sensors using machine learning approaches. *Journal of Recent Innovations in Computer Science and Technology, 2*(1), 16–27. https://doi.org/10.70454/JRICST.2025.20108
9. Mohan, S., Jayakumar, V., & Selvaraj, R. (2025). TinyML-based intrusion detection systems for sustainable and energy-constrained IoT devices. *Results in Engineering, 24*, 103171. https://doi.org/10.1016/j.rineng.2025.108013
10. Velázquez-Rodríguez, A., Iglesias-Martínez, M. E., & Fernández-de-Vega, F. (2025). Lightweight signal processing and edge AI for real-time anomaly detection in IoT sensor networks. *Sensors, 25*(21), 6629. https://doi.org/10.3390/s25216629
11. Xia, Y., Zhou, Y., Liu, J. N., Liu, X., Chen, J., Xiao, F., & Zhu, H. (2025). Hardware-enhanced data security for Internet of Things. *Fundamental Research*. https://doi.org/10.1016/j.fmre.2025.09.025
12. Zhurylo, O., Liashenko, O., & Avetisova, K. (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
13. García-Teodoro, P., Camacho, J., Maciá-Fernández, G., & Díaz-Verdejo, J. E. (2024). Strengthening Internet of Things security: Surveying physical unclonable functions for authentication, communication protocols, challenges, and applications. *Applied Sciences, 14*(5), 1700. https://doi.org/10.3390/app14051700
14. Almarri, S., & Aljughaiman, A. (2024). Blockchain technology for IoT security and trust: A comprehensive SLR. *Sustainability, 16*(23), 10177. https://doi.org/10.3390/su162310177
15. Gugueoth, V., Safavat, S., Shetty, S., & Rawat, D. (2023). A review of IoT security and privacy using decentralized blockchain techniques. *Computer Science Review, 50*, 100585. https://doi.org/10.1016/j.cosrev.2023.100585
16. Obaidat, M. A., Rawashdeh, M., Alja'afreh, M., Abouali, M., Thakur, K., & Karime, A. (2024). Exploring IoT and blockchain: A comprehensive survey on security, integration strategies, applications and future research directions. *Big Data and Cognitive Computing, 8*(12), 174. https://doi.org/10.3390/bdcc8120174
17. Kaushik, D., Gulia, P., Gill, N. S., Mohammad, Y., Shukla, P. K., & Shreyas, J. (2026). Synergizing blockchain and AI to fortify IoT security: A comprehensive review. *Artificial Intelligence Review, 59*(2), Article 41. https://doi.org/10.1007/s10462-025-11434-0
18. Juber, A. H., & Farhan, B. I. (2026). Innovative strategies for IoT security using AI and blockchain: A comprehensive review. *Iraqi Journal for Computers and Informatics, 52*(1), 99–112. https://doi.org/10.25195/ijci.v52i1.656
19. Hassan, J., Abid, M. K., Ahmad, M., Ghulam, A., Fakhar, M. S., & Asif, M. (2023). A survey on blockchain based intrusion detection systems for IoT. *VAWKUM Transactions on Computer Sciences, 11*(1). https://doi.org/10.21015/vtcs.v11i1.1385
20. AlE'mari, S., Anbar, M., Sanjalawe, Y., Manickam, S., & Hasbullah, I. (2022). Intrusion detection systems using blockchain technology: A review, issues and challenges. *Computer Systems Science and Engineering, 40*(1), 87–112. https://doi.org/10.32604/csse.2022.017941
21. Khraisat, A., Alazab, A., & Alazab, M. (2025). Federated learning for intrusion detection in IoT environments: A privacy-preserving strategy. *Discover Internet of Things, 5*, 72. https://doi.org/10.1007/s43926-025-00169-7
22. Pagano, A., Ferraro, G., & Petralia, G. (2025). Federated learning-driven cybersecurity framework for IoT networks with privacy preserving and real-time threat detection capabilities. *Informatics, 12*(3), 62. https://doi.org/10.3390/informatics12030062
23. Al-Sarem, M., Al-Hagery, M., & Saeed, F. (2025). A survey on cybersecurity in IoT. *Future Internet, 17*(1), 30. https://doi.org/10.3390/fi17010030
24. Rivadeneira, J. E., Díaz-Verdejo, J. E., García-Teodoro, P., & González-Manzano, L. (2025). A literature review on security in the Internet of Things: Identifying and analysing critical categories. *Computers, 14*(2), 61. https://doi.org/10.3390/computers14020061
25. Tuptuk, N., Hazell, P., Watson, J., & Hailes, S. (2023). A survey on cyber risk management for the Internet of Things. *Applied Sciences, 13*(15), 9032. https://doi.org/10.3390/app13159032

Отримано редакцією журналу / Received: 03.02.26
Прорецензовано / Revised: 16.02.26
Схвалено до друку / Accepted: 24.09.26