УДК 004.2 https://doi.org/10.32515/2664-262X.2025.11(42).1.46-55

Ю. І. Підлісний
Національний університет «Чернігівська політехніка», Чернігів, Україна
e-mail: ypodlesny@ukr.net

Шляхи підвищення конфіденційності в мережах інтернету речей

У статті представлено результати огляду існуючих найновітніші і найактуальніші системи захисту для мереж IoT, їх переваги та недоліки. Основну увагу приділено методам захисту даних на рівні пристроїв, мережевої інфраструктури та хмарних сервісів. Серед можливих шляхів підвищення конфіденційності розглядаються застосування шифрування, механізмів аутентифікації, впровадження блокчейн-технологій, штучного інтелекту та машинного навчання. Висновки підкреслюють важливість інтеграції багаторівневих стратегій захисту, адаптованих до специфіки мереж IoT, для забезпечення високого рівня конфіденційності та довіри до систем Інтернету речей. Мета статті - комплексне висвітлення і аналіз сучасних викликів, загроз та проблем конфіденційності та безпеки в мережах Інтернету речей (IoT), а також вивчення передових методів захисту чутливої інформації. Стаття також спрямована на формування уявлення про актуальність питань приватності для користувачів IoT, окреслення можливих підходів до вирішення існуючих проблем і підвищення обізнаності щодо впливу технологій на безпеку даних у глобальній IoT-інфраструктурі.
IoT, мережа IoT, штучний інтелект, машинне навчання, безпека інформації

Постановка проблеми. З розвитком Інтернету речей виникає проблема забезпечення конфіденційності даних, що передаються між пристроями та зберігаються в системах. Багато IoT-пристроїв мають обмежені обчислювальні ресурси, що ускладнює впровадження стандартних методів захисту. Крім того, централізовані моделі управління даними часто стають мішенню для атак, що призводить до витоку конфіденційної інформації. Законодавчі ініціативи, такі як GDPR[1], CCPA[2] та інші міжнародні нормативні акти, вимагають впровадження ефективних заходів захисту персональних даних у IoT-системах. Це підкреслює необхідність у розробці нових підходів та технологій, які б дозволили ефективно захищати дані в умовах обмежених ресурсів та розподіленої архітектури IoT-систем, включаючи інноваційні криптографічні механізми, децентралізовані технології та політику мінімізації збору даних.

Аналіз останніх досліджень і публікацій. Забезпечення конфіденційності в мережах Інтернету речей (IoT) є важливою темою сучасних досліджень. Так у систематичному огляду [3] досліджено підходи до створення персональних сховищ даних, які дозволяють користувачам контролювати свої дані в IoT-середовищах. Такі сховища забезпечують централізоване управління даними та підвищують конфіденційність, надаючи користувачам можливість визначати, які дані збираються та як вони використовуються. У статті [4] проведено систематичний огляд досліджень, присвячених шаблонам та архітектурам безпеки для IoT. Автори підкреслюють важливість розробки стандартизованих підходів до безпеки та конфіденційності, які можуть бути впроваджені на різних рівнях IoT-систем для забезпечення захисту даних. Технології, які підвищують конфіденційність в IoT, запропоновано у [5], а саме: анонімізацію даних, шифрування та децентралізовані моделі зберігання.

У статті [6] проведено детальний аналіз поточних викликів у сфері безпеки та конфіденційності Інтернету речей (IoT). Автори розглядають загрози на різних рівнях архітектури IoT та пропонують можливі рішення для їх усунення, підкреслюючи

важливість комплексного підходу до забезпечення конфіденційності. У [7] автори пропонують використовувати блокчейн-технологій для підвищення конфіденційності в IoT: «блокчейн може забезпечити децентралізоване управління даними та зменшити ризики несанкціонованого доступу, надаючи прозорість та контроль над транзакціями».

Підсумовуючи, можна зазначити, що ці дослідження підкреслюють важливість розробки та впровадження нових технологій і підходів для забезпечення конфіденційності в мережах Інтернету речей. Використання персональних сховищ даних, стандартизованих архітектур безпеки, технологій підвищення конфіденційності та блокчейн може сприяти захисту особистої інформації користувачів у сучасних IoT-системах. Дослідники відзначають, що IoT-пристрої стають ключовим елементом побудови «цифрового портрету» людини [9], а це підвищує ризики витоку даних і зловживань з боку зловмисників або комерційних структур. У дослідженнях звертається увага на те, що в сучасних умовах недостатньо тільки захистити сам пристрій - необхідно контролювати весь ланцюг обробки даних, включаючи зберігання і передачу інформації.

Незважаючи на активацію досліджень безпеки і конфіденційності IoT в останні роки , існує ряд недосліджених проблем**.** Більшість досліджень зосереджується на загальних питаннях захисту даних, але не всі аспекти конфіденційності обробки даних у різних типах IoT-систем детально вивчені. Потребують значної адаптації криптографічні алгоритми для пристроїв з обмеженими ресурсами, є нагальна потреба в розробці новітніх методів шифрування без значного впливу на продуктивність пристроїв. Виникає питання, що до розробки безпечної комунікації в мережах IoT, не вирішена проблема масштабованості при використовуванні децентралізованих технологій для захисту даних (наприклад блокчейн). Брак єдиних стандартів і нормативних актів створює розриви в системі захисту даних.

Постановка завдання. Провести аналіз основних загроз конфіденційності в IoT-мережах, оцінити існуючи методі захисту, а також визначення перспективних напрямів для підвищення рівня безпеки.

Для досягнення поставленої мети необхідно вирішити такі завдання: дослідити основні загрози конфіденційності в IoT-мережах; проаналізувати існуючі методи забезпечення конфіденційності в IoT; проаналізувати застосування технологій шифрування та анонімності для захисту даних; оцінити підходи до конфіденційності з урахуванням обмежених ресурсів IoT-пристроїв; визначити перспективні напрями розвитку технологій захисту конфіденційності в IoT.

Виклад основного матеріалу. Вперше поняття "інтернет речей" (IoT, Internet-of-Things) було застосовано у 1999 році, коли компанія Procter&Gamble створила мережу пристроїв, що були здатні обмінюватися інформацією без втручання людини. Близько 10 років термін не набував широкого розповсюдження і лише наприкінці нульових років до нього прийшла популярність завдяки розвитку нових сенсорів та засобів зв'язку. З середини 2010-х років (трохи більше ніж п'ять років від старту масового застосування) почалося вибухове експоненціальне зростання кількості IoT, яке не припиняється й нині (мова вже йде про 15 мільярдів пристроїв). З тих пір IoT-пристрої впроваджуються практично в усі аспекти життя людини: промисловість, охорону здоров'я, транспорт та звичайні "домашні господарства" (розумні кондиціонери, телевізори, електромобілі тощо).

Розумні пристрої дали людині безліч переваг, такі як зручність, швидкість ухвалення рішень, доступ до різних даних і параметрів і головне можливість швидко отримувати й опрацьовувати різну інформацію (про здоров'я, про дорожню ситуацію, про забруднення повітря тощо).

Є і зворотний бік таких інновацій, а саме пристрої IoT отримують і аналізують інформацію про практично про всі аспекти людського життя. Вони відстежують

геолокацію людини в реальному часі, мають доступ до показників її здоров'я, знають про вподобання в музиці, їжі та навіть про захоплення і хобі. Ця інформація дозволяє створювати "цифровий портрет" людини, що відображає її поведінку, звички, здоров'я та особисті переваги, і є критичною для забезпечення конфіденційності та безпеки в IoT-середовищі.

Однак багато IoT-пристроїв виготовляються з відносно слабкими обчислювальними ресурсами та мають обмежену операційну систему. Багато виробників не приділяли достатньої уваги кібербезпеці своїх продуктів (це питання ніколи не було на "чільному місці" - рахувалося, що такі пристрої працюють у середовищі, де це "нібито не так важливо"). А це призвело до того, що IoT-пристрої часто мають вразливості у програмному забезпеченні, які можуть бути використані для атак [10, стр. 76, 146-164]. IoT-пристрої збирають досить великі обсяги особистої і конфіденційної інформації. Недостатня захищеність цих даних може призвести до порушення приватності користувачів та потенційних фінансових або особистих втрат. Більш того, у випадку компрометації безпеки систем IoT, можуть виникнути серйозні загрози для фізичної безпеки. Наприклад, сучасні автомобілі стали частиною всесвіту Інтернет речей (концепція Connected Car) і отримання можливості злочинцю керувати дистанційно його системами може привести, в залежності від цілей зловмисника, до непередбачуваних наслідків для життя та здоров'я водія і оточуючих його людей.

Природно, що масштабність та розповсюдженість Інтернет речей створює великий потенціал для кіберзлочинців - впливати на широкий спектр систем. Як правило, IoT-пристрої інтегруються в загальну мережу (чи то домашня Wi-Fi мережа, чи то велика корпоративна), і якщо один із пристроїв у результаті злому буде скомпрометовано, можна отримати доступ до всієї мережі з усіма пристроями. Тому злочинні елементи можуть використовувати IoT-пристрої для створення ботнетів, здійснення DDoS-атак, зламу даних або навіть фізичного шкоди.

Збереження конфіденційної інформації про людину важливе і для самої індустрії IoT. Насамперед визначення конфіденційності звучить як право людей контролювати збір, використання та розкриття їхньої особистої інформації. Використовуючи це визначення, ми можемо сформулювати основні аспекти щодо важливості конфіденційності у мережах IoT:

- *захист особистої інформації:* кожна людина має право на приватність і її особиста інформація така як дані про здоров'я, фінансові транзакції, місцезнаходження або інші особисті дані не повинна бути доступна без її згоди. Порушення конфіденційності може призвести до крадіжки особистих даних або шахрайства.
- *захист від зловживання:* дані, які збирають IoT-пристрої, можуть використовуватися для зловживань, таких як відстеження або маніпуляція, якщо вони потраплять до зловмисників.
- *захист від дискримінації:* якщо особисті дані людини (наприклад, про здоров'я або політичні переконання) будуть відомі широкому загалу або недобросовісним організаціям, це може призвести до дискримінації або утисків.
- *цифрова репутація:* особисті дані формують цифровий слід, який впливає на репутацію людини в інтернеті. Незахищеність даних може зруйнувати довіру до людини або компанії.
- *психологічна безпека:* люди мають відчувати себе в безпеці та комфортно, знаючи, що їхня приватність зберігається. Постійне відчуття спостереження може створювати стрес та незадоволення.
- *право на самовизначення:* конфіденційність дає людині можливість контролювати, як і коли її інформація буде використовуватись, що забезпечує більше контролю над власним життям.

Якщо довіру до пристроїв IoT, через витік конфіденційної інформації буде підірвано, індустрія не зможе розвиватися і впроваджувати справді інноваційні та проривні технології. Тобто у нас фактично є *дилема і головна проблема*: з одного боку - через розмаїття пристроїв IoT (за призначенням, за принципами роботи тощо) не завжди є можливість забезпечити стандартні підходи до забезпечення безпеки, а з іншого боку - виробники не можуть отримати достатньо прибутку через недовіру та запитання щодо безпеки розумних пристроїв, щоб впровадити більш інноваційні підходи.

Дослідження конфіденційності в Інтернет речах полягає у тому, що стрімке зростання кількості IoT-пристроїв супроводжується значними загрозами для безпеки та приватності користувачів [11]. В той час, як ці пристрої забезпечують нові можливості для автоматизації, комфорту і ефективності, вони також збирають величезні обсяги чутливої інформації, включаючи дані про місцезнаходження, поведінку, медичні показники, відео та аудіо. У зв’язку з цим виникають наступні загрози:

- *вразливість IoT-пристроїв до кібератак*: через обмеженість апаратних і програмних ресурсів більшість IoT-пристроїв не мають достатнього рівня захисту. Це робить їх вразливими до атак типу "людина посередині", перехоплення даних, шкідливих програм, зломів і, як наслідок, зловмисники можуть отримати доступ до приватної інформації користувачів.
- *несанкціонований збір і використання даних*: багато IoT-пристроїв без відома користувачів збирають дані, які можуть бути використані для побудови цифрового профілю особи (дані про звички, уподобання, маршрути переміщень, стан здоров'я тощо). Без належних механізмів захисту ці дані можуть бути передані третім особам або використані для комерційних чи злочинних цілей.
- *відсутність єдиних стандартів і регулювання*: існує брак уніфікованих стандартів захисту даних та конфіденційності в IoT-системах. Різні виробники можуть використовувати різні протоколи та технології, що ускладнює забезпечення єдиної системи захисту. Крім того, правове регулювання в різних країнах відстає від темпів розвитку технологій, що робить захист даних у глобальному масштабі неповноцінним.
- *надійне управління даними*: проблемою є й те, хто несе відповідальність за безпеку даних. IoT-пристрої часто використовують хмарні сервіси для зберігання та обробки даних. У випадку витоку даних або атаки виникають питання щодо відповідальності за ці інциденти.
- *низька обізнаність користувачів*: багато користувачів IoT-пристроїв не усвідомлюють рівень загроз, пов'язаних із конфіденційністю та захистом даних. Вони часто не знають, як правильно налаштувати пристрої або застосувати необхідні заходи безпеки.

Як вже було зазначено вище, пристрої IoT охоплюють все більше сфер людського життя, аналізують і збирають великий обсяг інформації, тому і розробляються новітні методи захисту чутливих даних і системи захисту анонімності людини (аномайзери). Для пристроїв IoT сьогодення характерно об’єднання останніх у мережі IoT (рис.1).

Проаналізуємо існуючі найновітніші і найактуальніші системи захисту для мереж IoT, їх переваги та недоліки.

1. Штучний інтелект та машинне навчання для виявлення аномалій є однією з найбільш ефективних та інноваційних технологій захисту мереж Інтернету речей. Ці методи використовуються для автоматизованого аналізу великих обсягів даних, які генеруються IoT-пристроями, та ідентифікації підозрілої або нехарактерної поведінки. Машинне навчання (МН) створює моделі, які навчаються на попередньо

отриманих даних (історичних даних), які розпізнають закономірності та виявляють аномалії. Штучний інтелект (ШІ) здатний самостійно аналізувати дані в реальному часі, порівнюючи їх з еталонними моделями для виявлення нетипової поведінки в мережі. Аномалії — це відхилення від стандартної поведінки IoT-пристроїв, які можуть свідчити про кібератаку або технічну несправність [13].

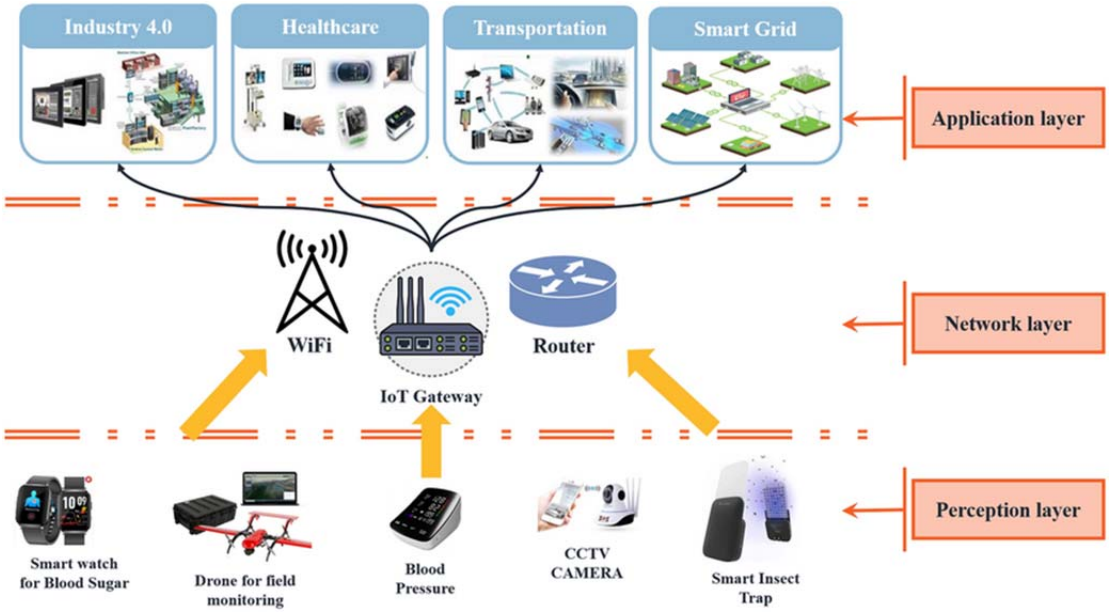

Рисунок 1 - Сучасна мережа пристроїв IoT

Джерело: розроблено на основі [12]

Переваги застосування ШІ та МН для виявлення аномалій: швидкість виявлення (автоматизовані алгоритми здатні виявляти аномалії в реальному часі, що мінімізує час реакції на потенційні загрози); виявлення нових типів атак (на відміну від традиційних методів на основі сигнатур, ШІ та МН здатні виявляти невідомі або нові види атак, які ще не були занесені в бази даних кіберзагроз); адаптивність (моделі МН можуть адаптуватися до нових умов, що дозволяє системам безпеки еволюціонувати разом із розвитком загроз); масштабованість (ці системи можуть обробляти величезні обсяги даних від багатьох пристроїв одночасно, що робить їх ідеальними для масштабних IoT-мереж) . Недоліки застосування ШІ та МН: помилкові спрацьовування (неправильно налаштовані моделі можуть призводити до великої кількості хибних спрацювань, що може перевантажити систему безпеки); обчислювальні ресурси (алгоритми ШІ та МН потребують значних обчислювальних потужностей, що може бути проблемою для малопотужних IoT-пристроїв); потреба у високоякісних даних (для налаштування моделей потрібні великі обсяги даних - якщо дані є неповними або нерелевантними, ефективність моделей може бути низькою).

- **Блокчейн для захисту даних та транзакцій** використовує децентралізовану базу даних для зберігання інформації, забезпечуючи при цьому високий рівень безпеки, прозорості та надійності. Блокчейн може бути використаний для безпечного зберігання та обміну даними між IoT-пристроями, забезпечуючи їх автентичність і цілісність [14]. Переваги застосування: висока безпека (завдяки децентралізованій природі та криптографічним методам); прозорість і відстежуваність (дозволяє учасникам мережі перевіряти дані в будь-який час); скорочення витрат (зменшує витрати на обробку і зберігання даних); недоліки – складність інтеграції (впровадження блокчейн-технологій може бути складним і вимагати великих зусиль), проблеми масштабованості (деякі

блокчейн-системи можуть стикатися з обмеженнями в обробці великої кількості транзакцій), правові та регуляторні питання (блокчейн ще не регулюється чітко в багатьох країнах, що може створювати правові проблеми).

- **Диференціальна конфіденційність** додає "шум" до даних, щоб приховати інформацію про окремих осіб або IoT-пристрої, водночас зберігаючи корисність загальних аналітичних даних. Вона дозволяє зберігати конфіденційність інформації про індивідуумів у наборі даних, забезпечуючи при цьому можливість отримувати статистичні висновки без розкриття особистої інформації [15]. Переваги: забезпечення конфіденційності (захищає особисті дані користувачів від несанкціонованого доступу); збереження аналітичної цінності (дозволяє отримувати корисну інформацію з даних, не розкриваючи особисту інформацію). Недоліки – втрата точності (додавання шуму може знизити точність аналізу), складність впровадження (реалізація диференціальної конфіденційності може вимагати значних зусиль у розробці)

- **Гомоморфне шифрування** дозволяє виконувати обчислення над зашифрованими даними без необхідності їх дешифрування. Це означає, що навіть оброблені дані залишаються захищеними [16]. Переваги: конфіденційність даних (гомоморфне шифрування дозволяє захищати чутливу інформацію, що збирається IoT-пристроями ,наприклад, дані про здоров'я, фінансову інформацію); обробка даних на сторонніх серверах (дозволяє виконувати обробку даних на хмарних серверах без необхідності їх розшифровувати, що знижує ризики витоку інформації); захист даних під час передачі (дослідження показують, що дані, які передаються між IoT-пристроями, можуть бути зашифровані, що запобігає їх перехопленню). Недоліки: висока обчислювальна складність (виконання обчислень над зашифрованими даними потребує значних обчислювальних ресурсів, що може бути проблемою для IoT-пристроїв з обмеженою потужністю); часова затримка (гомоморфне шифрування може викликати затримки в обробці даних через високу складність обчислень).

- **Zero-Trust архітектура** означає, що жоден пристрій чи користувач не довіряється за замовчуванням, навіть якщо він знаходиться у внутрішній мережі. Усі доступи повинні бути постійно перевірені та підтверджені. . У контексті Інтернету речей ця архітектура стає все більш важливою через зростаючу кількість підключених пристроїв, які можуть бути вразливими до атак [17]. Переваги: зменшення ризиків (Zero-Trust допомагає знизити ймовірність успішних атак, оскільки кожен доступ перевіряється); гнучкість (архітектура дозволяє безпечно інтегрувати нові пристрої та технології без необхідності переглядати всю мережу), покращення видимості (постійний моніторинг та аналіз допомагають у виявленні аномалій і підозрілої активності). Недоліки: складність налаштування (впровадження Zero-Trust вимагає детального аналізу всіх пристроїв і систем, що може бути складним); обмеження ресурсів (IoT-пристрої часто мають обмежені ресурси, що може ускладнити реалізацію вимог Zero-Trust),

- **Edge Computing (крайові обчислення) із безпекою на рівні пристрою** дозволяє обробляти дані безпосередньо на пристроях або поблизу них, замість відправлення всіх даних до централізованого хмари або серверів. Це має особливе значення для Інтернету речей, де швидкість обробки даних і безпека є критично важливими. Переваги: зниження затримок (Edge Computing дозволяє швидко реагувати на події, що покращує загальну ефективність системи); покращення безпеки (обробка даних на місці зменшує ризики, пов'язані з передачами даних через інтернет); зменшення навантаження на мережу (зменшення обсягу даних, які передаються до централізованих серверів, дозволяє економити ресурси). Недоліки: диверсифікація пристроїв (існує велика кількість різноманітних пристроїв в IoT, що ускладнює

забезпечення однорідного рівня безпеки); обмежені ресурси (багато IoT-пристроїв мають обмежені обчислювальні потужності, що може ускладнювати реалізацію складних механізмів безпеки); вразливість до фізичних атак (пристрої можуть бути вразливими до фізичного доступу, що може призвести до компрометації даних).

- **Контроль автентичності даних (Data Integrity Verification)** є критично важливою складовою, що забезпечує точність, повноту та захищеність даних, які збираються та передаються між пристроями. Наразі основні методи контролю це *хешування* (використання хеш-функцій (наприклад, SHA-256) для створення унікальних ідентифікаторів даних, це дозволяє перевіряти, чи дані були змінені, порівнюючи хеш значення), *цифрові підписи, контроль доступу, аудит і моніторинг, протоколи безпеки* (використання безпечних протоколів передачі даних, таких як TLS/SSL, для шифрування даних під час передачі, це захищає дані від перехоплення і модифікацій) [18-19]. Недоліки: обмежені ресурси**,** різноманітність пристроїв **(**існує велика кількість різних типів пристроїв в IoT, що ускладнює стандартизацію підходів до контролю автентичності даних); складність мережі (IoT-мережі часто є динамічними та розподіленими, що ускладнює відстеження та перевірку автентичності даних у реальному часі [5]).

- **Мультифакторна автентифікація (MFA) для IoT** теж є критично важливою складовою безпеки пристроїв Інтернету речей. Вона дозволяє значно знизити ризики несанкціонованого доступу, забезпечуючи додатковий рівень захисту [20]. Переваги: захист від атак (пристрої IoT часто є мішенню для хакерів через їх вразливості. MFA ускладнює доступ до системи навіть у разі компрометації одного з факторів); зниження ризику несанкціонованого доступу (навіть якщо зловмисник отримує пароль користувача, йому все ще потрібно пройти додаткові етапи автентифікації); захист конфіденційності (MFA допомагає захистити особисті дані користувача, які можуть бути вразливими в разі атаки на IoT пристрої). Недоліки: обмежені ресурси, зручність для користувача (надмірна складність процесу автентифікації може викликати незручності для користувачів, тому важливо знайти баланс між безпекою та зручністю).

Висновки. У процесі дослідження були розглянуті основні загрози конфіденційності в IoT-мережах, а також методи та технології, які можуть забезпечити захист даних в умовах обмежених ресурсів IoT-пристроїв. Результати дозволяють виявити важливі аспекти забезпечення конфіденційності в таких мережах, а також вказують на перспективні напрямки розвитку для покращення безпеки в IoT.

Зокрема, були визначені проблеми з методами аутентифікації та авторизації, вразливості в програмному забезпеченні та недостатній рівень захисту каналів зв'язку, що створюють серйозні загрози для конфіденційності. Крім того, було проаналізовано існуючі методи захисту та виявлено необхідність їх адаптації до специфіки IoT, зокрема з огляду на обмеження по ресурсах пристроїв.

Основні висновки та рекомендації:

1. Дослідження основних загроз конфіденційності в IoT-мережах:

Виявлено, що однією з головних загроз для конфіденційності в IoT є недостатньо надійні методи аутентифікації та авторизації користувачів. Крім того, вразливості в програмному забезпеченні пристроїв, а також незахищеність каналів зв'язку можуть призвести до несанкціонованого доступу до особистих даних.

2. Аналіз існуючих методів забезпечення конфіденційності в IoT:

Існуючі методи, такі як шифрування даних, використання багатофакторної аутентифікації та протоколів безпечної передачі даних (наприклад, TLS), є важливими, але недостатньо ефективними в умовах обмежених ресурсів IoT-пристроїв. Технології

повинні бути адаптовані до специфіки IoT, щоб забезпечити баланс між безпекою та енергоефективністю.

3. Вивчення застосування технологій шифрування та анонімності для захисту даних:Технології шифрування, зокрема симетричні та асиметричні алгоритми, дозволяють ефективно захищати конфіденційність даних в IoT-мережах. Однак високі вимоги до обчислювальних ресурсів вимагають застосування більш легких та адаптованих алгоритмів, таких як гібридне шифрування або постквантові методи.

4. Оцінка підходів до конфіденційності з урахуванням обмежених ресурсів IoT-пристроїв:Призначення IoT-пристроїв із обмеженими ресурсами потребує спеціальних методів, які дозволяють зберігати конфіденційність при мінімальних витратах на обчислення та енергію. Найбільш ефективними є моделі з використанням хмарних платформ для зберігання та обробки великих обсягів даних, що дозволяє знизити навантаження на самі пристрої.

5. Визначення перспективних напрямів розвитку технологій захисту конфіденційності в IoT:Перспективними напрямами розвитку є використання блокчейн-технологій для забезпечення прозорості та надійності даних, а також вдосконалення алгоритмів машинного навчання для виявлення аномалій в мережах IoT. Інші інноваційні підходи включають використання технологій квазі-анонімності для підвищення рівня анонімності користувачів і впровадження інтегрованих систем безпеки на апаратному рівні.

Хоча новітні методи захисту пристроїв IoT постійно вдосконалюються досі залишаються невирішеними проблеми стандартизації їх систем безпеки, актуальність оновлення програмного забезпечення, конфіденційність даних, недостатня обізнаність користувачів, складність інтеграції новітніх технологій.

Список літератури

1. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 15.02.2025).
2. California Consumer Privacy Act (CCPA). March 13, 2024. URL: https://oag.ca.gov/privacy/ccpa (дата звернення: 15.02.2025).
3. Pinto G.P., Donta P.K., Dustdar S., Prazeres C. A Systematic Review on Privacy-Aware IoT Personal Data Stores. Sensors. 2024. Vol. 24, No. 7. 2197. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC11014407/ (дата звернення: 10.02.2025).
4. Rajmohan T., Nguyen P.H., Ferry N. A decade of research on patterns and architectures for IoT security. Cybersecurity. 2022. Vol. 5. Article No. 2. URL: https://cybersecurity.springeropen.com/articles/10.1186/s42400-021-00104-7 (дата звернення: 12.02.2025).
5. Ataullah M., Chauhan N. Exploring security and privacy enhancement technologies in the Internet of Things: A comprehensive review. Security and Privacy. 2024. Vol. 7, Issue 6. e448. URL: https://onlinelibrary.wiley.com/doi/10.1002/spy2.448 (дата звернення: 15.02.2025).
6. Lu Y. Security and Privacy of Internet of Things: A Review of Challenges and Solutions. Journal of Cyber Security and Mobility. 2023. Vol. 12, Issue 6. URL: journals.riverpublishers.com/index.php/JCSANDM/article/view/22587/ (дата звернення: 15.02.2025).
7. Abomhara M., Køien G.M. Security and privacy in the Internet of Things: Current status and open issues. 2014 International Conference on Privacy and Security in Mobile Systems (PRISMS). 2014. DOI: 10.1109/PRISMS.2014.6970594. URL: https://www.researchgate.net/publication/269687360 (дата звернення: 15.02.2025).
8. Pinto G.P., Donta P.K., Dustdar S. A Systematic Review on Privacy-Aware IoT Personal Data Stores. Sensors. 2024. Vol. 24, No. 7. 2197. URL: https://pubmed.ncbi.nlm.nih.gov/38610408 (дата звернення: 15.02.2025).
9. Ystgaard K.F., Atzori L., Palma D., et al. Review of the theory, principles, and design requirements of human-centric Internet of Things (IoT). Journal of Ambient Intelligence and Humanized Computing. 2023. Vol. 14. P. 2827–2859. URL: https://link.springer.com/article/10.1007/s12652-023-04539-3 (дата звернення: 15.02.2025).

10. Sicari S., Rizzardi A., Grieco L.A., Coen-Porisini A. Security, privacy and trust in Internet of Things: The road ahead. Computer Networks. 2015. Vol. 76. P. 146–164. URL: https://www.sciencedirect.com/science/article/abs/pii/S1389128614003971 (дата звернення: 15.02.2025).
11. Roman R., Zhou J., López J. On the Features and Challenges of Security and Privacy in Distributed Internet of Things. Computer Networks. 2013. Vol. 57, Issue 10. P. 2266–2279. URL: https://www.sciencedirect.com/science/article/abs/pii/S1389128613000054 (дата звернення: 15.02.2025).
12. Ben Henda N., Msolli A., Hagui I., Helali A. Attack Detection in IoT Network Using Support Vector Machine and Improved Feature Selection Technique. Journal of Network and Systems Management. 2024. Vol. 32, No. 4. DOI: 10.1007/s10922-024-09871-3. URL: https://www.researchgate.net/figure/The-conventional-architecture-for-IoT-network_fig1_383984303 (дата звернення: 15.02.2025).
13. Meidan Y., Bohadana M., Mathov Y., et al. Network-based Detection of IoT Botnet Attacks Using Deep Autoencoders. IEEE Pervasive Computing. 2018. Vol. 17, Issue 3. URL: https://ieeexplore.ieee.org/document/8490192 (дата звернення: 15.02.2025).
14. Ul Haque E., Abbasi W., Almogren A., Choi J., et al. Performance enhancement in blockchain-based IoT data sharing using lightweight consensus algorithm. Scientific Reports. 2024. Vol. 14, Article No. 26561. URL: https://www.nature.com/articles/s41598-024-77706-x (дата звернення: 20.02.2025).
15. Jiang B., Li J., Yue G., Song H. Differential Privacy for Industrial Internet of Things: Opportunities, Applications and Challenges. IEEE Internet of Things Journal. 2021. Vol. 8, Issue 13. P. 10430–10451. URL: https://arxiv.org/abs/2101.10569 (дата звернення: 20.02.2025).
16. Chauhan K.K., Sanger A.K.S., Verm A. Homomorphic Encryption for Data Security in Cloud Computing. International Conference on Information Technology (ICIT). 2015. DOI: 10.1109/ICIT.2015.39. URL: https://ieeexplore.ieee.org/document/7437616 (дата звернення: 20.02.2025).
17. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. National Institute of Standards and Technology. 2020. DOI: 10.6028/NIST.SP.800-207.
18. Alkhonaini M.A., Alenizi F.A., Jazyah Y.H., Lee S. A two-phase spatiotemporal chaos-based protocol for data integrity in IoT. Scientific Reports. 2024. Vol. 14, Article No. 8629. URL: https://www.nature.com/articles/s41598-024-58914-x (дата звернення: 14.02.2025).
19. Baker A., Technologist P., River W. Maintaining data integrity in Internet of Things applications Arlen Baker, Principal Technologist, Wind River. URL: https://files.iccmedia.com/pdf/windriver160823.pdf (дата звернення: 14.02.2025).
20. Amos Z. Multi-Factor Authentication Is Crucial for IoT Security. URL: https://www.iotforall.com/multi-factor-authentication-is-crucial-for-iot-security (дата звернення: 19.02.2025).

References

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. (2016). Verkhovna Rada of Ukraine. Retrieved February 15, 2025, from https://zakon.rada.gov.ua/laws/show/984_008-16#Text [in Ukrainian].
2. California Consumer Privacy Act (CCPA). (2024, March 13). Retrieved February 15, 2025, from https://oag.ca.gov/privacy/ccpa.
3. Pinto, G. P., Donta, P. K., Dustdar, S., & Prazeres, C. (2024). A systematic review on privacy-aware IoT personal data stores. Sensors, 24(7), 2197. Retrieved February 10, 2025, from https://pmc.ncbi.nlm.nih.gov/articles/PMC11014407/.
4. Rajmohan, T., Nguyen, P. H., & Ferry, N. (2022). A decade of research on patterns and architectures for IoT security. Cybersecurity, 5, Article 2. Retrieved February 12, 2025, from https://cybersecurity.springeropen.com/articles/10.1186/s42400-021-00104-7.
5. Ataullah, M., & Chauhan, N. (2024). Exploring security and privacy enhancement technologies in the Internet of Things: A comprehensive review. Security and Privacy, 7(6), e448. Retrieved February 15, 2025, from https://onlinelibrary.wiley.com/doi/10.1002/spy2.448.
6. Lu, Y. (2023). Security and privacy of Internet of Things: A review of challenges and solutions. Journal of Cyber Security and Mobility, 12(6). Retrieved February 15, 2025, from https://journals.riverpublishers.com/index.php/JCSANDM/article/view/22587/.
7. Abomhara, M., & Køien, G. M. (2014). Security and privacy in the Internet of Things: Current status and open issues. Proceedings of the 2014 International Conference on Privacy and Security in Mobile Systems (PRISMS). https://doi.org/10.1109/PRISMS.2014.6970594.
8. Pinto, G. P., Donta, P. K., & Dustdar, S. (2024). A systematic review on privacy-aware IoT personal data stores. Sensors, 24(7), 2197. Retrieved February 15, 2025, from https://pubmed.ncbi.nlm.nih.gov/38610408
9. Ystgaard, K. F., Atzori, L., Palma, D., et al. (2023). Review of the theory, principles, and design requirements of human-centric Internet of Things (IoT). Journal of Ambient Intelligence and Humanized

Computing, 14, 2827–2859. Retrieved February 15, 2025, from link.springer.com/article/10.1007/s12652-023-04539-3.
10. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146–164. Retrieved February 15, 2025, from https://www.sciencedirect.com/science/article/abs/pii/S1389128614003971.
11. Roman, R., Zhou, J., & López, J. (2013). On the features and challenges of security and privacy in distributed Internet of Things. Computer Networks, 57(10), 2266–2279. Retrieved February 15, 2025, from https://www.sciencedirect.com/science/article/abs/pii/S1389128613000054.
12. Ben Henda, N., Msolli, A., Hagui, I., & Helali, A. (2024). Attack detection in IoT network using support vector machine and improved feature selection technique. Journal of Network and Systems Management, 32(4). https://doi.org/10.1007/s10922-024-09871-3.
13. Meidan, Y., Bohadana, M., Mathov, Y., et al. (2018). Network-based detection of IoT botnet attacks using deep autoencoders. IEEE Pervasive Computing, 17(3). Retrieved February 15, 2025, from https://ieeexplore.ieee.org/document/8490192.
14. Ul Haque, E., Abbasi, W., Almogren, A., Choi, J., et al. (2024). Performance enhancement in blockchain-based IoT data sharing using lightweight consensus algorithm. Scientific Reports, 14, Article 26561. Retrieved February 20, 2025, from https://www.nature.com/articles/s41598-024-77706-x.
15. Jiang, B., Li, J., Yue, G., & Song, H. (2021). Differential privacy for industrial Internet of Things: Opportunities, applications and challenges. IEEE Internet of Things Journal, 8(13), 10430–10451. Retrieved February 20, 2025, from https://arxiv.org/abs/2101.10569.
16. Chauhan, K. K., Sanger, A. K. S., & Verm, A. (2015). Homomorphic encryption for data security in cloud computing. Proceedings of the International Conference on Information Technology (ICIT). https://doi.org/10.1109/ICIT.2015.39.
17. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207.
18. Alkhonaini, M. A., Alenizi, F. A., Jazyah, Y. H., & Lee, S. (2024). A two-phase spatiotemporal chaos-based protocol for data integrity in IoT. Scientific Reports, 14, Article 8629. Retrieved February 14, 2025, from https://www.nature.com/articles/s41598-024-58914-x.
19. Baker, A., & River, W. (n.d.). Maintaining data integrity in Internet of Things applications. Retrieved February 14, 2025, from https://files.iccmedia.com/pdf/windriver160823.pdf.
20. Amos, Z. (n.d.). Multi-factor authentication is crucial for IoT security. Retrieved February 19, 2025, from https://www.iotforall.com/multi-factor-authentication-is-crucial-for-iot-security.

Yuriy Pidlisnyi
Chernihiv Polytechnic National University, Chernihiv, Ukraine

Possible Ways to Improve Privacy in IoT Networks

The rapid development of IoT technologies and their integration into everyday life are leading to a significant increase in the amount of data collected, transmitted and processed. This creates significant risks of confidential information leakage, which can have serious consequences for individual users, businesses and government agencies. In addition, the growing number of connected devices and their interaction in global networks increase the vulnerability of systems to cyberattacks, which can lead to unauthorized access to critical data.

The purpose of this article is to analyze the vulnerabilities of the Internet of Things (IoT) and to consider modern methods of detecting and counteracting cyber threats in such networks. The main objectives of the study include: Identification of the main threats and vulnerabilities of IoT networks at different levels of interaction; Analysis of modern attack methods applied to IoT systems and their consequences; Overview and classification of security methods, including cryptographic mechanisms, blockchain solutions, artificial intelligence-based anomaly detection systems, etc; Comparison of the effectiveness of different approaches to cybersecurity of IoT infrastructure and identification of their advantages and disadvantages; Formulating recommendations for the implementation of more reliable mechanisms to protect IoT networks.

Based on the analysis, the article proposes promising approaches to improving the security of IoT infrastructure, which can be used to minimize risks and improve the protection of users' personal information. The results of the study can be useful both for scientists dealing with cybersecurity issues and for practitioners working in the field of development and implementation of IoT solutions.

IoT network, artificial intelligence, machine learning, information security

Одержано (Received) 27.02.2025 *Прорецензовано (Reviewed) 07.03.2025*
Прийнято до друку (Approved) 14.03.2025