ПРОБЛЕМИ ЗАХИСТУ ДАНИХ В МЕРЕЖІ ІНТЕРНЕТ РЕЧЕЙ

Лотюк Юрій
кандидат педагогічних наук, доцент, доцент кафедри інформаційних систем та обчислювальних методів Приватного вищого навчального закладу «Міжнародний економіко-гуманітарний університет імені академіка Степана Дем'янчука»

Юскович-Жуковська Валентина
кандидат технічних наук, доцент, доцент кафедри інформаційних систем та обчислювальних методів Приватного вищого навчального закладу «Міжнародний економіко-гуманітарний університет імені академіка Степана Дем'янчука»
м. Рівне, Україна

Кот Василь
кандидат технічних наук, викладач вищої категорії Відокремленого структурного підрозділу «Рівненський фаховий коледж Національного університету біоресурсів і природокористування України»
м. Рівне, Україна

Стрімкий розвиток інформаційних технологій та поширення концепції Інтернету речей (IoT, Internet of Things) призвели до інтеграції мільярдів інтелектуальних пристроїв у єдину цифрову екосистему, в якій пристрої взаємодіють між собою та користувачем. За прогнозами аналітиків, кількість підключених IoT-пристроїв у світі перевищить 30 мільярдів до 2030 року.

Разом із цим зростає і обсяг генерованих, переданих та оброблюваних даних, значна частина яких має конфіденційний характер (персональні дані користувачів, медична інформація, фінансові транзакції, конфіденційні дані підприємств). Тому дослідження проблематики належного рівня безпеки та захисту цих даних являється актуальною проблемою мережі IoT.

Особливість IoT-мереж полягає у великій кількості гетерогенних пристроїв, що створює складнощі у впровадженні традиційних механізмів кіберзахисту, які успішно функціонують у класичних комп'ютерних мережах. Звідси випливають нові ризики: уразливості протоколів комунікації, складність централізованого моніторингу, високий рівень потенційних кіберзагроз. Ефективні механізми безпеки гарантують захист

інформації від несанкціонованого доступу. Але висока масштабність та різнорідність суттєво ускладнюють завдання забезпечення безпеки даних. Основні проблеми захисту можна узагальнити наступним чином:

1. Обмежені ресурси пристроїв. Більшість IoT-пристроїв характеризуються низькою обчислювальною потужністю, невеликим обсягом пам’яті та обмеженим енергоспоживанням. Це унеможливлює використання класичних криптографічних алгоритмів, що застосовуються у традиційних комп’ютерних мережах [1].

2. Уразливість протоколів зв’язку. У системах IoT активно застосовуються протоколи *MQTT, CoAP, ZigBee, LoRaWAN*, які зазвичай не мають вбудованих механізмів шифрування або автентифікації. Це створює ризик атак типу *«людина посередині» (Man-in-the-Middle, MITM),* перехоплення даних чи підробки повідомлень [2].

3. Масовість та децентралізація. IoT-мережі складаються з величезної кількості вузлів, розташованих у різних географічних точках. Централізоване управління безпекою в таких умовах ускладнене, а компрометація навіть одного «слабкого» вузла може поставити під загрозу всю систему [3].

4. Недостатність стандартів та регулювання. Попри активний розвиток IoT, єдиних міжнародних стандартів із забезпечення безпеки поки що не існує. Це призводить до того, що виробники реалізують власні підходи до захисту даних, які можуть бути несумісними або неефективними [4].

5. Ризики конфіденційності. У пристроях «розумних» будинків, медичних сенсорах або системах відеоспостереження часто обробляються персональні дані користувачів. Несанкціонований доступ до них може призвести до *порушення конфіденційності, шахрайства чи маніпуляцій поведінкою людини* [5].

Для раннього виявлення кіберзагроз у IoT використовують алгоритми машинного й глибинного навчання. Їх застосовують для аналізу мережевого трафіку, поведінкових закономірностей пристроїв та прогнозування атак. Це дозволяє оперативно реагувати на нові типи загроз, навіть коли традиційні сигнатурні методи не спрацьовують.

Сучасні дослідження пропонують інноваційні алгоритми захисту, наприклад, Attuned Data Protection with Privacy Scheme (ADP2S) на основі рептильного (swarm intelligence) пошуку — для миттєвого реагування на кіберінциденти в критичних IoT-інфраструктурах.

У межах IoT-екосистеми ефективний захист даних базується на комбінації криптографії, автентифікації, децентралізації, автоматичного виявлення загроз та розподілу функціоналу на edge та fog рівнях. Це особливо важливо враховувати з огляду на специфіку пристроїв — їхню

обмеженість ресурсів, географію, а також постійний розвиток кіберзагроз. Таким чином, методами захисту даних в мережі IoT можуть бути:

1. Шифрування даних. Використання алгоритмів симетричного та асиметричного шифрування (наприклад, AES, RSA) для захисту переданої інформації між пристроями.

2. Аутентифікація та управління доступом. Впровадження багатофакторної аутентифікації та ролей користувачів дозволяє зменшити ризик несанкціонованого доступу [2].

3. Виявлення аномалій. Використання алгоритмів машинного навчання для моніторингу поведінки пристроїв і виявлення підозрілих дій у реальному часі.

4. Регулярні оновлення та патчі. Оскільки більшість IoT-пристроїв мають обмежені ресурси, виробники часто ігнорують оновлення. Проте впровадження централізованих механізмів оновлення є критично важливим для безпеки.

5. Блокчейн для IoT. Використання блокчейн-технологій для розподіленого зберігання даних дозволяє підвищити прозорість і захист від маніпуляцій.

До найперспективніших напрямів у сфері захисту даних в IoT належать використання енергоефективних криптографічних алгоритмів, блокчейн-технологій, алгоритмів машинного навчання для виявлення аномалій, а також впровадження концепцій edge та fog обчислень для локалізації обробки даних та зменшення загроз централізованим вузлам.

Комплексне поєднання технічних, організаційних і нормативних заходів може забезпечити належний рівень кіберзахисту у сфері Інтернету речей та сприяти подальшому безпечному розвитку цієї технології у ключових сферах життєдіяльності суспільства.

ЛІТЕРАТУРА

1. Sun, P. та ін. (2025). *A survey on privacy and security issues in IoT-based* — всеохопний огляд ризиків/контрзаходів і рамка захисту приватності для різних рівнів IoT. // https://ssrn.com/abstract=5085989
2. Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). *Internet of Things security: A survey*. Journal of Network and Computer Applications, 88, 10–28.
3. 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.
4. Pinto, G. P. та ін. (2025). *Data Privacy in the Internet of Things: A Perspective of Personal Data Stores* — користувацько-центричні PDS як механізм контролю над персональними даними + регуляторні аспекти // *Journal of Cybersecurity and Privacy*, 2025, Vol. 5, No. 2, Article 25. https://www.mdpi.com/2624-800X/5/2/25
5. Zhou, J., Cao, Z., Dong, X., & Vasilakos, A. V. (2019). *Security and privacy for cloud-based IoT: Challenges*. IEEE Communications Magazine, 57(1), 26–33.