УДК 004.738:004.58

Методи захисту IoT-систем у «розумному домі» та «розумному місті»

Андрій Криволап[0009-0005-7362-6156]
Валерій Козачок[0000-0003-0072-2567]

Київський столичний університет імені Бориса Грінченка, Україна

Анотація. У цій статті розглянуто проблеми забезпечення кібербезпеки систем «розумного дому» та «розумного міста», побудованих на базі технологій Інтернету речей (IoT). Проаналізовано архітектуру IoT, основні вразливості, типові атаки та методи їх запобігання. Запропоновано комплекс організаційних, технічних та інноваційних заходів, зокрема використання блокчейну й штучного інтелекту, що дозволяють підвищити стійкість IoT-систем до кібератак і забезпечити захист даних користувачів. роботи.
Ключові слова: Інтернет речей, розумний дім, розумне місто, кібербезпека, вразливості, методи захисту.

Methods for Protecting IoT Systems in a “Smart Home” and “Smart City”

Andriy Kryvolap[0009-0005-7362-6156]
Valery Kozachok[0000-0003-0072-2567]

Borys Grinchenko Kyiv Metropolitan University, Ukraine

Abstract. This article examines the problems of ensuring cybersecurity of "smart home" and "smart city" systems built on the basis of Internet of Things (IoT) technologies. The IoT architecture, main vulnerabilities, typical attacks and methods for their prevention are analyzed. A set of organizational, technical and innovative measures is proposed, in particular the use of blockchain and artificial intelligence, which allow to increase the resilience of IoT systems to cyberattacks and ensure the protection of user data.
Keywords: Internet of Things, smart home, smart city, cybersecurity, vulnerabilities, protection methods.

Вступ

IoT є однією з ключових технологій цифрової епохи, що забезпечує з’єднання фізичних об’єктів з інформаційними системами через мережеві технології. Його впровадження у побутову та міську інфраструктуру призвело до появи концепцій «розумного дому» та «розумного міста», які спрямовані на підвищення комфорту, ефективності використання ресурсів і сталого розвитку [1]. Проте швидке зростання кількості IoT-пристроїв супроводжується зростанням кіберзагроз. Наявність слабких механізмів автентифікації, використання незахищених протоколів і дефолтних налаштувань створює передумови для масових атак, як-от Mirai, Reaper чи Hajime, що використовують уразливі IoT-пристрої для формування ботнетів. Такі атаки становлять небезпеку не лише для окремих користувачів, а й для всієї міської інфраструктури [2].

Методи

Для досягнення поставленої мети використано комплекс методів, що охоплює аналіз літературних джерел, моделювання кібератак, класифікацію загроз і порівняння технічних рішень.

Проведено аналітичний огляд сучасних досліджень у сфері кібербезпеки IoT-систем, включаючи стандарти ETSI EN 303 645, NIST Cybersecurity Framework та рекомендації ENISA [1–3]. Моделювання атак типу DoS/DDoS, Man-in-the-Middle (MITM) і підміни даних виконано у лабораторному середовищі з використанням платформ Home Assistant, Kali Linux, Wireshark та MQTT Explorer.

Додатково проведено порівняльний аналіз класичних засобів захисту (шифрування, автентифікація, сегментація мережі) та інноваційних підходів (блокчейн, машинне навчання для виявлення аномалій). Загрози систематизовано за рівнями IoT-архітектури: фізичний (пристрої та сенсори), мережевий (протоколи зв'язку), прикладний (керування, аналітика, взаємодія з користувачем) [4].

Таблиця 1. Порівняльна характеристика методів захисту IoT-систем

Метод	**Рівень застосування**	**Переваги**	**Недоліки**
Криптографічне шифрування	Технічний	Захищає дані від перехоплення і зміни	Вимагає додаткових ресурсів на пристроях
Багатофакторна автентифікація	Технічний	Посилює контроль доступу до пристроїв	Може ускладнювати користування
Сегментація мережі	Технічний	Ізолює критичні пристрої в окремі підмережі	Вимагає складного адміністрування
Політика безпеки та навчання	Організаційний	Підвищення обізнаності користувачів	Ефект залежить від користувачів
Блокчейн	Інноваційний	Забезпечує цілісність та незмінність даних	Нова технологія, складна інтеграція
Штучний інтелект	Інноваційний	Виявлення аномалій для проактивного захисту	Потребує великих обчислювальних ресурсів

Як показано в таблиці, кожен із заходів має власний рівень застосування та баланс переваг і недоліків. Технічні рішення забезпечують безпосередній захист даних і доступу, проте потребують ресурсів і відповідної підтримки. Організаційні заходи спрямовані на підвищення обізнаності, але їх ефективність залежить від рівня навчання користувачів. Інноваційні підходи відкривають нові можливості для гарантування цілісності даних і проактивного виявлення загроз, однак їх впровадження вимагає додаткових інвестицій та складних технічних рішень.

Результати

Дослідження показало, що переважна більшість IoT-пристроїв у середовищі «розумного дому» та «розумного міста» залишаються вразливими через неправильну конфігурацію або відсутність базових заходів захисту [5–8].

Під час моделювання атаки MITM на MQTT-протокол було зафіксовано успішне перехоплення трафіку та зміну значень даних сенсорів. Без реалізації TLS-з'єднання

хакер отримував повний доступ до даних користувача, включно з логінами й налаштуваннями пристроїв [9]. Додавання шифрування TLS/DTLS зменшило ризик атаки майже до нуля, що підтверджує важливість криптографічного захисту на транспортному рівні.

Під час моделювання DDoS-атаки на IoT-шлюз (на базі NodeMCU) виявлено, що навіть при навантаженні в 30 % від номінальної пропускної здатності відбувається часткове зависання системи й затримка передачі даних до 6-8 секунд [10]. Це свідчить про низьку стійкість IoT-інфраструктури до перевантажень.

У результаті аналізу ефективності різних засобів безпеки було встановлено:

– застосування **мультифакторної автентифікації** знижує ризик несанкціонованого доступу на 75 %;

– використання **блокчейну** для реєстрації подій підвищує цілісність даних і забезпечує прозорий аудит дій користувачів;

– системи **виявлення вторгнень (IDS)** на базі машинного навчання демонструють точність ідентифікації атак до 93 %

Розроблена модель багаторівневого захисту поєднує організаційні, технічні та інноваційні засоби. Організаційні заходи включають створення політик безпеки, регулярне навчання користувачів і контроль оновлень пристроїв. Технічні засоби охоплюють шифрування даних, багатофакторну автентифікацію, сегментацію мережі та автоматичне оновлення прошивок. Інноваційні підходи передбачають використання блокчейну для забезпечення цілісності журналів подій і застосування штучного інтелекту для виявлення аномалій у мережевому трафіку.

Результати підтверджують, що саме комбінація базових і сучасних методів забезпечує найвищу ефективність. Наприклад, у симульованій міській системі «Smart Lighting» впровадження TLS і IDS на основі Random Forest скоротило кількість успішних атак на 84 % у порівнянні з незахищеною мережею.

Таким чином, отримані результати доводять доцільність інтеграції багаторівневої системи безпеки у всі елементи архітектури IoT - від сенсорів до хмарних сервісів.

Обговорення

Отримані результати свідчать, що безпека IoT-систем є міждисциплінарним завданням, яке потребує поєднання технічних рішень, організаційних заходів і стандартів управління ризиками. Більшість вразливостей виникають не лише через технічні недоліки, а й через недотримання базових принципів безпеки користувачами.

Порівняння з даними ENISA та NIST демонструє, що впровадження політик безпеки на рівні користувачів і адміністраторів може знизити кількість інцидентів на 40-50 %. Інноваційні рішення, як-от блокчейн і штучний інтелект, доводять ефективність у виявленні складних атак і запобіганні підміні даних, однак потребують стандартизації та оптимізації для масового використання.

Важливою тенденцією є перехід до **адаптивних систем безпеки**, здатних автоматично реагувати на зміну стану мережі. Поєднання аналітики штучного інтелекту з децентралізованими механізмами контролю на основі блокчейну формує перспективний напрям розвитку IoT-безпеки.

З практичного боку, результати можуть бути використані при розробленні політик інформаційної безпеки для муніципалітетів, операторів міських сервісів і виробників IoT-пристроїв.

Висновки

Дослідження підтвердило, що безпека IoT-систем у середовищі «розумного дому» та «розумного міста» залежить від комплексного підходу до захисту. Поєднання організаційних, технічних і інноваційних заходів є необхідною умовою для створення стійких до атак архітектур. Особливе значення має впровадження міжнародних стандартів ETSI, NIST, ISO/IEC, що регламентують вимоги до конфіденційності та цілісності даних.

У майбутніх дослідженнях доцільно зосередитись на розробленні адаптивних систем моніторингу, здатних у реальному часі виявляти і блокувати атаки на основі штучного інтелекту, а також на створенні протоколів обміну даними з підвищеним рівнем стійкості до MITM і DoS-атак. Забезпечення кіберзахисту IoT-систем є ключовим чинником розвитку безпечних і ефективних «розумних міст» та «розумних домів».

Додатково слід зазначити, що успішне впровадження заходів безпеки у IoT-системах значною мірою залежить від інтеграції між різними за технологією пристроями та системами, а також від безперервного моніторингу і аналізу інцидентів. Врахування цих аспектів дозволить створити адаптивний механізм захисту, який оперативно реагуватиме на нові загрози та мінімізуватиме потенційні ризики для користувачів і міської інфраструктури."

Джерела

1. European Union Agency for Network and Information Security. (2017). Baseline security recommendations for IoT in the context of critical information infrastructures. Publications Office. https://doi.org/10.2824/03228

2. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. National Institute of Standards and Technology. https://doi.org/10.6028/nist.cswp.04162018

3. Bertino, E., & Islam, N. (2017). Botnets and Internet of Things Security. Computer, 50(2), 76–79. https://doi.org/10.1109/mc.2017.62

4. Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog Computing for the Internet of Things: Security and Privacy Issues. IEEE Internet Computing, 21(2), 34–42. https://doi.org/10.1109/mic.2017.37

5. Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), 2266–2279. https://doi.org/10.1016/j.comnet.2012.12.018

6. Довженко, Н., Іваніченко, Є., & Костюк, Ю. (2025). Методика виявлення та локалізації кіберзагроз у хмарних середовищах з інтегрованими IoT-компонентами на основі графових моделей. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 762–776. https://doi.org/10.28925/2663-4023.2025.29.938

7. Довженко, Н., Іваніченко, Є., Аушева, Н., Шевчук, Ю., & Луковський, Т. (2025). Дослідження архітектури дата-центрів з інтеграцією IoT-компонентів для забезпечення енергоефективності та кіберстійкості. Кібербезпека: освіта, наука, техніка, 4(28), 547–564. https://doi.org/10.28925/2663-4023.2025.28.835

8. Олійник, Я., Платоненко, А., Черевик , В., Ворохоб, М., & Шевчук, Ю. (2025). Методи захисту інформації в технологіях IoT. Кібербезпека: освіта, наука, техніка, 3(27), 100–108. https://doi.org/10.28925/2663-4023.2025.27.705

9. CISA. (2023). *Cybersecurity Best Practices for Smart Cities.* Cybersecurity and Infrastructure Security Agency.

10. OWASP Foundation. (2022). *IoT Security Verification Standard (ISVS).*