УДК 004.415.2
DOI https://doi.org/10.32782/2663-5941/2025.4.2/27

Мовчан К.О.
Український науково-дослідного інститут спеціальної
техніки та судових експертиз Служби безпеки України

КОМПЛЕКСНИЙ ПІДХІД ДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ГЕТЕРОГЕННИХ ЕКОСИСТЕМАХ ІНТЕРНЕТУ РЕЧЕЙ

У статті розглядається проблематика забезпечення інформаційної безпеки в гетерогенних екосистемах Інтернету речей (IoT), які характеризуються експоненційним зростанням кількості пристроїв та їх інтеграцією в критичні інфраструктури. Акцентується увага на обмеженості обчислювальних ресурсів та енергетичної автономності IoT-пристроїв, що унеможливлює застосування традиційних методів захисту та створює значні ризики для стабільності та безпеки систем у таких галузях, як енергетика, транспорт, охорона здоров'я та оборонно-промисловий комплекс.

Проаналізовано сучасні тенденції зростання кіберзагроз, зокрема атак із використанням штучного інтелекту, апаратних троянів та радіочастотних атак, які часто залишаються невиявленими через відсутність інтегрованих систем моніторингу. Окремо висвітлено вразливості хмарних інфраструктур, де відбувається обробка даних IoT-пристроїв, а також проблему фрагментації IoT-екосистеми, що ускладнює впровадження комплексних систем безпеки.

Визначено ключові вектори атак, що проявляються на різних рівнях п'ятирівневої архітектури IoT (перцепційний, мережевий, транспортний, прикладний та презентаційний). Детально розглянуто апаратні вразливості (апаратні «трояни», мікрозондові втручання, RF-атаки) на перцепційному рівні, мережеві атаки (DDoS/E-DDoS, MITM, sniffer-атаки) на мережевому та транспортному рівнях, а також програмні вразливості (переповнення буфера, hardcoded credentials, слабкі схеми автентифікації, інжекції коду) на рівні прикладної логіки.

Запропоновано багаторівневі контрзаходи, що включають криптографічний захист даних (AES-256, ECC, TLS/DTLS), використання систем виявлення вторгнень на базі глибоких згорткових нейронних мереж, honeypot-архітектури, автентифікацію за близькістю та інтеграцію систем динамічного управління патчами. Підкреслюється необхідність адаптивних підходів до безпеки в контексті специфічних IoT-впроваджень (розумні міста, медицина, аграрна та військова сфери). Підсумовується, що комплексний підхід до захисту IoT, який враховує мультишаровість систем, особливості застосування та обмеження обчислювальних ресурсів, є критично важливим. Формування чітко структурованої класифікації загроз у поєднанні з детальним описом механізмів реалізації атак та ефективних контрзаходів забезпечує комплексне бачення вразливостей IoT-систем, сприяє виявленню критичних точок впливу та створює основу для розробки стратегії проактивного захисту, що дозволяє прогнозувати розвиток загроз та проектувати адаптивні й стійкі до вторгнень IoT-рішення.

Ключові слова: *інтернет речей, IoT захист, IoT протоколи, аналіз вразливості, запобігання атакам.*

Постановка проблеми. Інтернет речей (IoT – Internet of Things) являє собою гетерогенну мережеву інфраструктуру, в якій фізичні об'єкти, оснащені сенсорами, виконавчими пристроями та програмним забезпеченням, інтегруються з глобальними мережами передачі даних за допомогою різноманітних бездротових протоколів для автономного обміну інформацією та взаємодії [1]. Згідно з аналітичними прогнозами, очікується, що до 2030 року кількість розгорнутих IoT-пристроїв досягне понад 30 мільярдів [2]. Їх системна інтеграція поширюється на сектори критичної інфраструктури, що включають енергетичні системи, транспортні мережі, охорону здоров'я, оборонно-промисловий комплекс та аграрний сектор. Водночас, таке стрімке масштабування та ускладнення архітектури IoT-косистем неминуче призводить до експоненційного зростання поверхні атаки [3]. Це, у свою чергу, провокує зростання кіберзагроз, серед яких розподілені атаки на відмову в обслуговуванні (DDoS), несанкціонований доступ до даних через вразливості вбудованого програмного забезпечення та несанкціонований доступ до пристроїв на фізичному рівні, що ство-

рює значні ризики для стабільності та безпеки зазначених критичних галузей.

IoT-пристрої, у порівнянні з класичними комп'ютерними системами, мають обмежені обчислювальні ресурси, енергетичну автономність, і часто проектуються з пріоритетом на економічну ефективність, а не на інформаційну безпеку [4]. Ці обмеження унеможливлюють використання традиційних методів захисту, що призводить до створення критично уразливого інформаційного середовища. Як наслідок, атаки на IoT можуть мати катастрофічні наслідки: порушення роботи медичних пристроїв, втручання в транспортні системи (наприклад, у протоколи V2V/V2I), саботаж енергомереж, або витік персональних даних мільйонів користувачів.

Станом на 2024 рік фіксується тенденція до зростання атак на основі штучного інтелекту, в використанням можливості автоматичного сканування мережі, здійснення адаптивних DDoS-атаки або можливість обходити класичні механізми автентифікації [5]. Згідно з доповіддю ENISA (2024), близько 67% IoT-інцидентів пов'язані з несанкціонованим доступом до пристроїв через слабкі або відсутні протоколи автентифікації. Значна частина IoT-пристроїв має відкриті порти, які не блокуються за замовчуванням.

Особливу загрозу становить використання апаратних троянів (Hardware Trojans) у фазі виробництва, які є маловиявляємі і можуть активуватися лише за специфічних умов [6]. Це відкриває потенціал для державного або корпоративного шпіонажу. Не менш небезпечними є атаки через радіочастотні канали (RF Attacks), які дозволяють перехоплювати та інжектувати сигнали без фізичного доступу до пристрою. При цьому, більшість сучасних пристроїв не має інтегрованих систем виявлення RF-перешкод.

Окрему категорію загроз становлять уразливості в хмарних інфраструктурах (Cloud Layer Vulnerabilities), де IoT-пристрої часто обробляють дані без шифрування, що надає противнику змогу перехоплювати трафік, вбудовувати шкідливий код або підмінювати відповіді серверів. Атаки типу Man-in-the-Middle та Packet Injection є особливо небезпечними в середовищах, де використовуються слабозахищені протоколи на кшталт MQTT без TLS.

Проблема також ускладнюється фрагментацією IoT-екосистеми – різні стандарти, протоколи (наприклад, ZigBee, BLE, LoRa, SigFox, NB-IoT), а також відсутність уніфікованих політик оновлення мікропрограмного забезпечення створюють серйозні бар'єри для впровадження комплексних систем безпеки.

У контексті оборонних технологій (IoBT – Internet of Battlefield Things) недоліки в захисті можуть не лише створити загрозу даним, а й призвести до фізичної загибелі солдат або провалу операцій. Наприклад, уразливі військові сенсори або дрони можуть бути віддалено перехоплені чи виведені з ладу через сигнальні атаки.

Таким чином, проблема забезпечення надійної інформаційної безпеки IoT є міждисциплінарною, комплексною і потребує негайного вирішення. Відсутність глибокої формалізації ризиків і недосконаліть існуючих контрзаходів лише підкреслюють нагальність досліджень у цьому напрямі.

Аналіз останніх досліджень і публікацій. Як правило дослідження у сфері IoT-безпеки фокусуються на вузькоспеціалізованих аспектах – зокрема, шифруванні протоколів (наприклад, MQTT, CoAP), IDS-системах на базі машинного навчання, або уразливостях фізичних сенсорів [7]. У публікації приділено увагу загрозам у smart home-середовищах, уразливості хмарних платформ, а також питанням реінжинірингу (reverse engineering) в IoT-пристроях [8]. Проте більшість досліджень мають обмежений оглядовий характер і не охоплюють повний спектр уразливостей із системним категоризуванням.

Сучасні дослідження все частіше вказують на тенденцію до застосування системного аналізу безпеки екосистеми Інтернету речей [9]. Сучасні системи використовують багаторівневі структури моделей для категоризації вразливостей за типом: апаратні (hardware), програмні (software), мережеві (network) та хмарні (cloud). Такий підхід дозволяє не лише ідентифікувати, але й систематизувати загрози. Наприклад, дослідження 2024 року підкреслюють, що ключовими векторами атак залишаються переповнення буфера (28.25% виявлених вразливостей) та атаки на відмову в обслуговуванні (27.20%) [10]. На основі цієї класифікації розробляються матриці атак, що зіставляють конкретні типи загроз із відповідними превентивними та реактивними заходами. Важливим елементом цих контрзаходів є активне застосування методів штучного інтелекту, зокрема для проактивного виявлення аномалій у поведінці пристроїв та автоматизації реагування на інциденти, що значно підвищує точність ідентифікації загроз та мінімізує кількість хибних спрацьовувань у порівнянні з традиційними системами безпеки.

Постановка завдання. Систематизація наявних векторів атак на IoT-системи та аналіз техно-

логій захисту з метою зниження площини атаки є одним із актуальних завдань у сфері кіберзахисту IoT-систем. Основна увага дослідження акцентується на важливості формалізованої архітектури п'ятирівневого IoT (перцепційний, доступу, передачі, прикладної підтримки та презентаційний шари), в якій і проявляються ключові вектори атак. Актуальність проблеми зумовлена швидким впровадженням IoT-пристроїв у критично важливі інфраструктури – від військових до медичних – де несанкціонований доступ навіть до одного вузла може мати катастрофічні наслідки [11]. Метою даного дослідження є систематизація та класифікація вразливостей IoT-екосистем, аналіз механізмів реалізації атак та обґрунтування ефективних контрзаходів для зниження загальної поверхні атаки.

Виклад основного матеріалу. Для забезпечення ефективного аналізу загроз у середовищі Інтернету речей (IoT) необхідним є системний розгляд архітектурної побудови IoT-систем з подальшою класифікацією векторів атак, що проявляються на різних технологічних рівнях. У контексті сучасної п'ятирівневої архітектури, яка включає перцепційний, мережевий, транспортний, прикладний та презентаційний рівні, виникає необхідність ідентифікації типових вразливих точок, характерних для кожного з рівнів [12].

На **перцепційному рівні** функціонують сенсорні модулі, RFID-мітки, камери та інші пристрої збору первинних даних. Саме тут закладається основа IoT-екосистем, однак одночасно формується й найбільш критичне середовище для атак фізичного доступу. **Апаратні вразливості**, характерні для цього рівня, охоплюють як навмисну модифікацію схемотехніки (впровадження апаратних "троянів"), так і високотехнологічні засоби аналізу, зокрема мікрозондові втручання, електромагнітне зчитування та реінжиніринг мікросхем. Особливо небезпечними є **RF-атаки**, що здійснюються шляхом пасивного аналізу сигналів та активного перехоплення, наприклад, під час перепідключення Bluetooth-пристроїв або підміни сигналів BLE через атаки типу spoofing. За даними дослідників, такі вектори атак часто залишаються невиявленими через обмежені ресурси обчислювальних блоків і відсутність моніторингових підсистем на фізичному рівні.

На **мережевому та транспортному рівнях** реалізуються протоколи зв'язку – від класичних WiFi та Ethernet до спеціалізованих рішень ZigBee, LoRaWAN, BLE, 5G-NR, NB-IoT [13]. Ці технології забезпечують взаємодію пристроїв та передачу даних, однак вони є вразливими до **мережевих атак**. Зокрема, поширеними загрозами залишаються атаки типу **DDoS/E-DDoS**, які спрямовані на перевантаження ресурсів пристрою чи його енергетичного модуля. Крім того, **атаки типу «людина посередині» (MITM)**, а також **sniffer-атаки** на основі аналізу нешифрованого трафіку (особливо у застарілих реалізаціях WPA/WEP) створюють прямий вектор несанкціонованого зняття інформації. За останніми дослідженнями, розповсюдженими також є **over-the-air атаки**, які поєднують методи радіочастотного моніторингу з машинним навчанням для ідентифікації пристроїв та сценаріїв їх взаємодії у мережі. Застосування нейронних мереж для моделювання мережевого трафіку дозволяє не лише виявляти активні вузли, а й передбачати їх поведінкові шаблони, що відкриває простір для здійснення прогнозованих атак.

На рівні **прикладної логіки** загрозу становлять **програмні вразливості**, до яких належать:

– **переповнення буфера**, що відкриває шлях до виконання шкідливого коду;

– **hardcoded credentials** – типова помилка розробників, яка створює бекдор-доступ до пристрою;

– **слабкі схеми автентифікації**, включно з відсутністю багатофакторної перевірки;

– **несанкціоноване оновлення мікропрограмного забезпечення**, що допускає впровадження модифікованого програмного забезпечення;

– **інжекції коду** (наприклад, через IoT API або веб-інтерфейси).

Особливої уваги заслуговують ситуації, коли пристрій фізично доступний зловмиснику: у такому випадку відновлення прошивки, доступ до Hex-даних та декомпіляція бінарних образів за допомогою таких програмних продуктів, як Ghidra або IDA Pro, дають змогу реконструювати логіку роботи пристрою, що у свою чергу, дозволяє впровадити backdoor-логіку або змінити потік керування без виявлення порушень функціонування системи з боку користувача.

У світлі вищеописаних ризиків, потреба в **багаторівневих контрзаходах** є нагальною. Найбільш ефективними заходами вважаються:

– **криптографічний захист** даних – AES-256, ECC, TLS/DTLS;

– **використання систем виявлення вторгнень (IDS)** на базі глибоких згорткових нейронних мереж, які забезпечують аналіз трафіку в реальному часі;

– **honeypot-архітектури**, які діють як пастки для виявлення ботів та активних атак;

– **автентифікація за близькістю (proximity-based authentication)**, яка забезпечує захист на фізичному рівні [14].

Особливу увагу слід приділяти інтеграції систем **динамічного управління патчами (dynamic patch management)**, які дозволяють автоматично і своєчасно оновлювати прошивку без втрати цілісності або функціональності пристрою. В цьому сенсі застосування цифрових підписів та контрольованих каналів доставки оновлень – критично необхідна умова безпечної експлуатації.

Нарешті, специфіка IoT-впроваджень у критичних середовищах – таких як **розумні міста (smart cities)**, **медицина (IoMT)**, **аграрна галузь (IoAT)** та **військова сфера (IoBT)** – потребує адаптивних підходів до безпеки [15]. Наприклад, для розгортання IoBT критично важливо забезпечити захист сенсорів на полі бою від фізичних і електромагнітних загроз, а також застосовувати надійні протоколи обміну даними, які запобігають їх перехопленню. IoMT-пристрої потребують сертифікації відповідно до медичних протоколів і стандартів HIPAA/GDPR, а в IoAT – особливу увагу слід приділяти захисту телеметрії з віддалених ділянок.

Таким чином, захист IoT-інфраструктури потребує інтегрованого підходу, що враховує мультишаровість систем, особливості застосування та обмеження обчислювальних ресурсів. Реалізація таких стратегій можлива лише за умов формалізованої політики безпеки, тісної співпраці виробників з експертами з кібербезпеки та постійного моніторингу загроз.

Висновки. Проведене дослідження виявляє необхідність комплексного підходу до захисту IoT, що дозволяє оцінити вразливості в контексті всього ланцюга передачі даних. Формування чітко структурованої класифікації загроз у поєднанні з детальним описом механізмів реалізації атак та ефективних контрзаходів забезпечує комплексне бачення вразливостей IoT-систем, сприяє виявленню критичних точок впливу та створює основу для розробки стратегії проактивного захисту. Такий підхід дозволяє не лише ідентифікувати потенційні вектори атак на різних рівнях архітектури, а й прогнозувати їх розвиток у контексті динамічної еволюції загроз, що особливо важливо для проектування адаптивних і стійких до вторгнень IoT-рішень.

Список літератури:

1. Atzori L., Iera A., Morabito G. The Internet of Things: A survey. Computer Networks, 54(15), 2010, pp. 2787-2805.

2. Statista Research Department. Internet of Things – number of connected devices worldwide, Statista, pp. 2019-2030, 2024.

3. Zhang Y., Xu C., Li H., Yang K., Zhou J., Lin X. HealthDep: An efficient and secure deduplication scheme for cloud-assisted eHealth systems. IEEE Transactions on Industrial Informatics, 14(9), 2018, pp. 4101-4112.

4. Roman R., Zhou J., Lopez J. On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), 2013, pp. 2266-2279.

5. Kumar S., Tiwari P., Zymbler M. Internet of Things is a revolutionary approach for future technology enhancement. Journal of Big Data, 6(1), 2019, pp. 1-21.

6. Tehranipoor M., Koushanfar F. A survey of hardware trojan taxonomy and detection. IEEE Design & Test of Computers, 27(1), 2010, pp. 10-25.

7. Granjal J., Monteiro E., Silva J.S. Security for the internet of things: a survey of existing protocols and open research issues. IEEE Communications Surveys & Tutorials, 17(3), 2015, pp. 1294-1312.

8. Zhao K., Ge L. A survey on the internet of things security. Ninth International Conference on Computational Intelligence and Security, 2013, pp. 663-667.

9. Sicari S., Rizzardi A., Grieco L.A., Coen-Porisini A. Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 2015, pp. 146-164.

10. Li S., Xu L.D., Zhao S. The internet of things: a survey. Information Systems Frontiers, 17(2), 2015, pp. 243-259.

11. Burhan M., Rehman R.A., Khan B., Kim B.S. IoT elements, layered architectures and security issues: A comprehensive survey. Sensors, 18(9), 2018, p. 2796.

12. Al-Fuqaha A., Guizani M., Mohammadi M., Aledhari M., Ayyash M. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2015, pp. 2347-2376.

13. Raza S., Wallgren L., Voigt T. SVELTE: Real-time intrusion detection in the Internet of Things. Ad Hoc Networks, 11(8), 2013, pp. 2661-2674.

14. Zhang Z.K., Cho M.C.Y., Wang C.W., Hsu C.W., Chen C.K., Shieh S. IoT security: ongoing challenges and research opportunities. IEEE 7th International Conference on Service-Oriented Computing and Applications, 2014, pp. 230-234.

15. Whitmore A., Agarwal A., Da Xu L. The Internet of Things–A survey of topics and trends. Information Systems Frontiers, 17(2), 2015, pp. 261-274.

Movchan K.O. A COMPREHENSIVE APPROACH TO ENSURING INFORMATION SECURITY IN HETEROGENEOUS INTERNET OF THINGS ECOSYSTEMS

The article discusses the issue of ensuring information security in heterogeneous Internet of Things (IoT) ecosystems, which are characterised by exponential growth in the number of devices and their integration into critical infrastructures. It highlights the limited computing resources and energy autonomy of IoT devices, which makes it impossible to use traditional protection methods and creates significant risks to the stability and security of systems in sectors such as energy, transport, healthcare, and the defence industry.

The paper analyses current trends in the growth of cyber threats, in particular attacks using artificial intelligence, hardware Trojans and radio frequency attacks, which often remain undetected due to the lack of integrated monitoring systems. The vulnerabilities of cloud infrastructures, where IoT device data is processed, are highlighted separately, as well as the problem of fragmentation of the IoT ecosystem, which complicates the implementation of comprehensive security systems.

Key attack vectors are identified that manifest themselves at different levels of the five-level IoT architecture (perceptual, network, transport, application, and presentation). Hardware vulnerabilities (hardware Trojans, microprobe interference, RF attacks) at the perception level, network attacks (DDoS/E-DDoS, MITM, sniffer attacks) at the network and transport levels, as well as software vulnerabilities (buffer overflow, hardcoded credentials, weak authentication schemes, code injection) at the application logic level.

Multi-level countermeasures are proposed, including cryptographic data protection (AES-256, ECC, TLS/DTLS), the use of intrusion detection systems based on deep convolutional neural networks, honeypot architectures, proximity authentication, and the integration of dynamic patch management systems. The need for adaptive approaches to security in the context of specific IoT implementations (smart cities, medicine, agriculture, and military) is emphasised. It is concluded that a comprehensive approach to IoT protection, which takes into account the multi-layered nature of systems, application characteristics, and computing resource limitations, is critically important. The formation of a clearly structured classification of threats, combined with a detailed description of attack mechanisms and effective countermeasures, provides a comprehensive view of the vulnerabilities of IoT systems, helps identify critical points of impact, and creates a basis for developing a proactive defence strategy that allows for the prediction of threat development and the design of adaptive and intrusion-resistant IoT solutions.

Key words: *Internet of Things, IoT protection, IoT protocols, vulnerability analysis, attack prevention.*

Дата надходження статті: 28.07.2025
Дата прийняття статті: 08.08.2025
Опубліковано: 27.10.2025