УДК 004.056

І. С. Зоря
О. В. Ніколайчук

ТЕХНОЛОГІЇ ЗАХИСТУ API ТА ВЕБ-ІНТЕРФЕЙСІВ У СИСТЕМАХ УПРАВЛІННЯ IOT-ПРИСТРОЯМИ

Вінницький національний технічний університет

Анотація: *Робота присвячена дослідженню проблеми кібербезпеки систем управління пристроями Інтернету речей, зокрема комплексному аналізу сучасних технологій захисту їхніх програмних та веб-інтерфейсів. Стрімке розширення екосистеми Інтернету речей зумовило безпрецедентне зростання ризиків у сфері кібербезпеки. Основою взаємодії в таких архітектурах є прикладні програмні інтерфейси та веб-інтерфейси управління, які забезпечують обмін даними між пристроями та хмарними платформами. У роботі розглядаються особливості сучасних кіберзагроз на основі OWASP API Security Top 10, еволюція методів автентифікації та авторизації, а також проблеми впровадження криптографії на ресурсообмежених пристроях. Особливий акцент зроблено на необхідності переходу до архітектури нульової довіри та дотриманні міжнародних стандартів безпеки для побудови надійних систем управління.*

Ключові слова*: Інтернет речей, безпека API, веб-інтерфейси управління, OWASP, авторизація, автентифікація, OAuth 2.0, JWT, mTLS, архітектура нульової довіри.*

Вступ

Сьогодні системи IoT інтегровані практично в усі сфери життя – від розумних будинків і медичних пристроїв до промислової автоматизації та критичної інфраструктури. За прогнозами аналітиків, кількість підключених IoT-пристроїв у найближчі роки перевищить десятки мільярдів. Фундаментом, який забезпечує керованість цієї глобальної екосистеми, виступають прикладні програмні інтерфейси та веб-інтерфейси управління.

Однак API за своєю природою створені для того, щоб бути відкритими та забезпечувати прямий доступ до бізнес-логіки систем. Це робить їх однією з найпривабливіших мішеней для кіберзлочинців. Традиційні засоби захисту периметра мережі часто виявляються неефективними, оскільки зловмисники імітують легітимний трафік, експлуатуючи логічні недоліки інтерфейсів. Ситуація ускладнюється тим, що більшість IoT-пристроїв мають жорсткі обмеження щодо обчислювальної потужності та енергоспоживання, що унеможливлює використання "важких" класичних методів шифрування.

Метою цієї роботи є оглядовий аналіз сучасних векторів атак на API та веб-інтерфейси систем управління IoT-пристроями, а також розгляд актуальних технологій і архітектурних підходів для їх ефективного захисту.

Результати дослідження

Сучасні вектори атак на IoT-системи остаточно змістилися від спроб зламати безпосередньо фізичне обладнання до експлуатації вразливостей хмарних API, які цим обладнанням керують. Згідно з актуальними дослідженнями та даними організації Open Web Application Security Project [1], домінуючими загрозами є:

– порушення авторизації на рівні об'єктів. Зловмисник підміняє ідентифікатор пристрою в API-запитів наприклад, ID чужого розумного замка або камери. Отримуючи несанкціонований доступ до обладнання через відсутність належної криптографічної перевірки прав на стороні сервера [2].

– слабка та / або зламана автентифікація. Використання статичних, жорстко закодованих у прошивку API-ключів або слабких паролів за замовчуванням дозволяє хакерам легко отримувати доступ до систем управління. Наслідком цього стають масові компрометації та створення глобальних ботнетів, таких як виявлений у 2025 році BadBox 2.0, що інфікував мільйони пристроїв через компрометацію ланцюга поставок та ботнет Raptor Train [3].

– необмежене споживання ресурсів. Відсутність суворих лімітів на кількість запитів до API дозволяє проводити DDoS-атаки. Для IoT це означає перевантаження хмарних серверів [4].

– "тіньові" та "зомбі" API. Застарілі, тестові або недокументовані версії веб-інтерфейсів, які залишаються активними в мережі без підключення до сучасних систем моніторингу та авторизації, перетворюються на невидимі "чорні ходи" для витоку чутливих даних [5].

Оскільки класичні методи автентифікації на основі сесій є нежиттєздатними для масштабних IoT-мереж, індустрія масово переходить до сучасних криптографічних протоколів. Для надійного захисту застосовуються такі технології:

– JSON Web Tokens [6]. Компактні токени доступу, які не вимагають від сервера зберігання стану. Вони забезпечують надзвичайно високу швидкість перевірки прав на API-шлюзах, що є критичним для систем з мільйонами підключених пристроїв. Оскільки вкрадений токен важко відкликати, передовою практикою є встановлення дуже короткого терміну його дії та використання безпечних асиметричних алгоритмів цифрового підпису .

– OAuth 2.0 [7]. Індустріальний стандарт для захищеної міжмашинної взаємодії. Цей фреймворк дозволяє автономним IoT-пристроям централізовано отримувати тимчасові токени з чітко та вузько обмеженими правами доступу, усуваючи небезпечну необхідність передачі постійних паролів мережею.

– взаємна автентифікація Mutual TLS та mTLS. Найвищий стандарт транспортної безпеки. При mTLS і сервер (API), і сам IoT-пристрій пред'являють та криптографічно перевіряють цифрові сертифікати X.509 один одного під час встановлення з'єднання. Це повністю унеможливлює атаки типу "людина посередині" та підміну пристроїв, хоча і вимагає розгортання складної інфраструктури управління відкритими ключами [8].

– токени, жорстко прив'язані до сертифіката, специфікація RFC 8705 [9]. Найсучасніший підхід, який поєднує гнучкість JWT та транспортну безпеку mTLS. Навіть якщо хакер перехопить такий токен, він буде для нього марним без наявності апаратного закритого ключа скомпрометованого пристрою.

Впровадження цих надійних методів шифрування неминуче стикається з об'єктивними обмеженнями найдешевших мікроконтролерів, дефіцит оперативної пам'яті, слабкі процесори. Спроби прямого використання важких алгоритмів (наприклад, RSA) призводять до значних затримок. Тому сучасним рішенням є активне застосування криптографії на еліптичних кривих та методів легкої криптографії Lightweight Cryptography. Зокрема, нещодавно стандартизований NIST алгоритм ASCON, а також швидкий потоковий шифр XChaCha20 демонструють видатну продуктивність виключно на програмному рівні, гарантуючи конфіденційність даних без суттєвого енергетичного навантаження на систему [10] .

Масове розгортання гібридних хмарних систем та IoT остаточно зруйнувало концепцію "захищеного корпоративного периметра". На сьогодні найбільш перспективною парадигмою захисту визнано Архітектуру нульової довіри, яка базується на аксіомі "ніколи не довіряй за замовчуванням, завжди перевіряй"[11]. Її практична імплементація передбачає:

– безперервну верифікацію. Кожен окремий запит до API перевіряється та автентифікується незалежно від того, чи надійшов він із публічного відкритого Інтернету, чи з нібито "захищеної" внутрішньої мережі [12] .

– мікросегментацію на базі API-шлюзів. Шлюзи діють як інтелектуальні цифрові контролери, що суворо розмежовують трафік і не дозволяють різним категоріям пристроїв наприклад, системам відеонагляду та медичним датчикам, несанкціоновано взаємодіяти між собою [13].

– поведінкову аналітику. Системи оцінюють поточний стан та контекст роботи пристрою. Якщо датчик температури раптово починає генерувати тисячі важких запитів, система автоматично ізолює його від API до з'ясування обставин [14].

Ефективність цих технологічних підходів закріплюється на рівні міжнародних нормативних баз. Розробка безпечних веб-інтерфейсів та систем управління сьогодні вимагає безумовного дотримання керівних принципів, таких як стандарт NIST SP 800-213 [15] для державних систем США та глобальний стандарт ISO/IEC 27402 [16]. Ці документи вимагають впровадження концепції безпека на етапі проектування архітектури та повної відмови від практики використання статичних паролів ще на конвеєрі виробництва.

Підсумовуючи, перетворення прикладних програмних інтерфейсів на критичну магістраль цифрової економіки вимагає комплексного, ешелонованого захисту. Використання застарілих методів, таких як базові API-ключі, є небезпечним. Лише синергія Архітектури нульової довіри, сучасних протоколів делегованої авторизації OAuth 2.0, JWT, транспортної криптографії mTLS та легкої криптографії для мікроконтролерів дозволить забезпечити надійну безпеку, стійкість та конфіденційність у глобальних мережах Інтернету речей.

Висновок

Розширення сфери застосування Інтернету речей перетворює прикладні програмні інтерфейси на критичну інфраструктуру, яка потребує багаторівневого захисту. Оглядове дослідження демонструє, що застарілі методи безпеки, такі як статичні API-ключі або надія на брандмауери, є абсолютно недостатніми проти сучасних загроз логічного рівня.

Найперспективнішою стратегією захисту веб-інтерфейсів та API у системах управління IoT є комплексний підхід: впровадження концепції нульової довіри, перехід на сучасні стандарти делегованої авторизації, застосування жорсткої взаємної автентифікації пристроїв та використання легковагої криптографії для збереження ресурсів мікроконтролерів. Лише використання розумних API-шлюзів у поєднанні із суворим дотриманням міжнародних галузевих стандартів NIST та ISO здатне забезпечити стабільність, безпеку та конфіденційність даних у глобальних IoT-мережах.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1) OWASP top 10 API security risks – 2023 - OWASP API security top 10. *OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation*. URL: https://owasp.org/API-Security/editions/2023/en/0x11-t10/ (дата звернення: 08.03.2026).

2) 7 API Security Issues in 2025, and How to Deal With Them URL: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-application-security-appsec/what-is-api-security/7-api-security-issues-in-2025-and-how-to-deal-with-them/ (дата звернення: 08.03.2026).

3) IoT hacking statistics 2025: threats, risks & regulations. *DeepStrike*. URL: https://deepstrike.io/blog/iot-hacking-statistics (дата звернення: 08.03.2026).

4) Axe-Web D. API security in 2025: practical assessment & modern protection strategies. *GlobalDots*. URL: https://www.globaldots.com/resources/blog/api-security/ (дата звернення: 8.03.2026).

5) What is API security?. *Trend Micro*.URL: https://www.trendmicro.com/en_gb/what-is/cloud-security/api-security.html (дата звернення: 10.03.2026).

6) Song J. Detailed Explanation of Common Authentication Methods in Microservices | Jimmy Song. *Jimmy Song*. URL: https://jimmysong.io/blog/microservice-auth-methods/ (дата звернення: 10.03.2026).

7) Karre S. OAuth client credentials vs mutual TLS for M2M authentication. *Scalekit: Auth Stack for AI Apps | Start Free*. URL: https://www.scalekit.com/blog/oauth-client-credentials-vs-mtls (дата звернення: 10.03.2026).

8) Buckle Up Your mTLS With OAuth 2.0 Client Authentication and Certificate-Bound Access. *Form3 | Payment technology reimagined*. URL: https://www.form3.tech/blog/engineering/buckle-up-your-mtls-with-oauth-2-0-client-authentication (дата звернення: 14.03.2026).

9) RFC 8705: OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens. *IETF Datatracker*. URL: https://datatracker.ietf.org/doc/html/rfc8705 (дата звернення: 14.03.2026).

10) Comparative Performance Analysis of Lightweight Cryptographic Algorithms on Resource-Constrained IoT Platforms - PMC. *PMC Home*. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC12473500/ (дата звернення: 14.03.2026).

11) What Is Zero Trust Architecture? Key Elements and Use Cases. *Palo Alto Networks*. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture (дата звернення: 16.03.2026).

12) Zero Trust API Security: What It Is and Why It Matters. *Cequence Security*. URL: https://www.cequence.ai/blog/api-security/zero-trust-api-security-model/ (дата звернення: 16.03.2026).

13) API Security in the Age of IoT - API7.ai. *API Security in the Age of IoT - API7.ai*. URL: https://api7.ai/learning-center/api-101/api-security-in-the-age-of-iot (дата звернення: 18.03.2026).

14) Why Zero Trust Is Critical for IoT Security | Zscaler. *Leading Cloud Enterprise Security Provider for Zero Trust*. URL: https://www.zscaler.com/zpedia/why-zero-trust-is-critical-for-iot-security (дата звернення: 18.03.2026).

15) SP 800-213, IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements | CSRC. *NIST Computer Security Resource Center | CSRC*. URL: https://csrc.nist.gov/pubs/sp/800/213/final (дата звернення: 18.03.2026).

16) INTERNATIONAL STANDARD ISO/IEC 27402. *Cybersecurity – IoT security and privacy – Device baseline requirements*. URL: https://cdn.standards.iteh.ai/samples/80136/91e2567c20bf456aa0dc2048a93bf518/ISO-IEC-27402-2023.pdf (дата звернення: 18.03.2026).

Ніколайчук Олександр Вікторович – студент групи КІТС-25м, факультет менеджменту і інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: oleksandernikol@gmail.com

Науковий керівник: ***Зоря Ірина Сергіївна*** – ас. каф. Менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: ira.zoria@vntu.edu.ua

Nikolaychuk Oleksandr V. student of group CITS-25м, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: oleksandernikol@gmail.com

Supervisor: ***Zoria Iryna S.*** – assistant of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: e-mail: ira.zoria@vntu.edu.ua