protection — Information security management systems — Requirements. URL: https://www.iso.org/standard/27001
2. ISO/IEC 27031:2025. Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity. URL: https://www.iso.org/standard/27031
3. The NIST Cybersecurity Framework (CSF) 2.0. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
4. NIST Special Publication 800-160, Volume 2. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf
5. MITRE ATT&CK Framework. URL: https://attack.mitre.org/\
6. Cyber Resilience Review. URL: https://www.cisa.gov/resources-tools/services/cyber-resilience-review-crr
7. Cyber Resilience Index. URL: https://www3.weforum.org/docs/WEF_Cyber_Resilience_Index_2022.pdf
8. Cyber Assessment Framework. URL: https://www.ncsc.gov.uk/collection/cyber-assessment-framework
9. Cyber Resilience Assessment Framework. URL: https://uploads-ssl.webflow.com/59d28ad983887e000196f803/5fecc1fe13498132b4fa835b_HKMA CFI - Cyber Resilience Assessment Framework - Dec 2016.pdf
10. IT Governance Cyber Resilience Framework. URL: https://www.itgovernance.co.uk/cyber-resilience-framework

Мережева безпека IoT-пристроїв у кіберфізичних системах розумного міста

УДК 004.056:004.738.5:681.5

Андрій Микитишин[1], Сергій Козак[2]
Роман Ніколайчук[3]

Тернопільський національний технічний університет імені Івана Пулюя,
[1]mikitishin@gmail.com, [2]serhii_kozak1710@tntu.edu.ua,
[3]romanikolaychuk2017@gmail.com

Концепція розумного міста передбачає використання кіберфізичних систем, у яких IoT-пристрої поєднують фізичні об'єкти інфраструктури з цифровими сервісами, сенсорними мережами, edge-вузлами, хмарними платформами та системами підтримки рішень. Вони забезпечують телеметрію, дистанційне керування, автоматичне реагування й інтеграцію з сервісами освітлення, транспорту, екологічного моніторингу, енергоменеджменту, водопостачання та безпеки громадських просторів. Ключовою проблемою є мережева безпека IoT-пристроїв, оскільки через мережеву взаємодію передаються дані між сенсорами, шлюзами, платформами оброблення й операторськими інтерфейсами. Розподіленість вузлів, різнорідні протоколи, обмежені ресурси, фізична доступність частини обладнання, бездротові канали й залежність від хмарних сервісів підвищують ризик перехоплення або підміни телеметрії, відмови сервісу, втрати керованості виконавчими механізмами та помилкових

управлінських рішень[1]. Для IoT-систем це означає потребу в моделі, що враховує маршрути передавання даних, сегментацію, правила доступу, журнали подій, захищене оновлення та взаємодію з хмарними платформами. Базові вимоги IoT-безпеки передбачають відмову від універсальних стандартних паролів, безпечне зберігання облікових даних, керування вразливостями, оновлення програмного забезпечення й мінімізацію поверхні атаки [2].

Основними загрозами є перехоплення трафіку, MITM-атаки, несанкціоноване підключення вузлів, сканування портів, слабкі паролі, підміна ідентифікаторів, атаки на MQTT, CoAP, HTTP, Modbus TCP та порушення доступності.

Таблиця 1

Основні рівні мережевого захисту IoT-пристроїв

Рівень захисту	Об'єкти захисту	Типові ризики	Захисні заходи
Рівень пристроїв	сенсори, контролери, виконавчі модулі	несанкціонований доступ, слабкі паролі, вразлива прошивка	унікальні облікові дані, безпечне оновлення, вимкнення зайвих сервісів
Мережевий рівень	канали зв'язку, шлюзи, маршрутизатори, протоколи	перехоплення трафіку, MITM-атаки, DDoS, підміна пакетів	шифрування, VPN, TLS, сегментація, фільтрація трафіку
Рівень платформ	edge-вузли, хмарні сервіси, API, панелі керування	компрометація доступу, витік даних, порушення доступності	контроль доступу, журналювання, резервування, SIEM-моніторинг

Практична реалізація має починатися з інвентаризації IoT-пристроїв і класифікації їх за критичністю. Для кожного вузла визначають функцію, мережеву адресу, протоколи обміну, рівень доступу, залежності та наслідки компрометації. Далі формують окремі сегменти для критичних пристроїв, тестових вузлів, адміністративного доступу, публічних сервісів і платформ оброблення даних, що зменшує ризик горизонтального поширення атаки.

Технічний захист має включати TLS для прикладних протоколів, VPN для віддаленого адміністрування, сертифікати пристроїв для взаємної автентифікації, контроль цілісності повідомлень і керування ключами. Для обмежених IoT-вузлів слід застосовувати легковагові, але криптографічно стійкі механізми, поєднані з контролем доступу, оновленнями та журналюванням.

Моніторинг мережевої активності є важливим, бо багато сенсорних і виконавчих вузлів мають передбачувані шаблони поведінки. Ознаками компрометації можуть бути різке збільшення з'єднань, звернення до невідомих адрес, зміна частоти передавання даних, нетипові команди або спроби автентифікації з невідомих джерел. З огляду на актуальні атаки на доступність, експлуатацію вразливостей і загрози даним моніторинг потрібно інтегрувати з реагуванням на інциденти [3].

Для підвищення стійкості слід застосовувати принцип мінімально необхідного доступу: пристрій взаємодіє лише з ресурсами, потрібними для його функцій, а адміністративні інтерфейси ізолюються від публічних мереж і захищаються багатофакторною автентифікацією. Європейський підхід до критичних суб'єктів акцентує безперервність функцій, урахування взаємозалежностей і здатність до відновлення після інцидентів [4].

Отже, мережева безпека IoT-пристроїв є базовою умовою надійності кіберфізичних систем розумного міста. Запропонований підхід охоплює автентифікацію, шифрування, сегментацію, моніторинг, журналювання та реагування. Подальші дослідження доцільно спрямувати на автоматизоване виявлення аномалій трафіку, адаптацію Zero Trust і моделі оцінювання ризиків для різних IoT-мереж.

1. Humayed A., Lin J., Li F., Luo B. Cyber-physical systems security - A survey. IEEE Internet of Things Journal. 2017. Vol. 4(6). P. 1802-1831.
2. Mosenia A., Jha N.K. A comprehensive study of security of Internet-of-Things. IEEE Transactions on Emerging Topics in Computing. 2017. Vol. 5(4). P. 586-602.
3. Khan M.A., Salah K. IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems. 2018. Vol. 82. P. 395-411.
4. Dritsas E., Trigka M. A survey on cybersecurity in IoT. Future Internet. 2025. Vol. 17(1). Article 30.

AI bots as a factor reducing the cyber resilience of virtual communities on social networking services

UDK 004.056:004.738.5(045)

Vadym Kolesnyk

Kharkiv National University of Radio Electronics, vadym.kolesnyk@nure.ua

The cyber resilience of virtual communities on social networking services is determined by their ability to maintain functionality, uphold trust among participants, ensure communicative continuity, adapt to disruptive influences, and recover from them. One factor reducing cyber resilience is AI bots, which can mimic human behavior, automatically generate messages, perpetuate specific narratives, provoke conflicts, and complicate the detection of coordinated inauthentic activity [1–2].

The urgency of the issue is heightened by the fact that AI is already considered one of the defining factors of the modern cyberthreat landscape. In particular, ENISA notes that AI is used to enhance social engineering, generate content, and increase the effectiveness of destructive campaigns [3]. In the case of virtual communities, the danger lies not only in the spread of misinformation but also in the gradual degradation of the socio-technical environment.

The goal is to identify sets of indicators that can be used to assess the impact of AI bots on the cyber resilience of virtual communities on social networking services.

Existing research has primarily focused on bot detection, disinformation analysis, automated moderation, network resilience, and the assessment of behavioral