УДК 004.056.7

В. І. Маліновський[1]
В.О. Олійник[1,2]
В.В.Ткаченко[1]

СУЧАСНІ ТЕНДЕНЦІЇ КІБЕРАТАК НА ПРИСТРОЇ ІНТЕРНЕТУ РЕЧЕЙ

[1]Вінницький національний технічний університет
[2]Маркетингова агенція NDA

Анотація

Розглянуто основні сучасні тенденції кібератак, які здійснюються на пристрої Інтернету речей і підходи та розвиток технік кіберзахисту від них. Відзначено актуальність кіберзахисту пристроїв Інтернету речей і необхідні дієві практики для їх кіберзахисту у сучасному і динамічному кіберпросторі. Описані основі підходи і техніки кібербезпеки IoT-пристроїв в сучасній інформаційній екосистемі Інтернету речей.

Ключові слова: Інтернет речей IoT, кібератака, кіберзагроза, кіберзахист МК, інформаційний та кіберзахист, вразливості.

Abstract

The basic current trends in field of cyberattacks, which carried out on Internet of Things devices and the approaches of cyberdefense techniques are considered. The are noted a relevance and actuality of cyberdefense of Internet of Things devices and also the necessary effective practices for their cyberdefense in modern and dynamic cyberspace where considered. The basic approaches and techniques of effective cybersecurity of IoT devices in the modern information ecosystem of the Internet of Thing (IoT)s are described.

Keywords: Internet of Things (IoT), cyberattack, MC cyberdefense, information and cyberdefense, vulnerabilities, cyberthreat, cyberdefense.

Вступ

Останнім часом поряд із розвитком інформаційних впливів та суттєвим зростанням загального числа кібератак і кіберзагроз у інформаційній глобальній мережі, поряд із подальншим достатньо стрімким розвитком інформаційних технологій, значно зростає загальний відсоток кібератак на пристрої Інтернету речей [1-7] та окремі їх локальні програмні додатки. Це призводить до витоків і втрат даних, до матеріальних і нематеріальних втрат власників цих пристроїв. Значний розвиток сучасних технологій програмних модулей і платформ для реалізації інформаційних впливів кіберзагроз на пристрої IoT призводить до значного збільшення числа активно впроваджених загроз на IoT[1-5].

Метою роботи є проведення базового аналізу і огляду сучасних векторів і тенденцій кіберзагроз і огляд основних практик захисту від кібератак в IoT-інфраструктурі, для покращення кіберзахисту та визначення потенційних подальших заходів захисту.

Проблема кібербезпеки Інтернету речей

Оцінка кіберзагроз і впливів по основним та вторинним каналам в IoT пристроях, розглянуті в роботах [1-8], дали можливість зрозуміти тенденціїі і основні напрями загрози для пристроїв Інтернету речей із метою подальшої оцінки факторів шкідливого впливу на інформаційні процеси в IoT і їх програмному забезпеченні.

Основні кібервтручання та інформаційні впливи здійснюються саме по інформаційно-комунікаційним каналам та зовнішнім інтерфейсам IoT (близько 30-45%). Інша частина – на вторинні елементи IoT, каналам (близько 2-7%), в т.ч. і по сервісним каналам. Інша. досить велика частка кіберзагроз здійснюється саме на програмне зебезпечення IoT (близько 45-55%), і невелике число інцидентів (близько 1-5%) відбувається по незалежним не прямим каналам або із використанням інших чинників.

Сучасні технології інформаційних систем і пристроїв IoT, в силу своєї анізотропності будови і чисельності задіяних програмних і апаратних технологій, створюють середовища із наявними

вразливостями і відкритими активними відкритими і доступними із зовні мережевими сокетами (IP-адреса та порт, наприклад, 192.168.1.1:8081) . Також, як показує практика і числені дослідження [1-5], в багатьох пристроях пристроях IoT відсутні проведені надійні специфічні налаштування безпеки, відмінні від заводських (default settings), що робить можливим активні впливи і дистанційне надсилання команд та взаємодію із такими пристроями Інтернету речей (IoT). Це, в сукупності, робить можливості провадження активних загроз на такі пристрої IoT. Наявність у їх складі мікроконтрролерів МК із архітектурою АРМ, зовнішньої флеш-пам'яті (Flash RAM) і програмного забезпечення (ПЗ) у вигляді додатків і системних модулів із розгалудженою і часто складною та не оптимізованою архітектурою, робить вразливим середовище IoT до різних типів кібератак і впоивів. Архітектура сучасних дадатків часто не враховує базові принципи кібербезпеки і побудови безпечних вебдодатків і WEB-технологій. Це створює можливості для дистанційного доступу у пристроях IoT, мережах та розгалуджених систем Інтернету речей (IoT) на основі таких пристроїв. Як зазначено у роботах [1, 2, 4] дуже гостро стоїть проблема кібербезпеки у пристроях IoT, які не мають механіщму регульяних і частих оновлень ПЗ і додатків, наприклад у IP-камерах. Це можлеве також за рахунок ряду додаткових причин:

- складності і “жорсткості” програмної архітектури ПЗ ;
- складності та відсутності гнучкості зв’язків застарілості мікропроцесорів в IoT ;
- складності контролю внутрішніх і зовнішніх інформаційних зв'язків в IoT(в т.ч. сервісних комунікацій IoT-пристрою із зовнішніми дата-сервісам виробника);
- складністю і важкістю контролю внутрішніх інформаційних комунікацій між IoT пристоями.
- недосконалостями налащтувань IoT пристроїв чи взагалі їх відсутністю ;
- недосконалістю архітекрути ПЗ додатків і системних мікропрограм IoT пристроїв;
- інших факторів, в т.ч. постійно зростаючих і еволюціонуючих технологій і інструментів здійснення кібератак на IoT-пристрої і їх інфраструктуру.

Тому, вирішення проблеми захисту від кібератак та зовнішніх інформаційних втручань по первинним і вторинним каналам на IoT надзвичано актуальне і вимагає нових підходів і ефективних практик захисту.

Основні тенденції кіберзагроз в IoT

Аналізуючи основні тенденції кібератак на IoT-пристрої і сектора Інтернету речей взагалі, можна відзначити основні із кіберзагроз, які найбільш активно і характерно впроваджуються в сучасних пристроях IoT і їх інфраструктурі:

- атаки на пам'ять IoT (зокрема на RAM, xSSD) із використанням нетривіальних методів доступу (xDNA) до різних ділянок пам'яті, в т.ч. із використання принципу переповнення буфера;
- атаки на комунікаційні Інтерфейси IoT (WiFi, 3/4/5G GSM, Bluethooth, RFID);
- атаки на програмны додатки IoT і окремий їх функціонал;
- використання атак із підміною (spoofing) ПЗ додатків IoT;
- DDoS та DoS - атаки на IoT пристрої та конкретні сокети(наприклад, 192.168.1.1:8081) ПЗ додатків IoT, в тому числі і з використанням засобів радіоелектронного впливу на інтерфейси IoT;
- атаки на системні мікропрограмні компоненти пршивки(firmware) IoT пристрої.
- MITM-атаки (Man in the Midle, людина посередині) та перехоплення сесій зв'язку (Session Hijacking);
- несанкціонований дистанційний доступ (НСД) до IoT-пристрою за допомогою RAT (Remote Adminoistration Trojan, троян дистанційцного доступу) і перезхоплення даних за допомогою ПЗ IoT: keyloger та stealler.
- інші загрози і загрози нульового, "0-го" дня - Zero Day Threat (ZDT), які завжди наявні.

Розробка ефективних підходів кіберзахисту IoT на нових принципах дозволить враховувати й компенсувати сумарні інформаційний впливи та кібератаки, та в оптимістичних прогнозах забезпечити повну нейтралізацію основних кіберзагроз в мікропроцесорних системах в складі як спеціалізованих і загальних систем управління.

Для захисту IoT на якісному рівні в сучасному середовищі та кіберпросторі, враховуючи широкий ландшафт кіберзагроз і поверхню кібератак, застосовують такі практики:

- використання спеціального модульного антивірусногом (AV IoT) захисту для IoT ;

- використання мережевого екранування для оточення і мережевого інформаційного периметру IoT-пристроїв;

- використання тунелювання і проміжних сервірів "proxy" для мережевого оточення IoT-пристроїв;

- використання постійного контролю дозволів і встановлення ПЗ додатків в пристроях IoT;

- використання контролю системних ресурсів і ПЗ застосунків, їх роботи в складі ОС IoT і у фоні , для зменшення і оптимізації ресурсів пристрою і програмного середовища ОС;

- використання контролю підключень і контролю усіх інтерфейсів в IoT пристрої;

- використанні контролю пам'яті і вмісту праграмного "сміття" в RAM та xSSD-пам'яті пристрою (в т.ч. і кеш-памті ПЗ додатків);

- використання зовнішніх проміжних технологій безпеки і захисту IoT-пристроїв(наприклад, End-Point Security продуктів та інших пристроїв IoT);

- інші прогресивні практики та інструменти.

Дуже складно і часто практично неможливо вирішити проблему кіберзахисту без нового релізу і апаратного перевипуску (нового виготовлення) нової архітектури пристрою IoT чи без оновлення ПЗ додатку із оптимізованою та закритою вразливістю CVE .

Основна проблема кібербезпеки IoT вимагає комплексності, організованості і складності в підборі і використанніпрактик захисту. За допомогою якоїсь одної практики не можливо забезпечити кібербезпеку IoT. Аналогічно, неможливо усунути основні вразливості в ПЗ додатку і апаратній структурі IoT без їх оновлень або перевиготовлення. Також, дуже часто виникають та тривалий час існують “сліпі зони” безпеки і приховані вразливості CVE в IoT-пристроях і системах, які неможливо швидко виправити шляхом базових оновлення коду програмних засобів. Є основні характерні вразливості CVE для мікроконтролерів і пам'яті в складі IoT, які роблять можливими кібератакм на пам’ять та інтерфейси, а самі принципи реалізації кіберзагрози лежать в площині системних команд мікропроцесорів IoT на рівні порядку виконання машинних інструкцій, та є критичними.

Висновки

Більшість класичних методів і засобів кібербезпеки для класичних інформаційних компютерних систем і багатофункціональних інформаційних (IT) пристроїв із оперативних систем (ОС) неможливо застосувати безпосередньо на рівні архітектури самого IoT в т.ч. окремих пристроїв і схем на базі МК, в силу відсутності достатньої гнучкості ОС і ПЗ для окремих IoT. В оригінальних дослідженнях визначено, що більшість із методів кібербезпеки вимагають окремих апаратних засобів забезпечення кібербезпеки для IoT чи додаткових спеціальних методів і підходів захисту (наприклад, використання End-point Security Architecture), що не завжди є раціональним та економічно обгрунтованим для окремих IoT пристроїв і досить часто є достатньо дороговартісним для впровадження захисту для локальних IoT систем і пристроїв.

Реалізація кіберзахисту IoT на практиці є не простою і тривіальною задачею. Те, що легко аналізується і обчислюється теоретично, на практиці має зовсім інші рівні складності при впровадженні. Досягнення дієвого, ефективного та релевантного кіберзахисту для IoT пристроїв і систем досить складно практично реалізувати, враховуючи широкий ландшафт та різноманітність сучасних кіберзагроз, в т.ч. із боку мережі Інтернет, до якої ці пристрої часто підключаються. Але досягти прийнятного високого рівня кіберзахисту IoT можно при використанні комплексних принципів і підходів кіберзахисту в екосистемі IoT.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1.Маліновський В.І. Сучасні кіберзагрози і захист даних в системах і пристроях Internety речей // Матеріали Міжнародної наукової Internet-конференції "Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення" (випуск 69), 4-5 липня 2022. URL: http://www.konferenciaonline.org.ua/ua/article/id-595/ (Дата звернення 24.02.2026).

2. N. J. Singh, N. Hoque, K. R. Singh, and D. K. Bhattacharyya, ‘‘Botnetbased IoT network traffic analysis using deep learning,’’ Secur. Privacy, vol. 7, no. 2, p. 355, Mar. 2024, doi: 10.1002/spy2.355.

3. B. I. Mukhtar, M. S. Elsayed, A. D. Jurcut, and M. A. Azer, ‘‘IoT vulnerabilities and attacks: SILEX malware case study,’’ Symmetry, vol. 15, no. 11, p. 1978, Oct. 2023, doi: 10.3390/sym15111978.

4. B. Sutheekshan, S. Basheer, G. Thangavel, and O. P. Sharma, ‘‘Evolution of malware targeting IoT devices and botnet formation,’’ in Proc. IEEE Int. Conf. Comput., Power Commun. Technol. (IC2PCT), Feb. 2024,

5. Securing the IoT Cyber Environment: Enhancing Intrusion Anomaly Detection With Vision Transformers LARAIB SANA, MUHAMMAD MOHSIN NAZIR,JING YANG,YEN-LIN CHEN,CHIN SOON KU,MOHAMMED ALATIYYAH, SULAIMAN ABDULLAH ALATEYAH, LIP YEE POR . IEEE ACCess, Vol. 12, 2024, 24.05.2024, doi: 10.1109/ACCESS.2024.3404778 URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10538333 (Дата звернення 24.02.2026).

6.Dawit Dejene Bikila, Jan Čapek . Machine Learning-Based Attack Detection for the Internet of Things. Future Generation Computer Systems, Volume 166, May 2025, 107630, https://doi.org/10.1016/j.future.2024.107630 URL: https://www.sciencedirect.com/science/article/abs/pii/S0167739X24005946 (Дата звернення 24.02.2026).

7. S. M. Taghavinejad, M. Taghavinejad, L. Shahmiri, M. Zavvar, and M. H. Zavvar, ‘‘Intrusion detection in IoT-based smart grid using hybrid decision tree,’’ in Proc. 6th Int. Conf. Web Res. (ICWR), Apr. 2020, pp. 152–156, doi: 10.1109/ICWR49608.2020.9122320.

8.G. Fortino, C. Savaglio, G. Spezzano, and M. Zhou, “Internet of Things as system of systems: A review of methodologies, frameworks, platforms, and tools,” IEEE Trans. Syst., Man, Cybern. Syst., vol. 51, no. 1, pp. 223–236, Jan.2021.

9. A. Čolaković and M. Hadžialić, “Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues,” Comput. Netw., vol. 144, pp. 17–39, 2018.

10."Security Onion Control Scripts". Applied Network Security Monitoring. Elsevier. 2014. pp. 451–456. doi:10.1016/b978-0-12-417208-1.09986-4. ISBN 978-0-12-417208-1. Retrieved 2021-05-29.

11. Шологон Ю. З. Вразливості апаратного забезпечення кіберфізичних систем./ Репозитарій Національного університету «Львівська політехніка» (Lviv Polytechnic National University Institutional Repository). - t12. с. - 2023. [Електронний ресурс]. - Режим доступу URL: http://ena.lp.edu.u. (Дата звернення 24.02.2026).

12. Dependability and Security Internet of Things: Practicum /V. V. Sklyar, V. V. Yatskiv, N. G. Yatskiv // Ministry of Education and Science of Ukraine. - National Aerospace University “KhAI”, Ternopil Na-tional Economic University. - 2019. - 98p.

Маліновський Вадим Ігоревич — канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м.Вінниця, Україна.

Олійник Володимир Олегович — студент кафедри захисту інформації, Вінницький національний технічний університет, Факультет інформаційних технологій та комп’ютерної інженерії, гр.2БС-22, Маркетингова агенція NDA, м.Вінниця, Україна.

Ткаченко Владислав Вікторович — студент кафедри захисту інформації, Вінницький національний технічний університет, Факультет інформаційних технологій та комп’ютерної інженерії, гр.2БС-22, м.Вінниця, Україна.

Malinovskyi Vadym — PhD, associate professor, Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, Ukraine.

Oliynyk Volodymyr Olegovych — student, Department of Information Protection, Vinnytsia National Technical University, Facility of Information Technologies and Computer Engineering, gr.2BS-22, NDA Marketing Agency, Vinnytsia, Ukraine.

Tkachenko Vladyslav Viktorovych — student, Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, Ukraine.