УДК 621.9

ЗАГРОЗИ ТА ВРАЗЛИВОСТІ СИСТЕМ ІНТЕРНЕТУ РЕЧЕЙ У КІБЕРПРОСТОРІ

Григоренко О.Г., Сачек Р.В.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: olenagri@ukr.net, srv300333@gmail.com

THREATS AND VULNERABILITIES OF INTERNET OF THINGS SYSTEMS IN CYBERSPACE

The main threats, vulnerabilities, and attacks in Internet of Things networks have been analyzed, which allows for timely application of countermeasures and safe use of IoT in cyberspace.

Проаналізовані основні загрози, вразливості, атаки в мережах Інтернету речей, що дозволяє вчасно застосувати заходи протидії і безпечно використовувати IoT у кіберпросторі.

Інтернет речей безсумнівно є сьогодні одним з головних компонентів науково-технічного прогресу. Кількість пристроїв невпинно зростає (рис.1) і ця тенденція зберігатиметься і надалі [1,3]. За визначенням компанії Gartner: “Інтернет речей (IoT) — це мережа фізичних об’єктів, які містять вбудовану технологію для спілкування та сприйняття або взаємодії з їхнім внутрішнім станом або зовнішнім середовищем” [4]. Тобто, це екосистема пристроїв і технологій, підключених через Інтернет, які постійно збирають і передають дані. Часто такі пристрої називають «смарт» або «розумний».

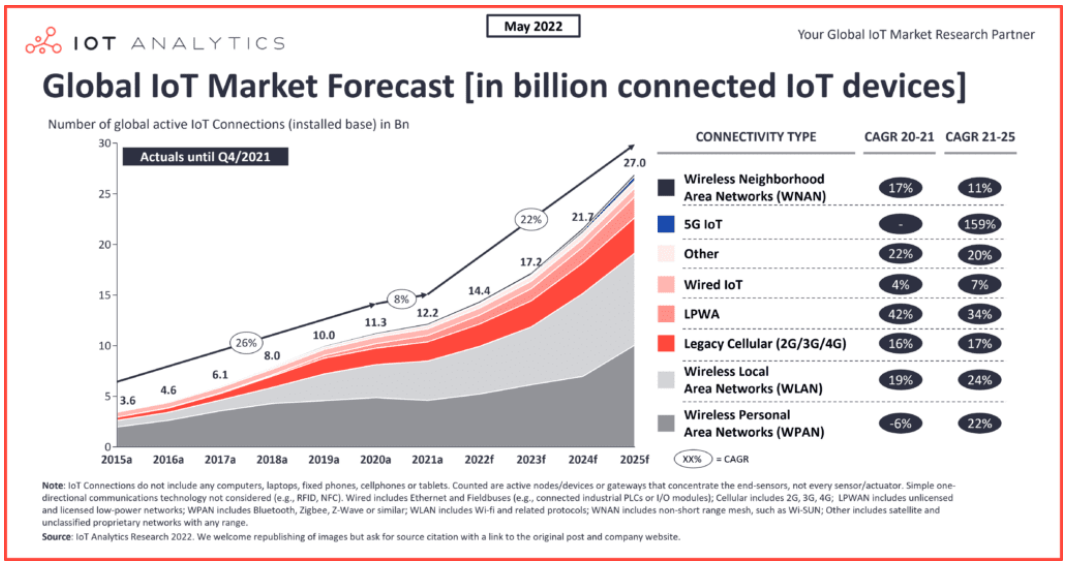

Рис.1. Тенденція розвитку IoT(в мільярдах підключених пристроїв IoT) [1].

IoT є дуже зручним та корисним набором технологій, що значно спрощує як повсякденне життя людини, так і роботу організацій. Проте, пристрої і мережі IoT мають вразливості, які важко вчасно визначати. Також IoT мережі – це екосистема речей, де нікому відслідковувати нетипову ситуацію і віруси. Кожен пристрій IoT є потенційно вразливою точкою входу в мережу та бізнес-процеси.

Тому такі мережі можуть стати (і стають) першим етапом більших зламів, особливо якщо атака таргетована саме на конкретну організацію. Зважаючи на це, кібербезпека пристроїв Інтернету речей стає все більш критичним питанням, оскільки кількість пристроїв, які можуть отримувати та надсилати конфіденційні дані, щоденно росте. Тож впровадження й оновлення заходів безпеки пристроїв має стати пріоритетом на найближчі роки для технології IoT [1].

Найпоширенішими атаками на пристрої Інтернету речей (IoT) є [1,2,5]:

DDoS-атаки (Distributed Denial of Service) – Хакери використовують зламані IoT-пристрої для створення ботнетів (наприклад, Mirai) і перевантажують сервери жертви трафіком.

Brute-force атаки на паролі – Багато IoT-пристроїв мають слабкі або стандартні паролі (типу "admin/admin"), які зловмисники легко підбирають.

Атаки через незахищені API – Якщо IoT-пристрій взаємодіє з сервером через API без належної автентифікації або шифрування, хакери можуть отримати контроль над ним.

MITM-атака (Man-in-the-Middle) – Перехоплення незашифрованих даних між IoT-пристроєм і сервером, що дозволяє змінювати або викрадати інформацію.

Фізичний злам пристрою – Якщо хакер отримує фізичний доступ до пристрою, він може витягнути дані з пам’яті, підключитися до управляючих портів (наприклад, JTAG, UART) або змінити мікропрограму (firmware).

Атака на оновлення прошивки – Якщо пристрій оновлюється без перевірки цифрового підпису, зловмисники можуть підсунути шкідливе програмне забезпечення (ПЗ).

Перехоплення та підміна радіосигналів – Наприклад, атаки на Wi-Fi, Zigbee, Bluetooth, RFID, LoRaWAN, коли хакери перехоплюють або модифікують передані дані.

Експлуатація вразливостей у ПЗ – Використання дефектів у прошивці або операційній системі IoT-пристрою для виконання шкідливого коду або отримання доступу до системи.

Зловживання стандартними сервісами (MQTT, CoAP, UPnP) – Деякі IoT-протоколи не мають шифрування за замовчуванням, що дає змогу хакерам шпигувати або підробляти команди.

Атаки на блокчейн у IoT – Якщо IoT-пристрій використовує блокчейн для збереження даних, можливі атаки на смарт-контракти або мережу (наприклад, 51% атака).

Захист пристроїв Інтернету речей є життєво важливим компонентом безпеки сучасної мережі в організаціях. Одним із засобів захисту від різного роду атак є процес аутентифікації в мережі.

Ризики IoT легко не помітити, якщо не використовувати призначені для цього інструменти. Іноді співробітники з інформаційної безпеки нехтують інвентаризацією кінцевих точок, через це легко можна пропустити потенційно вразливий до атак пристрій. Сьогодні існують програмні продукти для проведення інвентаризації та моніторингу всіх підключених IoT пристроїв.

Такий тип рішень з безпеки значно знижує ризики, аналізуючи потенційні атаки.

Різноманітність пристроїв IoT у поєднанні з їх широким розгортанням у критичних секторах, потребує багатогранного підходу до безпеки, який виходить за рамки традиційних заходів. Удосконалення методів шифрування, алгоритмів збереження конфіденційності, виявлення аномалій за допомогою штучного інтелекту представляють важливі кроки в забезпеченні безпеки середовищ IoT [5,6].

Також необхідно застосовувати цілісні наскрізні структури кібербезпеки, які можна легко інтегрувати в життєвий цикл IoT — від проєктування мережі, виробництва та розгортання пристроїв до поточної експлуатації та виведення з неї. Відсутність стандартизованих протоколів безпеки та інфраструктури в різних екосистемах Інтернету речей є значною перешкодою для досягнення надійної безпеки, що призводить до непослідовних положень безпеки на різних пристроях і мережах, створюючи вразливості, які можуть бути використані зловмисниками. Майбутні дослідження мають надавати пріоритет розробці сумісних і масштабованих інфраструктур безпеки, які можна адаптувати до різноманітних пристроїв IoT [5].

Однією з перспектив є інтеграція штучного інтелекту та машинного навчання в кібербезпеку [5,6]. Тому важливим є розробка стійких моделей ШІ, які можуть протистояти різним атакам, а також необхідність постійного моніторингу та оновлення цих моделей, щоб не відставати від нових загроз.

З вищезазначених векторів атак на IoT можна зробити висновок, що основні компоненти систем Інтернету речей є досить вразливими до атак зловмисників, тому безпека IoT повинна розглядатися ще на етапі проектування, щоб покращити її інтегрування.

Література

1. Д.Діденко. Поширені атаки на IoT та захист від них. / [Електронний ресурс] – Режим доступу: https://corewin.ua/blog/attacks-on-iot-how-protect/
2. Kupershtein L., Malinovskyi V., Kaplun V. CYBER SECURITY OF MOBILE DEVICES AND INTERNET OF THINGS / КІБЕРБЕЗПЕКА МОБІЛЬНИХ ПРИСТРОЇВ ТА ІНТЕРНЕТУ РЕЧЕЙ.-2024/ [Електронний ресурс] – Режим доступу: https://www.researchgate.net/publication/379257182_CYBER_SECURITY_OF_MOBILE_DEVICES_AND_INTERNET_OF_THINGS_KIBERBEZPEKA_MOBILNIH_PRISTROIV_TA_INTERNETU_RECEJ
3. IoT-analytics/ [Електронний ресурс] – Режим доступу:https://iot-analytics.com/
4. Gartner:/ [Електронний ресурс] – Режим доступу:https://www.gartner.com/en/information-technology/glossary/internet-of-things
5. E.Dritsas, M.Trigka. A Survey on Cybersecurity in IoT. – Future Internet 2025, 17(1), 30 / [Електронний ресурс] – Режим доступу: https://www.mdpi.com/1999-5903/17/1/30
6. M.Aziz Al Kabira, W.Elmedanya, M.Saeed Sharif. Securing IoT Devices Against Emerging Security Threats:Challenges and Mitigation Techniques. – JOURNAL OF CYBER SECURITY TECHNOLOGY. – 2023, VOL. 7, NO. 4, 199–223 / [Електронний ресурс] – Режим доступу: https://www.tandfonline.com/doi/epdf/10.1080/23742917.2023.2228053?needAccess=true