УДК 004.056:004.77
DOI: 10.31673/2412-9070.2024.046569
О. В. ЖИДКА[1], аспірант,
ORCID: 0009-0009-4272-9071;
Т. Р. АНДРІЙЧЕНКО[2], викладач,
ORCID: 0009-0009-4145-3915,
[1] Державний університет інформаційно-комунікаційних технологій, Київ
[2] Київський фаховий коледж зв'язку

ІНФОРМАЦІЙНА БЕЗПЕКА СИСТЕМ IoT

Немає сумніву, що концепція Інтернету речей (IoT) продовжує швидко розвиватися, спричинюючи швидке поширення передових технологій IoT. Парадигма мереж впливає на всі сфери життя, від автоматизованих будинків до систем розумного здоров'я та моніторингу навколишнього середовища, інтегруючи інтелект у всі аспекти оточення світу. Впровадження IoT вимагає значних зусиль та сучасних рішень з питань забезпечення безпеки та конфіденційності.

Багато дослідників по всьому світу займаються проблемами безпеки в Інтернеті речей на сьогоднішній день, особливо через ряд проблем, що виникають при експлуатації IoT пристроїв. У статті розглядаються питання забезпечення доступу до захищених мереж IoT пристроїв. Існування великої кількості недостатньо захищених пристроїв сприяє проведенню DDoS-атак, під час яких побутові пристрої можуть бути використані для нападу на корпоративні системи. Також розглянуті деякі можливі загрози безпеці систем IoT. На основі аналізу технологій найпоширеніших атак було розроблено перелік рекомендацій для забезпечення цілісності мережі з пристроями IoT.

Ключові слова: Інтернет речей; мережа; передавання даних; інформаційна безпека; кібератака; кібербезпека; DDoS-атака.

Вступ

На сьогоднішній день системи інтелектуального керування широко використовуються у всіх галузях людського життя, від побутових ситуацій до промисловості. Це призвело до значного збільшення обсягу інформації, яка циркулює в мережах передавання даних. Проте, такий розвиток систем керування часто відбувається без загальної стандартизації, і розробники зазвичай не надають належної уваги методам та засобам захисту. Інформаційні системи Інтернету речей все ще мають багато недоліків, навіть при високій популярності та використанні сучасних технологій при їх створенні.

Оскільки в системах Інтернету речей використовуються пристрої, які постійно збирають та обробляють дані про оточуюче середовище, вони стають потенційно небезпечними для кінцевих користувачів. З урахуванням зростання рівня кіберзлочинності, особлива увага повинна бути приділена саме цим пристроям, оскільки загроза не обмежується лише втратою даних, а може також включати в себе використання обчислювальних ресурсів систем для здійснення різноманітних кібератак [2].

Серед недоліків таких систем можна відзначити необхідність використання сучасних датчиків, контролерів, а також методів та засобів передавання інформації. Тому, впровадження пристроїв Інтернету речей та вирішення найбільш поширених проблем, пов'язаних з ними, є актуальним напрямком досліджень.

Аналіз останніх досліджень. Інтернет речей змінює спосіб життя, дозволяючи підключати та керувати різноманітними пристроями — від смартфонів і ноутбуків до побутової техніки та промислового обладнання — через єдину мережу. Однак із зростанням кількості підключених пристроїв збільшуються й проблеми безпеки. Далі будуть оглянуті основні проблеми безпеки та можливі рішення для IoT, які можуть допомогти в їх вирішенні [3]. Мета дослідження полягає в аналізі поточного ландшафту загроз, які є актуальними для IoT-пристроїв у 2023 році, а також вивченні можливих рішень для IoT, що допоможуть уникнути цих загроз. Використання різноманітних пристроїв ускладнює боротьбу з кіберзагрозами через складність архітектури Інтернету речей. Тому, необхідно провести аналіз і розробити ефективні заходи забезпечення безпеки, щоб користувачі могли повністю довіряти цій технології.

Основна частина

Кількість IoT-пристроїв — роутерів, камер, NAS-сховищ, компонентів «розумного будинку» зростає з кожним роком. Прогнозується, що до 2025 року загальна кількість встановлених розумних пристроїв досягне позначки 30,9 млрд (рис. 1) [4]. Із збільшенням кількості підключених пристроїв зростає і необхідність їх захисту. Перші масові атаки на IoT-пристрої з використанням шкідливого програмного забезпечення були зафіксовані ще у 2008 році, а з тих пір подібних атак стає тільки більше.

Для запобігання атакам на пристрої Інтернету речей важливо з'ясувати різноманітні види атак, які можуть бути використані кіберзлочинцями.

1. Одним з таких видів атак є DDoS-атака. DDoS-атаки (атаки з відмовою в обслуговуванні) є

© О. В. Жидка, Т. Р. Андрійченко, 2024

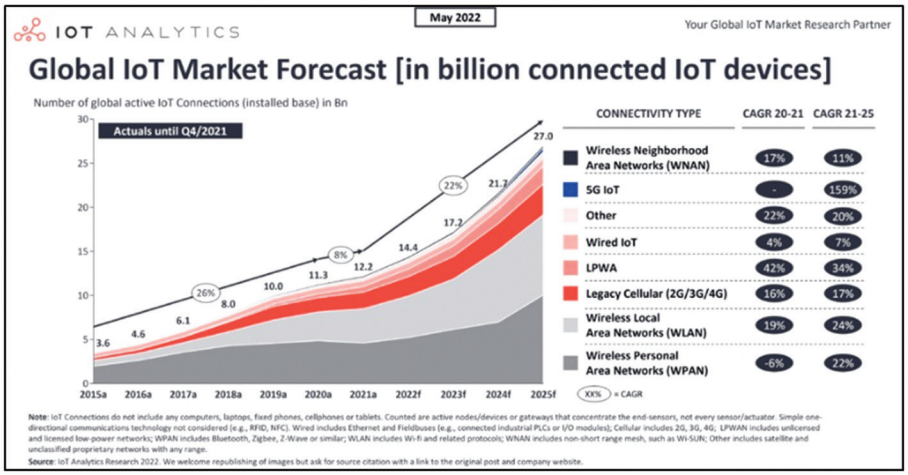

Рис. 1. Прогноз глобального ринку IoT (в млрд підключених пристроїв IoT)

серйозною загрозою для пристроїв IoT. У цих атаках ботнет, що складається з компрометованих пристроїв, надсилає велику кількість запитів до цільової системи або мережі, намагаючись перевантажити їхні ресурси. Через велику кількість запитів, які надходять від ботнету, мережа або цільова система може перевантажитися, що призводить до зниження її продуктивності або навіть до повного зупинення роботи. Вдало налаштована DDoS-атака може призвести до виникнення системних помилок або вразливостей безпеки, які можуть бути використані для отримання несанкціонованого доступу до системи. Кіберзлочинці можуть скомпрометувати пристрої IoT та використовувати їх для створення ботнету, який буде виконувати DDoS-атаки. Це особливо небезпечно, оскільки пристрої IoT можуть бути менш захищеними та менш виявленими для користувачів. Зловмисники можуть використовувати компрометовані пристрої IoT для внутрішніх атак у локальній мережі. Це може призвести до порушення безпеки всієї мережі та втрати конфіденційної інформації.

Усього за першу половину 2023 року аналітики виявили понад 700 оголошень про послуги з проведення DDoS-атак на різних форумах у даркнеті (рис. 2) [5] .

2. Експлойти програмного забезпечення є серйозною загрозою для пристроїв IoT та можуть призвести до небезпечних наслідків. Кіберзлочинці можуть використовувати відомі вразливості у програмній частині пристроїв для здійснення атак. Це може включати в себе відкриті порти, недоліки в аутентифікації, неадекватні обмеження доступу, тощо. Не всі виробники пристроїв IoT завантажують оновлення програмного забезпечення вчасно. Це робить пристрої вразливими до атак, оскільки зловмисники можуть використовувати вразливості, які були виправлені у нових версіях програмного забезпечення. Не всі виробники надають достатню інформацію користувачам щодо програмного забезпечення, яке використовується в їхніх пристроях. Це може ускладнювати процес виявлення та усунення вразливостей, оскільки користувачі можуть бути несвідомі щодо потенційних загроз безпеці [6].

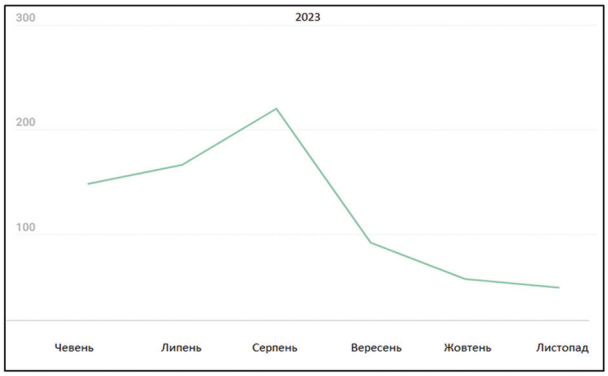

Рис. 2. Розподіл кількості публікацій, пов'язаних із послугами з проведення DDoS-атак

3. MITM-атака (Man-in-the-Middle attack) або атака посередника є однією з найбільш хитрих та широко використовуваних методів кібератак. Вона полягає в тому, що зловмисник вставляється між сторонами, які спілкуються, що зазвичай є пристроєм відправника та пристроєм отримувача, та перехоплює і маніпулює комунікаційним потоком. Зловмисники можуть змінювати дані під час їх передавання між пристроями. Це дозволяє їм впливати на поведінку пристроїв та маніпулювати результатами комунікації. Багато смарт-пристроїв часто не зашифровані, що робить їх особливо вразливими до MITM-атак. З отриманими даними зловмисники можуть отримати несанкціонований доступ до систем, пристроїв або мереж, що може призвести до витоку чутливої інформації або виконання небажаних дій [7].

4. Фізичне втручання: просте підключення кіберзлочинцем USB-флешки із шкідливим кодом до зовнішнього пристрою IoT може бути достатнім, щоб розповсюдити зловмисне програмне забезпечення через мережу та шпигувати за комунікаціями, що проходять у ній.

5. Брутфорс-атаки: факт того, що в компаніях зазвичай не приділяється достатньо уваги парольній безпеці пристроїв IoT, що робить їх вразливими до потенційних атак методом грубої сили або «Брутфорс». Часто паролі пристроїв IoT залишаються незмінними після встановлення, що дозволяє зловмисникам легко їх підібрати.

За першу половину 2023 року 97,91% спроб перебору паролів, зафіксованих ханіпотами, були пов'язані з протоколом Telnet та 2,09% — із SSH. Найбільше інфікованих пристроїв, які здійснювали ці атаки, перебували у Китаї, Індії та США (рис. 3), а за кількістю атак лідирують Китай та Пакистан [8].

Рис. 3. ТОР-10 країн та територій, в яких знаходилася більшість пристроїв, атакувавших ханіпоти

6. Викрадення прошивки є серйозною загрозою для безпеки пристроїв IoT. Прошивка, яка контролює роботу пристрою, може містити критичні дані та налаштування, а також бути ключовим елементом захисту. Зловмисники можуть використовувати вкрадену прошивку для отримання контролю над пристроєм. Це може включати в себе виконання шкідливих команд або встановлення додаткового шкідливого програмного забезпечення. Якщо викрадена прошивка містить конфіденційні дані, такі як облікові записи або ключі шифрування, зловмисники можуть отримати доступ до цих даних і використовувати їх у своїх цілях, включаючи витік конфіденційної інформації. Зловмисники можуть модифікувати викрадену прошивку, щоб вона містила шкідливе програмне забезпечення. Після цього вони можуть поширювати це програмне забезпечення на інші пристрої, що працюють на тій же або подібній прошивці [9].

Обговорення результатів проведеного дослідження

З вищезазначених векторів атак на IoT можна зробити висновок, що основні компоненти систем Інтернету речей є досить вразливими до атак зловмисників. Незалежно від масштабу та типу середовища, у яке вбудовується система IoT, безпека повинна розглядатися ще на етапі проєктування, щоб покращити її інтегрування. Особливим викликом для інженерів та офіцерів інформаційної безпеки є те, що через технологічні особливості IoT не дозволяється встановити агента для перевірки наявності заражень або вразливостей.

Провівши аналіз відкритих джерел, можна надати кілька основних рекомендацій, щоб запобігти кібератакам на пристрої та загалом зменшити ризики безпеки компанії.

1. *Управління поверхнею атаки, інвентаризація та моніторинг усіх пристроїв.* Під час планування захисту IoT однією з головних задач має бути створення карти підключених пристроїв для їх інвентаризації. Команди безпеки повинні знати точну кількість пристроїв, що використовуються, а також ідентифікатори виробників, серійні номери, версії обладнання та прошивки. Моніторинг, аналіз та звітність в режимі реального часу є вкрай важливими для організацій, щоб мати можливість керувати ризиками Інтернету речей. Проте, традиційні рішення безпеки кінцевих точок зазвичай використовують технологію так званих програмних агентів, які не підходять для пристроїв IoT. На щастя, існують кращі сучасні підходи — безагентні рішення (наприклад DeviceTotal) моніторингу поверхні атаки. Вони забезпечують оцінку рівня ризику в режимі реального часу, неперервно аналізуючи поведінку і стан всіх підключених пристроїв Інтернету речей. Деякі рішення такого плану навіть дозволяють керувати поверхнею прекогнітивних атак, враховуючи ризики потенційних «атак нульового дня». Ці інструменти безпеки дають можливість організаціям використовувати всі переваги технології IoT, виправивши її основний недолік — недостатній рівень безпеки [10].

2. *Сегментація мережі.* У разі успішної кібератаки зловмисник може отримати доступ до всієї мережі організації. Сегментація запобігає цьому, обмежуючи поверхню атаки та мінімізуючи збитки. Сегментація мережі — це процес поділу внутрішньої мережі на кілька окремих підмереж. Хоча сегменти можуть час від часу спілкуватися між собою, зазвичай вони незалежні та ізольовані один від одного. Цей метод дає змогу зосереджувати більше уваги на окремих частинах мережі, які місять найбільш критичні дані, для їх посиленого захисту.

3. *Встановлення надійних паролів для IoT.* Багато пристроїв IoT постачаються зі слабкими попередньо встановленими паролями, які дуже легко підібрати. Як тільки IoT-пристрій вперше реєструється в мережі, для початку, найкращою методикою буде змінити його попередньо встановлений пароль на значно складніший. Новий пароль має бути стійким для підбору, унікальним

для кожного захищеного пристрою та відповідати політикам керування паролями нашої команди з безпеки ІТ.

4. ***Захист всіх пристроїв IoT на фізичному рівні.*** Фізичний захист пристроїв має дуже велике значення, оскільки пристрої, що доступні ззовні, можуть піддатися фізичному втручанню зловмисників з метою отримання несанкціонованого доступу або завантаження в систему шкідливого програмного забезпечення. Тому, слід забезпечити надійне розташування пристрою, щоб до нього не мали відкритого доступу.

5. ***Своєчасні оновлення прошивок.*** Нові версії прошивок можуть містити виправлення наявних програмних вразливостей пристрою. Саме тому їх регулярне оновлення значно покращить загальну безпеку IoT. Проте, оновлення також слід перевіряти на підробки, оскільки зловмисники можуть під виглядом оновлення завантажити на пристрій шкідливе програмне забезпечення. Інша сторона оновлень — це вразливості в офіційних оновленнях. Потрібно контролювати версійність і тримати найновішу з безпечних версій прошивки, в цьому допоможуть автоматизовані системи аналізу прошивки пристроїв.

Висновки

Інтернет речей приносить багато переваг, але також створює низку проблем безпеки. Ці виклики включають вразливість пристроїв, проблеми з конфіденційністю даних і незахищеність мережі.

Для вирішення цих проблем можна звернутися до компанії, яка розробляє додатки для Інтернету речей. Вони можуть впровадити надійні заходи безпеки, такі як аутентифікація пристрою, шифрування та регулярні оновлення програмного забезпечення.

Крім того, пристрої IoT слід розробляти з урахуванням безпеки з самого початку, а компанії повинні мати чітку та прозору політику конфіденційності даних. Розробники додатків IoT можуть забезпечити безпеку пристроїв і даних, які вони збирають і передають.

Виконання наведених вище рекомендацій допоможе безпечно користуватися пристроями IoT, використовуючи їх користь на повну та при цьому мінімізуючи ризики. Проте, слід пам'ятати, що кібератаки постійно розвиваються, тому важливо бути в курсі нових подій в кіберпросторі та регулярно оновлювати заходи безпеки, використовуючи сучасні передові рішення для забезпечення моніторингу пристроїв та аналізу поверхні атаки.

Список використаної літератури

1. ***Поширені*** *атаки на IoT та захист від них // електрон. текст. дані URL:*
https://corewin.ua/blog/attacks-on-iot-how-protect/
2. ***Безагентне*** *управління вразливостями для IoT та OT // електрон. текст. дані URL:*
https://corewin.ua/blog/agentless-vulnerability-management-for-iot-and-ot/
3. ***11 Biggest*** *security challenges & solutions for IoT// електрон. текст. дані URL:*
https://www.peerbits.com/blog/biggest-iot-security-challenges.html
4. *IoT Explained — How Does an IoT System Actually Work? // електрон. текст. дані URL:*
https://medium.com/iotforall/iot-explained-how-does-an-iot-systemactually-work-e90e2c435fe7
5. ***A Survey*** *on Sensor-based Threats to Internet-of-Things (IoT) Devices and Applications // електрон. текст. дані URL:*
https://arxiv.org/pdf/1802.02041.pdf
6. ***The*** *advantages and disadvantages of Internet Of Things // електрон. текст. дані URL:*
https://e27.co/advantages-disadvantages-internet-things-20160615/
7. ***IoT*** *security guide // електрон. текст. дані URL:*
https://www.dsci.in/files/content/knowledge-centre/2023/IoT-Security-Guide.pd
8. ***Gloukhovtsev,*** *IoT_Security_Challenges_Solutions_and_Future_Prospects // електрон. текст. дані URL:*
https://education.dell.com/content/dam/dell.documents/en-us/2018KS_ Gloukhovtsev -IoT Security_Challenges_Solutions_and_Future_ Prospects.pdf
9. ***IoT****-Security-Challenges-and-Best-Practices // електрон. текст. дані URL:*
https: //www happiestminds.com/wp-content/uploads/2020/12/IoT-Security-Challenges-and-Best-Practices.pdf
10. ***IMDA*** *IoT Cyber Security Guide Version 1, Jan 2019 // електрон. текст. дані URL:*
https://www.imda.gov.sg/-/media/imda/files/regulation-licensing and consultations/consultations/ open-for-public-comments/imda-iot-cyber-security -guide.pdf

O. Zhydka, T. Andriichenko

INFORMATION SECURITY OF IoT SYSTEMS

There is no doubt that the concept of the Internet of Things (IoT) continues to develop rapidly, causing the rapid adoption of advanced IoT technologies. The networking paradigm affects all areas of life, from automated homes to smart health systems and environmental monitoring, integrating intelligence into all aspects of the world's environment. The implementation of IoT requires significant efforts and modern security and privacy solutions.

To date, intelligent control systems have become quite widespread in all spheres of human life, from household to industry. Considering this, the volume of information in data transmission networks is also increasing. At the same time, such management systems are developing rather chaotically and do not have general standardization, and their developers do not yet pay much attention to methods and methods of protection. Information systems such as IoT still have a large number of disadvantages, despite the high popularity and use of modern technologies in development.

Since the Internet of Things includes devices that constantly collect and process information about the environment, they are potentially dangerous for the end user. Given the growing level of cybercrime, special attention should be paid to such devices, because not only data loss is the main problem. It is also possible to use computing resources of systems in the design of various cyber attacks.

The disadvantages of these systems are the need for modern sensors, controllers, methods and methods of information transmission, etc. Therefore, the introduction of IoT devices and the solution of the most common tasks and problems related to them is a very relevant area of research.

Many researchers around the world are dealing with security issues in the Internet of Things today, especially due to a number of problems that arise in the operation of IoT devices. The article discusses issues of providing access to secure networks of IoT devices. The existence of a large number of poorly protected devices facilitates DDoS attacks, in which household devices can be used to attack corporate systems. Some possible threats to the security of IoT systems are also considered. Based on the analysis of the most common attack technologies, a list of recommendations was developed to ensure the integrity of the network with IoT devices [1].

Keywords: IoT; Internet of Things; network; data transfer; technology; information security; cyber attack; cyber security.