УДК 681.281

А.А. Краєвська

АНАЛІЗ ТЕХНОЛОГІЙ БЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ

Вінницький національний технічний університет

Анотація

В роботі розглянуті технології сучасного Інтернету речей, які дозволяють змінювати і покращувати різні сфери життя, забезпечуючи зручність, комфорт, ефективність, автоматизацію та економію ресурсів та різних процесів. Водночас технології IoT створюють нові виклики у сфері кібербезпеки, зокрема ризики витоку даних.

Ключові слова: Інтернет речей, IoT, кібербезпека, кібератаки, автоматизація, технології, інновації, особисті дані.

Abstract

The paper examines the technologies of the modern Internet of Things, which allow changing and improving various areas of life, providing convenience, comfort, efficiency, automation and saving of resources and various processes. At the same time, IoT technologies create new challenges in the field of cybersecurity, in particular, the risks of data leakage.

Keywords: Internet of Things, IoT, cybersecurity, cyberattacks, automation, technology, innovation, personal data.

Вступ

Інтернет речей (IoT) трансформує різні сфери життя, забезпечуючи зручність, автоматизацію та економію ресурсів. Водночас IoT створює нові виклики у сфері кібербезпеки, зокрема ризики витоку даних. Для безпечного використання IoT важливий розвиток захисних технологій та стандартів IoT, в тому числі для забезпечення кібербезпеки пристроїв і систем Інтернету речей.

Інтернет речей (IoT, Internet of Things)– це концепція мережевої інфраструктури, що полягає в об'єднанні фізичних об'єктів між собою за допомогою мереж. Збір інформації, обробка та аналіз відбуваються в цифровому світі автоматично. Основні елементи інтернету речей це безпосередньо пристрої, які генерують збирану інформацію. Датчики, які збирають інформацію та передають в мережу зв'язку(н.д. Wi-Fi Bluetooth, LTE…). З мережі дані перетікають в хмарну обчислювальну платформу, що дозволяє розширити масштаб використання IoT. Найчастіше наступним кроком є аналітика даних за допомогою ШІ в ході якої прогнозуються події та відбувається автоматичне керування пристроями. Фінальною точкою є інтерфейс користувача, де він може ознайомитися з інформацією, налаштувати параметри роботи IoT.

Метою є аналіз технологій Інтернету речей і визначення доступних методів і засобів для подальшого вдосконалення пристроїв і систем Інтернету речей, в т.ч. підвищення рівня кібербезпеки в них.

Результати дослідження

Інтернет речей бере початок у 1999 році та активно розвивається у сьогоденні. Розвиток технологій IoT впливає на більшість сфер життя людини, такі як ведення бізнесу, будівництво, екологія, логістика, промисловість, та звісно сфера послуг, усі ці речі якими наповнене повсякденне життя пов'язані з IoT. Інтернет речей є шляхом, який об'єднує\передає інформацію через мережу. Більшість сучасних розумних пристроїв, які об'єднані в мережу. За принципом «Інтернет речей» пристрої працюють синхронно і дозволяють здійснювати розподілений або «розумний» функціонал. Іншими словами принцип роботи IoT полягає в тому, що пристрої об'єднані між собою різні інтелектуальні пристрої та сервіси за допомогою комунікаційних можливостей мережі Інтернет. Принцип показано на рис. 1.

Різновиди технологій IoT. Існує велике різноманіття шляхів застосування пристроїв та систем IoT, розглянемо декілька з них: розумний дім: (через телефон користувач має змогу контролювати Smart-замок, який використовує відбиток пальця як ключ, регулювання температури за допомогою датчиків тепла, датчики світла, робот пилосос та загалом будь-який пристрій, під'єднавши до мережі можна контролювати дистанційно, Зняття готівки з банкомату також підтримується інтернетом речей, отримання посилок у поштоматах, за допомогою програми. Також охорона здоров'я, транспортна логістика(відстежування стану вантажу, геолокація), сільське господарство(прогнози погоди, агродрони), промисловість(роботизація виробничих процесів, оптимізація споживання ресурсів,

сенсори моніторингу\контролю обладнання), торгівля і фінанси(інтерактивні вітрини), безпека і порядок(Face ID, сканери відбитків пальців і тп.).

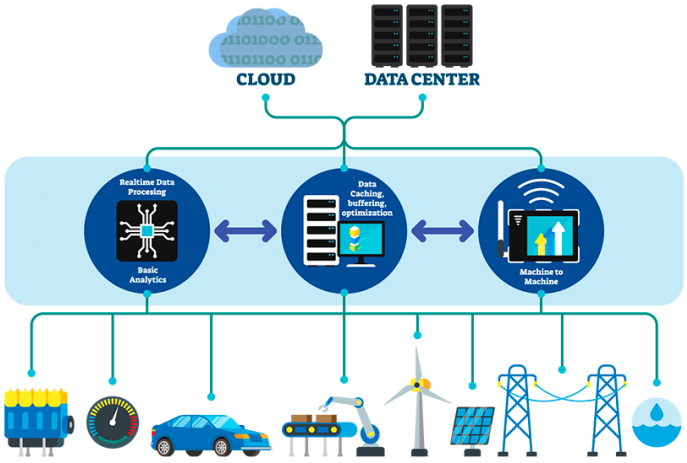

Рисунок 1. Принцип роботи технологій IoT

Інтернет речей в промисловості. Інтернет речей в промисловості займає вагому позицію. Контроль процесів за допомогою датчиків та дистанційне керування, передача даних та аналітика процесів у виробництві. Також за допомогою IoT є можливість оптимізувати та зробити більш екологічним використання обладнання, шляхом постійного моніторингу та автоматичної діагностики, що також підвищує безпеку, енергозбереження.

Огляд кібератак, найбільшою загальною загрозою кібератак на IoT є витік особистих данних користувача. Інтернет-повідомлення розширює поле можливих кібератак, оскільки кожен новий підключений пристрій створює додаткову точку доступу до мережі, яка потребує надійного захисту. Збільшення поверхневої атаки означає збільшення кількості негативних вразливостей, якими можуть зменшитися зловмисники.

Серед основних кібератак на інфраструктуру Інтернету речей можна визначити наступні:

1. Атаки типу "відмова в обслуговуванні" (DoS/DDoS). Характеризується перевантаженням мережі або пристроїв надмірними запитами, що робить їх недоступними.
2. Злом пристроїв. Використання слабких паролів або вразливостей у прошивках для несанкціонованого доступу.
3. Перехоплення даних. Атаки "людина посередині" (MitM) для отримання конфіденційної інформації.
4. Модифікація даних. Зміна даних, що передаються між пристроями, для введення користувачів в оману.
5. Шкідливе ПЗ для IoT. Використання зловмисного програмного забезпечення для створення ботнетів або викрадення даних.
6. Експлуатація вразливостей протоколів. Атаки на протоколи зв’язку, такі як MQTT або Zigbee.
7. Фізичні атаки. Отримання доступу до пристроїв для їх компрометації.

Основними методами захисту даних в пристроях IoT є класичне використання надійних паролів, регулярне оновлення паролі. Також важливо шифрувати данні при передачі чи зберіганні. Сегментація мережі для ізоляції IoT-пристроїв також є важливим етапом у запобіганні зламу. Можна додати ще моніторинг мережевого трафіку для виявлення аномалій. Ці захлди стануть ключовими в мінімізації ризику зламу та в забезпеченні безпеки системи Інтернет речей.

Впровадження IoT-пристроїв у домашньому, офісному середовищі та інших галузях зумовлює появу нових викликів у забезпеченні безпеки й забезпеченні рівня.

Висновки

Отже Інтернет речей надзвичайно зручна система, яка неодмінно повинна бути впроваджена в повсякденне життя людей, бо він неодмінно покращує якість життя. IoT економить час, ресурси та загалом спрощує життя. Звісно існують ризики використання абсолютної автоматизації, проте на мою думку ризики існують завжди, потрібно лише дотримуватись правил безпеки. Підтримка та впровадження нових технологій IoT потребують паралельного розвитку надійних кібербезпечних

рішень, здатних запобігти теперішнім загрозам. Завдяки розвитку інноваційних технологій та захисту постійного вдосконалення стандартів безпеки ми можемо безпечно використовувати потенціал IoT.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Гончарук, О. Ю. Інтернет речей: перспективи та ризики / О. Ю. Гончарук // Інформаційні технології і безпека. – 2023. – № 2. – С. 22–28.
2. ISO/IEC 30141:2018. Internet of Things (IoT) — Reference Architecture. International Organization for Standardization. – URL: https://www.iso.org/standard/65695.html
3. Макаренко, І. І. Технології безпеки в системах Інтернету речей / І. І. Макаренко // Сучасні інформаційні системи. – 2022. – № 3(45). – С. 34–40.
4. Гузь, О. В. Основи безпеки IoT-пристроїв: сучасні підходи / О. В. Гузь // Захист інформації. – 2021. – № 1. – С. 17–23.
5. McKinsey & Company. The Internet of Things: Mapping the value beyond the hype. – 2023. – URL: https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/the-internet-of-things
6. Сич, І. О. Кібербезпека Інтернету речей: загрози та методи захисту / І. О. Сич // Безпека інформаційних технологій. – 2023. – № 2. – С. 8–13.
7. Gartner. IoT Security: Best Practices and Key Challenges. – 2023. – URL: https://www.gartner.com/en/documents/iot-security-best-practices
8. Власенко, А. В. Хмарні технології та IoT: перспективи взаємодії / А. В. Власенко // Комп’ютерні науки та кібербезпека. – 2022. – № 4. – С. 45–52.
9. Коваленко, Д. А. Методи захисту персональних даних в IoT-системах / Д. А. Коваленко // Інформаційна безпека. – 2021. – № 3. – С. 60–65.
10. NIST. Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. – National Institute of Standards and Technology. – URL: https://csrc.nist.gov/publications/detail/nistir/8228/rev-1/final

Краєвська Анастасія Андріївна — студентка групи 1КІТС-24б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: anastasiakraievska@gmail.com

Науковий керівник: ***Маліновський Вадим Ігоревич*** — доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця .

Kraievska Anastasia Andriivna — a student of group 1KITS-24b at the Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia. Email: anastasiakraievska@gmail.com.

Scientific Supervisor: **Malinovskyi Vadym Igorevych** - Associate Professor of the Department of Information Security, Vinnytsia National Technical University, Vinnytsia.