АКТУАЛЬНІСТЬ БЕЗПЕКИ ІНТЕРНЕТ РЕЧЕЙ

Міланка І.Ю., Волотка В.С.

Кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Харківський національний університет радіоелектроніки,
Україна.

E-mail: ihor.milanka@nure.ua,
vadym.volotka@nure.ua

Abstract

The article is devoted to the use of the Internet of Things (IoT), because it plays an important role in improving our lives and increasing the efficiency of various industries and has various applications. IoT security risks can include network attacks, leaks of personal information, intrusions, and more. Therefore, the relevance of IoT security lies in the need to develop and implement best practices, standards, and technologies that ensure data privacy, integrity, and availability, as well as protection against potential security threats.

Інтернет речей (Internet of Things, IoT) - це концепція, що описує мережу фізичних об'єктів або "речей", які підключені до Інтернету і можуть обмінювати даними та взаємодіяти з іншими пристроями, за допомогою вбудованих сенсорів, програмного забезпечення та комунікаційних засобів. І якщо тема відноситься до обміну та взаємодії, то воно потребує і безпеки.
Інтернет речей приніс безліч переваг, таких як підвищена ефективність, зручність і автоматизація. Наведемо приклад деяких переваг IoT:

- Зручність і автоматизація: IoT дозволяє підключати різні пристрої до мережі та дистанційно керувати ними. Це робить життя більш зручним і спрощує багато щоденних завдань. Наприклад, ви можете керувати освітленням, опаленням, кондиціонером та іншими системами вдома за допомогою смартфона або голосового асистента.
- Вища ефективність і оптимізація ресурсів: IoT допомагає виробникам, логістиці та сільському господарству вдосконалювати процеси та оптимізувати використання ресурсів. Наприклад, в сільському господарстві можна використовувати сільськогосподарські сенсори для моніторингу вологості грунту, погоди та рослин, що допомагає підвищити врожайність та зменшити витрати на ресурси.
- Покращення якості послуг: IoT може поліпшити якість послуг у багатьох галузях, таких як медицина, транспорт і логістика. Наприклад, медичні IoT-пристрої можуть відстежувати стан пацієнтів в реальному часі та надавати медичному персоналу важливі дані для прийняття рішень.
- Зменшення витрат і ефективність енергоспоживання: IoT дозволяє більш ефективно використовувати ресурси, такі як електроенергія та вода. Системи керування енергоспоживанням та водопостачанням можуть регулювати витрати залежно від реальних потреб, що допомагає зменшити витрати та покращити екологічну стійкість.
- Моніторинг та аналітика: IoT надає можливість збирати велику кількість даних, які можна використовувати для моніторингу та аналізу різних процесів. Це допомагає приймати обґрунтовані рішення та прогнозувати події.
- Забезпечення безпеки та нагляду: IoT-пристрої можуть використовуватися для нагляду і безпеки. Відеоспостереження, системи контролю доступу та сигналізація можуть бути підключені до IoT для забезпечення безпеки будівель і територій.

- Розвиток нових бізнес-моделей: IoT відкриває нові можливості для бізнесу, які раніше були неможливими. Від послуг "розумного будинку" до підприємств, які спеціалізуються на IoT-рішеннях, індустрія IoT пропонує нові можливості для розвитку бізнесу.

Тема безпеки Інтернету речей (IoT) залишається актуальною і важливою в сучасному світі. Інтернет речей включає в себе підключені до мережі пристрої, які здатні обмінюватися даними та взаємодіяти один з одним через Інтернет. Це можуть бути смарт-пристрої, веб-камери, автомобілі, медичні пристрої, побутова техніка, сільськогосподарські пристрої та багато інших речей.

Інтернет речей (IoT) створює безліч ризиків для безпеки, і ці ризики варіюються від технічних атак до порушень приватності та фізичної безпеки. Ось деякі з основних ризиків безпеки IoT:

1. Кібератаки і вторгнення: захоплення або атаки на IoT-пристрої можуть призвести до небажаних наслідків. Атаки можуть бути спрямовані на відключення пристроїв, крадіжку даних або використання пристроїв у якості частини ботнету для масштабних кібератак.
2. Недостатній захист даних: IoT-пристрої збирають і обробляють велику кількість особистих даних. Якщо ці дані не належним чином захищені, вони можуть бути доступні недобросовісним особам і використовуватися для кіберзлочинів.
3. Відсутність оновлень та патчів: багато IoT-пристроїв не отримують регулярних оновлень і патчів для виправлення виявлених вразливостей. Це робить їх вразливими перед новими загрозами безпеки.
4. Недостатнє керування ідентифікацією та доступом: поганий контроль доступу може дозволити недозволеним особам отримувати доступ до IoT-пристроїв і мережі.
5. Використання захоплених пристроїв у мережі ботнету: атакувачі можуть захопити беззахисні IoT-пристрої та використовувати їх для створення ботнетів для здійснення розподілених атак, таких як DDoS (розподілений запит на обслуговування).
6. Загроза фізичній безпеці: в деяких випадках компрометовані IoT-пристрої можуть вплинути на фізичну безпеку. Наприклад, атаки на автомобільні системи IoT можуть призвести до аварій, а порушення безпеки в системах контролю доступу можуть спричинити проникнення злочинців.
7. Недостатній моніторинг і виявлення інцидентів: багато організацій не мають ефективної системи моніторингу та виявлення інцидентів для IoT, що робить їх нездатними вчасно реагувати на загрози безпеки.
8. Приватність: IoT-пристрої можуть надавати особисту інформацію про користувачів, яка може бути використана без їхньої згоди. Порушення приватності може виникнути, якщо ці дані попадуть в недобросовісні руки.

Підвищення безпеки Інтернету речей (IoT) вимагає комплексного підходу і використання різних методів та стратегій. Наведені далі методи сприятимуть підвищенню безпеки IoT:

1. Шифрування даних: застосування шифрування даних на рівні пересилання та зберігання може захистити інформацію, що пересилається між IoT-пристроями та серверами. Використання протоколів шифрування, таких як TLS (Transport Layer Security) або SSL (Secure Sockets Layer), допомагає захистити дані від недозволених доступів.
2. Аутентифікація: вимагати аутентифікації для доступу до IoT-пристроїв і мережі. Це може включати в себе використання паролів, біометричних методів або двофакторної аутентифікації для перевірки справжності користувача.
3. Управління доступом: обмеження доступу до IoT-пристроїв для тих користувачів та систем, яким це дозволено. Встановлення ролей та прав доступу допомагає запобігти недозволеному вторгненню та маніпуляціям з даними.
4. Виявлення вразливостей: регулярно проводити аудит безпеки та тестування на вразливості IoT-пристроїв і програмного забезпечення. Швидка ідентифікація та виправлення вразливостей є важливим аспектом безпеки.

5. Оновлення та патчі: забезпечити регулярні оновлення програмного забезпечення IoT-пристроїв для виправлення відомих вразливостей і підвищення їх безпеки.
6. Захист мережі: використання брандмауера, систем виявлення вторгнень та інших заходів для захисту мережі IoT від несанкціонованого доступу та атак.
7. Захист фізичного доступу: фізичний доступ до IoT-пристроїв повинен бути обмежений, щоб запобігти фізичним атакам і викраденню пристроїв.
8. Моніторинг та відстеження інцидентів: встановлення систем моніторингу та виявлення інцидентів допомагає вчасно виявляти підозрілу активність і реагувати на неї.
9. Впровадження стандартів безпеки: дотримання визнаних стандартів безпеки, таких як ISO 27001 або NIST Cybersecurity Framework, сприяє покращенню безпеки IoT.

Література

1. Що таке Інтернет Речей? – Internet of Things. IoT NULP ukr – Lviv IT Cluster. URL: http://iot.lviv.ua/що-таке-інтернет-речей (дата звернення: 06.11.2023).

2. Безпека інтернету речей - Безпека та відеоспостереження. Безпека та відеоспостереження. URL: https://oxorona.com/iot-security (дата звернення: 06.11.2023).

3. CyberLympha. Информационная безопасность в IoT. Хабр. URL: https://habr.com/ru/articles/700800/ (дата звернення: 06.11.2023).