УПРАВЛІННЯ РИЗИКАМИ В СИСТЕМАХ ІНТЕРНЕТУ РЕЧЕЙ

Комарець К.А., Ляшенко О.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Інтернет речей поєднує фізичні пристрої з інтернет-зв'язком, що дозволяє об'єднувати різні об'єкти в єдину мережу і забезпечувати надійний обмін інформацією між ними.

Проте збільшення кількості підключених пристроїв і об'єктів створює додаткові ризики для безпеки системи. Ці ризики можуть бути пов'язані зі зломом системи, витоком конфіденційної інформації, атаками на мережевий рівень, шкідливими програмами тощо.

Оцінка ризиків включає в себе ідентифікацію потенційних загроз, оцінку наслідків вразливостей системи та визначення ймовірності виникнення конкретного ризику.

Після оцінки ризиків розробляється стратегія управління ризиками, що передбачає прийняття заходів для зменшення ризиків до прийнятного рівня.

Метою доповіді є дослідження та аналіз проблем, пов’язаних із безпекою систем Інтернету речей, а також надання рекомендацій щодо ефективного управління ризиками в цих системах.

Управління ризиками в системах Інтернету речей є надзвичайно важливим, оскільки забезпечує безпеку системи та знижує ризики її порушення. При цьому необхідно пам'ятати, що управління є динамічним процесом, оскільки загрози безпеці можуть змінюватися з часом.

Ось деякі можливі рішення проблеми безпеки:

1. Використання захисту периметра: це означає встановлення мережевих фільтрів та інших заходів безпеки на межі мережі.
2. Використання шифрування: шифрування може використовуватися для захисту конфіденційної інформації, наприклад паролів і даних користувачів.
3. Постійне оновлення програмного та апаратного забезпечення: це допомагає запобігти використанню застарілих версій програмного та апаратного забезпечення, які можуть бути вразливими до кібератак.

Підсумовуючи, управління ризиками в системах Інтернету речей є надзвичайно важливим елементом забезпечення безпеки цих систем.

Загалом, рішення для управління ризиками в системах IoT повинні бути комплексними та включати в себе різноманітні заходи безпеки, контроль ризиків та навчання користувачів.

Список літератури

1. Popescu, T.M.; Popescu, A.M.; Prostean, G. IoT Security Risk Management Strategy Reference Model (IoTSRM2). Future Internet 2021, 13, 148. https://doi.org/10.3390/fi13060148.