СЕКЦІЯ 2

БЕЗПЕКА ІНТЕРНЕТ РЕЧЕЙ

УДК 004.08: 621.37

Є. ДІДИК, І. ЯРОВА

Національний університет Одеська Політехніка

ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ RFID-СИСТЕМ В КІБЕРПРОСТОРІ

Вступ. Постійне зростання використання RFID-технологій (Radio-Frequency Identification Technology) у різних сферах - від логістики та торгівлі до безпеки та доступу до об'єктів - підвищує важливість захисту цих систем від кіберзагроз. Використання RFID-технологій для ідентифікації, відстеження й управління матеріальними ресурсами має низку переваг, але водночас зумовлює загрози, пов'язані з можливістю несанкціонованого доступу до даних, переданих між RFID-мітками і зчитувачами. Це дослідження присвячено аналізу вразливостей RFID-систем, визначенню загроз, які вони створюють, і методів захисту від них.

Мета: дослідження кібербезпеки RFID-систем, їхньої структури, вразливостей, а також шляхів підвищення захисту від кіберзагроз.

1. Аналіз архітектури та елементів RFID-систем

RFID-системи складаються з трьох основних компонентів: RFID-мітки, RFID-зчитувача та централізованої системи управління даними. Ці елементи спільно забезпечують передачу інформації між об'єктами і системою управління, що дозволяє автоматизувати процеси відстеження та ідентифікації. RFID-зчитувачі можуть встановлюватися у різних об'єктах: торгових центрах, підприємствах, транспортних засобах, забезпечуючи безконтактний обмін даними в режимі реального часу. Використання цих систем дозволяє контролювати доступ до приміщень, вести облік продукції на складі та організовувати різні автоматизовані процеси.

На рисунку 1 наведена структурна схема RFID-системи та необхідне технічне устаткування.

Рисунок 1 - Структурна схема RFID-системи та технічне устаткування

Процес функціонування RFID-системи зазвичай наступний. За допомогою RFID-терміналу завантажується завдання по інвентаризації. На терміналі обирається тип інвентаризації (повна або за певним фільтром) і за допомогою курка або кнопки запускається процес зчитування міток. Для цього не потрібно наводити термінал на мітку, а достатньо здійснювати рух в бік ОЗ з мітками на відстані від 10 см до 10 м, періодично змінюючи положення терміналу. Про всі виявлені мітки термінал буде сигналізувати звуком, а знайдені мітки позначаються відповідним символом на екрані.

Натиснувши на терміналі на назву мітки, можна зайти в картку ОЗ, переглянути і при необхідності змінити інформацію про ОЗ (наприклад, місцезнаходження, стан тощо). Після закінчення інвентаризації результати вивантажуються на сервер. Приклад організації системи обліку ОЗ у складському приміщенні наведений на рисунку 2 [1].

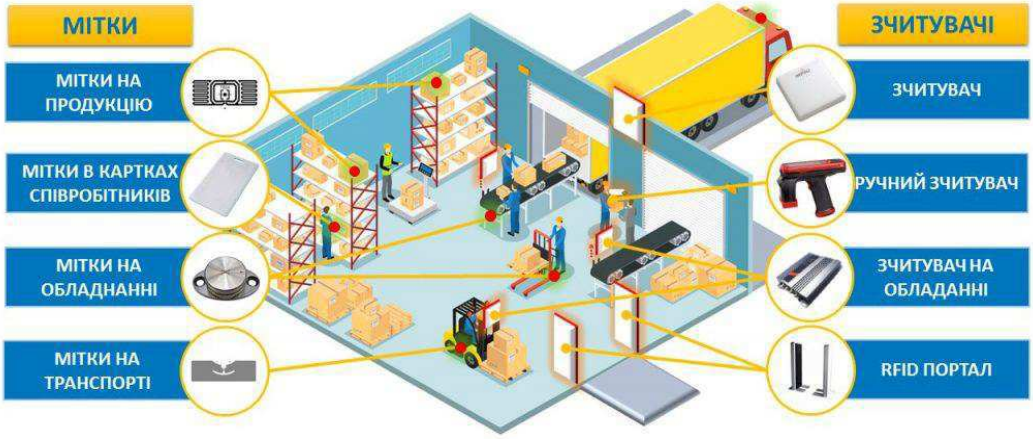

Рисунок 2 - Приклад організації системи обліку ОЗ у складському приміщенні

2. Аналіз ключових вразливостей RFID-систем

Вразливості RFID-систем можна поділити на чотири основні групи [2].

Загрози, пов'язані з клонуванням міток. Використання відкритих стандартів без захищених каналів зв'язку дозволяє зловмисникам клонувати мітки для отримання несанкціонованого доступу. Під час атаки спуфінгу зловмисник видає себе за законну мітку RFID або зчитувач, щоб отримати неавторизований доступ чи маніпулювати системою. Цього можна досягти шляхом клонування міток RFID або створення підроблених зчитувачів, які імітують поведінку легальних пристроїв.

Загрози пасивного та активного перехоплення даних. При несанкціонованому перехопленні сигналу можлива підробка інформації, яка передається між міткою і зчитувачем. Оскільки RFID-зв'язок відбувається через радіохвилі, він чутливий до перехоплення. Зловмисник може підслухати зв'язок між міткою і зчитувачем, потенційно отримуючи доступ до конфіденційної інформації або відстежуючи переміщення людей чи об'єктів.

Загрози для зчитувачів. Використання спеціального обладнання для атаки на зчитувачі може призвести до відмови в обслуговуванні або передачі помилкових даних у систему. Зловмисне програмне забезпечення, наприклад віруси чи хробаки, становить значний ризик для RFID-систем. Зараження ним RFID-зчитувача може призвести до несанкціонованого доступу або

маніпулювання даними, що зберігаються на мітках.

Фізичні атаки на системи RFID. Ці атаки включають втручання в мітку або зчитувач для отримання несанкціонованого доступу або порушення функціональності системи. Наприклад, зловмисник може фізично видалити або замінити RFID-мітку, щоб отримати доступ до зони обмеженого доступу.

3. Засоби захисту RFID-систем

Існують певні заходи забезпечення кібербезпеки RFID-систем.

Шифрування переданих даних для забезпечення конфіденційності інформації. Щоб усунути вразливість перехоплення сигналів, слід запровадити криптографічні протоколи та безпечні канали зв'язку для захисту конфіденційності та цілісності даних.

Динамічне шифрування сигналу: регулярна зміна ключів шифрування допомагає мінімізувати ризики перехоплення.

Аутентифікація між RFID-міткою та зчитувачем з метою зменшення ризику атак підробки. Це може включати використання унікальних ідентифікаторів, криптографічних ключів і протоколів запиту-відповіді, щоб гарантувати, що лише авторизовані мітки та зчитувачі можуть взаємодіяти з системою. Регулярні аудити та оцінки вразливості також можуть допомогти виявити та усунути будь-які потенційні недоліки в інфраструктурі RFID.

Захист від клонування міток: використання сучасних протоколів захисту з динамічною автентифікацією, які роблять неможливим копіювання міток.

Контроль доступу до зчитувачів через надійне адміністрування з використанням програмного забезпечення, що дозволяє налаштовувати права доступу і обробляти отримані дані з мінімальною затримкою. Для зменшення ризику зараження шкідливим програмним забезпеченням, на зчитувачах RFID слід проводити регулярне антивірусне сканування та оновлення програмного забезпечення.

Моніторинг і аналіз підозрілих сигналів для своєчасного виявлення несанкціонованого втручання. Постійний моніторинг трафіку дозволяє виявляти аномальні патерни, які можуть свідчити про атаку на систему.

Фізичні заходи безпеки. Пломби, що захищають від несанкціонованого доступу, і надійні огородження повинні бути використані для зменшення ризику втручання в мітку або зчитувач.

Висновок. Вразливості кібербезпеки в RFID-системах можна значно знизити завдяки впровадженню багаторівневих засобів захисту. Впровадження динамічного шифрування, захищених протоколів автентифікації та моніторингу трафіку зменшує ризик несанкціонованого доступу та перехоплення даних, підвищуючи надійність і безпеку RFID-технологій у різних сферах застосування.

Перелік використаних джерел.

1. Програмні рішення для автоматизації обліку. [Електронний ресурс]. - Режим доступу: https://ardix.systems/portfolio/

2. Top RFID Cybersecurity Vulnerabilities. [Електронний ресурс]. - Режим доступу: https://bluegoatcyber.com/blog/top-rfid-cybersecurity-vulnerabilities/