УДК 681.12

О. М. Жагловська[1]
В. І. Магденко[2]

РАДІОЧАСТОТНИЙ ЗЧИТУВАЧ НА МІКРОКОНТРОЛЕРІ ATtiny13

[1] Вінницький національний технічний університет

Анотація

Запропоновано схемотехнічне рішення даного пристрою, яке дозволило підвищити рівень безпеки при використанні радіочастотного зчитувача.

Ключьові слова : радіочастотна ідентифікація, транспондер, епітична крива, мікроконтролер.

Abstract

A schematic solution of this device was proposed that allowed to increase the level of safety when using the radio frequency reader.

Keywords: radio frequency identification, transponder, epithelial curve, microcontroller.

Вступ

Останніми роками набули широкої популярності різні проекти на основі ключів з радіочастотною ідентифікацією (Radio Frequency IDentification або RFID), що застосовуються в різноманітних системах безпеки, охорони та доступу. На багатьох підприємствах такі системи, доповнені спеціалізованим програмним забезпеченням, застосовуються для фіксування робочого часу, обліку тощо.

Будь-яка RFID-система складається з зчитуючого пристрою (зчитувач або рідер) і транспондера (RFID-мітка). Широке розповсюдження технології RFID пояснюється такими її перевагами, як відносно великий обсяг даних (наприклад, в порівнянні зі штрих-кодом), що зберігаються на мітці; відсутність потреби прямої видимості; можливість змінювати інформацію на мітці; унікальний ідентифікатор, що гарантує високий ступінь захисту тощо. Але використання RFID-міток пов'язано також і з такими негативними явищами, як: покупець може навіть не знати про наявність RFID-мітки або не може її видалити; дані з мітки можуть бути зчитані дистанційно без відома власника; проблема стандартів. Остання проблема на сьогодні є чи не найболючішою. Хоча процес вдосконалення стандартів не закінчився, у багатьох фірм простежується тенденція приховувати від публіки частину команд міток за своїми стандартами. І потім, ввівши певну секретну команду, працівники фірми можуть зчитати з мітки шифровану інформацію [1].

Метою роботи є підвищення ступеню безпеки при використанні радіочастотного зчитувача.

Результати дослідження

Вище розглянуто основні проблеми у безпеці NFC пристроїв. Розглянемо основні методи протиставлення загрозам.

Підслуховування

Так як NFC технологія сама не може захистити себе від підслуховування. Відмітимо, що, в пасивному режимі, передачу даних значно важче підслухати, але використання тільки пасивного режиму недостатньо для більшості програм, що передають конфіденційні дані.

Рішенням проти підслуховування є створення захищеного каналу, який не дасть можливості підслуховувати сторонніми пристроями

Пошкодження даних

NFC пристрої можуть протистояти такій атаці, оскільки вони можуть РЧ поля перевірити, в той час коли йде передача даних. Якщо пристрій NFC зробить це, він виявить атаку. Адже,

потужність, яка необхідна, для пошкодження даних значно більша, ніж потужність, яка може бути виявлена за допомогою NFC пристрою.

«NFC» або «Near Field Communication» («зв'язок на малих відстанях») — технологія високочастотного зв'язку (бездротового) малого радіусу дії. Дана технологія дає можливість обміну між пристроями даними, насамперед безконтактними платіжними терміналами та смартфонами, що знаходяться на відстані до 10 см.

Захищений канал для NFC

Створення такого каналу між пристроями NFC, звичайно, є найкращим підходом до захисту від будь-яких загроз.

Стандартний протокол узгодження ключа, на основі RSA як Diffie-Hellmann або еліптичні криві, для створення загального секретного ключа між двома пристроями, можуть бути застосовані. Оскільки, такий секретний ключ може бути використано для отримання симетричного ключа такого, як AES або 3DES. Його потім можна використати для забезпечення безпечного каналу [2].

Відповідно до визначених задач розроблено структурну схему пристрою, яку показано на рис. 1.

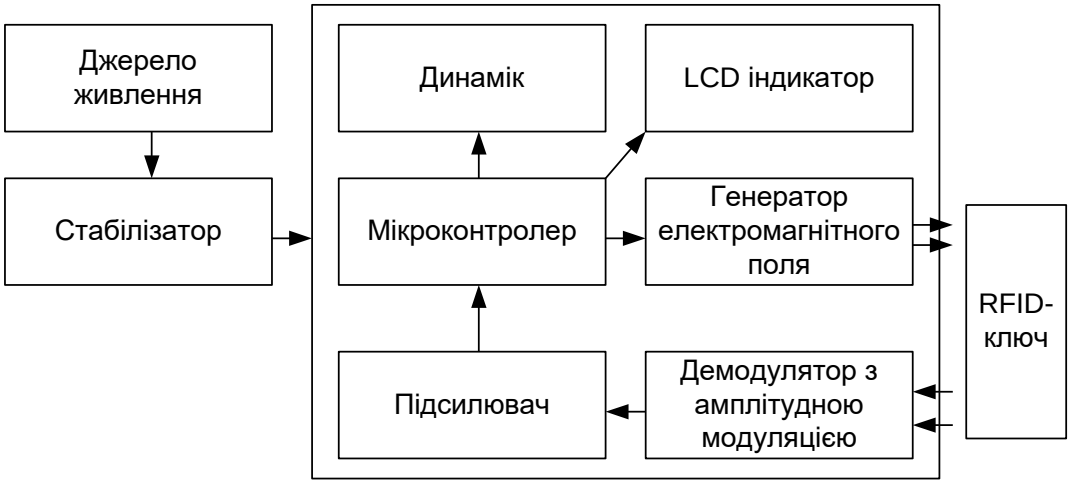

Рисунок 1 - Структурна схема радіочастотного зчитувача

До розробленої структурної схеми входять наступні елементи:

- блок живлення для забезпечення живленням усіх елементів радіочастотного зчитувача;
- стабілізатор для стабілізування вхідної напруги на необхідному рівні;
- мікроконтролер – генерує прямокутні імпульси необхідної частоти, які після подальшої обробки утворюють сигнал опитування RFID-ключа; приймає підсилений демодульований сигнал від RFID-ключа; аналізує прийнятий сигнал та видає відповідні повідомлення на LCD індикатор та динамік; забезпечує загальне керування процесом радіочастотного обміну інформацією;
- генератор електромагнітного поля формує вихідний сигнал для опитування та живлення RFID-ключа;
- демодулятор з амплітудною модуляцією для прийому та демодуляції сигналу від RFID-ключа;
- підсилювач для підсилення прийнятого сигналу до необхідного рівня;
- LCD індикатор для відображення результатів процесу радіочастотної ідентифікації;
- динамік видає сигнал про успішну або неуспішну ідентифікацію [3].

Висновки

Розглянуто можливі загрози використання пристроїв та систем RFID-технології, а також надано рекомендації щодо боротьби з ними. Наведено конкретні приклади реалізації RFID-модулів.

СИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. "Information technology - Telecommunications and information exchange between systems — Near Field Communication — Interface and Protocol (NFCIP-1)", ISO/IEC 18092, First Edition, 2004-04-01. -76с.
2. Технология NFC – связь на близком расстоянии [Електронний ресурс]. – Режим доступу: http://www.russianelectronics.ru. – ISSN 1813 - 8586.
3. Near Field Communication Technology Standards [Електронний ресурс]. – Режим доступу : http://www.nearfieldcommunication.org. – ISSN 2071 – 7342.

Жагловська Олена Миколаївна - старший викладач кафедри електроніки та наносистем, Вінницький національний технічний університет, Вінниця.

Магденко Владислав Івнович – студент групи МНТ-18м, факультет інфокомунікацій, радіоелектроніки та наносистем, Вінницький національний технічний університет, Вінниця, e-mail: vlad.mag97@gmail.com.

Ghaglovska Olena M. - senior lecturer of Department of Electronics and Nanosystems, Vinnytsa National Technical University, Vinnytsia.

Mahdenko Vladyslav I. - student group ME-14b, faculty of infocommunication, radio electronics and nanosystems, Vinnitsa National Technical University, Vinnitsa, e-mail: vlad.mag97@gmail.com.