Родичев Кирилл Федорович, студент кафедры геоинформатики и информационной безопасности, E-mail: kirill.rodichev38@gmail.com. Научный руководитель: доцент Н.Л. Додонова.

УДК 004.087.4; 004.67

БЕЗОПАСНОСТЬ И ЗАЩИТА ДАННЫХ В ИМПЛАНТИРУЕМЫХ RFID-МЕТКАХ

С.В. Жуков, Т.М. Казанцева
«Самарский национальный исследовательский университет имени академика С.П. Королева», г. Самара

Ключевые слова: имплантируемые RFID-метки, методы шифрования, защита данных, обработка численных данных.

В современном мире с переизбытком информации одной из самых актуальных проблем является безопасность данных и их эффективная защита [1]. Для реализации было предложено использование технологичных, удобных для ношения, биосовместимых имплантируемых RFID-чипов. Однако на данном этапе все еще остается нерешенным вопрос о безопасности данных в таких системах.

На данный момент передача данных в имплантируемых метках происходит по радиочастотному каналу в соответствии с протоколом ISO/IEC 14443 — стандарт, описывающим частотный диапазон, метод модуляции и протокол обмена бесконтактных пассивных карт (RFID) ближнего радиуса действия (до 0.1 м) на магнитосвязанных индуктивностях. По частоте метки обычно разделяются на три категории: LF, HF, UHF. Первая (LF, Low frequency) работает на частоте 100—150 кГц, и наиболее часто используется для подкожных имплантируемых меток. Рабочую частоту обычно выбирают среднюю — 125 кГц или 134 кГц. [2]

Примером такой передачи служит EM410x — это обобщенное название семейства совместимых чипов: EM4100, EM4200, TK4100, EM4102, TK28, КБ5004ХК2. Принцип работы таких меток заключается в следующем: считыватель генерирует переменное магнитное поле частотой 125 кГц, попадая в него, карта получает энергию и начинает циклически модулировать магнитное поле считывателя сигналом. Идентификационный код содержит 64 бита, в том числе 40 бит собственно уникального номера, специальная синхронизирующая последовательность и контрольные биты четности.

Данная проблема может иметь три варианта решения:

1. Использование проверенных стандартных алгоритмов.
2. Модификация известных алгоритмов с целью повышения производительности и снижения логической сложности.

3. Разработка новых алгоритмов.

Второй подход заключается в модификации шифра, который был изначально разработан для применения в аппаратном обеспечении. Однако стоит учесть, что при усложнении систем кодирования, при возникновении ошибок, могут возникнуть более серьезные проблемы, связные с защитой данных. Большинство же решений в области LW-криптографии основывается на третьем подходе. Ясно, что создание нового шифра без определенных изъянов стойкости представляет собой довольно сложную задачу, однако существующие алгоритмы показывают неплохие результаты и, возможно, в будущем найдут свое применение в криптосистемах, обеспечивающих безопасность RFID-устройств.

Из вышеизложенного следует, что разработка новой более простой и надежной модификации системы кодирования поможет устранить проблемы с утечкой информации и защитой данных в индивидуальных имплантируемых RFID-системах.

Список использованных источников

1. Имплантация RFID-меток, умный дом и безопасность интернета вещей [Электронный ресурс] : многопредмет. широковещ. науч.-поп. журн. – Электрон. журн. – Москва - Режим доступа к журн.: https://beardycast.com/podcast/beardycast/special/iot-special/

2. Идентификаторы RFID: новые веяния, новые опасности [Электронный ресурс] : медиа порт. – Электрон. журн. – Казахстан – Режим доступа к журн.: https://www.caravan.kz/articles/identifikatory-rfid-novye-veyaniya-novye-opasnosti-369071/

Жуков Семен Викторович, аспирант кафедры радиотехники. E-mail: zhukovsv91@inbox.ru.

Казанцева Татьяна Михайловна, студентка группы 6464-120304D. E-mail: tanyastud2712@gmail.com