6. Гизатуллин З.М., Нуриев М.Г., Шкиндеров М.С., Назметдинов Ф.Р. Простая методика исследования электромагнитного излучения от электронных средств // Журнал радиоэлектроники. – 2016. – №9. – С. 7.

7. 7 причин, почему Интернет вещей должно вас пугать [Электронный ресурс]. URL: https://alfa-service42.com/tehnologii/internet-veschey-obzor-problem-bezopasnosti.html (дата обращения: 12.05.2019).

Т.А. Курзенева

NFC-МЕТКИ КАК ЭЛЕМЕНТ «УМНОГО ДОМА» И ОБЕСПЕЧЕНИЕ ИХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ)

В настоящее время экономия времени на выполнении бытовых задач и соответствующая адаптация устройств является актуальным направлением в информационных технологиях. Обеспечение дома или любого другого помещения с использованием элементов и устройств вычислительных систем, позволяющих выполнять повседневные задачи или иные пожелания владельца относится к системам «Умного дома». Данные системы разрабатываются на основе различных технологий: от высокотехнологичных систем, позволяющих объединить множество устройств и отдать их под управление искусственного интеллекта до небольших элементов, обеспечивающих работу таких систем.

Near field communication, NFC («коммуникация ближнего поля», «ближняя бесконтактная связь») – технология беспроводной высокочастотной связи малого радиуса действия. Такая технология позволяет обмениваться данными между устройствами, расположенными на близком расстоянии (не более 10 сантиметров). Разработано 2 вида устройств на основе NFC технологии: активные (создают поля, позволяющее считывать) и пассивные (не создают полей, с них можно только считать).

NFC-метки представляют собой антенну минимальных размеров (обычно толщиной с бумажный лист и диаметром 1,5-2 сантиметра), осуществляющую пассивную передачу данных. NFC-метки можно запрограммировать для выполнения различных задач, облегчающих жизнь современного человека.

В настоящее время привычным стало использование NFC технологий в телефонах для оплаты. Однако возможности применения такой технологии гораздо шире. Например, можно установить NFC-метку на зарядное устройство в машине и обеспечить тем самым беспроводную зарядку или можно запрограммировать девайс на автоматическое подключение к точке доступа. Наклеив чип на поверхность прикроватной тумбы и задав правильную команду, можно установить будильник, изменить мелодию или отрегулировать яркость экрана на ночную. NFC-метку можно наклеить на лобовое стекло машины вместо номера, тогда если ваша машина будет мешать проезду, используя одно

движение, появится возможность отправить сообщение на ваш телефон с просьбой освободить проезд.

Возможно использовать NFC-метку для удостоверения личности или совершения платежей, хранения идентифицирующей информации. В данных случаях беспроводные технологии хоть и облегчают жизнь, но также несут в себе опасность нежелательного разглашения информации. Как и любые новые технологии NFC имеет ряд уязвимостей и слабостей, существуют ошибки в конкретных девайсах, использующих эту технологию.

С точки зрения информационной безопасности основные уязвимости NFC связаны с невозможностью использовать шифрования, криптографию при передаче данных с помощью существующих протоколов NFC. При эмуляции применяются слабые криптографические алгоритмы и закладывается излишнее доверие к информации, хранящейся на метках, то есть фактически не выполняется фильтрация данных. Это приводит к тому, что широкое распространение получают атаки на NFC-метки: несанкционированный доступ к информации, Reply Attack (позволяет повторить команду и получить доступ от имени другого лица).

Нужно иметь в виду, что запрограммировать NFC-метку только кажется сложным и не является задачей для профессионального хакера. Для записи команд достаточно выбрать одно из многочисленных приложений в магазинах для разных платформ смартфонов. В связи с этим необходимо с особым вниманием относится использованию NFC-меток для хранения информации, несанкционированный доступ к которой может повлечь ущерб.

Использование NFC-меток является современным способом автоматизации и упрощения привычных действий, выделяющимся универсальностью своего применения – какие именно команды будет выполнять девайс после прочтения метки, зависит только от потребностей человека.

Литература

1. Карнаухов В., Безнос О. Технология Near Field Communicatoin (NFC) // Современные наукоемкие технологии, № 3, 2014. [Электронный источник] — Режим доступа. — URL: http://cyperleninka.ru/article/n/tecnologiya-near-field-communication-nfc/

2. Рабинович А.С., Казарин О.В. Методика аутентификации пользователя в информационной системе с использованием технологии NFC [Электронный ресурс] // Вопр. кибербезопасности. 2013. № 2. URL: http://cyberleninka.ru/article.ru

3. FIDO NFC Protocol Specification v1.0 [Электронный ресурс] // 11.04.2017 [Электронный источник] — Режим доступа. — URL: https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/fido-u2f-nfc-protocol-v1.2-ps-20170411.pdf