5. Специальный съемный носитель информации. Патент на полезную модель № 94751. 27.05.2010, бюл. №15.

6. Съемный носитель информации на основе энергонезависимой памяти с расширенным набором функций информационной безопасности. Патент на полезную модель № 130441. 20.07.2013, бюл. № 20.

7. *Конявская С. В.* Безопасный Интернет: видимость как необходимое и достаточное [Электронный ресурс] /С. В. Конявская, В. В. Кравец, А. Ю. Батраков. – 2015. – Режим доступа: http://www.okbsapr.ru/konyavskaya_2015_2.html. – Дата доступа: 24.04.2015.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИЙ БЕСПРОВОДНОЙ СВЯЗИ МАЛОГО РАДИУСА ДЕЙСТВИЯ

Л. Л. УТИН, М. А. САБЕРИАН

Одной из новейших информационно-телекоммуникационных технологий, получивших свое развитие в последние годы, является обмен данными с использованием средств обеспечения беспроводной связи малого радиуса действия (Near Field Communication (далее – NFC)). В докладе предлагаются к обсуждению полученные результаты исследований возможностей различных криптографических алгоритмов, которые могут быть использованы для шифрования информации, передаваемой с использованием технологий NFC. Об этой технологии впервые стало известно в 2004 г. на международной конференции с участием крупных компаний Nokia, Philips, Sony. В ходе данного мероприятия крупнейшие разработчики телекоммуникационного оборудования обсудили одно из альтернативных решений передачи данных с мобильного телефона к различным приемным устройствам, обладающее определенными преимуществами по сравнению с известными стандартами. В результате были разработаны рекомендации ECMA-340 и ISO/IEC 18092 по применению средств NFC.

Финансовые вложения в развитие данного направления связи способствовали тому, что уже в 2006 г. компания Nokia выпускает первый мобильный телефон с встроенными средствами обеспечения беспроводной связи малого радиуса действия. Явные преимущества новых средств мобильной связи по сравнению с аналогами других производителей привели к резкому возрастанию спроса на данные устройства. По данным аналитической компании MarketsandMarkets, в 2013 г. в Японии, Корее, Великобритании, Франции, Германии, Бразилии, России и других странах было реализовано около 180 млн телефонов с поддержкой стандартов NFC, что составило около 20 % всех мобильных устройств проданных за этот период [1]. По мнению экспертов вышеуказанной компании, рынок NFC будет процветать и в ближайшем будущем. При этом прогнозируется его ежегодное увеличение на 16,25 млрд долларов.

Основными преимуществами технологии NFC по сравнению с аналогами являются низкое время установления связи (до 0,1 мс), безопасность и удобство. Благодаря этим свойствам технология NFC может применяться:

- для обмена файлами между телефонами (отдельно либо в сочетании с каналом Bluetooth);
- эмуляции смарт-карт;
- в качестве средства оплаты за проезд в общественном транспорте, магазинах, кафе, автомобильных заправочных станциях, на парковках и других местах, в которых одновременно обслуживается большое количество людей и требуется быстрая (в масштабе времени, близком к реальному) авторизация платежа, а сумма оплаты невелика;
- для открытия электронных замков в квартиру или машину;
- в качестве удостоверения личности, страховой карты;

• в системах учета рабочего времени сотрудников предприятий;

• в рекламных плакатах («Smart Posters»), для быстрого получения дополнительной информации о продуктах, приобретения скидки на товар, обеспечения участия граждан в маркетинговых голосованиях.

По данным исследований компании Frost&Sullivan, уже к 2018 г. с помощью устройств, поддерживающих стандарт NFC, будет осуществляться до 50 % мобильных платежей.

Однако, несмотря на достоинства рассматриваемой в докладе технологии, ей присущи определенные недостатки, приводящие к следующим угрозам информационной безопасности:

• до настоящего времени существует потенциальная опасность заражения банковской системы вирусами при использовании мобильного телефона в качестве средства по оплате платежей;

• использование средств постановки помех в диапазоне 13,56 МГц приводит к срыву сеансов связи с использованием технологии NFC;

• потенциальная возможность утечки персональных данных при осуществлении связи.

Например, 28 июня 2012 г. корпорация Symantec сообщила о появлении мобильного приложения Andoid.Ecardgrabber, способного считывать номера пластиковых карт, срок их действия и номер банковского счета пользователя с использованием технологии NFC [2]. После обнаружения потенциальной опасности данного приложения оно было удалено, однако более 500 пользователей Интернета успели скачать его на свои мобильные устройства.

Известно, что одним из способов защиты информации от утечки является применение различных методов криптографического преобразования данных и антивирусных программ. При этом в ходе анализа современных подходов к шифрованию данных в мобильной связи было установлено, что в настоящее время ужесточены требования к пропускной способности, объему оперативной памяти и потреблению энергии.

Список использованных источников

1. Обзор рынка систем NFC [Электронный ресурс] / tadviser. – Минск, 2015. Режим доступа: http: //www.tadviser.ru. – Дата доступа: 12.04.2015.

2. Andoid.Ecardgrabber считывает данные бесконтактной пластиковой карты по радиоинтерфейсу [Электронный ресурс] / CNEWS. – Минск, 2015. – Режим доступа: http: //www.cnews.ru. – Дата доступа: 12.04.2015.

НЕАТОМАРНЫЙ ВЗГЛЯД НА РКВ КАК НА КОМПОЗИЦИЮ ПЕРЕХВАТА УПРАВЛЕНИЯ И КОНТРОЛЯ ЦЕЛОСТНОСТИ

А. А. АЛТУХОВ

Концепция доверенной вычислительной среды (ДВС) [1, с. 204] в настоящий момент является одной из основных парадигм доверенных вычислений, применяемых на практике. В рамках этой концепции одной из основных задач обеспечения безопасности является обеспечение целостности вычислительной среды, где под целостностью вычислительной среды понимается стабильность работы в течение рассматриваемого периода в требуемом диапазоне состава объектов и процессов, их взаимосвязей и параметров функционирования [1, с. 207].

Для создания ДВС обязателен резидентный компонент безопасности (РКБ) [1, с. 207]. Одной из возможных реализаций РКБ является аппаратный модуль доверенной загрузки (АМДЗ) [2; 3].