АДАПТИВНЫЙ ВЫБОР СПОСОБОВ БЕЗОПАСНОЙ ПЕРЕДАЧИ ДАННЫХ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИЙ БЕСПРОВОДНОЙ СВЯЗИ МАЛОГО РАДИУСА ДЕЙСТВИЯ

Л.Л. Утин, М.А. Сабериан

Анализ возможностей технологий обмена данными с использованием средств обеспечения беспроводной связи малого радиуса действия (Near Field Communication (далее — NFC) показал, что в последние годы ее популярность возрастает. Это обусловлено тем, что мобильные устройства, поддерживающие стандарт NFC, могут в режиме реального времени устанавливать соединения для передачи и приема информации. Кроме того, из-за малого радиуса действия передающих средств такие мобильные устройства имеют высокую степень защищенности от перехвата информации злоумышленником.

Сфера применения технологий NFC начинается от обмена файлами между телефонами и заканчивается эмуляцией банковских карт [1].

Не смотря на достоинства рассматриваемой в докладе технологии ей присущи определенные недостатки, приводящие к различным угрозам информационной безопасности. Например, 28 июня 2012 года корпорация Symantec сообщила о появлении мобильного приложения Andoid.Ecardgrabber, способного с использованием технологии NFC считывать номера пластиковых карт, срок их действия и номер банковского счета пользователя [2].

Известно, что одним из методов защиты информации от утечки, является применение различных методов криптографического преобразования данных. При этом для реализации более стойких алгоритмов в мобильных телефонах, как правило, необходимо предусмотреть дополнительный объем оперативной памяти, а также качественную аккумуляторную батарею.

Анализ условий применения устройств мобильной связи, поддерживающих стандарт NFC, показывает, что при разработке адаптивных методов выбора способа передачи данных можно найти компромис между требованиями по безопасности и расходом электроэнергии.

В докладе предлагаются к обсуждению полученные результаты исследований возможностей различных криптографических алгоритмов, которые могут быть использованы для передачи информации с использованием технологий NFC.

Литература

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.

СОПРОВОЖДЕНИЕ ВОЗДУШНЫХ ОБЪЕКТОВ В УСЛОВИЯХ НАЛИЧИЯ РАЗРЫВОВ ЗОН РАДИОЛОКАЦИОННОГО НАБЛЮДЕНИЯ

Е.И. Михненок А.С. Белый

Обеспечение безопасного движения воздушных судов при постоянно растущем количестве новых международных трасс и маршрутов навигации является актуальной проблемой. С данной целью развернута широкая сеть наземных центров управления воздушным движением, которая позволяет организовать взаимодействие с воздушными судами, проводить мониторинг воздушной обстановки и в целом управлять ею.

Однако возникают случаи, когда происходит потеря связи с воздушным объектом и появляется задача определения его местоположения. Альтернативным способом решения данной задачи может служить совместное применение с аппаратурой аэронавигации центров управления воздушным движением средств радиолокационного наблюдения, которые позволяют производить сопровождение наблюдаемых объектов с выдачей их координатной информации. В тоже время для данного способа характерно наличие разрывов зон радиолокационного наблюдения, в которых сопровождение воздушных объектов

производиться не может. Таким образом, возникает задача идентификации вновь обнаруженных воздушных объектов преодолевших разрыв зон радиолокационного наблюдения и отождествление с ранее сопровождаемыми объектами.

В виду актуальности данной проблемы разработана методика сопровождения воздушных объектов в условиях наличия разрывов зон радиолокационного наблюдения.

Она основывается на выделении областей пространства вероятного нахождения воздушного объекта, рассчитанных на основе его летно-тактических характеристик и информации получаемой от средств радиолокации.

Применение данной методики в алгоритмах сопровождения воздушных объектов комплексов средств автоматизации, позволяет повысить достоверность радиолокационной информации, а в целом качество функционирования информационной подсистемы.

Литература

1. *Дубровский В.И.* Эксплуатация средств навигации и УВД. М., 2005.

2. *Кузьмин С.В.* Цифровая обработка РЛИ. Киев. 2001

ПРИМЕНЕНИЕ ОБМАННЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В ЛОКАЛЬНОЙ ИНФОРМАЦИОННОЙ СЕТИ

А.А. Черкас, В.В. Моисеев, Е.И. Хижняк

Главным недостатком существующих методов и средств защиты информации, включая современные средства поиска уязвимостей автоматизированных систем и обнаружения несанкционированных действий, является то, что они, в большинстве случаев организуют защиту информации лишь от уже выявленных угроз, что показывает определенную степень пассивности защиты.

Одним из возможных направлений решения проблемы защиты информации в локальной информационной сети от несанкционированных действий является применение методов обмана. Такие системы получили название ложных или обманных.

Механизм функционирования обманной системы заключается в том, чтобы вовлечь злоумышленника в диалог с системой. При этом обманные системы имитируют уязвимости реальных информационных систем. Злоумышленнику приходится постоянно решать: работает он с реальной системой или обманной, затрачивая при этом ресурсы.

Выполняющий все инструкции пользователь, преодолевает все области с наименьшими временными затратами. Нарушитель, пытаясь определить уязвимые места в СЗИ, сканирует поверхность упругого экрана, в результате чего он либо отражается от экрана, либо поглощается областями. Так как площади эмулированных уязвимостей значительно больше, чем реально существующих, то нарушитель с большой вероятностью попадает именно в "муляж". При этом, до некоторого момента времени нарушитель не подозревает, что работает с обманной системой. Пытаясь закрепиться в системе, и найти слабое место в следующей ступени защиты, он проявляет себя. В момент работы обманной системы настоящая система продолжает функционировать и успешно решать возложенные на нее задачи.

Применение обманных систем защиты информации в локальной информационной сети позволяет ввести в заблуждение противника, увеличить время для принятия необходимых мер администратором и с некоторой долей вероятности отвести угрозу от реальной работающей информационной системы.

Литература

1. Гладких А.А. Базовые принципы информационной безопасности информационных систем. Ульяновск, 2009.

2. Пескова О.Ю. Использование обманных систем для защиты локальной сети от внешних угроз. М., 2011.