брэндмауэров, технология цифровой подписи, защищенные протоколы: Secure HTTP (S–HTTP), Secure Sockets Layer (SSL), Secure Electronic Transaction (SET).

Угроза информации: данные преднамеренно перехватываются, читаются или изменяются; пользователи идентифицируют себя неправильно (с мошенническими целями); пользователь получает несанкционированный доступ из одной сети в другую. Действия по защите. Шифрование данных, препятствующее их прочтению или искажению; проверка подлинности отправителя и получателя осуществляется технологией цифровой подписи, фильтрация трафика, поступающего в сеть или на сервер защищается брэндмауэрами. Криптографические технологии обеспечивают три основных типа услуг для электронной коммерции: аутентификацию (которая включает идентификацию), невозможность отказа от совершенного и сохранение тайны.

Технология ЦП. При помощи хеш–функции получается дайджест — уникальным образом сжатый вариант исходного текста. Дайджест шифруется с помощью личного ключа и превращается в цифровую подпись, которая посылается вместе с самим сообщением.

Некоторые стандарты защиты данных для ЭК включают защищенные протоколы: S–HTTP (защищенный HTTP), SSL (является составной частью всех известных браузеров и Веб–серверов.), SET (используется для операций с кредитными карточками.).

МОНИТОРИНГ МЕСТОПОЛОЖЕНИЯ ПОЛЬЗОВАТЕЛЕЙ НА ОСНОВЕ ИХ АКТИВНОСТИ В СОЦИАЛЬНЫХ СЕТЯХ

Д.И. ЖУКОВСКИЙ

Мы живем во время стремительно развивающихся технологий. Вместе с повышением доступности персональных компьютеров, ноутбуков и мобильных телефонов, а также улучшения качества интернета социальные сети становятся неотъемлемой частью жизни современного человека.

Ежедневно пользователи социальных сетей публикуют большое количество различного контента, среди которого комментарии, заметки, фотографии и др. Проблема в том, что зачастую вся эта информация находится в свободном доступе и посторонний человек может узнать место, где находился пользователь в момент публикации контента. Данные о геолокации могут быть явно связаны с контентом (foursquare, twitter) или получены неявно, например на основе EXIF метаданных (vk.com, facebook).

EXIF (Exchangeable Image File Format) — стандарт, позволяющий добавлять к изображениям и прочим медиафайлам дополнительную информацию (метаданные), комментирующую этот файл, описывающий условия и способы его получения, авторство и т.д. EXIF метаданные добавляются на фотографии и видео большинством современных фотоаппаратов и телефонов.

Собирая и анализируя геолокационные данные пользователей социальных сетей можно, например, выяснить, какие места являются наиболее живописными в туристических районах, или где именно можно встретить определенного человека в различные промежутки времени в будни и выходные. С кем пересекается или общается конкретный пользователь. Если взять весь контент определенного пользователя, публикуемый им, скажем после 21:00 и до 07:00, нанести на тепловую карту, то с большой вероятностью можно определить, где именно он проживает.

Показательный пример — 20.03.2012 г. ФБР арестовало хакера Higinio O. Ochoa III, ему были предъявлены обвинения во взломе государственных сайтов и выкладывании в сеть телефонов и домашних адресов сотрудников полиции. Выйти на хакера помогла фотография, которую он разместил на странице с украденными данными. Фотография содержала EXIF метаданные с GPS координатами места, где она была сделана.

Зачастую вы сами можете отключить привязку геолокационных данных к публикуемому вами в социальных сетях контенту, тем самым обезопасив себя от открытия личной информации.

ОДНОКВАНТОВАЯ СИСТЕМА ПЕРЕДАЧИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ПО ВОЛОКОННО-ОПТИЧЕСКОЙ ЛИНИИ СВЯЗИ

А.О. ЗЕНЕВИЧ, А.М. ТИМОФЕЕВ, А.Ю. ЗЯБЛИКОВ,
А.Г. КОСАРИ, А.А. ЛИПАЙ, В.С. ТОЛКАЧЕВА

В настоящее время высокоскоростные волоконно-оптические системы связи получают все более широкое распространение. При разработке таких систем важно обеспечивать скрытность и конфиденциальность передаваемой информации, т.к. несанкционированный доступ может осуществляться достаточно просто, например, путем создания макроизгибов оптического волокна (МОВ). Существующие системы связи [1,2] позволяют обнаруживать МОВ, однако они малоэффективны при несанкционированном заборе не более десяти фотонов оптического излучения из каждого бита передаваемой информации. В этих случаях для передачи конфиденциальной информации целесообразно использовать оптические импульсы малой мощности, содержащие до десятка фотонов на каждый бит информации. Для формирования и регистрации оптических импульсов малой мощности применяют одноквантовые системы связи. Поскольку до настоящего времени отсутствуют исследования таких систем по определению длин волн и мощностей передаваемых оптических сигналов, при которых обеспечивается конфиденциальность передаваемых данных за счет обнаружения каналов утечки информации, сформированных МОВ, это являлось целью данной работы.

На основе созданной системы одноквантовой регистрации оптического излучения предложена одноквантовая система передачи конфиденциальных данных по волоконно-оптической линии связи. Применительно к такой системе связи экспериментально обоснован выбор длины волны 850 нм для передачи информации и длины волны 1625 нм для синхронизации времени передачи и приема информации и обнаружения несанкционированного доступа к информации.

Получено, что при мощности оптического сигнала $1{,}9\cdot10^{-12}$ Вт с длиной волны 850 нм обеспечивается наиболее высокая скорость передачи конфиденциальной информации и, вместе с тем, наиболее эффективно обнаруживаются возможные каналы утечки этой информации. Установлено, что наибольшее значение пропускной способности созданной одноквантовой системы связи достигается при использовании в качестве приемного модуля счетчика фотонов, построенного на базе лавинного фотоприемника со структурой n^+-p-π-p^+.

Работа выполнена при поддержке Белорусского республиканского фонда фундаментальных исследований (договор №Т13-018).

Литература

1. Патент Российской Федерации. № 2251810, H 04B 10/08, 2003.
2. Патент Российской Федерации. № 2252405, G 01M 11/00, 2004.

МЕТОДИКА ТЕСТИРОВАНИЯ ПОСЛЕДОВАТЕЛЬНОСТЕЙ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

Н.Г. Киевец

Существующие методы статистического тестирования предназначены для оценки качества работы генераторов случайных чисел (ГСЧ) на основе вырабатываемых ГСЧ случайных последовательностей. ГСЧ электронных пластиковых карт (ЭПК) генерируют