пропускной способностью и может быть выявлен как для электронного документа, так и для его напечатанной копии. Предлагается использовать в качестве стеганографического контейнера документ Microsoft Word и изменять смещение междустрочного интервала только неотображаемых символов. Анализ абзаца штатными средствами не показывает наличия смещения, изменение начертания или размера шрифта не выявляют наличия осажденных данных. Для контроля целостности осажденных данных предлагается также внести изменения в структуру электронного документа. Исходя из того, что файл документа Microsoft Word является архивом, содержащим набор XML файлов, можно использовать метод замены кавычек для размещения контрольной суммы осажденного сообщения.

Разработано программное средство, реализующее данную модификацию стеганографического метода изменения смещения междустрочного расстояния электронного документа с контролем целостности осаждаемого сообщения.

Литература

1. Блинова Е.А. Стеганографический метод на основе изменения междустрочного расстояния неотображаемых символов строк электронного текстового документа// Труды БГТУ. Сер. Физико-мат. науки и информатика № 6. С. 166–169.

2. Сущеня А.А. Стеганографическое преобразование текстов-контейнеров на основе языков разметки // 68-я научно-техническая конференция учащихся, студентов и магистрантов: сборник научных работ. Ч. 4. Минск, 17–22 апреля 2017 г. С. 145–149.

СИСТЕМА КОНФИДЕНЦИАЛЬНОЙ СВЯЗИ С ВОЗМОЖНОСТЬЮ ПРОВЕРКИ ПОДЛИННОСТИ ИНФОРМАЦИИ И ЕЕ ИСТОЧНИКА

А.М. Тимофеев

В настоящее время одной из наиболее важных задач, решаемых при разработке высокоскоростных систем передачи и приема конфиденциальной информации, является обеспечение проверки подлинности передаваемой информации и ее источника [1]. Такая задача может быть решена путем использования механизмов аутентификации информации и ее источника посредством электронных цифровых подписей (ЭЦП) [1, 2]. При этом используемые алгоритмы ЭЦП, включающие процедуры постановки и проверки подписи, зачастую требуют достаточно больших вычислительных ресурсов и не позволяют обеспечить максимально возможную пропускную способность канала связи. Это объясняется необходимостью генерирования больших простых чисел, вычисления хэш-функций и инверсий в системе наименьших вычетов, а также передачи по каналу связи кроме электронного документа его ЭЦП. В связи с этим целью данной работы являлась разработка высокоскоростной системы передачи конфиденциальной информации, свободной от указанных выше недостатков существующих систем и позволяющей определять подлинность как передаваемой информации, так и ее источника. В работе предложена система конфиденциально связи, информационная безопасность которой основана на использовании процедуры поблочного смешивания данных, подлежащих передачи, с идентификационной информацией отправителя и режимов асинхронной передачи и приема информации при помощи оптических импульсов слабой мощности, которые содержат от одного до нескольких десятков фотонов. Разработанная система связи позволяет обнаруживать факт навязывания ложных данных, которые злоумышленник может пытаться выдавать за подлинные, транслируя в канал связи, а также в автоматическом режиме обнаруживать несанкционированный съем данных, передаваемых по волоконно-оптическому каналу связи.

Литература

1. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия. М., НОУ «Интуит», 2016. 608 с.

2. Молдовян Н.А. Практикум по криптосистемам с открытым ключом. СПб., БХВ-Петербург, 2015. 304 с.