Выполненные конструктивно-программные доработки позволяют создать 3D-принтер с расширенными функциональными возможностями, который в обновленном виде способен будет печатать с увеличенной скоростью многими видами пластика без потери качества печати.

Литература

1. Столер В.А. Особенности использования трехмерной печати при решении инженерно-технических задач // Технические средства защиты информации: тезисы докладов XIV Белорусско-российской науч.-техн. конф. Минск, 25–26 мая 2016 г. С. 70.

КИБЕРУГРОЗЫ И ОТКАЗОУСТОЙЧИВОСТЬ

Судани Хайдер Хуссейн Карим, М.Б. Абросимов

Киберугрозы – это возможность (вероятность) несанкционированного проникновения в распределенные информационные системы для копирования, модификации, уничтожения находящихся в них данных или для затруднения или приостановки функционирования программной или аппаратной части информационной системы. Киберугрозы, в основном, исторически будучи формой деятельности отдельных высококвалифицированных преступников, к настоящему времени превратились в форму политического и военного воздействия спецслужб государств и террористических групп, систематически ведущих активную борьбу за передел международных сфер влияния. Объектами вмешательства становятся информационные системы государственного, военного, экономического и социального управления, а также устройства с выходом в Интернет отдельных граждан от чиновников и предпринимателей высокого ранга, известных лиц до рядовых служащих и несовершеннолетних детей. При реализации киберугроз возможные отказы и затруднения в работе информационных устройств, сбои и ошибки при информационных запросах способны привести в масштабе страны к значительным экономическим, военным и социальным последствиям и к ощутимым материальным ущербам. В этой связи, обеспечение отказоустойчивости информационных систем, как способности сохранять свою работоспособность в условиях реализации киберугроз, является актуальной научно-технической задачей, имеющей важнейшее социально-политическое значение. Для решения данной задачи следует определить всю номенклатуру киберугроз для заданной распределенной информационной системы. Каждой киберугрозе необходимо поставить в соответствие ожидаемый информационный, экономический, социальный, военный или иной ущерб, который произойдет в случае ее реализации применительно к рассматриваемой информационной системе. Необходимо оценить способность информационной системы выполнять свои функции в условиях реализации отдельной угрозы или их совокупности. Далее, исходя из результатов оценки, следует определить диапазон мер информационной защиты, а также состав резервных элементов программного и аппаратного обеспечения, который заменит вышедшие из строя элементы системы. Эффективность защиты от киберугроз будет измерена на интервале времени как отношение предотвращенного ущерба от реализации данного вида угрозы к стоимости мер защиты от данного вида угрозы и стоимости резервных элементов программного и аппаратного обеспечения. Уровень отказоустойчивости информационной системы применительно к номенклатуре киберугроз будет определяться заданным уровнем эффективности, для которой защищенность системы вначале будет спроектирована разработчиком, а в процессе эксплуатации будет постоянно совершенствоваться в ответ на возникающие новые формы киберугроз.

МОДИФИКАЦИЯ СТЕГАНОГРАФИЧЕСКОГО МЕТОДА ИЗМЕНЕНИЯ МЕЖДУСТРОЧНОГО РАССТОЯНИЯ ЭЛЕКТРОННОГО ДОКУМЕНТА

А.А. Сущеня, Е.А. Блинова, П.П. Урбанович

Предлагается модификация стеганографического метода изменения смещения междустрочного расстояния электронного документа, так называемого line-shift coding. В его стандартной реализации предлагается скрывать сообщение в изменении междустрочных интервалов. Однако такой метод имеет несколько существенных недостатков: обладает малой

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.