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