ВВЕДЕНИЕ

В современном, быстро трансформирующемся, высокотехнологичном мире, в котором количество информации уже превышает возможности человека по ее восприятию, все более острой становится проблема защиты различных типов данных в каналах их передачи и хранения от несанкционированного доступа (с целью уничтожения, модификации, использования и реинжениринга) приобретает все большую актуальность. Одно из проявлений этой проблемы – защита авторских прав на электронные документы (тексты, базы данных, коды компьютерных программ, графические объекты).

Настоящий отчет по проекту задания 1.2.12 (на 2019-20 гг.) ГПНИ «Информатика, космос и безопасность; Подпрограмма «Информатика и космические исследования» содержит результаты, являющиеся логическим продолжением и развитием исследований, выполненных авторским коллективом в 2016-2018 гг.

В предыдущие годы была обоснована и сформулирована концепция многоключевой стеганографической системы. Основным ее отличием от известных стеганографических систем является разделение используемой ключевой информации (КИ) на три типа: основную, определяющую базовый метод осаждения (или извлечение) тайного сообщения в (из) текстовый документ (документ-контейнер), и два типа дополнительной ключевой информации: КИ первого рода, относящуюся к методам предварительного преобразования сообщения (до его осаждения), и КИ второго рода, относящуюся к порядку размещения элементов осаждаемого сообщения среди элементов документа для защиты права интеллектуальной собственности на него. Это позволило более полно сформулировать требования к разработке математической модели стеганографической систем, определить понятные логические связи между информационными процессами, происходящими в такой системе, и структурой самой системы. Кроме того, в этот же период были разработаны теоретические основы новых методов текстовой стеганографии, основанных на модификации некоторых пространственно-геометрических (апрош, кернинг) и цветовых параметров символов текста при осаждении тайной информации в текстовый документ-контейнер, которая может быть использована для защиты авторских прав на такой документ.

За 2019 год исполнителями НИР в соответствии с техническим заданием выполнены в запланированном объеме исследования в двух взаимосвязанных направлениях:

– развиты теоретические основы компьютерной стеганографии для приложений-контейнеров в виде текстов, электронных таблиц, web-приложений и графически объектов, созданных на основе языков разметки семейства XML;

– разработана математическая модель стеганографической системы на основе стеганоконтейнеров в виде электронных книг формата EPUB;

– разработаны новые эффективные методы и алгоритмы стеганографического осаждения/извлечения данных, позволяющие сохранять целостность

информации и защищать от взлома приложения-контейнеры на основе форматов *XML* и *EPUB* при их конвертации в компьютерных системах.

В 2020 году:

– разработаны новые элементы прикладной теории компьютерной стеганографии для стеганоконтейнеров в виде текстов, электронных таблиц, web-приложений и графических объектов на основе XHTML-формата;

– на основе предложенной методики оценки стойкости текстовых стеганоконтейнеров к взлому, основанной на анализе системных свойств и параметров файла-контейнера при проведении манипуляций над ними (такие манипуляции отождествляются с операцией стеганографического осаждения информации), исследованы более 200 указанных параметров и свойств;

– разработаны и зарегистрированы в государственном реестре информационных ресурсов РБ 2 компьютерные программы.

Далее в отчете излагаются основные результаты выполненных в рамках данной НИР исследований.

Рецензия

на выполненную НИР ГБ 19-105 «Разработать стеганографические методы передачи информации в XML-документах, программные средства для реализации этих методов и методику оценки стойкости стеганоконтейнеров к взлому» (ГР №20192461), ГПНИ «Информатика, космос и безопасность; подпрограмма «Информатика и космические исследования» (задание 1.2.12, н. рук. П.П. Урбанович)

В рамках рецензируемой НИР разработаны (2019-2020 гг.) основы компьютерной стеганографии для стеганоконтейнеров в виде текстов, электронных таблиц, web-приложений и графических объектов на основе XML-формата. Основой разработанных стеганографических методов является общая особенность всех языков разметки, состоящая в том, что они перемешивают текст документа с инструкциями разметки в потоке данных или файле.

Новизна и сущность метода защиты электронных карт заключается во внедрении тайной информации в виде дополнительных точек в описания пространственных объектов в виде фигур, изображений и текстовых фрагментов;

Новизна и сущность метода защиты электронных книг основана на внедрении тайной информации в три типа контейнеров при использовании трех различных стеганографических ключей.

Научная значимость метода зашиты электронных географических карт основана на том, что описания геометрических фигур позволяют использовать среди прочего точки, линии, многоугольники и кривые Безье, что позволяет обеспечить целостность и подтверждение авторства электронных карт, загружаемых в базу данных, причем любое изменение, вносимое в атрибутивные столбцы либо в описания пространственных фигур, приводит к нарушению стеганографической метки.

Считаю, что НИР «Разработать стеганографические методы передачи информации в XML-документах, программные средства для реализации этих методов и методику оценки стойкости стеганоконтейнеров к взлому» государственной программы научных исследований «Информатика, космос и безопасность» следует признать выполненной в полном объеме, в установленный срок и принятой.

Рецензент:
заведующий кафедрой
информатики и веб-дизайна БГТУ
доцент, к.т.н Д. М. Романенко