(Устройство автоматизации). Первый поток находится между пользователем и управляющей системой – в нем передаются команды пользователя программной платформе, на которой реализован умный дом. Второй - между управляющей системой и конечными устройствами автоматизации. К слабому звену можно так же отнести: открытость для внешнего доступа («торчание в интернет», передачу данных во внешние облачные хранилища), беспроводное общение между устройствами.

Чтобы обезопасить экосистему умного дома, необходимо в первую очередь повысить защищенность всех описанных выше слабых звеньев. К числу таких методов можно отнести: выбор безопасного протокола передачи данных – Zig-Bee, Z-Wave; реагирование на физическое вмешательство, которое может создать аномальное состояние; аутентификацию на стороне конечного устройства.

К особенностям нашего подхода к защите умного дома нужно отнести и использование специализированных устройств, называемых «защищенные шлюзы». Они обеспечивают контроль доступа, маршрутизацию трафика, аутентификацию пользователей, мониторинг и обнаружение взломов. Также защищенные шлюзы могут иметь функцию бэкапа и восстановления системы.

В заключение можно сказать, что защита устройств умного дома от киберугроз является важной задачей, которой необходимо уделить должное внимание. Пользователи должны соблюдать базовые меры по обеспечению безопасности, а производители должны уделять внимание безопасности на всех этапах разработки и выпуска смарт-устройств. По-нашему мнению, в сфере IoT, безопасность – основной сдерживающий фактор [1].

Список литературы

1. Kanev A.N., Nasteka A.V., Bessonova C.E. Automation Device Authentication at «Smart Home» // Vestnik policii. 2016. Vol. 7, iss. 1.

ПЕРЕДАЧА ТЕКСТОВОЙ ИНФОРМАЦИИ НА ОСНОВЕ ИЗМЕНЕНИЯ АПРОША С ИСПОЛЬЗОВАНИЕМ ОСОБЕННОСТЕЙ ФОРМАТА XML

Н.П. Шутько

Учреждение образования «Белорусский государственный технологический университет», г. Минск, Беларусь

Стеганография − это метод передачи информации с помощью скрытого текста, изображений или звука. Ранее автором был рассмотрен алгоритм встраивания секретной информации засчет модификации такого исходного пространственного параметра как апрош, т. е. изменения расстояния между соседними буквами или другими шрифтовыми знаками [1]. Апрош – это альтернативный способ записи слов, который может использоваться для создания скрытых сообщений в тексте. При таком методе стеганографии скрытые сообщения могут быть переданы тайно и незаметно для посторонних.

Как известно, формат *.docx представляет собой архив, содержащий файлы в формате *.xml. Дальнейший интерес представляет более детальное изучение тегов, которые формируют содержание данных файлов. В частности, содержимое файла document.xml, который описывает контент рассматриваемого документа, а также стили, которые к нему применяются.

При модификации апроша символа документа, созданного с помощью текстового процессора MS Word, соответствующее значение будет записано в указанный выше документ в теге <w:spacing/>. Так, например, разреженный интервал

со значением в 1 пт будет записан как <w:spacing w:val="-20"/>. Определение отклонений от исходного значения будет служить для осаждения или извлечения тайного сообщения.

Список литературы

1. Шутько Н.П., Урбанович П.П. Особенности использовании параметров апроша в методах текстовой стеганографии // Технические средства защиты информации: тез. докл. XIX Белорусско-российской науч.-техн. конф., Минск, 8 июня 2021 г. С. 103.

АЛГОРИТМ ГЕНЕРАЦИИ ШТРИХОВЫХ ЗАЩИТНЫХ ИЗОБРАЖЕНИЙ ПО ЗАДАННОМУ КЛЮЧУ

А.Н. Щербакова, Д.М. Романенко

Учреждение образования «Белорусский государственный технологический университет», г. Минск, Беларусь

При формировании изображений с защитой следует исходить из вида изображения и возможности его декодирования. Следует учитывать, что векторные изображения при их воспроизведении имеют определенные ограничения по типу линий, их цветности, передаваемой частоте. Однако с точки зрения кодирования в цифровом виде наложенные ограничения снимаются, что позволяет представить достаточно большое количество вариантов кодирования различных знаков.

Кодирование авторской информации в векторных изображениях может осуществляться в виде набора линий или простых геометрических фигур с разными параметрами (тип линии, толщина линии, цвет линии, расстояние между линиями).

Защита любых документов строится на внедрении защитного ключа. Каждому набору линий ставится в соответствие определенный символ. Также особенностью векторных изображений с внедренной защитой является их цветность.

Для генерации штрихового изображения по ключу первым шагом необходимо задать размеры изображения по горизонтали и вертикали и выбрать фоновый цвет. Далее ввести ключ. Каждый символ включает в себя свой набор параметров для кодирования. К этим параметрам относятся: количество линий, цвет линии, толщина линии, тип линии, схема штрихования линии. Тип линии может быть либо сплошной, либо штриховой. При выборе штрихового типа есть возможность настроить схему штрихования, задавая длину штриха и пробела. Если будет задано нечетное количество значений, то список значений будет повторяться. После необходимо ввести открытый текст, который и будет закодирован этим ключом.

Формат ключа:

[символ] [количество линий] [цвет линии] [толщина линии] [тип линии] [схема штрихования (необязательный параметр)]

Например, необходимо закодировать текст следующего содержания: «АБВ», ключ кодирования может выглядеть следующим образом:

А 2 #ff69b4 7 1 5,5

Б 1 #ff8c00 2 0

В 4 #00ff7f 7 1 2,3

Первый параметр – сам символ, далее количество линий, цвет в формате HEX, толщина линии, следующий параметр 1 или 0: 1 указывает на штриховую линию, 0 – на сплошную. При выборе штриховой линии вводятся параметры схемы штрихования.

В результате можно получить уникальное защитное изображение, которое будет содержать в себе авторский текст.