УДК 004.415.24:004.056.5

ЗАЩИТА ИНФОРМАЦИИ С ОГРАНИЧЕННЫМ ДОСТУПОМ МЕТОДАМИ КОМПЬЮТЕРНОЙ СТЕГАНОГРАФИИ

Ковальчук С. О., Крыжановская О. Л., Чудинова Н. В., ЛГУ БЖД, г. Львов, Украина
Кухарская Н. П., ЛГУ БЖД, доцент, канд. физ.-мат. наук, доцент

В последние десятилетие человечество вступило в новую фазу своего развития, для которой характерны популяризация информационных технологий и их стремительная интеграция практически во все области человеческой деятельности. Благодаря информационным технологиям возможна мгновенная передача и обмен различными видами информации (текст, изображения, аудио и видеоданные) между пользователями глобальной и корпоративных сетей. Не исключено, передаваемая информация может быть секретного характера, например, обновляемые ежедневно, пароли доступа. Понятно, что в случае передачи информационного сообщения ограниченного доступа по открытым каналам возникает опасность его перехвата. В связи с этим, особое внимание службами безопасности информации, в том числе структурных подразделении Государственной службы Украины по чрезвычайным ситуациям, должно уделяться созданию информационных систем, защищенных от угроз.

Еще в древности выделилось два основных направления защиты информационных ресурсов: криптография и стеганография. Криптография блокирует несанкционированный доступ к данным путем их шифрования. Стеганография же идет принципиально далее – ее цель скрыть сам факт существования конфиденциальной информации.

Хотя стеганография имеет очень длинную и богатую историю, но только в последнее время в связи с бурным развитием информационных технологий, в частности с появлением компьютерных сетей, а также из-за чрезвычайной актуальности проблемы защиты интеллектуальной собственности и наличия в некоторых странах ограничений на использование криптосредств, она становится объектом растущего интереса и активных научных исследований.

Предмет изучения цифровой стеганографии – нового направления защиты информации – составляют стеганографические методы, которые скрывают информацию в потоках оцифрованных сигналов посредством использования компьютерной техники и программного обеспечения в рамках отдельных вычислительных систем, корпоративных или глобальных сетей. Скрытие одной информации в другой производится таким образом, чтобы, во-первых, не были утрачены свойства и некоторая ценность скрываемой информации, а во-вторых, чтобы неизбежная модификация информационного носителя, не только не уничтожила его смысловые функции, но даже, на определенном уровне абстракции, не меняла их. Тогда сам факт передачи одного сообщения внутри другого не будет выявлен традиционными методами.

В компьютерной стеганографии в качестве носителя скрытой информации (контейнера) выступает объект (файл), допускающий искажения собственной информации, не нарушающие его функциональность. Современные стегосистемы обычно используют файлы изображений или звуковые файлы. Такие контейнеры обладают большой избыточностью и, кроме того, обычно велики по размеру, обеспечивая достаточно места для скрытия простого или форматированного текста.

Нами разработано ряд стеганопрограмм, которые допускают использование в качестве носителя скрытой информации графические файлы формата BMP, аудиофайлы формата WAV и текстовые файлы. Скрываемое сообщение может быть простым набором чисел, изображением, обыкновенным или зашифрованным текстом.

ЛИТЕРАТУРА

1. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – К. : МК-Пресс, 2006. – 249 с.