УДК 372.862

Изучение стеганографических методов защиты информации

Пасюков Александр Андреевич
Приамурский государственный университет имени Шолом-Алейхема
Студент

Аннотация
В статье описаны программы для ознакомления студентов направления «информационные системы и технологии» защите информации от несанкционированного доступа и хищения методом стеганографии в целях дальнейшего развития и совершенствования данной науки.
Ключевые слова: стеганография, криптография, программа, контейнер, защита информации.

Study of information steganography methods

Abstract
This article describes the program to introduce students of the direction «Information systems and technologies» protect information from unauthorized access and theft of the method of steganography, in order to further development and improvement of the science.
Keywords: steganography, cryptography, software, container, data protection.

Задача обеспечения защиты информации от несанкционированного доступа была актуальна во все времена. В современном обществе, когда информационные технологии проникают во все сферы жизнедеятельности человека, науку, бизнес стоит вопрос обеспечения защиты информации от угроз неправомерного использования хищения или уничтожения.

Одним из способов информационной безопасности является защита с помощью стеганографии. Стеганография в отличие от криптографии скрывает сам факт существования информации, которую необходимо защитить от вмешательства посторонних лиц. Скрываемая информация встраивается в некий контейнер, который располагается в безобидном файле. Это может быть речь, изображение, видео и аудио записи, не привлекающие особого внимания, которые открыто передаются адресату. Нужную информацию может извлечь только получатель.

Стеганографией в образовании занимались многие российские и зарубежные исследователи. Д.А.Коноваленко, Р.И.Баженов [1] рассмотрели разработку лабораторно-практических работ по стеганографии в курсе «Информационная безопасность». А.Н.Земцов описал стеганографические алгоритмы в электронном. А.П.Алексеев [3] провел анализ изучения стеганографии в Поволжском государственном университете телекоммуникация и информатики. О.Б.Макаревич [4] рассмотрел важные

аспекты учебного процесса на кафедре безопасности информационных технологий. В.В.Орлов [5] описал изучение стеганографии на уроках информатики. Г.М.Чернокнижный, Е.В.Черток, А.П.Бахрушин показали изучение методов защиты [6-10]. S.Stanev [11, 12] описал систему преподавания стеганографии в Болгарии и сделал обзор стеганографии как защиты информации.

Цифровая стеганография сравнительно молодая наука, требуется дальнейшее ее развитие. Для решения этой задачи необходимо совершенствовать подготовку молодых специалистов – бакалавров по направлению информационные системы и технологии в области информационной безопасности. В целях ознакомления студентов с защитой информации с помощью стеганографии следует использовать три бесплатные программы FoxSecret, ImageSpyer и FreeFileCamouflage.

Для демонстрации встраивания информации в аудио файлы формата mp3 будет использоваться программа FoxSecret. Она скрывает файлы любого формата в графических файлах формата: png, gpeg, tiff, аудио файлах формата:wav и mp3, и текстовых файлах формата txt, rtf и html. Для шифрования программа использует симметричные алгоритмы шифрования blowfish, RC5, IDEA, AES32, ГОСТ 28147-89, 3Way и ассиметричный алгоритм RSA. Интерфейс интуитивно понятен, для выбора контейнера требуется воспользоваться меню «Секрет», после чего выбрать нужный тип файла и при переходе на следующую страницу в открывшемся окне выбрать формат контейнера (рис. 1).

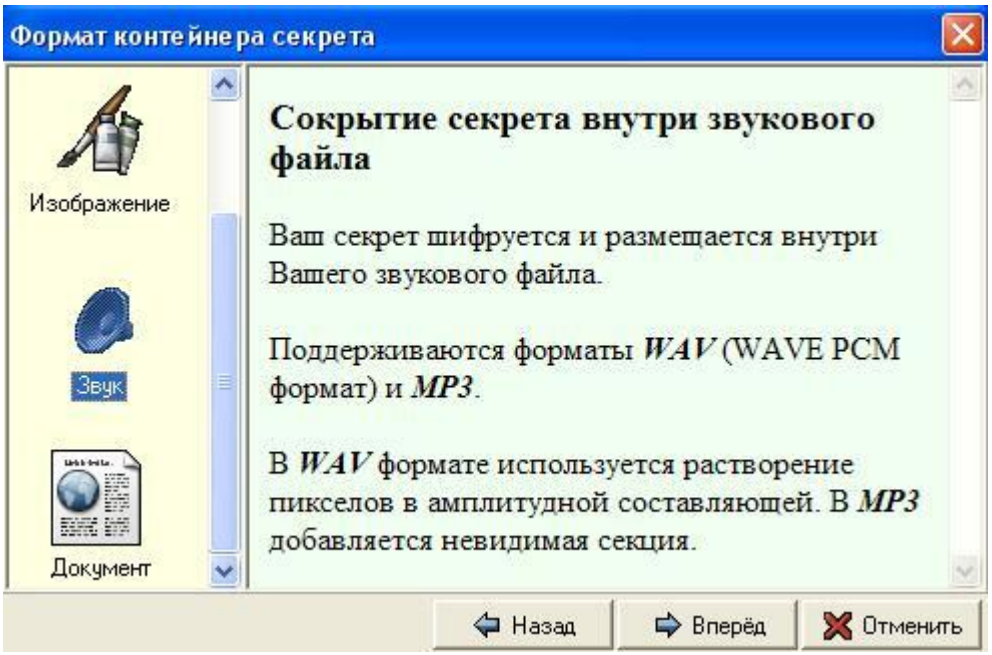

Рисунок 1 - Окно выбора формата файла

После выбора файла для контейнера следует задать ему пароль шифрования и ввкладке «настройка» выбрать нужный способ шифрования (Рис 2). Потом требуется выбрать файл, который нужно защитить и после нажатия кнопки «вперед» выбранный файл будет помещен в контейнер.

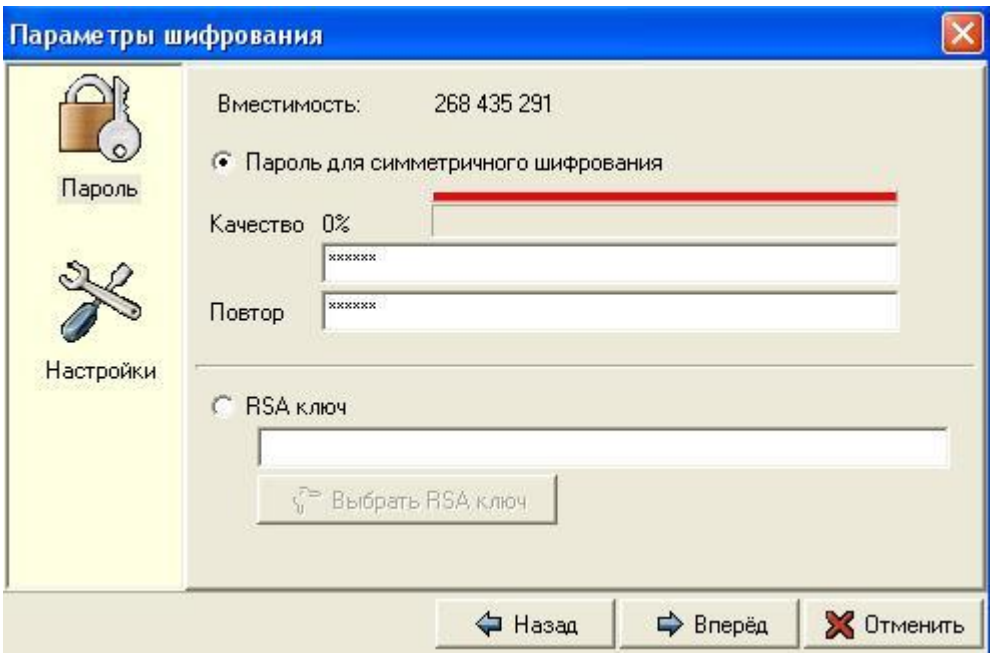

Рисунок 2 - Окно настройки и ввода пароля

Для расшифровки скрытой информации требуется в программе воспользоваться меню «Секрет», выбрать функцию «открыть» и указать файл с защищенной информацией. Откроется окно, где программа запросит ввод пароля и после ввода его в выбранном месте сохранится извлеченный файл (Рис 3).

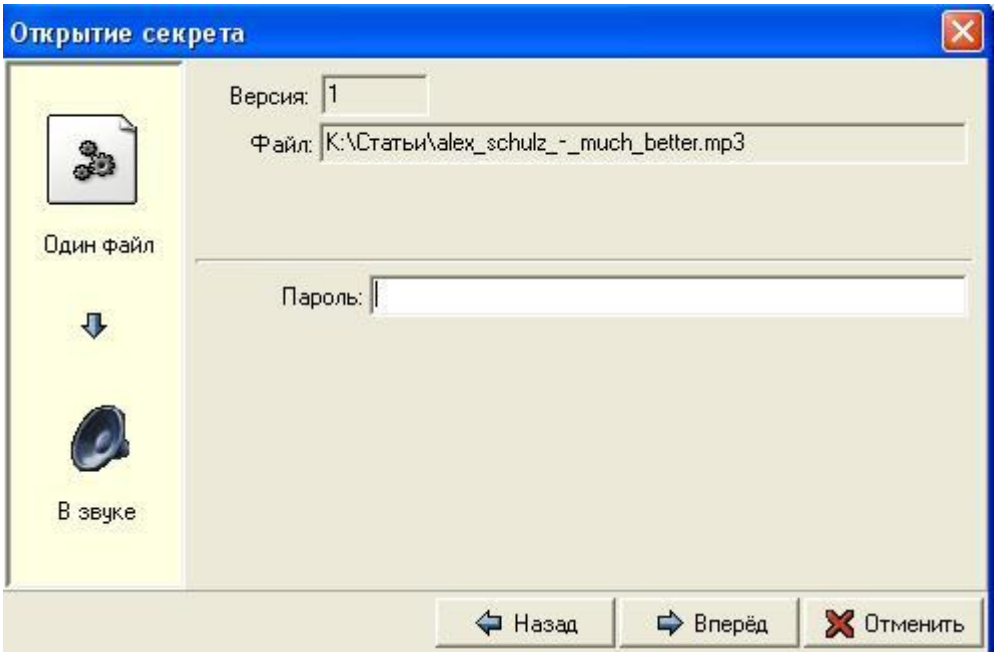

Рисунок 3 - Окно извлечения скрытой информации

Для демонстрации внедрения скрытой информации в изображение формата bmp выбрана программа ImageSpyer. Она скрывает информацию в изображениях форматов bmp и tiff. Благодаря методам современной стеганографии информация может быть зашифрована тридцатью разными

алгоритмами шифрования и при помощи более двадцати хеш-функций позволяет добиться надежного шифрования контейнера. Для начала работы программы следует загрузить файл нажатием кнопки «Load» и затем в открывшемся окне выбрать нужный файл. Перейдя по кнопке «Setup» можно перейти в настройки и выбрать нужный способ шифрования, а также задать требуемый формат ключа. Для внедрения другого файла в выбранное изображение требуется после нажатия кнопки «Flash» выбрать файл любого формата, после чего потребуется ввести ключ контейнера и пароль ввода данных, а также выбрать формат и имя сохраняемого файла. Для извлечения скрытой информации требуется загрузить файл в данную программу и после нажатия кнопки «Catch» ввести пароль контейнера и ввода данных, после чего выбрать место сохранения скрытой информации (Рис - 4).

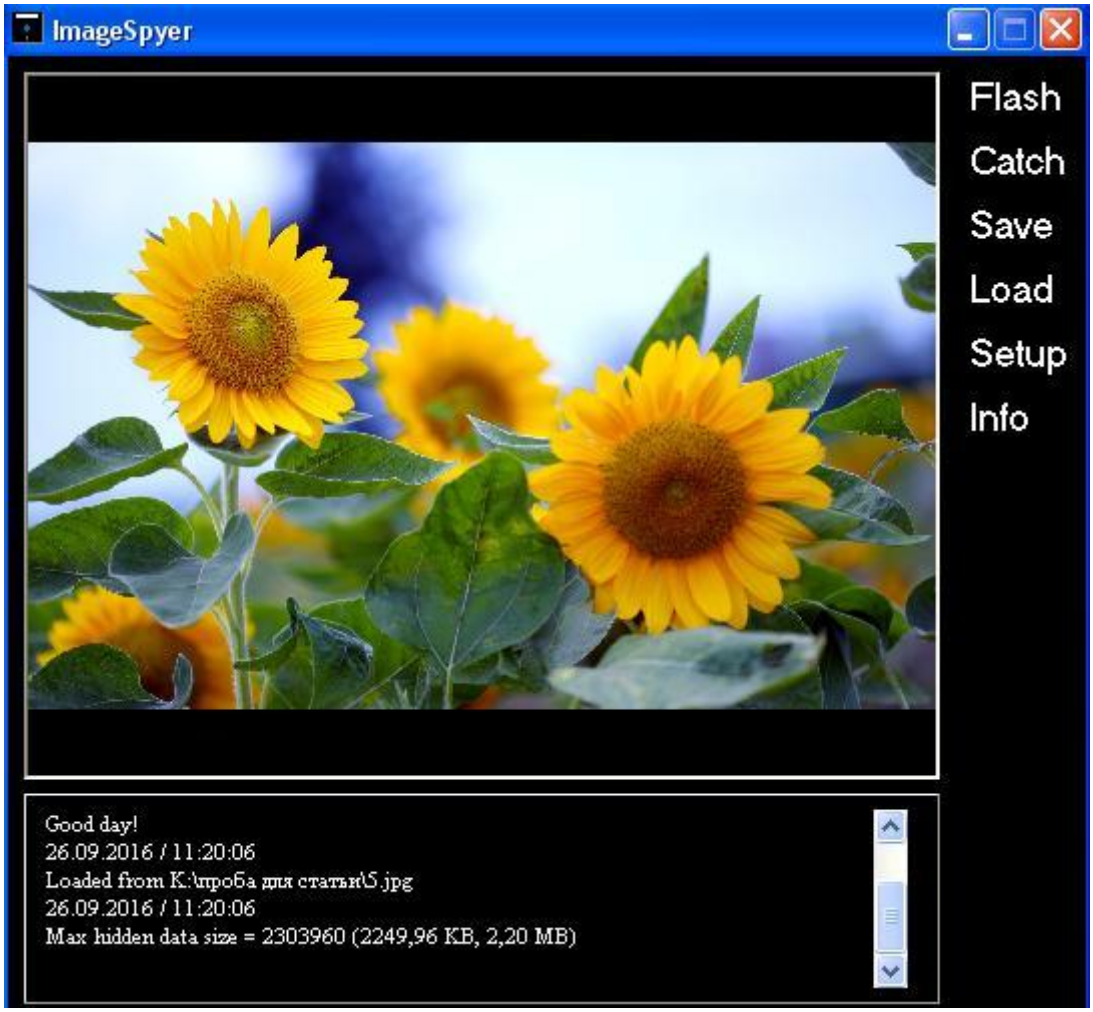

Рисунок 4 - Внешний вид программы ImageSpyer

Еще одна программа для демонстрации скрытия информации, но уже в изображениях форматаjpeg – программа Free File Camouflage. Хранимые в контейнере файлы скрыты внутри изображения и защищены от любого взлома. Огромным плюсом программы является ее маленький объем и то, что программа не требует установки. В отличие от других программ Free File Camouflage не имеет сложного алгоритма встраивания информации в

изображения, она добавляет их в конце выбранного файла. Для начала работы программы следует загрузить в строку «File to hide» файл любого формата, который требуется скрыть и в строку «Jpeg image» файл для контейнера формата jpg (Рис - 5).

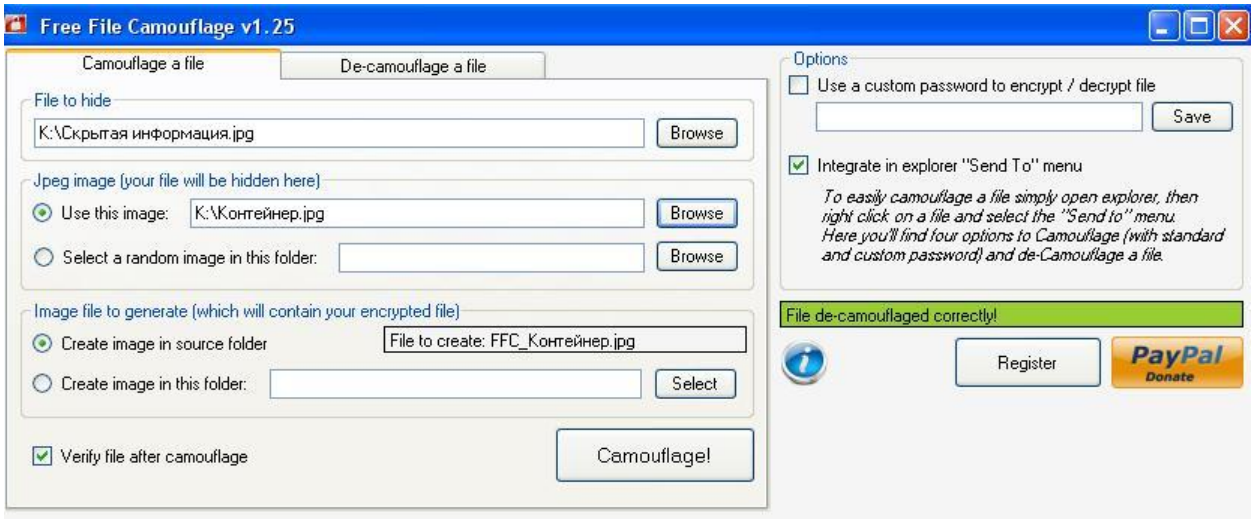

Рисунок 5 - Окно шифрования программы FreeFileCamouflage

Для расшифровки информации требуется перейти на вкладку «De-camouflage a file», в строке «Jpeg image to de-camouflage» требуется указать файл для расшифровки и в строке «Destination directory – save decrypted file to» выбрать место сохранения. После чего в указанном месте сохранится уже извлеченная информация (Рис.6).

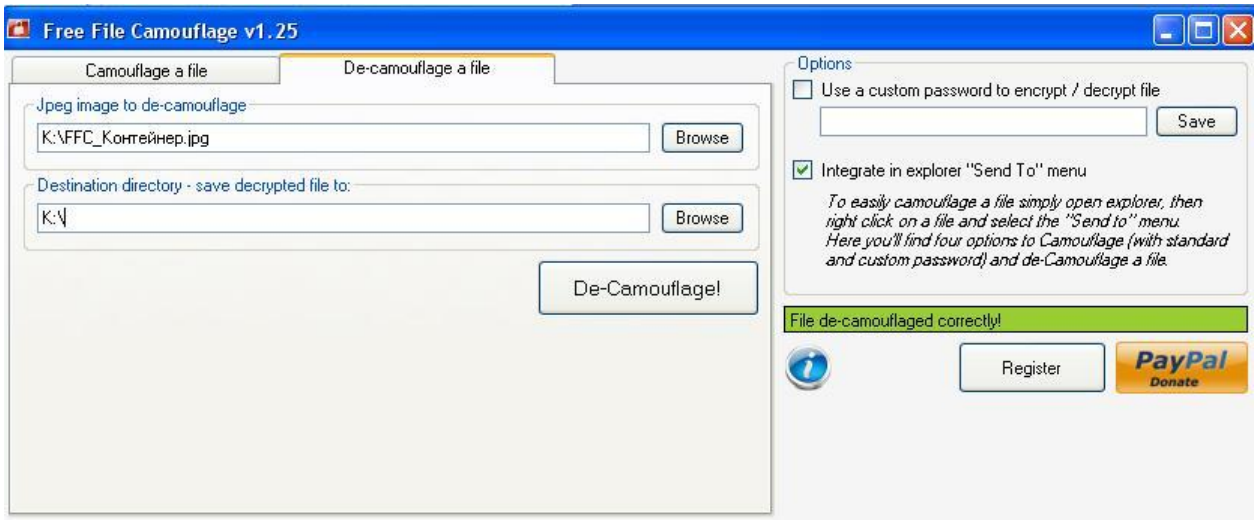

Рисунок 6 - Окно расшифровки скрытой информации программы FreeFileCamouflage

Выше описанные программы помогут студентам ознакомиться с основами стеганографии. Освоив эти программы, студент узнает, как работает стеганография, ее преимущества над криптографией. Это может заинтересовать студентов и привлечь их к дальнейшему углублённому изучению этой науки.

Благодарности.

Выражаю благодарность научному руководителю Р.И.Баженову в помощь в подготовке статьи.

Библиографический список

1. Коноваленко Д.А., Баженов Р.И. Разработка лабораторно-практических работ по стеганографическим и криптографическим методам защиты информации в курсе «Информационная безопасность» // Современная педагогика. 2014. № 11 (24). С. 27-33.
2. Земцов А.Н. Стеганографические алгоритмы в электронном обучении // Информационные технологии. Радиоэлектроника. Телекоммуникации. 2012. Т. 2. № 2. С. 112-118.
3. Алексеев А.П. Изучение криптографии и стеганографии в поволжском государственном университете телекоммуникаций и информатики. URL: http://info.fmi.shu-bg.net/skin/pfiles/12.pdf (дата обращения 03.10.2016)
4. Макаревич О.Б. Основные направления научных разработок кафедры бит ТТИ ЮФУ и их внедрение в НИОКР и учебный процесс // Известия ЮФУ. Технические науки. 2008. №8.
5. Алексеев А.П., Орлов В.В., Сухова Е.Н. Изучение стеганографии на уроках информатики // Информатика и образование. 2007. №8. С. 65-71
6. Чернокнижный Г.М. Лабораторные практикумы по сетевым дисциплинам информационной безопасности // Информационное противодействие угрозам терроризма. 2015. Т. 1. № 25. С. 403-408.
7. Черток А.В., Черток Е.В. Анализ уязвимостей локальной сети и разработка рекомендаций по их устранению // Вопросы защиты информации. 2015. № 3 (110). С. 55-61.
8. Бахрушин А.П. Применение методов спектрального анализа при обработке зашумленных изображений // Вестник Приамурского государственного университета им. Шолом-Алейхема. 2011. № 2. С. 5-17.
9. Бондаренко В.В., Козич В.Г., Бахрушин А.П. Создание программы для защиты информации водяными знаками // Постулат. 2016. № 7 (9). С. 13.
10. Бахрушин А.П., Бахрушина Г.И., Баженов Р.И., Цой Р.И. Использование фазо-частотного спектра при разработке алгоритма защиты изображений, устойчивого к геометрическим атакам // Телекоммуникации. 2015. № 4. С. 25-32.
11. Stanev S., Szczypiorski K. Steganography Training: a Case Study from University of Shumen in Bulgaria // Intl journal of electronics and telecommunications, 2016, vol. 62, no. 3, pp. 315-318
12. Stanev S. Steganological protection of information. Konstantin: Preslavski University Press, Shumen, 2013. 320 p.