

Министерство образования Республики Беларусь
Учреждение образования «Барановичский государственный университет»
Студенческое научное общество БарГУ

СОДРУЖЕСТВО НАУК. БАРАНОВИЧИ-2016

Материалы XII Международной
научно-практической конференции
молодых исследователей

(Барановичи, 19—20 мая 2016 года)

В трёх частях

Часть 2

Барановичи
БарГУ
2016

В части 2 сборника материалов XII Международной научно-практической конференции молодых исследователей «Содружество наук. Барановичи-2016» представлены результаты исследований в области физики и математики, а также рассмотрены актуальные проблемы в области информационных систем и технологий в образовании, науке и технике. Особое внимание уделено современным тенденциям в технологиях и материалах машиностроительного и сельскохозяйственного производств, а также экономическим аспектам развития предприятия, региона.

Сборник адресован научным работникам, аспирантам, магистрантам и студентам инженерных и экономических специальностей учреждений высшего образования.

Редакционная коллегия:

А. В. Никишова (гл. ред.), Ю. Е. Горбач, В. Н. Кременевская (отв. секретари), Е. Н. Кирюхова,
О. И. Наранович, А. К. Гавриленя, М. В. Нерода, В. Н. Познякевич, Г. Я. Житкевич

Рецензент

кандидат технических наук, заведующий лабораторией механофизики гетерогенных систем
Государственного научного учреждения «Физико-технический институт
Национальной академии наук» А. М. Милюкова

Научное издание

СОДРУЖЕСТВО НАУК.
БАРАНОВИЧИ-2016

Материалы XII Международной
научно-практической конференции
молодых исследователей

(Барановичи, 19—20 мая 2016 года)

На русском, белорусском, английском языках

В трёх частях

Часть 2

Ответственный за выпуск Е. Г. Хохол
Технический редактор А. Ю. Сидоренко
Компьютерная вёрстка С. М. Глушак
Корректор Н. Н. Колодко

Подписано в печать 04.10.2016. Формат 60 × 84 ¹/₈. Бумага ксероксная.

Отпечатано на копировально-множительной технике. Усл. печ. л. 28,00. Уч.-изд. л. 25,10. Тираж 9 экз. Заказ 681.

Учреждение образования «Барановичский государственный университет».
Свидетельство о государственной регистрации издателя № 1/424 от 09.09.2016.
Ул. Войкова, 21, 225404 г. Барановичи. Тел. 8 (0163) 45 46 28, e-mail: rio@barsu.by .

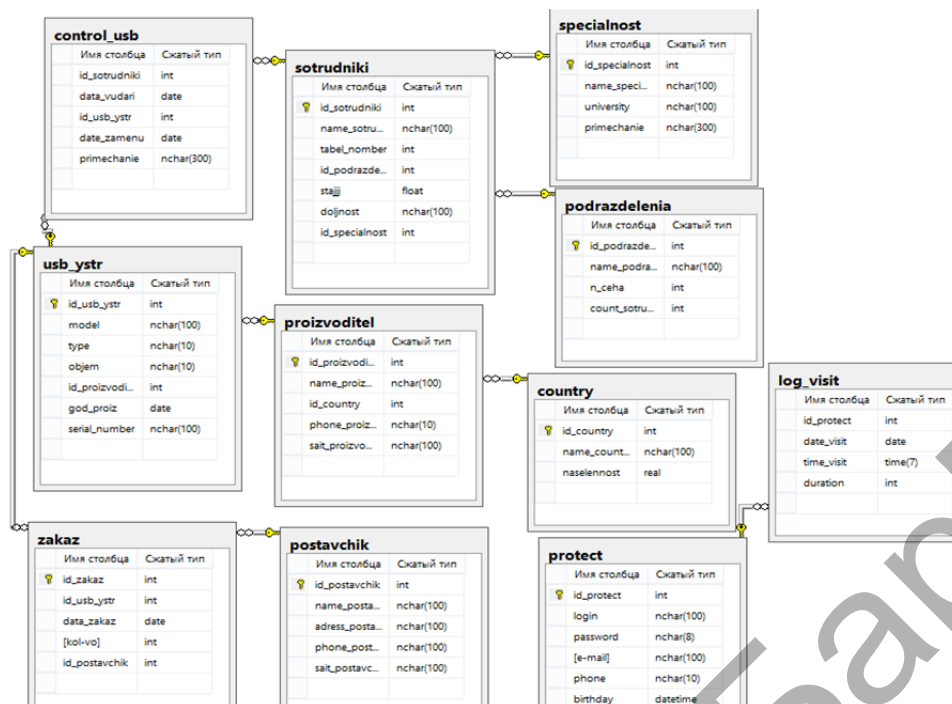


Рисунок 2 — Физическая модель базы данных

Заключение. Внедрение системы повысит работоспособность сотрудника, сократит поиск информации, необходимой для ведения учёта USB-носителей.

Список цитируемых источников

1. Онлайн-журнал о саморазвитии . URL: <http://selfdevelop.ru/compute/kompyuter-v-zhizni-cheloveka.htm> (дата обращения: 14.03.2016).
2. Microsoft Developer Network. URL: <https://msdn.microsoft.com/ru-ru> (дата обращения: 14.03.2016).
3. Microsoft Developer Network. URL: <https://msdn.microsoft.com/ru-ru> (дата обращения: 14.03.2016).

УДК 004.056.5

А. В. Гаврон, А. С. Рогозник

Учреждение образования «Барановичский государственный университет», Барановичи

СИСТЕМЫ СОКРЫТИЯ И ШИФРОВАНИЯ ИНФОРМАЦИИ. СТЕГАНОГРАФИЯ

Введение. Стеганография — это область знаний, которая занимается вопросами скрытой передачи информации. Стеганография (гр. steganos секрет, тайна и graphy запись) буквально означает «тайнопись» [1]. В отличие от криптографии, скрывается сам факт передачи информации. Наибольший эффект от использования стеганографических методов достигается при использовании их совместно с криптографическими. Стеганографические методы и алгоритмы заключаются в том, что информация встраивается в какой-либо объект, а далее открыто передаётся адресату. Встроенное сообщение никак не отражается на основном объекте и не привлекает внимания. Цель работы заключается в сокрытии информации и предотвращении её утечки третьим лицам.

Основная часть. Программа вшивает текстовые данные в контейнер для дальнейшей передачи.

Алгоритм работает следующим образом (для изображения типа Bitmap, расширение BMP) [2]:

1. Текст преобразуется в массив типа byte[];
2. Открывается очередной пиксель изображения;
3. Определяется цветовая маска RGB для пикселя;
4. Каждый канал добавляется в массив бит (Bits);
5. В каждый из цветовых потоков добавляется по биту шифруемого текста;

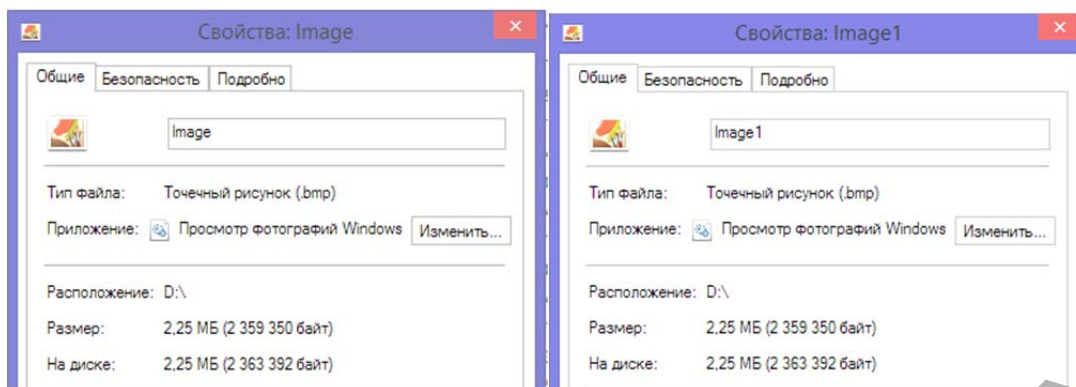


Рисунок 1 — Размеры файлов

207C30: 02 22 BB 0C 2C C5 09 0F . " » . , E . .	207C30: 02 22 BB 0C 2C C5 0C 0B . " » . , E . .
207C38: 52 03 09 4C 00 05 48 00 R . . L . . H .	207C38: 51 03 09 4C 00 05 48 00 Q . . L . . H .
208830: 03 23 BC 0D 2D C6 09 0F . # j . - X . .	208830: 03 23 BC 0D 2D C6 0E 0D . # j . - X . .
208838: 52 03 09 4C 00 05 48 00 R . . L . . H .	208838: 50 03 09 4C 00 05 48 00 P . . L . . H .
209430: 03 23 BC 0D 2D C6 09 0F . # j . - X . .	209430: 03 23 BC 0D 2D C6 0E 0D . # j . - X . .
209438: 52 03 09 4C 00 05 48 00 R . . L . . H .	209438: 50 03 09 4C 00 05 48 00 P . . L . . H .

Рисунок 2 — Различия в файлах

6. Преобразованный пиксель сохраняется;
7. Преобразования продолжают, пока весь текст не будет добавлен в изображение.

Для восстановления информации производятся обратные действия:

1. Открывается очередной пиксель изображения;
2. Определяется цветовая маска RGB для пикселя;
3. Из битов (Bits) цветового потока синтезируется символ (пока тоже в формате бита);
4. Биты преобразуются в номер (int) и добавляются в контейнер;
5. Поиск продолжается до нахождения определённой последовательности символов;
6. После завершения операции данные из массива конвертируются в последовательность байт (byte[]);
7. Массив байт преобразуется в текст кодировки UTF8.

Для видеофайлов формата Audio Video Interleave (AVI) производятся дополнительные подготовительные действия перед шифрованием:

1. Иницируется видеопоток;
2. Открывается кадр, и определяются его характеристики;
3. Выбирается изображение, в которое будет добавляться информация;
4. Кадр закрывается;
5. Выполняется основной алгоритм.

После работы алгоритма размер контейнера не изменяется (рисунок 1). Слева — размер оригинального файла, справа — размер файла после работы алгоритма.

Различия можно найти при сравнении файлов в hex-редакторе (рисунок 2).

Заключение. В данной работе был продемонстрирован метод, позволяющий защитить данные (секретную переписку и т. д.) от несанкционированного доступа к ней третьих лиц. Для улучшения приватности передаваемой информации предварительно она может быть зашифрована любым криптографическим методом.

Список цитируемых источников

1. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. М. : МК-Пресс, 2006. 288 с.
2. Там же.