**Практическая работа**

**«Работа с программами шифрования»**

ЦЕЛИ РАБОТЫ:

1. Сделать обзор программ шифрования.

2. Получить навыки работы с методами шифрования информации с помощью различных программ.

ОБОРУДОВАНИЕ: ПК, Windows 10, Интернет.

ВРЕМЯ ВЫПОЛНЕНИЯ: 45 минут

КРАТКАЯ ТЕОРИЯ И МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ:

Криптографические методы зашиты информации в автоматизированных системах могут применяться как для зашиты информации, обрабатываемой в ЭВМ или хранящейся в различного типа ЗУ, так и для закрытия информации, передаваемой между различными элементами системы по линиям связи. Криптографическое преобразование как метод предупреждения несанкционированного доступа к информации имеет многовековую историю. В настоящее время разработано большое количество различных методов шифрования, созданы теоретические и практические основы их применения. Подавляющие число этих методов может быть успешно использовано и для закрытия информации.

Почему проблема использования криптографических методов в информационных системах (ИС) стала в настоящий момент особо актуальна?

С одной стороны, расширилось использование компьютерных сетей, в частности глобальной сети Интернет, по которым передаются большие объемы информации государственного, военного, коммерческого и частного характера, не допускающего возможность доступа к ней посторонних лиц.

С другой стороны, появление новых мощных компьютеров, технологий сетевых и нейронных вычислений сделало возможным дискредитацию криптографических систем, еще недавно считавшихся практически не раскрываемыми.

Проблемой зашиты информации путем ее преобразования занимается криптология (kryptos — тайный, logos — наука). Криптология разделяется на два направления — крип-тографию и крипгпоанализ. Цели этих направлений прямо противоположны.

Криптография занимается поиском и исследованием математических методов пре-образования информации. Это сокрытие смысла сообщения по средствам шифрования и раскрытие его по средствам расшифровки.

Сфера интересов криптоанализа — исследование возможности расшифровывания информации без знания ключей.

Итак, криптография дает возможность преобразовать информацию таким образом, что ее прочтение (восстановление) возможно только при знании ключа.

Ключ — информация, необходимая для беспрепятственного шифрования и дешифрирования текстов.

Современная криптография включает в себя четыре крупных раздела:

1. Симметричные криптосистемы.

2. Криптосистемы с открытым ключом

3. Системы электронной подписи.

4. Управление ключами.

Основные направления использования криптографических методов — передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений, хранение информации (документов, баз данных) на носителях в зашифрованном виде.

Криптографические методы зашиты информации в автоматизированных системах могут применяться как для защиты информации, обрабатываемой в ЭВМ или хранящейся в различного типа ЗУ, так и для закрытия информации, передаваемой между различными элементами системы по линиям связи. Криптографическое преобразование как метод пре-дупреждения несанкционированного доступа к информации имеет многовековую исто-рию. В настоящее время разработано большое количество различных методов шифрова-ния, созданы теоретические и практические основы их применения. Подавляющие число этих методов может быть успешно использовано и для закрытия информации.

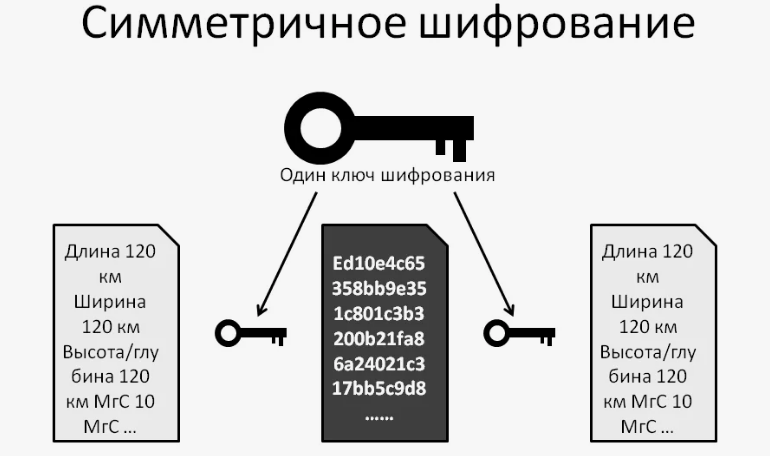
*ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ И ФОРМА ОТЧЕТНОСТИ:*

**Задание 1. Понятие шифрование и дешифрование.**

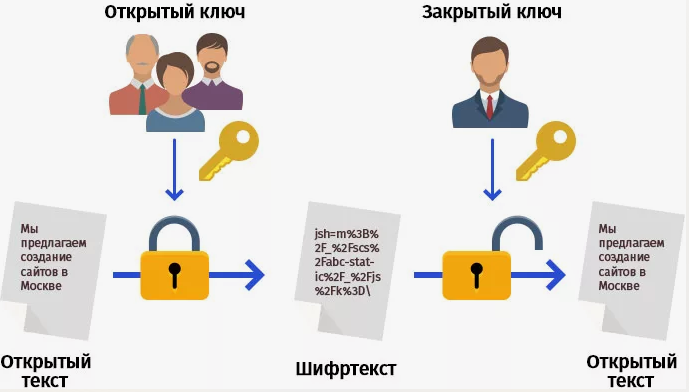
Шифрование — это процесс преобразования данных обычного текста при помощи ключа (открытого текста) в то, что, как представляется, является случайным и бессмысленным (шифр). Дешифрование — это процесс преобразования зашифрованного текста при помощи ключа обратно в открытый текст.

**Задание 2. Структура криптосистем.**

Симметричное шифрование ключом

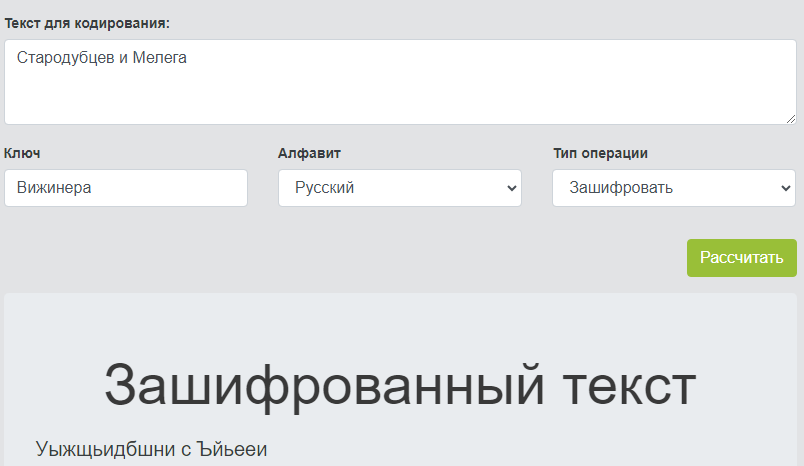


Открытым ключом

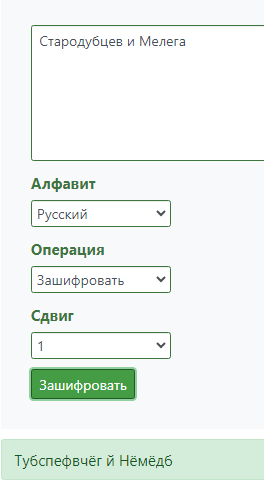


**Задание 3. Зашифровать текст в режиме онлайн с помощью шифра Вижинера, Цезаря.**

Вижинера

****

Цезаря

****

**Задание 4. Скачать и установить TrueCrypt. Назначение и описать приемы работы с программой. Удалить программу.**

|  |  |
| --- | --- |
| **Описание** | **Скриншот** |
| Зайти на сайт и скачать программу |  |
| Открываем программу и ставим галочку. Нажимаем на кнопку «Next >» |  |
| Выбираем нужный режим установки и нажимаем на кнопку «Next >» |  |
| Выбираем путь установки и устанавливаем необходимые параметры и нажимаем кнопку «Install» |  |
| Процесс установки программы |  |
| Установка завершена |  |
| После завершения установки нажимаем кнопку «Finish» |  |

|  |  |
| --- | --- |
| **Назначение** | **Программа** |
| TrueCrypt - Компьютерная программа для шифрования на «лету» для 32- и 64-разрядных операционных систем семейств Microsoft Windows NT 5 и новее (GUI-интерфейс), Linux и Mac OS X. Позволяет создавать зашифрованный логический (виртуальный) диск, хранящийся в виде файла. С помощью TrueCrypt также можно полностью зашифровать раздел жёсткого диска или иной носитель информации, например USB-флеш-накопитель. Все сохранённые данные в томе TrueCrypt полностью шифруются, включая имена файлов и каталогов. Смонтированный том TrueCrypt подобен обычному логическому диску, поэтому с ним можно работать с помощью обычных утилит проверки и дефрагментации файловой системы |  |

|  |  |
| --- | --- |
| **Описание** | **Скриншот** |
| Для шифрования файла «Create Volume» |  |
| Выбираем тип носителя, который планируем превратить в носитель «Next >» |  |
| Выбрать тип тома, нажать «Next >» |  |
| Выбираем путь создания контейнера, нажимаем «Next >» |  |
| Выбираем алгоритм шифрования и хэш алгоритм, нажимаем «Next >» |  |
| Выбираем размер тома, нажимаем «Next >» |  |
| Вводим пароль для тома, подтверждаем пароль, нажимаем «Next >» |  |
| Выбираем формат тома, нажимаем «Format», ожидаем завершения форматирования |  |
| Форматирование тома завершено, нажимаем «ОК» |  |
| Том создан, теперь можно закрыть окно или создать ещё один том |  |
| Для открытия созданного тома, выбрать путь к тому, затем необходимо нажать «Mount»  Ввести пароль от тома и нажать «ОК» |  |
| Результат проделанной работы |  |

|  |  |
| --- | --- |
| **Описание** | **Скриншот** |
| Для удаления программы необходимо зайти в «Панель управления» и перейти «Программы» |  |
| Находим «TrueCrypt», нажимаем «Удалить» |  |
| Для удаления необходимо нажать «Uninstall» |  |
| После удаления, необходимо нажать на кнопку «OK», для закрытия окна |  |

**Задание 5. Привести примеры программ шифрования.**

|  |  |  |
| --- | --- | --- |
| Название | Описание | Логотип |
| Folder Lock | Folder Lock, мощное программное обеспечение для защиты важных данных и файлов, устанавливает защиту паролем для выбранных файлов и папок на ПК с Windows. Он позволяет пользователям скрывать файлы, шифровать файлы и даже безопасно удалять файлы. |  |
| VeraCrypt | Программное обеспечение, используемое для шифрования «на лету». Это бесплатный и открытый проект, начатый 22 июня 2013 года в качестве форка TrueCrypt.  Запущен и по настоящее время поддерживается Mounir Idrassi, основателем компании IDRIX. После того как 28 мая 2014 года было объявлено о прекращении поддержки программы TrueCrypt. |  |
| AxCrypt | **AxCrypt** - программа для шифрования файлов и папок, которая предоставляет защиту файлов с помощью 128-bit или 256-bit шифрования, автоматическое шифрование своих файлов в Dropbox, Google Drive и т.д., легкое управление своими паролями, возможность другим пользователям **AxCrypt** открывать защищенные файлы с помощью своего собственного пароля и пр. |  |
| DiskCryptor | DiskCryptor — **это свободное программное обеспечение с открытым исходным кодом, предназначенное для шифрования логических дисков, внешних USB-накопителей и образов CD/DVD.**  Программа поддерживает следующие алгоритмы шифрования: AES, Twofish, Serpent, а также их комбинации.  Основные возможности DiskCryptor:  — Прозрачное шифрование дисковых разделов. — Полная поддержка динамических дисков. — Поддержка дисковых устройств с большим размером сектора. — Высокая производительность работы, сравнимая с производительностью незашифрованной системы. — Поддержка аппаратного ускорения AES. |  |
| WinRAR | Один из первых архиваторов, появившийся ещё во времена MS-DOS (одна из первых операционных систем, без графической оболочки), умеющий открывать и создавать архивы во многих форматах.  Программа WinRAR условно-бесплатная, период ознакомительного использования — 40 дней. Однако разработчики по окончании пробного периода не блокируют функционал архиватора, а лишь показывают уведомления с просьбой приобрести лицензию. Это не стало препятствием для её популярности у пользователей в России. |  |

**Задание 6. Шифрующая файловая система EFS.**

**6.1.Назначение**

Зашифрованная файловая система (EFS) обеспечивает дополнительный уровень безопасности для файлов и каталогов. Он обеспечивает криптографическую защиту отдельных файлов на томах файловой системы NTFS с помощью системы с открытым ключом.

Как правило, управления доступом к объектам файлов и каталогов, предоставляемого моделью безопасности Windows, достаточно для защиты несанкционированного доступа к конфиденциальной информации.

**6.2.Использование системы EFS для шифрования папок (Свойство папки-Общие-кнопка Другие)**

|  |  |
| --- | --- |
| Описание | Скриншоты |
| Для использования шифрования папок, необходимо нажать «Свойства» |  |
| В подпункте «Общие» необходимо нажать «Другие…» |  |
| В атрибутах сжатия и шифрования необходимо поставить галочку подпункта «Шифровать содержимое для защиты данных» |  |