**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 — метод защиты данных путем их преобразования таким образом, чтобы сообщение могли прочитать только авторизованные пользователи.

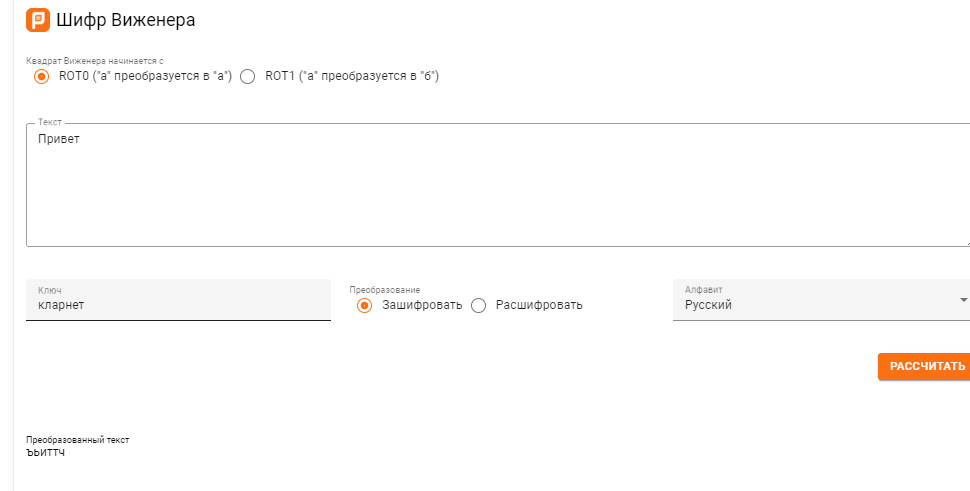
Дешифрование - это трансформация кодированного текста в простой текст при помощи криптографического алгоритма под названием шифр.

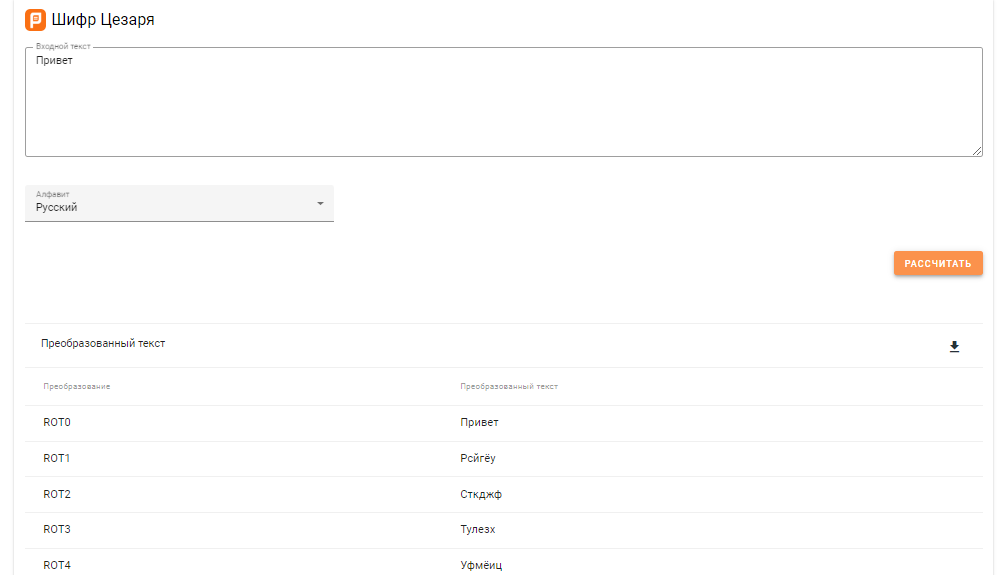
**Задание 2. Структура криптосистем.**

****



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

****

****

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

Скачивание

|  |  |
| --- | --- |
| Шаг | Фото |
| №1 Заходим на сайт установки |  |
| №2 Принимаем условия |  |
| №3 Нажимаем Install |  |
| №4 Выбираем путь установки |  |
| №5 Ждем установки |  |
| №6 Программа установлена |  |

**Назначение**

TrueCrypt — это программной обеспечение, позволяющее создавать виртуальный зашифрованный логический диск, хранящийся в файловой системе как файл. Все записываемые данные на этот диск, включая имена файлов и каталогов «шифруются на лету». Так же существуют возможность полностью зашифровать разделы жесткого диска или usb носителя. Смонтированный раздел идентичен обычному логическому диску или съемному накопителю, что дает возможность работать с ним всеми утилитами, встроенными в операционную систему, таких как проверка диска и дефрагментация.

**Пример работы**

Работаем с зашифрованным диском

Ну вот, теперь мы можем работать с нашим новым файлом.

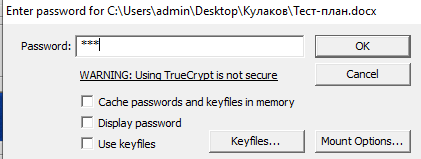
Шаг 1 - выбираем на своё усмотрение букву для диска. Например "Q".



Шаг 2 - нажимаем "Select file", находим наш файл и жмём "ОК".



Шаг 3 - нажимаем кнопку "Mount" и через несколько секунд в проводнике можно будет найти появившийся новый виртуальный диск. Всё. Программу можно свернуть и пользоваться новым диском по назначению.



Шаг 4 - По окончании работы снова открываем программу и кнопкой "Dismount All" отключаем от системы наш виртуальный диск, после чего программу можно закрыть.

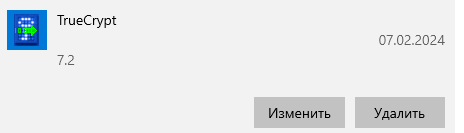


**Удаление программы**

В поиск пишем удаление программы

****

Выбираем программу для удаления

****

Программа удалена

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

|  |  |  |
| --- | --- | --- |
| **Название** | **Фото** | **Описание** |
| Cryptomator |  | это программа для шифрования, разработанная для приватного хранения файлов в любом облачном хранилище. Программа может создавать хранилища в виртуальном диске, содержимое которых зашифровано и синхронизировано с твоим облачным хранилищем |
| Picocrypt |  | это маленькая и простая программа, предоставляющая современное шифрование. Picocrypt использует безопасный шифр XChaCha20 и функцию формирования ключа Argon2id для обеспечения высокого уровня безопасности. Для функций шифрования он использует стандартные модули Go x/crypto. |
| VeraCrypt |  | это свободно распространяемая утилита с исходным кодом, используемая для шифрования "на лету". Программа может создавать виртуальный зашифрованный диск в файле, зашифровать логический раздел или даже зашифровать все устройство с предзагрузочной аутентификацией. |
| BitLocker |  | решение для полного шифрования диска в Microsoft Windows. |
| FileVaul |  | это решение для шифрования томов "на лету", встроенное в macOS. FileVault рекомендуется, поскольку он использует аппаратные возможности безопасности, представленные в SoC процессорах Apple или чипе безопасности T2. |

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

**6.1. Назначение**

Шифрованная файловая система КриптоПро EFS – это базовая технология шифрования, которая позволяет шифровать и восстанавливать файлы, хранящиеся на томах с файловой системой NTFS.

Средство КриптоПро EFS предназначено для обеспечения конфиденциальности и контроля целостности информации при ее хранении.

Технология шифрования данных, предоставляемая КриптоПро EFS, может быть применена как к отдельным файлам, так и ко всем файлам в директории или на диске.

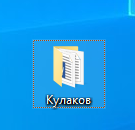
Файлы, зашифрованные с использованием КриптоПро EFS, невозможно расшифровать без соответствующего ключа. Зашифрованные файлы будут защищены даже в том случае, если злоумышленник получит физический доступ к компьютеру. Кроме того, к файлам, зашифрованным с помощью КриптоПро EFS, не будут иметь доступа даже те пользователи, которым дано право управления компьютером (например, администраторы).

Тем не менее, КриптоПро EFS предоставляет возможность восстановления данных при помощи агентов восстановления. При правильной настройке агентов восстановления можно гарантировать восстановление данных при необходимости.

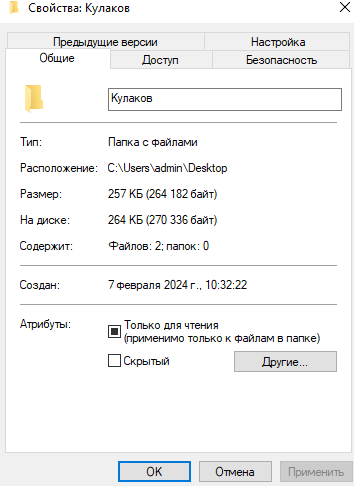
Файловая система КриптоПро EFS интегрирована в NTFS и отличается простотой управления и стойкостью к атакам.

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

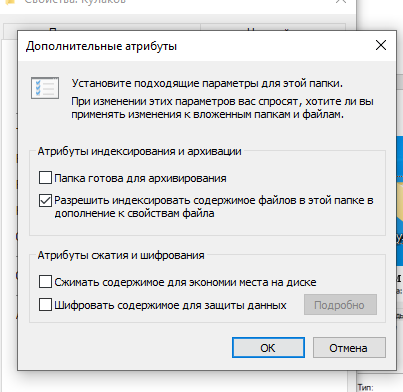
Выбираем папку



Заходим в свойства папки



Нажимаем на кнопку другие



Ставим галочку и нажимаем «Ок»

