**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.

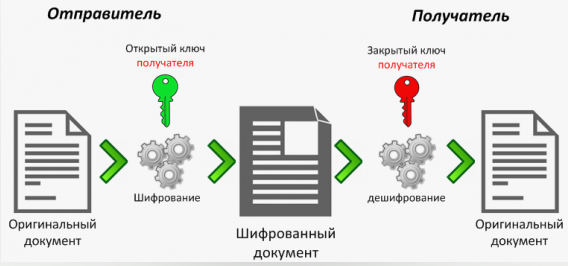
*ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ И ФОРМА ОТЧЕТНОСТИ:*

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

Шифрование - это процесс преобразования обычного текста в набор символов (шифр), который невозможно понять без специального ключа. Это помогает обезопасить данные от несанкционированного доступа или прочтения.

Дешифрование - обратный процесс, при котором зашифрованный текст преобразуется обратно в исходную форму с использованием специального ключа. Только тот, кто обладает ключом, может успешно дешифровать информацию.

**Задание 2. Структура криптосистем.**

****



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

**Шифр Вижинера:**

|  |  |  |
| --- | --- | --- |
|  | **Зашифровка** | **Расшифровка** |
| **Шифр Виженера** |  |  |
| **Шифр Цезаря** |  |  |

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

|  |  |
| --- | --- |
| Переходим на сайт [TrueCrypt — Скачать (softonic.ru)](https://truecrypt.softonic.ru/) и скачиваем ПО |  |
| Подтверждаем и жмем далее |  |
| Выбираем тип установки и жмем далее |  |
| Выбираем путь и жмем установить |  |
| Приложение установлено жмем ok и жмем finish |  |
| **Прием работы** | |
| Первое, что потребуется сделать — создать том, нажмите соответствующую кнопку. |  |
| Выбираем «зашифрованный файловый контейнер» и жмем далее. |  |
| Выпираем путь где будет находиться том и жмем далее |  |
| Следующим этапом будет задание размера зашифрованного тома, в зависимости от того, какой объем файлов вы планируете хранить в секрете. |  |
| Нажмите «Далее» и вас попросят ввести пароль и подтверждение пароля на том. Если вы хотите действительно защитить файлы, следуйте рекомендациям, которые вы увидите в окне, там все подробно описано. |  |
| На этапе форматирования тома вам предложат перемещать мышь по окну для генерации случайных данных, которые помогут увеличить стойкость шифрования. Кроме этого, вы можете задать файловую систему тома (например, для хранения файлов больше 4 Гб следует выбрать NTFS). После того, как это сделано, нажмите «Разметить», подождите немного, а после того, как увидите, что том был создан, выйдите из мастера создания томов TrueCrypt. |  |
| Следующий шаг — смонтировать зашифрованный том в системе. В главном окне TrueCrypt выберите букву диска, которая будет присвоена зашифрованному хранилищу и, нажав «Файл» укажите путь к файлу .tc, который вы создавали ранее. Нажмите кнопку «Смонтировать», а затем укажите пароль, который вы устанавливали. |  |
| После этого, смонтированный том отразится в главном окне TrueCrypt, а если вы откроете проводник или «Мой компьютер», вы увидите там новый диск, который и представляет ваш зашифрованный том. |  |
| **Удаление** | |
| Заходим в панель управления выбираем пункт удаление программ |  |
| Выбираем приложение и жмем удалить далее подтверждаем |  |

TrueCrypt — это программа для шифрования с открытым исходным кодом.

Основное назначение программы — создание зашифрованных контейнеров для хранения файлов в защищённом виде. В последних версиях утилиты контейнеры могут даже монтироваться как диски Windows.

Основные возможности программы:

* создание виртуального зашифрованного диска в виде файла-контейнера, который монтируется в системе как обычный диск;
* шифрование целого раздела как на жёстком диске, так и на USB-накопителе;
* шифрование системы Windows «на лету» с предзагрузочной аутентификацией;
* поддержка скрытых и неидентифицируемых томов;
* поддержка различных алгоритмов шифрования, а также каскадного шифрования различными шифрами.

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

|  |  |
| --- | --- |
| **Название** | **Назначение** |
| **VeraCrypt** | форк проекта TrueCrypt с дополнительными функциями и улучшенной безопасностью. |
| **PGP (Pretty Good Privacy)** | программное обеспечение для шифрования электронной почты и файлов. |
| **AES Crypt** | простой инструмент для шифрования файлов с использованием алгоритма AES. |
| **GnuPG (GNU Privacy Guard)** | программа для шифрования и подписи данных, доступная на различных платформах. |
| **BitLocker** | интегрированная программа шифрования диска в операционной системе Windows. |

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

**6.1.Назначение**

Шифрующая файловая система (EFS) – это функция операционных систем Windows, которая позволяет шифровать файлы и папки на уровне файловой системы, обеспечивая защиту данных на диске. Назначение EFS включает:

1. Конфиденциальность данных: EFS позволяет шифровать конфиденциальные файлы и папки, предотвращая несанкционированный доступ к ним.

2. Защита данных при утере устройства: Шифрование данных с помощью EFS обеспечивает защиту в случае утери или кражи устройства, так как несанкционированные пользователи не смогут просто прочитать шифрованные файлы.

3. Безопасность сетевых передач данных: EFS обеспечивает защиту данных, передаваемых по сети, так как файлы остаются зашифрованными даже в процессе передачи.

4. Управление доступом: EFS позволяет настраивать доступ к зашифрованным файлам и папкам, а также разрешения на их редактирование и просмотр.

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

|  |  |
| --- | --- |
| Жмем пкм по папке и выбираем свойства |  |
| Делее жмем другие |  |
| Здесь можно выбирать атрибуты индексирования и архивации а также атрибуты сжатия и шифрования |  |