**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.**

**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.**

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

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

**6.1.Назначение**

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