**Лабораторная работа № 14**

Тема: «Изучение программных продуктов защиты информации. Программа PGP»

Цель: изучение программного средства для защиты информации PGP (Pretty Good Privacy).

Порядок выполнения работы:

1. Изучить теоретический материал

2. Выполнить задания.

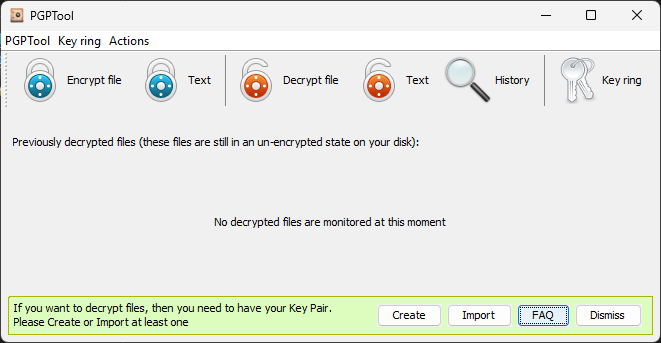
3. Ответить на контрольные вопросы.

4. Оформить отчет.

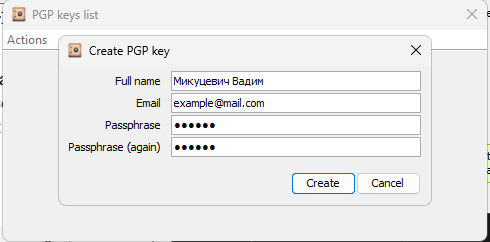
Практическая часть.

1 Ознакомиться со сведениями о программе PGP.

2 Запустить программу PGPtools (с помощью меню ПУСК или значка PGPtray на панели задач), ознакомиться и отразить в отчете о лабораторной работе состав программных средств, входящих в систему PGP (при необходимости воспользоваться справкой о системе PGP).

Рисунок 2 – Главная форма.

3. Создать криптографические ключи с помощью программы PGP-keys. Включить в отчет о лабораторной работе сведения о порядке создания ключей шифрования в системе PGP, а также копии используемых при этом экранных форм.

Рисунок 3 – Создание PGP-ключа.

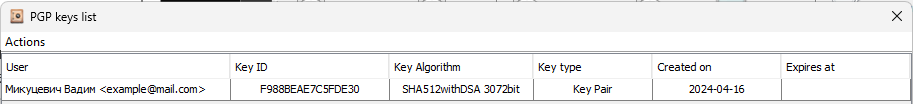
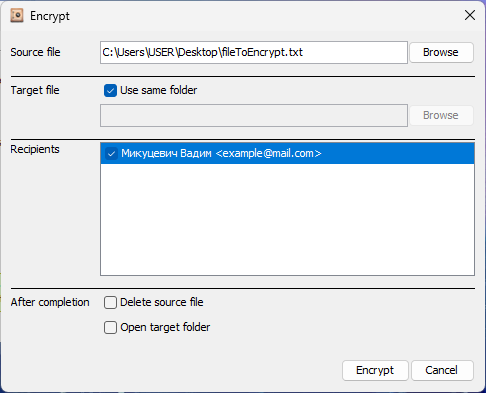


Рисунок 4 – Список PGP-ключей.

4-6. изучить (на примере обычных текстовых файлов и файлов изображений) способы шифрования и расшифрования файлов с помощью функций Encrypt и Decrypt программы PGPtools. Изучить (на примере документов из своей папки) способы получения и проверки электронной цифровой подписи под файлами с помощью функций Sign и Verify программы PGPtools.изучить способы одновременного шифрования (расшифрования) и получения (проверки) электронной цифровой подписи в систе- ме PGP с помощью функций Encrypt Sign и Decrypt/Verify программы PGPtools. Включить в отчет о лабораторной работе сведения о порядке шифрования и расшифрования файлов в системе PGP, а также копии используемых при этом экранных форм.

Рисунок 6 – Шифрование файла.

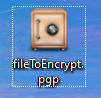


Рисунок 7 – Зашифрованный файл.

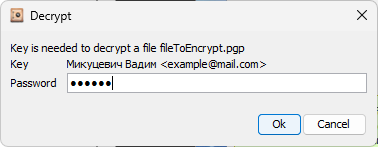


Рисунок 8 – Расшифровка файла.

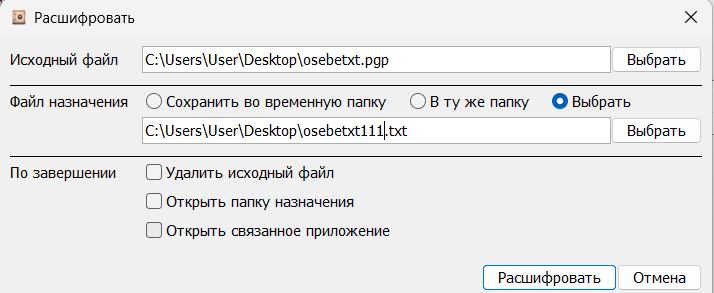


Рисунок 8 – Расшифровка файла.

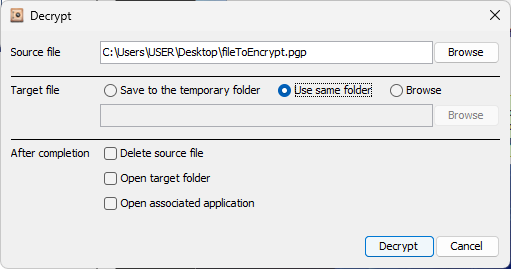
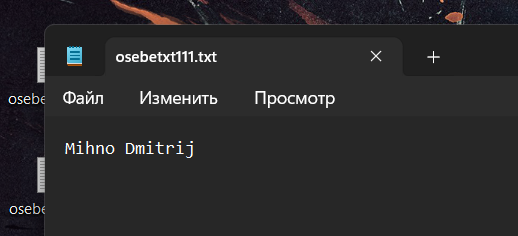
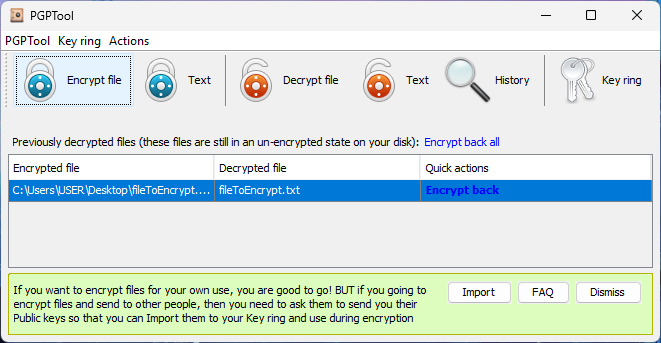
****

Рисунок 9 – Сохранение зашифрованного файла.

Рисунок 10 – Файл расшифрован.

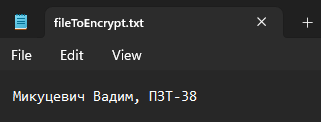


Рисунок 11 – Содержимое расшифрованного файла.

Контрольные вопросы:

1. Как выбрать длину криптографического ключа в системе PGP?

Выбор длины криптографического ключа зависит от требуемого уровня безопасности и вычислительных возможностей атакующего. В системе PGP рекомендуется использовать ключи длиной от 2048 бит для обеспечения достаточной стойкости к атакам.

2. В чем достоинства и недостатки криптографических методов защиты информации?

Достоинства: обеспечивают высокий уровень безопасности, защищают информацию от несанкционированного доступа и подмены, обеспечивают конфиденциальность и целостность данных.

Недостатки: требуют значительных вычислительных ресурсов, могут замедлить процесс обработки данных, необходимы специалисты в области криптографии для правильной реализации и настройки.

3. Какие компьютерные системы называются безопасными?

Безопасные компьютерные системы – это системы, которые обладают высоким уровнем защиты от угроз безопасности, таких как взлом, вирусы, кража данных и другие виды кибератак.

4. В чем заключаются основные требования к защищенности компьютерных систем?

Основные требования к защищенности компьютерных систем включают:

* Конфиденциальность: гарантия, что информация доступна только тем, кому она предназначена.
* Целостность: обеспечение правильности и неповрежденности информации.
* Доступность: возможность получения доступа к информации в нужный момент.
* Аутентификация: проверка подлинности пользователей и ресурсов.

5. Для выполнения каких требований к защищенности компьютерных систем могут применяться криптографические методы защиты?

Криптографические методы защиты могут применяться для обеспечения конфиденциальности и целостности информации, а также для аутентификации пользователей и ресурсов.

6. Насколько, надежны методы криптографической защиты информации, используемые в программе PGP?

Методы криптографической защиты информации, используемые в программе PGP, считаются очень надежными при правильной настройке и использовании. Они обеспечивают высокий уровень конфиденциальности и целостности данных.

7. Какими основными функциями защиты информации обладает программа PGP?

Основными функциями защиты информации в программе PGP являются шифрование, аутентификация и создание цифровой подписи.

8. Какой принцип лежит в основе функции надежного уничтожения остаточной конфиденциальной информации программы PGP?

Принцип надежного уничтожения остаточной конфиденциальной информации в программе PGP заключается в том, что данные удаляются таким образом, чтобы они не могли быть восстановлены ни с помощью обычных методов, ни с использованием специализированного программного обеспечения.