Министерство образования и науки Российской Федерации  
Государственное бюджетное образовательное учреждение высшего профессионального образования  
Российский государственный педагогический университет им. А. И. Герцена.

**Сети и телекоммуникации.**

**ЛАБОРАТОРНАЯ РАБОТА № 4.**

**ИЗУЧЕНИЕ ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ**

Выполнила

студентка 3 курса,   
ИКНИТО

Волкова А. И.

Санкт-Петербург

2017 г.

**Цель работы***-*освоение программных средств защиты информации PGP, предназначенных для:

- шифрования конфиденциальных информационных ресурсов;

- обеспечения целостности информационных ресурсов с помощью механизма;

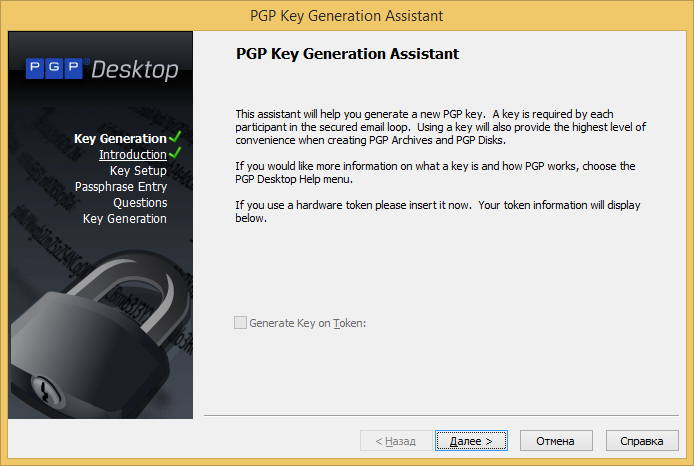
- электронной цифровой подписи;

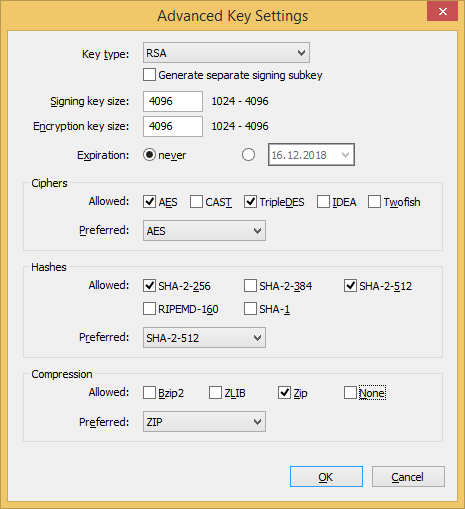
- надежного уничтожения остаточной конфиденциальной информации;

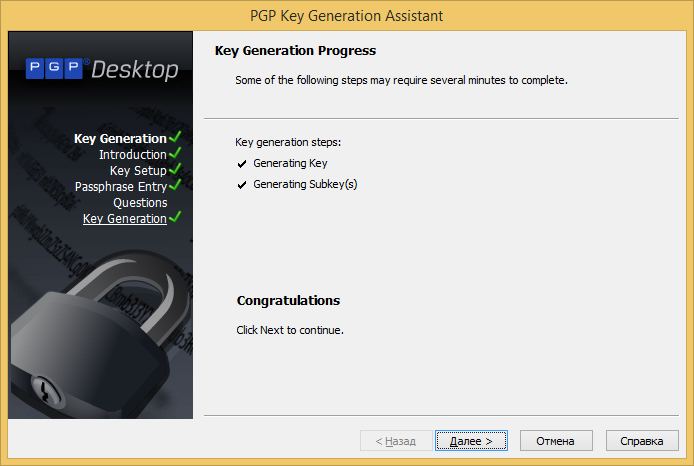
- скрытия присутствия в компьютерной системе конфиденциальной информации с помощью виртуального диска.

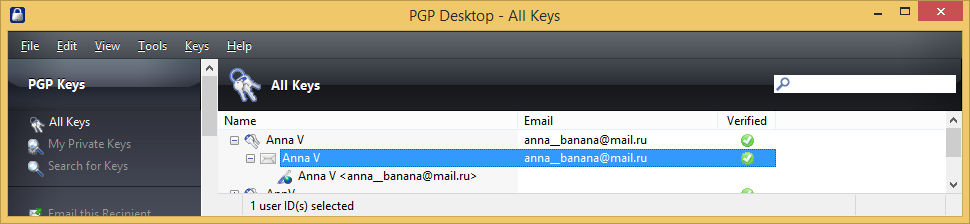
**1. PGP Keys**

***Просмотр ключей***

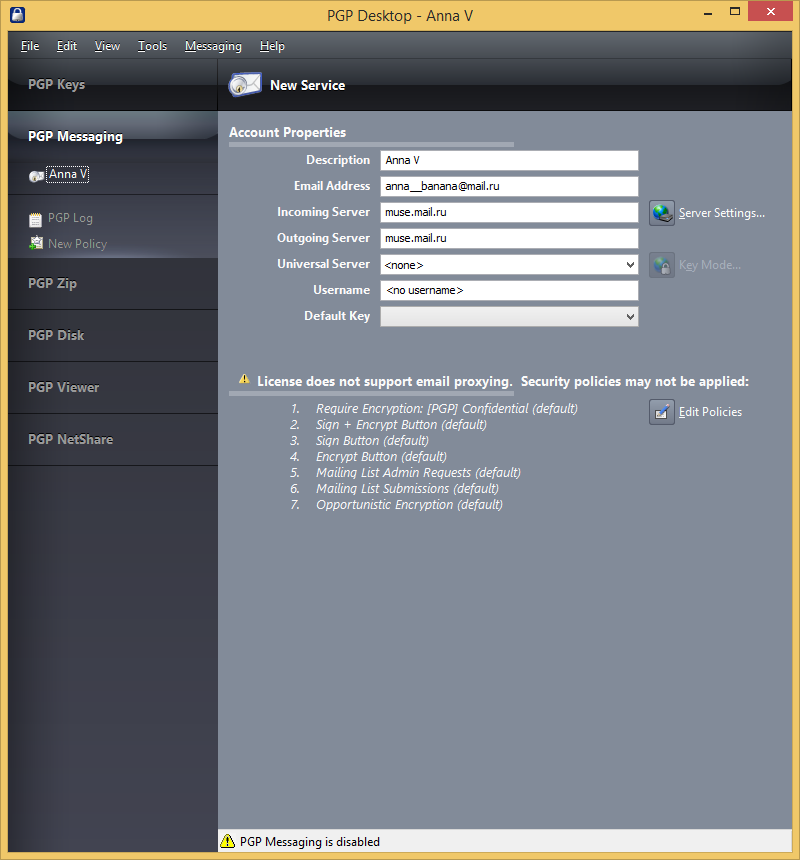


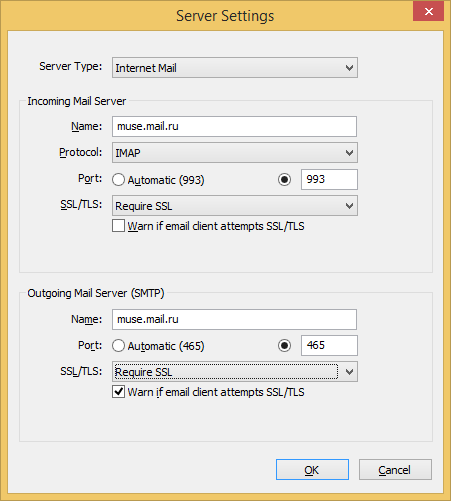


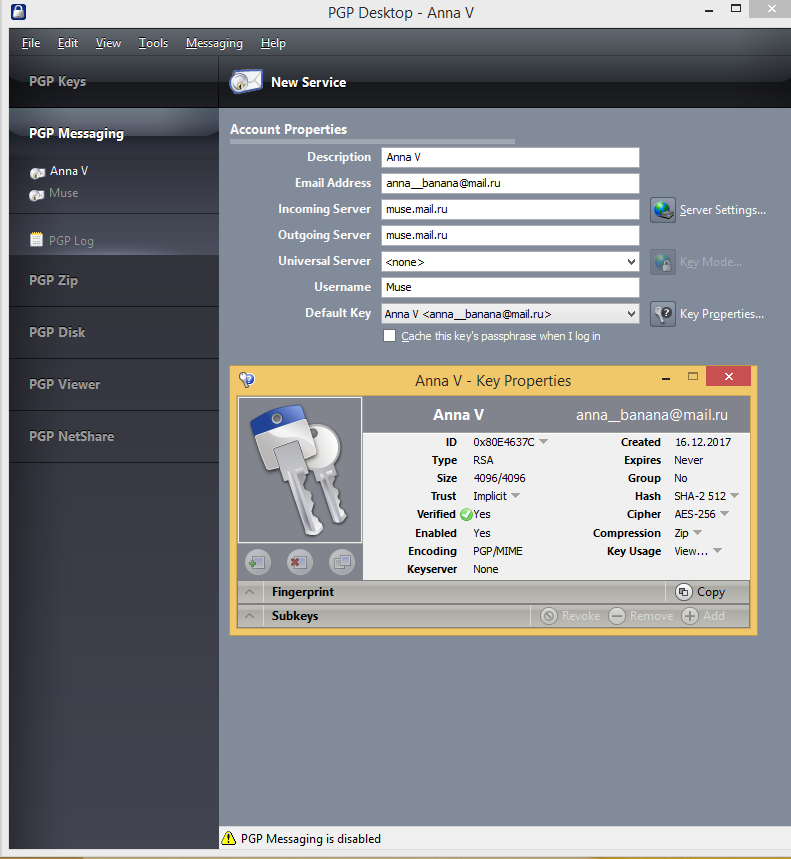




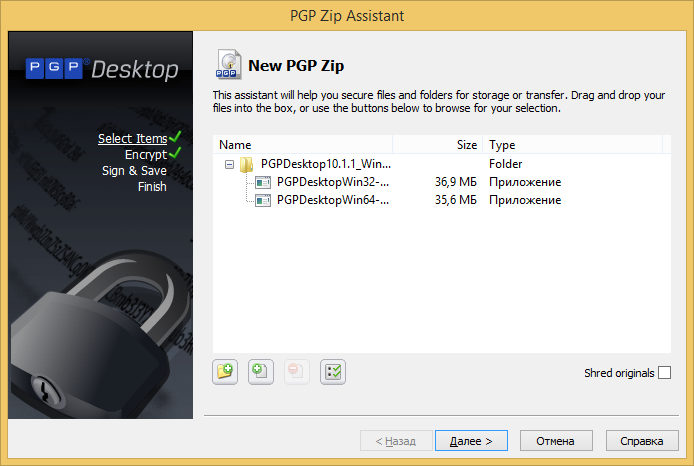
**2. PGP Messaging**

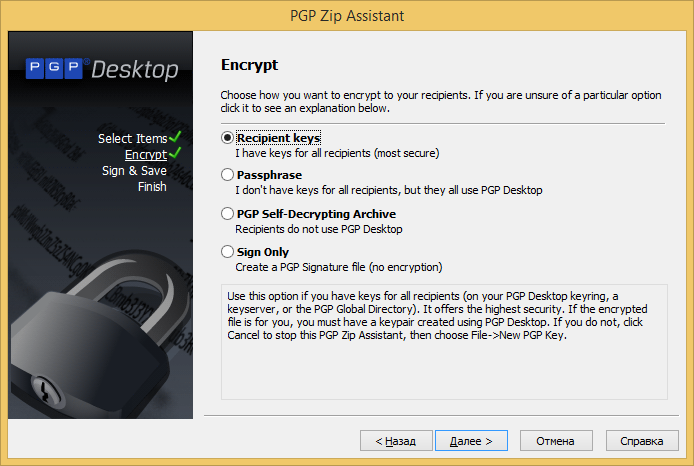
****

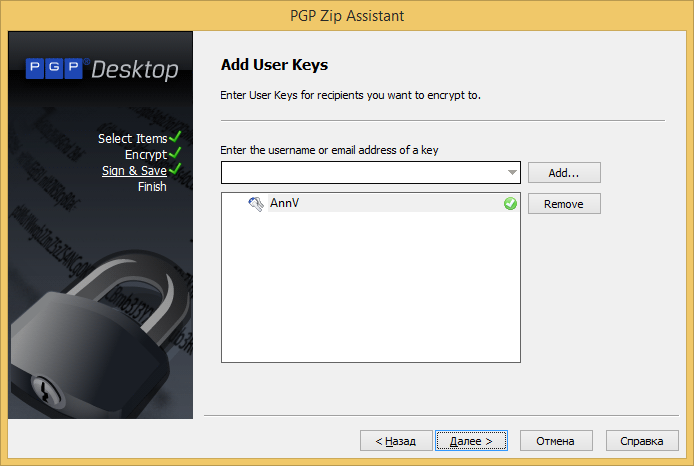


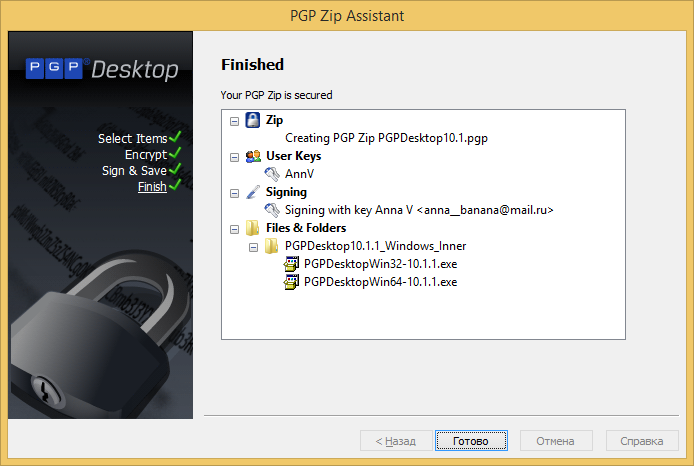


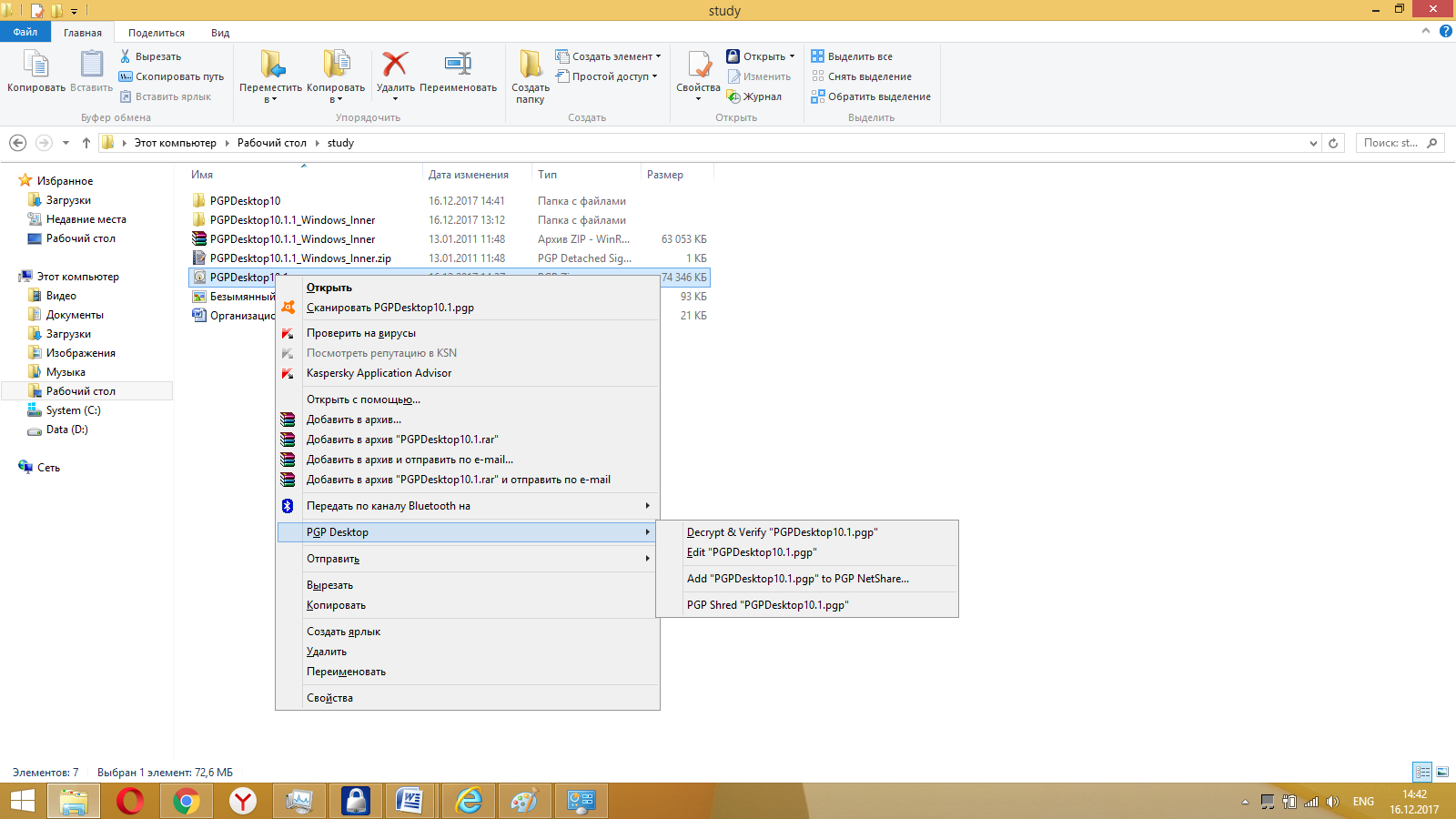
**3. PGP Zip**



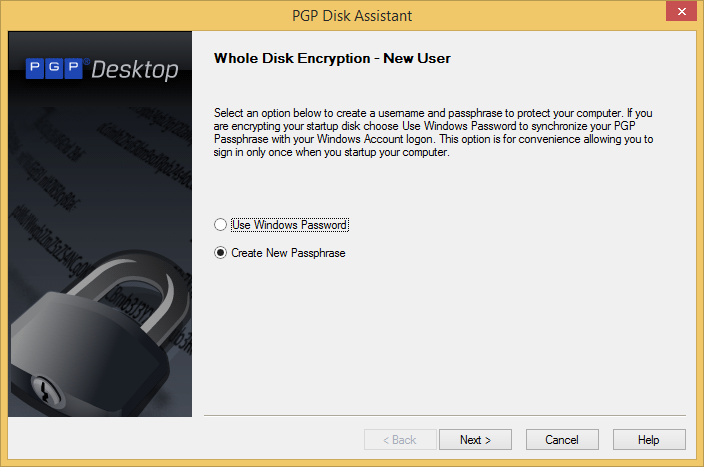








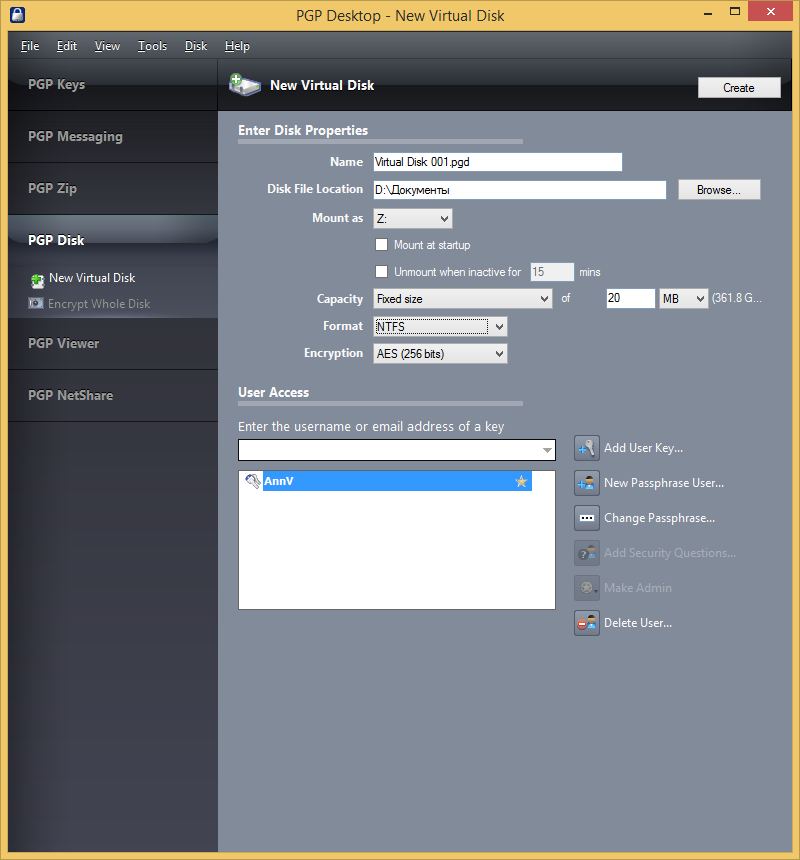
**4. PGP Whole Disk Encryption**

****





**5. Virtual Disk**



2. Программы объединены в семейство PGP Desktop (PGP Desktop EMail, PGP Whole Disk Encryption и PGP NetShare).

PGPTools - это мобильный мультиплатформенный кодер текстовых сообщений на мобильном устройстве.

3.

* **Как обеспечивается случайность выбираемых криптографических ключей в системе PGP?**

Компонент PGP, ответственный за выдачу случайных чисел, называется генератором (истинно) случайных чисел (ГСЧ), в противовес так называемым ГПСЧ, алгоритмам, генерирующим детерминированный поток, похожий на случайные данные. ГСЧ использует гибридный подход: он обращается к внешним источникам для обеспечения непредсказуемости и использует функцию хэширования, чтобы сгладить отклонения.

* **Как и где хранится секретный ключ пользователя в системе PGP?**

Ключи хранятся в виде «сертификатов ключей», которые включают в себя идентификатор пользователя владельца ключа (обычно это имя пользователя), временную метку, которая указывает время генерации пары ключей, и собственно ключи. Сертификаты секретных ключей — секретные. Каждый секретный ключ также шифруется с отдельным паролем.

* **Как может быть обеспечена в системе PGP возможность восстановления секретного ключа пользователя при его случайной потере.**

Сохранением его резервной копии.

4.

* **Какие дополнительные параметры шифрования могут быть использованы и в чем их смысл и возможное применение?**

1. Файл ключа, введите расположение файла PGP ключа, который будет использоваться для шифрования файлов. Если оставить это поле пустым, действия файла шифрования PGP используется файл, укажите в папки Keyring поля. Файлы могут иметь любое расширение имени файла, но \*.asc является стандартным.

2. Папка Keyring, введите расположение папки, содержащей keyring, который будет использоваться для шифрования файлов. Файл открытого keyring (\*.pkr) могут быть переименованы с расширением \*.gpg.

3. Пользователь, введите имя пользователя, который был указан при создании ключа шифрования. Это поле является обязательным.

4. COMMENT, введите комментарий, который был указан при создании ключа шифрования. Если это поле был завершен, когда был создан ключ шифрования, необходимо предоставить эти сведения при использовании этого действия.

5. Электронная почта, введите адрес электронной почты, который был указан при создании ключа шифрования. Это поле является обязательным.

* **Как генерируется, как и где хранится ключ симметрического шифрования файла в системе PGP?**

Генерируется ГСЧ, хранится в самом зашифрованном файле.

* **Как может быть обеспечен доступ к зашифрованному файлу со стороны других пользователей?**

Отправить свой открытый ключ на публично доступный сервер ключей, с которого этот ключ смогут получить другие пользователи.

* **Изменяется ли и как размер файла после его шифрования?**

Когда пользователь шифрует сообщение с помощью PGP, то программа сначала сжимает текст, что сокращает время на отправку сообщения.

8.

* **Какие функции по управлению криптографическими ключами пользователей предоставляет администратору программа PGP?**

С помощью команд строчного интерфейса ее пользователь может выполнять все базовые криптографические функции, а именно:

* генерацию пары из закрытого/открытого ключа;
* шифрование файла с помощью открытого ключа любого пользователя PGP (в том числе своего);
* расшифровку файла с помощью своего закрытого ключа;
* наложение цифровой подписи с помощью своего закрытого ключа на файл (аутентификация файла) или на открытый ключ другого пользователя (сертификация ключа);
* проверку (верификацию) своей подписи или подписи другого пользователя с помощью его открытого ключа.

**Какими основными функциями защиты информации обладает программа PGP?**

PGP (Pretty Good Privacy) — решает практически любые проблемы с конфиденциальной передачей данных.

Главное преимущество этой программы состоит в том, что для обмена зашифрованными сообщениями пользователям нет необходимости передавать друг другу тайные ключи т.к. эта программа построена на новом принципе работы – публичной криптографии или обмене открытыми (публичными) ключами, где пользователи могут открыто посылать друг другу свои публичные ключи с помощью сети «Интернет» и при этом не беспокоиться о возможности несанкционированного доступа каких-либо третьих лиц к их конфиденциальным сообщениям.

Контрольные вопросы:

### 1. Компоненты PGP

* PGPdisk — шифрование данных на жестких дисках;
* PGPkeys — доступ к таблице собственных ключей, а также открытых ключей корреспондентов;
* PGPmail — шифрование и дешифрование данных;
* PGPtray — шифрование и дешифрование данных в буфере обмена и управление основными приложениями PGP;
* PGPAdmin — создание криптографической системы для организации;
* PGP ICQ — шифрование текста сообщений ICQ;
* PGP Net — реализация стека протоколов IPSec (Internet Protocol Security) и IKE (Internet Key Exchange).

2. PGP использует для шифрования алгоритм с открытым ключом RSA в паре с обычным методом шифрования IDEA.

3. Для ключей RSA legacy длина ключа может составлять от 1024 до 2048 бит, а для Diffie-Hellman/DSS и RSA — от 1024 до 4096