Лабораторная работа 4

Изучение программных средств защиты информации

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

- шифрования конфиденциальных информационных ресурсов;

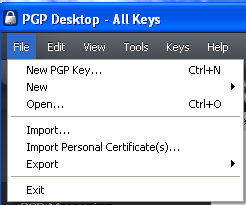
- обеспечения целостности информационных ресурсов с помощью механизма;

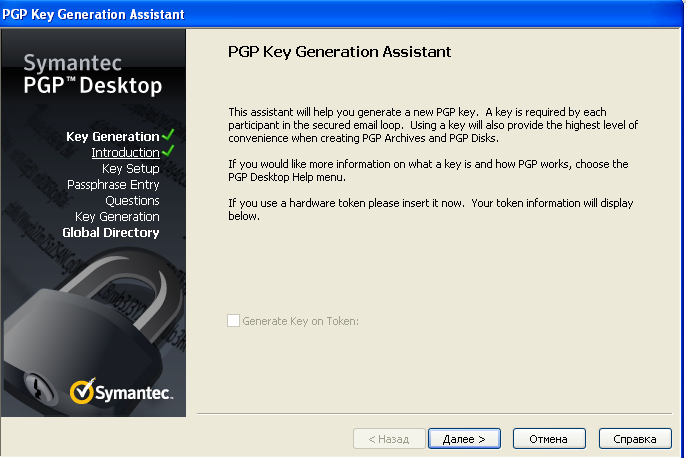
- электронной цифровой подписи;

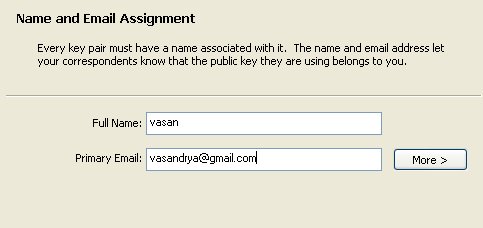
- надежного уничтожения остаточной конфиденциальной информации;

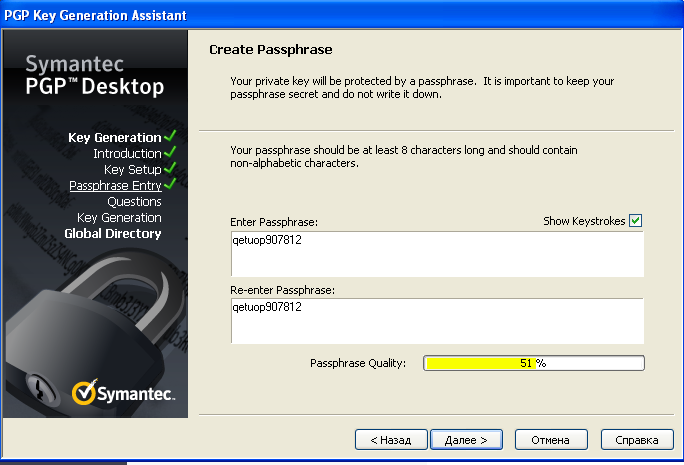
- скрытия присутствия в компьютерной системе конфиденциальной информации с помощью виртуального диска.

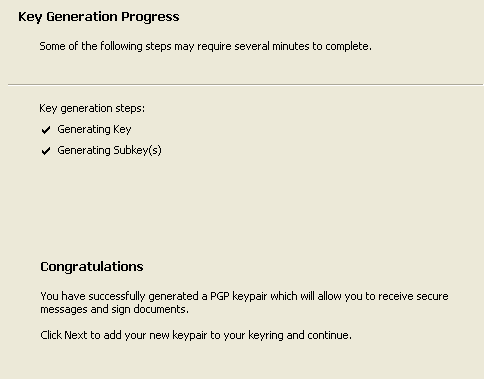
Ход работы:

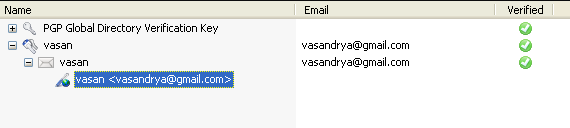




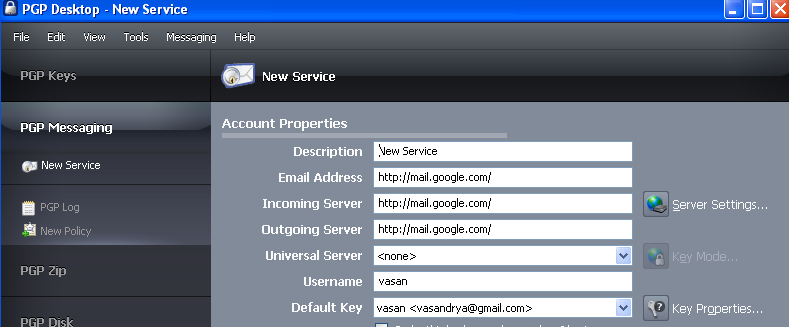


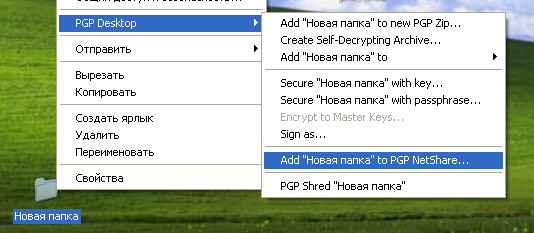


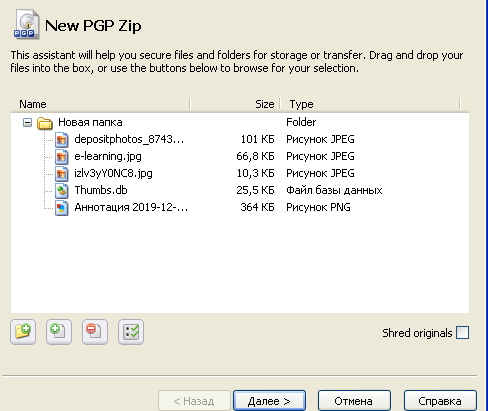


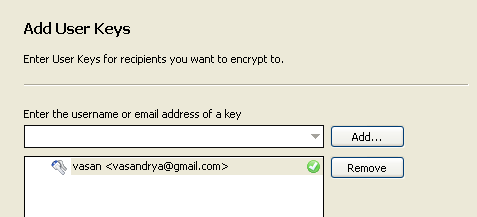


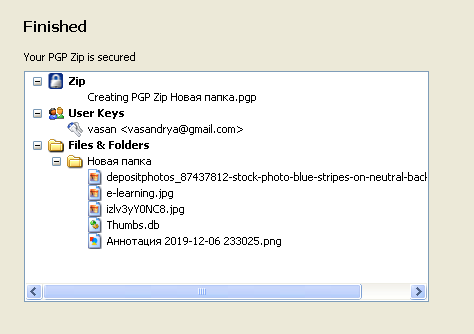


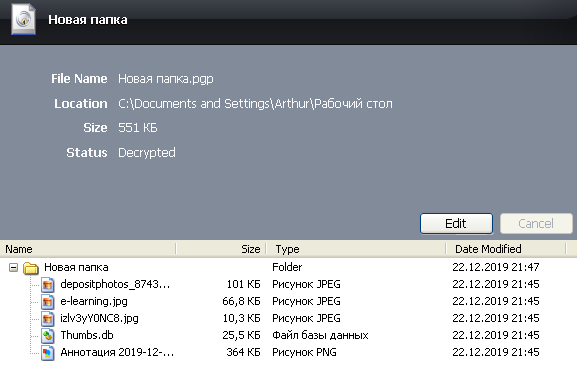


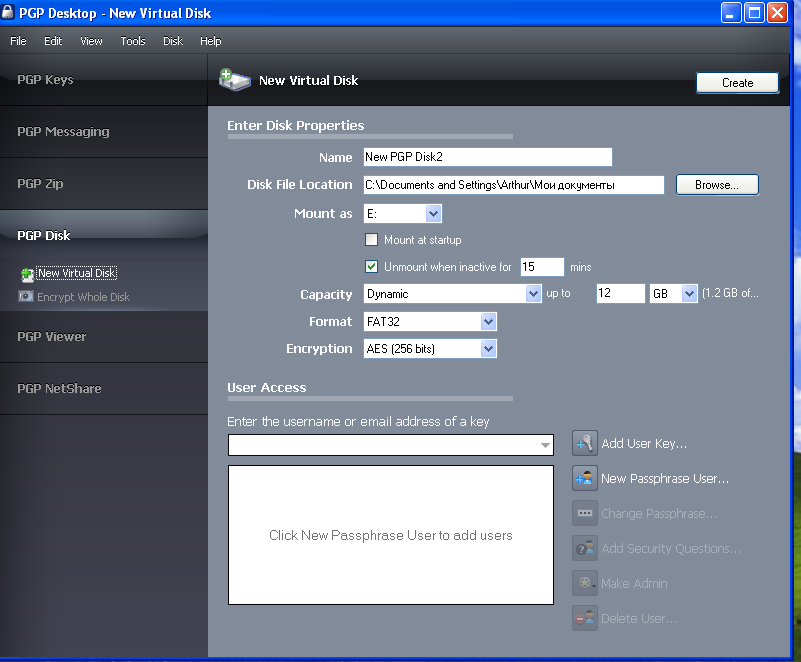


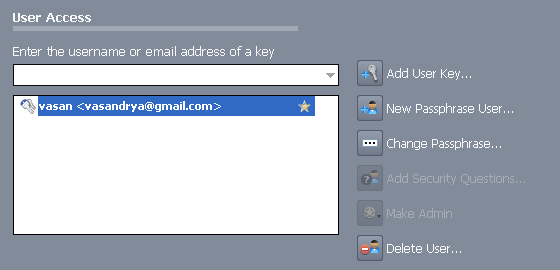




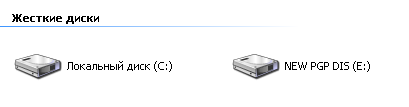












Ответы на вопросы:

1. Какие компоненты включает программа PGP?

*PGP Desktop состоит из следующих компонентов:*

* *PGP Keys - используется для создания и хранения вашей ключевой пары и открытых ключей других пользователей;*
* *PGP Messaging - используется для контроля за электронной почтой, трафиком между клиентом и почтовым сервером, чтобы обеспечить безопасную передачу/получение электронных писем;*
* *PGP Zip - создает и шифрует архивы, также при создании архива может использоваться сжатие;*
* *PGP Whole Disk Encryption - шифровании всего диска, каждый сектор шифруется с использованием симметричного ключа. Шифруются все файлы, в том числе файлы операционной системы, файлы приложений, файлы данных, файлы подкачки, свободного пространства и временные файлы.*
* *PGP Virtual Disk - это создание зашифрованной области, на любом диске, подключенном к компьютеру. PGP VD отображается как ещё один диск, хотя и располагается на одном из физических дисков.*
* *PGP NetShare - обеспечивает прозрачное шифрование файлов общего пользования;*
* *PGP Shredder - уничтожитель документов. После уничтожения документов посредством PGP Shredder их невозможно восстановить*

1. Какие алгоритмы шифрования используются в программе PGP?

*Алгоритм симметричного шифрования AES-256 и ХЭШ-функция SHA-1.*

1. Каким образом достигается надежное уничтожение остаточной конфиденциальной информации в PGP?

*PGP Shredder*

1. Реакция программы на нарушение целостности подписанного документа

*Программа блокируется.*

1. Длина ключевой пары.

*От 1024 до 4096*