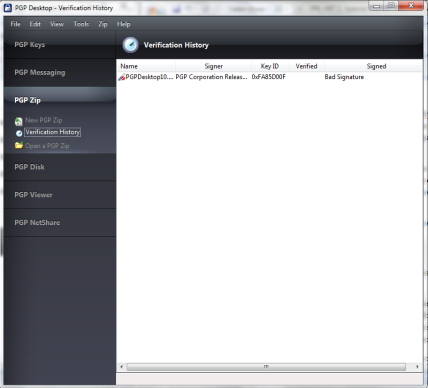
Лабораторная работа № 4.

Изучение программных средств защиты информации

**Выполнение работы**

1. Ознакомиться со сведениями о программе PGP.

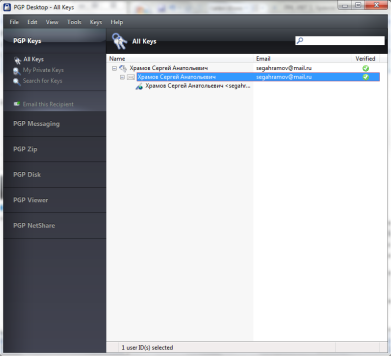
2. Запустить программу PGPtools (с помощью меню «Пуск» или значка PGPtray на панели задач), ознакомиться и отразить в отчете о лабораторной работе состав программных средств, входящих в систему PGP (при необходимости воспользоваться справкой о системе PGP).  


3. Создать криптографические ключи с помощью программы PGPkeys. Включить в отчет о лабораторной работе сведения о порядке создания ключей шифрования в системе PGP и включить в электронную версию отчета копии используемых при этом экранных форм, а также ответы на вопросы:

• как обеспечивается случайность выбираемых криптографических ключей в системе PGP;  
Сообщение, зашифрованное одним ключом, может быть расшифровано только другим, взаимосвязанным ключом.

• как и где хранится секретный ключ пользователя в системе PGP;  
Секретные ключи хранятся в виде "сертификатов ключей. Файл ключей, или каталог ключей содержит один или несколько сертификатов. В каталогах секретных ключей хранятся сертификаты секретных ключей.

• как может быть обеспечена в системе PGP возможность восстановления секретного ключа пользователя при его случайной потере.  
Сохранением его резервной копии.

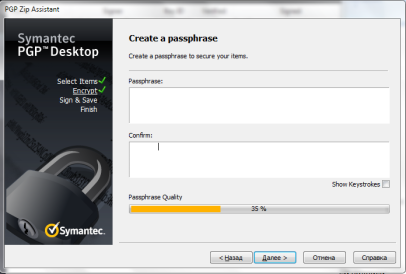
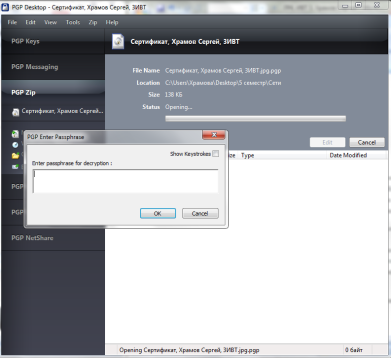
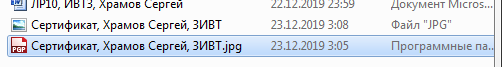
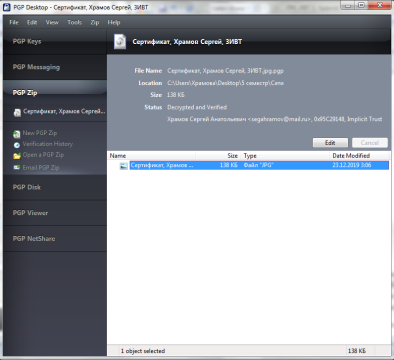
4. Изучить способы шифрования и расшифрования файлов с помощью функций Encrypt и Decrypt программы PGPtools. Включить в отчет о данной лабораторной работе сведения о порядке шифрования и расшифрования файлов в системе PGP, включить в электронную версию отчета копии используемых при этом экранных форм и ответы на вопросы:

• какие дополнительные параметры шифрования могут быть использованы и в чем их смысл и возможное применение;  
Вы можете использовать обычное шифрование (только с паролем, без ключа), что означает, что Вы полагаетесь на обычный пароль, а не на шифрование с открытым ключом. Файл шифруется, используя временный ключ сеанса, который шифруется с использованием вашего пароля.

• как генерируется, как и где хранится ключ симметрического шифрования файла в системе PGP;  
Генерируется на основе введенного нами пароля и хранится C:\Users\Храмова\Documents\PGP \secring.skr.

• как может быть обеспечен доступ к зашифрованному файлу со стороны других пользователей;  
Вводом пароля.

• изменяется ли и как размер файла после его шифрования (привести конкретные примеры для разных типов файлов)  
Да, размер файлов увеличивается.

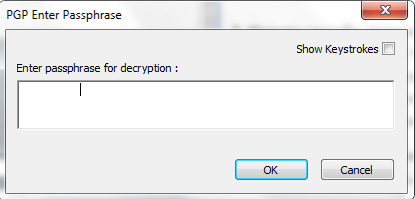
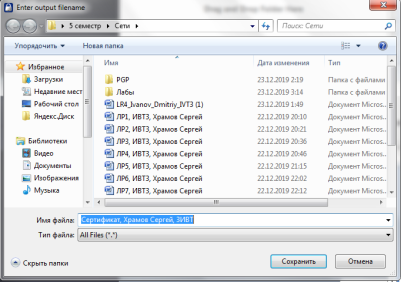
  
  
  
  
  


5. Изучить способы получения и проверки электронной цифровой подписи под файлами с помощью функций Sign и Verify программы PGPtools. Включить в отчет сведения о порядке обеспечения аутентичности и целостности электронных документов в системе PGP, включить в электронную версию отчета копии используемых при этом экранных форм и ответы на вопросы:

• какие дополнительные параметры получения электронной цифровой подписи могут быть использованы, в чем их смысл и возможное применение;

* Detached Signature – создает подпись отдельным файлом
* Text Output – Записывает подпись как ASCII текст

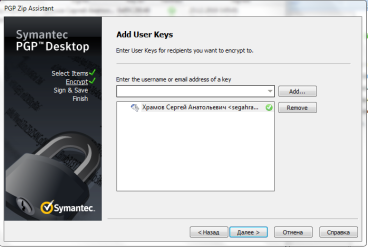
• какова реакция программы на нарушение целостности подписанного документа.  
Выведет сообщение о нарушении подписи


6. Изучить способы одновременного шифрования (расшифрования) и получения (проверки) электронной цифровой подписи в системе PGP с помощью функций Encrypt Sign и Decrypt/Verify программы PGPtools. Включить в отчет сведения о порядке одновременного обеспечения конфиденциальности, аутентичности и целостности электронных документов в этой системе, а также включить в электронную версию отчета копии используемых при этом экранных форм.

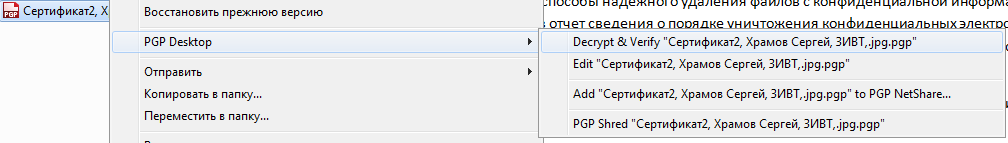


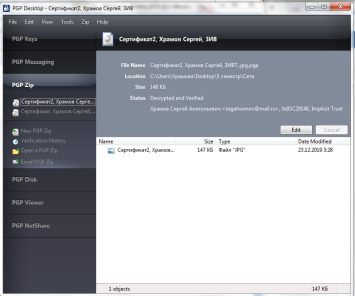










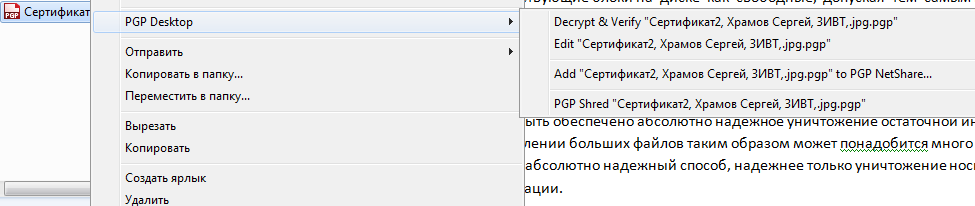


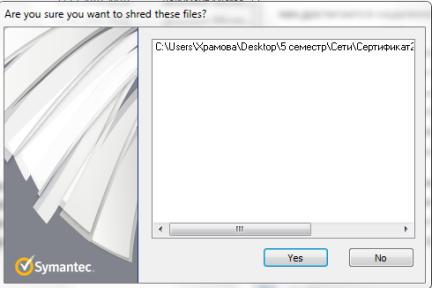
7. Изучить способы надежного удаления файлов с конфиденциальной информацией. Включить в отчет сведения о порядке уничтожения конфиденциальных электронных документов в системе PGP и включить в электронную версию отчета копии используемых при этом экранных форм.

Включить в отчет сведения о назначении и порядке использования этой функции программы, копии используемых в ней экранных форм и ответы на вопросы:

• как достигается надежное уничтожение остаточной конфиденциальной информации в системе PGP;  
Когда вы шифруете файл и затем удаляете файл с исходным открытым текстом, операционная система не стирает данные физически. Она просто помечает соответствующие блоки на диске как свободные, допуская тем самым повторное использование этого пространства. Единственный способ предотвратить восстановление данных - это каким-либо образом обеспечить перезапись места, занимаемого удаленными файлами. Такими возможностями обладает многие криптосистемы PGP.

• является ли подобный метод уничтожения абсолютно надежным и, если нет, как может быть обеспечено абсолютно надежное уничтожение остаточной информации.  
При удалении больших файлов таким образом может понадобится много времени, но зато это абсолютно надежный способ, надежнее только уничтожение носителя информации.

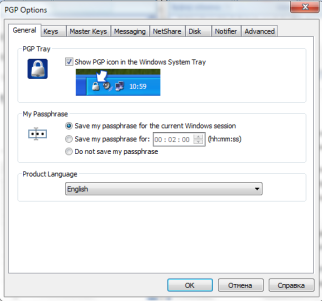


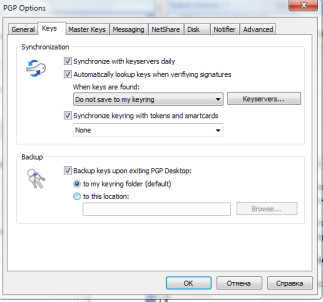


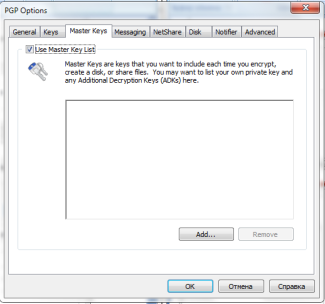
8. Изучить способы управления настройками системы PGP. Включить в отчет сведения о возможностях и порядке администрирования системы PGP, включить в электронную версию отчета копии используемых при этом экранных форм и ответы на вопросы:

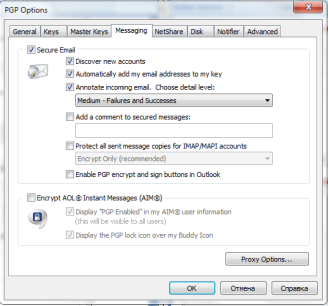
• какие функции по управлению шифрованием и обеспечением целостности информационных ресурсов предоставляет администратору программа PGP;  
Возможность включить в программу Корпоративный ключ подписи, Дополнительные ключи расшифровки, Определенные ключи отзыва, разрешить или запретить генерацию ключей служащими, указать минимальную длину пароля и его качество.

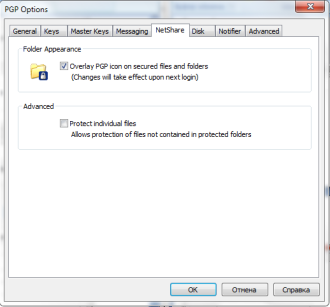
• какие функции по управлению криптографическими ключами пользователей предоставляет администратору программа PGP.  
Разрешить или запретить генерацию ключей служащими, указать минимальную длину пароля и его качество

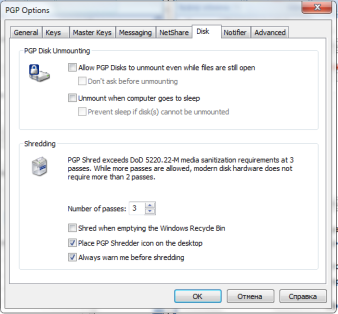


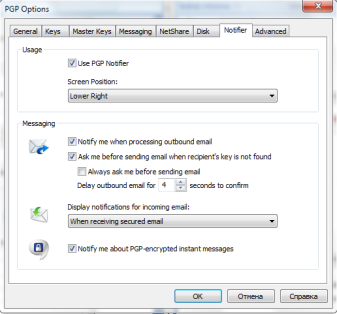


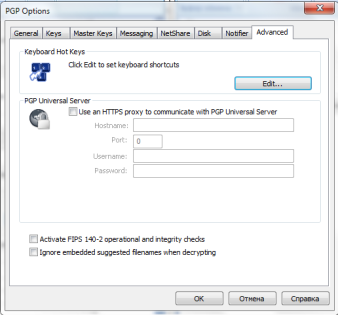












9. После проверки отчета преподавателем удалить систему PGP с помощью функции «Установка и удаление программ» Панели управления Windows.

10. Включить в отчет о лабораторной работе ответы на контрольные вопросы, выбранные в соответствии с номером варианта из прил. 1.

|  |  |  |
| --- | --- | --- |
| 10,26,27 29 | Какой принцип лежит в основе функции надежного уничтожения остаточной конфиденциальной информации программы PGP? | Несколько раз перезаписывает остаточные данные на диске случайными единицами и нулями. |

**Контрольные вопросы**

1. Какие компоненты включает программа PGP.

* 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 Disk - шифрование данных на жестких дисках;
* 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.

2. Какие алгоритмы шифрования используются в программе PGP.  
PGP использует для шифрования семь симметричных алгоритмов (AES, CAST5, 3DES, IDEA, Twofish, Blowfish, Camellia) на сеансовом ключе.

3. Каким образом достигается надежное уничтожение остаточной конфиденциальной информации в PGP.  
Когда вы шифруете файл и затем удаляете файл с исходным открытым текстом, операционная система не стирает данные физически. Она просто помечает соответствующие блоки на диске как свободные, допуская тем самым повторное использование этого пространства. Единственный способ предотвратить восстановление данных - это каким-либо образом обеспечить перезапись места, занимаемого удаленными файлами. Такими возможностями обладает многие криптосистемы PGP.

4. Реакция программы на нарушение целостности подписанного документа.  
Выведет сообщение о нарушении подписи.

5. Длина ключевой пары.  
Для ключей RSA legacy длина ключа может составлять от 1024 до 2048 бит, а для Diffie-Hellman/DSS и RSA — от 1024 до 4096. Ключи RSA legacy содержат одну ключевую пару, а ключи Diffie-Hellman/DSS и RSA могут содержать один главный ключ и дополнительные ключи для шифрования.