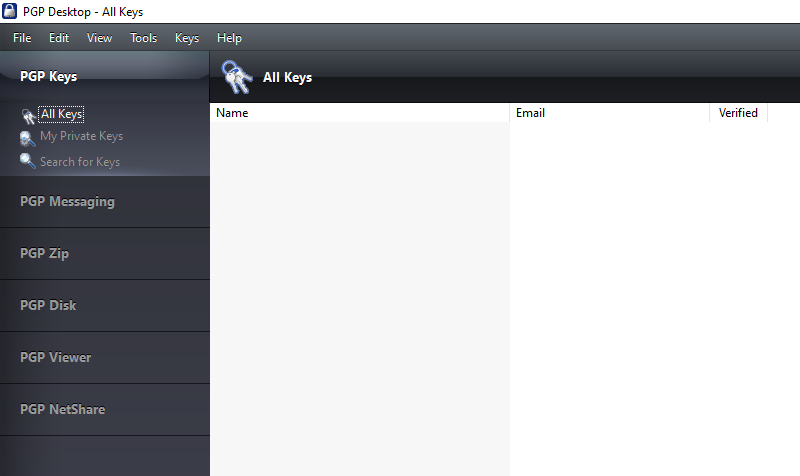
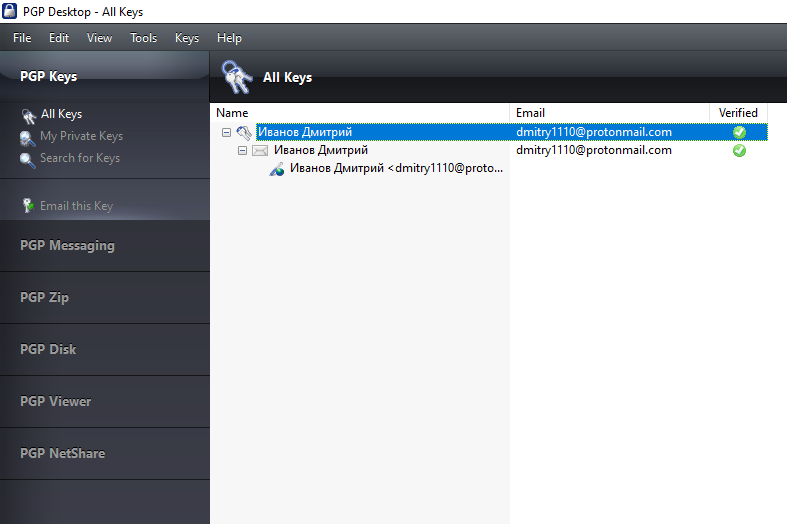
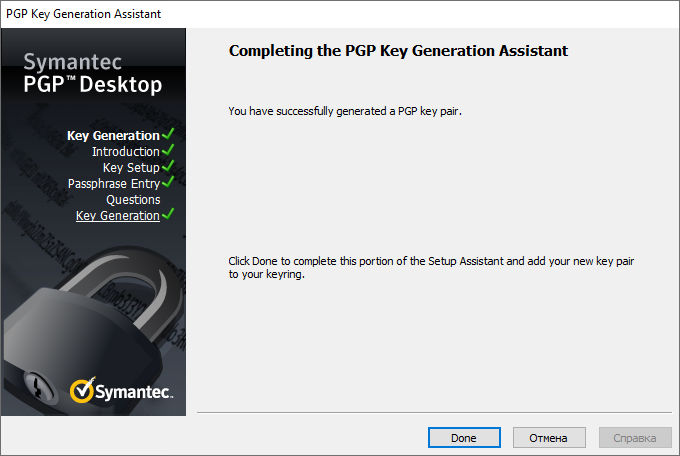
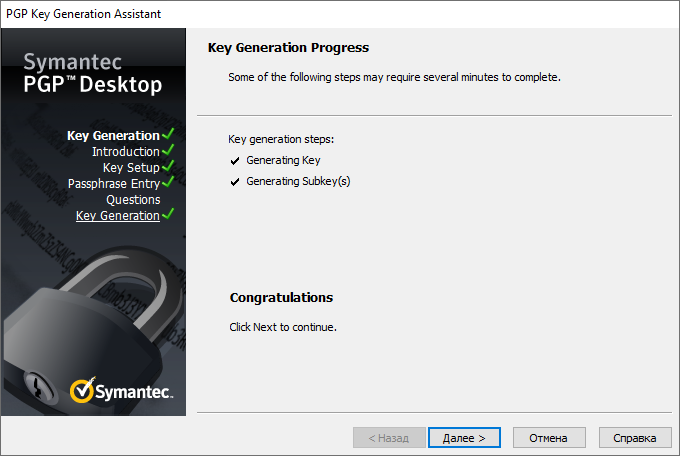
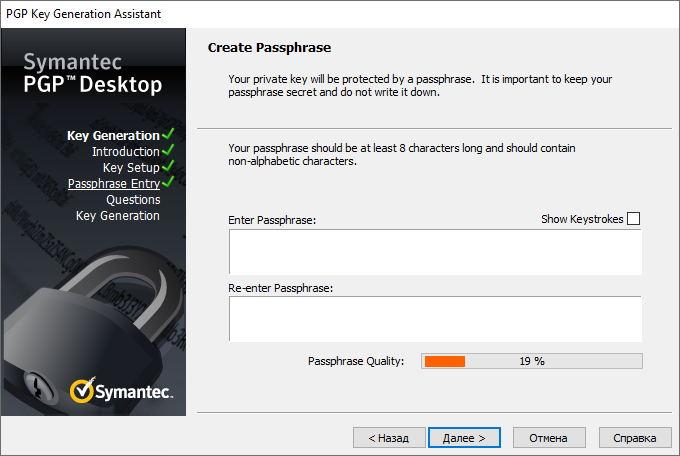
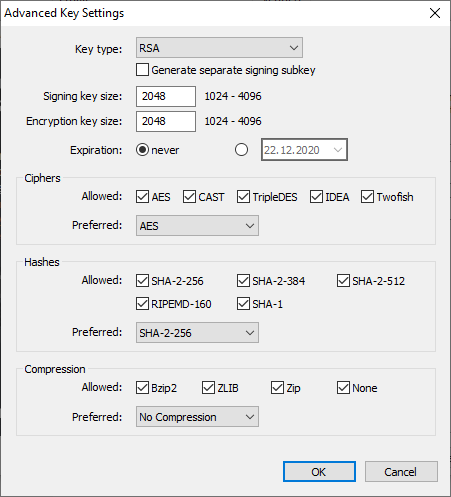
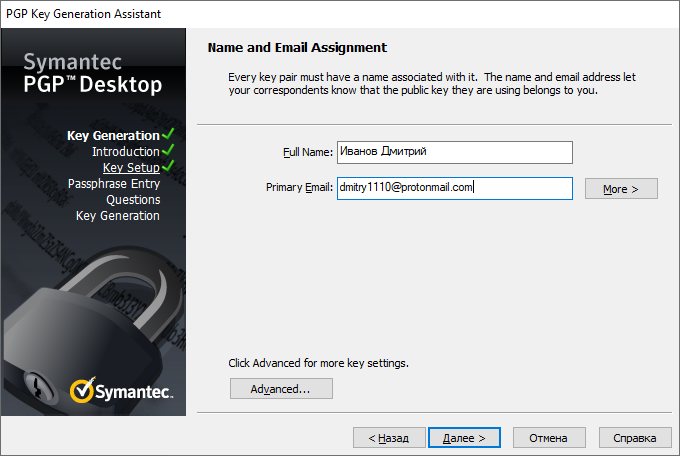
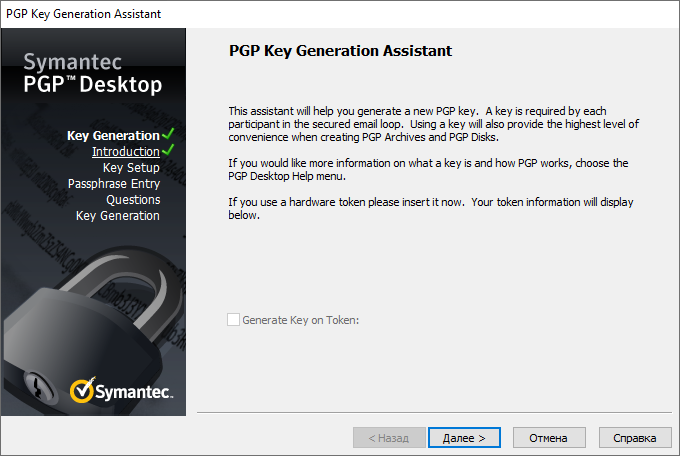
## ЛАБОРАТОРНАЯ РАБОТА № 4. Изучение программных средств защиты информации

# Выполнение работы

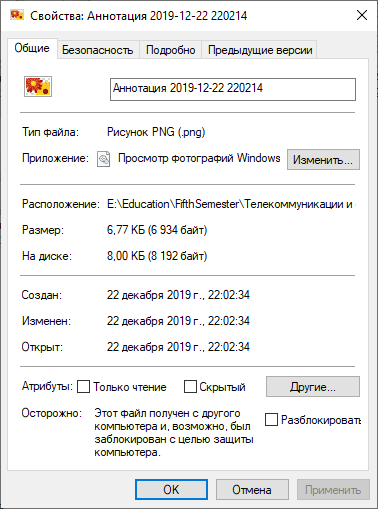
1. Ознакомиться со сведениями о программе PGP.
2. Запустить программу PGPtools (с помощью меню «Пуск» или значка PGPtray на панели задач), ознакомиться и отразить в отчете о лабораторной работе состав программных средств, входящих в систему PGP (при необходимости воспользоваться справкой о системе PGP). 
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;
  + Шифрование PGP построено на принципе несимметричной криптографии. Вкратце это означает следующее. Сообщение, зашифрованное одним ключом, может быть расшифровано только другим, взаимосвязанным ключом. Эти два ключа образуют пару - публичный и секретный. Такая пара ключей есть у каждого участника переписки. Главное преимущество PGP состоит в том, что для обмена зашифрованными сообщениями пользователям нет необходимости передавать друг другу тайные ключи. Хотя ключ, которым шифруется текст сообщения, доступен посторонним, с его помощью это сообщение расшифровать невозможно. Этот ключ называется публичным. Пользователи могут открыто посылать друг другу свои публичные ключи через Интернет. При этом риска несанкционированного доступа к их конфиденциальной переписке не возникает. Секретный ключ тщательно оберегается от посторонних. С помощью секретного ключа получатель дешифрует сообщения, которые были зашифрованы его публичным ключом. Но даже заполучив секретный ключ, противник не сможет им воспользоваться, не зная пароля.
* как и где хранится секретный ключ пользователя в системе PGP;
  + Секретные ключи хранятся в виде "сертификатов ключей", включают идентификатор пользователя владельца ключа (имя пользователя), временную метку, которая указывает время генерации пары ключей, и ключи. Каждый секретный ключ также шифруется с отдельным паролем. Файл ключей, или каталог ключей ("кольцо с ключами" — "keyring") содержит один или несколько сертификатов. В каталогах секретных ключей хранятся сертификаты секретных ключей. генерация секретного ключа пользователя (RSA-key). Для этого система запрашивает фразу пароля, которая потом будет неоднократно использоваться при каждом использовании секретного ключа. Кроме того, запрашивается собственно имя (идентификатор) пользователя, куда входит и его адрес (E-mail, FIDO), а основании этих данных и с использованием ряда случайных чисел (которые получаются путем измерения интервалов времени между нажатиями клавиш человеком) генерируется СЕКРЕТЫЙ ключ пользователя. Это просто бинарная последовательность
* Как может быть обеспечена в системе PGP возможность восстановления секретного ключа пользователя при его случайной потере
  + Сохранением его резервной копии
  + Копии экранных форм:

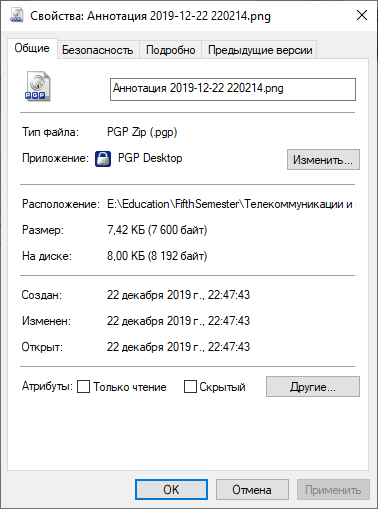


1. Изучить способы шифрования и расшифрования файлов с помощью функций Encrypt и Decrypt программы PGPtools. Включить в отчет о данной лабораторной работе сведения о порядке шифрования и расшифрования файлов в системе PGP, включить в электронную версию отчета копии используемых при этом экранных форм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

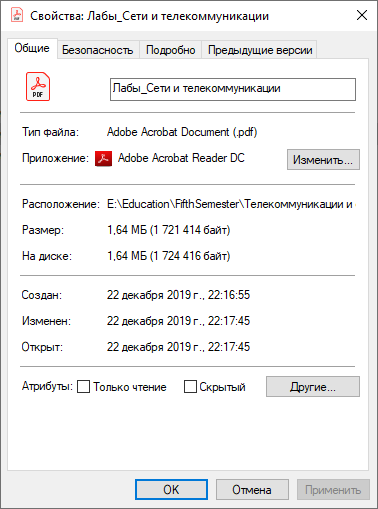
* какие дополнительные параметры шифрования могут быть использованы и в чем их смысл и возможное применение;
  + При посылке файлов как вложения (аттачменты) с некоторыми программами электронной почты, Вы должны выбрать флажок "Текстовый вывод" (Text Output), чтобы файл был записан как ASCII текст. Это иногда необходимо, чтобы послать двоичный файл, используя старые программы электронной почты. Этот выбор увеличивает размер файла примерно на 30 процентов. 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. Для обычного шифрования установите флажок "Conventional Encryption". Затирание оригинала уничтожает оригинал документа, который Вы шифруете или подписываете, так что ваша важная информация становится нечитаема для любого, кто имеет доступ на ваш жесткий диск. Для затирания оригиналов установите флажок "Wipe Original".
* как генерируется, как и где хранится ключ симметрического шифрования файла в системе PGP;
* Генерируется на основе введенного нами пароля и хранится в нашем случае C:\Program Files\Network Associates\PGP60\PGP Keyrings\secring.skr
* как может быть обеспечен доступ к зашифрованному файлу со стороны других пользователей;
  + Знанием пароля, который был введен при создании ключей.
* изменяется ли и как размер файла после его шифрования (привести конкретные примеры для разных типов файлов).
  + Да, размер файлов увеличивается.
  + Файл .png до:



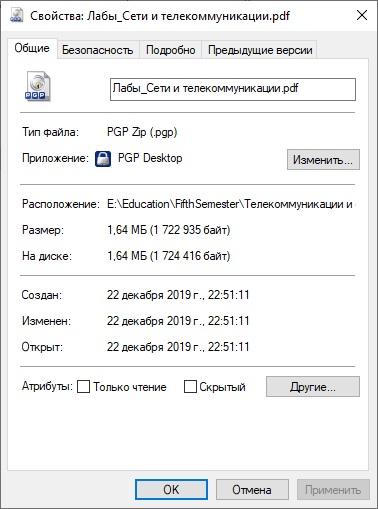
* + Файл .png после:



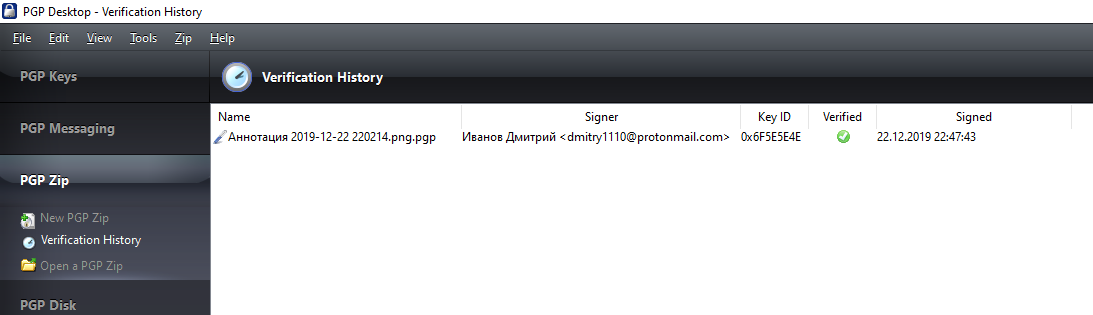
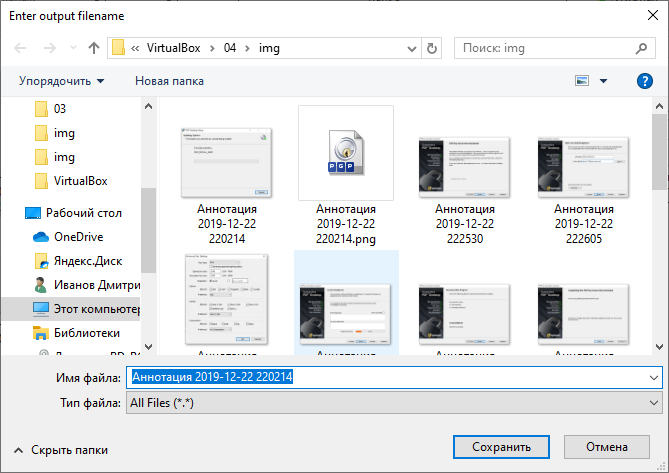
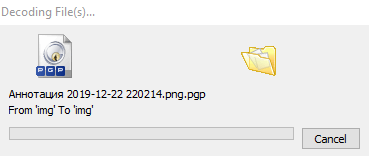
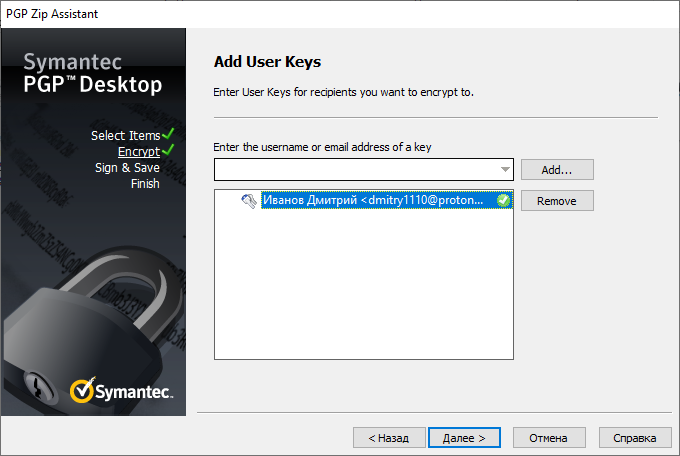
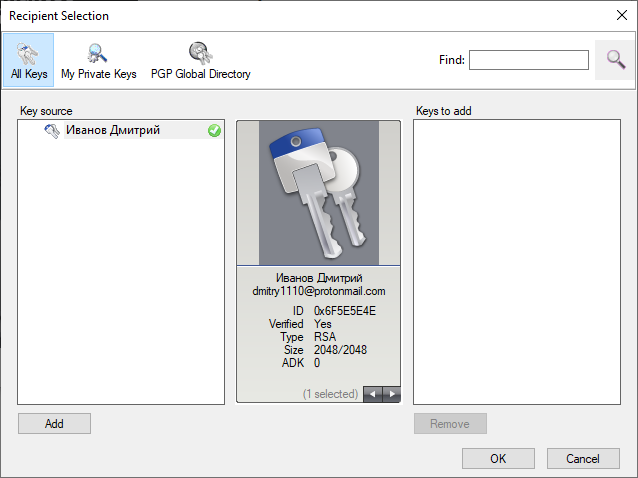
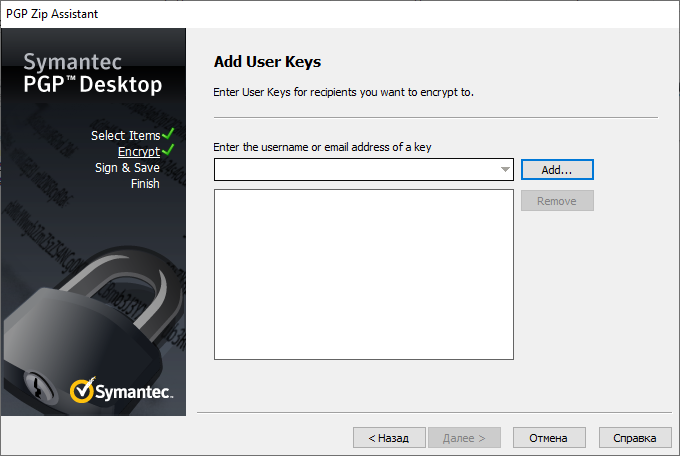
* + Файл .pdf до:



* + Файл .pdf после:

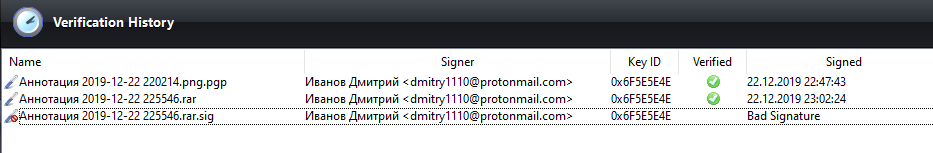


* + Копии экранных форм

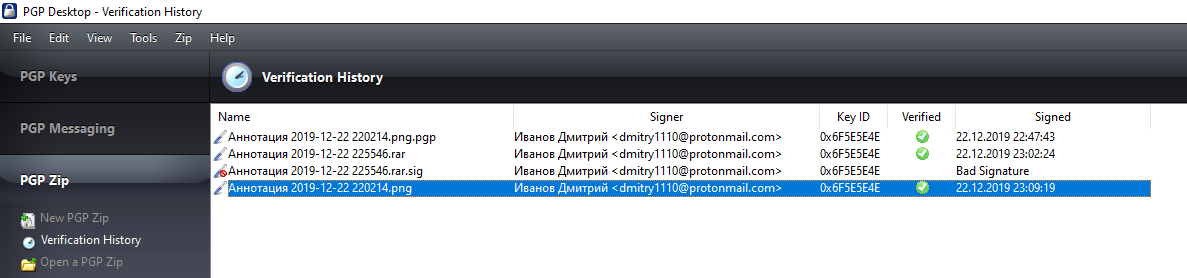
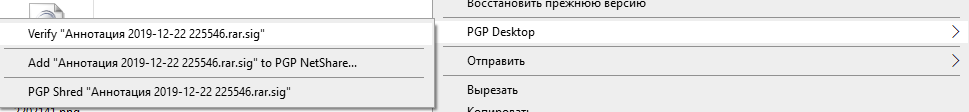
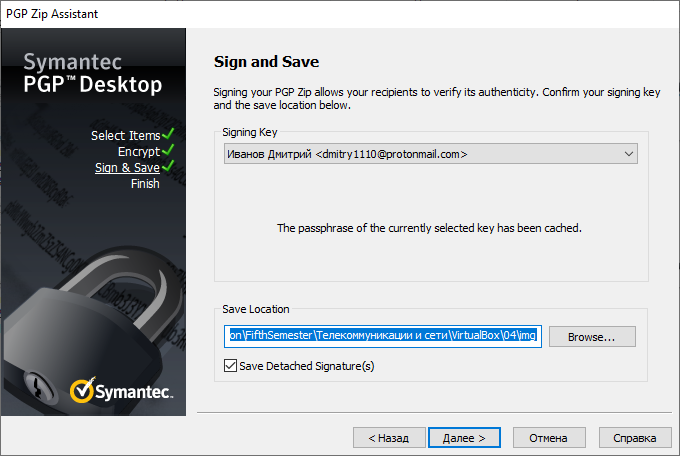
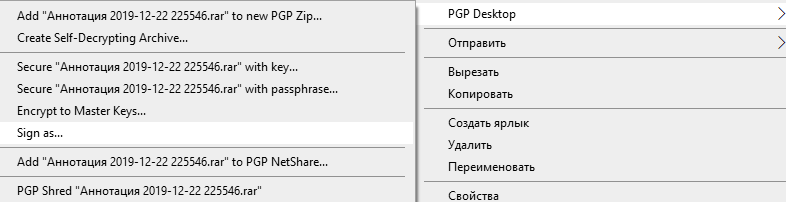


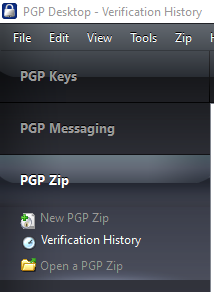
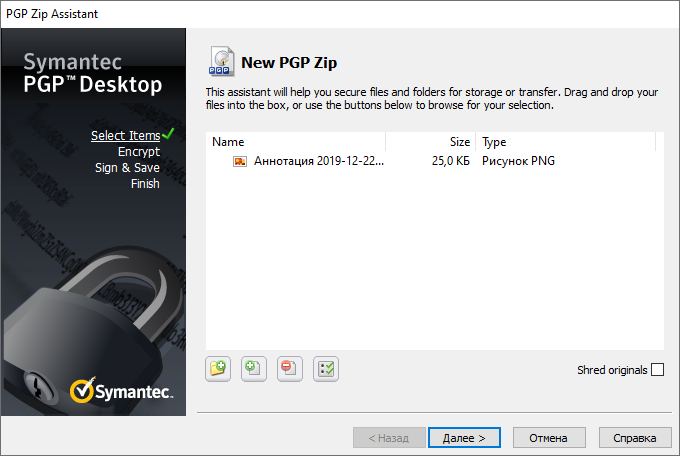
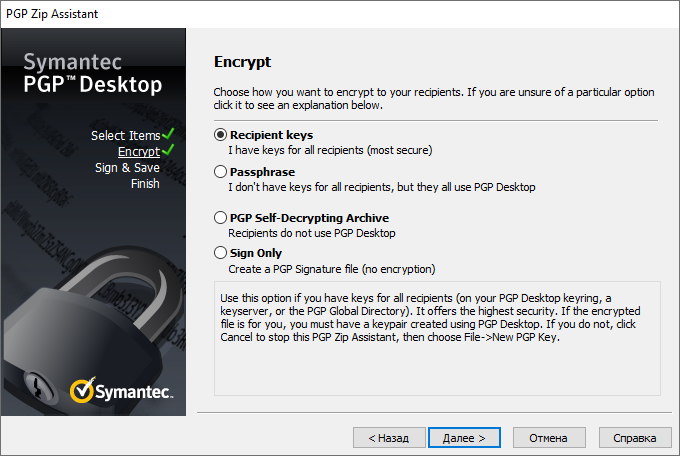
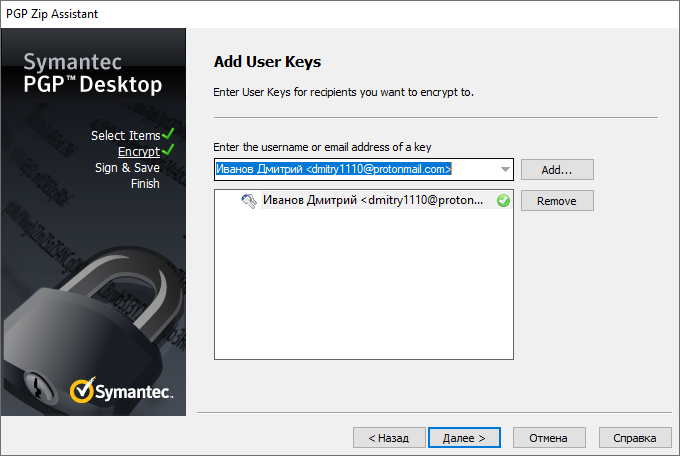
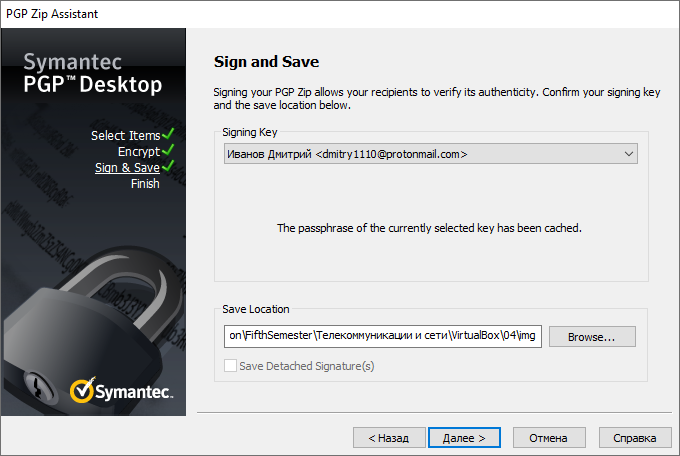
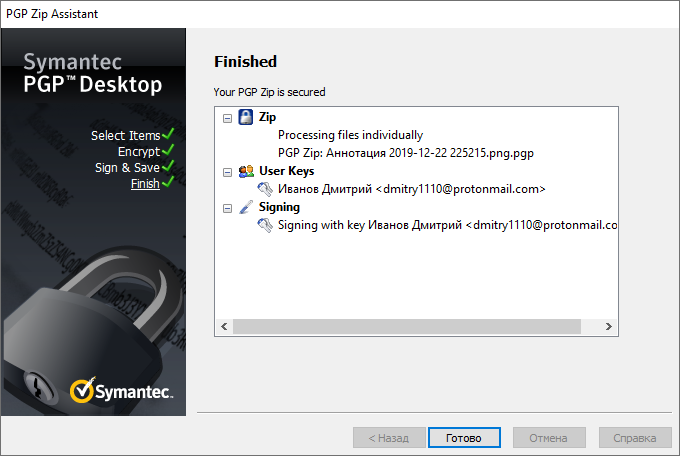
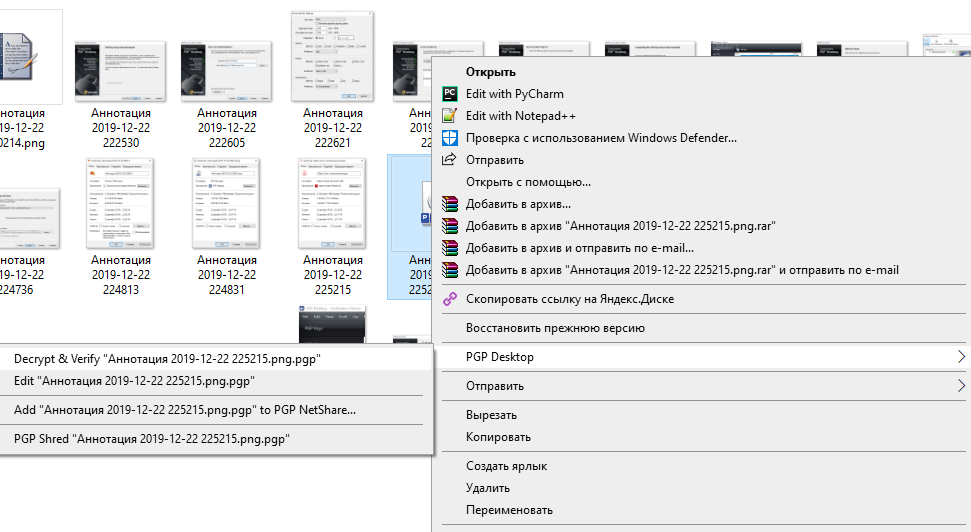
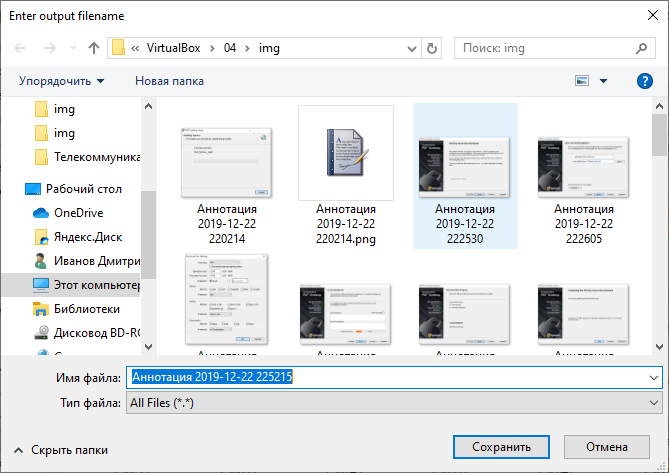
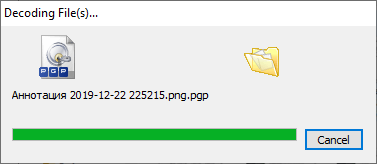
1. Изучить способы получения и проверки электронной цифровой подписи под файлами с помощью функций Sign и Verify программы PGPtools. Включить в отчет сведения о порядке обеспечения аутентичности и целостности электронных документов в системе PGP, включить в электронную версию отчета копии используемых 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.
  + Нарушение подписи документа.



* + Копии экранных форм



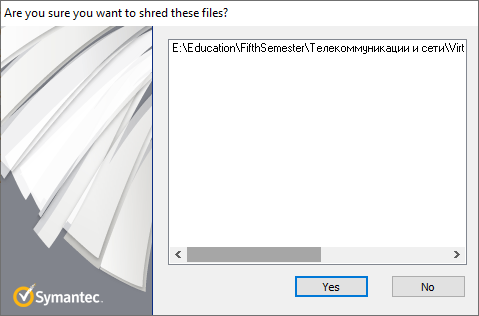
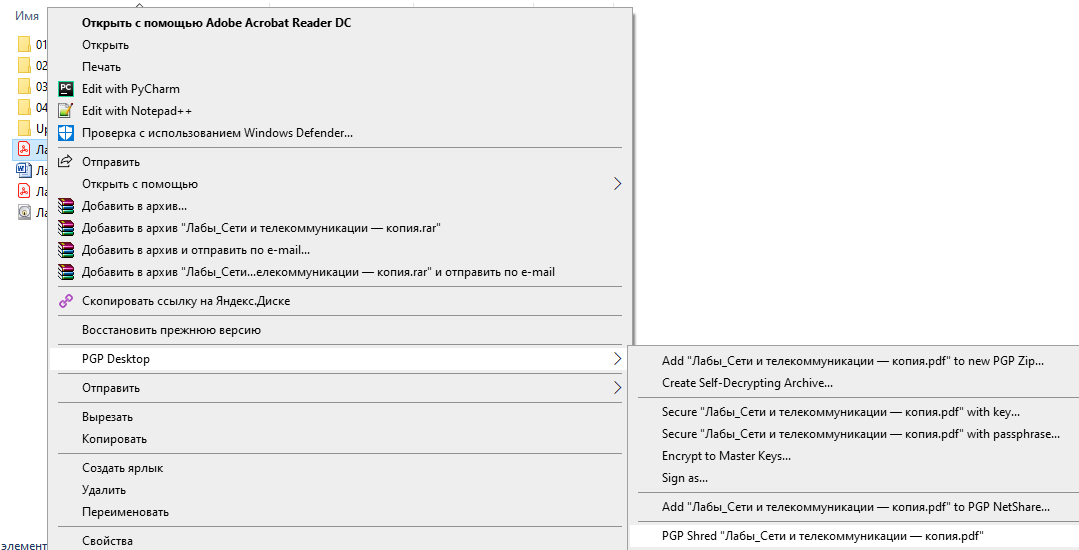
1. Изучить способы одновременного шифрования (расшифрования) и получения (проверки) электронной цифровой подписи в системе PGP с помощью функций Encrypt Sign и Decrypt/Verify программы PGPtools. Включить в отчет сведения о порядке одновременного обеспечения конфиденциальности, аутентичности и целостности электронных документов в этой системе, а также включить в электронную версию отчета копии используемых при этом экранных форм.
   * Нажимаем кнопку New PGP Zip в левой части меню
   * Выбираем нужный файл на жестком диске
   * Выбираем нужный режим шифрования
   * Выбираем нужный ключ
   * Меню выбора подписи (Sign) и выбор директории 
   * Готово!
   * Для расшифровки файла нужно выбрать зашифрованный файл правой кнопкой мыши, выбрать пункт Decrypt & Verify
   * Выбрать директорию для расшифрованных и “расписанных” файлов
   * Нажать кнопку сохранить
   * Готово!
2. 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;

Wipe несколько раз (По умолчанию три) перезаписывает остаточные данные на диске случайными единицами и нулями.

* + является ли подобный метод уничтожения абсолютно надежным и, если нет, как может быть обеспечено абсолютно надежное уничтожение остаточной информации.

Специалисты по восстановлению данных в действительности могут восстановить данные даже после нескольких перезаписей. Можно увеличить число проходов до 28, и в этом случае даже Агентство национальной безопасности будет бессильно. Отметим, что при стирании больших файлов с большим числом проходов может потребоваться довольно много времени. Это высокоинтенсивная дисковая операция. Поэтому абсолютно надежным средством уничтожения остаточной информации является физическое уничтожение носителя информации.

Копии экранных форм



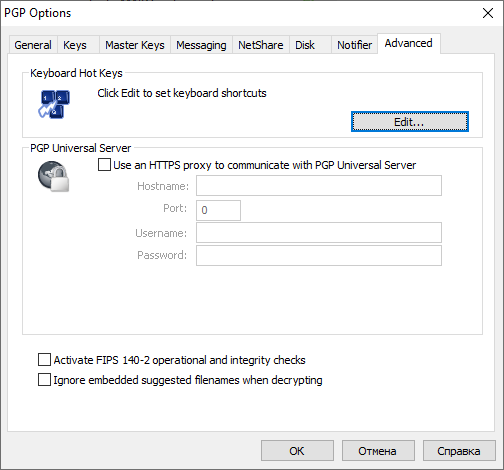
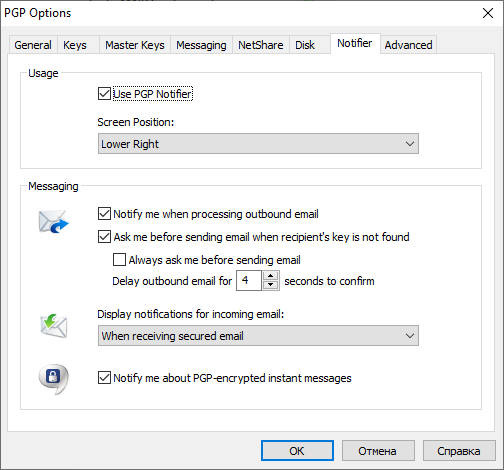
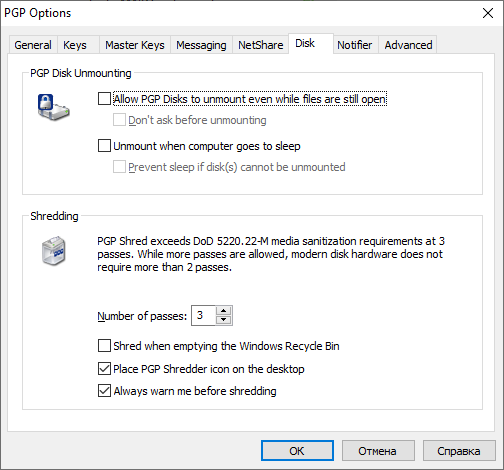
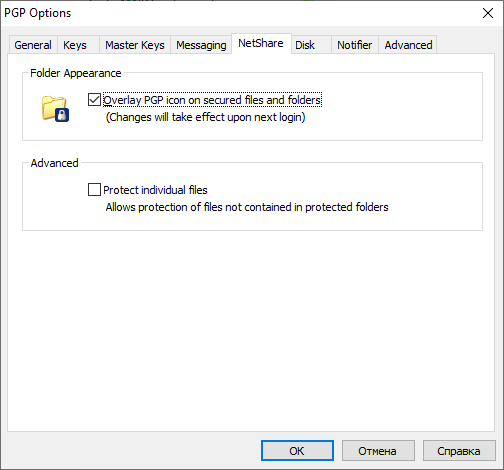
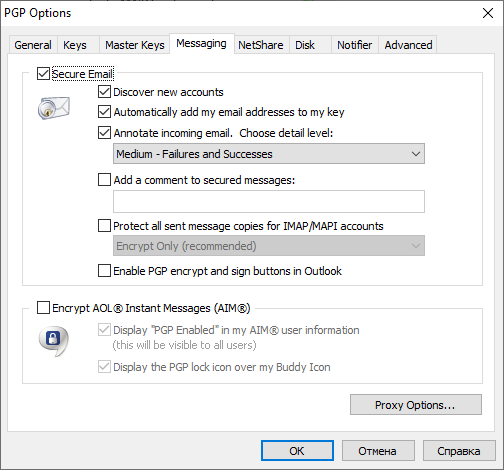
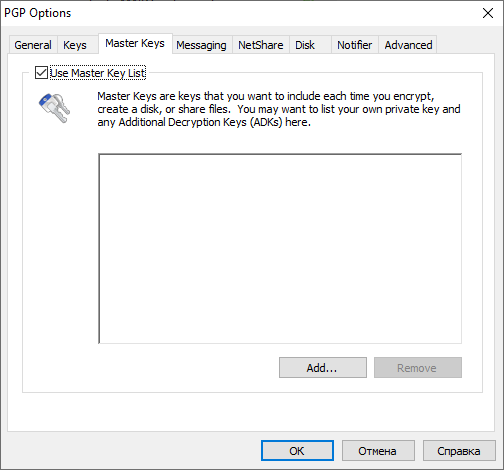
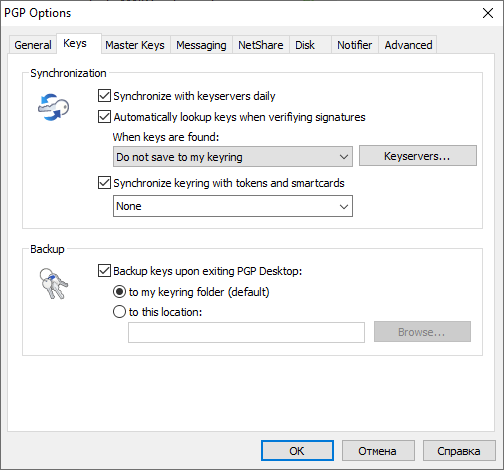
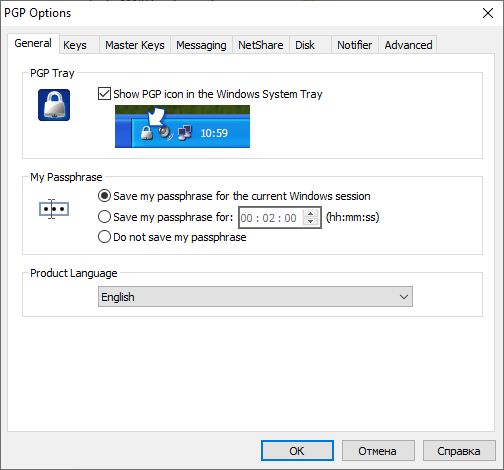
1. Изучить способы управления настройками системы PGP. Включить в отчет сведения о возможностях и порядке администрирования системы PGP, включить в электронную версию отчета копии используемых при этом экранных форм и ответы на вопросы:
   * какие функции по управлению шифрованием и обеспечением целостности 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.

Копии экранных форм



1. После проверки отчета преподавателем удалить систему PGP с помощью функции «Установка и удаление программ» *Панели управления* Windows.
   * Включить в отчет о лабораторной работе ответы на контрольные вопросы, выбранные в соответствии с номером варианта из прил. 1.

|  |  |
| --- | --- |
| **Номер варианта** | **Контрольные вопросы** |
| 3 | Какими основными функциями защиты информации обладает программа PGP?  Подписывание файлов цифровой подписью, Шифрование данных |

Какие компоненты включает программа PGP.

PGP Keys - доступ к таблицам собственных ключей и ключей корреспондентов,

PGP Messaging - управление службами обмена сообщениями. При установке программа автоматически обнаруживает ваши учетные записи и автоматически шифрует коммуникации AOL Instant Messenger,

PGP Zip - управление зашифрованными архивами. Программа поддерживает прозрачное и непрозрачное шифрование. Этот раздел как раз и реализует непрозрачное шифрование. Вы можете создать зашифрованный Zip-архив (PGP Zip) или саморасшифровывающийся архив,

PGP Disk - это реализация функции прозрачного шифрования. Программа может, как зашифровать весь раздел жесткого диска (или даже весь диск) или создать новый виртуальный диск (контейнер). Здесь же есть функция Shred Free Space, которая позволяет затереть свободное пространство на диске,

PGP Viewer - здесь можно расшифровать PGP-сообщения и вложения.,

PGP NetShare - для безопасной передачи файлов и их совместного использования с выбранными коллегами

Какие алгоритмы шифрования используются в программе PGP.

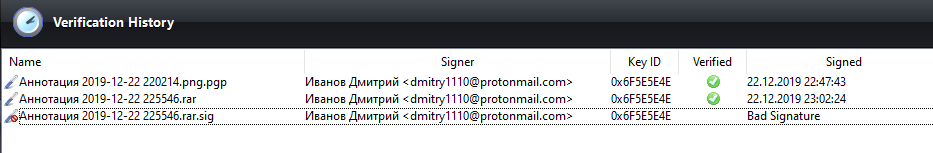
Шифрование PGP осуществляется последовательно хешированием, сжатием данных, шифрованием с симметричным ключом, и, наконец, шифрованием с открытым ключом, причём каждый этап может осуществляться одним из нескольких поддерживаемых алгоритмов. Симметричное шифрование производится с использованием одного из семи симметричных алгоритмов (AES, CAST5, 3DES, IDEA, Twofish, Blowfish, Camellia) на сеансовом ключе. Сеансовый ключ генерируется с использованием криптографически стойкого генератора псевдослучайных чисел. Сеансовый ключ зашифровывается открытым ключом получателя с использованием алгоритмов RSA или Elgamal (в зависимости от типа ключа получателя). Каждый открытый ключ соответствует имени пользователя или адресу электронной почты. Первая версия системы называлась Сеть Доверия и противопоставлялась системе X.509, использовавшей иерархический подход, основанной на удостоверяющих центрах, добавленный в PGP позже. Современные версии PGP включают оба способа.

Каким образом достигается надежное уничтожение остаточной конфиденциальной информации в PGP.

PGP Shredder используется для безвозвратного уничтожения на диске нежелательных файлов и папок.

Реакция программы на нарушение целостности подписанного документа.

* + Нарушение подписи документа.



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

* + Сохранить отчет о выполнении лабораторной работы в папке, созданной при выполнении п. 1.
  + Завершить работу с ОС *Windows*.