МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра защиты информации и систем связи

УТВЕРЖДАЮ
Проректор по учебной работе
_____О.Г. Локтионова
«___»_____2015 г.

ПРИМЕНЕНИЕ ПРОГРАММНЫХ КРИПТОСИСТЕМ ШИФРОВАНИЯ. ИЗУЧЕНИЕ ПРОГРАММНОГО ПРОДУКТА PGP

Методические указания по выполнению лабораторной работы по дисциплине «Криптографические методы защиты информации» для студентов специальностей 10.05.03, 10.05.02, 10.03.01

Курск 2015

УДК 004.056.55 (076.5)

Составитель: М.А. Ефремов, А.Л. Ханис

Рецензент
Кандидат технических наук, доцент *И.В. Калуцкий*

Применение программных криптосистем шифрования. Изучение программного продукта PGP: методические указания по выполнению лабораторной работы по дисциплине «Криптографические методы защиты информации» / Юго-Зап. гос. ун-т; сост.: М.А. Ефремов, А.Л. Ханис. Курск, 2015. 19 с.: ил. 13.

Содержат сведения о применении программных криптосистем шифрования. Рассматриваются основные этапы по настройке и установке программного продукта PGP. Указывается порядок выполнения лабораторной работы, правила оформления и содержание отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по образованию в области информационной безопасности (УМО ИБ).

Предназначены для студентов специальностей 10.05.03, 10.05.02, 10.03.01 дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.
Усл.печ. л. . Уч.-изд.л. . Тираж 30 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

1. ЦЕЛЬ РАБОТЫ

Цель лабораторной работы - ознакомление с работой программных систем шифрования на примере программного продукта PGP. Установить программу, настроить требуемые параметры шифрования, изучить применение программного продукта в области криптографической защиты информации.

2. ЗАДАНИЕ

Произвести установку программного продукта PGP. Сгенерировать пару ключей с помощью программы PGPkeys. Переслать открытый ключ другому пользователю. Зашифровать и отправить зашифрованное сообщение с помощью программы Outlook Express. Расшифровать полученное сообщение. Изучить три основных способа шифрования информации. Создать и установить PGP диск. Закрыть PGP диск.

3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить задание.
2. Изучить теоретическую часть.
3. Сгенерировать ключи.
4. Зашифровать и отправить сообщение.
5. Расшифровать сообщение.
6. Установить новый PGP диск.
7. Закрыть PGP диск.
8. Составить отчет.

4. СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист.
2. Краткая теория.
3. Описание выбора требуемых параметров.
4. Процесс выполнения работы со скриншотами.
5. Вывод.

5. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

5.1 Введение

PGP (Pretty Good Privacy) - программа, служащая для кодирования и/или подписывания сообщений, файлов и любой другой информации, представленной в электронном виде. PGP представляет собой гибридную систему, которая включает в себя алгоритм с открытым ключом (асимметричный алгоритм) и обычный алгоритм с секретным ключом (симметричный алгоритм), что дает высокую скорость, характерную для симметричных алгоритмов и существенные удобства, характерные для криптографии с открытым ключом. С точки зрения пользователя PGP ведет себя как система с открытым ключом. В криптосистемах с открытым ключом генерируется с помощью специального математического алгоритма пара ключей - один открытый и один секретный. Сообщение шифруется с помощью одного ключа, и дешифруется с помощью другого (причем неважно каким именно из двух ключей производится шифрование). Сообщение нельзя расшифровать с помощью ключа шифрования. Обычно вы опубликовываете свой открытый ключ, делая его доступным любому, кто захочет послать вам зашифрованное сообщение. Такой человек зашифрует сообщение вашим открытым ключом, при этом ни он сам, никто другой не могут расшифровать шифрованное сообщение. Только вы можете расшифровать сообщение, то есть тот человек, который имеет секретный ключ, соответствующий открытому ключу. Очевидно, что секретный ключ должен храниться в секрете своим обладателем.

Огромным преимуществом такого способа шифровки является то, что в отличие от обычных методов шифрования, нет необходимости искать безопасный способ передачи ключа адресату. Другой полезной чертой таких криптосистем является возможность создать цифровую "подпись" сообщения, зашифровав его своим секретным ключом. Теперь, с помощью вашего открытого ключа любой сможет расшифровать сообщение и таким образом убедиться, что его зашифровал действительно владелец секретного ключа.

PGP использует для шифрования алгоритм с открытым ключом RSA в паре с обычным методом шифрования IDEA. В методе IDEA для шифрования используется один ключ, как и в других симметричных криптосистемах, тот же ключ дешифровывает сообщение. PGP использует алгоритм RSA для зашифровки ключа IDEA с помощью открытого ключа адресата. Адресат, приняв сообщение с помощью PGP, расшифрует этот секретный ключ IDEA. Далее остальная часть сообщения расшифровывается принимающей стороной методом IDEA.

5.2 Установка программы

Запустить программу PGP8.exe. Появится окно приветствия (рис.1). Нажимаем кнопку Next.

Рисунок 1 – Окно приветствия программы

Затем принимаем лицензионное соглашение (кнопка Yes). Открывается файл руководства для пользователей данного программного продукта и нажимаем кнопку Next (рис.2). В окне выбора типа пользователя указать, есть ли у вас файл ключей (Yes, I already have keyrings) или же вы новый пользователь (No, I’m a New user).

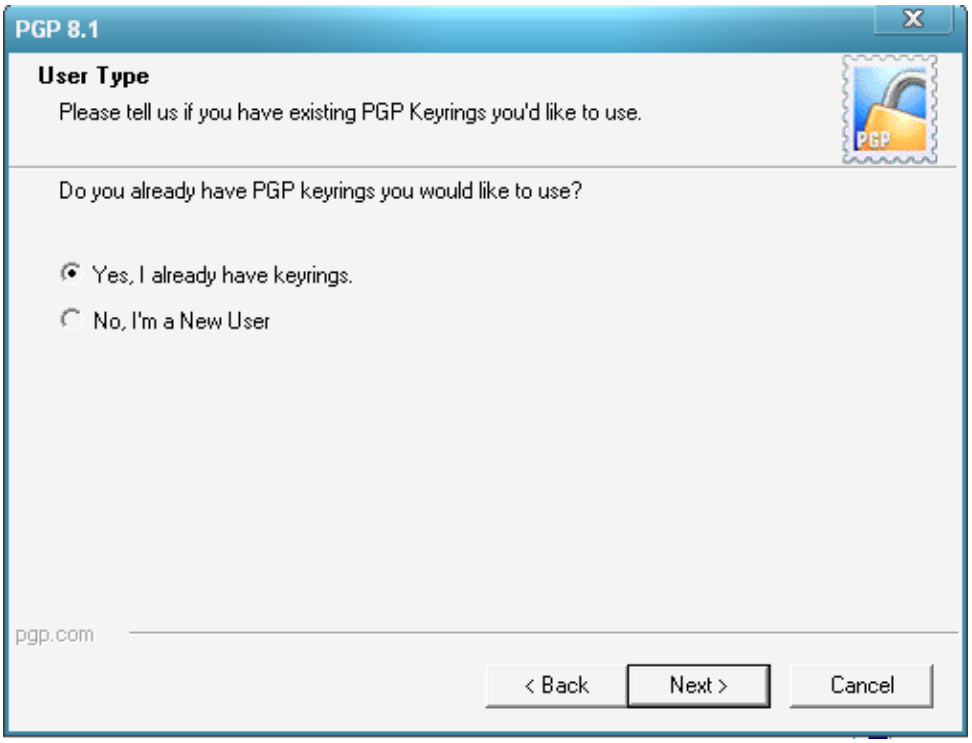

Рисунок 2 – Окно выбора типа пользователя

В следующем окне выбираем директорию, в которую будет установлена программа.

Далее откроется окно выбора компонентов программы:

- *PGPdisk* – включает программные файлы для PGP-диска;
- *PGPmail for ICQ* - включает программные файлы для защищенного общения по ICQ;
- *PGPmail for Microsoft Outlook (PGPmail for Microsoft Outlook Express)* - включает программные файлы для защищенного обмена письмами с использованием почтового клиента Microsoft Outlook (PGPmail for Microsoft Outlook Express);
- *PGPmail for Qualcomm Eudorra* - включает программные файлы для защищенного обмена письмами с использованием почтовой программы Qualcomm Eudorra (GroupWise);
- *PGPmail for GroupWise* - включает программные файлы для защищенного обмена письмами с использованием почтовой программы GroupWise.

Выбираем те компоненты, которые необходимы для пользования и нажимаем кнопку Next (рис.3).

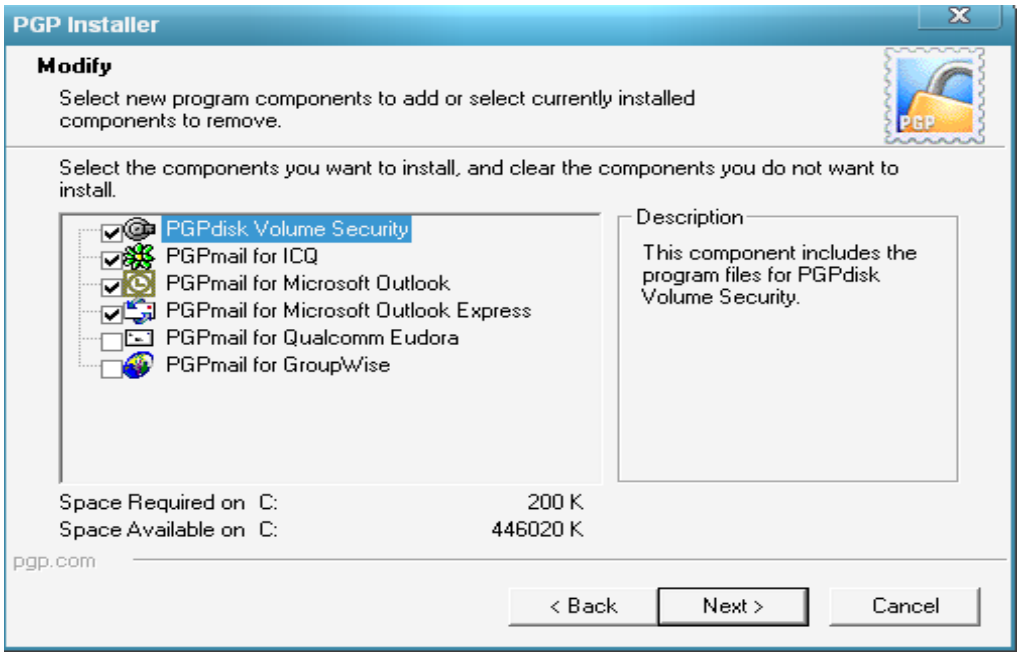

Рисунок 3 – Выбор компонентов программы

Начнется копирование программных файлов на жесткий диск компьютера. Затем появится окно с сообщением «Установка программы завершена», после чего нужно перезагрузить компьютер и заполнить форму авторизации программы. Теперь установка завершена.

6. ВЫПОЛНЕНИЕ РАБОТЫ

6.1 Генерация ключей

Запустите программу PGPkeys.exe. Если вы используете PGP в первый раз, сначала вам нужно сгенерировать пару ключей, выбрав в меню Keys пункт New Key. Это можно сделать автоматически через Помощник генерации ключа (рис.4).

Рисунок 4 – Запуск программы PGP key

Нажав кнопку Expert, вы сможете ввести в специальные поля параметры, которые будут использованы при генерации ключевой пары (на указанный электронный адрес будет выслано подтверждение сгенерированных ключей). Нажать кнопку ДАЛЕЕ (рис.5).

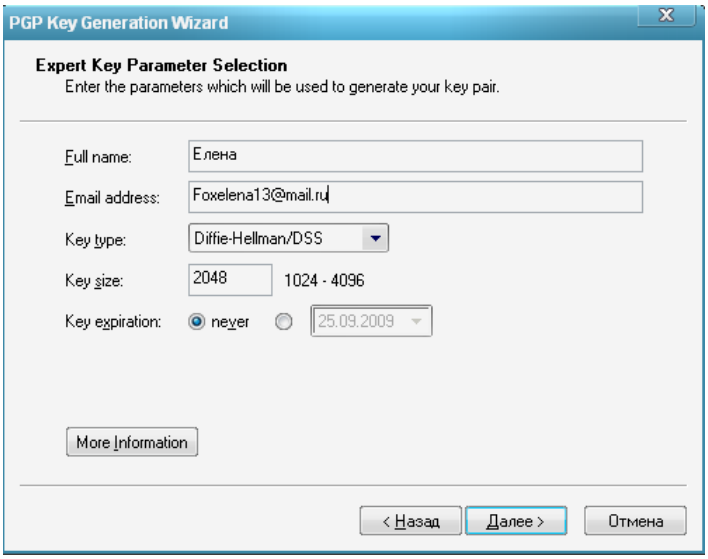

Рисунок 5 – Ввод параметров

В следующем окне нужно ввести парольную фразу дважды (рис.6). Парольная фраза – это сочетание нескольких слов, которое теоретически более надежно, чем парольное слово. В виду того, что парольная фраза состоит из нескольких слов, она практически неуязвима против так называемых «словарных атак», где атакующий пытается разгадать ваш пароль с помощью компьютерной программы, подключенной к словарю. Самые надежные парольные фразы должны быть достаточно длинными и сложными и должны содержать комбинацию букв из верхних и нижних регистров, цифровые обозначения и знаки пунктуации.

Нажать кнопку ДАЛЕЕ.

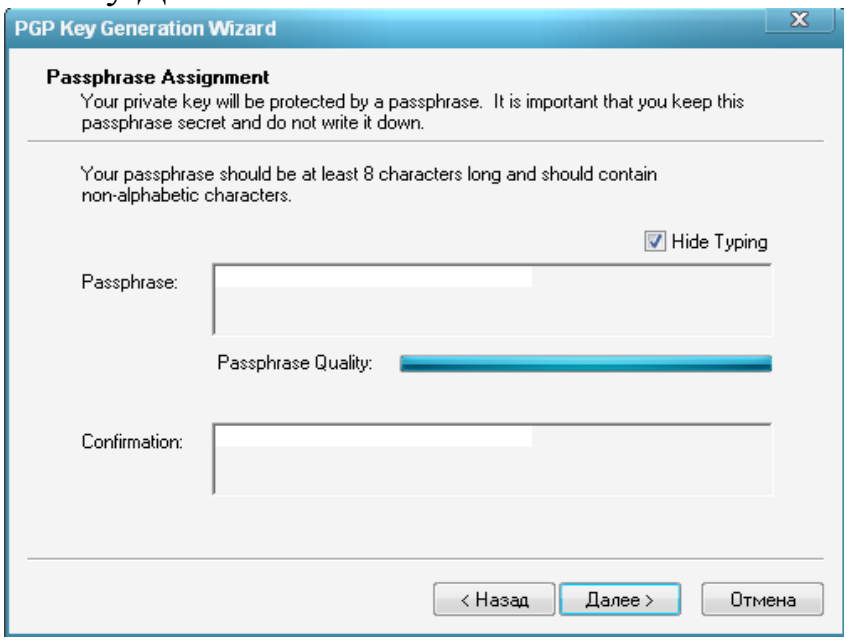

Рисунок 6 – Ввод парольной фразы

Появится окно, в котором сообщается, что генерация ключевой пары завершена успешно. Нажать кнопку ГОТОВО и сохранить ключи в файле (открытый в pubring.pkr, а секретный - secring.skr).

Затем нужно будет послать открытый ключ другому пользователю (рис.7). Для этого перетащите мышью ключ из главного окна PGPkeys в окно почтового сообщения. После этого пользователь, который получил ваш ключ, сможет шифровать направляемую вам почту. Чтобы посылать зашифрованные письма ему, вам потребуется получить его открытый ключ. Подписывать письма вы можете и без отправки своего открытого ключа другим

пользователям, но тогда никто не сможет проверить вашу подпись. Вы также можете отправить свой открытый ключ на публично доступный сервер ключей, с которого этот ключ смогут получить другие пользователи.

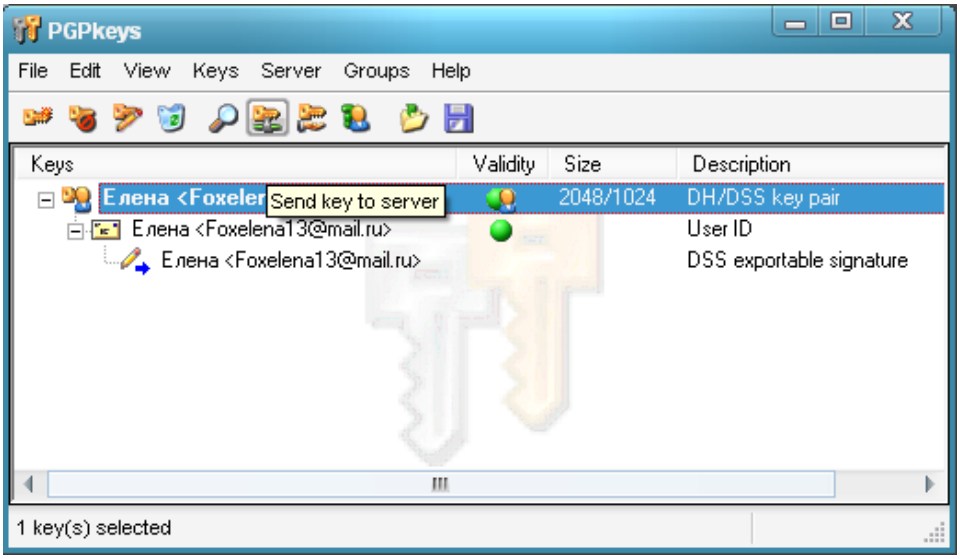

Рисунок 7 – Отправка открытого ключа

По завершению отправки ключа на сервер вы увидите следующее сообщение (Рис.8):

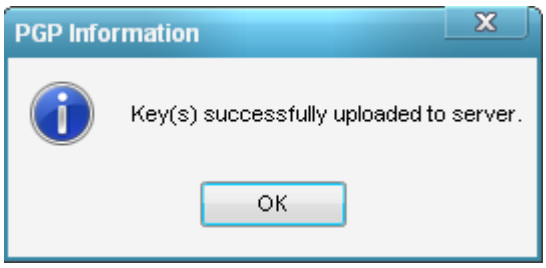

Рисунок 8 – Сообщение о завершении отправки

Как только вы получите открытый ключ своего корреспондента, надо его запустить, нажав на него двойным щелчком мышки, выделить его в окошке и выполнить команду IMPORT.

Теперь можно пересылать друг другу зашифрованные сообщения, которые шифруются открытым ключом получателя сообщения.

Чтобы подписать ключ, выделите его и выберите пункт Sign из меню Keys в PGPkeys. Вы можете затем указать степень

доверия, с которой вы относитесь к данному ключу, щелкнув на нем правой кнопкой мыши и выбрав из контекстного меню пункт Key Properties. Если вы укажете, что степень доверия к этому ключу является "полной" ("Complete"), другие ключи, подписанные его владельцем, будут считаться действительными.

Чтобы отозвать ключ, выделите его и выберите пункт Revoke из меню Keys в PGPkeys.

6.2 Отправка зашифрованного сообщения

После того, как открытый (публичный) ключ вашего корреспондента установится на вашем компьютере, сообщение можно отправлять получателю следующим образом:

1) Составляем сообщение в почтовой программе Outlook Express.

2) После того, как сообщение готово к отсылке, нажимаем один раз либо на третий значок справа на панели Outlook Express с изображением желтого конверта (Рис. 9) и замка (при этом кнопка просто вдавливается и больше ничего не происходит), либо в меню tools нажимаем на encrypt using PGP и затем нажимаем на команду в меню file под названием send later.

Рисунок 9 – Изображение значка панели Outlook Express

Тогда сразу же появится окошко программы PGP под названием Recipient selection, в котором необходимо найти и выделить мышкой публичный ключ своего корреспондента (получателя сообщения, который обычно именуется именем получателя) и нажать на O'K.

3) Сразу же после этого программа автоматически зашифрует сообщение и поместит его в папку исходящих сообщений outbox. Теперь можно заходить в Интернет и отправлять все сообщения, готовые к отправке.

6.3 Расшифровка сообщений

1. Открываем полученное зашифрованное сообщение и нажимаем на второй справа значок на панели Outlook Express, либо на команду меню PGP decrypt message. Через несколько секунд сообщение будет расшифровано и появится в окошке.

2. Существует еще один способ использования PGP, который чуть-чуть сложнее, чем шифрование через Outlook Express. Этот способ можно применять в том случае, если не удается установить PGP вместе с программой Outlook Exress.

Создаем сообщение в Outlook Express, затем выделяем его через команды edit - select all и копируем в буфер Windows через команду copy. После этого ставим мышку на значок PGP в панели задач, нажимаем на мышку и исполняем команду encrypt clipboard. Появляется окно диалога с PGP под названием key selection dialog (Рис.10).

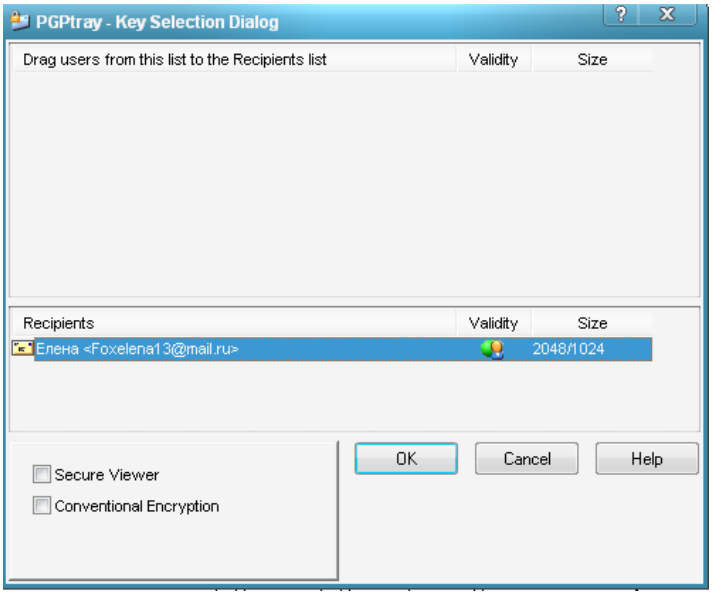

Рисунок 10 – Окно Key selection dialog

Необходимо выделить адрес (открытый ключ) корреспондента (ключ получателя сообщения)) в этом окне и щелкнуть по нему мышкой два раза, чтобы он появился внизу, потом нажимаем на O'K и программа зашифрует все содержимое clipboard.

После этого заходим в сообщение с текстом, который был ранее выделен, ставим мышку на поле сообщения, нажимаем на

правую кнопку мышки и исполняем команду paste. В результате зашифрованное содержимое clipboard заменяет предыдущее сообщение и на этом процесс шифровки закончился. Теперь можно отправлять сообщение обычным образом.

Расшифровывать полученные сообщения можно таким же образом: т.е. выделяем полученный зашифрованный текст, копируем его в буфер Windows clipboard, заходим мышкой в меню PGP через панель задач Windows и выбираем команду decrypt and verify clipboard. Появляется окно программы PGP, в которое необходимо ввести пароль (Рис.11).

Рисунок 11 – Окно для ввода пароля

Вводим пароль в это окно, нажимаем на O'K и перед нами предстает расшифрованное сообщение.

3. Также кроме этого способа можно применить еще один способ шифрования.

Можно создать текст в каком-либо редакторе, например в блокноте, и сохранить его в виде файла. После этого в проводнике выделяем файл, нажимаем на правую кнопку мышки и видим, что в нижней части команды опций появилась еще одна команда под названием PGP, после чего, поставив мышку на PGP, мы увидим раскрывающееся меню, состоящее из 4 команд:

- Encrypt;
- Sign;
- encrypt and sign;
- wipe.

Нажимаем на первую команду и перед нами появляется диалог выбора открытого ключа корреспондента, выбираем ключ, нажимаем на O'K, вводим пароль и файл зашифрован.

После этого рекомендуется выполнить еще одну команду в меню PGP: wipe (стереть, уничтожить оригинальный файл).

После этой операции у файла остается то же самое имя, но меняется тип расширения на <*.pgp>

Теперь этот файл можно прикрепить к сообщению и отправить вместе с ним.

В результате мы узнали, что существует три основных способа шифрования информации:

- напрямую в почтовой программе;
- через копирование текста в буфер обмена Windows;
- через шифрование всего файла, который затем прикрепляется к сообщению.

При работе с программой PGP появляется следующая проблема: при шифровании исходящих сообщений открытым ключом своего корреспондента, отправитель сообщений не может их потом прочитать, ввиду того, что исходящее сообщение шифруется с помощью закрытого ключа отправителя и открытого ключа его корреспондента, т.е. только получатель может прочитать такое сообщение. В результате получается, что отправитель не может впоследствии прочитать свои сообщения, отправленные им ранее.

В настройках PGP есть опция, позволяющая зашифровывать свои исходящие сообщения таким образом, чтобы их можно было потом прочитать (взять из архива и прочитать).

Для этого надо щелкнуть мышкой по символу PGP на панели задач, исполнить команду PGP preferences, зайти в General и поставить галочку напротив команды Always encrypt to default key

Кроме этого нужно зайти в PGP keys, выбрать мышкой свой ключ, зайти в меню keys и исполнить команду set as default key

Здесь же можно изменить свою парольную фразу: выделить мышкой свой ключ, нажать на правую кнопку мышки, исполнить команду key properties, change passphrase и поменять свою парольную фразу.

Кроме того, там же (в key properties) можно увидеть fingerprint или своеобразные "отпечатки пальцев", состоящие из комбинации цифр и букв. Эти отпечатки пальцев (идентификатор ключа) хороши тем, что можно предотвратить незаконное вторжение какими-либо людьми в вашу переписку. Т.е. кто-либо может перехватить ваш открытый ключ при отправке вашему корреспонденту или кому-либо еще и заменить своим открытым ключом. Когда ваш корреспондент получит этот ключ, то он будет думать, что это ваш ключ, когда в действительности это ключ третьего лица. Вы зашифровываете свое сообщение этим открытым ключом и в результате получается, что ваше сообщение не доходит до вашего корреспондента, а прочитывается другой третьей стороной, которая затем меняет это сообщение и отсылает вам под видом ответа от вашего корреспондента. Для того чтобы исключить такие проблемы, владельцы открытых ключей созваниваются по телефону и зачитывают друг другу отпечатки своих ключей. В таком случае достигается 100% надежность того, что информация не попала в чужие руки.

6.4 PGP диск

PGP диск – это удобное приложение, которое позволяет вам отвести некоторую часть вашего жесткого диска для хранения конфиденциальной информации. Это зарезервированное место используется для создания файла под именем <PGP disk>.

Этот один файл действует подобно вашему жесткому диску - он выполняет функцию хранения ваших файлов и исполняемых программ. Для того, чтобы использовать программы и файлы, находящиеся на нем, вы его устанавливаете <mount>, после чего его можно использовать также, как любой другой диск. После того, как вы отключите <unmount> этот диск, он станет недоступным для третьих лиц и для того, чтобы открыть его, необходимо ввести парольную фразу, которая известна только вам. Но даже разблокированный диск защищен от несанкционированного доступа. Если ваш компьютер зависнет во время использования диска, то его содержание будет зашифровано.

Одним из наиболее важных преимуществ и удобств использования программы PGPdisk является тот факт, что теперь

нет необходимости шифровать большое количество файлов, в которых находится конфиденциальная информация. Теперь можно переместить все конфиденциальные файлы и даже программы на такой диск и таким образом избежать необходимости каждый раз расшифровывать какой-либо файл при его открытии.

Для того чтобы установить новый PGP диск, необходимо выполнить следующие команды:

Пуск – Программы – PGP – PGPdisk, после чего появится окно приветствия. Нажать кнопку ДАЛЕЕ. В следующем окне выбрать расположение и размер PGP диска.

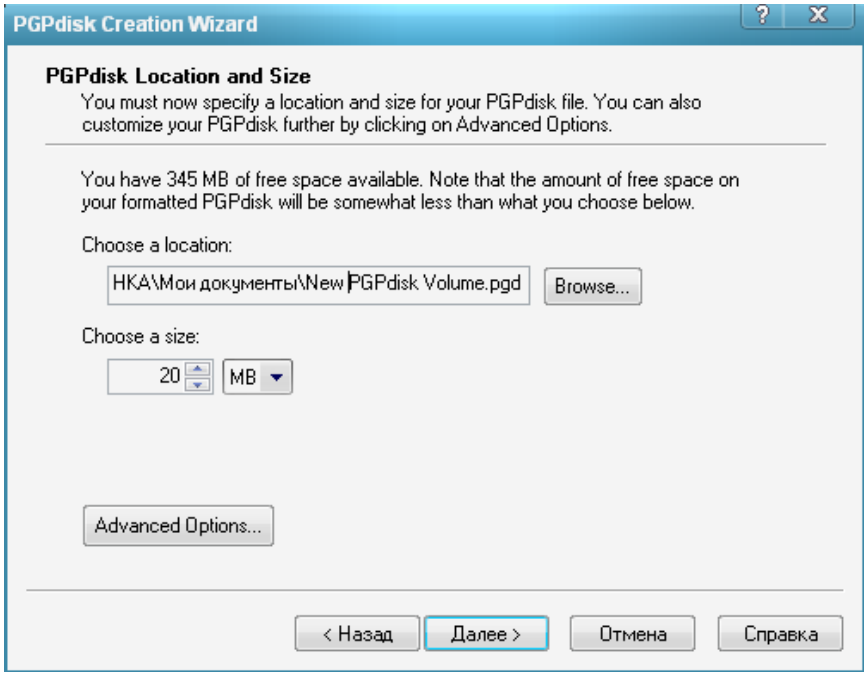

Рисунок 12 – Окно расположения PGP диска

Далее следует выбор метода защиты: открытый ключ или парольная фраза. Начнется процесс создания PGP диска. Нажать кнопку ГОТОВО.

6.5 Установка PGP диска

Как только новый диск будет создан, программа PGP автоматически его установит с тем, чтобы вы могли начать его использовать (рис.13).

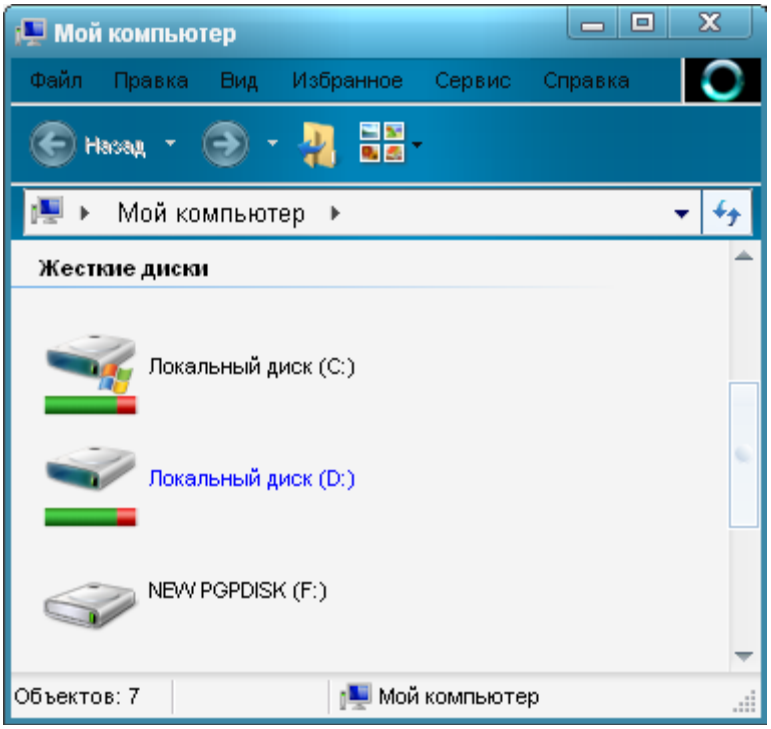

Рисунок 13 – Отображение нового PGP диска

После того, как вы закончили работу с конфиденциальной информацией, необходимо отключить диск. После отключения диска его содержимое будет зашифровано в виде зашифрованного файла.

Для открытия PGP диска надо дважды щелкнуть по нему мышкой и дважды ввести парольную фразу в появившееся окно программы. Вы сможете убедиться в том, что PGP диск открылся, зайдя в мой компьютер и увидев, что рядом с диском C появился диск D. В том случае, если у вас уже есть диск D, то новый диск получит следующую букву E и т.д. Зайти на новый диск можно через мой компьютер или другую оболочку просмотра файлов.

6.6 Закрытие PGP диска

Закройте все программы и файлы, имеющиеся на диске PGP, т.к. невозможно закрыть диск, если файлы на этом диске до сих пор еще открыты. Теперь зайдите в мой компьютер выделите мышкой диск PGP, нажмите на правую кнопку мышки и выберите команду <unmount> в появившемся меню <PGP disk>.

Как только диск будет закрыт, то он исчезнет из моего компьютера и превратится в зашифрованный файл на диске С.

Еще один важный момент, на который необходимо обратить внимание, это настройки программы, которые позволяют автоматически закрыть диск в случае не обращения к диску в течение какого-либо периода времени. Для этого надо исполнить команду <prefs> в программе PGPdisk и в появившемся меню под названием <auto unmount> (автоматическое закрытие) выделить флажками все три команды:

- auto unmount after __ minutes of inactivity (автоматически закрыть после __ минут бездействия). Здесь также необходимо указать количество минут.
- auto unmount on computer sleep (автоматически закрыть при переходе компьютера в спящее состояние)
- prevent sleep if any PGPdisks could not be unmounted (не позволить компьютеру перейти в состояние спячки, если PGP диск не был закрыт).

7. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Для чего служит программный продукт PGP?
2. Какие алгоритмы лежат в основе работы PGP?
3. Каким образом шифруется сообщение?
4. Кто может расшифровать сообщение?
5. Каковы преимущества используемого способа шифрования?
6. Можно ли расшифровать сообщение с помощью ключа шифрования?
7. Что такое парольная фраза?
8. Опишите процесс отправки зашифрованного сообщения.
9. Перечислите три основных способа шифрования информации.
10. Как происходит расшифровка сообщений?
11. Для чего предназначена программа PGPdisk?
12. Каковы преимущества использования программы PGPdisk?