Указания к выполнению лабораторных работ

УСТАНОВКА И ПРИМЕНЕНИЕ ПРОГРАММЫ PGP

Настоящая глава посвящена основным приемам работы с криптографической программой PGP (Pretty Good Privacy).

PGP – это криптографическая (шифровальная) программа с высокой степенью надежности, которая позволяет пользователям обмениваться информацией в электронном виде в режиме полной конфиденциальности.

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.

В PGP применяется принцип использования двух взаимосвязанных ключей: открытого и закрытого. К закрытому ключу имеете доступ только вы, а свой открытый ключ вы распространяете среди своих корреспондентов.

Великолепное преимущество этой программы состоит также в том, что она бесплатная и любой пользователь, имеющий доступ к Интернету, может ее «скачать» на свой компьютер в течение получаса. PGP шифрует сообщение таким образом, что никто кроме получателя сообщения, не может ее расшифровать. Создатель PGP Филипп Циммерман открыто опубликовал код программы, который неоднократно был исследован специалистами крипто-аналитиками высочайшего класса и ни один из них не нашел в программе каких-либо слабых мест.

Филипп Циммерман следующим образом объясняет причину создания программы: *«Людям необходима конфиденциальность. PGP распространяется как огонь в прериях, раздуваемый людьми, которые беспокоятся о своей конфиденциальности в этот информационный век. Сегодня организации по охране прав человека используют программу PGP для защиты своих людей за рубежом. Организация Amnesty International также использует ее».*

Пользователям сети «Интернет» рекомендуется использовать эту программу именно по той же причине, почему люди предпочитают посылать друг другу письма в конвертах, а не на открытках, которые могут быть легко прочитаны почтовыми служащими. Дело в том, что электронные сообщения, в том виде и формате, который существует на сегодняшний день, легко могут быть прочитаны и архивированы любым человеком, имеющим доступ к серверу Интернет провайдера (поставщика услуг сети «Интернет»). В настоящий момент спецслужбам проще и дешевле подключиться к электронным адресам большого количества лиц, нежели к телефонным разговорам. Здесь вообще ничего делать не надо. Все сделает компьютер. Агенту спецслужбы или другому заинтересованному человеку остается только сесть за компьютер и просмотреть все ваши сообщения. Научно-технический прогресс облегчил задачу таким людям, однако, этот же самый прогресс предоставил возможность пользователям сети «Интернет» скрыть свои сообщения от третьих лиц таким образом, что даже суперкомпьютер стоимостью несколько десятков миллионов долларов не способен их расшифровать.

КАК PGP РАБОТАЕТ

Когда пользователь шифрует сообщение с помощью PGP, то программа сначала сжимает текст, что сокращает время на отправку сообщения через модем и увеличивает надежность шифрования. Большинство приемов криптоанализа (взлома зашифрованных сообщений) основаны на исследовании «рисунков», присущих текстовым файлам, что помогает взломать ключ. Сжатие ликвидирует эти «рисунки» и таким образом повышает надежность зашифрованного сообщения. Затем PGP генерирует сессионный ключ, который представляет собой случайное число, созданное за счет движений вашей мышки и нажатий на клавиши клавиатуры.

Как только данные будут зашифрованы, сессионный ключ зашифровывается с помощью публичного ключа получателя сообщения, который отправляется к получателю вместе с зашифрованным текстом.

Расшифровка происходит в обратной последовательности. Программа PGP получателя сообщения использует закрытый ключ получателя для извлечения временного сессионного ключа, с помощью которого программа затем дешифрует зашифрованный текст.

КЛЮЧИ

Ключ – это число, которое используется криптографическим алгоритмом для шифрования текста. Как правило, ключи - это очень большие числа. Размер ключа измеряется в битах. Число, представленное 1024 битами – очень большое. В публичной криптографии, чем больше ключ, тем его сложнее взломать.

В то время как открытый и закрытый ключи взаимосвязаны, чрезвычайно сложно получить закрытый ключ исходя из наличия только открытого ключа, однако это возможно при наличии большой компьютерной мощности. Поэтому крайне важно выбирать ключи подходящего размера: достаточно большого для обеспечения безопасности и достаточно малого для обеспечения быстрого режима работы. Кроме этого, необходимо учитывать личность того, кто намеревается прочитать ваши зашифрованные сообщения, насколько он заинтересован в их расшифровке, каким временем он обладает, и какие у него имеются ресурсы.

Более большие ключи будут более надежными в течение более длительного срока времени. Поэтому если вам необходимо зашифровать информацию с тем, чтобы она хранилась в течение нескольких лет, то необходимо использовать более крупный ключ.

Ключи хранятся на жестком диске вашего компьютера в зашифрованном состоянии в виде двух файлов: одного для открытых ключей, а другого - для закрытых. Эти файлы называются «кольцами» (keyrings). В течение работы с программой PGP вы, как правило, будете вносить открытые ключи ваших корреспондентов в открытые «кольца». Ваши закрытые ключи хранятся в вашем закрытом «кольце». При потере вашего закрытого «кольца» вы не сможете расшифровать любую информацию, зашифрованную с помощью ключей, находящихся в этом «кольце».

ЦИФРОВАЯ ПОДПИСЬ

Огромным преимуществом публичной криптографии также является возможность использования цифровой подписи, которая позволяют получателю сообщения

удостовериться в личности отправителя сообщения, а также в целостности (верности) полученного сообщения. Цифровая подпись исполняет ту же самую функцию, что и ручная подпись. Однако ручную подпись легко подделать. Цифровую же подпись почти невозможно подделать.

ХЭШ-ФУНКЦИЯ

Еще одно важное преимущество использования PGP состоит в том, что PGP применяет так называемую «хэш-функцию», которая действует таким образом, что в том случае какого-либо изменения информации, пусть даже на один бит, результат «хэш-функции» будет совершенно иным. С помощью «хэш-функции» и закрытого ключа создается «подпись», передаваемая программой вместе с текстом. При получении сообщения получатель использует PGP для восстановления исходных данных и проверки подписи.

При условии использования надежной формулы «хэш-функции» невозможно вытащить подпись из одного документа и вложить в другой, либо каким-то образом изменить содержание сообщения. Любое изменение подписанного документа сразу же будет обнаружено при проверке подлинности подписи.

ПАРОЛЬНАЯ ФРАЗА

Большинство людей, как правило, знакомы с парольной системой защиты компьютерных систем от третьих лиц.

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.

Парольная фраза должна быть такой, чтобы ее потом не забыть и чтобы третьи лица не могли ее разгадать. Если вы забудете свою парольную фразу, то уже никогда не сможете восстановить свою зашифрованную информацию. Ваш закрытый ключ абсолютно бесполезен без знания парольной фразы и с этим ничего не поделаешь.

ОСНОВНЫЕ ШАГИ В ИСПОЛЬЗОВАНИИ ПРОГРАММЫ PGP

1. Установите программу на свой компьютер. Руководствуйтесь краткой инструкцией по инсталляции программы, приведенной ниже.

2. Создайте закрытый и открытый ключ. Перед тем, как вы начнете использовать программу PGP, вам необходимо генерировать пару ключей, которая состоит из закрытого ключа, к которому имеете доступ только вы, и открытый ключ, который вы копируете и свободно передаете другим людям (вашим корреспондентам).

3. Распространите свой открытый ключ среди своих корреспондентов в обмен на их ключи. Ваш открытый ключ, это всего лишь маленький файл, поэтому его можно либо воткнуть в сообщение, копировать в файл, прикрепить к почтовому сообщению или разместить на сервере.

4. Удостовериться в верности открытого ключа. Как только вы получите открытые ключи своих корреспондентов, то их можно внести в «кольцо» открытых ключей. После этого вам необходимо убедиться в том, что у вас действительно открытый ключ вашего корреспондента. Вы можете это сделать, связавшись с этим корреспондентом и, попросив его зачитать вам по телефону «отпечатки пальцев» (уникальный идентификационный номер) его открытого ключа, а также сообщив ему номер вашего ключа. Как только вы убедитесь в том, что ключ действительно принадлежит ему, вы можете его подписать и таким образом подтвердить ваше доверие к этому ключу.

5. Шифрование и удостоверение корреспонденции вашей цифровой подписью. После генерации пары ключей и обмена открытыми ключами вы можете начать шифрование и удостоверение ваших сообщений и файлов своей цифровой подписью. Если вы используете почтовую программу, которая поддерживается программой PGP, то вы можете шифровать и дешифровать всю вашу корреспонденцию, находясь прямо в этой программе. Если же ваша почтовая программа не поддерживается программой PGP, то вы можете шифровать вашу корреспонденцию другими способами (через буфер обмена или шифрованием файлов целиком).

6. Дешифровка поступающих к вам сообщений и проверка подлинности отправителя. Когда кто-либо высылает вам зашифрованное сообщение, вы можете дешифровать его и проверить подлинность отправителя этого сообщения и целостность самого сообщения. Если ваша почтовая программа не поддерживается PGP, то вы можете сделать это через буфер обмена.

7. Уничтожение файлов. Когда вам необходимо полностью удалить какой-либо файл, вы можете исполнить команду wipe (стереть). Таким образом, удаленный файл уже невозможно будет восстановить.

ИНСТАЛЛЯЦИЯ ПРОГРАММЫ PGP

Ниже приводятся заголовки сообщений, появляющиеся при инсталляции программы (нажатии на инсталляционный файл с расширением .exe) и команды, которые необходимо исполнять при инсталляции:

PGP Installation program

Нажмите на **Next**

Software License agreement

Нажмите на **Yes**

User information

*Name*_____

Company _____

Введите свое имя, название компании и нажмите на Next

Setup: choose installation directory

Нажмите на **Next**

Select components:

Здесь необходимо выбрать компоненты для установки

*** Program files**

Eudora Plugin

*** Microsoft Exchange/Outlook plugin**

*** Microsoft Outlook Express plugin**

*** User's manual Adobe**

*** PGP disk for Windows**

Выделите те компоненты, которые необходимо установить. Если вы не используете почтовую программу Eudora, то ее не нужно выделять. Если вы используете Microsoft Exchange/Outlook для работы в сети «Интернет», то выделите ее. То же самое касается Microsoft Outlook, почтовой программы, встроенной в Windows-98.

Нажмите на **Next**

Check setup information

Нажмите на **Next**

Начинается копирование программных файлов на жесткий диск компьютера.

Для того чтобы программа автоматически запустила операцию создания ключей после перезагрузки компьютера нажать на кнопку **"Yes I want to run PGP keys"**

Нажмите на **Finish**

Restart Windows для перезагрузки Windows.

Нажмите на **O'K**

Компьютер перезапустится и на этом программа установки завершится.

Теперь необходимо установить на компьютер два ключа:

public key - открытый ключ

private key - закрытый ключ

ГЕНЕРАЦИЯ КЛЮЧЕЙ

После перезагрузки компьютера в нижнем правом углу (панель задач) появится значок PGP - символ амбарного замка.

Поставьте на него мышку, нажмите на мышку и выберите в открывшемся меню команду **Launch PGP keys.**

Зайдите в меню KEYS и выполните команду **NEW KEY**

Нажмите на **next**

Введите свое имя и электронный адрес

Нажмите на **next**

Выберите размер ключа **2048** и нажмите на **next**

Затем выделите фразу **key pair never expires** (срок действия ключевой пары никогда не истекает) и нажмите на **next.**

Два раза введите секретный пароль и нажмите на **next.**

Программа начнет генерировать пару ключей. Если программе не хватает информации, то она может попросить нажать на несколько клавиш наугад и подвигать мышку. Это необходимо выполнить.

Затем программа сообщит, что процесс генерации ключей закончен.

Нажмите на **next.**

Потом еще раз нажмите на **next.**

Затем нужно нажать на команду **done.**

На этом процесс создания пары ключей закончился и можно начинать пользоваться программой.

Теперь после установки программы необходимо обменяться со своими корреспондентами открытыми ключами. Для этого необходимо исполнить команду **LAUNCH PGP KEYS**, выделить свой ключ (файл со своим именем) в окошке, нажать на правую кнопку мышки и выбрать команду **EXPORT.**

Появится окошко, с помощью которого можно указать путь, где сохранить файл с названием <ваше имя.asc>

Этот файл необходимо выслать своему корреспонденту, в обмен на его открытый ключ.

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.

КАК ПОСЛАТЬ ЗАШИФРОВАННОЕ СООБЩЕНИЕ

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

Составляем сообщение в почтовой программе Outlook Express.

После того, как сообщение готово к отсылке, нажимаем один раз либо на третий значок справа на панели Outlook Express с изображением желтого конверта 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.**

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.

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.

РАСШИФРОВКА СООБЩЕНИЙ

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.

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**

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

Естественно, перед тем, как это сделать, необходимо создать пару ключей, как было описано ранее.

Также кроме этого способа можно применить еще один способ шифрования **(третий способ).**

Можно создать текст в каком-либо редакторе, например 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). Иначе, какой смысл шифровать файл, если на диске компьютера остался первоначальный 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:

- Первый - самый удобный, напрямую в почтовой программе;
- Второй - через копирование текста в буфер обмена Windows;
- Третий - 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.

Парольную фразу рекомендуется менять, по крайней мере, раз в полгода, хотя если вы постарались создать надежную парольную фразу и исключили какую-либо возможность разгадки этой фразы кем бы то ни было, то этого можно и не делать.

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.

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>.

Хотя это всего лишь один файл, он действует подобно вашему жесткому диску в том отношении, что он выполняет функцию хранения ваших файлов и исполняемых программ. Вы можете его себе представить в виде флоппи дискеты или внешнего жесткого диска. Для того, чтобы использовать программы и файлы, находящиеся на нем, вы его устанавливаете <mount>, после чего его можно использовать также, как любой другой диск. Вы можете установить программы внутри этого диска либо копировать на

него файлы. 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 программы со следующими командами:

new – создать новый PGP диск

mount – установить созданный диск путем ввода парольной фразы

unmount – закрыть диск (зашифровать), который был ранее установлен

prefs – опции настройки

Как создать новый PGP диск

1. Запустите программу PGPdisk

2. Исполните команду New, после чего на экране появится мастер создания PGP диска.

3. Нажмите на next

4. Появится окошко создания PGP диска, в котором необходимо указать путь, где новый диск под названием <New PGPdisk1> надо сохранить.

5. Нажмите на кнопку Save и файл под этим названием сохранится на диске, выбранном вами (по умолчанию на диске C).

6. Под надписью <PGPdisk Size field> введите цифру, обозначающую размер PGP диска и не забудьте выбрать килобайты или мегабайты там же.

7. Под надписью <PGPdisk Drive Letter Field> подтвердите букву, которую вы присвоите новому диску.

8. Нажмите на next

9. Введите парольную фразу, которую в дальнейшем необходимо будет вводить для установки нового диска. Введите парольную фразу два раза.

10. Нажмите на next

11. При необходимости подвигайте мышку или нажимайте на кнопки на клавиатуре для того, чтобы программа сгенерировала новый ключ

12. Нажмите на next. Столбик покажет вам инициализацию создания нового диска.

13. Еще раз нажмите на next, с тем, чтобы окончательно установить новый PGP диск.

14. Нажмите на Finish.

15. Введите название нового диска.

16. Нажмите на Start

17. Нажмите на OK (на диске еще нет данных). Компьютер скажет вам, когда закончится форматирование диска.

18. Нажмите на кнопку Close на окне форматирования. Теперь ваш новый диск появится на том диске, который вы ранее указали (по умолчанию диск C). Для того, чтобы открыть диск, надо дважды нажать на него мышкой.

Как установить PGP диск

Как только новый диск будет создан, программа PGP автоматически его установит с тем, чтобы вы могли начать его использовать. После того, как вы закончили работу с конфиденциальной информацией, необходимо отключить диск. После отключения диск 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.

Использование установленного PGP диска

На диске PGP можно создавать файлы, каталоги, перемещать файлы или каталоги, либо стирать, т.е. можно делать те же самые операции, что и на обычном диске.

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 C.

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)

Смена парольной фразы:

1. Убедитесь в том, что PGP диск не установлен. Невозможно сменить парольную фразу в том случае, если диск установлен.

2. Выберите команду <Change Passphrase> из меню <File>

3. Выберите тот диск, парольную фразу для которго вы хотите изменить.

4. Введите старую парольную фразу. Нажмите на OK. Появится окошко для ввода новой парольной фразы.

5. Введите новую парольную фразу. Минимальная длина парольной фразы: 8 знаков

6. Нажмите на OK. Окошко новой парольной фразы <New passphrase> закроется.

Удаление парольной фразы

1. Убедитесь в том, что PGP диск не установлен.

2. Выберите команду <Remove passphrase> из меню <File>. Появится окошко, которое попросит вас ввести парольную фразу, которую необходимо отменить.

3. Введите пароль и нажмите на OK.

Примечание: программу PGP можно бесплатно скачать в Интернете по следующему адресу: http://www.pgpi.com