А.М. Голиков

ЗАЩИТА ДАННЫХ С ПОМОЩЬЮ PGP

**Методические указания по лабораторной работе для студентов специальностей
090106 «Информационная безопасность телекоммуникационных систем» и
210403 «Защищенные системы связи»**

Томск - 2007

ЗАЩИТА ДАННЫХ С ПОМОЩЬЮ PGP

1 Цель работы

Целью данной лабораторной работы является получение практических навыков по управлению ключами, шифрованию, расшифрованию, электронному подписанию документов/файлов и их безвозвратному удалению с диска посредством криптографической программы Pretty Good Privacy (PGP).

2 Методические указания

Все пользователи Интернета должны отчётливо понимать, что отправка обычного незашифрованного электронного послания аналогична отправке открытки почтой неэлектронной: такое сообщение может быть прочитано кем угодно и где угодно на участке между отправителем и получателем даже без всякой нужды осуществлять его целенаправленный перехват. Копия сообщения остаётся в кэше сервера вашего Интернет-провайдера, сетевые серверы у вас на работе, в университете или в Интернет-кафе, не говоря о бесплатных почтовых службах вроде mail.ru, также сохраняют копию, копии остаются на всех серверах, через которые сообщение проходит по пути к адресату. Системные администраторы этих серверов могут по своему желанию прочитать письмо и переслать его, кому захотят. Спецслужбы крупных государств в рабочем порядке сканируют электронную почту на предмет подозрительных ключевых слов и фраз. Деловые послания могут представлять интерес для ещё большего круга лиц – от конкурентов до организованной преступности – и ставки в этой игре оказываются гораздо выше.

С помощью PGP вы можете зашифровать сообщение для своего адресата, даже если никогда прежде с ним не общались. Все эти организации и люди смогут по-прежнему получить доступ к зашифрованному письму, но уже не будут иметь ни малейшего представления о его содержании, словно вы поместили его в непроницаемый конверт.

Pretty Good Privacy (буквально – "очень неплохая защита приватности"), свободно распространяемая криптографическая программа. Простая в использовании, PGP сегодня стоит на страже частной жизни миллионов пользователей Интернета.

PGP была придумана американским математиком и программистом Филипом Зиммерманом (Philip Zimmermann) в 1991 году. Получилась бесплатная программа для массового пользователя на основе алгоритма с открытым ключом. Она сразу стала набирать популярность. Правительство США пыталось бороться с распространением PGP (да и вообще стойкой гражданской криптографии). Зиммерману даже было предъявлено обвинение в "незаконном экспорте вооружений". Но энтузиасты со всех стран мира уже вовсю размещали PGP у себя на сайтах, изучали код программы и переводили ее на другие языки. В конце концов власти махнули рукой на это дело, и сегодня PGP работает на миллионах компьютеров.

2.1 Основы

2.1.1 Интерфейс

PGP предоставляет пользователю ряд альтернативных путей для доступа функциям программы, выбор конкретного зависит от решаемой вами задачи.

Существует четыре способа, которыми вы можете добраться до нужных функций и компонентов программы:

- Иконка PGPtray.
- Контекстное меню Проводника Windows.
- Меню Пуск.

- Плагины в email-клиентах.

Наиболее удобный и часто используемый путь – это иконка PGPtray (, в зависимости от версии Windows может быть либо золотой, либо серой), расположенная в системном трее – в правой части панели задач Windows рядом с системными часами (рисунок 2.1). Оттуда вы можете быстро произвести любые операции шифрования с содержимым буфера обмена или активного окна, например, email-клиента, текстового редактора или формы на интернет-сайте, получить доступ к меню настроек PGP или к любому из компонентов программы.

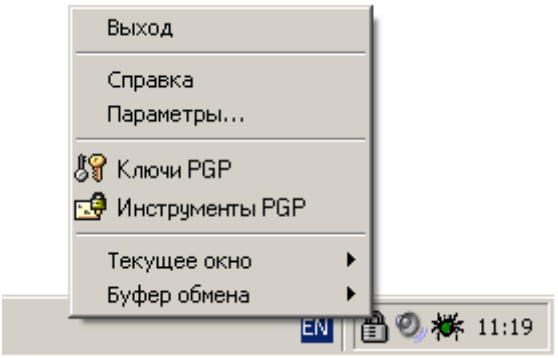

Рис. 2.1

Нажав на эту иконку, вам открывается следующее меню:

- *Выход* – скрыть иконку PGPtray.
- *Справка* – справочник по работе с программой.
- *Параметры* – меню настроек программы.
- *Ключи PGP* – позволяет быстро получить доступ к соответствующему компоненту программы.
- *Инструменты PGP* – предоставляет доступ к основным функциям шифрования, уничтожения файлов и очистки свободного пространства дисков.
- *Текущее окно* – операции с содержимым активного окна позволяют зашифровать, расшифровать, поставить или сверить электронную подпись с текстовой информации используемого в данный момент приложения (например, текстового редактора).
- *Буфер обмена* – аналогичные операции с содержимым буфера обмена позволяют, кроме перечисленного выше, быстро очистить или отредактировать находящийся в нём текст.

Вы можете воспользоваться средствами шифрования PGP из Проводника, нажав правой кнопкой на имя того или иного файла или папки, а затем в появившемся контекстном меню из пункта *PGP* выбрав нужную операцию (рисунок 2.2). Это весьма удобный способ работы с файлами.

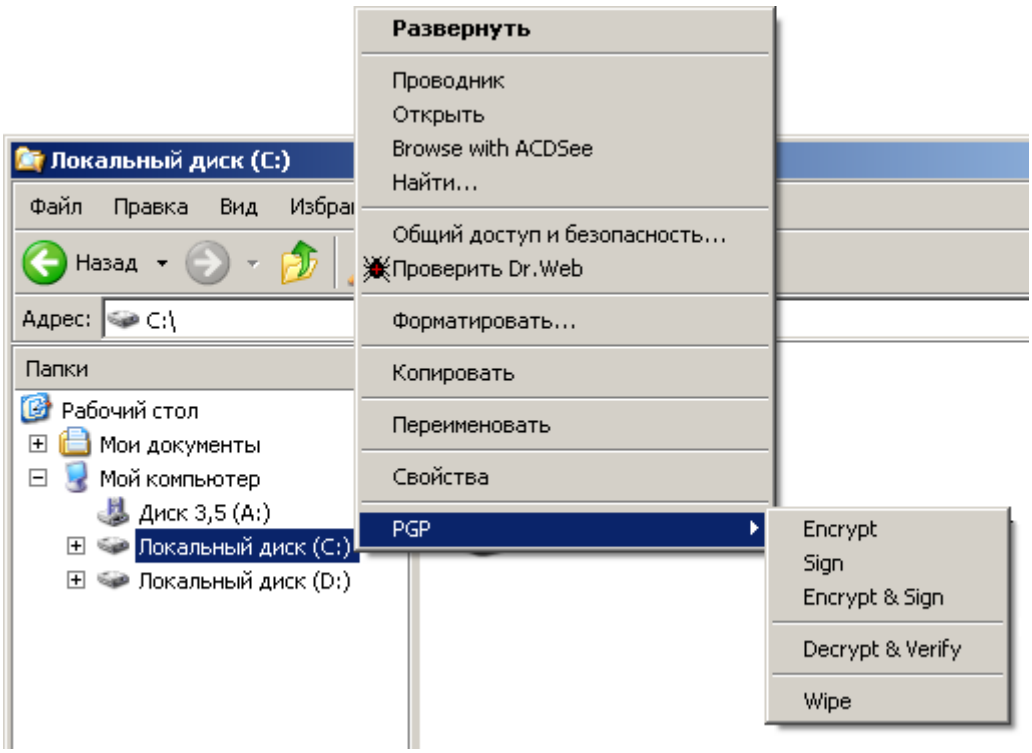

Рис. 2.2

Содержимое контекстного меню и список доступных функций напрямую зависят от выбранного объекта.

- **Для дисков и папок.** Нажав правой кнопкой на любой из накопителей или папку и выбрав в главном контекстном меню пункт *PGP*, вы можете сделать следующее:
  - Зашифровать (*Encrypt*), расшифровать (*Decrypt*), поставить (*Sign*) или сверить (*Verify*) электронные подписи с содержащихся на диске / в папке файлов.
  - Удалить файлы с диска или папку со всем ее содержимым (*Wipe*).
- **Для файлов.** Нажав правой кнопкой на файл и выбрав в главном контекстном меню пункт *PGP*, в зависимости от типа файла вы можете сделать следующее:
  - Если выбран любой незашифрованый файл, вы можете уничтожить его (*Wipe*), зашифровать (*Encrypt*), подписать (*Sign*).
  - Если выбран зашифрованный / подписанный файл, вы можете уничтожить его (*Wipe*) или расшифровать / сверить подпись (*Decrypt* & *Verify*).
  - Если выбран файл в ASCII-формате (*.asc), вы можете уничтожить его (*Wipe*) или расшифровать / сверить подпись (*Decrypt* & *Verify*). При выборе последнего варианта для файла, содержащего материал ключа, вам будет предложено импортировать его на свою связку.
  - Если выбран файл связки открытых или закрытых ключей (*.pkr или *.skr соответственно), вы можете уничтожить его (*Wipe*) или импортировать содержащиеся в нём ключи на свою связку.

2.1.2 Компоненты PGP

Основными компонентами PGP являются ключи PGP (PGPkeys) и инструменты PGP (PGPtools).

Менеджер PGPkeys имеет средства управления вашими парами открытых и закрытых ключей, а также открытыми ключами ваших корреспондентов (рисунок 2.3).

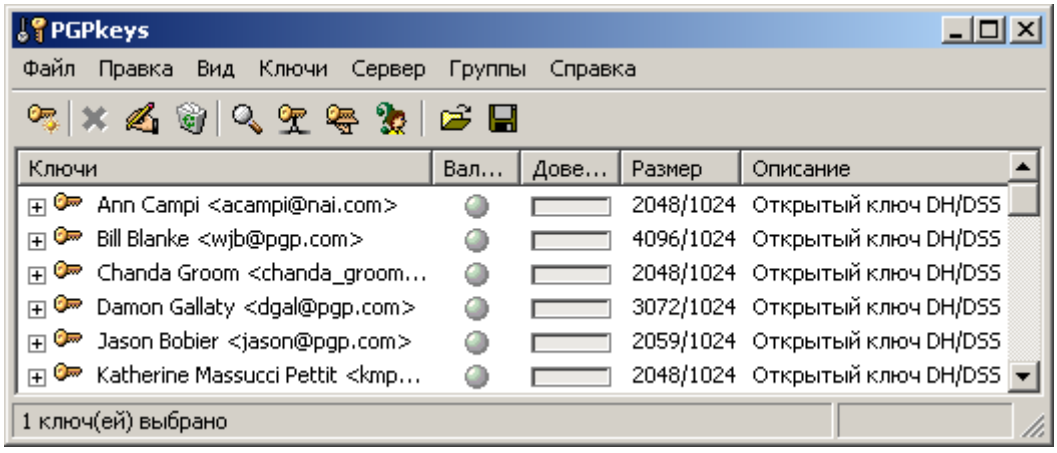

Рис. 2.3

Чтобы открыть компонент PGPkeys:

1. нажмите иконку PGPtray ( );
2. из меню выберите *Ключи PGP*.

PGPtools – это небольшое плавающее окошко, предоставляющее доступ к основным функциям шифрования, уничтожения файлов и очистки свободного пространства дисков (рисунок 2.4).

Рис. 2. 4

Чтобы открыть компонент PGPtools:

1. нажмите иконку PGPtray ( );
2. из меню выберите *PGPtools*.

2.1.2 Настройка

Изначальная настройка PGP пригодна для большинства пользователей. Тем не менее, предпочтительно перенастроить программу под специфику ваших условий и нужд до начала её эксплуатации. Ниже приведено описание всех опций настройки программы и рекомендации, могущие помочь в выборе конкретного варианта. Если сомневаетесь, какой вариант выбрать, опирайтесь на здоровую параною: чуть более строгие меры безопасности не доставят много дискомфорта, но помогут надёжнее сберечь информацию.

Будьте очень внимательны: некорректная настройка способна сильно повлиять на функциональность и безопасность работы программы.

Открыть меню настроек программы можно двумя разными способами:

- Нажать иконку PGPtray ( ) > *Параметры*.
- В окне любого компонента PGP в строке меню выбрать *Правка* > *Настройки*.

2.1.2.1 Общие

Вкладка *Общие* содержит основные настройки PGP, связанные с общим функционированием программы (рисунок 2.5).

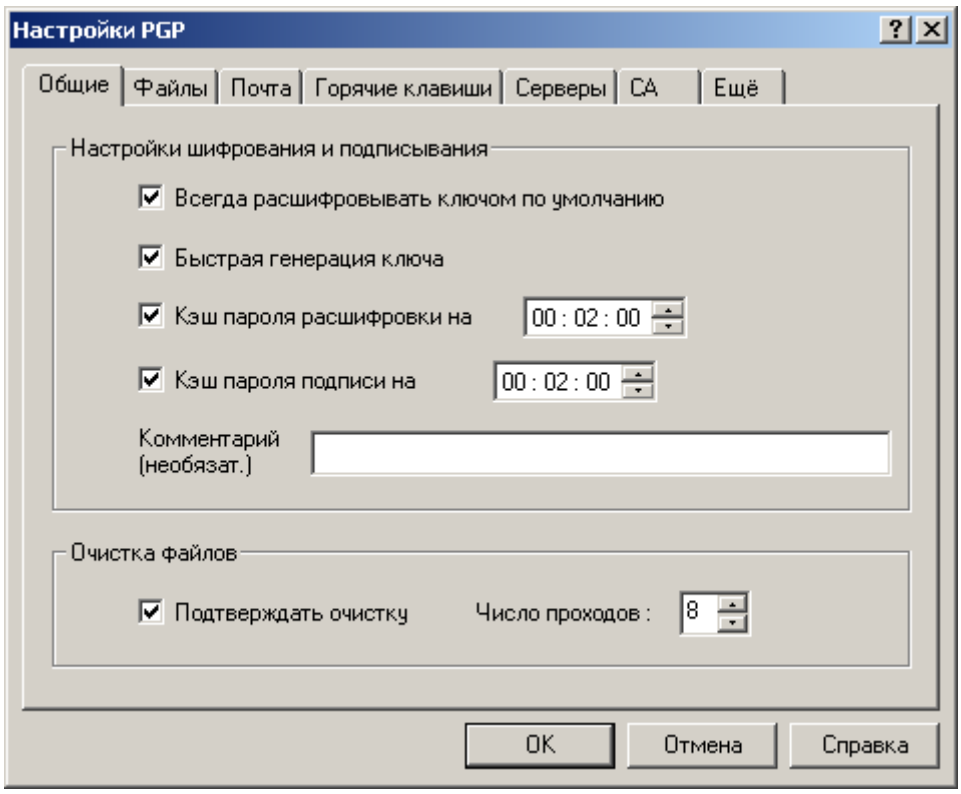

Рис. 2.5

Раздел Настройки шифрования и подписывания

- *Всегда расшифровывать ключом по умолчанию.*
- *Быстрая генерация ключа* – быстрая генерация ключей Diffie-Hellman / DSS. При включении данной опции, программа будет в несколько раз быстрее создавать ключи DH/DSS, используя набор предварительно расчитанного математического материала, ложащегося в их основу, вместо его вычисления с нуля. Учтите, эта опция имеет значение только для генерации ключей DH/DSS, но не для RSA вследствие особенностей самих алгоритмов. Считается, что знание этого предрассчитанного материала не даёт взломщику преимуществ для осуществления атаки на ключи DH/DSS, и включение опции не несёт ущерба безопасности; но если вам от этого всё равно неуютно, можете эту опцию отключить, что и рекомендуется сделать, если вы не планируете генерировать очень много ключевых пар (чего, как правило, не требуется).
- *Комментарий* – сюда можно вписать короткий комментарий, который будет отображаться во всех зашифрованных или подписанных вами сообщениях в поле *Comment* после служебного заголовка *BEGIN PGP MESSAGE* или *BEGIN PGP SIGNATURE*. Комментарий никак не влияет на безопасность и сам может быть любым образом изменён вами или посторонним уже в зашифрованном или подписанном сообщении, поскольку не входит в сообщение, а является только служебным блоком данных. Для этой опции рекомендации отсутствуют: пишите или не пишите на своё усмотрение.
- *Кэш пароля расшифровки/подписи на …* Если вы покинете рабочее место не перезагрузив компьютер или не очистив кэш, любой посторонний человек сможет беспрепятственно расшифровать ваши файлы и подделать подпись! В этом режиме программа будет хранить введённую ключевую фразу в памяти только указанный здесь срок. Это удобно, когда нужно расшифровать / подписать сразу несколько файлов, но не хочется несколько раз подряд вводить длинную ключевую фразу.

Раздел Очистка файлов

Здесь можно настроить параметры уничтожения файлов (удаления без возможности восстановления).

- *Число подходов* – количество проходов очистки определяет, сколько раз сектора диска, содержавшие удаляемый файл, будут перезаписаны случайными данными. Обычно достаточно 3 (столько, например, предусматривает инструкция Минобороны США 5220.22). Для крайне ценных файлов увеличьте параметр до 9-12. Большее число проходов повышает надёжность уничтожения данных и снижает риск их намеренного восстановления, но и делает процесс стирания крайне долгим. Рекомендации таковы:
  - 1-3 прохода – для использования на домашнем компьютере;
  - 10-12 проходов – для использования в коммерческой и бизнес-сфере;
  - 16-18 проходов – для использования в военной сфере;
  - 26-28 проходов – для максимальной надёжности (может потребовать вплоть до нескольких часов работы для удаления достаточно крупного файла).

  Коммерческие фирмы, специализирующиеся на восстановлении информации, могут восстановить данные, которые были перезаписаны примерно до девяти раз. Но вы должны учесть, что если ваша информация представляет чрезвычайную ценность (вероятно, ценность государственного масштаба), даже максимальное число проходов не обеспечит должного уровня надёжности. Питер Гутман, разработавший методику стирания информации, реализованную в PGP, рекомендует один достаточно надёжный способ уничтожения столь ценных данных: сжечь носитель информации, пепел растереть в порошок и развеять по ветру.

- *Подтверждать очистку* – если включить, PGP будет выдавать предупреждение перед уничтожением файлов с просьбой подтвердить ваши намерения – последний шанс передумать. Рекомендую включить, поскольку специально или случайно уничтоженные данные будет исключительно трудно восстановить не только злоумышленнику, но и вам самим.

2.1.2.2 Файлы

Вкладка *Файлы* содержит местоположение связок ключей и пула случайных чисел (рисунок 2.6).

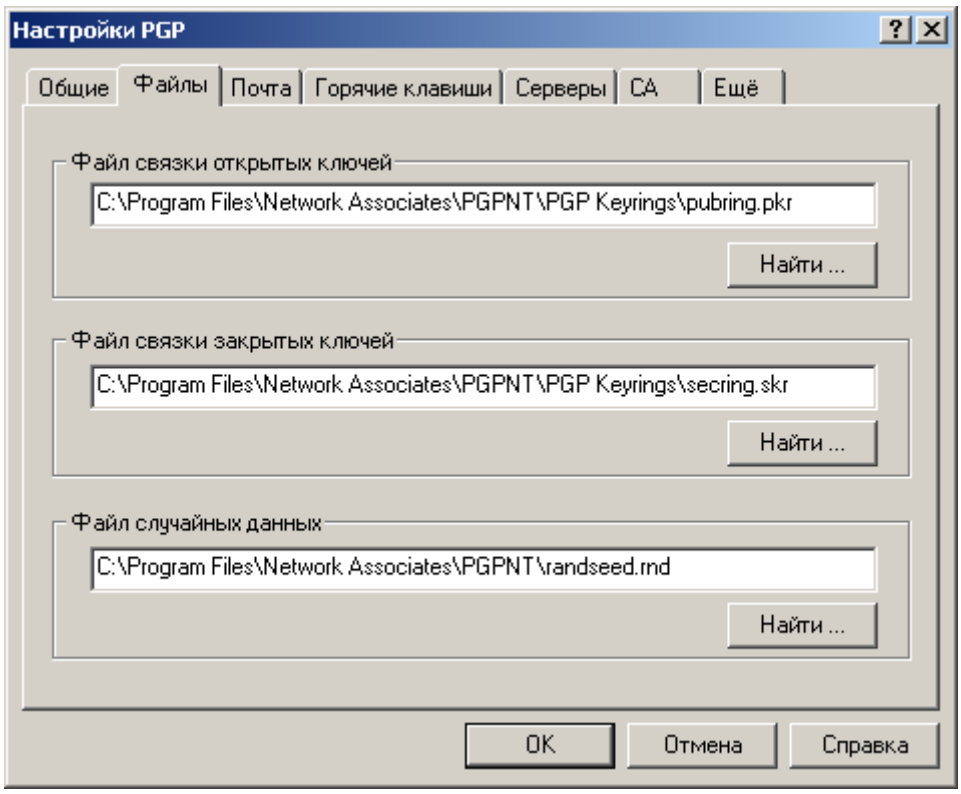

Рис. 2.6

Раздел “Файл связки открытых ключей” указывает директорию и файл, где находится ваша связка открытых ключей; именно на ней хранятся ваши открытые ключи и открытые ключи всех ваших корреспондентов. Если необходимо, переместите файл в каталог, где он не будет случайно удалён вами или кем-то посторонним. В то же время не стоит помещать файл на внешний носитель, тем более на CDR-диск, поскольку для редактирования, добавления новых и удаления ненужных ключей файл должен быть доступен для записи.

Раздел “Файл связки закрытых ключей” указывает директорию и файл, где находится связка ваших закрытых ключей. ВНИМАНИЕ: удаление или порча этого файла приведёт к фактической потере всей зашифрованной информации! Крайне желательно переместить закрытые ключи на аппаратное криптографическое устройство (смарт-карту или USB-токен) либо всю связку – на внешний носитель, скажем, дискету, ZIP или CD-RW диск: в этом случае, во-первых, будет снижен риск случайного или злонамеренного удаления файла и, во-вторых, все закрытые ключи всегда будут под вашим физическим контролем (при условии надёжного хранения носителя), и могут быть использованы как обыкновенный ключ от дверного замка: подключаете к компьютеру, расшифровываете / подписываете что-либо, отключаете от компьютера и прячете.

В разделе “Файл случайных данных” указан путь к файлу с пулом псевдослучайных чисел, используемых программой для генерации сеансовых ключей и другого криптографического материала. Этот файл не содержит сколь-нибудь ценных данных, он лишь накапливает показатели энтропии. Чтобы воспользоваться этими показателями для проведения атаки на шифртекст, взломщику по меньшей мере придётся взломать гамма-генератор, обновляющий содержимое этого файла. Всё же стоит разместить его на логическом диске в оперативной памяти компьютера, дабы он (файл, а не компьютер) уничтожался при каждой перезагрузке.

2.1.2.3 Электронная почта

Вкладка *Почта* содержит настройки интеграции с почтовым клиентом (рисунок 2.7).

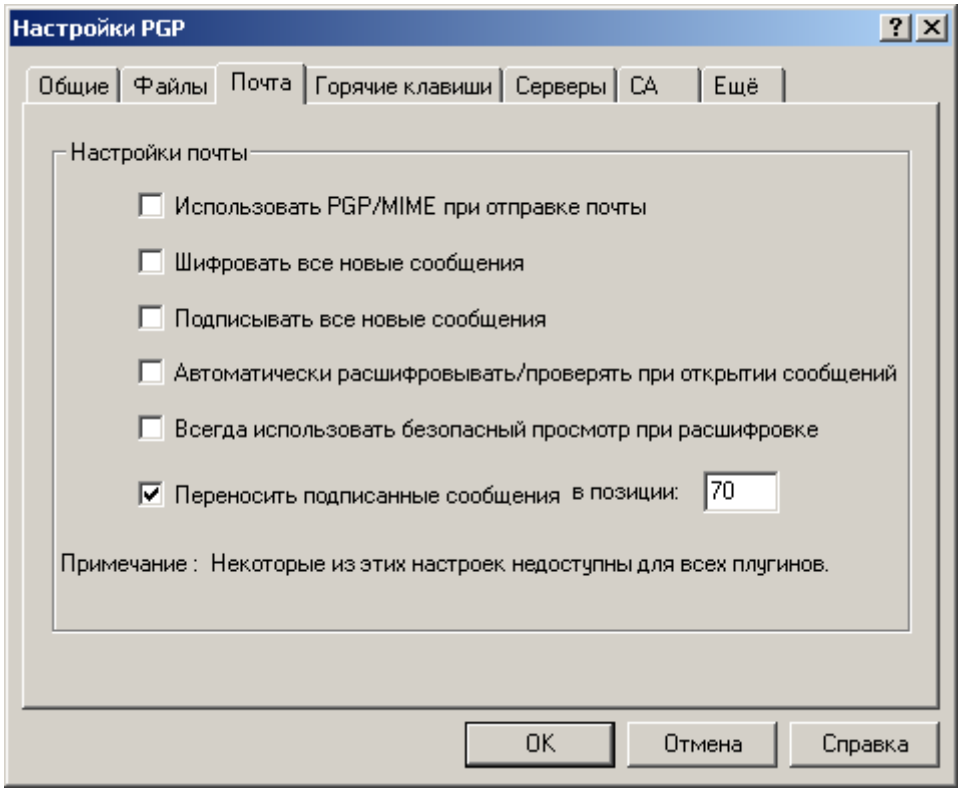

Рис. 2.7

Если наряду с PGP вы установили плагин для интеграции с почтовым клиентом, здесь можно настроить некоторые параметры обработки почты. Не все из этих опций поддерживаются каждой почтовой программой. Кроме того, перед включением той или иной опции убедитесь, что и почтовая программа получателя также её поддерживает.

- *Использовать PGP/MIME при отправке почты* – если вы и ваши корреспонденты используете email-клиент Qualcomm Eudora, включение этой опции позволит PGP автоматически зашифровывать всё содержимое письма (включая вложенные файлы и т.д.) и отправлять его в особом MIME-формате OpenPGP. Получателю нужно будет только нажать на ярлычок в пришедшем сообщении, и оно расшифруется с сохранением оригинального форматирования и всяческих украшательств в виде картинок и HTML-шаблонов. Данная опция (как для отправки, так и для получения) поддерживается только email-клиентом Qualcomm Eudora! Если вы не уверены в обратном, рекомендую отключить.
- *Шифровать все новые сообщения* – автоматически зашифровывать сообщения перед отправкой открытым ключом получателя. Поддерживается всеми email-клиентами. Если вам приходится часто пересылать зашифрованную корреспонденцию, лучше включить.
- *Подписывать все новые сообщения* – автоматически подписывать сообщения перед отправкой. Поддерживается всеми email-клиентами. Рекомендация аналогична предыдущей.
- *Автоматически расшифровывать / проверять при открытии сообщения* – автоматически расшифровывать / сверять подписи с открываемых сообщений. Поддерживается большинством email-клиентов.
- *Всегда использовать безопасный просмотр при расшифровке* – если включить, то любой расшифрованный текст (не только письма) будет выводиться в специальном окне *Secure Viewer*, используя шрифт, предотвращающий так называемую TEMPEST-атаку (удалённый съём информации по

электромагнитному излучению монитора); кроме того, в этом случае сообщение невозможно будет сохранить в виде открытого текста. Для большинства случаев эту опцию лучше отключить (ещё и потому, что этот поставляемый с PGP TEMPEST-защитный шрифт не имеет кириллических символов).

- *Переносить подписанные сообщения в позиции ...* – производить на указанном символе в строчке жёсткий перенос (возврат каретки). Не меняйте установленное по умолчанию 70, если твёрдо не уверены, что в вашей почтовой программе используется меньший показатель, в противном случае сделайте эту цифру ниже, иначе ваш email-клиент, отформатировав текст перед отправкой, повредит цифровую подпись и шифртекст.

2.1.2.4 Горячие клавиши

Вкладка *Горячие клавиши* содержит настройки клавиш быстрого доступа к функциям PGP (рисунок 2.8).

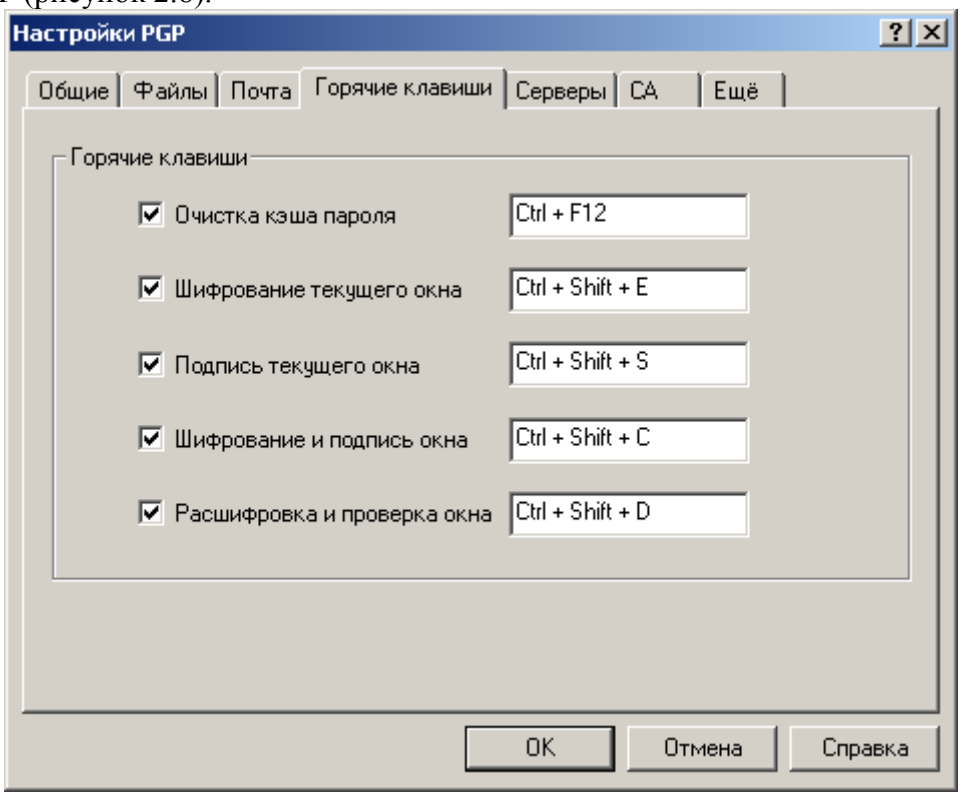

Рис. 2.8

Здесь можно указать комбинации клавиш для быстрого выполнения тех или иных основных операций: шифрования, подписания и пр.

- *Очистка кэша пароля* – быстрая очистка кэша от ключевых фраз. Если вы включили режим кэширования ключевых фраз, обязательно нажимайте эту комбинацию клавиш, когда отлучаетесь от компьютера.
- *Шифрование текущего окна* – зашифровать содержимое активного окна.
- *Подпись текущего окна* – подписать содержимое активного окна.
- *Шифрование и подпись окна* – зашифровать и подписать содержимое активного окна.
- *Расшифровка и проверка окна* – расшифровать / сверить подпись с содержимого активного окна.

2.1.2.5 Серверы

Вкладка *Серверы* содержит настройки списка серверов-депозитариев (рисунок 2.9).

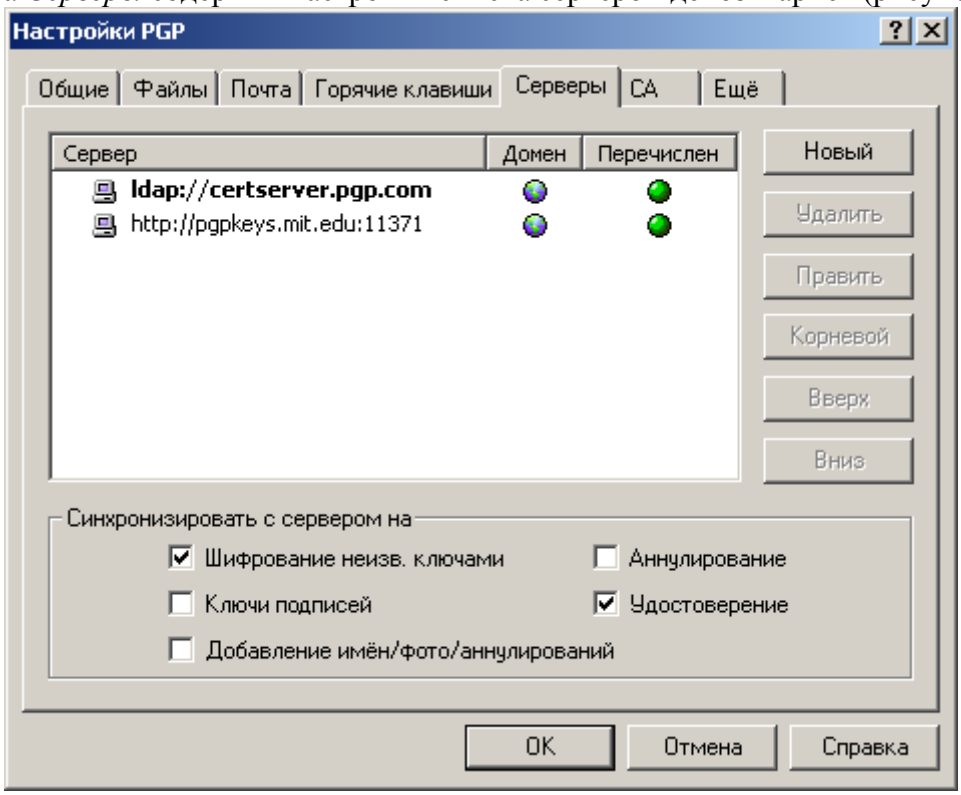

Рис. 2.9

Кнопки справа от списка серверов позволяют вносить в него следующие изменения:

- *Новый* – добавить в список новый сервер-депозитарий.
- *Удалить* – удалить из списка указанный сервер.
- *Править* – редактировать параметры выделенного сервера.
- *Корневой* – сделать выбранный сервер корневым (или доменным). В корпоративной среде таковой используется для специфических задач, в частности, для обновления списков рассылки, настроек программы, доверенных поручителей и т.д. Для частных пользователей эта опция не представляет ценности.
- *Вверх* и *Вниз* – сдвинуть сервер в списке вверх или вниз. Поиск ключей на серверах в ходе синхронизации происходит в приоритетном порядке: если ключ не найден на первом сервере, производится поиск на втором и т.д. Поэтому крупные общественные серверы-депозитарии (как ldap://certserver.pgp.com) лучше оставить на самом верху.

Настройки в разделе “Синхронизировать с сервером на” позволяют указать, в каких случаях будет производиться синхронизация ключей с серверами. Желательно включить их все.

- *Шифрование неизв. ключами* – если включить, при отправке электронного письма человеку, открытого ключа которого нет на вашей связке, PGP попытается подключиться к депозитарию и самостоятельно найти ключ по email-адресу получателя. (Только при использовании почтового плагина.)
- *Ключи подписей* – если включить, при подписании чужого открытого ключа PGP сначала обновит его с сервера, а затем отправит на сервер подписанную вами копию.
- *Добавление имен / фото / аннулирований* – аналогично предыдущей опции, если вы внесёте в сертификат своего ключа новую запись (имя или фото) либо

добавите т.н. "отменителя", PGP обновит ключ с сервера, а затем загрузит на сервер внесённые вами изменения.

- *Аннулирование* – после аннулирования открытого ключа PGP синхронизирует его с сервером, дабы в дальнейшем ваши корреспонденты не могли его применять.
- *Удостоверене* – если сверяете с сообщения или файла чужую ЭЦП, к которой на вашей связке не может быть найден подходящий открытый ключ, PGP попытается связаться с сервером и найти ключ по номеру ID.

2.1.2.6 Центр сертификации

Вкладка *CA* (*Certificate Authority*) содержит настройки установки соединения с Центром сертификации (ЦС) и объединения с инфраструктурой PKI. В основном эта функция применяется в корпоративной среде с развёрнутой PKI, основанной на стандарте X.509. Для частных пользователей она может не представлять интереса.

2.1.2.7 Дополнительные

Вкладка *Еще* содержит расширенные настройки PGP (рисунок 2.10).

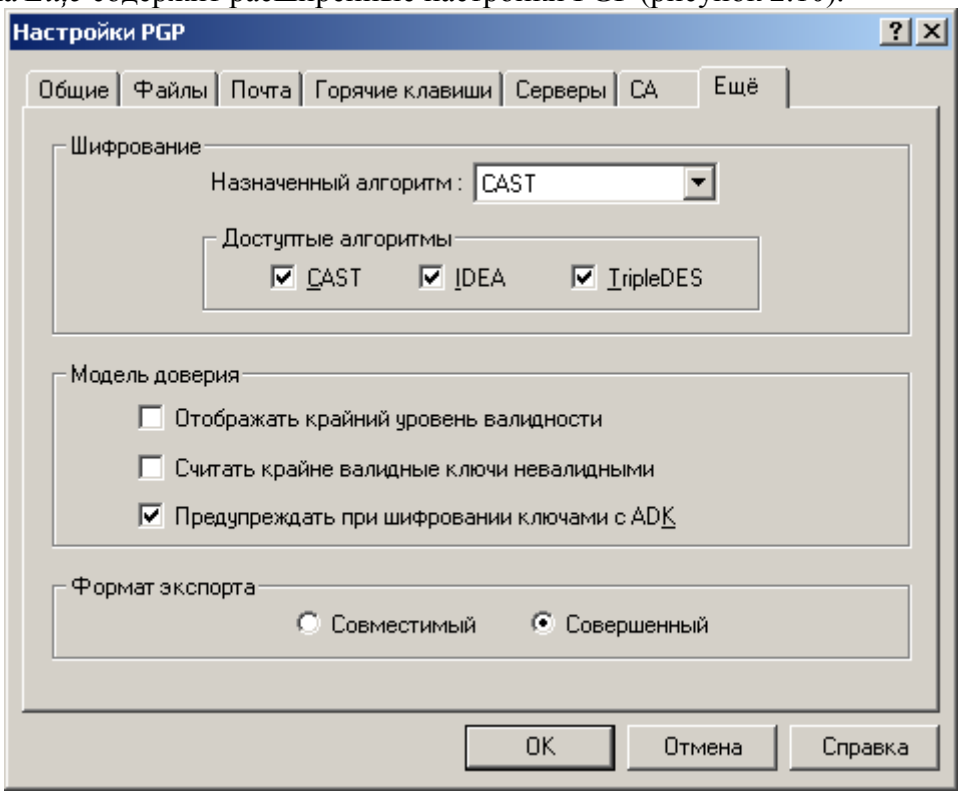

Рис. 2.10

Раздел Шифрование

Настройки используемых шифровальных алгоритмов. Учтите, выбранные здесь настройки ложатся в материал генерируемых вами ключей, поэтому для уже существующих ключевых пар вы не обнаружите никаких изменений.

- *Назначенный алгоритм* – предпочтительный алгоритм симметричного шифрования. Следующая сгенерированная вами ключевая пара будет предпочтительно использовать указанный здесь блочный шифр. Иными словами, программа PGP отправителя зашифрует сообщение, предназначенное вам, именно этим алгоритмом, если и сама его поддерживает. Кроме того, этот

же шифр будет применятся в дальнейшем и для симметричного шифрования с помощью обычного пароля.

По умолчанию выставлен CAST, в самых ранних был IDEA. С точки зрения обычного пользователя практических различий между ними нет – все чрезвычайно стойки. Некоторые были изобретены раньше, другие несколько новее:

- *CAST* – разработанный в 1993 году шифр со 128-битовым ключом и 64-битовым блоком. Дизайн основан на формальной архитектуре DES. Совершенно устойчив к линейному и диффиренциальному криптоанализу, может быть взломан только "в лоб". Имеет множество модификаций, часть которых была признана ненадёжными. В PGP реализован стойкий вариант CAST5.
- *Triple-DES* – он же 3DES или тройной DES. Базовый алгоритм DES был разработан IBM в середине 1970-х и принят в качестве государственного стандарта шифрования США (и весьма распространился по миру). 3DES – это его вариация, в которой базовый DES выполняется трижды на одном блоке данных. В PGP он реализован в режиме EDE (зашифрование-расшифрование-зашифрование) с тремя независимыми подключами. Длина общего ключа – 168 бит, оперирует на 64-битовых блоках. Теоретическая расчётная стойкость такого алгоритма к лобовой атаке составляет 112 бит, практическая – по меньшей мере 129 бит, что, вкупе с его проверенной годами надёжностью, крайне хороший показатель.
- *IDEA* – опубликованный в 1990, именно он лёг в основу первых версий PGP. Имеет ключи длиной 128 бит и оперирует на 64-битовых блоках открытого и шифртекста. Построен на концепции смешения операций различных алгебраических групп, а именно: XOR, сложение по модулю 2^{16} и умножение по модулю $2^{16}+1$. В ослабленных вариантах может быть подвержен криптоаналитическим атакам, но в базовом, который реализован в PGP, – нет.

- *Доступные алгоритмы* – допустимые симметричные алгоритмы. Как и предыдущая опция, данные установки ложатся в материал следующих генерируемых ключевых пар, а также используются вашей программой для шифрования отправляемых сообщений. Назначение этих опций в следующем: если программа PGP отправителя не поддерживает алгоритм, указанный у вас в качестве предпочтительно, она воспользуется одним из отмеченных здесь алгоритмов в качестве альтернативы. Выбор осуществляет в приоритетном порядке слева направо: скажем, если отправитель не поддерживает CAST, он зашифрует сообщение с помощью IDEA; если он не поддерживает CAST, а IDEA выключил, считая недостаточно надёжным, программа воспользуется 3DES, и т.д.

Снимайте галочки с перечисленных алгоритмов только в том случае, если у вас возникнут серьёзные и обоснованные (!) опасения в их стойкости, например, если станет доподлинно известно, что один из них был взломан! Если снять галочку с того или иного алгоритма, вы запретите вашей программе шифровать с его помощью сообщения для корреспондентов, а корреспонденты не смогут с его помощью шифровать сообщения для вас, если те же настройки легли в материал вашего открытого ключа.

Раздел Модель доверия

Ряд расширенных настроек отношений доверия PGP.

- *Отображать крайний уровень валидности* – показывать или нет частичный уровень достоверности ключей. Если включить, уровень достоверности

(подлинности) ключей в окне PGPkeys будет показан в виде шкалы с тремя состояниями: недостоверен (пустая шкала), частично достоверен (наполовину заполненная шкала), достоверен (целиком заполненная шкала). Если опция выключена, уровень достоверности будет показан как зелёный (достоверный ключ) или серый (недостоверный ключ) кружок. Если вам необходимо иметь полное представление о состоянии ключей на вашей связке – включите.

- *Считать крайне валидные ключи невалидными* – расценивать частично достоверные ключи как недостоверные. Если включено, при попытке зашифровать сообщение частично достоверным ключом, будет показано окно выбора ключей *Key Selection Dialog*, дабы предупредить о состоянии достоверности открытого ключа получателя.
- *Предупреждать при шифровании ключами с ADK* – выдавать ли предупреждение при зашифровании, если ключ получателя содержит дополнительный ключ расшифрования (ADK). ADK используются в корпоративной среде, чтобы в определённых случаях иметь возможность расшифровать информацию своих служащих. Таким образом, наличие ADK говорит о том, что в этих определённых чрезвычайных случаях доступ к отправляемой информации могут иметь третьи лица, а не только фактический получатель.

Раздел Фомат экспорта

Выбор формата экспортируемых со связки ключей:

- *Совместимый* – совместимый с версиями PGP до 6.x. Будет экспортирован только сам ключ и связанные с ним текстовые поля сертификата.
- *Совершенный* – новый формат, совместимый с PGP 6.x и выше. Кроме ключа будут экспортированы фотографии и прочее.

2.2 Управление ключами

Первая задача, возникающая после инсталляции и настройки программы – это генерация пары "открытый ключ / закрытый ключ". Именно асимметричные ключи позволят вам беспрепятственно обмениваться зашифрованными и подписанными сообщениями с людьми, живущими в любом конце света.

В рамках дельнейшего описания будут использованы следующие термины:

- *Ключевая пара* – асимметричная пара "открытый ключ / закрытый ключ".
- *Ключ* – в зависимости от контекста может подразумевать открытый ключ или ключевую пару.
- *Ключевая фраза, парольная фраза, пароль* – уникальная последовательность символов и/или слов, позволяющая использовать закрытый ключ асимметричной ключевой пары.
- *Связка* – связки открытых и закрытых ключей; pkr-, skr-файлы, указанные в настройках программы.
- *Основной ключ* – ключ, указанный как "ключ по умолчанию".
- *"Отменитель"* – designated revoker, человек, уполномоченный вами при необходимости аннулировать ваш ключ.

PGP предоставляет на выбор следующие типы асимметричных ключей: *Diffie-Hellman / DSS* (или просто *DH/DSS*) и *RSA*. В старых версиях PGP (до 5.0) применялись только ключи RSA, использующие для шифрования и цифровой подписи асимметричный алгоритм RSA. В PGP 5.0 были добавлены ключи Diffie-Hellman, использующие шифрование по схеме Эльгамаля и подписание по стандарту DSS.

При генерации нового ключа вам придётся сделать выбор его типа:

- Если вам нужна полная функциональность последних версий PGP и широкая совместимость вплоть до PGP 5.0, выбирайте *DH/DSS*. В большинстве случаев это предпочтительно. Однако следует помнить, что размер ключа подписания DSS всегда равен 1024 битам, независимо от размера ключа шифрования DH.
- Если вы не хотите быть скованными ограничением на 1024-битовый ключ подписания, выбирайте тип *RSA*.
- Если вы планируете общаться с людьми, использующими исключительно старые версии PGP (до 5.0), выбирайте *RSA*. Для целей совместимости эти ключи имеют ограничение длины до 2048 бит и не поддерживают множества новых функций (фотографические удостоверения, "отменителей" и пр.).

Также не забывайте, что вы можете сгенерировать столько ключей различных типов, сколько пожелаете.

Если вы прежде не использовали PGP и не имеете готовых связок ключей, которые указали в ходе инсталляции, то первое, что нужно сделать после установки и настройки программы – это создать свой первый ключ.

Хотя это может показаться увлекательным занятием, не создавайте больше одной ключевой пары, если в ином нет явной необходимости! Тому есть ряд причин. Во-первых, не пройдёт много времени, как вы окончательно в них запутаетесь. Во-вторых, что более важно, ни один ключ не может быть надёжнее защищающей его ключевой фразы. Нет смысла создавать множество ключей с идентичными ключевыми фразами (а много разных и *хороших* вы вряд ли запомните), поскольку взлом любой из них будет равносилен взлому всех. Наконец, в-третьих, при необходимости отправить вам сообщение, незнакомый корреспондент может столкнуться с проблемой выбора ключа для зашифрования.

Чтобы сгенерировать новую ключевую пару сделайте следующее:

1. Откройте менеджер PGPkeys.
2. Нажмите иконку *Создать новую пару ключей* () в панели инструментов менеджера. Появится окно генерации ключа с описанием того, что такое открытые и закрытые ключи.
3. Нажмите кнопку *Далее* для продолжения.
4. В поле *Полное имя* введите своё имя, а в поле *Адрес Email* – адрес электронной почты. Несмотря на то, что указывать своё настоящее имя не обязательно, это может помочь корреспондентам идентифицировать данный открытый ключ как принадлежащий вам. То же касается и email-адреса, по которому ваш ключ будет проще отыскать на сервере и упростит корреспондентам отправку вам сообщений.
5. В меню *Тип пары ключей* выберите тип создаваемого ключа.
6. В поле *Размер пары ключей* укажите размер создаваемого ключа в битах. Более крупный ключ потребует больше времени на генерацию и на дальнейшие операции зашифрования / расшифрования, в то же время предоставляя бо̲льшую степень надёжности. Если передаваемая вами информация не представляет ценность, сопоставимую с ценой проведения чрезвычайно дорогостоящей криптоаналитической атаки, будет более чем достаточно выставленных по умолчанию 2048 бит.
7. В разделе *Срок годности ключа* укажите дату истечения срока действия создаваемого ключа. Выберите либо установленное по умолчанию *“Вечный” ключ* (бессрочный), либо укажите определённую дату, с которой ключавая пара не сможет применяться для задач зашифрования и подписания (тем не менее, ею можно будет продолжать пользоваться для расшифрования и сверки ЭЦП). *“Вечный” ключ* является предпочтительным. Если, однако, вы планируете использовать данный ключ только определённый период (например, в течение

срока действия контракта с работодателем), укажите здесь дальнюю границу этого периода.

8. Нажмите *Далее*.
9. В окне выбора ключевой фразы введите в оба представленных поля пароль, которым хотите защитить свой новый закрытый ключ.
   Парольная фраза – это единственный и по этой причине самый главный механизм защиты закрытого ключа от несанкционированного использования. Вся надёжность PGP упирается в качество выбранной вами на этом этапе ключевой фразы. В порядке меры предосторожности программа скрывает вводимые символы. Если вам от этого неудобно и вы уверены, что в помещении нет посторонних глаз, снимите галочку со *Скрыть*.
   ВНИМАНИЕ: Если вы позднее забудете введённую на этом этапе парольную фразу, никто не сможет помочь вам воспользоваться закрытым ключом данной ключевой пары, и вся зашифрованная с её помощью информация фактически будет утеряна!

В целях совместимости крайне не рекомендуется использовать для ключевой фразы кириллицу и другие нелатинские национальные буквенные символы. Если же вы считаете, что их использование необходимо, протестируйте созданный ключ на не представляющей ценности информации и убедитесь, что можете свободно её расшифровать, прежде чем применять ключ по назначению.

10. Нажмите *Далее*.
11. Если введённая на предыдущем этапе ключевая фраза не соответствует нормам безопасности, PGP выдаст предупреждение. Вернитесь назад и устраните проблему, ибо её игнорирование повлечёт серьёзные проблемы с защищённостью ключа.
12. Движения вашей мышки и нажатия на клавиши создают множество случайной информации (энтропии), обязательной для генерации ключей. Однако бывает так, что PGP не успевает накопить достаточно энтропии до начала генерации ключа. В таком случае появится окно сбора случайных данных *PGP Random Data*: просто подвигайте мышкой и понажимайте на произвольные клавиши, пока шкала не заполнится целиком. Если же всё нормально, PGP приступит к формированию ключа.
13. В зависимости от мощности компьютера и от длины создаваемого ключа на этот этап может потребоваться разное количество времени: от нескольких секунд до десятков минут. Дождитесь, пока не появится сообщение *Завершено*. После этого можете нажать кнопку *Далее* и затем *Готово*.

PGP самостоятельно разместит открытый и закрытый ключи в соответствующих файлах связки, а имя ключа появится в окне менеджера PGPkeys.

Зашифровать файл, а после обнаружить, что не можешь его расшифровать – это болезненный опыт, тем не менее, помогающий понять, как правильно выбирать ключевую фразу, которую удастся запомнить.

Большинство приложений с ограничением доступа предлагают использовать в качестве пароля слово из трёх-восьми букв. Очень нежелательно использовать подобные пароли по ряду причин. Во-первых, они сильно уязвимы к атакам "по словарю", когда взломщик заставляет компьютер перебирать все слова из словаря, пока не угадает пароль. Во-вторых, они могут взломаны полным перебором всех возможных комбинаций букв, печатных символов и цифр.

Чтобы защититься от подобного рода атак рекомендуется создавать парольное слово, состоящее из заглавных и строчных букв, цифр, знаков препинания и пробелов. В результате получается пароль, который довольно сложно подобрать, но ещё труднее запомнить. Использование в составе пароля множества произвольных небуквенных символов повышает его стойкость к атакам "по словарю", но и затрудняет его

запоминание, что, рано или поздно, может привести к катастрофической потере информации по той лишь причине, что вы не сможете расшифровать собственные файлы.

С другой стороны, ключевая фраза, или *осмысленный пароль*, – это последовательность логически связанных слов, обычно, длинное предложение, которое гораздо менее уязвимо к "словарным" атакам. Однако, если вы не выберите в качестве ключевой фразы нечто, давно хранящееся в долгосрочной памяти мозга, то едва ли сможете запомнить её буквально.

Выбор ключевой фразы под влиянием обстоятельств скорее всего приведёт к тому, что вы начисто её забудете; не поможет и попытка "зазубрить" – так устроена память. Выберите что-то, уже находящееся в вашей долгосрочной памяти. *Это не должна быть* фраза, которой вы с кем-то недавно делились или которую часто любите повторять, и не должен быть известный афоризм или цитата, поскольку всё это будет со временем подобрано опытным взломщиком. Можете построить ключевую фразу на ассоциации или ассоциативном ряде, задав себе вопрос, ответ на который знаете только вы. Но это должно быть нечто, давно и глубоко хранящееся в вашем мозге, однако и не что-то очевидное и легко предсказуемое. Альтернативный вариант – это мнемотехнические методики, но они требуют определённой практики и опыта. Постарайтесь несколько "усилить" результат заглавными буквами в произвольных местах и небуквенными символами, только не переусердствуйте.

Разумеется, если вы будете столь недальновидны, что запишите результат на листке бумаги и положите его в ящик письменного стола, не имеет большого значение, сколь хорошую ключевую фразу вы придумаете.

> Сгенерировав новую ключевую пару немедленно сделайте несколько её резервных копий на разных внешних носителях! (В действительности, PGP сам предложит вам это сделать, когда вы закроете окно PGPkeys. Ни в коем случае не пренебрегайте этой рекомендацией!) Игнорирование этого требования приводит к неоправданному риску потери всех ценных данных. Если что-то случится с единственным файлом связки закрытых ключей, никто во всём мире не поможет вам расшифровать ваши файлы.

Кроме резервного копирования pkr- и skr-файлов связки ключей, обратите особое внимание на то, где хранится ваш закрытый ключ. Хотя закрытый ключ защищён ключевой фразой, известной только вам, посторонний может узнать её, например, просто подсмотрев из-за спины, какие клавиши вы нажимаете, или перехватив нажатия клавиш через локальную сеть или даже через Интернет, а затем воспользоваться закрытым ключом, чтобы расшифровывать вашу информацию и подделывать подпись.

Чтобы избежать подобных сценариев, храните закрытый ключ только на своём компьютере. Если ваш компьютер подключён к локальной сети, убедитесь, что файлы связок не подлежат автономному резервному копированию на носители, к которым могут получить доступ посторонние лица. Учитывая лёгкость, с которой злоумышленник может проникнуть в компьютер через сеть, установите дополнительные защитные барьеры в виде межсетевых экранов и антивирусных программ. Работая со сверхценной информацией, разместите свой закрытый ключ на дискете или, что предпочтительнее, на смарт-карте, которую можно использовать аналогично ключу от дверного замка, подключая к компьютеру, только когда нужно подписать или расшифровать информацию.

Ещё одна мера предосторожности заключается в переименовании связки закрытых ключей (skr-файла) и перемещении её в отдельный от открытых ключей каталог. Для этого воспользуйтесь вкладкой *Файлы* меню настроек программы.

2.3 Управление связкой ключей

Ключи, созданные вами или полученные от корреспондентов, хранятся на связках, по сути представляющих собой два файла (базы данных): один содержит открытые ключи и по умолчанию назван *pubring.pkr*, другой предназначен для закрытых и называется

secring.skr. Изначально эти файлы хранятся в каталоге с программой PGP или в папке “Мои документы\PGP”.

В некоторых случаях вам может потребоваться изучить атрибуты ключей и их сертификатов или изменить их параметры. Скажем, получив от корреспондента открытый ключ, вы захотите установить его тип, проверить отпечаток и по содержащимся на сертификате подписям определить достоверность. Затем вы решите сами подписать этот ключ, чтобы указать на его подлинность, и настроить уровень доверия владельцу в заверении других ключей.

Порой может возникнуть необходимость изменить ключевую фразу вашего собственного закрытого ключа или найти чей-то открытый ключ на общественном сервере.

Для выполнения всех перечисленных и некоторых других мероприятий служит менеджер PGPkeys.

2.3.1 Основы PGPkeys

Окно менеджера PGPkeys содержит список всех ваших ключевых пар и чужих открытых ключей, добавленных вами на связку. В верхней части окна расположена панель инструментов, предназначенная для выполнения наиболее обыденных задач, и строка меню, предоставляющая доступ к дополнительным функциям.

Большинство операций с ключами может быть выполнено четырьмя разными способами:

- Через иконки в панели инструментов.
- Через строку меню в верхней части окна.
- Через контекстное меню по нажатии правой кнопкой на имя ключа или составляющих его элементов.
- С помощью горячих клавиш PGPkeys (они отображены напротив соответствующих функций в меню в верхней части окна).

Все эти способы совершенно равноправны.

2.3.1.1 Атрибуты ключей

Наряду с именами ключей окно PGPkeys отображает некоторые из их параметров и атрибутов. В меню *Вид* вы можете указать, какие атрибуты будут отображаться в окне менеджера, а в самом окне при желании можете изменить порядок расположения столбцов атрибутов (перетащив столбец за шапку) и сортировку списка ключей по любому из атрибутов (нажав левой кнопкой на шапку нужного столбца).

Окно PGPkeys может показывать следующие параметры ключей:

- ***Ключи* (*Keys*)** – этот атрибут представлен набором пиктографических изображений, обозначающих различные параметры ключа. Также он содержит имя владельца, сведения сертификата ключа и имена его поручителей. В таблице 2.1 приведено описание пиктограмм, соответствующих атрибуту “Ключи”.

Таблица 2.1

	Золотой ключ и человечек обозначают принадлежащую пользователю пару "открытый ключ / закрытый ключ" типа Diffie-Hellman / DSS.
	Серый ключ и человечек обозначают принадлежащую пользователю пару "открытый ключ / закрытый ключ" типа RSA.
	Золотой ключ обозначает открытый ключ типа Diffie-Hellman / DSS.
	Серый ключ обозначает открытый ключ типа RSA.

	Пара ключей обозначает разделённый ключ. Такой может использоваться для расшифрования / подписания только после объединения.
	Тусклый ключ обозначает временно дезактивированный открытый ключ. Такой не может использоваться для зашифрования. Это удобно при большом количистве открытых ключей на связке, сильно захламляющих окно *Key Selection Dialog*.
	Серый ключ на золотой карте обозначает сохранённый на смарт-карте ключ типа RSA.
	Ключ с красным запрещающим знаком обозначает аннулированый открытый ключ. Это значит, что он либо был скомпрометирован, либо по иным причинам более не используется владельцем.
	Ключ с часиками обозначает просроченный открытый ключ, чей период действия уже истёк.
	Два человечка обозначают группу открытых ключей списка рассылки.

В таблице 2.2 приведены пиктограммы, обозначающие содержимое сертификата:

Таблица 2.2

	Конверт обозначает обычное имя в сертификате ключа; как правило, это просто имя и email-адрес владельца ключа. Конверт может быть жёлтым или серым в зависимости от типа ключа (DH/DSS или RSA).
	Конверт с красным запрещающим знаком обозначает аннулированную запись сертификата.
	Картинка обозначает фотографическое удостоверение в сертификате.
	Карандаш (или шариковая ручка) обозначает подпись, подтверждающую ту или иную запись сертификата ключа. Иконка карандаша без дополнилнительных символов – это неэкспортируемая подпись, заверяющая ключ только на связке пользователя.
	Карандаш с синей стрелкой обозначает экспортируемую со связки подпись. Такая используется как поручительство пользователя в подлинности ключа и данной записи сертификата
	Карандаш с красным запрещающим знаком обозначает отозванную подпись.
	Тусклый карандаш обозначает неверную или повреждённую подпись.

- ***Достоверность* (*Validity*)** – jбозначает степень убеждённости в том, что открытый ключ действительно принадлежит предполагаемому владельцу. Зависит от состава подписей, заверяющих данный ключ, и уровней доверия пользователя поручителям (людям, подписавшим ключ). Ключ, подписанный непосредственно пользователем, становится полностью достоверным, исходя из логики программы, что пользователь не станет подписывать поддельный открытый ключ. Ключ, не имеющий подписей, считается недостоверным, о чём программа будет напоминать всякий раз при попытке зашифровать информацию данным ключом. Атрибут достоверности может быть показан либо в виде цветного кружка, либо в виде шкалы, в зависимости от установок параметра

Display marginal validity level в настройках программы. Если опция выключена, то атрибут отображается следующим образом (таблица 2.3):

Таблица 2.3

	Серый кружок обозначает недостоверные ключи (и частично достоверные ключи, если опция *Treat marginally valid keys as invalid* в настройках программы включена).
	Зелёный кружок обозначает достоверные открытые ключи.
	Зелёный кружок и человечек обозначают безусловно достоверную ключевую пару пользователя.

- ***Размер* (*Size*)** – длина асимметричного ключа в битах. Для ключей типа DH/DSS и RSA отображается два числа: первое – длина подключа шифрования, второе – длина ключа подписания. Ключ подписания DSS всегда равен 1024 битам.
- ***Доверие* (*Trust*)** – обозначает указанный пользователем уровень доверия владельцу данного ключа в заверении чужих открытых ключей (таблица 2.4). Это влияет на степень достоверности чужих ключей, поручителем которых выступает владелец данного.

Таблица 2.4

	Пустая шкала говорит о том, что владелец данного ключа не имеет доверия и не может выступать поручителем (его подпись не учитывается при расчёте достоверности ключей).
	Частично заполненная шкала говорит о том, что подписанный владельцем данного ключа открытый ключ будет иметь частичную достоверность.
	Полностью заполненная шкала обозначает, что владелец данного ключа имеет полное доверие в заверении других открытых ключей, и любой ключ, подписанный им, считается программой достоверным.
	Заштрихованная шкала указывает на безусловно доверенный ключ пользователя.

- ***Описание* (*Description*)** – краткое описание объекта в колонке ***Ключи***: тип и состояние ключа, тип удостоверения, вид подписи и т.п.
- ***ID ключа* (*Key ID*)** – уникальный идентификационный номер, помогающий отличить несколько открытых ключей с одинаковыми именами владельца (в очень редких случаях сами номера ID у разных ключей совпадают).
- ***Создание* (*Creation Date*)** – указывает дату, когда ключ был сгенерирован. Иногда можно исходить из этой информации при анализе подлинности ключа. Если он был создан довольно давно, маловероятно, что его станут подменять, поскольку за прошедшее время оригинальные копии должны были получить широкое распространение. Но никогда не полагайтесь на этот показатель как на единственный параметр анализа (его крайне легко сфальсифицировать)!
- ***Срок годности* (*Expiration Date*)** – указывает дату, когда ключ станет неприменим для новых криптографических задач, либо “Вечный” (*Never*), т.е. неограниченный срок действия.
- ***ADK*** – наличие дополнительных ключей расшифрования. Серым или зелёным кружком показывает, содержит ли конкретный ключ ADK.

Также в меню *Вид* можно включить или выключить показ панели инструментов (*Панель инструментов*).

2.3.1.2 Выбор основного ключа

Основной ключ пользователя, или ключ по умолчанию, используется программой, чтобы автоматически зашифровывать информацию не только для получателя, но и для вас самих, дабы в дальнейшем вы имели возможность, например, расшифровать и прочитать отправленное письмо. Подписывая сообщение или чей-то открытый ключ, PGP будет также предлагать использовать ваш ключ по умолчанию (разумеется, если вы пожелаете воспользоваться другим своим закрытым ключом, то сможете это сделать). В окне PGPkeys основной ключ выделен **жирным шрифтом**, дабы отличить его от остальных. Если вы используете несколько ключевых пар, выбор одной как основной сделает работу с PGP более удобной.

Чтобы выбрать основной ключ:

1. В окне PGPkeys выделите тот свой ключ, который хотите сделать основным.
2. В строке меню нажмите *Ключи* > *Назначить ключом по умолчанию*.

Имя ключа станет жирным, обозначая, что теперь он используется по умолчанию.

2.3.1.3 Импортирование и экспортирование ключей

Наиболее удобным способом обмена ключами является их пересылка через сервер-депозитарий, но иногда может потребоваться отправить открытый ключ в виде отдельного файла (например, через FTP-сервер). Или вы можете захотеть сохранить резервную копию отдельных ключей, а не связок целиком (чтобы зарезервировать связку, достаточно скопировать файлы pubring.pkr и secring.skr, расположение которых можно узнать во вкладке *Файлы* меню настроек программы). В этом случае можно экспортировать или копировать ключи в файл.

Если же ваш корреспондент изберёт в качестве способа передачи отправку открытого ключа по электронной почте, воспользуйтесь возможностью импортирования, чтобы добавить полученный ключ на свою связку. То же касается и восстановления резервных копий, и иных схожих задач.

Ниже приведены способы импортирования / экспортирования ключей.

Экспортирование ключа со связки в файл:

1. В окне PGPkeys выделите ключ, который хотите экспортировать. Можете экспортировать сразу группу ключей, выделив несколько нужных.
2. В строке меню нажмите *Ключи* > *Экспорт*.
3. Чтобы вместе с ключами экспортировать фото-удостоверения, отметьте опцию *Включить расширения 6.0*. Однако учтите, что в этом случае экспортированные ключи будут несовместимы с версиями PGP до 6.0.
4. Если в числе экспортируемых ключей присутствуют ваши ключевые пары, и кроме открытых вы хотите сохранить и закрытые ключи, отметьте галочкой опцию *Включить закрытые ключи*. В этом случае будьте внимательны, чтобы экспортированный файл не попал в руки к посторонним.
5. Укажите имя файла и каталог, где хотите его сохранить.

Копирование материала ключа со связки позволяет позднее вставить его в любой текстовый файл или в тело письма. Весьма удобный способ для некоторых мероприятий. Но копировать таким образом материал закрытых ключей невозможно.

Копирование материал ключа со связки в документ:

1. В окне PGPkeys выделите ключ, который хотите копировать. Можете копировать сразу группу ключей, выделив несколько нужных.
2. В строке меню нажмите *Правка* > *Копировать*.

Материал ключа (или ключей) помещён в буфер обмена (рисунок 2.11). Теперь можете вставить его в любой текстовый документ простой функцией *Вставить* или комбинацией клавиш *Ctrl+V*.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 6.5.8 for non-commercial use <http://www.pgp.com>
Comment: Копированный блок открытого ключа

mQCNBEFiQG8BBACyXzMkqNm0gEB6CejyiftiHtAbahwF79++mwGnA2nEWW+g7iUt
Y9/ZXjpKEEM6Y3ZeOCiCtlSyOq4aqpiM+74BoBgoqCPkcQ7eFAOq3Ihkoiz3CmjR
LLNo1yz5N12/Q6fU+U4LTAC3u4en+m+MavdLp85EhOEiEmPxiUcbgVE4BwARAQAB
tAMxMjOJAK4EEAECABgFAkFiQG8ICwIDCQgHAQoCGQEFGwMAAAACgkQ4+j9xbFm
GcOKBQP+Nr17DYyzatk7gtgXLJvjYbfNIEgTDww97kocBYOAfq1ETDD3ObVkWP0F
y8hOUpkpxBE4+C7F1CCv6CWpk96dN/F3w0v6XkHMeP170WOGhk7dJKaH70y0aWK0
/mMNpnz5ZtzLvodANG6Q0ddHBvXuJW8KBl3yOxVm0nT7AjbBmZi5AI0EQWJAcAEE
AJ+kaOL9lYIbOMd/mfRw5yiAMrU/QdSLKhyzYf98OVuSTqDH1BLwXbAOvEN5U/al
eKNWegfmFdXqRct9PXv8ECtZCVVxobo5IhXAOkL3nCyxAdadBgMV1BASdKZtd8QZ
BcFeUEdSqcAVe992jXWs4xec0aIwlk2gRk3J3kFlgjGjABEBAAGJAKIEGAECAAwF
AkFiQHAFGwwAAAACgkQ4+j9xbFmGcOBagQAqF/ODSYBha5+dC/95PkTtPGulF7M
BqWwrPv3luIPOSCmNCobHVZCRYsl5O7WLoirMwi7sSA8K0OeWASbXJMtgKSXHxnq
M5A3TD9rkPlCOvB8iS1jM6qPlguD9CTuIU6hSQGtGtSnZBQ51wgcTyg42aR/D5YZ
KCmMi1mVpwrKZqI=
=lZr7
-----END PGP PUBLIC KEY BLOCK-----
```

Рис. 2.11

Импортирование ключа из файла на связку:

1. В строке меню PGPkeys нажмите *Ключи* > *Импорт*.
2. В меню *Тип файла* (*File Types*) выберите тип импортируемого файла. Это может быть *txt* или *asc* для текстового материала ключа PGP, файлы связок PGP с расширениями *pkr*, *skr*, *pubkr*, *seckr* и *pgp*.
3. Укажите импортируемый файл и нажмите кнопку *Открыть* (*Open*).
4. В появившемся окошке *Укажите ключ*(*и*) отметьте те ключи из выбранного файла, которые хотите импортировать, и жмите *Импорт*.

Ключи будут присоединены к вашим связкам. Если среди импортированных были и закрытые ключи, программа предупредит, что им необходимо указать соответствующий уровень доверия. Для этого откройте свойства этих ключей (*Ключи* > *Свойства* в строке меню) и установите флажок на опцию *Имплицитное доверие*, наделяющую ключ безусловным уровнем доверия.

Если полученное вами письмо или текстовый файл содержат материал ключа, можете добавить его на связку следующим образом:

1. В полученном тексте выделите блок, начиная с заголовка “-----BEGIN PGP PUBLIC KEY BLOCK-----” (или “PRIVATE KEY BLOCK” для закрытого ключа) и заканчивая строкой “-----END PGP PUBLIC KEY BLOCK-----” и копируйте выделенный материал в буфер обмена (обычно можно просто нажать *Ctrl+C*).
2. В строке меню PGPkeys нажмите *Правка* > *Вставить*.
3. В появившемся окошке *Укажите ключ(и)* отметьте те ключи из полученного материала, которые хотите импортировать, и жмите *Импорт*.

2.3.1.4 Удаление ключей, подписей и сертификатов

Иногда может потребоваться удалить со связки ненужный ключ, заверяющую его подпись или запись из сертификата.

Удаление ключа со связки необратимо. Хотя вы можете повторно импортировать открытый ключ, добавить запись в сертификат или снова заверить ключ прежде удалённой подписью, удаление закрытого ключа, не имеющего резервных копий,

приведёт к фактической потере всей информации, зашифрованной соответствующим открытым ключом, поскольку эта информация более не сможет быть расшифрована!

Не забывайте, что удаление своего ключа со связки не аналогично его аннулированию. Если вы больше не собираетесь использовать ключевую пару, аннулируйте её и обновите на сервере, чтобы корреспонденты не использовали данный открытый ключ для отправки вам сообщений.

Чтобы удалить ключ, сертификат или подпись со связки:

1. В окне PGPkeys выделите объект, который хотите удалить.
2. В строке меню нажмите *Правка* > *Удалить* либо нажмите кнопку *Удалить выбранный элемент* () в панели инструментов.
3. На просьбу подтвердить удаление нажмите *Да*.

Выбранный объект будет удалён со связки.

2.3.1.5 Активирование / дезактивирование ключей

Если количество ключей на вашей связке становится угрожающе велико, и поиск нужного для зашифрования письма оборачивается всё более трудной задачей, вы можете временно дезактивировать ключи, которые не используете постоянно, но и не хотите удалять. С этого момента они не будут захламлять окно *Key Selection Dialog*.

Для дезактивации открытых ключей корреспондентов:

1. В окне PGPkeys выделите ключ, который хотите дезактивировать.
2. В строке меню нажмите *Ключи* > *Запретить*.

Пиктограмма ключа потускнеет, обозначая, что он временно отключён. Чтобы снова активировать ключ для использования:

1. Выделите ключ, который хотите активировать.
2. В строке меню нажмите *Ключи* > *Разрешить*.

Пиктограмма станет обычной, а ключ – готовым к работе.

Если фраза об угрожающем количестве ключей на связке справедлива для ваших собственных ключевых пар, некоторыми из которых вы пользуетесь относительно редко, можете дезактивировать и их. В этом случае конкретный ключ не сможет применяться для зашифрования и подписания данных, но вы сможете продолжать им пользоваться для расшифрования файлов и сверки своих ЭЦП.

Чтобы дезактивировать ключевую пару:

1. В окне PGPkeys нажмите правой кнопкой на ключ, который хотите дезактивировать > *Свойства ключа*.
2. В окне свойств ключа снимите галочку с опции *Имплицитное доверие*, а затем с *Разрешен*. Закройте окно свойств.

Изображение человечка с пиктограммы ключа пропадёт, а сам ключ потускнеет, обозначая, что он временно неактивен. Чтобы снова активировать ключевую пару:

1. Нажмите правой кнопкой на ключ, который хотите активировать > *Свойства ключа*.
2. В окне свойств ключа отметьте галочкой параметр *Разрешен*, а затем – *Имплицитное доверие*. Закройте окно свойств.

Пиктограмма станет обычной, а ключевая пара – готовой к работе.

2.3.2 Просмотр и настройка свойств ключей

Кроме просмотра наиболее общих атрибутов ключей непосредственно в окне менеджера PGPkeys, вы можете изучить и отредактировать дополнительные параметры любого ключа в окне его свойств.

Сведения в окне свойств ключа (*Свойства ключа*) разбиты по четырём вкладкам (рисунок 2.12):

- “*Общие*” содержит основные параметры и описание ключа;
- “*Подключи*” позволяет редактировать подключи шифрования;
- в “*Аннуляторы*” перечислены "отменители" данного ключа;
- в “*ADK*” указаны дополнительные ключи расшифрования.

Учтите, что вкладки “*ADK*” и “*Аннуляторы*” могут отсутствовать, если ключи ADK и "отменители" не были добавлены к данному ключу.

Чтобы открыть окно свойств, в менеджере PGPkeys нажмите правой кнопкой на имя ключа > *Свойства ключа*. Либо выделите нужный ключ и в панели инструментов нажмите кнопку *Показать свойства ключа или сертификата* ().

2.3.2.1 Основные свойства и смена ключевой фразы

Во вкладке основных свойств *Общие* (рисунок 2.12) содержатся следующие сведения и настройки.

Рис. 2.12

- Технические параметры ключа, а именно:
  - *ID* – уникальный идентификационный номер ключа.
  - *Тип* – тип асимметричного ключа.
  - *Размер* – длина асимметричного ключа в битах.
  - *Создан* – дата создания ключа.
  - *Срок* – окончание срока действия ключа (*Вечный*, если не имеет ограничения).
  - *Шифр* – симметричный алгоритм, используемый для шифрования этим ключом.
- Опцию *Разрешен*, позволяющую активировать / дезактивировать ключ.
- Фото-удостоверение.

- Кнопку *Смена пароля* для смены ключевой фразы либо *Соединение с ключом* для восстановления разделённого ключа в единое целое.
- Параметры *Отпечаток* с отпечатком открытого ключа и *Модель доверия*, показывающий уровень достоверности открытого ключа и степень доверия его владельцу.

Регулярная смена ключевой фразы не является обязательной практикой для асимметричных ключей (важнее, чтобы она просто была очень надёжной): если кто-то получит ваш закрытый ключ в своё распоряжение, замена прежней ключевой фразы уже не избавит ключ от угрозы компрометации. Поэтому важно менять её только при угрозе компрометации самой ключевой фразы, например, если кто-то стоял у вас за спиной и, вероятно, мог подсмотреть за нажатиями клавиш, когда вы её набирали.

Но если злоумышленник уже похитил копию закрытого ключа, процедура смены пароля вас не спасёт. В этом случае немедленно изготовьте новую ключевую пару и перешифруйте все зашифрованные документы, файлы и корреспонденцию, уничтожив копии, зашифрованные скомпрометированным ключом.

Чтобы изменить текущую ключевую фразу:

1. Во вкладке *Общие* нажмите кнопку *Смена пароля*.
2. Введите текущую ключевую фразу и нажмите *OK*.
3. В оба представленных поля введите новую ключевую фразу. Если хотите видеть, что набираете, снимите галочку с *Скрыть* (убедитесь, что в помещении нет посторонних). Нажмите *OK*.

Если вы сменили ключевую фразу из-за подозрений её компрометации, после процедуры обязательно примите меры к уничтожению всех резервных копий своих связок и данной ключевой пары, а затем очистите свободное пространство диска, поскольку оставшиеся копии закрытого ключа по-прежнему защищены скопрометированной ключевой фразой!

2.3.2.2 Свойства подключей шифрования и их настройка

Каждая асимметричная ключевая пара по определению состоит из двух ключей: открытого и закрытого. В PGP версии 6.0 и выше появилась возможность создавать, удалять и аннулировать дополнительные подключи шифрования без необходимости жертвовать своей базовой ключевой парой и собранными на её сертификате подписями. В целом это похоже на превращение вашего базового ключа в своего рода связку с хранищимися на ней подключами. Сущностное отличие лишь в том, что эти подключи используются только для зашифрования и расшифрования; для задач подписания информации служит только базовый закрытый ключ.

Основным назначением описанной функции является создание нескольких подключей шифрования, каждый из которых будет действовать в строго определённый период жизни базового ключа. Скажем, если вы сгенерировали базовый ключ со сроком жизни 3 года, можно создать ему три дополнительных подключа шифрования для каждого года жизни. Эта дополнительная система безопасности будет автоматически и регулярно заменять вам ключ шифрования без трудоёмкого процесса генерации и распространения нового открытого ключа. Но гораздо лучше не создавать несколько подключей сразу, а добавлять каждый новый по мере необходимости, когда период действия текущего начинает подходить к концу. Так каждый новый подключ будет совершенно непредсказуем для взломщика, что в свою очередь, многократно повысит надёжность всей системы.

Для просмотра и настройки подключей шифрования в окне свойств откройте вкладку *Подключи* (рисунок 2.13).

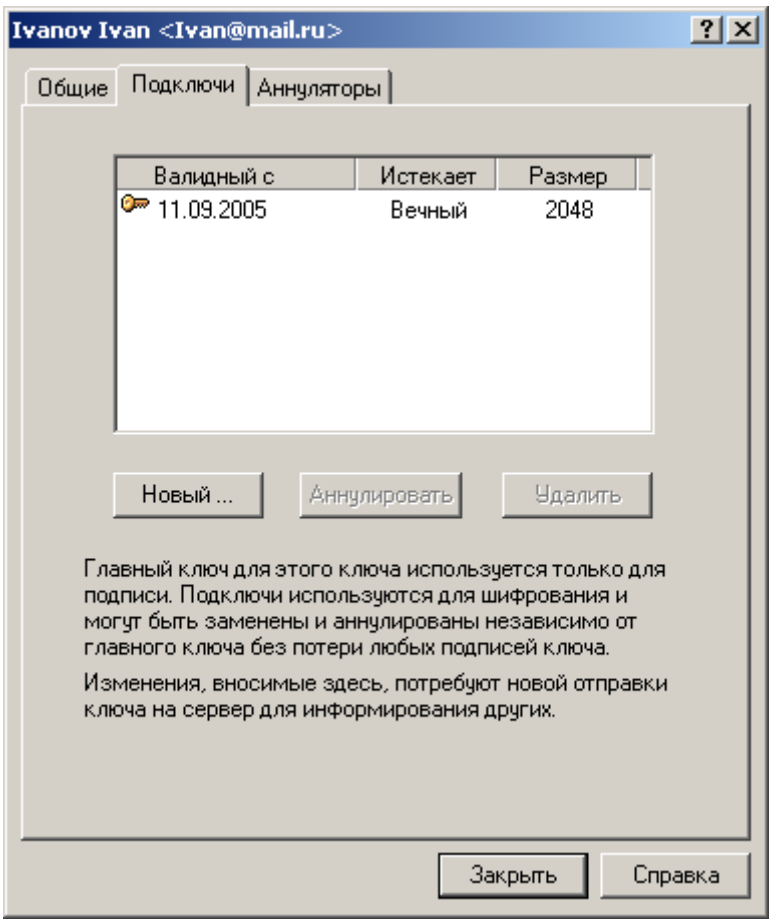

Рис. 2.13

Чтобы создать новый подключ:

1. Во вкладке *Подключи* нажмите кнопку *Новый*.
2. В появившемся окне в поле *Размер ключа* введите необходимый размер подключа в пределах 1024-4096 бит или выберите один из заданных в списке.
   Не создавайте подключ меньшей длины, чем базовый ключ шифрования.
   Скажем, если ваш базовый ключ имеет длину 2048 бит, не создавайте подключи меньшего размера – это снизит стойкость вашей ключевой пары.
3. В поле *Начальная дата* укажите дату, когда данный подключ должен быть активирован.
4. Для параметра *Срок истекает* выберите либо *Никогда*, чтобы не ограничивать период действия подключа, либо *Дата* и укажите дату окончания его действия.
   Во избежание недоразумений при использовании нескольких подключей не допускайте совпадения, наложения и пересечения дат начала и окончания их действия.
5. Нажмите *OK*.
6. Введите ключевую фразу и снова нажмите *OK*.

Дополнительный подключ шифрования будет сгенерирован и добавлен к базовому ключу. Теперь вам нужно обновить ключ на сервере или самостоятельно передать его всем корреспондентам с тем, чтобы при шифровании они использовали новые сгенерированные подключи.

Если у вас возникли подозрения, что любой из подключей был скомпрометирован (обычно это относится к тому, который действует в настоящий момент), вы можете аннулировать его вместо аннулирования открытого ключа в целом.

Чтобы аннулировать подключ шифрования:

1. Во вкладке *Подключи* выделите нужный и нажмите кнопку *Аннулировать*.

2. PGP предупредит, что аннулирование подключа сделает невозможным зашифрование с его помощью любой информации. Если вы уверены в своих действиях, нажмите *Да*.
3. Введите ключевую фразу и нажмите *OK*. Обязательно обновите свой открытый ключ на сервере и разошлите соответствующие уведомления своим постоянным корреспондентам!

Чтобы удалить подключ с базового ключа:

1. Во вкладке *Подключи* выделите нужный и нажмите кнопку *Аннулировать*.
2. PGP предупредит, что удаление подключа носит необратимый характер и сделает невозможным расшифрование любой зашифрованной им информации (поскольку будет удалена и соответствующая часть с базового закрытого ключа).
3. Если действительно хотите это сделать, нажмите *Да*. Обязательно обновите свой открытый ключ на сервере и разошлите обновлённые копии своим постоянным корреспондентам!

2.3.2.3 Свойства "отменителя"

Вкладка *Аннуляторы* (рисунок 2.14) содержит список ключей, владельцы которых уполномочены при необходимости аннулировать данный открытый ключ.

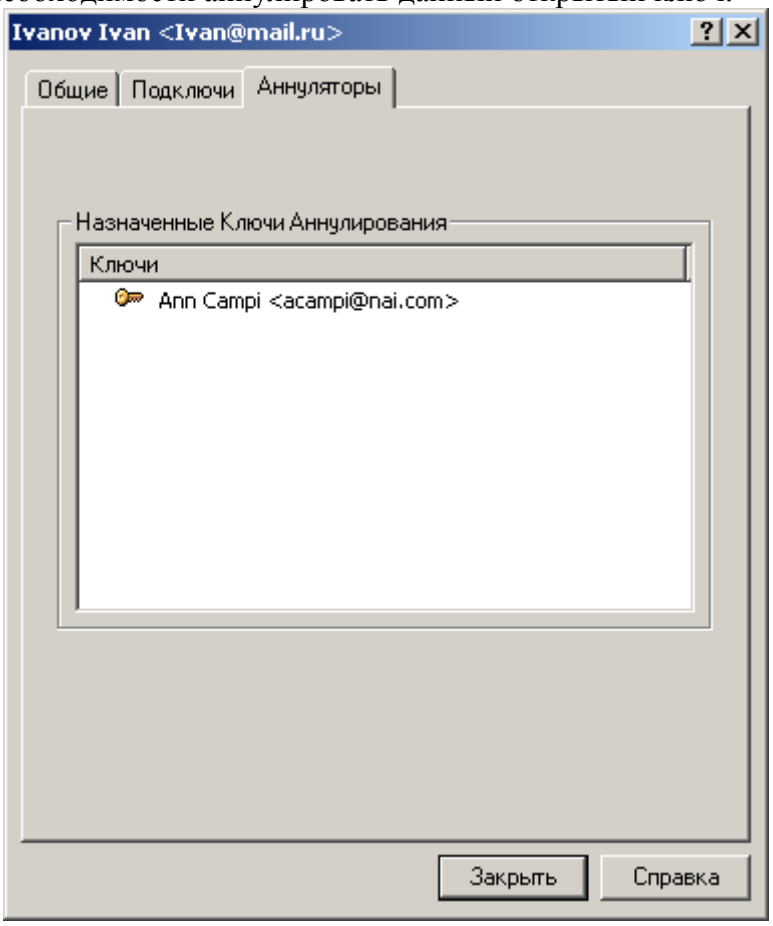

Рис. 2.14

Если ключ "отменителя" отсутствует на вашей связке, он будет представлен строкой *"Неизвестный ключ"*, за которой следует идентификационный номер. Выделите номер и нажмите кнопку *Update from Server*, чтобы загрузить копию открытого ключа с сервера.

Обязательно загружайте к себе на связку ключи всех уполномоченных вашими корреспондентами "отменителей". В противном случае PGP не сможет корректно

проверять ключи на предмет "аннулированности" и в итоге вы можете использовать скомпрометированный ключ!

2.3.3 Сертификация открытых ключей

Хотя асимметричные криптосистемы являются лучшим решением для обмена ключами и зашифрованной информацией, они крайне уязвимы к атакам "человек в середине", когда злоумышленник пытается выдать свой поддельный открытый ключ за ключ вашего корреспондента, чтобы позднее перехватывать, читать и изменять пересылаемые сообщения. Взаимное заверение пользователями открытых ключей друг друга – это краеугольный камень распределённой модели доверия Web of Trust, лежащей в основе PGP и служащей мерой противодействия таким атакам.

Считать открытый ключ корреспондента априорно подлинным можно лишь в одном случае – если он вручил вам свой ключ на жёстком носителе при личной встрече или если очно передал вам отпечаток (не номер ID!) своего ключа. Но зачастую это невозможно, ведь через Интернет приходится общаться с людьми, живущими за тысячи километров. Специально для цели точной идентификации любого открытого ключа они снабжены так называемыми отпечатками. Цифровой отпечаток открытого ключа (fingerprint) – это хэш-значение его материала, столь же уникальное, сколь и сам ключ.

Лучший способ установить подлинность полученной вами копии открытого ключа корреспондента – позвонить ему и попросить прочитать отпечаток с оригинала, хранящегося на его связке (прочитать отпечаток должен именно он вам, а не вы ему!). Маловероятно, что злоумышленник сможет перехватить такой произвольный звонок и провести активную атаку, попытавшись выдать себя за корреспондента. А если вам знаком голос корреспондента, это сделать будет практически невозможно.

Чтобы просмотреть отпечаток ключа, в менеджере PGPkeys нажмите правой кнопкой на имя ключа > *Свойства ключа*. Либо выделите нужный ключ и в панели инструментов нажмите кнопку *Показать свойства ключа или сертификата* (). В появившемся окне свойств ключа обратите внимание на *Отпечаток* (рисунок 2.15).

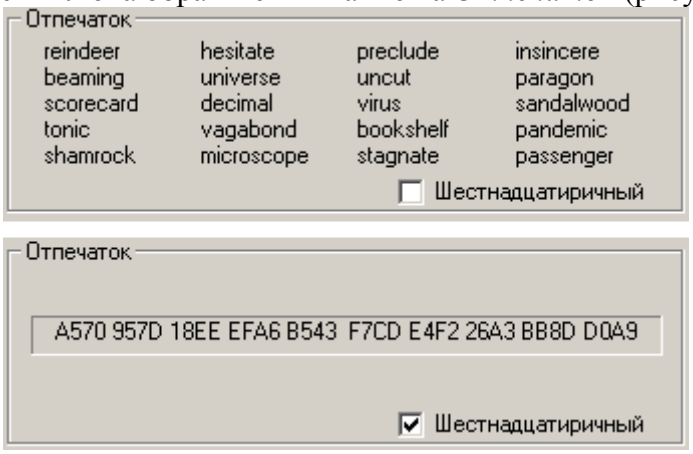

Рис. 2.15

Отпечаток ключа может быть представлен в двух формах: в виде уникального списка слов или в виде уникальной буквенно-числовой последовательности.

По умолчанию отпечаток представлен уникальным списком т.н. биометрических слов. Эти слова по своему назначению аналогичны международному авиационному алфавиту (наверное, вы слышали в западных фильмах эти "альфа-зулу-фокстрот-гольф" и т.п.), предназначенному для безошибочной передачи буквенной информации по аудио-каналу с сильными помехами, но в отличие от того алфавита, содержащего всего 26 букв-слов, биометрический словарь PGP включает 256 слов. Если вы решите сравнить отпечаток ключа, позвонив его владельцу, эти фонетически отчётливые слова позволят

точно идентифицировать ключ даже по плохой междугородней связи и даже если вы или корреспондент не знаете английского языка.

Отметив галочкой опцию *Шестнадцатиричный*, вы отобразите отпечаток в виде шестнадцатеричного числа. Такой формат удобен для передачи отпечатка через Интернет или его размещения на своём веб-сайте. Можно выделить и копировать число, а затем вставить его в любой документ. Кроме того, отпечаток открытого ключа в шестнадцатеричной форме иногда печатают на оборотной стороне визитных карточек.

Кроме непосредственно заверения чужого открытого ключа вы можете указать некоторый уровень доверия его владельцу в заверении других ключей и в выступлении в качестве их поручителя. Этот показатель считается вашим субъективным мнением о том, насколько данный пользователь компетентен в проверке подлинности открытых ключей, и насколько весомой вы считаете его подпись, заверяющую тот или иной ключ. Это значит, что если в будущем к вам в руки попадёт ключ, подписанный данным пользователем, он изначально будет для вас достоверным, хотя вы лично и не проверяли его подлинность.

Поскольку показатель степени доверия является вашим субъективным конфиденциальным мнением, он не экспортируется вместе с ключом и действенен только на вашей связке.

Чтобы установить степень доверия владельцу ключа убедитесь, что этот ключ вами подписан (экспортируемой или неэкспортируемой подписью). Затем:

1. В окне PGPkeys выделите ключ, и в строке меню выберите *Ключи* > *Свойства ключа*. В появившемся окне свойств ключа обратите внимание на раздел *Модель доверия* (рисунок 2.16).

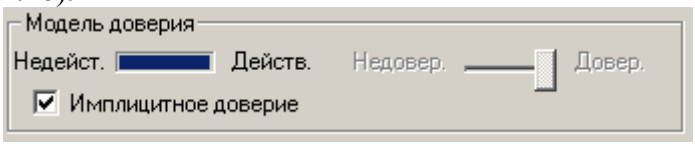

Рис. 2.16

2. Используйте регулятор *Уровень доверия*, чтобы установить нужный уровень доверия.
   - По умолчанию уровень доверия ключа установлен на *Недовер.* (нет доверия): подписи этого ключа не будут приниматься в расчёт при вычислении достоверности других ключей.
   - Если сдвинуть регулятор на средний уровень, подпись станет частично доверяемой и будет частично заверять другие ключи, т.е. одной этой подписи будет недостаточно, чтобы считать подписанные ключи достоверными: потребуется по меньшей мере две частично доверяемых подписи.
   - Если вы считаете, что владелец этого ключа достаточно осторожен и с большой тщательностью проверяет подлинность подписываемых ключей, установите регулятор в положение *Довер.* (полное доверие), и подпись этого ключа будет заверять другие так же, как ваша собственная. Учтите, что ключ, заверенный вами с помощью подписи *Экспортируемая доверенного представителя* или *Неэкспортируемая псевдо-представителя*, уже имеет максимальный уровень доверия, снизить который невозможно.
3. Сделав выбор, закройте окно свойств, чтобы сохранить изменения.

Учтите, что вы не можете менять уровень доверия своих ключей, поскольку логика программы исходит из допущения, что вы полностью доверяете собственным действиям, и ставит вас в основу иерархии вашего дерева сертификации. Программа считает, что конкретный открытый ключ принадлежит вам, если находит на связке соответствующий ему закрытый. Полная ключевая пара всегда имеет уровень доверия *Имплицитное доверие* – безусловное доверие.

2.3.4 Редактирование сертификата ключа

Сертификат каждого открытого ключа PGP содержит по меньшей мере одну идентифицирующую запись (удостоверение), позволяющую соотнести ключ с владельцем или с одним из его реквизитов: адресом электронной почты, номером ICQ и пр. Новый только что сгенерированный ключ имеет лишь одну такую запись. Но если вы хотите использовать данный ключ для различных email-адресов и других средств связи, хотите добавить фото-удостоверение как дополнительный способ опознавания, то в любой момент можете это сделать.

Обычная запись сертификата OpenPGP включает имя или псевдоним владельца ключа и, по желанию, его email-адрес.

Чтобы добавить обычную запись в сертификат ключа:

1. В окне PGPkeys выделите нужный ключ, в строке меню нажмите *Ключи* > *Добавить* > *Имя*.
2. В появившемся окне *Имя нового пользователя* в поле *Новое имя для добавления к ключу* введите своё имя и в поле *Новый адрес для добавления к ключу* – адрес электронной почты. Нажмите *OK*.
3. Введите ключевую фразу и снова *OK*.

Новая идентифицирующая запись будет внесена в сертификат ключа. Если вы захотите сделать только что добавленную или любую другую запись сертификата главной (имя и email-адрес главной записи отображаются в имени ключа напротив иконки , а сама запись стоит первой в списке), выберите нужную, в строке меню нажмите *Ключи* > *Установить как основное имя* и введите ключевую фразу.

Не забывайте, что после редактирования открытого ключа или внесения любых изменений в содержание его сертификата, ключ нужно обновить на сервере.

Кроме адреса электронной почты сертификат ключа может включать любые другие идентификационные сведения.

Чтобы внести в сертификат иные записи с различными типами идентификации:

1. В окне PGPkeys выделите нужный ключ, в строке меню нажмите *Ключи* > *Добавить* > *Имя*.
2. В появившемся окне *Имя нового пользователя* в поле *Новое имя для добавления к ключу* введите своё имя и в поле *Новый адрес для добавления к ключу* – идентификационные сведения. Если добавляете свой номер ICQ для шифрования переговоров при помощи плагина, укажите ID в следующем формате: *ICQ:номер*. Нажмите *OK*.
3. Введите ключевую фразу и снова *OK*.

Не забудьте обновить ключ на сервере.

В PGP 6.0 и выше вы также можете добавить в сертификат ключа типа DH/DSS фотографическое удостоверение.

Никогда не опирайтесь на фото-удостоверения для определения подлинности полученного открытого ключа! Используйте их только для первичной идентификации.

Чтобы добавить фото-удостоверение:

1. В окне PGPkeys выделите нужный ключ, в строке меню нажмите *Ключи* > *Добавить* > *Фотографию* (рисунок 2.17).

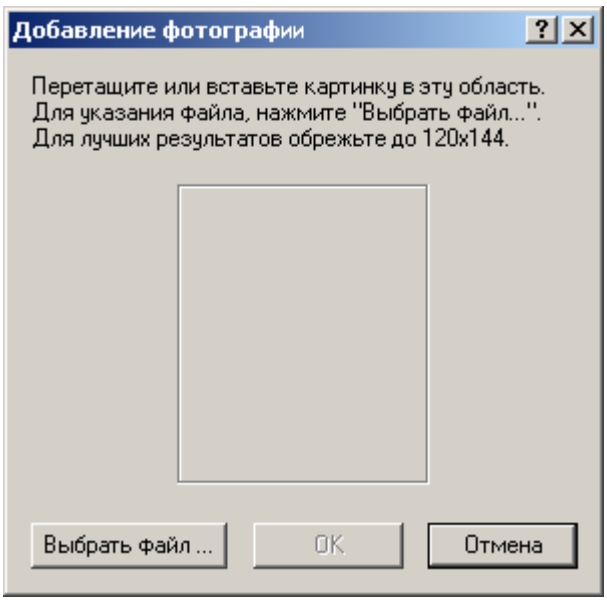

Рис. 2.17

2. Можете добавить фотографию в появившееся окно *Добавление фотографии* тремя разными способами: её можно копировать и вставить (используя клавиши *Ctrl+C / Ctrl+V*), можно перетащить графический файл из Проводника, можно нажать кнопку *Выбрать файл* и выбрать его вручную. Так или иначе, используйте картинку в формате jpeg или bmp (в последнем случае программа конвертирует файл в jpeg автоматически) и, для лучшего качества, с габаритами 120x144 пикселей.
3. Выбрав картинку нажмите *OK*.
4. Введите ключевую фразу и снова *OK*.

Фотография будет добавлена к сертификату в виде отдельной записи. Теперь обновите ключ на сервере, чтобы каждый пользователь мог её увидеть в окне свойств полученной им копии вашего ключа.

Если хотите заменить текущую фотографию (при замене будут потеряны все подписи, заверяющие текущее фото-удостоверение):

1. В окне PGPkeys разверните список записей сертификата нужного ключа. Найдите запись вида “ Фотография”.
2. Выделите эту запись, в строке меню нажмите *Правка > Удалить*.
3. Добавьте новую фотографию, как было описано выше. По окончании не забудьте обновить ключ на сервере.

2.3.5 Аннулирование ключа

Если по какой-то причине у вас возникнет подозрение или станет доподлинно известно, что ваша ключевая пара была скомпрометирована, нужно немедленно уведомить всех текущих и будущих корреспондентов не использовать данный открытый ключ для обмена информацией с вами, ибо велик шанс её попадания в чужие руки. Наиболее быстрый и удобный способ сделать это – выпустить сертификат аннулирования ключа (Key Revocation Certificate, KRC). Он будет присоединён к открытому ключу и аннулирует его, а после импортирования этой копии ключа на связку корреспондент не сможет использовать его для зашифрования информации.

Аннулированная ключевая пара не может использоваться для зашифрования и подписания информации. Но ей можно продолжать пользоваться для расшифрования и сверки ЭЦП (в последнем случае вы всякий раз будете получать предупреждение, что ключ аннулирован).

Кроме аннулирования своих ключей вы можете отзывать с чужих ключей собственные сертифицирующие подписи, например, если посчитаете, что ключ скомпрометирован и вы более не можете гарантировать его целостность и принадлежность только изначальному владельцу, или если по иным причинам не захотите, чтобы другие пользователи полагались на вашу подтверждающую подпись. Аннулированная подпись никогда не берётся в расчёт при вычислении достоверности ключа.

Чтобы аннулировать свою ключевую пару или отозвать подтверждающую подпись с чужого сертификата:

1. В окне PGPkeys выделите нужный ключ или свою ЭЦП, и в строке меню нажмите *Ключи* > *Аннулировать*.
2. На просьбу подтвердить свои намерения ответьте *Да*, если действительно хотите это сделать.
3. Введите ключевую фразу (при отзыве подписи – ключевую фразу того ключа, которым ставили эту подпись) и нажмите *OK*.

Ключевая пара или подтверждающая подпись будет аннулирована и отмечена иконкой или соответственно. Обязательно обновите ключ на сервере и разошлите уведомления с копиями ключа всем своим постоянным корреспондентам!

Но может сложится и иная ситуация. Допустим, вы забудете свою ключевую фразу или потеряете закрытый ключ (например, после серьёзного системного сбоя). Без закрытого ключа и ключевой фразы вы не сможете издать KRC, чтобы аннулировать открытый ключ и не допустить шифрование им информации, которую теперь тоже невозможно прочитать. Если вы не резервировали свой закрытый ключ, чтобы восстановить его в случае потери, описанный сценарий безнадёжен.

В качестве меры предосторожности можно уполномочить одного или нескольких доверенных человек в чрезвычайной ситуации аннулировать ваш ключ. Эти "отменители" смогут издать сертификат KRC собственными закрытыми ключами без всякого вмешательства с вашей стороны. (Эта функция поддерживается только в PGP 6.0 и выше для ключей типа DH/DSS.)

Чтобы добавить "отменителя":

1. В окне PGPkeys выделите нужный ключ, и в строке меню нажмите *Ключи* > *Добавить* > *Аннулирование*.
2. В появившемся списке ключей выделите те из них, владельцам которых хотите дать полномочия аннулирования. Нажмите *OK*.
3. На просьбу подтвердить свои намерения ответьте *Да*, если действительно хотите это сделать.
4. Введите ключевую фразу и нажмите *OK*.

Владельцы указанных вами ключей получат полномочия аннулирования и смогут аннулировать ваш ключ, как и любой собственный. Обязательно передайте им обновлённую копию своего ключа, а также отправьте его на сервер.

Также нужно отметить один крайне важный нюанс. Если ваш ключ был аннулирован "отменителем", то, чтобы у стороннего пользователя он выглядел таковым (), и ваш открытый ключ, и открытый ключ "отменителя" должны присутствовать на его связке. Если ключа "отменителя" на связке пользователя нет, ваш аннулированный ключ будет казаться ему нормальным, и он будет продолжать шифровать им информацию. Поэтому ключ "отменителя" должен находиться в относительно широком распространении и, по меньше мере, его копия должна храниться на общественном сервере-депозитарии.

Если уполномоченный отменитель недостаточно добросовестен и есть опасение, что он может злонамеренно аннулировать ваш ключ без всякой на то необходимости, можно поступить иначе. Небезынтересна такая схема: вы создаёте новую ключевую пару, которую добавляете к своему главному ключу в качестве доверенного отменителя.

Открытый ключ этой новой пары вы отправляете на сервер, закрытый разделяете на несколько долей, каждую из которых отдаёте на хранение относительно доверенному человеку. В форс-мажорной ситуации все они по вашей просьбе реконструируют этот закрытый ключ и аннулируют им ваш собственный.

2.4 Работа с буфером обмена и активным окном

Хотя шифрование электронной почты более удобно осуществлять с помощью плагинов, далеко не все мэйл-клиенты поддерживают их, да и сами плагины отсутствуют в бесплатной freeware-версии PGP. Однако программа предоставляет ничуть не более сложный способ криптографирования текста – это работа с активным окном и с содержимым буфера обмена через PGPtray. Через PGPtray можно легко зашифровать, расшифровать или подписать любой текст, будь то электронное письмо или содержимое любого текстового файла, а использование комбинаций "горячих клавиш" сделает выполнение этих операций совершенно необременительным.

Два способа работы с текстом через PGPtray – активное окно и буфер обмена – в целом равнозначны. Но если для зашифрования текста в буфере обмена этот текст предварительно нужно туда скопировать, работа с содержимым активного окна более автоматизирована. Немного попрактикуйтесь, и вы сами почувствуете разницу и определите применимость каждого способа для решения тех или иных задач.

2.4.1 Зашифрование и подписание текста

Как правило, удобнее и проще шифровать текст с помощью функции активного окна. Если вам нужно зашифровать или подписать не всё содержимое окна, а только фрагмент находящегося там текста, достаточно его выделить и, оставив окно в фокусе, выполнить те же инструкции, что и для содержимого окна целиком.

1. Напишите своё письмо, как вы делаете это в обычных условиях. Можно использовать любой текстовый редактор, мэйл-клиент и даже веб-интерфейс почтовой службы. (Желательно отправлять важные сообщения с пустым заголовком темы, чтобы не давать потенциальному злоумышленнику даже малейшей информации о содержании письма.)
2. Составив письмо, выполните одно из следующих действий – они равноправны:
   - оставьте окно текстового редактора активным и нажмите на иконку PGPtray () > *Текущее окно* > *Зашифровать* (чтобы только зашифровать), *Подписать* (чтобы только подписать) или *Зашифровать и подписать* (чтобы одновременно подписать и зашифровать своё письмо);
   - оставьте окно текстового редактора активным и нажмите комбинацию "горячих клавиш", соответствующую требуемой операции с текстом;
   - выделите и копируйте текст в буфер обмена (Ctrl+C), нажмите на иконку PGPtray () > *Буфер обмена* > *требуемая операция с текстом* (опция *Очистить* так же позволяет очистить буфер обмена, а *Редактировать* – отредактировать его содержимое).
3. Если вы шифруете текст, а не только подписываете его, то в открывшемся окне выбора ключей получателей *Выбор ключа* (рисунок 2.18) укажите, для каких корреспондентов хотите зашифровать своё сообщение. Не удивляйтесь количеству пунктов в верхней части окна – там представлены не отдельные открытые ключи с вашей связки, а все записи сертификатов этих ключей, которых может быть намного больше. Поэтому для каждого получателя сообщения достаточно указать всего одну запись с его ключа.

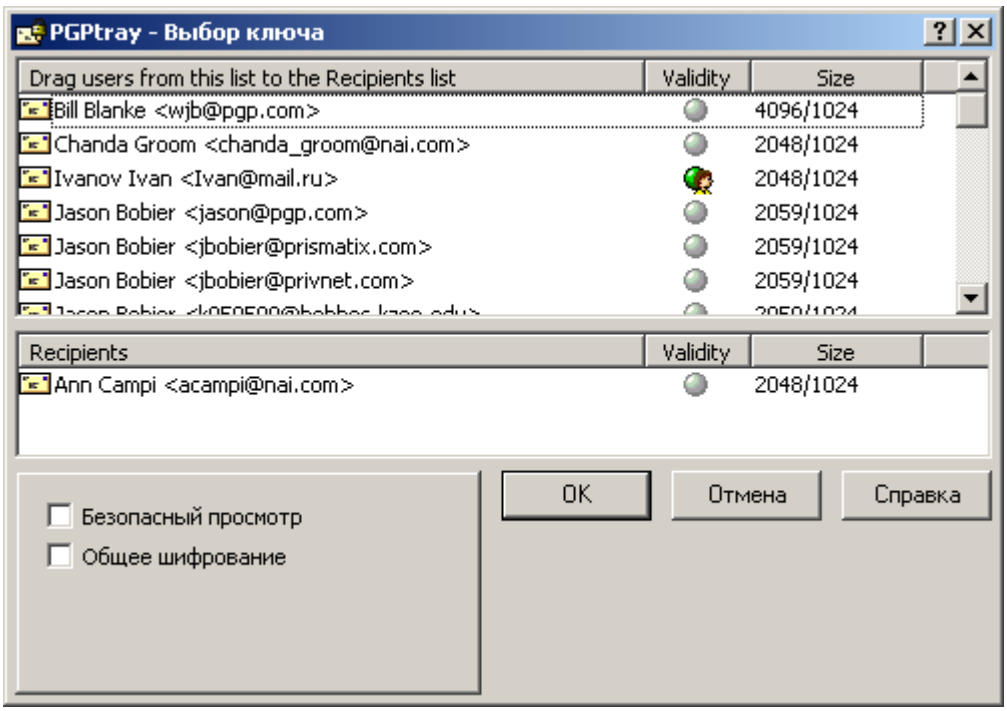

Рис. 2.18

Перетащите в нижнюю часть окна те из них, для кого вы хотите зашифровать своё послание (можно не перетаскивать, а дважды щёлкнуть по любой записи, чтобы переместить её вниз или вверх). Если у вас выбран ключ "по умолчанию", то он изначально будет присутствовать в числе получателей сообщения. Не стоит его убирать, иначе впоследствии вы сами не сможете расшифровать отправленное письмо, чтобы, скажем, его перечитать.

Индикатор *Validity* показывает степень достоверности каждой из идентификационных записей. Крайне нежелательно шифровать сообщение теми ключами (и отправлять на те адреса), которые отмечены как недостоверные. Проведите хотя бы самую элементарную и минимальную проверку подлинности данного ключа и соответствующей записи и подпишите её.

4. При необходимости отметьте дополнительные опции шифрования и нажмите *OK*:
   - *Безопасный просмотр* – отображать у получателя расшифрованный текст письма в специальном окне *Безопасный просмотр*, используя шрифт, предотвращающий так называемую TEMPEST-атаку (удалённый съём информации по электромагнитному излучению монитора); кроме того, в этом случае сообщение невозможно будет сохранить в виде открытого текста. Разумно использовать для сообщений крайней секретности, но не для повседневных писем (ещё и потому, что этот поставляемый с PGP TEMPEST-защитный шрифт не имеет кириллических символов, и, соответственно, письмо придётся писать латиницей). Также имейте в виду, что в PGP до 6.0 поддержка функции *Безопасный просмотр* отсутствует, и если получатель использует более раннюю версию программы, она выбранную вами опцию просто проигнорирует.
   - *Общее шифрование* – симметричное шифрование паролем вместо открытого ключа. При выборе этой опции программа предложит ввести ключевую фразу, которая потребуется и для расшифрования текста. Понятно, что использовать эту функцию для пересылки электронной почты нерационально – криптография с открытым ключом для этой цели практичнее и удобнее. Однако шифрование простым паролем может пригодиться для защиты

документов, хранящихся на вашем собственном диске. (С технической точки зрения программа использует введённый пароль для шифрования сеансового ключа, которым шифруется само сообщение по алгоритму, указанному как *Назначенный алгоритм* в настройках PGP.)

5. Если вы электронно подписываете текст, а не только шифруете его, программа попросит ввести ключевую фразу вашего закрытого ключа (если у вас несколько ключевых пар, в меню *Ключи подписи* можно выбрать ключ для подписания).
   Учтите, что если у вас выбран ключ "по умолчанию", и его ключевая фраза в данный момент хранится в кэше, этот запрос не появится – PGP автоматически подпишет текст вашим основным ключом. Чтобы выбрать другой ключ вам потребуется предварительно удалить ключевую фразу из оперативной памяти (*PGPtray* > *Буфер обмена* > *Очистить*).

PGP зашифрует / подпишет текст и заменит оригинал криптографированным материалом (рисунок 2.19). (Если вместо работы с активным окном вы предпочли работу с буфером обмена, вам самим придётся вставить обработанный текст в нужное приложение.)

```
-----BEGIN PGP MESSAGE-----
Version: PGPfreeware 6.5.8 for non-commercial use <http://www.pgp.com>
Comment: Так будет выглядеть зашифрованное сообщение

qANQR1DBwU4DJdJ0oint1icQCADpr4Q6iSkbMZz0MTfTHSGFfpiFv7nPMUmO90El
olIbO8y1d7i2qqCE3PvcWd8jGEvQrtOk0pW2ACslJaVfLaVr45CAE7YX/BCGismx
rq9fvZd10RhlyeVcbqyAn5i4RRVJzKugQRyVxYajfMrJpObqVfbj76JElfNQZTFV
bR0bQd2JLLz/6mRN/zqAZf/LLJRVPoAhjM6JQQ1jZ+PmIID9tpX1WWCJ0sHuHgzE
qJDtGChTlIA1QtCgssmPQwIAOgcPI+laCeJ7b7ZR/agyAGlk2TXifnBch/8wyiLN
EbLeywjxbbkWSR11/Ce2/Kzg7z5mhGKjr7ddrLrN+DG7VrJ7B/9Lo3fgeehFMJ7o
iteuOS7xVflSKbMUMRrPBAEb0mOmRJyMgzNFxJLY3raaTIPSwjmAlZn/4rnFYYxr
yIm8r2Vts0C/50PD1N5j59UEXWI5jbJbb4Tn/49jAISTiEHrUmAG2SQSU8GMIafr
JFyYrLOutvhdPR4DR2o/K2zjT23YooWuH2Cqw05SSnex2I84IZMt8OljfQ6NshKV
NCXvJ0DA1gUKKbs0o/7GdKfdb7D/TIAKrptBrujYNlli/OARaeA9p7rygZXXy0gj
j16vPmQ9hw8phjENM21PnxRTWS5rKcC6mcs+eRQoTsL9GtyLn4gzrhrNRLTt23pF
cDK1qP60ycGhMO7aJLo2aLVruBYu5rX1kqkgCox/r1bexHmWqBEpYqRZ8+wRhgdu
nk4RFFe4/qSVK343CeHZiedOIDBCXAi3a20arH6XU+gZQQ+1IKNSws6vw8bOnf9S
WZ3f/IuZTZDpZbU6FymkPvRv+6sSsbAugff4asW5PD8rEXBrE74EZNUSMPTzyWxO
IbkCD/s7nTbOlVQQJu0iiNHxza2eU3Qs19CjfADzFYehVkpGWv/CP4KrhzFYFuZR
yTKtPqaiu5NzYlS/hDxcjYTYfnAja3RLLgC2JWNSIqJ0kX7vweNo8oApI+nLxlaO
SvZ8yoheelMcU4TK02jWRKXSSKMQwLYfLiHWiiTU6zHbeFGpvqkhKTVtSe1QrNG6
nIPgyYB3/33psJgBUCq0IhlrvYIU09gmyjsDNB/VX0EgCWKmOakduUWbREEDgXNr
Jxdj5ZDmBBnfBMCEg6Jgo40hiYroh+Z1IrhLTGNd9iKCENlCz6Tpv5FI6vi1wYpi
9GZtepAkD9RSdC6Puu2esi4uGWHmGkb/d17DKn2zZ9xMxzjI8kViIYzsKxVzDb/M
bNFQL24pQndFzwkKdDIi2sXAEn/fZradtbs7caSsxC2dBu+wc7UAnGoTbWp6p+r7
m0VL2ioUwPodvc09zAxB3TdLPGu9/n4qFh0fZHjSpw+Hom77aQerE1KhbkQs34KT
X67eVp4Upm0OIPWJgQW3U8VMksYxFgCuUrHGZWaV6N3ZtFUCqSAF52zdHgOYV1GJ
38US8ztJqQ3nkwIC6wJCJX3NOSAjqZaR1TGT7NCtfx+JV6NYSBRxv5wa
=G8km
-----END PGP MESSAGE-----
```

Рис. 2.19

2.4.2 Расшифрование и сверка ЭЦП

Расшифрование текста и сверка цифровой подписи особенно легки с использованием "горячих клавиш" – достаточно пары нажатий. В остальных случаях, как и с шифрованием, можно использовать PGPtray. Если вы хотите расшифровать сообщение через буфер обмена, нужно выделить весь блок шифртекста вместе с заголовками типа “-----BEGIN PGP MESSAGE-----”, “-----END PGP SIGNATURE-----” и др. и целиком копировать его в буфер обмена.

Как правило, попытка расшифровать сообщение через активное окно прямо со страницы веб-сайта приводит к ошибке. Так случается потому, что веб-страницы обычно содержат графику и множество других нетекстовых элементов. Но чтобы не копировать шифртекст в буфер обмена можно пойти на маленькую хитрость: достаточно выделить шифртекст в окне браузера и затем нажать комбинаю клавиш для расшифрования или указать эту же команду через меню работы с активным окном в PGPtray.

Чтобы расшифровать текстовое сообщение и/или сверить его электронную подпись:

1. Откройте сообщение в своём мэйл-клиенте (если это письмо), текстовом редакторе или веб-браузере. Если оно зашифровано, а не только подписано, вы увидите лишь нечитаемый шифртекст.
2. Выполните одно из следующих действий – они равноправны:
   - оставьте окно текстового редактора активным и нажмите на иконку PGPtray () > *Текущее окно* > *Расшифровать и Проверить* (чтобы расшифровать сообщение и/или сверить ЭЦП);
   - оставьте окно текстового редактора активным и нажмите комбинацию "горячих клавиш", соответствующую операции расшифрования;
   - выделите блок шифртекста вместе с заголовками и копируйте его в буфер обмена (Ctrl+C), нажмите на иконку PGPtray () > *Буфер обмена* > *Расшифровать и Проверить*.
3. Появится окно *Введите пароль* со списком открытых ключей, которыми зашифровано сообщение. Если сообщение предназначено вам, программа попросит ввести ключевую фразу одного из ваших закрытых ключей. Если же вместо поля для ввода ключевой фразы в окошке указана ошибка *"Невозможно расшифровать данное сообщение ..."*, причина этого в том, что у вас на связке нет нужного для расшифрования закрытого ключа (он мог быть удалён, либо отправитель намеренно или случайно не зашифровал письмо вашим открытым ключом).
4. Введите ключевую фразу и нажмите *OK*.

Программа расшифрует сообщение и отобразит результат в окошке *Просмотр текста*. Если сообщение было подписано, там же будет указано состояние цифровой подписи.

Если при зашифровании отправитель отметил опцию *Безопасный просмотр*, PGP выдаст предупреждение, что письмо предназначено только для ваших глаз и его стоит читать с соблюдением максимальных мер предосторожности. Когда будете готовы открыть сообщение, нажмите *OK*. Текст будет выведен в окне *Безопасный просмотр* с помощью специального TEMPEST-защитного шрифта. (Имейте в виду, что ни копировать его, ни сохранить в расшифрованном виде вам не удастся.)

Если полученное сообщение было подписано, программа также сообщит вам некоторые сведения о цифровой подписи (рисунок 2.20).

```
*** СТАТУС ПОДПИСИ PGP: хороший
*** Подписыватель: Ivanov Ivan <Ivan@mail.ru>
*** Подписано: 17.12.04 13:21:52
*** Проверено: 19.12.04 5:58:28
*** НАЧАЛО РАСШИФРОВАННОГО/ПРОВЕРЕННОГО СООБЩЕНИЯ PGP ***

Текст подписанного сообщения

*** КОНЕЦ РАСШИФРОВАННОГО/ПРОВЕРЕННОГО СООБЩЕНИЯ PGP ***
```

Рис. 2.20

Это выглядит как набор заголовков, где в строке *Подписано* указана дата подписания (относительно вашего часового пояса), в *Проверено* – дата сличения подписи (т.е. текущий момент), в *Подписыватель* – имя владельца ключа, которым была поставлена подпись, а в *Статус подписи PGP* – собственно, состояние подписи:

- *Good* – информация получена вами ровно в том виде, в каком была подписана и отправлена автором.
- *Bad* – подписанная информация была каким-то образом изменена (искажена). Причиной тому могло послужить не только злонамеренное вмешательство, но и более тривиальные вещи, например, плохое качество связи, повлекшее искажение информации в процессе передачи, случайное редактирование сообщения автором уже после подписания, изменение, внесённое почтовой программой отправителя или вашей. В любом случае, к подобного рода сообщениям следует относиться с большой осторожностью; желательно также в кратчайшие сроки выяснить причину происшедшего.
- *Unknown* – это говорит о том, что на вашей связке ключей отсутствует тот, которым информация была подписана, и, следовательно, программа не может сверить подпись. В таких ситуациях PGP пытается самостоятельно связаться с сервером-депозитарием, чтобы найти соответствующий открытый ключ (если в настроках программы во вкладке *Серверы* включена опция *Удостоверение*).
- *Invalid* – так PGP уведомит вас о том, что ключ автора сообщения есть на вашей связке, но не признан подлинным, и, соотственно, программа не может оценить целостность подписанной информации. Вам нужно проверить достоверность ключа и заверить его.

При сличении подписи обязательно проверяйте, чтобы дата/время, указанные в строке *Проверено*, совпадали с текущими показаниями системных часов! Если вы не будете этого делать либо будете делать недостаточно тщательно, злоумышленник сможет одурачить вас, подсунув сформированное определённым образом составное сообщение, при расшифровании выглядящее так, словно было подписано одним из ваших доверенных корреспондентов. Но поскольку мошенник не может доподлинно знать с точностью до секунд, в какой момент времени вы откроете письмо, указанная им в строке *Проверено* дата будет иметь расхождение с реальной датой расшифрования сообщения (т.е. с текущим моментом).

Учтите, что метка времени, стоящая в строке *Подписано*, указывает время системного таймера отправителя. Отправителю эту метку крайне легко сфальсифицировать – достаточно перед подписанием перевести системные часы.

2.5 Защита файлов

PGP позволяет шифровать не только текст, но и файлы для их безопасного хранения на диске или для пересылки в качестве вложений к электронным письмам. Зашифрованный файл можно без опасений размещать и в Интернете, поскольку никто кроме владельца соответствующего закрытого ключа не сможет узнать его содержание.

При шифровании папки она не будет зашифрована целиком; напротив, PGP индивидуально зашифрует находящиеся в ней файлы. Чтобы зашифровать папку с сохранением структуры каталогов, стоит предварительно упаковать её в архив (например, с помощью WinZip) и уже затем зашифровать сам архивный файл.

Плагин PGP в некоторых мэйл-клиентах не способен автоматически зашифровывать и расшифровывать вложения электронной почты. Поэтому чтобы безопасно переслать файл или извлечь его из полученного письма вам придётся вручную выполнить с ним описанные ниже действия.

Зашифрование и подписание файлов можно производить двумя способами: через контекстное меню в Проводнике Windows или с помощью утилиты PGPtools, которую

можно вызвать через PGPtray. Расшифровывать же файлы проще всего в Проводнике, просто дважды щёлкнув на имя зашифрованного файла; вам понадобится только ввести нужную ключевую фразу, и в том же каталоге появится расшифрованная копия этого файла.

Чтобы выполнить ту или иную операцию над файлом с помощью PGPtools, можно либо нажать на соответствующую кнопку и указать этот файл в меню *Обзор*, либо перетащить этот файл из Проводника на нужную кнопку инструмента. Кроме того, в меню *Обзор*, вызываемом с помощью этих кнопок, присутствует опция *Буфер обмена*, позволяющая выполнить данную операцию над содержимым буфера обмена. Назначение кнопок инструмента следующее (рисунок 2.4, слева направо):

- *PGPkeys* – открыть менеджер ключей;
- *Encrypt* – зашифровать файл;
- *Sign* – подписать файл;
- *Encrypt and Sign* – подписать и зашифровать файл;
- *Decypt / Verify* – расшифровать файл и / или сверить цифровую подпись;
- *Wipe* – стереть файл с диска (уничтожить без возможности восстановления);
- *Freespace Wipe* – очистить диск от фрагментов прежде удалённых файлов.

Нажав в верхнем левом углу окошка и выбрав *Stay On Top*, вы заставите инструмент находиться поверх остальных окон.

Если вы зашифровываете файл, а не только подписываете его, то откроется окно выбора ключей получателей *Выбор ключа* (рисунок 2.21), где нужно указать, для каких корреспондентов вы хотите зашифровать этот файл. Не удивляйтесь количеству пунктов в верхней части окна – там представлены не отдельные открытые ключи с вашей связки, а все записи сертификатов этих ключей, которых может быть намного больше. Поэтому для каждого получателя файла достаточно указать всего одну запись с его ключа.

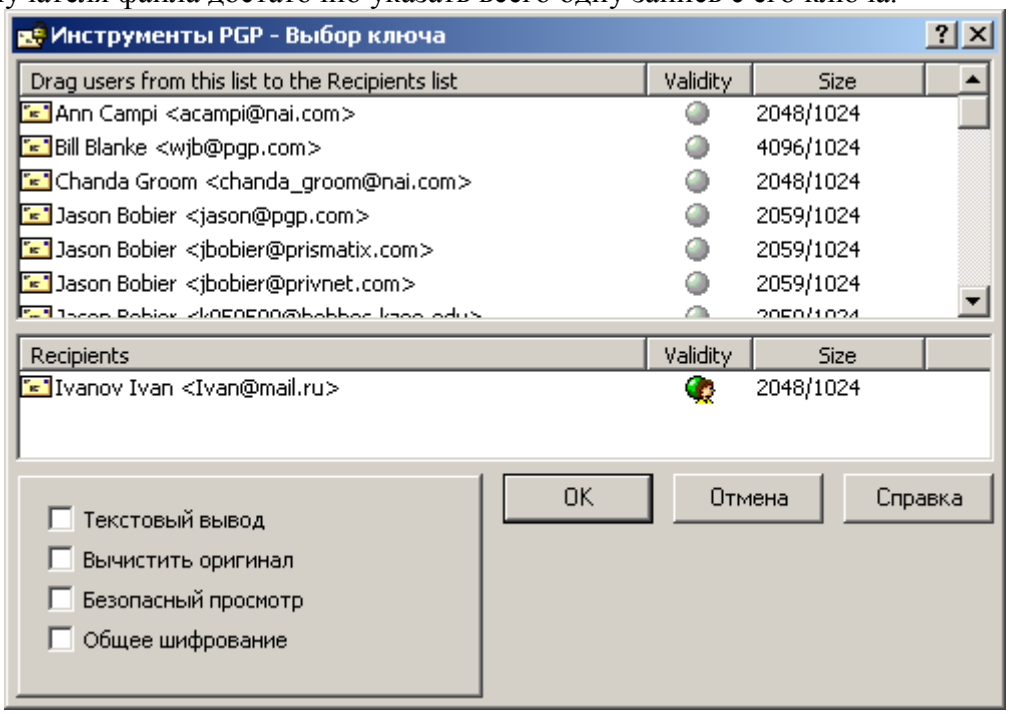

Рис. 2.21

Перетащите в нижнюю часть окна те из них, для кого вы хотите зашифровать файл (можно не перетаскивать, а дважды щёлкнуть по любой записи, чтобы переместить её вниз или вверх). Если у вас выбран ключ "по умолчанию", то он изначально будет присутствовать в числе получателей. Не стоит его убирать, иначе впоследствии вы сами не сможете расшифровать отправленный файл, и ни в коем случае не убирайте его, если

шифруете файл для сохранения у себя на диске (только если ни собираетесь заменить его другим своим ключом).

Индикатор *Validity* показывает степень достоверности каждой из идентификационных записей. Крайне нежелательно шифровать файл теми ключами (и отправлять на те адреса), которые отмечены как недостоверные. Проведите хотя бы самую элементарную и минимальную проверку подлинности данного ключа и соответствующей записи и подпишите её.

При необходимости отметьте дополнительные опции шифрования и нажмите *OK*:

- *Текстовый вывод* – сохранить шифртекст не в двоичном, а в ASCII-формате (в текстовом виде). Некоторые старые мэйл-клиенты не позволяют пересылать двоичный код, и эта опция может оказаться полезной. Кроме того, таким образом можно отправлять файл не вложением, а прямо в теле письма, если открыть зашифрованный файл любым текстовым редактором и скопировать содержимое в письмо. Учтите, однако, что использование этой опции увеличит объём файла примерно на 30% (в сравнении с шифрованием с выключенной опцией, а не с исходным файлом).
- *Вычистить оригинал* – уничтожить исходный файл с открытым текстом после зашифрования, перезаписав его на диске случайными данными. Так, файл останется только в виде шифртекста, а оригинал будет более недоступен.
- *Безопасный просмотр.*
- *Общее шифрование* – симметричное шифрование паролем вместо открытого ключа. При выборе этой опции программа предложит ввести ключевую фразу, которая потребуется и для расшифрования файла. Понятно, что использовать эту функцию для пересылки файла по электронной почте нерационально – криптография с открытым ключом для этой цели практичнее и удобнее. Однако шифрование простым паролем может пригодиться для защиты файлов, сохраняемых на вашем собственном диске. (С технической точки зрения программа использует введённый пароль для шифрования сеансового ключа, которым шифруется файл по алгоритму, указанному как *Назначенный алгоритм* в настройках PGP.)

Если вы электронно подписываете файл, а не только шифруете его, программа попросит ввести ключевую фразу вашего закрытого ключа (если у вас несколько ключевых пар, в меню *Ключи подписи* можно выбрать ключ для подписания). Учтите, что если у вас выбран ключ "по умолчанию", и его ключевая фраза в данный момент хранится в кэше, этот запрос не появится – PGP автоматически подпишет файл вашим основным ключом. Чтобы выбрать другой ключ вам потребуется предварительно удалить ключевую фразу из оперативной памяти (*PGPtray > Буфер обмена > Очистить*).

Если вы только подписываете файл, окно *Введите пароль* будет содержать несколько дополнительных опций:

- *Нарушенная подпись* – изготовить "съёмную" цифровую подпись. Если опция включена (а она включена по умолчанию), цифровая подпись будет сохранена в виде отдельного крохотного файла, имеющего такое же имя, что и у подписанного файла, но с расширением.sig. Такой файл-подпись можно передавать и публиковать отдельно от подписанного, дабы не осложнять использование подписанного файла людям, не пользующимся PGP. Если опцию выключить, файл будет сохранён, как при обычном шифровании, и использовать его без сверки ЭЦП будет невозможно.
- *Текстовый вывод* – сохранить "съёмную" ЭЦП или подписанный файл (в зависимости от предыдущей настройки) не в двоичном, а в ASCII-формате (в текстовом виде). Некоторые старые мэйл-клиенты не позволяют пересылать двоичный код, и эта опция может оказаться полезной. Кроме того, таким образом можно отправлять файл не вложением, а прямо в теле письма, если

открыть зашифрованный файл любым текстовым редактором и скопировать содержимое в письмо. Учтите, однако, что использование этой опции увеличит объём подписанного файла примерно на 30% (в сравнении с шифрованием с выключенной опцией, а не с исходным файлом); для "съёмной" ЭЦП это несущественно.

PGP зашифрует / подпишет файл и сохранит эту копию в том же каталоге, что и исходный файл (если при зашифровании была отмечена опция *Вычистить оригинал*, PGP уничтожит исходную копию с открытым текстом). В зависимости от характера содержимого зашифрованного файла он будет представлен одним из трех значков (таблица 2.5).

Таблица 2.5

	Файл, зашифрованный с опцией *Текстовый вывод* (шифртекст в ASCII-формате, asc-файл).
	Обычный зашифрованный файл (шифртекст в двоичном формате, pgp-файл).
	"Съёмная" цифровая подпись (sig-файл).

Чтобы расшифровать файл и/или сверить ЭЦП, достаточно дважды щёлкнуть в Проводнике на имя зашифрованного файла или на sig-файл. Если файл был зашифрован, появится окно *Введите пароль* со списком открытых ключей получателей. Если файл предназначен вам, программа попросит ввести ключевую фразу одного из ваших закрытых ключей. Если же вместо поля для ввода ключевой фразы в окошке указана ошибка *"Невозможно расшифровать данное сообщение ..."*, причина этого в том, что у вас на связке нет нужного для расшифрования закрытого ключа (он мог быть удалён, либо отправитель намеренно или случайно не зашифровал файл вашим открытым ключом). Введите ключевую фразу и нажмите *OK*. Программа расшифрует исходный файл и сохранит его в одном каталоге с шифртекстом.

Если файл был только подписан, вы сразу увидете окно отчёта PGPlog, содержащее некоторые сведения о цифровой подписи. Так, в столбце *Name* указано имя подписанного файла, в *Signer* – имя владельца ключа, которым была поставлена подпись, в *Validity* – степень достоверности ключа подписания, а в *Signed* – состояние ключа подписания (дезактивирован, аннулирован и т.п.) и самой ЭЦП: если подпись корректна, и файл был получен ровно в том виде, в как был подписан отправителем, здесь будет указана дата подписания (относительно вашего часового пояса), в иных случаях будет отмечено одно из следующих значений:

- *Bad signature* – подписанный файл был каким-то образом изменён (искажён). Причиной тому могло послужить не только злонамеренное вмешательство, но и более тривиальные вещи, например, плохое качество связи, повлекшее искажение информации в процессе передачи, случайное редактирование файла автором уже после подписания, изменение, внесённое почтовой программой отправителя или вашей. В любом случае, к подобного рода файлам следует относиться с большой осторожностью; желательно также в кратчайшие сроки выяснить причину происшедшего.
- *Unknown signing key* – это говорит о том, что на вашей связке ключей отсутствует тот, которым файл был подписан, и, следовательно, программа не может сверить подпись. В таких ситуациях PGP пытается самостоятельно связаться с сервером-депозитарием, чтобы найти соответствующий открытый ключ (если в настроках программы во вкладке *Серверы* включена опция *Удостоверение*).

- *Invalid key* – так PGP уведомит вас о том, что ключ отправителя файла есть на вашей связке, но не признан подлинным, и, соотственно, программа не может оценить целостность подписанной информации. Вам нужно проверить достоверность ключа и заверить его.

Учтите, что метка времени, стоящая в строке *Signed*, указывает время системного таймера отправителя. Отправителю эту метку крайне легко сфальсифицировать – достаточно перед подписанием перевести системные часы.

2.6 Уничтожение данных

Создавая и удаляя важные документы обычными средствами операционной системы, вы оставляете информацию, содержавшуюся в удалённых файлах, лежать в освободившемся пространстве жёсткого диска. Когда вы удаляете файл, помещая его в Корзину, он по сути просто перемещается из одного каталога в другой. Но и очистив Корзину, вы не сотрёте файл с диска окончательно, пока ОС не перезапишет высвобожденные сектора (это может случиться очень нескоро). Более того, многие программы и почти все текстовые процессоры создают в ходе работы множество резервных копий редактируемых документов. Хотя эти копии удаляются программой по завершении работы, содержавшаяся в них информация по-прежнему остаётся записанной на диске. В общем смысле, ценные файлы никогда не исчезают полностью, и при наличии должных инструментов могут быть восстановлены в первоначальный вид.

Если вам нужно безвозвратно стереть файл с лица жёсткого диска, используйте утилиту PGP Wipe. Она удаляет файл, многократно перезаписывая сектора диска, в которых он находился, случайными данными ("мусором") так, что его не удастся восстановить даже самыми совершенными коммерческими средствами.

Для очистки всего диска от остатков прежде удалённых файлов предназначена утилита PGP Freespace Wipe. Во-первых, она перезаписывает все свободные сектора диска, уничтожая фрагменты невостребованной информации, во-вторых, очищает частично занятые сектора диска в "хвостах" хранящихся на диске файлов (так называемый slack space).

Эти файловые системы сохраняют в своей специальной внутренней области резервные копии всех записей, вносимых ОС в файловую систему – ведут журнал изменений. Такой журнал представляет собой последовательное описание всех изменений, произведённых на диске, и служит цели надёжного восстановления ФС и содержимого диска после системных сбоев, однако, и усложняет задачу надёжного уничтожения данных. Стирание файла с помощью PGP Wipe не способно удалить все журнальные записи, вероятно сделанные файловой системой.

Обе утилиты можно вызвать из PGPtools с помощью соответствующих кнопок в правой части инструмента:  для PGP Wipe и  для Freespace Wipe. Кроме того, функция PGP Wipe доступна из контекстного меню в Проводнике Windows по нажатии правой кнопки на имени файла или папки, а также через интерфейс шифрования файлов.

Чтобы надёжно стереть файл с жёсткого диска:

1. Выделите в Проводнике файлы и/или папки, подлежащие уничтожению.
2. Нажмите правой кнопкой мыши на выделенные объекты, выберите в контекстном меню пункт *PGP > Wipe*.
3. В появившемся окне с перечнем удаляемых файлов / папок нажмите *Да*, чтобы подтвердить свой выбор, или *Нет*, чтобы отказаться от уничтожения этих файлов. Не забывайте, это последняя возможность передумать.

Ту же операцию можно проделать с помощью PGPtools: для этого нажмите кнопку *Wipe* (), укажите файлы, подлежащие уничтожению (или перетащите файлы на эту кнопку из Проводника), и подтвердите свой выбор, нажав *Да*.

Чтобы очистить свободное пространство диска от остатков удалённых файлов с помощью утилиты PGP Freespace Wipe:

1. В окне PGPtools нажмите кнопку *Freespace Wipe* (). Появится окно мастера с приветственным сообщением (рисунок 2.22).

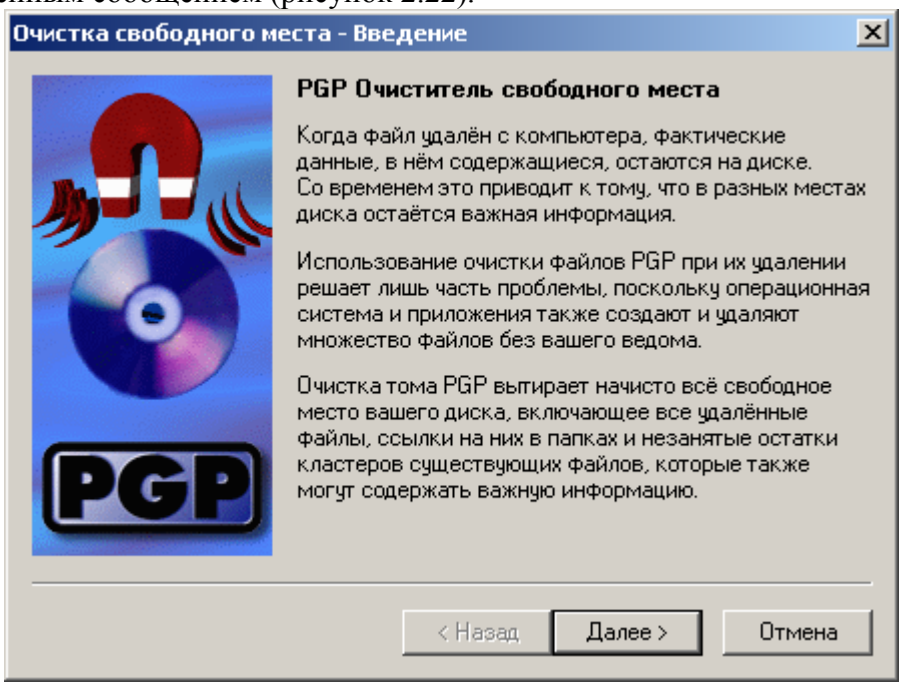

Рис. 2.22

2. Нажмите *Далее*.
3. Укажите параметры данного сеанса очистки (рисунок 2.23). В поле *Очистить диск* выберите диск, подлежащий очистке, и введите число проходов очистки (количество перезаписей свободного пространства диска).

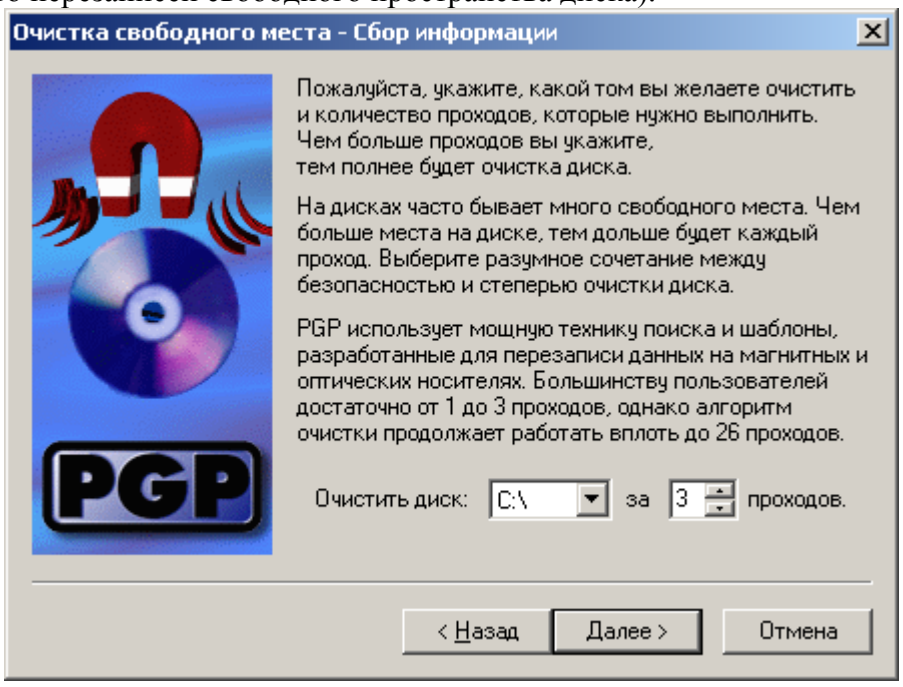

Рис. 2.23

4. Чтобы продолжить, нажмите *Далее*.

   На следующей странице мастера (рисунок 2.24) будут отображены технические сведения о выбранном для очистки разделе диска и график выполнения операции.

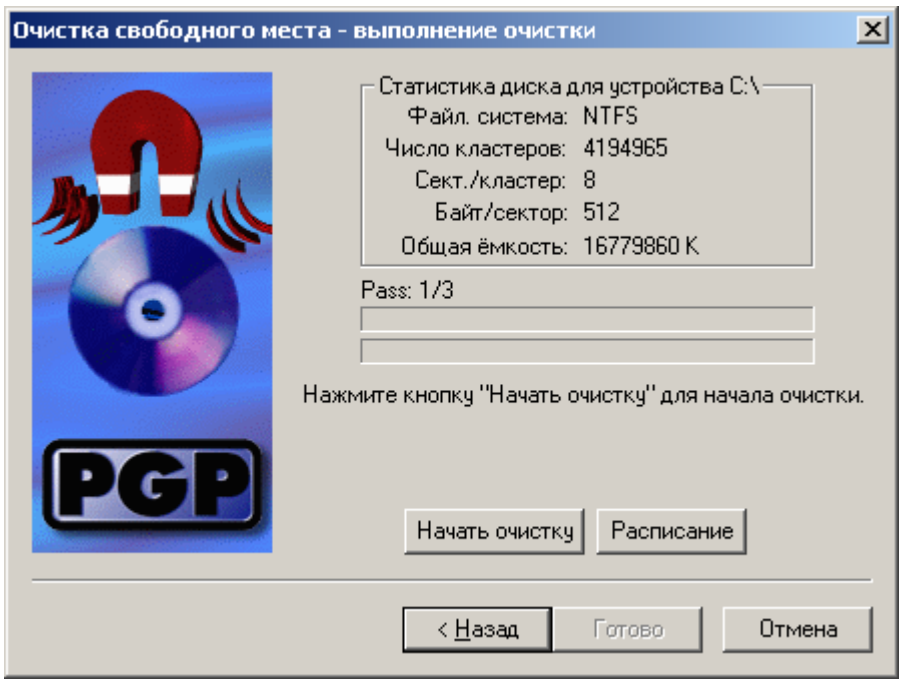

Рис. 2.24

5. Нажмите кнопку *Начать очистку*, чтобы приступить к очистке свободного пространства. Ход очистки можно прервать в любой момент, нажав кнопку *Отмена*. Однако это оставит на диске не перезаписанные фрагменты файлов.

   По окончании процесса очистки в нижней части окна появится сообщение *Поздравляем! Диск был очищен*.
6. Для завершения работы мастера нажмите *Готово* (рисунок 2.25).

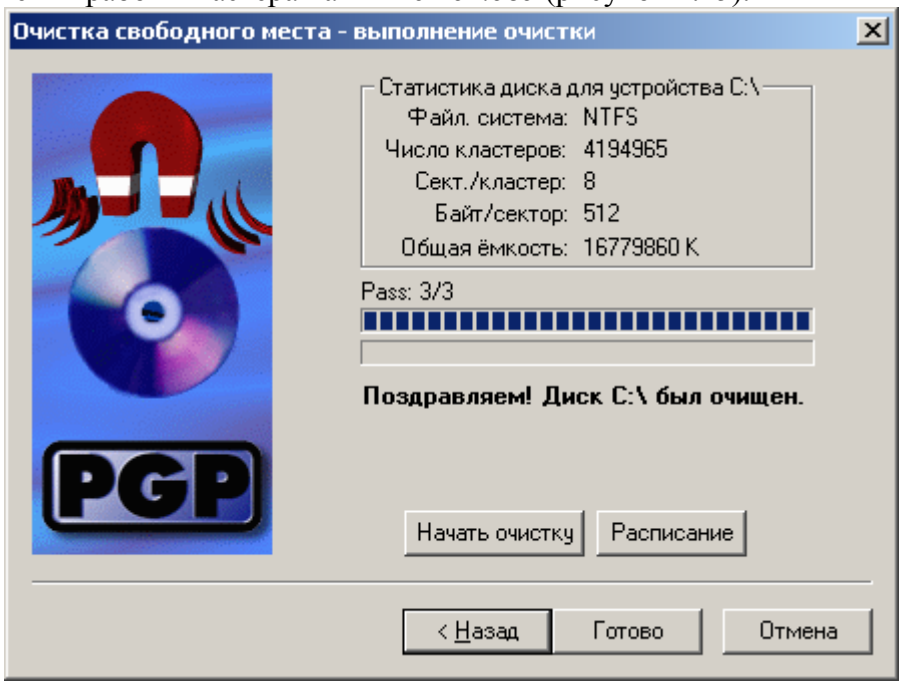

Рис. 2.25

С помощью утилит PGP Wipe и Freespace Wipe и Планировщика Windows можно создать ряд заданий для регулярной очистки свободного пространства тех или иных дисков или уничтожения содержимого определённых папок.

Чтобы запланировать регулярную очистку свободного пространства диска с помощью PGP Freespace Wipe:

1. В окне PGPtools нажмите кнопку *Freespace Wipe* ( ).

2. В окне мастера очистки нажмите *Далее*.
3. В поле *Очистить диск* выберите диск, подлежащий регулярной очистке, введите число проходов очистки
4. Чтобы продолжить, нажмите *Далее*.
5. На странице *Очистка свободного места – выполнение очистки* нажмите кнопку *Расписание*.
6. Если хотите запланировать регулярную очистку свободного пространства выбранного диска с указанными настройками, то в ответ на предупреждение нажмите *OK*.
   Работая в Windows NT вам потребуется ввести свой логин и пароль. Сделайте это в появившемся окошке.
7. В открывшемся окне Планировщика заданий Windows (рисунок 2.26) укажите периодичность выполнения операции (ежедневно, еженедельно, при простое и т.д.) и, если нужно, время начала выполнения очистки.

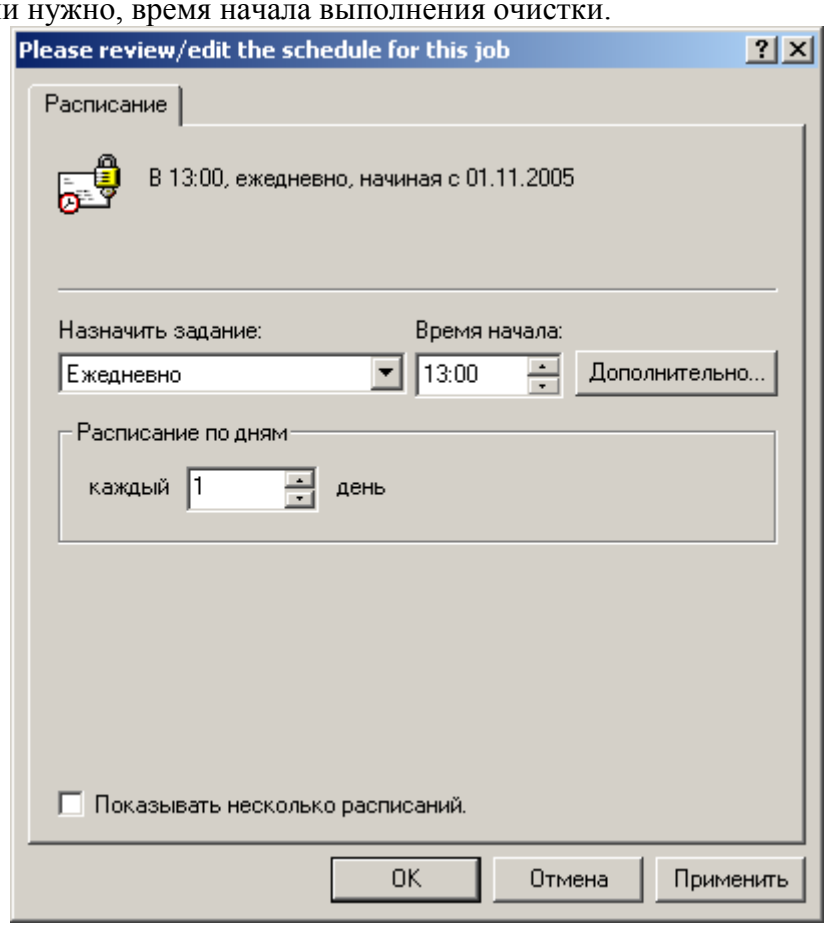

Рис. 2.26

8. В разделе *Дополнительных* настроек можете указать некоторые расширенные параметры выполнения задания, в частности, дату начала, дату окончания выполнения задания, график повторов и пр.
9. Закончив планирование задания нажмите *OK*.

Если в дальнейшем вам потребуется изменить порядок выполнения задания или отменить его, откройте Планировщик, находящийся в системном трее по соседству с PGPtray.

3 Задание на лабораторную работу

1. Изучите вкладки окна “Настройки PGP”.

2. Создайте с помощью менеджера PGPkeys ключи шифрования двух типов: RSA и DH/DSS.
3. Сохраните полученные ключи (открытые и секретные) в отдельный файл.
4. Назначьте ключ DH/DSS используемым по умолчанию.
5. Дезактивируйте ключевую пару RSA.
6. Активируйте ключевую пару RSA.
7. Аннулируйте ключевую пару RSA.
8. Изучите свойства ключевой пары DH/DSS:
   8.1. измените пароль;
   8.2. добавьте подключ;
   8.3. аннулируйте созданный подключ;
   8.4. добавьте фото-удостоверение.
9. Обменяйтесь с другим студентом открытыми ключами DH/DSS.
10. Импортируйте/вставьте полученный ключ на связку.
11. Установите подлинность полученного ключа с помощью его отпечатка.
12. Установите степень доверия к владельцу полученного ключа на максимальный уровень.
13. Зашифруйте произвольное сообщение/файл и обменяйтесь полученным результатом с другим студентом. Расшифруйте полученное сообщение.
14. Подпишите произвольное сообщение/файл и обменяйтесь полученным результатом с другим студентом. Проверьте достоверность источников полученного сообщения.
15. Подпишите и зашифруйте произвольное сообщение/файл и обменяйтесь полученным результатом с другим студентом. Расшифруйте полученное сообщение и проверьте достоверность его источников.
16. Уничтожьте все ненужные файлы, используя утилиту PGP Wipe.
17. Сделайте отчет по проделанной работе. Отчет должен содержать
    17.1. цель работы;
    17.2. описание выполненных действий по каждому пункту задания;
    17.3. открытые и секретные ключи, полученные в ходе выполнения работы;
    17.4. открытый ключ, полученный от другого студента;
    17.5. результаты шифрования/расшифрования, подписи/верификации сообщений/файлов;
    17.6. выводы по проделанной работе.

4 Контрольные вопросы

1. Что такое асимметричная криптографическая система? В чем ее преимущества перед симметричной системой? В чем недостатки?
2. Какие проблемы безопасности позволяет решить криптографическая защита информации? В чем они заключаются?
3. Что такое цифровая подпись? В чем ее отличие от рукописной подписи?
4. Какие задачи позволяет решить цифровая подпись?
5. Какие функции входят в состав PGP?
6. Какие типы ключей используются в PGP?
7. В чем различие между аннулированием и удалением ключа?
8. Что такое “отпечаток ключа” и для чего он используется?
9. Что такое “имплицитное доверие”?
10. Какую информацию может содержать сертификат открытого ключа PGP?
11. Каким образом в PGP производится надёжно удаление файлов с жёсткого диска?

5 Рекомендуемая литература

1. http://www.pgpru.com/
2. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 2001. – 376 с.
3. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии – М.: Гелиос АРВ, 2001. – 480 с., ил.
4. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: ТРИУМФ, 2002 – 816 с.