ЛАБОРАТОРНАЯ РАБОТА № 8

ИЗУЧЕНИЕ ПРОГРАММНЫХ ПРОДУКТОВ ЗАЩИТЫ ИНФОРМАЦИИ. ПРОГРАММА PGP

Цель работы: ознакомление с общими принципами построения и использования программных средств защиты информации, в частности с программой PGP (Pretty Good Privacy).

Для выполнения лабораторной работы при отсутствии на компьютере программы PGP ее необходимо инсталлировать.

Инсталляционный файл прилагается к описанию лабораторной работы PGPfreeware602i.

Выбрать для установки *только* следующие компоненты:

- PGP 6.0.2 Program Files;
- PGP 6.0.2 User's Manual;
- Unconfigured PGP 6.0.2 Client Install;
- PGP disk for Windows.

На вопрос программы установки о существовании ключей ответить «Нет», а на вопрос о необходимости перезагрузки системы — «Да».

Освоение средств программной системы PGP, предназначенных:

- для шифрования конфиденциальных ресурсов и разграничения доступа к ним;
- обеспечения целостности информационных ресурсов с помощью механизма электронной цифровой подписи;
- надежного уничтожения остаточной конфиденциальной информации;
- скрытия присутствия в компьютерной системе конфиденциальной информации с помощью виртуального диска.

Описание лабораторной работы. Основные задачи программы PGP — шифровать файлы и почтовые сообщения, заверять их электронными подписями, полностью уничтожать файлы на диске. Праграмма PGP предоставляет также следующие возможности:

- хранение открытых ключей на удаленном сервере;
- использование трех симметричных алгоритмов шифрования и двух асимметричных;
- четыре способа запуска: E-mail plugins, PGPtray, PGPtools, контекстное меню;
- разделение ключей;
- установка уровня валидности ключа и доверия владельцу ключа.

PGPkeys. Это программа, входящая в состав PGP 6.0 и обеспечивающая работу с ключами (рис. 2.7).

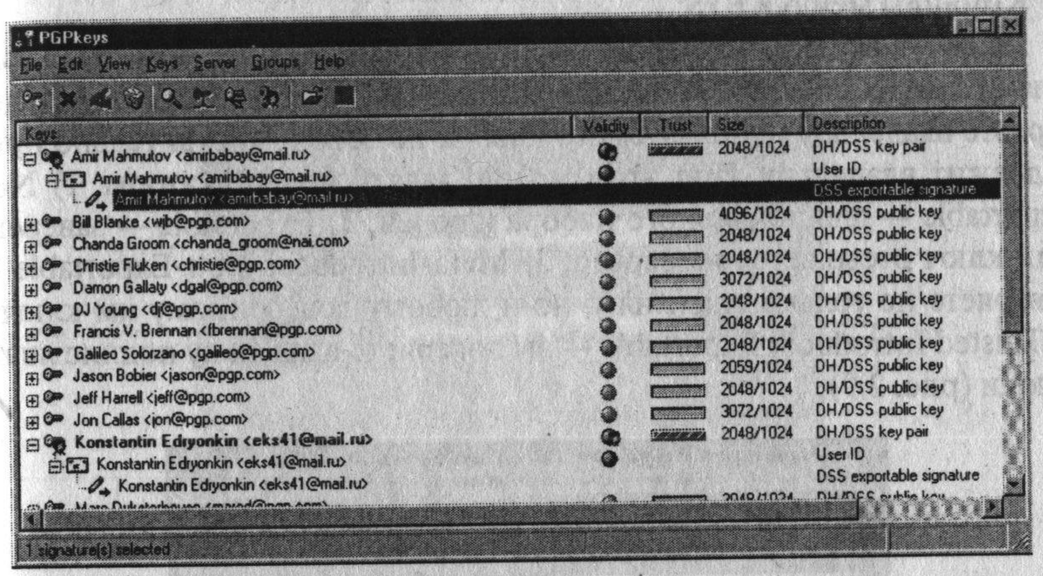

Рис. 2.7. Окно PGPkeys

В меню FILE содержатся две команды, одна из которых EXIT, другая — SEND KEY SHARES позволяет послать локальную копию разделенного ключа по сети.

Меню EDIT кроме обычных команд содержит команду PREFERENCES, которая служит для задания настроек программы (рис. 2.8).

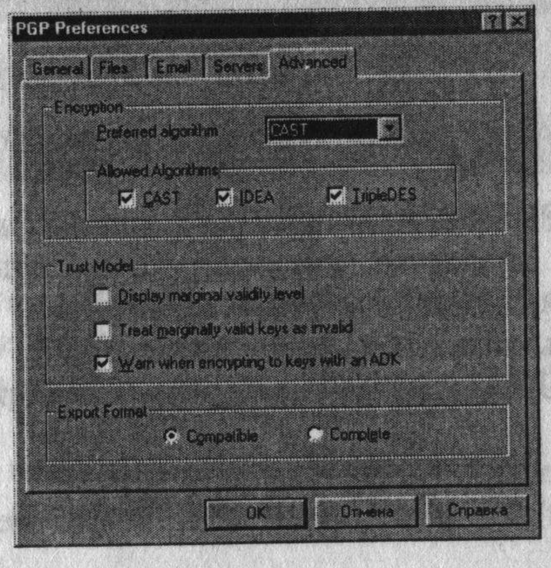

Рис. 2.8. Окно PGP Preferences

С помощью меню VIEW можно задать отображаемые на экране свойства ключей.

Команды меню KEYS:

SIGN — позволяет подписать своим закрытым ключом открытые ключи других пользователей. Тем самым вы можете показать, что доверяете владельцу используемого ключа, т.е. ключ действительно принадлежит владельцу. При этом можно задать модификаторы: 1) Non Exportable — для локального набора ключей; 2) Exportable — заверенный ключ отсылается на сервер; 3) Meta-introducer Non-Exportable — доверяете не только владельцу, но и любому доверенному им ключу; 4) Trusted Introducer Exportable — вы доверяете владельцу подписывать ключи (рис. 2.9);

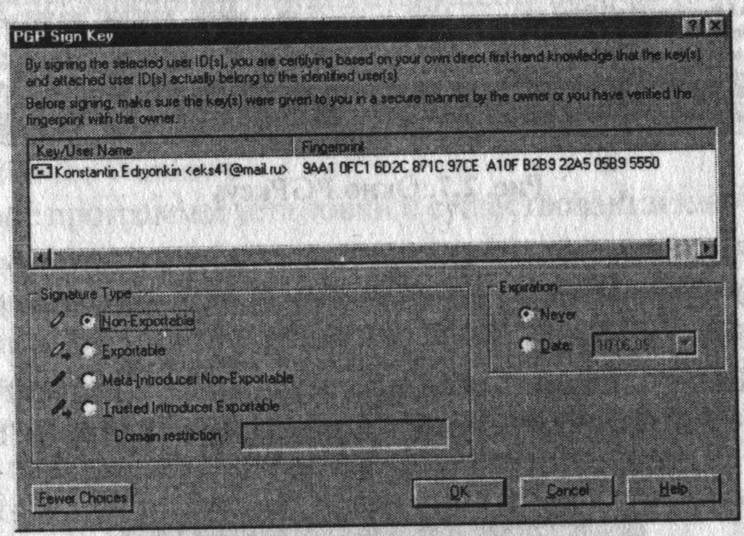

Рис. 2.9. Окно PGP Sign Key

SET AS DEFAULT KEY — назначить данный ключ ключом по умолчанию;

ADD NAME/PHOTO/REVOKER — позволяет добавить к свойствам ключа имя владельца, имеющего право объявить ваш ключ недействительным;

REVOKE — объявить ключ недействительным;

REVERIFY SIGNATURES — проверить сигнатуру (правильность) ключа;

NEW KEY — добавить новый ключ;

SHARE SPLIT — разделить ключ между несколькими владельцами;

IMPORT/EXPORT — импортировать/экспортировать ключ из/в текстовый файл;

KEY PROPERTIES — свойства (при этом можно задать степень доверия, валидность ключа) (рис. 2.10, 2.11);

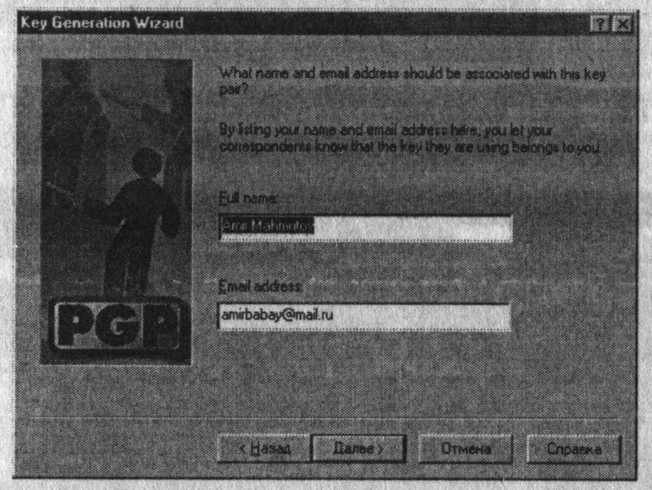

Рис. 2.10. Окно Key Generation Wizard

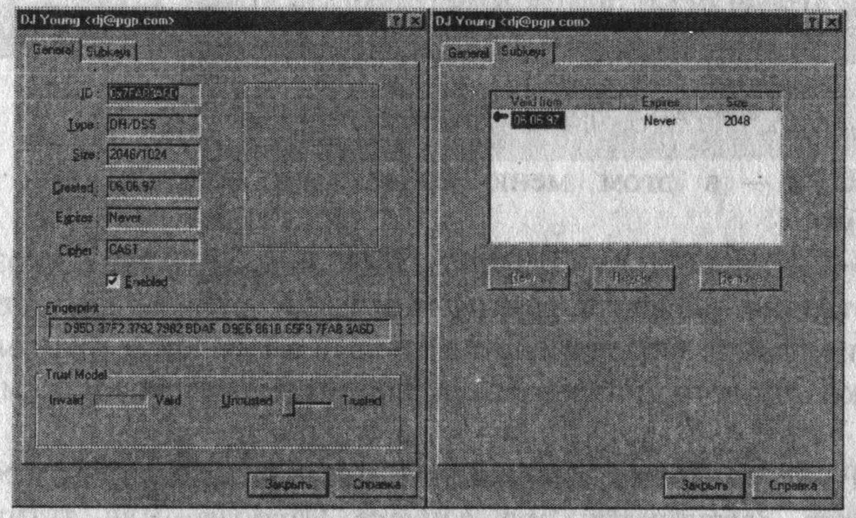

Рис. 2.11. Окна установки свойств ключа

SERVER — в этом меню сосредоточены команды для работы с удаленным сервером ключей;

SEND TO — позволяет послать ключи на выбираемый сервер (рис. 2.12);

SEARCH — с помощью этой команды можно попытаться найти на удаленном сервере ключ, задав соответствующие параметры (рис. 2.13);

UPDATE — позволяет обновить выбранный ключ, получив информацию с сервера;

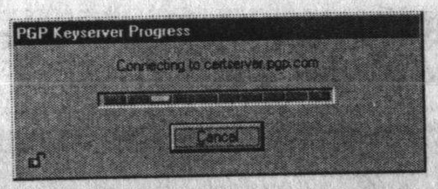

Рис. 2.12. Соединение с удаленным сервером

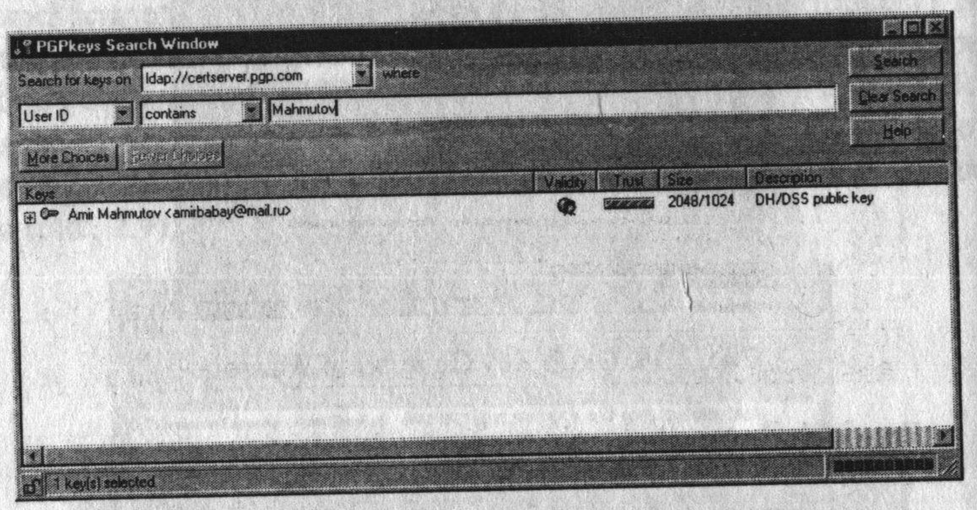

Рис. 2.13. Поиск ключа на удаленном сервере

GROUPS — в этом меню содержатся команды для работы с группами;

NEW GROUP, SHOW GROUPS, IMPORT GROUPS — позволяют соответственно добавить группу, показать группы, импортировать группы из файла. Объединение владельцев ключей в группы позволяет легко и просто шифровать сообщения для отправки всем членам группы;

HELP — стандартное для Windows, позволяет получить справку.

PGPtray. Загружается при запуске Windows. Для активизации меню достаточно нажать кнопкой мыши на значок рядом с часами (рис. 2.14).

В меню содержатся команды для выхода, запуска других компонентов PGP, редактирования буфера обмена, работы с буфером обмена (добавление ключа, расшифрование/проверка подписи, зашифрование и подпись, просто подпись и просто зашифрование).

Если в используемом почтовом клиенте нет встроенных команд PGP, то можно работать с помощью PGPtray. Например, для подписи письма достаточно скопировать его в буфер и исполнить команду Sign Clipboard, а затем вставить в тело письма уже подписанный текст (рис. 2.15).

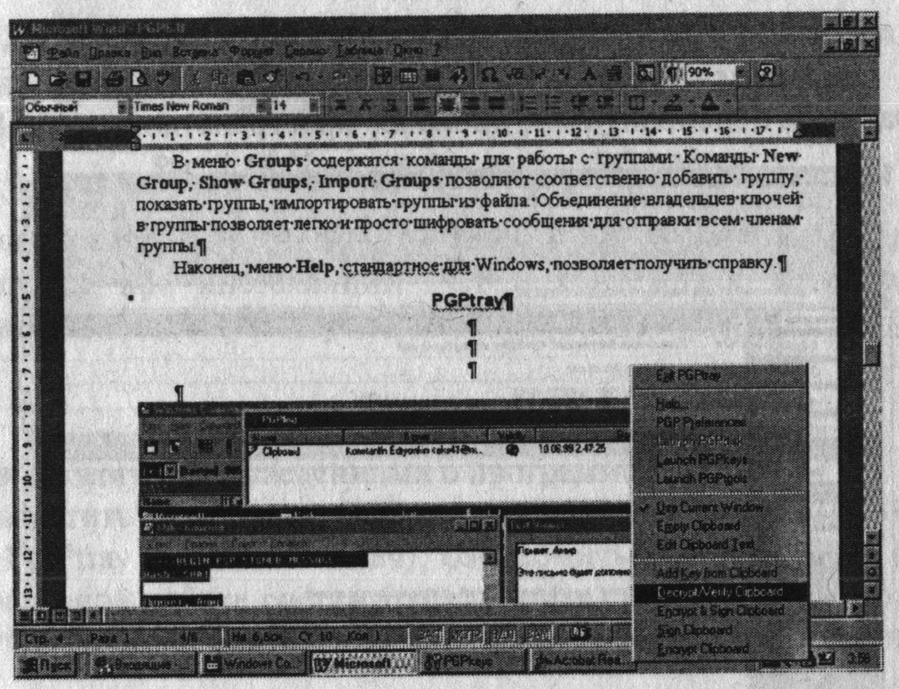

Рис. 2.14. Запуск PGP с использованием значка на панели задач

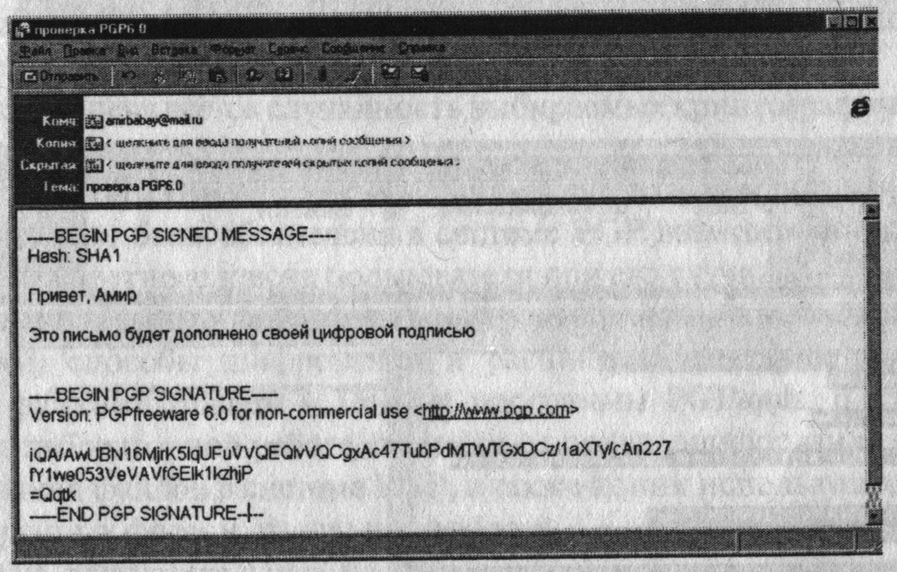

Рис. 2.15. Пример отправки письма с цифровой подписью

Аналогично получателю письма достаточно скопировать полученное письмо в буфер обмена и выбрать команду DECRIPT/VERIFY CLIPBOARD. Естественно, в коллекции ключей должен быть открытый ключ владельца, подписавшего письмо (рис. 2.16, 2.17).

PGPtools. Этот компонент программы PGP представляет собой небольшую панель с кнопками, позволяющими выполнить нужное дей-

ствие: открыть PGPkeys, зашифровать, подписать, зашифровать и подписать одновременно, расшифровать/проверить подпись, затереть файл, затереть неиспользуемое дисковое пространство (рис. 2.18).

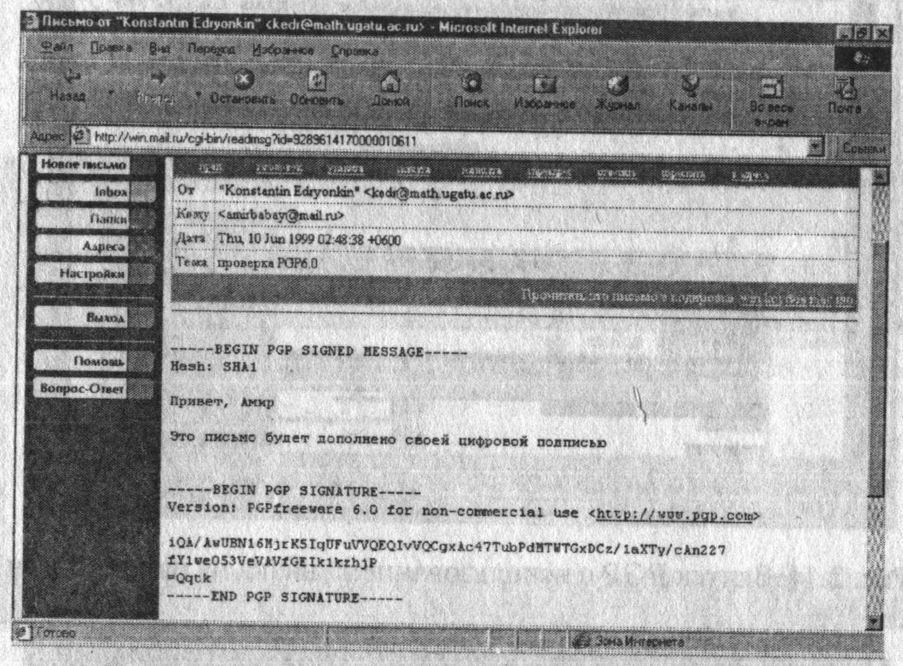

Рис. 2.16. Пример получения письма с цифровой подписью

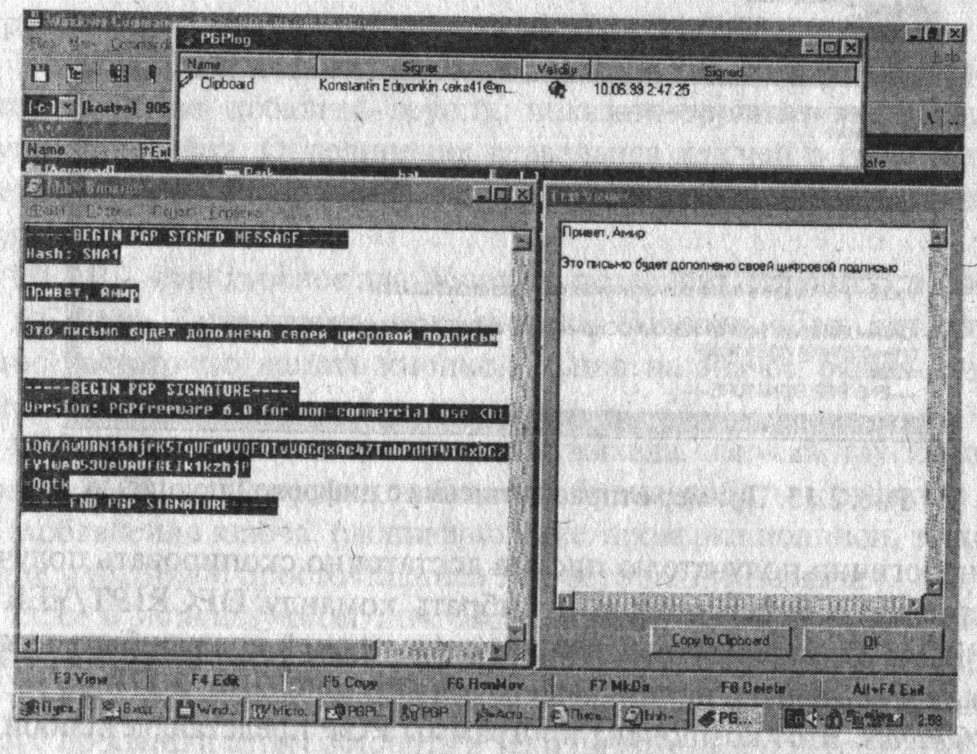

Рис. 2.17. Результаты проверки подписи

Рис. 2.18. Компоненты панели PGPtools

Альтернативой программы **PGPtools** могут служить команды, добавляющиеся при инсталляции PGP в контекстное меню работы с файлами и меню ФАЙЛ Проводника Windows.

Задание

1. Ознакомиться со сведениями о программе PGP.

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

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

- как обеспечивается случайность выбираемых криптографических ключей в системе PGP;
- как и где хранится секретный ключ пользователя в системе PGP;
- как может быть обеспечена в системе PGP возможность восстановления секретного ключа пользователя при его случайной утрате?

4. Изучить (на примере обычных текстовых файлов и файлов изображений) способы шифрования и расшифрования файлов с помощью функций Encrypt и Decrypt программы **PGPtools**. Включить в отчет о лабораторной работе сведения о порядке шифрования и расшифрования файлов в системе PGP, а также копии используемых при этом экранных форм и ответы на вопросы:

- какие дополнительные параметры шифрования могут быть использованы, в чем их смысл и возможное применение (обязательно проверить на примере и результаты проверки отразить в отчете);
- как генерируется, как и где хранится ключ симметричного шифрования файла в системе PGP;
- как можно обеспечить доступ к зашифрованному файлу со стороны других пользователей;
- изменяется ли и как размер файла после его шифрования (привести конкретные примеры для разных типов файлов)?

5. Изучить (на примере документов из своей папки) способы получения и проверки электронной цифровой подписи под файлами с помощью функций Sign и Verify программы **PGPtools**. Включить в отчет *сведения о порядке обеспечения аутентичности и целостности электронных документов в системе* PGP, а также копии используемых при этом экранных форм и ответы на вопросы:

- какие дополнительные параметры получения электронной цифровой подписи могут быть использованы, в чем их смысл и возможное применение (обязательно проверить на примере и результаты проверки отразить в отчете);
- какова реакция программы на нарушение целостности подписанного документа (обязательно проверить на примере и результаты проверки отразить в отчете)?

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

7. Изучить способы надежного удаления файлов с конфиденциальной информацией с помощью функции Wipe программы **PGPtools**. Включить в отчет *сведения о порядке уничтожения конфиденциальных электронных документов в системе* PGP, а также копии используемых при этом экранных форм.

8. Изучить способы надежного уничтожения остаточной информации, которая может содержать конфиденциальные сведения, с помощью функции Freespace Wipe программы PGPtools. Включить в отчет *сведения о назначении и порядке использования этой функции программы*, копии используемых в ней экранных форм и ответы на вопросы:

- как достигается надежное уничтожение остаточной конфиденциальной информации в системе PGP;
- является ли подобный метод уничтожения абсолютно надежным и, если нет, как может быть обеспечено абсолютно надежное уничтожение остаточной информации?

9. Изучить способы быстрого выполнения функций системы PGP с помощью программы **PGPtray**, ярлык которой размещен в правой части панели задач. Включить в отчет *сведения о назначении и порядке использования этой программы*, а также копии используемых экранных форм.

10. Изучить способы управления настройками системы PGP при ее использовании в организациях с помощью программы **PGPadmin** (пройти все шаги диалога с мастером вплоть до последнего, на котором вместо кнопки «Save» нажать кнопку «Отмена»). Включить в отчет *сведения о возможностях и порядке администрирования системы* PGP, копии используемых при этом экранных форм и ответы на вопросы:

- какие функции по управлению шифрованием и обеспечением целостности информационных ресурсов предоставляет администратору программа **PGPadmin**;
- какие функции по управлению криптографическими ключами пользователей PGP предоставляет администратору программа **PGPadmin**;
- какие возможности предоставляет программа **PGPadmin** по управлению доступными для пользователей функциями программы PGP и где сохраняется подобная информация?

11. Включить в отчет о лабораторной работе ответы на контрольные вопросы, выбранные в соответствии с номером варианта, указанным преподавателем (табл. 2.9).

Таблица 2.9

Номер варианта	Контрольные вопросы
1, 5, 7	Как выбрать длину криптографического ключа в системе PGP?
2, 4, 6, 8	В чем достоинства и недостатки криптографических методов защиты информации?
11, 13, 15, 17, 19	Какие компьютерные системы называются безопасными?
12, 14, 16	В чем заключаются основные требования к защищенности компьютерных систем?
20, 22, 24, 30	Для выполнения каких требований к защищенности компьютерных систем могут применяться криптографические методы защиты?
21, 23, 25	Насколько, на ваш взгляд, надежны методы криптографической защиты информации, используемые в программе PGP?
3, 9, 18, 28	Какими основными функциями защиты информации обладает программа PGP?
10, 26, 27, 29	Какой принцип лежит в основе функции надежного уничтожения остаточной конфиденциальной информации программы PGP?