ЗАЩИТА КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

♦ ИЗДАТЕЛЬСТВО ТГТУ ♦

Министерство образования и науки Российской Федерации

Тамбовский государственный технический университет

ЗАЩИТА КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Методические указания по выполнению лабораторных работ
для студентов дневного и заочного отделений,
обучающихся по специальности 021100

Тамбов
♦ Издательство ТГТУ ♦
2004

УДК [34:681.31]
ББК Х.с51я73-5
З-40

Утверждено Редакционно-издательским советом университета

Р е ц е н з е н т

Кандидат технических наук, доцент
М.Ю. Серегин

З-40 Защита компьютерной информации: Метод. указ. / Сост.: А.В. Терехов, А.В. Селезнев. Тамбов: Изд-во Тамб. гос. техн. ун-та, 2004. 16 с.

Представлены методические указания для выполнения лабораторных работ по дисциплине "Защита компьютерной информации".

Предназначены для студентов дневного и заочного отделений, обучающихся по специальности 021100 "Юриспруденция".

УДК [34:681.31]
ББК Х.с51я73-5

Учебное издание

ЗАЩИТА КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Методические указания

С о с т а в и т е л и:

ТЕРЕХОВ Алексей Васильевич
СЕЛЕЗНЕВ Андрей Владимирович

Редактор Т. М. Ф е д ч е н к о
Инженер по компьютерному макетированию М. Н. Р ы ж к о в а

Подписано к печати 15.10.2004
Формат 60 × 84 / 16. Бумага газетная. Печать офсетная
Гарнитура Times New Roman. Объем: 0,93 усл. печ. л.; 0,91 уч.-изд. л.
Тираж 200 экз. С. 714

Издательско-полиграфический центр
Тамбовского государственного технического университета
392000, Тамбов, Советская, 106, к. 14

ИЗУЧЕНИЕ ПРИЕМОВ РАБОТЫ С СОВРЕМЕННЫМИ АНТИВИРУСНЫМИ ПРОГРАММАМИ

Цель работы. Изучение приемов работы с современными антивирусными программами (на примере программы AVP Лаборатории Касперского).

Задание. Ознакомиться с приемами работы с AVP. Выполнить обновление антивирусных баз AVP. Выполнить настройки программы Центр Управления на еженедельный запуск AVP сканера в 12 часов 20 минут, а AVP Монитора постоянно. Выполнить проверку диска C:.

Общие сведения

Компьютерным вирусом называется программа (некоторая совокупность выполняемого кода/инструкций), которая способна создавать свои копии (не обязательно полностью совпадающие с оригиналом) и внедрять их в различные объекты/ресурсы компьютерных систем, сетей и т.д. без ведома пользователя. При этом копии сохраняют способность дальнейшего распространения.

Вирусы можно разделить на классы по следующим признакам:

- среде обитания вируса (сетевые файловые, загрузочные);
- способу заражения среды обитания (резидентный и нерезидентный);
- деструктивным возможностям (безвредные, неопасные, опасные и очень опасные);
- особенностям алгоритма вируса (вирусы-"черви", "стелс"-вирусы, "макро-вирусы", "паразитические" и др.)

Хотя вирусные атаки случаются не очень часто, общее число вирусов слишком велико, а ущерб от "хулиганских" действий вируса в системе может оказаться значительным. Существуют вирусы, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти, привести к серьезным сбоям в работе компьютера. В результате этих действий Вы можете навсегда потерять данные, необходимые для работы и понести существенный моральный и материальный ущерб. "Эпидемия" компьютерного вируса в фирме (неважно – большой или маленькой) может полностью дестабилизировать ее работу. При этом может произойти сбой в работе как отдельных компьютеров, так и компьютерной сети в целом, что повлечет за собой потерю информации, необходимой для нормальной работы и потерю времени, которое будет затрачено на восстановление данных и приведением компьютеров и/или сети в рабочее состояние.

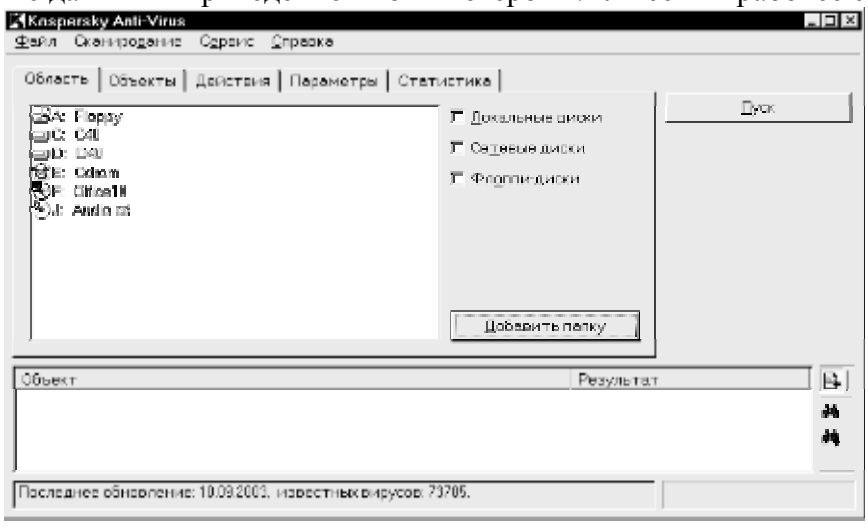

Рис. 1

AVP Сканер (рис. 1) представляет собой полностью 32 разрядное приложение, оптимизированное для работы в среде Microsoft Windows 95/98/NT/2000, и предназначенное для поиска и удаления вирусов.

AVP Сканер имеет удобный пользовательский интерфейс, большое количество настроек, выбираемых пользователем, а также одну из самых больших в мире антивирусных баз, что гарантирует надежную защиту от огромного числа самых разнообразных вирусов.

В ходе работы программа сканирует: оперативную память, файлы (включая архивные и упакованные), системные сектора, загрузочный сектор (Boot-сектор) и таблицу разбиения диска (Partition Table).

Используя команду Добавить папку, можно указывать объекты для сканирования на гибких, локальных, сетевых и CD-ROM дисках.

В повседневной работе, особенно при работе с Интернет, удобно использовать "AVP Monitor" – резидентный модуль, находящийся постоянно в оперативной памяти компьютера и отслеживающий все файловые операции в системе. Позволяет обнаружить и удалить вирус до момента реального заражения системы в целом.

Для надежной работы программы AVP необходимо своевременно обновлять антивирусную базу. Способ обновления (через Интернет или из локальной папки) выбирается командой Сервис/Автоматическое управление (см. рис. 2).

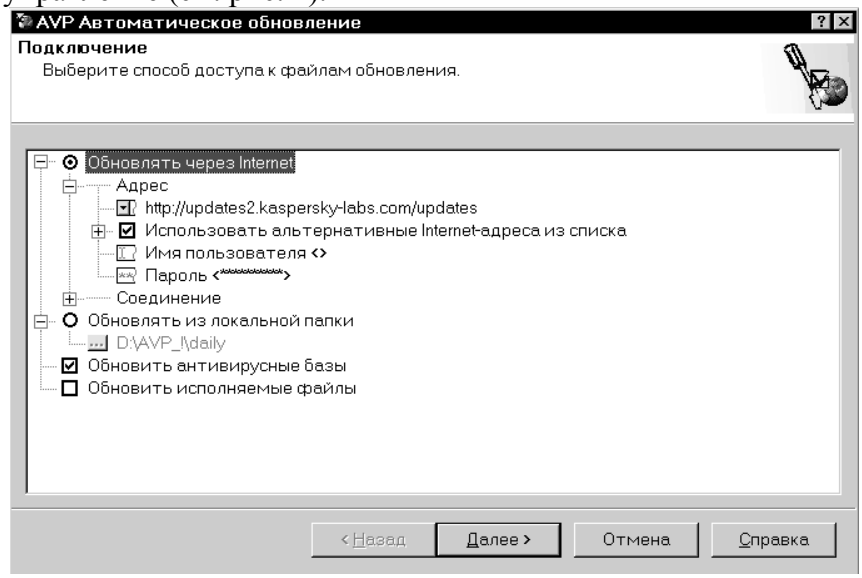

Рис. 2

Программа AVP Центр Управления, входящая в состав пакета антивирусных программ Антивирус Касперского, выполняет функции управляющей оболочки. Она предназначена для организации установки и обновления компонент пакета, формирования расписания для автоматического запуска задач, а также контроля результатов их выполнения.

Программа AVP имеет удобный пользовательский интерфейс и удобную систему помощи (команда Справка/Содержание).

Порядок выполнения работы

1. Загрузить программу AVP32 (программу можно загрузить, используя соответствующий ярлык на рабочем столе, либо через кнопку Пуск/Программы/Kaspersky AntiVirus/AVP32).
2. Ознакомиться с приемами работы с AVP, используя меню Справка/Содержание/Работа с AVP.
3. Ознакомиться с назначением и способами настройки и эксплуатации программы Центр Управления (Пуск/Программы/Kaspersky AntiVirus/avpcc).
4. Посетите WEB страницу http://www.kasperskylabs.ru/. Ознакомьтесь с новостями Лаборатории Касперского.
5. Выполнить обновление антивирусных баз AVP (меню Сервис/Автоматическое обновление/Обновление через Интернет (или по указанию преподавателя из локальной папки).
6. Задайте настройки программы Центр Управления на еженедельный запуск AVP сканера в 9 часов 00 минут, а AVP Монитора постоянно.
7. Выполнить проверку диска C:, установив в качестве объектов для проверки следующие: память, секторы, файлы, упакованные объекты, архивы, почтовые базы данных, почтовые текстовые форматы, программы по формату. Задать лечение инфицированных объектов без запроса, а сведения о подозрительных объектах копировать в папку "Suspicious".
8. Активизировать закладку "Статистика" для отслеживания процесса сканирования с заданными параметрами проверки.

9. О результатах проведенной проверки доложить преподавателю.

Контрольные вопросы

1. Какие действия должны быть предприняты при появление сообщения "Лечение не возможно"?
2. Что означает проверка программ по формату?
3. Что означает проверка программ по расширению?
4. Как задать проверку файлов по маске?
5. Каковы Ваши действия, если программа выдала сообщение о подозрении на заражение какого-либо объекта вирусом?
6. Назначение программы подготовки дисков аварийного восстановления в программе AVP?
7. Каково назначение AVP Монитор (AVPm)?

Лабораторная работа № 2

ОСНОВЫ БЕЗОПАСНОЙ РАБОТЫ ПРИ ПОЛУЧЕНИИ ИНФОРМАЦИИ ИЗ СЕТИ ИНТЕРНЕТ

Цель работы. Освоить основы безопасной работы при получении информации из сети Интернет.

Задание. Ознакомиться с основными положениями информационной безопасности при работе с Интернет.

Научиться выполнять первичные настройки броузера, связанные с безопасностью работы в Интернете на примере программы Microsoft Internet Explorer 5.0.

Общие сведения

Средства защиты в Internet Explorer 5.0 от потенциально опасного содержимого Web-документов предоставляет вкладка Безопасность. Она позволяет указать Web-узлы, взаимодействие с которыми следует считать опасным, и запретить прием с них информации, которая может оказаться разрушительной.

Для ограничения доступа к узлам с неприемлемым содержанием, а также для управления использованием электронных сертификатов служат элементы управления вкладки Содержание.

Прочие настройки сосредоточены на вкладке Дополнительно. Они позволяют:

- соблюдать конфиденциальность работы с помощью средств шифрования, использования электронных сертификатов и своевременного удаления временных файлов;
- контролировать использование средств языка Java;
- управлять отображением мультимедийных объектов;
- использовать дополнительные настройки оформления;
- управлять режимом поиска Web-страниц, содержащих нужную информацию.

Порядок выполнения работы

1 Запустите программу Internet Explorer (Пуск / Программы / Internet Explorer)

2 Дайте команду Сервис / Свойства обозревателя — откроется диалоговое окно Свойства обозревателя. В этом окне выберите вкладку Дополнительно (рис. 3).

3 На вкладке Дополнительно сбросьте флажок Задействовать профиль – тогда программа не будет передавать сведения о личности пользователя по запросам удаленных серверов.

4 Там же сбросьте флажок Автоматически проверять обновления Internet Explorer, чтобы программа самостоятельно не обращалась к "своему" серверу без ведома пользователя.

5 Сбросьте флажок Использовать автозаполнение для Web-адресов. Функция автозаполнения позволяет посторонним лицам выяснять, куда обращался владелец системы.

6 Сбросьте флажок Разрешить счетчик попаданий на страницы. Этот счетчик связан с ведением на компьютере пользователя "журнала посещений", подконтрольного удаленным серверам, что далеко выходит за рамки стандартного протокола HTTP.

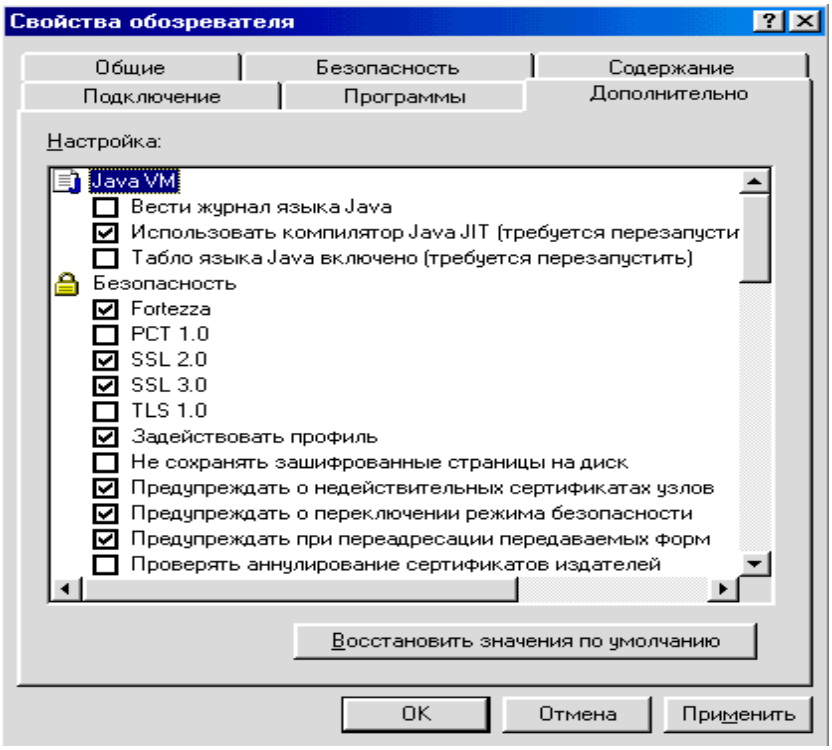

Рис. 3 Настройка системы безопасности броузера Internet Explorer

7 В разделе Поиск из панели адресов включите переключатель Не производить поиск из панели адресов.

8 Откройте вкладку Безопасность диалогового окна Свойства обозревателя.

9 Выберите зону Интернет и задайте настройку уровня безопасности для этой зоны с помощью кнопки Другой. Откроется диалоговое окно Правила безопасности.

10 В категории Java установите переключатель Отключить язык Java.

11 В категории Сценарии отключите все функции, установив переключатели Отключить.

12 В категории Файлы cookie установите переключатели Предлагать – тогда вы наглядно будете видеть, какие Web-узлы предлагают маркировать ваш компьютер своими метками.

13 Во всех разделах категории Элементы ActiveX и модули подключения включите переключатели Отключить.

14 Откройте вкладку Содержание диалогового окна Свойства обозревателя.

15 Щелкните на кнопке Автозаполнение – откроется диалоговое окно Настройка автозаполнения. В этом диалоговом окне отключите все функции автозаполнения. Очистите журнал автозаполнения с помощью кнопок Очистить формы и Очистить пароли. Закройте окно щелчком на кнопке ОК.

16 На вкладке Содержание диалогового окна Свойства обозревателя используйте командную кнопку Профиль – откроется диалоговое окно, в котором представлены персональные сведения о пользователе, известные программе. Проверьте эти сведения и убедитесь, что в них не содержится ничего лишнего. Подходите к ним как к сведениям, сообщаемым кому попало.

17 Закройте открытые диалоговые окна. Завершите работу с программой Internet Explorer.

В ходе работы Вы научились выполнять первичные настройки броузера, связанные с безопасностью работы в Интернете, обратив особое внимание на то, что они выполняются не только на вкладке Безопасность, но и на вкладках Дополнительно и Содержание.

Контрольные вопросы

1 Что такое должный уровень безопасности?

2 В какой мере стандартные сетевые средства, которые устанавливаются вместе с операционной системой Windows 98 обеспечивают должный уровень безопасности?

3 Какие основные виды нарушения режима сетевой безопасности Вы знаете?

4 Для чего предназначены маркеры cookie? Каков правовой режим маркеров cookie?

5 Зачем создатели Web-страниц встраивают в них активные объекты и активные сценарии? Какую угрозу они могут нести?

6 Что может послужить источником для сбора сведений о клиентах Сети?

7 Как обеспечивается защита от основных видов нарушения режима сетевой безопасности?

8 Как обычно обеспечивается режим безопасности на государственных предприятиях и в коммерческих структурах?

Лабораторная работа № 3

СОЗДАНИЕ КЛЮЧЕЙ В СИСТЕМЕ PGP

Цель работы. Ознакомление с программным средством создания ЭЦП – электронной цифровой подписи (на примере программы Pretty Good Privacy (PGP)) и создание ключей в системе PGP.

Задание. Создать пару ключей, используемых для несимметричного шифрования в системе PGP.

Порядок выполнения работы

Установленная на компьютере программа PGP, автоматически стартует при запуске операционной системы.

1 Щелкните на значке PGPtray на панели индикации правой кнопкой мыши и выберите в контекстном меню пункт PGPkeys. Откроется окно служебного средства PGPkeys.

2 Щелкните на кнопке Generate new keypair (Сгенерировать новую пару ключей). Произойдет запуск Мастера генерации ключей (Key Generation Wizard). Щелкните на кнопке Далее.

3 Введите свое полное имя в поле Full name (Полное имя) и свой адрес электронной почты в поле Email address (Адрес электронной почты). Открытые ключи, не содержащие полной и точной информации, не воспринимаются всерьез. Щелкните на кнопке Далее.

4 Установите переключатель Diffie-Hellman/DSS. Это более современный алгоритм генерации пары ключей. Щелкните на кнопке Далее.

5 Установите переключатель 2048 bits (2048 бит), определяющий длину ключа. Щелкните на кнопке Далее. (По надежности ключ такой длины соответствует примерно 128-битному ключу для симметричного шифрования).

6 В данном случае установите переключатель Key pair never expires (Пара ключей действует бессрочно). На практике рекомендуется задавать ограниченный срок действия ключей. Щелкните на кнопке Далее.

7 Дважды введите произвольную парольную фразу (Passphrase) в соответствующие поля. Так как в данном случае реальная секретность не существенна, можно сбросить флажок Hide Typing (Скрыть ввод), чтобы вводимый текст отображался на экране. Рекомендуется, чтобы парольная фраза легко запоминалась, но при этом содержала пробелы, буквы разного регистра, цифры, специальные символы. Качество (трудность подбора) ключевой фразы отображается с помощью индикатора Passphrase Quality (Качество ключевой фразы). После того как парольная фраза введена дважды, щелкните на кнопке Далее.

8 Просмотрите за процессом генерации пары ключей, что может занять до нескольких минут. После появления сообщения Complete (Готово) щелкните на кнопке Далее. Затем может потребоваться еще несколько щелчков на кнопках Далее и, в конце, Готово, чтобы завершить создание ключей (публикацию ключа на сервере выполнять не следует).

9 Посмотрите, как отображается только что созданный ключ в списке Keys (Ключи). Убедитесь что этот ключ автоматически подписывается его создателем, который, как предполагается, абсолютно доверяет самому себе.

10 Щелкните на ключе правой кнопкой мыши и выберите в контекстном меню пункт Key Properties (Свойства ключа). Ознакомьтесь со свойствами ключа, в том числе с «отпечатком» (fingerprint), предназначенным для подтверждения правильности ключа, например, по телефону. Убедитесь, что установлен флажок Implicit Trust (Полное доверие), указывающий, что вы доверяете владельцу данного ключа, т.е. самому себе.

Вы научились создавать пару ключей, используемых для несимметричного шифрования в системе PGP, а также познакомились с механизмом доверия, используемым для подтверждения подлинности ключей.

Контрольные вопросы

1 Для чего используется и каковы особенности ЭЦП – электронной цифровой подписи?
2 Каково правовое обеспечение ЭЦП?
3 Какие программы используются для создания ЭЦП в России и за рубежом?

Лабораторная работа № 4

ПЕРЕДАЧА ОТКРЫТОГО КЛЮЧА PGP КОРРЕСПОНДЕНТАМ

Цель работы. Научиться передавать открытые ключи системы PGP своим корреспондентам, а также получать ключи для расшифровки поступающих сообщений.

Задание. Подготовить открытые ключи системы PGP для передачи своим корреспондентам, а также ознакомиться с порядком получения ключей для расшифровки поступающих сообщений.

Порядок выполнения работы

1 Щелкните на значке PGPtray на панели индикации правой кнопкой мыши и выберите в контекстном меню пункт PGPkeys. Откроется окно служебного средства PGPkeys.
2 Выберите в списке ключ, который планируется передать корреспонденту, и дайте команду Edit / Copy (Правка / Копировать).
3 Запустите используемую по умолчанию программу электронной почты. Далее мы будем предполагать, что это программа Outlook Express (Пуск / Программы / Outlook Express).
4 Щелкните на кнопке Создать сообщение. В окне создания нового сообщения введите условный адрес корреспондента, тему сообщения (например, Мой открытый ключ) и произвольный текст сообщения, объясняющий его назначение.
5 Поместите курсор в конец сообщения и щелкните на кнопке Вставить на панели инструментов. Убедитесь, что в текст сообщения был вставлен символьный блок, описывающий открытый ключ. Сохраните сообщение (отправлять его не обязательно).
6 Проверьте, можно ли перенести ключ в сообщение электронной почты методом перетаскивания.
7 Теперь предположим, что созданное сообщение на самом деле было получено по электронной почте. Порядок действий в этом случае очень похож на тот, который использовался для отправки ключа.
8 Выделите текст ключа, включая специальные строки, описывающие его начало и конец.
9 Скопируйте ключ в буфер обмена с помощью комбинации клавиш CTRL+C.
10 Переключитесь на программу PGPkeys.
11 Нажмите комбинацию клавиш CTRL+V. В открывшемся диалоговом окне щелкните на кнопке Select All (Выбрать все), а затем на кнопке Import (Импортировать).
12 В самом окне PGPkeys вы после этого никаких изменений не обнаружите, так как соответствующий ключ уже хранится на данном компьютере.
13 На самом деле, пересылать ключи по электронной почте не вполне корректно, так как в таком случае корреспондент имеет естественное право на сомнение: действительно ли ключ поступил от вас. Ключ можно сохранить в файле и передать корреспонденту лично, при встрече.
14 Чтобы экспортировать ключ в файл, выберите его и дайте команду Keys / Export (Ключи / Экспортировать).
15 Выберите каталог и укажите имя файла. Щелкните на кнопке Сохранить, чтобы записать ключ в текстовый файл.
16 Самостоятельно выполните импорт ключа, сохраненного в файле, как минимум двумя разными способами.

Вы научились передавать открытые ключи системы PGP своим корреспондентам, а также получать ключи для расшифровки поступающих сообщений. Вы узнали, что ключ может передаваться по электронной почте или, что предпочтительнее, при личной встрече.

Контрольные вопросы

1 Как предпочтительнее передавать открытые ключи PGP своим корреспондентам?
2 Что такое компрометация ЭЦП?
3 Что влияет на криптостойкость ЭЦП?

Лабораторная работа № 5

ПЕРЕДАЧА ЗАЩИЩЕННЫХ И ПОДПИСАННЫХ СООБЩЕНИЙ С ПОМОЩЬЮ СИСТЕМЫ PGP

Цель работы. Научиться отправлять по электронной почте сообщения, снабженные электронной цифровой подписью, а также зашифрованные сообщения.

Задание. Создать сообщение, подписать и зашифровать его с помощью PGP и выполнить отправку сообщения с помощью программы Outlook Express.

Порядок выполнения работы

1 Запустите программу Outlook Express (Пуск / Программы / Outlook Express).
2 Щелкните на кнопке Создать сообщение. В окне создания нового сообщения введите адрес электронной почты, использованный при создании пары ключей, в качестве адреса отправителя, а также произвольные тему и текст сообщения.
3 Обратите внимание, что на панели инструментов в окне создания сообщения имеются кнопки Encrypt (PGP) (Зашифровать) и Sign (PGP) (Подписать), действующие в качестве переключателя. Щелкните на кнопке Sign (PGP) (Подписать), чтобы она была включена. Убедитесь, что шифрование отключено.
4 Щелкните на кнопке Отправить. Подключения к Интернету не требуется, так как мы будем анализировать получившееся сообщение в папке Исходящие. В открывшемся диалоговом окне введите парольную фразу, заданную при создании ключей, и щелкните на кнопке ОК.
5 Откройте папку Исходящие и выберите только что созданное сообщение. Просмотрите его текст. Обратите внимание на добавленные служебные строки и электронную подпись в виде последовательности символов, не имеющей видимой закономерности.
6 Выделите весь текст сообщения и нажмите комбинацию клавиш CTRL+C. Щелкните правой кнопкой мыши на значке PGPtray на панели индикации и выберите в контекстном меню команду Clipboard / Decrypt & Verify (Буфер обмена / Расшифровать и проверить). В открывшемся диалоговом окне обратите внимание на сообщение *** PGP Signature Status: good, указывающее на целостность сообщения.
7 Откройте это сообщение, внесите произвольные (большие или небольшие) изменения в текст сообщения или в саму подпись, после чего выполните повторную проверку, как описано в п. 6. Убедитесь, что программа PGP обнаружила нарушение целостности сообщения.
8 Создайте новое сообщение, как описано в п. 2. На этот раз включите обе кнопки: Encrypt (PGP) (Зашифровать) и Sign (PGP) (Подписать). Выполните отправку сообщения, как описано в п. 4.
9 Посмотрите как выглядит отправленное сообщение в папке Исходящие. Убедитесь, что посторонний не сможет прочесть его.
10 Скопируйте текст зашифрованного сообщения в буфер обмена и выполните его расшифровку как показано в п. 6. По запросу введите парольную фразу. Убедитесь, что как отображается текст исходного сообщения, так и выдается информация о его целостности.
11 Щелкните на кнопке Copy to Clipboard (Копировать в буфер обмена), чтобы поместить расшифрованный текст в буфер обмена.
12 Вставьте расшифрованный текст в любом текстовом редакторе и сохраните его как файл.

Вы научились отправлять по электронной почте сообщения, снабженные электронной цифровой подписью, а также зашифрованные сообщения.

Контрольные вопросы

1 Какой ключ используется при шифровании сообщения?

2 Какой ключ используется при создании цифровой подписи?
3 Какие системы создания ЭЦП и шифрования используются в России?

Лабораторная работа № 6

ШИФРОВАНИЕ ДАННЫХ НА ЖЕСТКОМ ДИСКЕ ПРИ ПОМОЩИ СИСТЕМЫ PGP

Цель работы. Ознакомиться с возможностями системы PGP для защищенного хранения файлов на жестком диске.

Задание. С помощью PGP создайте файл и отправьте его на защищенное хранение. Изучите различные механизмы для шифрования и расшифровки файлов.

Порядок выполнения работы

1 С помощью текстового процессора WordPad создайте произвольный документ и сохраните его под именем pgp-Proba.doc. Можно также скопировать под этим именем какой-либо из уже существующих файлов документов.
2 Откройте этот документ в программе WordPad и дайте команду Правка / Выделить все. Нажмите комбинацию клавиш CTRL+C.
3 Щелкните правой кнопкой мыши на значке PGPtray на панели индикации и выберите в контекстном меню команду Clipboard / Encrypt & Sign (Буфер обмена / Зашифровать и подписать).
4 В открывшемся диалоговом окне перетащите созданный вами ключ в список Recipients (Получатели) и щелкните на кнопке OK.
5 Введите парольную фразу, используемую для электронной подписи, и щелкните на кнопке OK.
6 Вернитесь в программу WordPad, нажмите клавишу DELETE и далее комбинацию CTRL+V. Сохраните документ под именем pgp-Proba-clp.doc. Закройте программу WordPad.
7 Любым способом запустите программу Проводник и откройте папку, в которой лежит файл pgp-Proba.doc.
8 Щелкните правой кнопкой мыши на значке файла и выберите в контекстном меню команду PGP / Encrypt & Sign (PGP / Зашифровать и подписать). Далее действуйте в соответствии с пп. 4-5.
9 Убедитесь, что в папке появился файл pgp-Proba.doc.pgp.
10 Теперь расшифруем созданные файлы. Запустите программу WordPad и откройте файл pgp-Proba-clp.doc.
11 Щелкните правой кнопкой мыши на значке PGPtray на панели индикации и выберите в контекстном меню команду Current Window / Decrypt & Verify (Текущее окно / Расшифровать и проверить).
12 Введите парольную фразу и щелкните на кнопке OK.
13 В открывшемся диалоговом окне Text Viewer (Просмотр текста) щелкните на кнопке Copy to Clipboard (Скопировать в буфер обмена).
14 Вставьте текст в окно программы WordPad и сохраните полученный файл.
15 Откройте программу Проводник и разыщите файл pgp-Proba.doc.pgp. Дважды щелкните на его значке.
16 Введите парольную фразу и щелкните на кнопке OK.
17 Так как оригинал файла не был уничтожен, программа предложит указать, под каким именем следует сохранить файл. Введите это имя по своему усмотрению.

Вы научились отправлять файлы на защищенное хранение, шифруя их при помощи программы PGP. Выяснили, что для текстовых данных эту операцию можно применять непосредственно в текущем окне редактора или к данным, находящимся в буфере обмена. Для произвольных файлов выполнять шифрование можно через контекстное меню. Вы также узнали как расшифровывать зашифрованные файлы, используя разные способы.

Контрольные вопросы

1 Как отправлять файлы на защищенное хранение при помощи программы PGP?
2 С помощью еще каких программ можно обеспечить защищенное хранение файлов?

3 Существует ли вероятность потери (удаления) защищенных файлов?

4 Что необходимо предпринять для исключения случайного или преднамеренного удаления файлов?

Библиографический список

1 Симонович С.В. Информатика для юристов и экономистов. СПб.: Питер, 2001. 688 с.

2 Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. М.: Академический Проект; Фонд "Мир", 2003. 640 с.

3 Соколов А.В., Степанюк О.М. Защита от компьютерного терроризма: Справочное пособие. СПБ.: БХВ – Петербург; Арлит, 2002. 496 с.

4 Терехов А.В., Чернышов В.Н., Селезнев А.В. Защита компьютерной информации: Учебное пособие. Тамбов: Изд-во Тамб. гос. техн. ун-та, 2003. 90 с.