Дагестанский Государственный Технический

Университет

Кафедра «Таможенное дело»

СОГЛАСОВАНО
Заведующий кафедрой

_____
Х.З.Халимбеков
_____
«___ » г.

СОГЛАСОВАНО
Декан Факультета

_____ _____
« » _____ 20 г.

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ПО УЧЕБНОЙ ДИСЦИПЛИНЕ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТАМОЖЕННЫХ ОРГАНОВ

для специальности 38.05.02 «Таможенное дело»

Составители:
Фастовец И.П., доцент кафедры «Таможенное дело», Халимбеков Х.З., зав. кафедрой "Таможенное дело"

____ _____ ____
« » 20 г., протокол №

Махачкала

ПЕРЕЧЕНЬ МАТЕРИАЛОВ

I. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Электронный учебно-методический комплекс составлен на основе требований включает краткий конспект лекций, лабораторный практикум, перечень вопросов к зачету, список литературы, учебную программу дисциплины. Навигация по комплексу осуществляется с помощью гиперссылок.

Целью изучения дисциплины «Информационная безопасность таможенных служб» является ознакомление студентов с фундаментальными понятиями, основными определениями и методами обеспечения информационной безопасности в условиях широкого применения современных информационных технологий. А именно, изучение информационных угроз, их нейтрализации, вопросов организации мер защиты информационных ресурсов, нормативных документов, регламентирующих информационную деятельность, криптографических методов защиты информации, другие вопросы, связанные с обеспечением безопасности компьютерных сетей.

В результате изучения дисциплины «Информационная безопасность таможенных служб» студент должен

знать:

- содержание основных понятий обеспечения информационной безопасности;
- основные виды угроз информационной безопасности, методы их выявления и блокирования;
- методы и средства защиты от несанкционированного доступа к информации в компьютерных системах;
- методы защиты информации от несанкционированного доступа в операционных системах;
- криптографические методы обеспечения информационной безопасности;
- способы защиты компьютерных систем от вредоносных программ;

уметь:

- обеспечивать защиту информации штатными средствами операционной системы;
- осуществлять эффективный выбор компьютерных систем защиты;
- применять различные технологии защиты информации в реальных инфраструктурах.

Знания и умения, полученные студентами при изучении данной дисциплины, необходимы для освоения последующих специальных дисциплин, связанных с таможенными информационными технологиями.

В соответствии с учебным планом специальности на изучение дисциплины отведено 74 часа, из них аудиторных – 34 часа, включая 17 часов лекций и 34 часов лабораторных занятий. Количество часов по каждой теме и по каждой лабораторной работе приведены в учебно-методической карте.

II. КРАТКИЙ КОНСПЕКТ ЛЕКЦИЙ

Тема № 1. Основные понятия и анализ угроз информационной безопасности

Защита информации – это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Объект защиты – это информация, носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

Цель защиты информации – это желаемый результат защиты информации. Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.

Система защиты информации – совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

Информационная безопасность – это защищённость информации от незаконного ознакомления, преобразования и уничтожения, а также защищённость информационных ресурсов от воздействий, направленных на нарушение их работоспособности.

Основными составляющими информационной безопасности являются: *конфиденциальность*, *доступность*, *целостность*.

Угроза – потенциальная возможность нарушить информационную безопасность (конфиденциальность, целостность и/или доступность информации), а также возможность нелегального использования ресурсов сети.

Классификация возможных угроз информационной безопасности автоматизированных систем (АС) может быть проведена по следующим базовым признакам:

1. По природе возникновения.
2. По степени преднамеренности проявления.
3. По непосредственному источнику угроз.
4. По положению источника угроз.
5. По степени зависимости от активности АС.
6. По степени воздействия на АС.
7. По этапам доступа пользователей или программ к ресурсам АС.
8. По способу доступа к ресурсам АС.
9. По текущему месту расположения информации, хранимой и обрабатываемой в АС.

Тема № 2. Защита информации от несанкционированного доступа

Несанкционированный доступ к информации (НСД) – нарушение установленных правил разграничения доступа. Лицо или процесс, осуществляющие НСД к информации, являются нарушителями правил разграничения доступа. НСД является наиболее распространённым видом компьютерных нарушений.

Основными способами несанкционированного доступа к информации в компьютерных системах (КС) являются:

- непосредственное обращение к объекту с конфиденциальной информацией;

- создание программных и технических средств, выполняющих обращение к объекту в обход средств защиты;
- модификация средств защиты для осуществления несанкционированного доступа;
- внедрение в технические средства СТВ (средств вычислительной техники) или АС (автоматизированных систем) программных или технических механизмов, нарушающих структуру и функции этих средств для осуществления несанкционированного доступа.

Основными направлениями обеспечения защиты СТВ и АС от несанкционированного доступа являются создание ***системы разграничения доступа (СРД)*** субъектов к объектам доступа и создание обеспечивающих средств для СРД.

Основными способами защиты от несанкционированного доступа к информации в компьютерных системах являются:

- аутентификация;
- авторизация;
- шифрование информации.

Тема № 3. Безопасное использование информационной среды

Межсетевой экран (МЭ) или **сетевой экран** – это специализированный комплекс аппаратной или программной межсетевой защиты, называемый также ***брандмауэром*** или системой *firewall*, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

В зависимости от охвата контролируемых потоков данных сетевые экраны делятся на: *традиционный сетевой* (или *межсетевой*) экран; *персональный сетевой* экран.

Функции МЭ следующие:

- фильтрация трафика;
- выполнение функций посредничества;
- дополнительные функции: идентификация и аутентификация пользователей; трансляция сетевых адресов; администрирование; регистрация событий и генерация отчётов.

Виртуальная частная сеть – VPN (Virtual Private Network) – технология безопасного подключения к корпоративной сети через Интернет.

Виртуальные частные сети являются комбинацией нескольких самостоятельных сервисов (механизмов) безопасности:

- *шифрования* на выделенных шлюзах;
- *экранирования*;
- *туннелирования*.

Временные файлы – файлы, создаваемые определённой программой или операционной системой для сохранения промежуточных результатов в процессе функционирования или передачи данных в другую программу.

Для нормальной работы операционной системы и любого другого программного обеспечения используются различные временные файлы, которые сохраняются в специальных системных папках Temp. Для удаления временных файлов можно воспользоваться стандартным инструментом ***Очистка диска***, который встроен в ОС Windows XP.

Ещё одним источником большого количества временных файлов (файлов *cookie*) является *Интернет*. Каждый раз, когда загружается интернет-страница, все составные

файлы страницы запоминаются в так называемом ***кэше*** (папке Cashe). По умолчанию Файлы *cookie* сохраняются в папке Cookies, которая находится на *C:\Documents and Settings\(имя пользователя)\Cookies*. Чтобы их удалить щёлкните правой кнопкой мыши по ярлыку программы-браузера и в открывшемся контекстном меню выберите команду **Свойства**/вкладку **Общие**/в области **Истории просмотра** кнопку **Удалить** (что позволит удалить временные файлы, файлы cookies, истории просмотра и др.).

Тема № 4. Защита компьютерных систем от вредоносных программ

К вредоносным программам относятся *компьютерные вирусы* и *программные закладки*.

Компьютерным вирусом называют автономно функционирующую программу, обладающую способностью к включению своего кода в тела других файлов и системных областей памяти компьютера, последующему самостоятельному выполнению и распространению в компьютерных системах.

Программной закладкой называют внешнюю или внутреннюю по отношению к атакуемой компьютерной системе программу, обладающую определёнными разрушительными функциями по отношению к этой системе.

Компьютерные вирусы классифицируются по следующим признакам:

- по способу распространения в КС.
- по способу заражения других объектов КС.
- по деструктивным возможностям.
- по особенностям реализуемого алгоритма.
- по наличию дополнительных возможностей.

Основными каналами распространения компьютерных вирусов в настоящее время являются:

- электронная почта;
- телеконференции и электронные доски объявлений в сети Internet;
- программное обеспечение, размещённое на общедоступных узлах сети Internet;
- информационные ресурсы сети Internet, содержащие ссылки на заражённые траянские Web-сайты с элементами управления Active-X или апплетами Java;
- локальные компьютерные сети организаций;
- обмен заражёнными файлами на дисках или записываемых компакт-дисках между пользователями сети;
- использование нелицензионных компакт-дисков с программным обеспечением и другими информационными ресурсами.

К основным методам обнаружения компьютерных вирусов относятся:

- метод сравнения с эталоном.
- эвристический анализ.
- антивирусный мониторинг.
- метод обнаружения изменений.
- встраивание антивирусов в BIOS компьютера.

Антивирусная программа – программа, предназначенная для поиска, обнаружения, классификации и удаления компьютерного вируса и вирусоподобных программ.

Различают следующие виды антивирусных программ:

- программы-фаги (сканеры);
- программы-ревизоры (CRC-сканеры);

- программы-блокировщики.
- программы-иммунизаторы.

Программные закладки классифицируются:

- по методу внедрения;
- по назначению.

Защита от программных закладок осуществляется в следующих вариантах:

- защита от внедрения закладок;
- выявление внедрённых программных закладок;
- удаление внедрённых закладок.

Тема № 5. Безопасное использование Интернет-ресурсов

Анонимность в Интернете – это достаточно актуальная тема для каждого пользователя Интернета, т.к. существует очень много способов узнать личную информацию о пользователе по его IP-адресу или другим характеристикам Интернет-соединения.

Когда пользователь набирает в строке браузера какой-нибудь адрес, то сначала запрос отправляется на сервер DNS, который преобразует строку символов в набор из 32 нулей и единиц, т.е. IP-**адрес**, использующийся для маршрутизации. Зная этот адрес, злоумышленник может выведать о пользователе очень многое.

Существуют следующие способы маскировки (скрытия) IP-адреса:

1. Использование *анонимного прокси-сервера*.
2. Использование *программ-анонимайзеров*.
3. Использование *socks-протоколов*.
4. Использование *VPN-технологии*.

Основными угрозами информационной безопасности при использовании электронной почты являются:

- блокирование электронного почтового ящика;
- потеря почтового сообщения;
- перехват электронной почтовой корреспонденции;
- несанкционированный доступ к электронному почтовому ящику;
- несанкционированный доступ к компьютеру пользователя электронной почты;
- подмена имени, электронного и/или IP-адреса отправителя в электронном почтовом сообщении;
- удаление имени и адреса отправителя;
- формирование подложного сообщения от имени адресата;
- несанкционированная рассылка сообщений – спам;
- внедрение в компьютер вредоносных программ, полученных с электронным почтовым сообщением;
- анализ почтового трафика;
- атаки на почтовые серверы.

Спам – это массовые неадресные рекламные рассылки по электронной почте.

Способы распространения спама:

1. Электронная почта.
2. Мгновенные сообщения.
3. Блоги, вики, форумы, доски объявлений.
4. Социальные сети и сайты знакомств.

5. Сетевые сообщения.
6. Поисковый спам.

Методы защиты от спама:

1. Ручная или автоматическая фильтрация почты по заголовкам.
2. Использование специальных служб фильтрации, находящихся у почтового провайдера или на отдельном сервере.
3. Применение входных фильтров, основанных на анализе IP-адреса хоста, передающего спам.
4. Фильтрация на основе автоматического пополнения access-листа адресами спамеров.
5. Использование программ или встраиваемых модулей для анализа содержимого письма.

Тема № 6. Криптографические методы обеспечения информационной безопасности

Криптография – это фундаментальная наука, изучающая методы преобразования информации, направленные на сокрытие её содержания.

Шифрование – криптографическая обработка информации с помощью одного из алгоритмов).

Сегодня широко распространено 2 типа шифрования:

1. *Традиционное* или *симметричное* (с секретным ключом).
2. *Асимметричное* (с открытым ключом).

Процесс традиционного шифрования включает две составляющие:

1. Алгоритм шифрования.
2. Ключ – значение, не зависящее от открытого текста.

Надёжность традиционного шифрования определяет нескольких факторов:

- сложность алгоритма шифрования;
- секретность ключа.

Классификация криптографических систем строится на основе следующих трёх характеристик:

1. Число применяемых ключей.
2. Тип операций по преобразованию открытого текста в шифрованный.
3. Метод обработки открытого текста.

Электронная цифровая подпись (ЭЦП) – это реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, установить отсутствие искажения информации в электронном документе, а также обеспечивает неотказуемость подписавшегося.

Известны следующие системы ЭЦП:

- на основе алгоритмов симметричного шифрования;
- на основе алгоритмов асимметричного шифрования.

Методы **стенографии** направлены на скрытие самого присутствия конфиденциальной информации.

Методы компьютерной стенографии делятся на две основные группы:

1. Методы, использующие специальные свойства форматов электронных документов.

2. Методы, использующие естественную избыточность оцифрованных графических изображений, звука и видеоинформации.

Тема № 7. Анализ защищённости локальной вычислительной сети и её узлов

Под **протоколированием** или **регистрацией** понимается сбор и накопление информации о событиях, происходящих в информационной системе организации.

К числу регистрируемых событий относятся:

- вход в систему;
- выход из системы;
- обращение к удалённым системам;
- операции с файлами;
- смена привилегий или иных атрибутов безопасности.

Протоколируемые данные помещаются в регистрационный журнал, который представляет собой хронологически упорядоченную совокупность записей результатов деятельности субъектов ИС, достаточную для восстановления, просмотра и анализа последовательности действий с целью контроля конечного результата.

Аудит – это анализ протоколируемой информации, проводимый оперативно, в реальном времени или периодически с целью оперативного выявления и предотвращения нарушений режима информационной безопасности.

Для предупреждения и своевременного выявления попыток несанкционированного входа в систему используются средства *активного аудита*.

Назначение механизма *протоколирования* и *аудита* следующее:

1) обеспечение подотчётности пользователей и администраторов;
2) обеспечение возможности реконструкции последовательности событий;
3) обнаружение попыток нарушений информационной безопасности;
4) предоставление информации для выявления и анализа технических проблем, не связанных с безопасностью.

Тема № 8. Защита таможенных информационных систем

Основными факторами, которые поднимают актуальность вопросов обеспечения информационной безопасности таможенных органов, являются:

– объединение в единое информационное пространство деятельности таможенных органов государств – участников Таможенного союза;

– динамическое развитие информационных технологий в таможенном деле;

– специфика закрытости технологий и средств защиты конфиденциальной информации таможенных органов.

По своей общей направленности угрозы информационной безопасности таможенных органов делятся на:

– угрозы конституционным правам и свободам человека и гражданина в информационной сфере деятельности таможенных органов;

– угрозы информационному обеспечению государственной политики в области таможенного дела;

– угрозы безопасности информационных и телекоммуникационных средств и систем таможенных органов.

В качестве вероятного *нарушителя информационной безопасности* объектов таможенной инфраструктуры рассматривается субъект, имеющий возможность реализовывать, в том числе с помощью технических средств, угрозы информационной безопасности, и осуществлять посягательства (способы воздействия) на информационные ресурсы и системы таможенных органов.

Основные направления обеспечения информационной безопасности таможенных органов Республики Беларусь, следующие:

− организационно-режимное обеспечение защиты сведений, составляющих государственную тайну;

− обеспечение физической защиты объектов и средств информатизации;

− обеспечение защиты информации от утечки по техническим каналам;

− обеспечение защиты информации от несанкционированного доступа в АИС и ЛВС;

− обеспечение конфиденциальности и целостности информации;

− обеспечение безопасного информационного взаимодействия ГТК Республики Беларусь с отечественными и зарубежными организациями, министерствами и ведомствами;

− организация, координация и финансирование научно-исследовательских и опытно-конструкторских работ в области обеспечения информационной безопасности;

− совершенствование нормативно-методической базы обеспечения информационной безопасности.

III. ЛАБОРАТОРНЫЕ ЗАНЯТИЯ

Лабораторная работа № 1

Программное обеспечение безопасности информационных систем

Цель работы: ознакомление со средствами защиты операционных систем, офисных приложений и данных на дисках.

Задание

1. Создайте в своей рабочей папке новую папку с именем **Мои файлы** и скопируйте в неё из архива сервера (под руководством преподавателя) любой один: текстовый файл, табличный файл, любую базу данных. Далее работайте со скопированными файлами.
2. Установите пароли на открытие текстового документа и на разрешение записи в текстовый документ. Выполните проверку установленных паролей в данном документе.
3. Снимите пароли с текстового документа и создайте его резервную копию. Проверьте наличие созданной резервной копии.
4. Отмените создание резервной копии текстового документа.
5. Установите пароли на открытие табличного файла (т.е. файла-Excel) и на разрешение записи в табличный файл. Выполните проверку установленных паролей в данном файле.
6. Снимите пароли с табличного файла и создайте его резервную копию. Проверьте наличие созданной резервной копии.
7. Отмените создание резервной копии табличного файла.
8. Установите пароль на открытие базы данных. Выполните проверку установленного пароля в базе данных.

9. Снимите пароль с базы данных и проверьте снятие пароля.
10. Заархивируйте содержимое папки **Мои файлы** в *самораспаковывающийся архив* под именем **Самораспаковка_архива**. Данный архив должен находиться в вашей рабочей папке.
11. Создайте в своей рабочей папке *многотомный архив* из содержимого папки **Мои файлы** (размер каждого тома должен быть по 1,44 Мбайт).
12. Проверьте наличие созданных архивов.
13. Создайте в своей рабочей папке две новых папки с именами **Самораспаковка** и **Многотомный**. В папку **Самораспаковка** разархивируйте созданный ранее самораспаковывающийся архив, а в папку **Многотомный** распакуйте созданный ранее многотомный архив.
14. Результаты работы продемонстрируйте преподавателю.

Лабораторная работа № 2

Безопасность компьютера в Сети Интернет

Цель работы: ознакомление со средствами защиты компьютера при работе в Интернете.

1. Безопасность в Интернете

Понятие безопасности и защиты в Интернете можно рассматривать в трёх аспектах:

1) Защита от опасного исполнимого содержимого. Имеется в виду безопасность собственного компьютера, его операционной системы и установленных на нём программ. Безопасность аппаратного и программного обеспечения может быть нарушена при получении опасного исполнимого кода. Простейшим примером такого кода являются компьютерные вирусы, хотя далеко не только вирусы могут иметь опасное исполнимое содержимое. Настройка защиты от опасного *исполнимого содержимого* выполняется в окне обозревателя Internet Explorer с помощью команд меню **Сервис/Свойства обозревателя**/вкладка **Безопасность** (или щелчок правой кнопкой мыши по значку Internet Explorer на рабочем столе и выбор из контекстного меню команды **Свойства**).

2) Защита от неприемлемого содержания. В силу многих причин, многим людям может быть неприемлемо содержание ряда материалов, публикуемых в Сети. Защиту от таких материалов можно рассматривать как защиту от психологического воздействия. В Интернете неприемлемое содержание часто маскируют или подбрасывают столь же неожиданно, как рекламу по телевизору. Не всегда щёлкая по гиперссылкам, пользователь точно знает, что его ждёт на другом конце соединения. Настройка ограничений по принимаемому содержанию выполняется в окне обозревателя Internet Explorer с помощью команд меню **Сервис/Свойства обозревателя**/вкладка **Содержание**.

3) Безопасность транспортировки данных. Чем сильнее коммерция проникает в Интернет, тем чаще приходится отправлять и получать конфиденциальные данные. Без средств защиты эти данные могут быть просмотрены или даже изменены на путях транспортировки. Настройка средств обеспечения защищённой связи выполняется в окне обозревателя Internet Explorer с помощью команд меню **Сервис/Свойства обозревателя**/вкладка **Содержание**.

1.1. Защита от опасного активного содержимого

Активные компоненты – это особые объекты, встраиваемые на Web-страницы для улучшения их оформления. По своей сути это микропрограммы, которые работают на машине клиента. В принципе, многое сделано для того, чтобы такой активный компонент не мог произвести на машине клиента разрушительных операций или стать агентом, поставляющим информацию с машины клиента в Сеть. Но абсолютной гарантии нет.

Средства вкладки **Безопасность** (щелчок правой кнопкой мыши по значку Internet Explorer на рабочем столе и выбор **Свойства**/вкладка **Безопасность**) позволяют настроить компьютер на тот или иной уровень защиты. Общий принцип такой: чем выше степень защиты, тем меньше функциональные возможности браузера, тем меньше услуг в Интернете можно получить.

В Internet Explorer Интернет условно разбивается на 4 зоны по степени опасности:

- *Надёжные узлы* (узлы, в надёжности которых вы уверены);
- *Ограниченные узлы* (узлы с сомнительным содержанием);
- *Местная интрасеть* (собственная локальная сеть предприятия);
- *Интернет* (все прочие узлы).

Для первых трёх категорий можно с помощью кнопки **Узел** задать собственный список узлов. Для каждой из категорий можно задать уровень безопасности от низкого до высокого. Чтобы понять, чем именно отличаются режимы безопасности, можно воспользоваться кнопкой **Другой**. Она позволяет:

- наглядно увидеть настройку параметров безопасности в части приёма потенциально опасного содержимого;
- сделать более тонкую настройку уровня безопасности.

Т.о., нажав на кнопку **Другой**, можно вручную отрегулировать защиту браузера, разрешив или запретив работу различных активных компонентов Web-страниц.

Настройка правил безопасности

Правила безопасности – это совокупность настроек, позволяющих Обозревателю автоматически принимать решения о том, как действовать при проведении операций, считающихся опасными.

Настройка правил безопасности выполняется в диалоговом окне **Параметры безопасности**. Чтобы его открыть нужно в окне обозревателя Internet Explorer выбрать **Сервис/Свойства обозревателя**/вкладка **Безопасность**/выбрать зону **Интернет**/кнопка **Другой**.

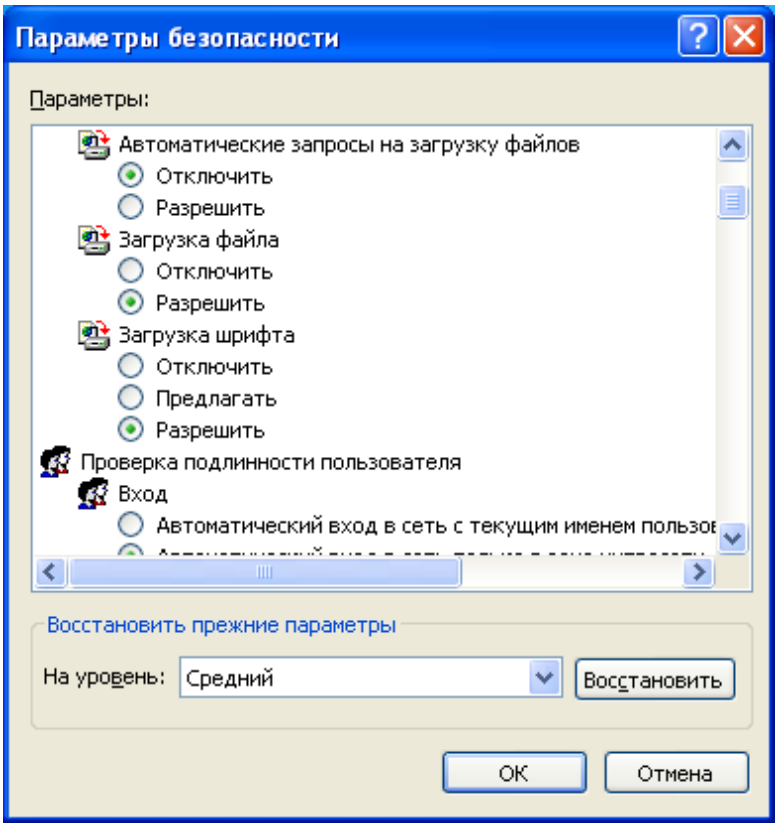


Рис. 1. ***Окно настройки параметров безопасности.***

В окне **Параметры безопасности** (см. рис. 1) содержится перечень настраиваемых операций. Настройка выполняется включением нужного переключателя.

Самый простой способ настройки – включить для каждой сомнительной операции переключатель **Предлагать**. В этом случае перед проведением операции Internet Explorer будет выдавать предупреждающее сообщение и делать запрос, надо или нет выполнять операцию. Если этих запросов станет так много, что они будут мешать нормальной работе, от них можно отказаться. Если включить переключатель **Разрешить**, то операция будет выполняться без предупреждения. Если включить переключатель **Отключить**, то операция выполняться не будет, но и предупреждение тоже не поступит, т.е. вы не узнаете, чего лишились.

В группах ***Загрузка файла*** и ***Загрузка шрифта*** можно оставить включённым переключатель **Разрешить**.

В группе ***Проверка подлинности пользователя*** включите переключатель **Анонимный вход**. Под именем пользователя здесь понимается то имя, которое было задано при установке операционной системе на компьютере. Зачем это имя нужно серверам – непонятно. Если владелец сервера хочет собирать статистику о клиентах – это его трудности – пусть устраивает гласную процедуру регистрации и проверки. Вам решать, что вы желаете сообщить о себе, а что – нет. Позволять же чужим серверам автоматически выяснять, на кого записан тот или иной компьютер, и на кого зарегистрирована его операционная система – совершенно ни к чему.

По всем остальным категориям можно включить нейтральный и ни к чему не обязывающий переключатель **Предлагать**. Решение в каждом конкретном случае будете принимать сами, и ваш компьютер будет работать под вашим контролем.

Чем опасны апплеты Java?

У протокола HTTP, на котором основана служба World Wide Web, есть одна особенность, связанная с тем, что этот протокол «одноразовый». Согласно ему браузер по щелчку на гиперссылке отправляет серверу запрос на поставку одного URL-ресурса, например текста Web-страницы. Сервер обрабатыва-

ет этот запрос и посылает затребованный ресурс, после чего разрывает HTTP-соединение. Если на Web-странице имеются какие-то рисунки и другие объекты, то в общем случае на поставку каждого объекта надо делать новый запрос. Правда, современные браузеры избавляют пользователей от необходимости щёлкать на каждом встроенном объекте и автоматически генерируют запросы на поставку всего того, что есть на Web-странице, но суть остаётся той же – протокол HTTP «одноразовый». Из-за этого трудно сделать динамическое или интерактивное взаимодействие между браузером и сервером.

Поэтому для создания интерактивных Web-страниц (или страниц с динамичным изменением содержимого) нужно, чтобы на компьютере клиента работала бы какая-то активная программа. Её можно передать клиенту в виде объекта, встроенного в Web-страницу, примерно так же, как встраивают рисунки, а на компьютере клиента она должна заработать и обеспечить непрерывный обмен данными между клиентом и сервером. Этот обмен мы видим на экране как анимацию или игру.

Такая активная программа не может быть большой, поскольку в этом случае она бы очень долго передавалась. Такие микропрограммы называются *апплетами*, а поскольку они создаются на языке Java, то их называют *Java-апплетами*.

Т.о., Java-апплеты – это настоящие полноценные программы, встроив в которые вредоносную начинку, создатели Web-страницы могут получить доступ к содержимому вашего жёсткого диска. Последствия от этого уже известны – от простой кражи пароля до форматирования жёсткого диска.

Java-апплет не работает напрямую ни с процессором, ни с операционной системой. Он общается с ними через браузер. Браузер интерпретирует команды апплета и переводит их в код, понятный процессору и системе. Поэтому один и тот же апплет способен работать на любом компьютере, если на нём есть браузер, способный понять его код.

Для разных типов компьютеров у разных браузеров, написанных под разные операционные системы, время от времени проскальзывают мелкие «дырки» в защите от подобных вредоносных Java-апплетов. Поэтому в каждой очередной версии браузера подобные дефекты устраняются. Соответственно рекомендуется браузер немедленно обновлять при появлении его новой версии.

Те, кто серьёзно опасаются свою безопасность, могут спокойно отключить какое-либо исполнение Java-апплетов на своих компьютерах (в диалоговом окне **Параметры безопасности**), правда, при этом снизится привлекательность и функциональность ряда Web-страниц.

Чем опасны сценарии JavaScript?

JavaScript – это язык для записи так называемых *сценариев* (групп операторов языка). Он был разработан, чтобы расширить возможностей стандартного языка HTML, а именно, предоставить средства для управления браузером. В код Web-документа операторы языка JavaScript вставляются между специальными тегами HTML <SCRIPT LANGUAGE = “JavaScript”> и </SCRIPT>. Исполняются операторы языка JavaScript с помощью браузера. Обычно их используют для обеспечения интерактивного взаимодействия между клиентом и сервером. Например, средствами JavaScript можно сделать так, чтобы при щелчке в определённом месте Web-страницы раскрывалось какое-то меню, предоставляющее пользователю тот или иной выбор.

Как и Java-апплеты, сценарии JavaScript могут представлять опасность для клиента, но характер этой опасности другой. Если Java-апплет может содержать разрушительный код, то операторы JavaScript такой угрозы не представляют, но зато с их помощью можно компроментировать конфиденциальную информацию. Известные ошибки в браузерах позволяют удалённому серверу проникать, например, к парольным файлам, а нередко и вообще к любым.

Ошибки браузеров, связанные с обработкой сценариев JavaScript, встречаются постоянно. Т.к. эти ошибки не угрожают уничтожению информации на компьютерах клиентов, производители браузеров не всегда спешат их «заделывать», как это бывает с ошибками в воспроизведении апплетов Java. Поэтому некоторые бреши в защите подолгу остаются неустранёнными.

Поэтому если на вашем компьютере есть чувствительная информация. О которой удалённому серверу знать не стоит (например, нелицензированные версии программных продуктов), то отключите возможность исполнения сценариев JavaScript в диалоговом окне **Параметры безопасности**.

Чем опасны элементы ActiveX?

Это ещё одна технология поставки активных объектов в составе Web-страниц. И если опасные команды, содержащиеся в Java-апплетах, блокируются браузером, то элементы ActiveX, напротив, браузером не контролируются. Они исполняются процессором под управлением операционной системы точно так же, как и любые программы, а потому могут иметь любое сколь угодно опасное содержимое.

Элементы ActiveX машинозависимы. Разработчик Web-страницы создаёт их для каждой компьютерной платформы и для каждой операционной системы отдельно. С помощью элементов ActiveX проще сделать выигрышное оформление Web-страниц. Пример применения элементов ActiveX – создание бегущих строк, анимации, фонового музыкального сопровождения и т.п.

Для элементов ActiveX реализована другая модель безопасности, отличающаяся от Java-апплетов и основанная на электронной подписи. Каждый элемент ActiveX, созданный разработчиком Web-страницы, должен быть им подписан собственным открытым ключом. Вместе с элементом мы принимаем и его сертификат с открытым ключом для воспроизведения. Если мы обращаемся на эту страницу не впервые, не исключено, что такой сертификат у нас уже есть, тогда он просто проверяется.

Сертификат разработчика гарантирует только то, что никто по пути следования элемента ActiveX не внёс изменений в его код или не сделал подмену. Но он не гарантирует, что этот элемент действительно принадлежит тому, кто его поставляет. Поэтому кроме подписи разработчика требуется ещё удостоверение от центра сертификации, заверяющего эту подпись.

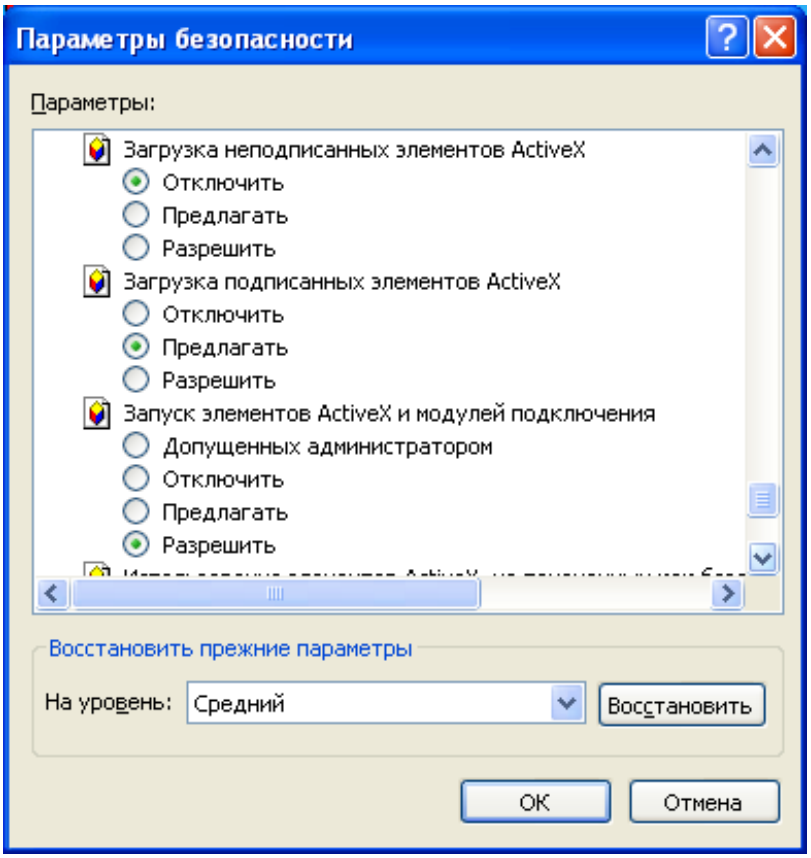


Рис. 2. ***Настройка параметров безопасности по приёму и исполнению элементов ActiveX.***

Настройкой правил безопасности (в диалоговом окне **Параметры безопасности**) пользователь может отключить приём и исполнение неподписанных (не имеющих сертификатов) элементов ActiveX (см. рис. 2). Он может принимать только элементы, созданные избранными разработчиками, подписи которых удостоверены и, наконец, он может принимать и исполнять все подписанные и удостоверенные элементы ActiveX. Если в этом случае что-то и случится с компьютером, можно утешить себя тем, что есть к кому предъявить претензии.

Файлы cookies

Файлы cookies (или «пирожки») сохраняют на диске пользовательского компьютера многие Интернет-страницы. Сохраняют, в общем-то, с благими целями: благодаря cookies Web-страничка может «узнать» вас при следующем визите на неё и будет каждый раз вежливо приветствовать вас, называя по имени, а заодно и предлагая вам именно те услуги, которые вы затребовали в прошлый раз. Сохраняются файлы cookies обычно на диске **C:** в папке Cookies.

«Пирожками» активно пользуются многие сайты: интернет-магазины, поисковики, порталы и блоги. Для нашей приватности cookies наименее опасны, но, тем не менее периодически необходимо очищать папку Cookies от подобных временных файлов. Это выполняется в окне обозревателя Internet Explorer с помощью команд меню **Сервис/Свойства обозревателя**/вкладка **Общие**/кнопка **Удалить** Cookie.

1.2. Центр обеспечения безопасности Windows XP.

Для защиты компьютера подключённого к компьютерной сети от вирусов, атак злоумышленников и других вторжений необходимо, чтобы на нём постоянно работали межсетевой экран (брандмауэр) и антивирусное ПО (с последними обновлениями). Кроме того, необходимо, чтобы все последние обновления были также установлены на вашем компьютере.

Поэтому компания Microsoft включила в состав SP2 для Windows XP такой инструмент, как "Центр обеспечения безопасности Windows" (Windows Security Center) (см. рис. 3).

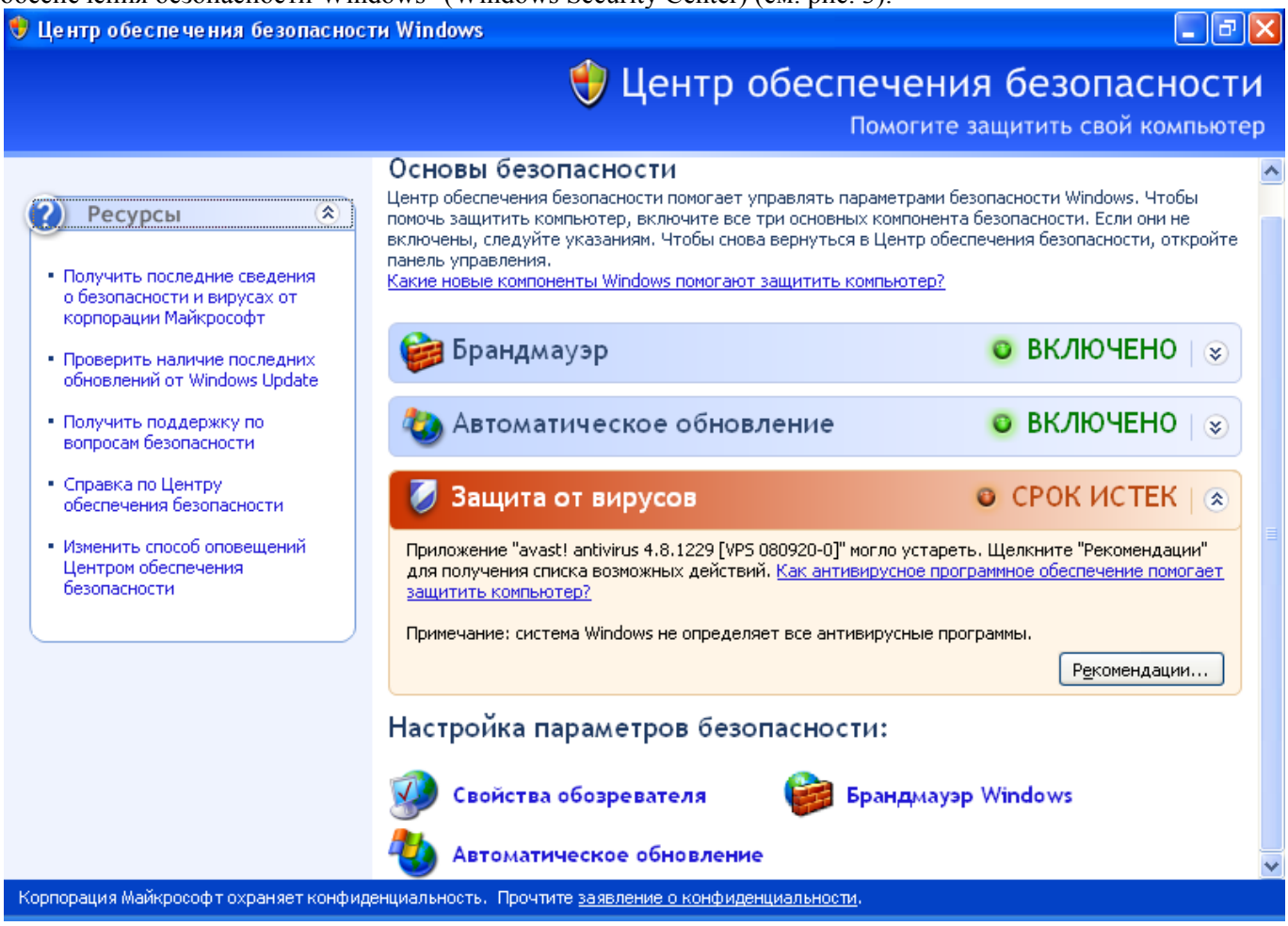


Рис. 3. ***Центр обеспечения безопасности*** *Windows*.

Основное назначение этого инструмента - информировать и направлять пользователя в нужном направлении.

Во-первых, он постоянно контролирует состояния трех основных компонентов ОС (брандмауэр, антивирус, система автоматического обновления). Если параметры любого из этих компонентов не будут удовлетворять требованиям безопасности компьютера, то пользователь получит соответствующее уведомление. Например, на рис. 4 представлено одно из таких уведомлений.

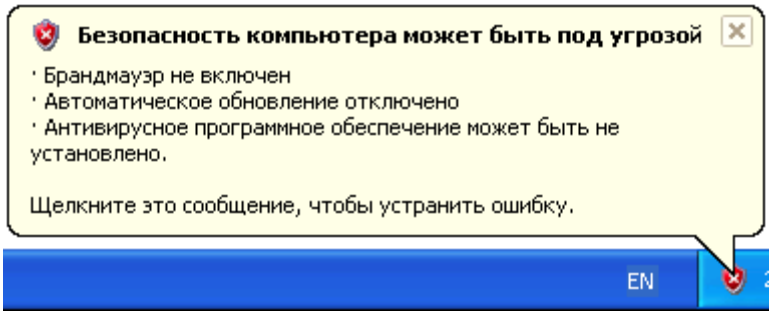


Рис. 4. ***Оповещение***.

Во-вторых, при открытии "Центра обеспечения безопасности Windows" пользователь может не только получить конкретные рекомендации о том, как исправить сложившуюся ситуацию, но также узнать, где находятся другие настройки, связанные с безопасностью компьютера, и где на сайте Microsoft можно прочитать дополнительную информацию по обеспечению безопасности.

1.2.1. Параметры безопасности Windows

Чтобы открыть "Центр обеспечения безопасности Windows", выберите **Пуск/Панель управления/Центр обеспечения безопасности**.

Окно Центра обеспечения безопасности Windows можно условно разделить на три части (см. рис. 5):

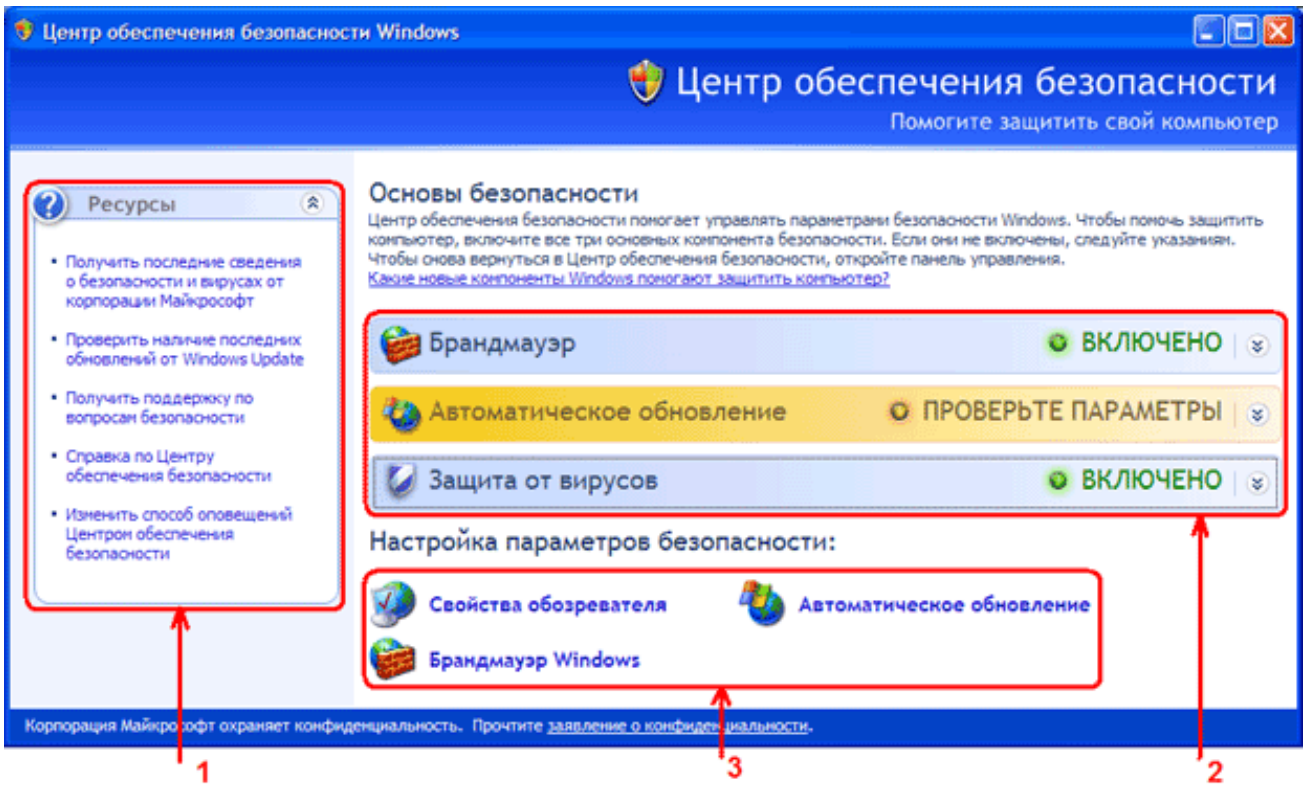


Рис. 5. ***Центр обеспечения безопасности.***

1. ***Ресурсы***. Здесь располагаются ссылки для перехода к Интернет-ресурсам, ко встроенной в Windows справочной службе и к окну настройки параметров оповещений.

2. ***Компоненты безопасности***. Здесь располагаются информационные элементы трех основных компонентов безопасности: брандмауэр, автоматическое обновление, антивирусная защита.

3. ***Параметры безопасности***. Здесь располагаются кнопки перехода к настройкам безопасности следующих компонентов: обозреватель Internet Explorer, автоматическое обновление, брандмауэр Windows.

Рассмотрим эти части более подробно.

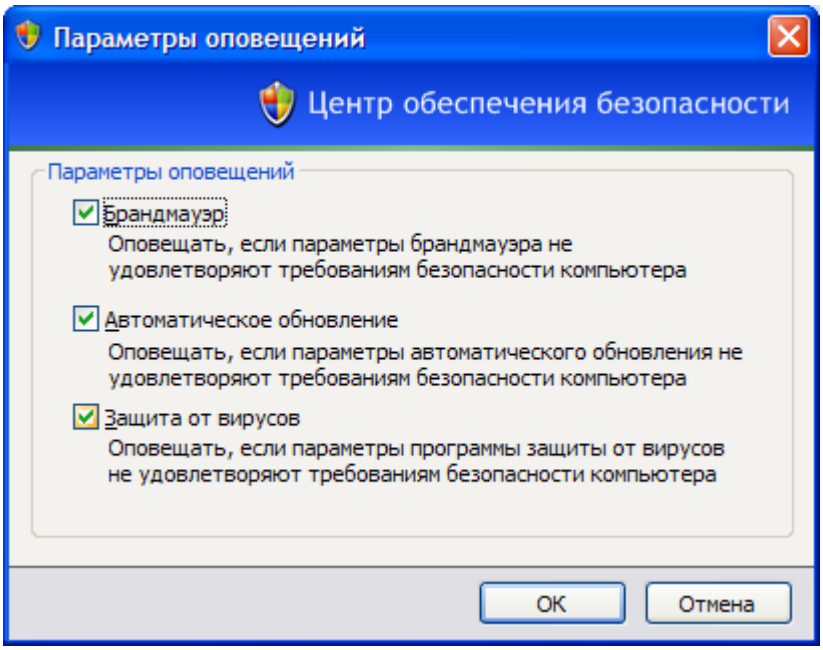


Рис. 6. ***Параметры оповещений.***

Ресурсы

В разделе 1 (см. рис. 5) первые три ссылки предназначены для перехода на соответствующие страницы на сайте Microsoft. Предпоследняя ссылка предназначена для открытия справочной службы Windows на странице "Общие сведения о центре обеспечения безопасности Windows". Последняя ссылка предназначена для открытия окна "Параметры оповещений" (рис. 6).

Если на компьютере установлен брандмауэр и антивирусное ПО, не определяемое Центром обеспечения безопасности, вы можете отключить соответствующие оповещения (см. рис. 6).

Компоненты безопасности

В разделе 2 (см. рис. 5) каждое информационное табло сообщает о состоянии соответствующего компонента. На рис. 7 представлены возможные состояния.

A	ВКЛЮЧЕНО
B	ПРОВЕРЬТЕ ПАРАМЕТРЫ
C	ВЫКЛЮЧЕНО
D	НЕ НАЙДЕНО
E	СРОК ИСТЕК
F	НЕ НАБЛЮДАЕТСЯ

Рис. 7. ***Состояния информационных табло.***

Состояния A-C понятны без комментариев.

Состояние D - "Не найдено" - соответствует невозможности определить присутствие соответствующего ПО (например, антивирус или брандмауэр).

Состояние E - "Срок истек" - возможно для антивирусной защиты, когда обновления антивирусных баз устарели.

Состояние F - "Не наблюдается" - соответствует отключенному контролю над соответствующим компонентом.

Центром обеспечения безопасности применяется двухуровневый подход к определению состояния компонентов:

1. Проверка содержимого реестра и файлов со сведениями о состоянии ПО (Microsoft получает перечень файлов и параметров реестра от производителей ПО).

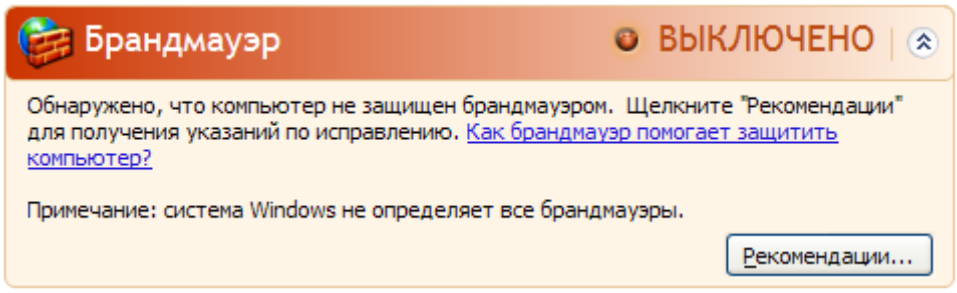


Рис. 8. ***Состояние "Брандмауэра".***

2. Сведения о состоянии ПО передаются от установленных программ средствами инструментария WMI (Windows Management Instrumentation - Инструментарий управления Windows).

На рис. 8 представлено одно из возможных состояний компонента "Брандмауэр". Нажав кнопку "Рекомендации…", вы получите возможность либо включить брандмауэр (рис. 4.9, кнопка "Включить сейчас"), либо отключить наблюдение за состоянием этого компонента (рис. 4.9, параметр "Я самостоятельно устанавливаю и слежу за брандмауэром").

После нажатия кнопки "Включить сейчас" (см. рис. 9), если брандмауэр Windows будет успешно запущен, на экране появится соответствующее сообщение (рис. 10).

На рис. 11 представлено одно из возможных состояний компонента "Автоматическое обновление". Нажав кнопку "Включить автоматическое обновление", вы задействуете рекомендуемый компанией Microsoft режим работы системы "Автоматическое обновление" (см. рис. 12).

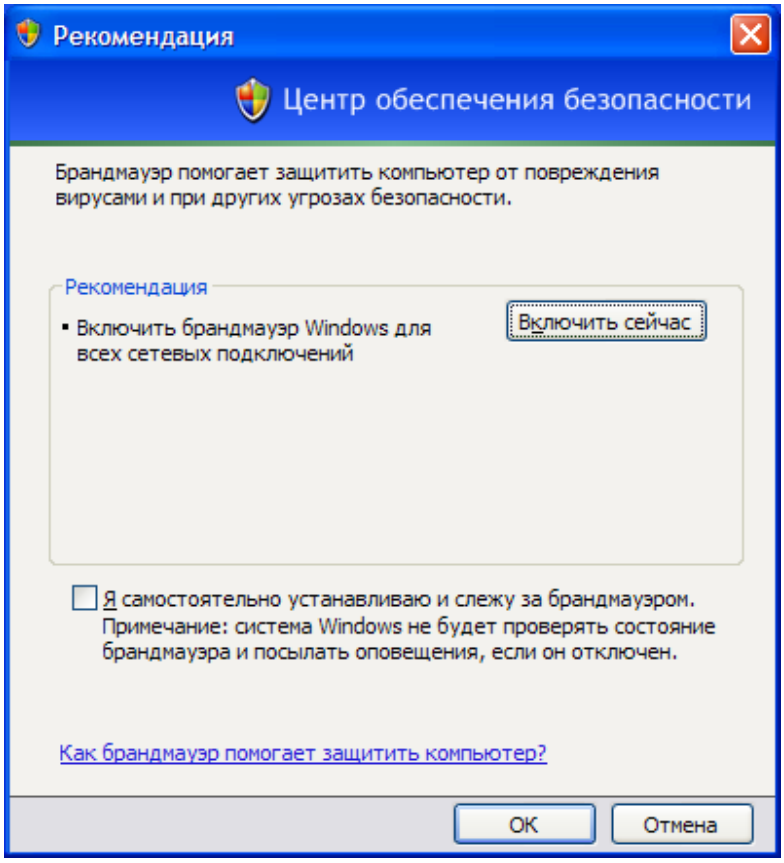


Рис. 9. ***Рекомендация.***

В зависимости от выставленного режима работы "Автоматического обновления" (см. рис. 12) в окне "Центра обеспечения безопасности" указывается краткое описание этого режима.

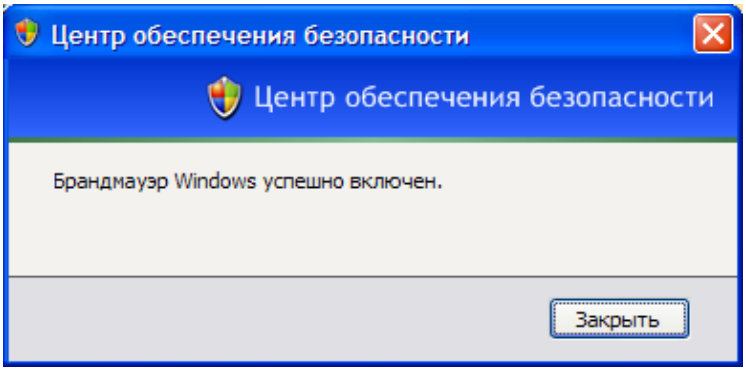


Рис. 10. ***Сообщение.***

На рис. 13 представлено одно из возможных состояний компонента "Защита от вирусов". Нажав кнопку "Рекомендации…", вы получите лаконичные указания (рис. 14): "включить антивирусную программу" (если она выключена), "установить другую антивирусную программу". В этом окне вы можете отключить наблюдение за состоянием этого компонента (параметр "Я самостоятельно устанавливаю и слежу за антивирусом").

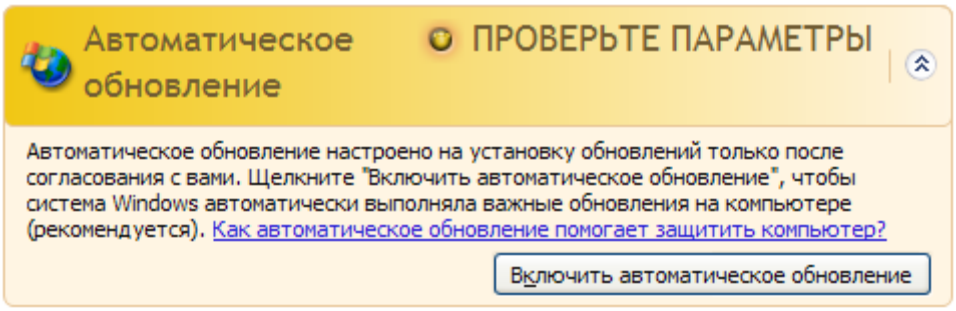


Рис. 11. ***Состояние "Автоматического обновления".***

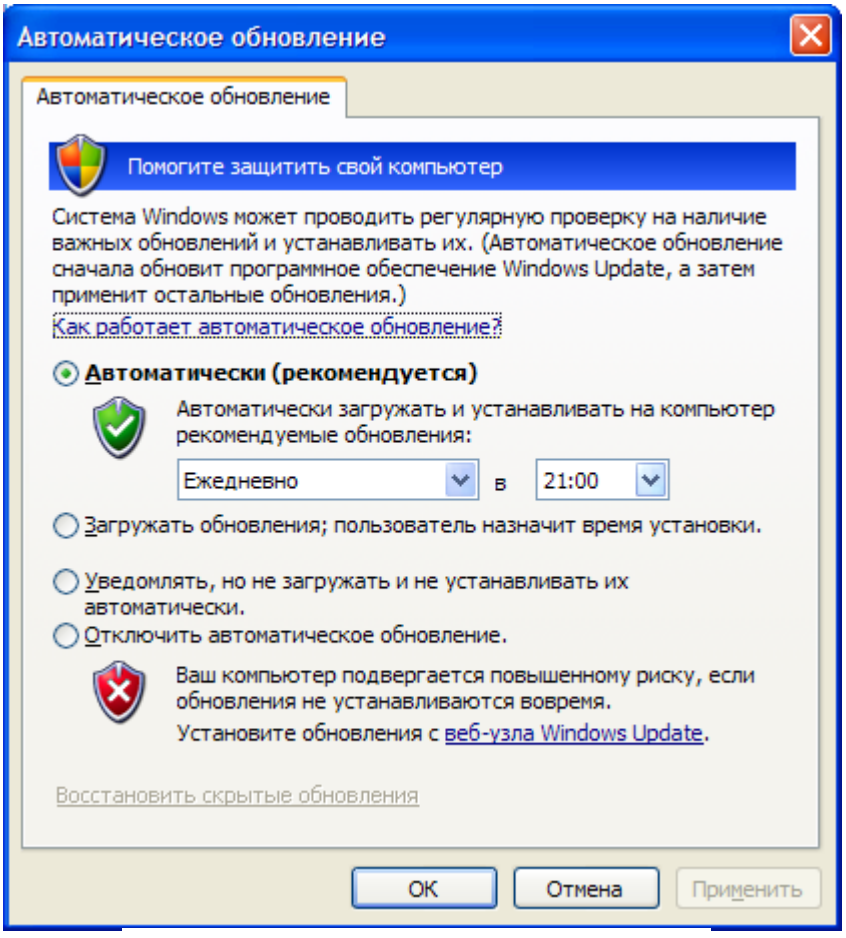


Рис. 12. ***Автоматическое обновление.***

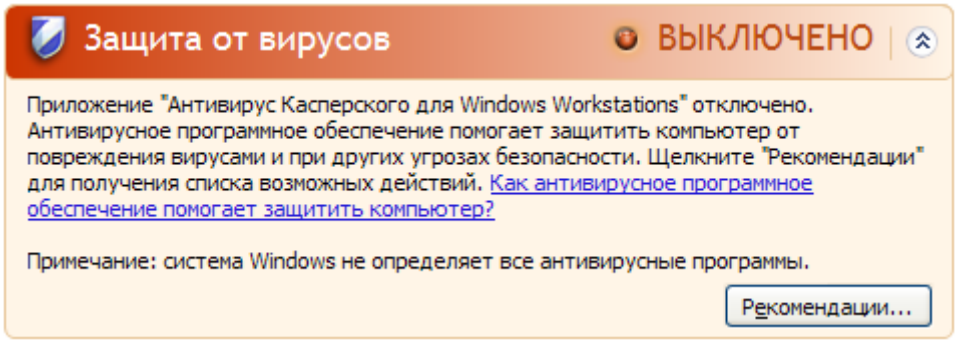


Рис. 13. ***Состояние "Защиты от вирусов".***

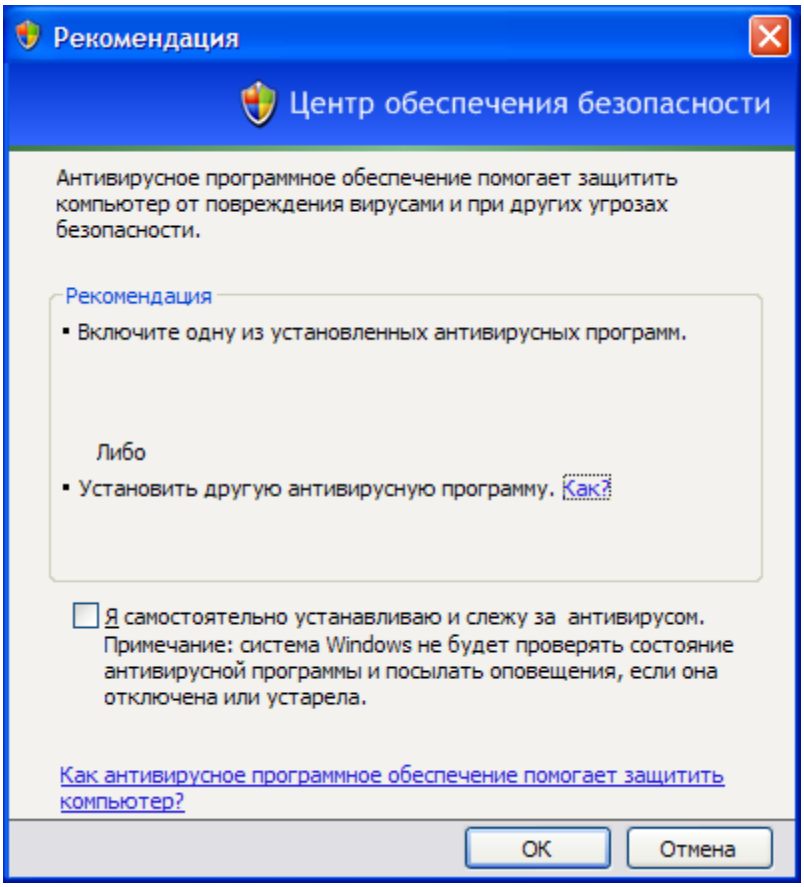


Рис. 14. ***Рекомендация.***

Параметры безопасности

В разделе 3 (см. рис. 5) расположены кнопки перехода к настройкам безопасности следующих компонентов: обозреватель Internet Explorer, автоматическое обновление, брандмауэр Windows.

Нажав кнопку **Свойства обозревателя**, вы попадёте на закладку "Безопасность" в окне настроек обозревателя Internet Explorer (рис. 15).

Нажав кнопку **Автоматическое обновление**, вы откроете окно настроек "Автоматического обновления" (см. рис. 12).

Нажав кнопку **Брандмауэр Windows**, вы попадёте в соответствующее окно настроек (см. рис. 16).

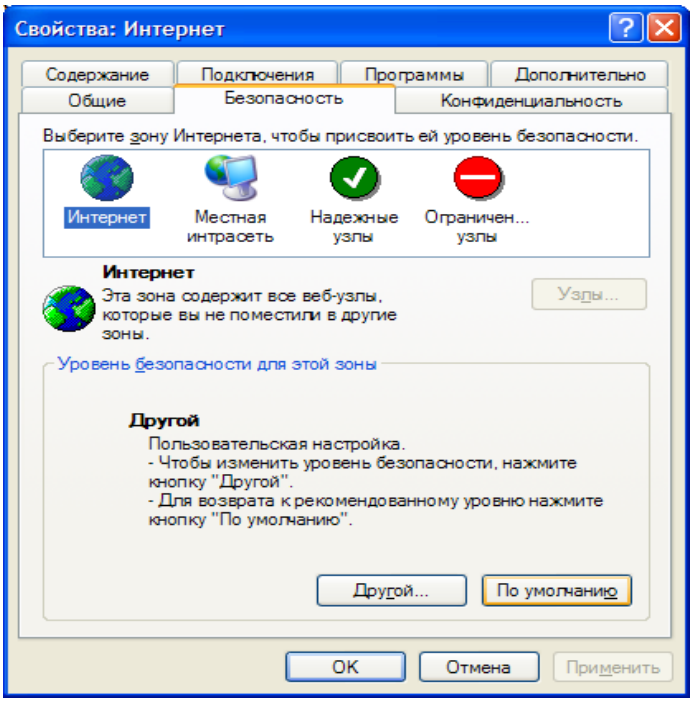


Рис. 15. ***Настройки Internet***

В Windows XP SP2 для обозначения настроек, касающихся безопасности (см. например, рис. 16), а также при оповещениях о состоянии безопасности компьютера (см. например, рис. 2) используются следующие значки:

- Означает важные сведения и параметры безопасности.

- Оповещает о потенциальном риске нарушения безопасности.

- Ситуация более безопасна. На компьютере используются рекомендуемые настройки безопасности.

- Предупреждение: ситуация потенциально опасна. Измените настройки параметров безопасности, чтобы повысить безопасность компьютера.

- Использовать текущие настройки параметров безопасности не рекомендуется.

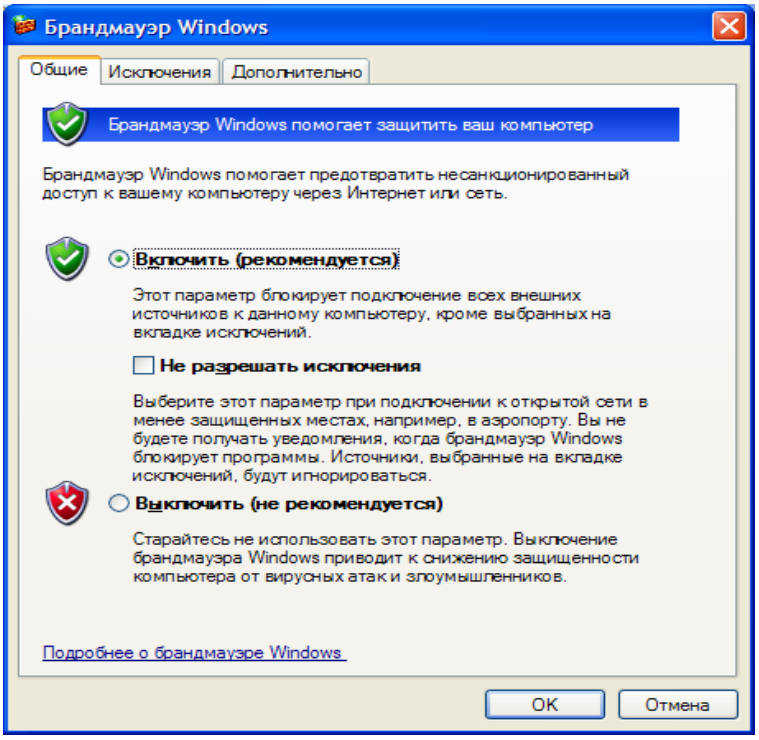


Рис. 16. ***Настройки Брандмауэра***

1.2.2. Свойства обозревателя

Нажав кнопку **Свойства обозревателя** в "Центре обеспечения безопасности Windows", вы попадёте в окно настроек обозревателя Internet Explorer на закладку "Безопасность" (рис. 17).

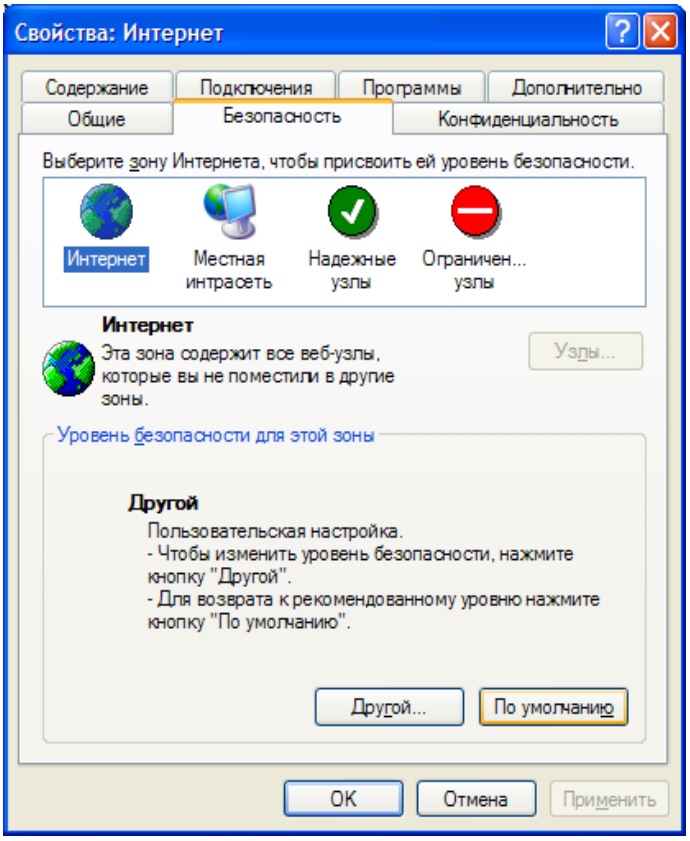


Рис. 17. ***Настройки безопасности***

На этой закладке в верхней части расположены четыре зоны: **Интернет**, **Местная интрасеть**, **Надежные узлы**, **Ограниченные узлы**. В таблице 1 дано описание для каждой зоны.

Для всех зон, кроме зоны "Интернет", вы можете определить входящие в зону узлы. Для этого необходимо выбрать нужную зону (см. рис. 17) и нажать кнопку "Узлы...". Для зоны "Местная интрасеть" в этом случае откроется окно, представленное на рис. 18. Если вы хотите указать конкретные узлы, нажмите кнопку "Дополнительно…". В результате появится окно, представленное на рис. 19. Аналогичное окно будет открыто, если вы будете определять узлы, входящие в зоны "Надежные узлы" и "Ограниченные узлы". Только для зоны "Ограниченные узлы" будет отсутствовать параметр "Для всех узлов этой зоны требуется проверка серверов (https:)".

Таблица 1. ***Описание зон.***

Зона	***Какие узлы может содержать зона***
Интернет	Содержит все веб-узлы, которые не помещены в другие зоны
Местная интрасеть	Может содержать указанные вами узлы. Может содержать все узлы интрасети, не перечисленные в других зонах, все узлы, подключаемые минуя прокси-сервер, все сетевые пути (UNC)
Надежные узлы	Может содержать указанные вами узлы
Ограниченные узлы	Может содержать указанные вами узлы

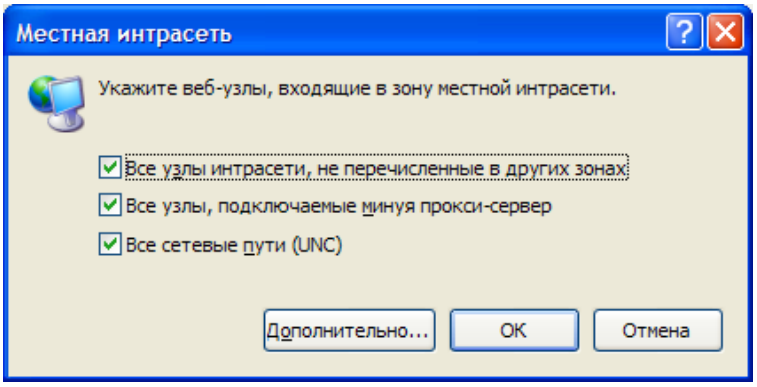


Рис. 18. ***Местная интрасеть.***

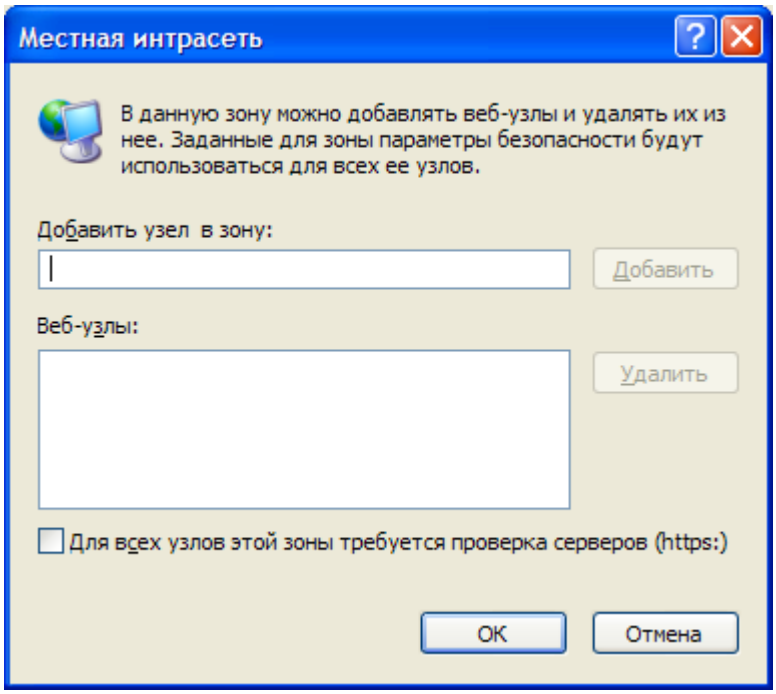


Рис. 19. ***Задание конкретных узлов.***

Каждой зоне можно присвоить нужный уровень безопасности: высокий, средний, ниже среднего, низкий. Низкий уровень безопасности соответствует минимальной защите и применяется для узлов, которым вы полностью доверяете.

Выберите нужную зону (см. рис. 17) и нажмите кнопку "По умолчанию". Закладка "Безопасность" изменит свой вид (рис. 20). В нижней части окна вы можете определить нужный уровень безопасности. Если вы не хотите использовать предлагаемые уровни безопасности, вы можете нажать кнопку "Другой…" и определить все параметры безопасности самостоятельно (рис. 21).

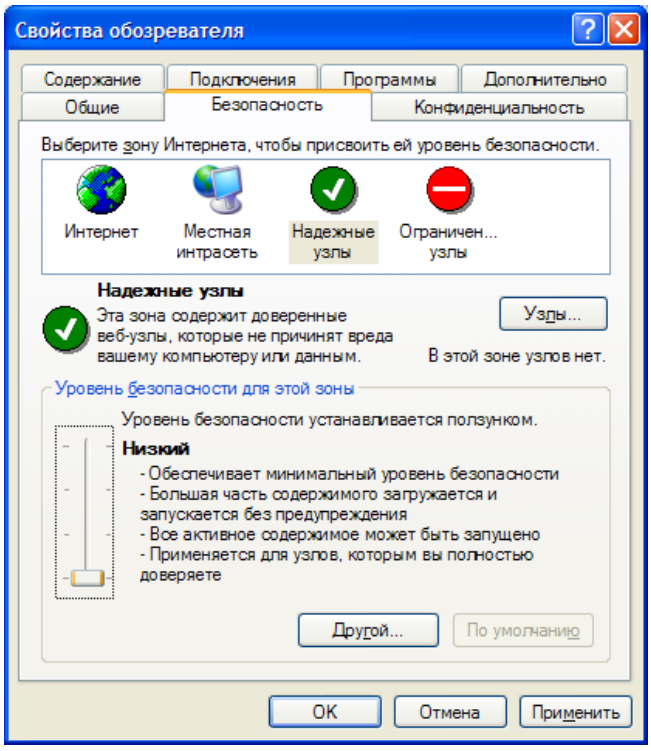


Рис. 20. ***Настройки безопасности*** *Internet Explorer.*

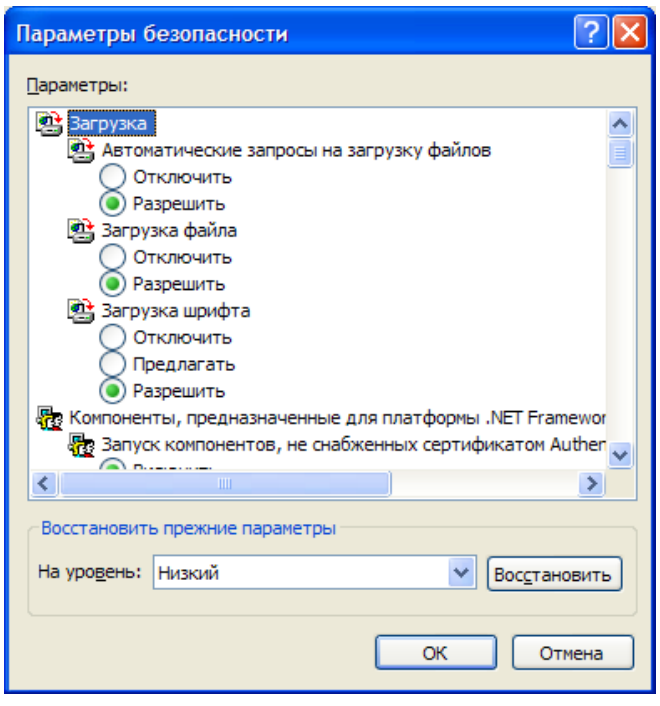


Рис. 21. ***Параметры безопасности.***

Описанные выше настройки безопасности обозревателя Internet Explorer также доступны через групповую политику (Конфигурация компьютера, Административные шаблоны, Компоненты Windows, Internet Explorer, Панель управления обозревателем, Страница безопасности).

1.2.3. Автоматическое обновление

Как уже указывалось ранее, нажав кнопку Автоматическое обновление в "Центре обеспечения безопасности Windows", вы откроете окно настроек "Автоматического обновления" (рис. 22).

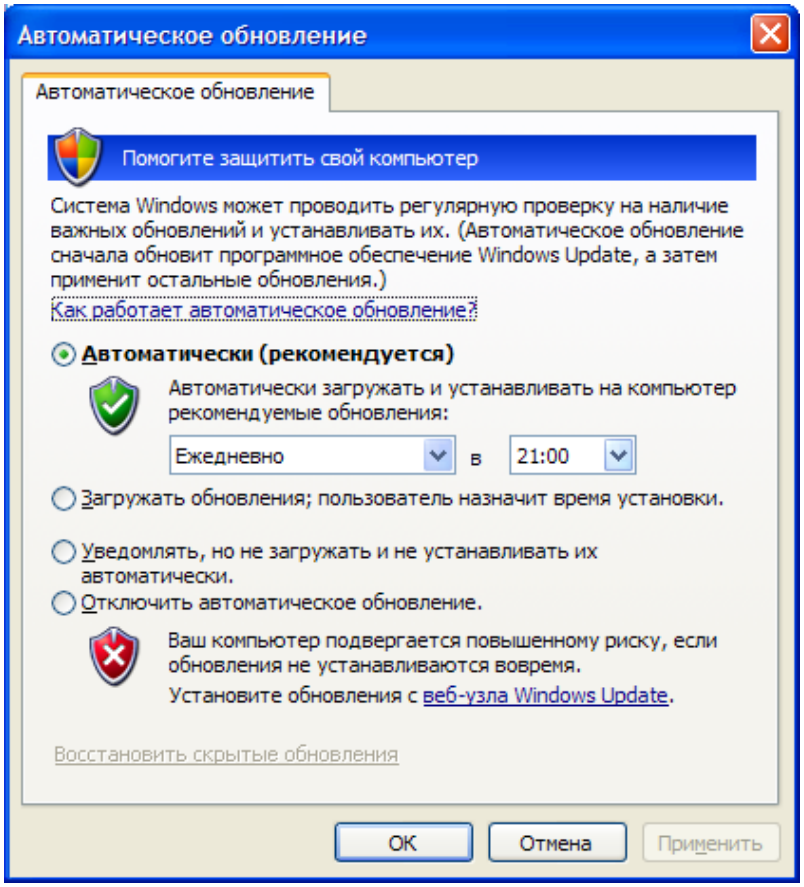


Рис. 22. ***Параметры автоматического обновления.***

Встроенная в Windows XP справочная система очень подробно описывает систему автоматического обновления. Для того чтобы воспользоваться этой справкой, щёлкните по надписи "Как работает автоматическое обновление?" (см. рис. 22). Некоторые моменты его работы, следующие.

Во-первых, необходимо различать понятия "загрузка" и "установка" обновлений. Загрузка означает процесс передачи файлов обновлений с сервера Microsoft (или с внутреннего сервера обновлений в организации) на компьютер пользователя. Установка обозначает собственно процесс инсталляции обновлений на компьютере пользователя. Возможна ситуация, когда обновления загружены на пользовательский компьютер, но еще не установлены.

Во-вторых, если вы выбрали вариант "Автоматически" (см. рис. 22), то обновления будут загружаться и устанавливаться в указанное вами время. Если компьютер в указанное время всегда выключен, то установка обновлений никогда не выполнится. При регистрации на компьютере пользователь с правами локального администратора может запустить установку вручную, не дожидаясь запланированного времени. При наступлении запланированного времени пользователю будет выдано соответствующее предупреждение о начале установки обновлений. Если в этот момент в системе работает администратор, у него будет возможность отложить установку до следующего запланированного времени. У других пользователей (без прав администратора) возможности отменить запланированную установку обновлений не будет.

Во всех остальных случаях (кроме варианта "отключить автоматическое обновление") уведомления о существующих обновлениях для вашего компьютера (готовых к загрузке или к установке) будут появляться только при регистрации на вашем компьютере пользователя с правами локального администратора. Таким образом, если на компьютере вы постоянно работаете с учетной записью, не входящей в группу локальных администраторов, то установка обновлений никогда не выполнится.

Описанные выше настройки автоматического обновления также доступны для настройки через групповую политику (Конфигурация компьютера, Административные шаблоны, Компоненты Windows, Windows Update). Кроме того, только через групповую политику можно задать дополнительные параметры. Например, можно указать адрес внутреннего сервера обновлений, который централизованно получает обновления с серверов Microsoft и отдает их внутренним компьютерам организации. В качестве примера такого сервера можно привести Microsoft® Windows Server™ Update Services (WSUS).

1.2.4. Брандмауэр Windows

Нажав кнопку 

в "Центре обеспечения безопасности Windows", вы откроете окно настроек "Брандмауэра Windows" (рис. 23).

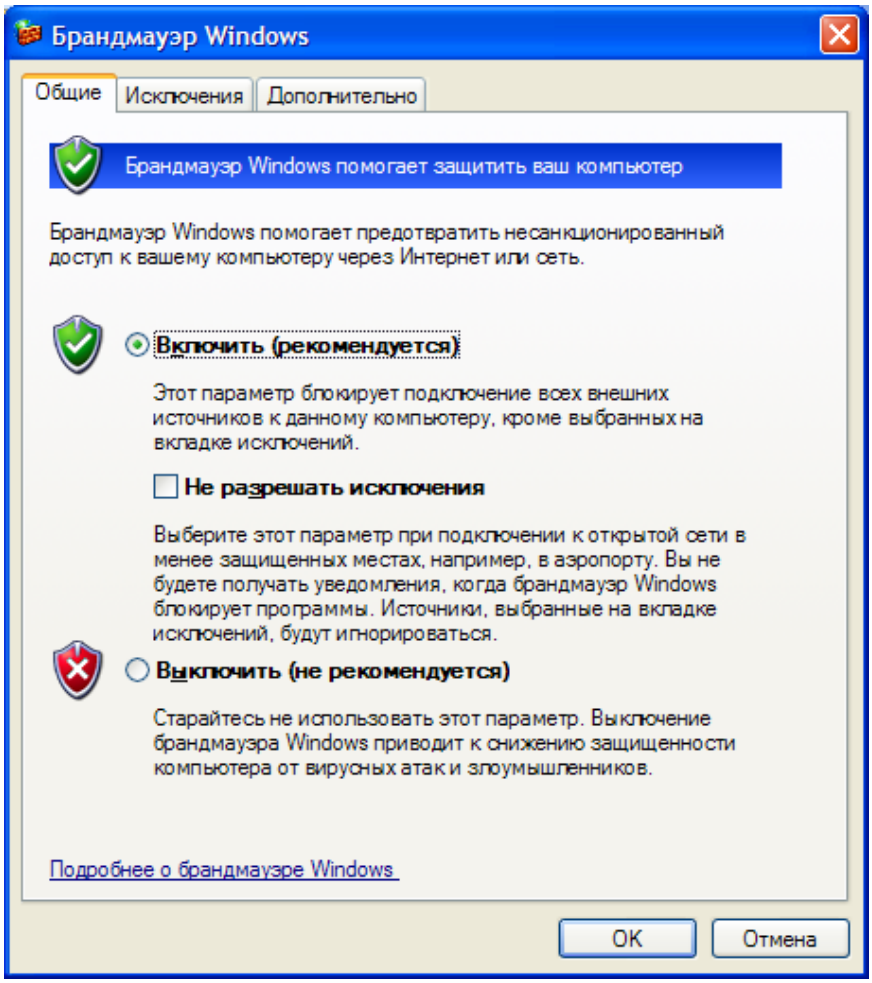


Рис. 23. ***Настройки Брандмауэра Windows.***

Если щёлкнуть по надписи "Подробнее о брандмауэре Windows" (см. рис. 23), то сможете прочитать краткую информацию о возможностях брандмауэра (межсетевого экрана), входящего в состав Windows XP SP2.

В отличие от продуктов других производителей, встроенный брандмауэр Windows предназначен только для контроля входящего трафика, т.е. он защищает компьютер только от внешних вторжений. Он не контролирует исходящий трафик вашего компьютера. Таким образом, если на ваш компьютер уже попал троянский конь или вирус, которые сами устанавливают соединения с другими компьютерами, брандмауэр Windows не будет блокировать их сетевую активность.

Кроме того, по умолчанию брандмауэр защищает все сетевые соединения, и запрос входящего эха по протоколу ICMP запрещен. Это означает, что если на компьютере включен брандмауэр Windows, то проверять личие такого компьютера в сети с помощью команды PING - бессмысленное занятие.

Очень часто в организациях, где используется программное ние, требующее разрешения входящих соединений на пользовательские компьютеры, возникает димость открыть некоторые порты на компьютерах с установленной Windows XP SP2. Для решения этой задачи необходимо задать исключения в настройках брандмауэра Windows. Существует два способа решить эту задачу:

1. Можно задать исключение, указав программу, требующую входящие соединения. В этом случае брандмауэр сам определит, какие порты необходимо открыть, и откроет их только на время выполнения указанной программы (точнее, на время, когда программа будет прослушивать этот порт).
2. Можно задать исключение, указав конкретный порт, по которому программа ожидает входящие соединения. В этом случае порт будет открыт всегда, даже когда эта программа не будет запущена. С точки зрения безопасности этот вариант менее предпочтителен.

Существует несколько собов задать исключение в стройках брандмауэра Windows. Можно воспользоваться графическим интерфейсом (рис. 24). Этот вариант достаточно подробно освещен в Центре справки и поддержки Windows XP SP2. Можно использовать доменную групповую политику. Этот вариант предпочтителен при большом количестве компьютеров в организации. Рассмотрим его более подробно.

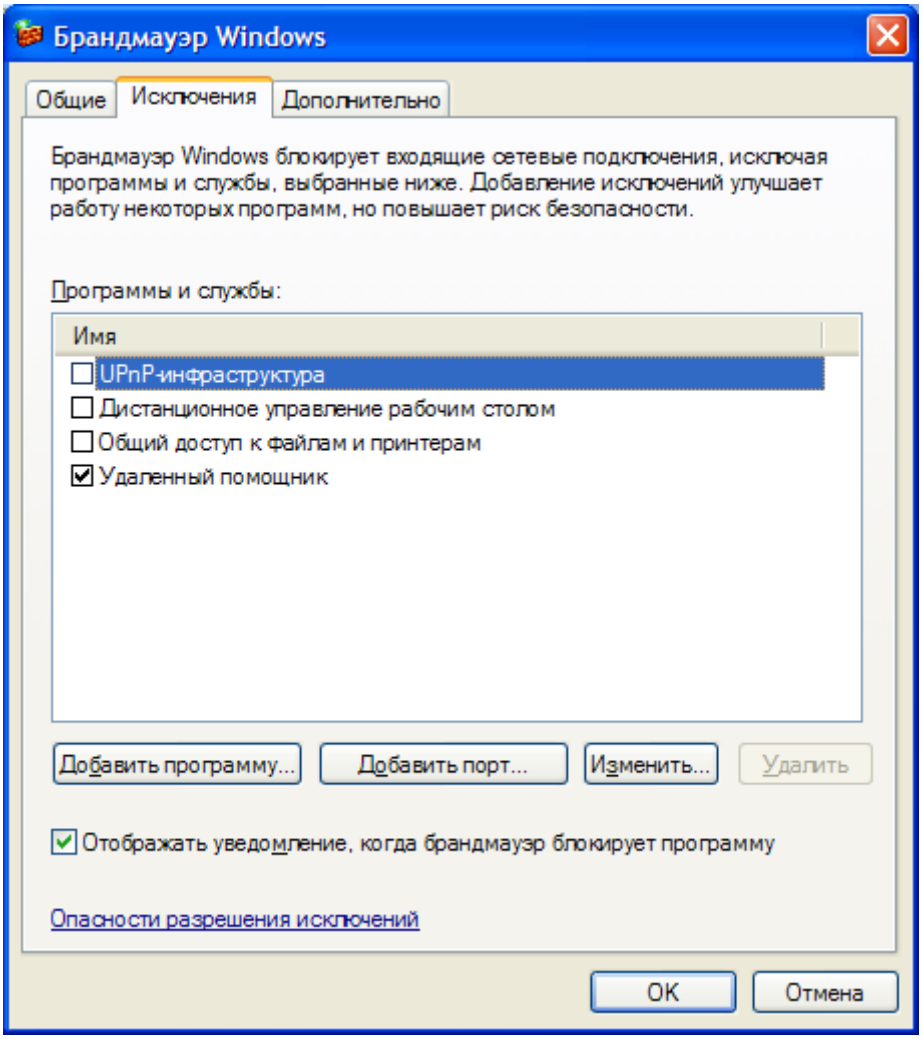


Рис. 24. ***Закладка Исключения.***

Параметры Брандмауэра Windows в групповой политике размещаются в узле "Конфигурация компьютера, Административные шаблоны, Сеть, Сетевые подключения, Брандмауэр Windows".

При настройке через групповую политику вам необходимо настроить два профиля:

1. Профиль домена. Настройки этого профиля используются, когда компьютер подключен к сети, содержащей контроллер домена организации.
2. Стандартный профиль. Настройки этого профиля применяются, когда компьютер не подключен к сети, содержащей контроллер домена организации. Например, если ноутбук организации используется в командировке и подсоединен к Интернету через Интернет-провайдера. В этом случае настройки брандмауэра должны быть более строгими по сравнению с настройками доменного профиля, так как компьютер подключается к публичной сети, минуя межсетевые экраны своей организации.

Рассмотрим, как задать исключения для программы и для заданного порта. В качестве конкретного примера возьмём обращение Сервера администрирования Kaspersky Administration Kit к компьютеру, на котором установлен Агент администрирования, для получения информации о состоянии антивирусной защиты. В этом случае необходимо, чтобы на клиентском компьютере был открыт порт UDP 15000 или разрешен прием входящих сообщений программой "C:\Program Files\Kaspersky Lab\NetworkAgent\klnagent.exe".

Контрольные вопросы

1. Что такое активные компоненты. Какие виды активных компонент могут содержать Web-страницы ?
2. Как осуществляется настройка правил безопасности ?
3. Что собой представляют элементы ActiveX и чем они опасны при работе компьютера в Интернете ?
4. Как можно отключить приём и исполнение элементов ActiveX ?
5. Как можно отключить исполнение других видов активных компонентов Web-страниц ?
6. Как появляются на пользовательском компьютере файлы cookies и где они помещаются. Можно ли избавиться от этих файлов и как?
7. Каково назначение «Центра обеспечения безопасности Windows» ?

8. Как можно открыть «Центр обеспечения безопасности Windows» ?
9. Каково назначение брандмауэра ?
10. Как осуществляются настройки безопасности следующих компонентов: обозревателя Internet Explorer, автоматического обновление, брандмауэра Windows.
11. На что указывает значок  при оповещениях о состоянии безопасности компьютера ?

Лабораторная работа № 3

Компьютерные вирусы и защита от них

Цель работы: ознакомление с антивирусными средствами защиты компьютера; изучение настроек сканера Dr.Web.

1. Вирусы как угроза информационной безопасности

Компьютерные вирусы одна из главных угроз информационной безопасности. Это связано с масштабностью распространения этого явления и, как следствие, огромного ущерба, наносимого информационным системам.

Современный компьютерный вирус – это практически незаметный для обычного пользователя "враг", который постоянно совершенствуется, находя все новые и более изощренные способы проникновения на компьютеры пользователей. Необходимость борьбы с компьютерными вирусами обусловлена возможностью нарушения ими всех составляющих информационной безопасности.

Компьютерные вирусы были и остаются одной из наиболее распространенных причин потери информации. Вирусные эпидемии способны блокировать работу организаций и предприятий.

Борьбой с компьютерными вирусами профессионально занимаются тысячи специалистов в сотнях компаний. Несмотря на огромные усилия конкурирующих между собой антивирусных фирм, убытки, приносимые компьютерными вирусами, не падают и достигают астрономических величин в сотни миллионов долларов ежегодно. Эти оценки явно занижены, поскольку известно становится лишь о части подобных инцидентов.

В последнее время вирусные эпидемии стали настолько масштабными и угрожающими, что сообщения о них выходят на первое место в мировых новостях. При этом следует иметь в виду, что антивирусные программы и аппаратные средства не дают полной гарантии защиты от вирусов, а большинство пользователей не имеют даже основных навыков "защиты" от вирусов.

Основная особенность компьютерных вирусов заключается в возможности их самопроизвольного внедрения в различные объекты операционной системы – присуща многим программам, которые не являются вирусами, но именно эта особенность является обязательным (необходимым) свойством компьютерного вируса. К более полной характеристике современного компьютерного вируса следует добавить способность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети или файлы, системные области компьютера и прочие выполняемые объекты.

Программный вирус – это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах.

1.1. Классификация компьютерных вирусов

По **среде "обитания"** вирусы делятся на:

- *файловые*;
- *загрузочные*;
- *макровирусы*;
- *сетевые*.

Файловые вирусы внедряются в выполняемые файлы (наиболее распространенный тип вирусов), либо создают файлы-двойники (*компаньон-вирусы*), либо используют особенности организации файловой системы (*link-вирусы*).

Загрузочные вирусы записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик жесткого диска (Master Boot Record), либо меняют указатель на активный boot-сектор.

Макровирусы заражают файлы-документы и электронные таблицы популярных офисных приложений.

Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

Существует большое количество сочетаний – например, ***файлово-загрузочные вирусы***, заражающие как файлы, так и загрузочные сектора дисков. Такие вирусы, как правило, имеют довольно сложный алгоритм работы, часто применяют оригинальные методы проникновения в систему, используют стелс- и полиморфик-технологии. Другой пример такого сочетания – ***сетевой макровирус***, который не только заражает редактируемые документы, но и рассылает свои копии по электронной почте.

Заражаемая операционная система является вторым уровнем деления вирусов на классы. Каждый файловый или сетевой вирус заражает файлы какой-либо одной или нескольких OS – DOS, Windows, и т. д. Макровирусы заражают файлы форматов Word, Excel, пакета Office. Загрузочные вирусы также ориентированы на конкретные форматы расположения системных данных в загрузочных секторах дисков.

По **особенностям алгоритма работы** вирусы делятся на:

- *резидентные;*
- *стелс-вирусы;*
- *полиморфик-вирусы;*
- *вирусы, использующие нестандартные приемы.*

Резидентный вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки операционной системы. *Нерезидентные вирусы* не заражают память компьютера и сохраняют активность ограниченное время. К резидентным относятся макровирусы, поскольку они постоянно присутствуют в памяти компьютера на все время работы зараженного редактора. При этом роль операционной системы берет на себя редактор, а понятие "перезагрузка операционной системы" трактуется как выход из редактора.

В многозадачных операционных системах время "жизни" резидентного DOS-вируса также может быть ограничено моментом закрытия зараженного DOS-окна, а активность загрузочных вирусов в некоторых операционных системах ограничивается моментом инсталляции дисковых драйверов ОС.

Использование ***стелс-алгоритмов*** позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным стелс-алгоритмом является перехват запросов операционной системы на чтение/запись зараженных объектов. Стелс-вирусы при этом либо временно лечат их, либо "подставляют" вместо себя незараженные участки информации. В случае макровирусов наиболее популярный способ – запрет вызовов меню просмотра макросов.

Самошифрование и полиморфичность используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуру детектирования (обнаружения) вируса. ***Полиморфик-вирусы*** (*polymorphic*) – это достаточно труднообнаружимые вирусы, не имеющие сигнатур, т. е. не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфик-вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

Различные ***нестандартные приемы*** часто используются в вирусах для того, чтобы как можно глубже спрятать себя в ядре операционной системы, защитить от обнаружения свою резидентную копию, затруднить лечение от вируса (например, поместив свою копию в Flash-BIOS) и т. д.

По **деструктивным возможностям** вирусы можно разделить на:

- ***безвредные***, т. е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);
- ***неопасные***, влияние которых ограничивается уменьшением свободной памяти на диске;
- ***опасные вирусы***, которые могут привести к серьезным сбоям в работе компьютера;
- ***очень опасные***, в алгоритм работы которых заведомо заложены процедуры, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти, и даже повредить аппаратные средства компьютера.

1.2. Виды "вирусоподобных" программ

К **"вредным программам"**, помимо вирусов, относятся:

- «троянские программы» (логические бомбы);
- утилиты скрытого администрирования удаленных компьютеров;
- "intended"-вирусы;
- конструкторы вирусов;
- полиморфик-генераторы.

1.2.1. "Троянские" программы (логические бомбы)

К "троянским" программам относятся программы, наносящие какие-либо разрушительные действия в зависимости от каких-либо условий. Например, уничтожение информации на дисках при каждом запуске или по определенному графику и т. д.

Большинство известных "троянских" программ являются программами, которые маскируются под какие-либо полезные программы, новые версии популярных утилит или дополнения к ним. Очень часто они рассылаются по электронным конференциям. По сравнению с вирусами "троянские" программы не получают широкого распространения по достаточно простым причинам – они либо уничтожают себя вместе с остальными данными на диске, либо демаскируют свое присутствие и уничтожаются пострадавшим пользователем.

К "троянским" программам также относятся так называемые *"дропперы" вирусов* – зараженные файлы, код которых подправлен таким образом, что известные версии антивирусов не определяют присутствие вируса в файле. Например, файл шифруется или упаковывается неизвестным архиватором, что не позволяет антивирусу "увидеть" заражение.

Еще один тип программ (программы – *"злые шутки"*), которые используются для устрашения пользователя, о заражении вирусом или о каких либо предстоящих действиях с этим связанных, т. е. сообщают о несуществующих опасностях, вынуждая пользователя к активным действиям. Например, к "злым шуткам" относятся программы, которые "пугают" пользователя сообщениями о форматировании диска (хотя никакого форматирования на самом деле не происходит), детектируют вирусы в незараженных файлах, выводят странные вирусоподобные сообщения и т. д. К категории "злых шуток" можно отнести также заведомо ложные сообщения о новых "супер-вирусах". Такие сообщения периодически появляются в Интернете и обычно вызывают панику среди пользователей.

1.2.2. Утилиты скрытого администрирования

Утилиты скрытого администрирования являются разновидностью "логических бомб" ("троянских программ"), которые используются злоумышленниками для удаленного администрирования компьютеров в сети. По своей функциональности они во многом напоминают различные системы администрирования, разрабатываемые и распространяемые различными фирмами-производителями программных продуктов. Единственная особенность этих программ заставляет классифицировать их как вредные "троянские" программы: отсутствие предупреждения об инсталляции и запуске. При запуске такая программа устанавливает себя в систему и затем следит за ней, при этом пользователю не выдается никаких сообщений о действиях программы в системе. Чаще всего ссылка на такую программу отсутствует в списке активных приложений. В результате пользователь может и не знать о ее присутствии в системе, в то время как его компьютер открыт для удаленного управления.

Внедренные в операционную систему утилиты скрытого управления позволяют делать с компьютером все, что в них заложил их автор: принимать/отсылать файлы, запускать и уничтожать их, выводить сообщения, стирать информацию, перезагружать компьютер и т. д. В результате эти программы могут быть использованы для обнаружения и передачи конфиденциальной информации, для запуска вирусов, уничтожения данных и т. п.

1.2.3. "Intended"-вирусы

К *Intended-вирусам* относятся программы, которые, на первый взгляд, являются стопроцентными вирусами, но не способны размножаться по причине ошибок. Например, вирус, который при заражении не помещает в начало файла команду передачи управления на код вируса, либо записывает в нее неверный адрес своего кода, либо неправильно устанавливает адрес перехватываемого прерывания (в большинстве приводит к "зависанию" компьютера) и т. д. К категории "intended" также относятся вирусы, которые по приведенным выше причинам размножаются только один раз – из "авторской" копии. Заразив какой-либо файл, они теряют способность к дальнейшему размножению. Появляются "intended"-

вирусы чаще всего из-за неумелой перекомпиляции какого-либо уже существующего вируса, либо по причине недостаточного знания языка программирования, либо по причине незнания технических тонкостей операционной системы.

1.2.4. Конструкторы вирусов

К данному виду "вредных" программ относятся утилиты, предназначенные для изготовления новых компьютерных вирусов. Известны ***конструкторы вирусов*** для DOS, Windows и макровирусов. Они позволяют генерировать исходные тексты вирусов, объектные модули, и/или непосредственно зараженные файлы. Некоторые конструкторы снабжены стандартным оконным интерфейсом, где при помощи системы меню можно выбрать тип вируса, поражаемые объекты (COM и/или EXE), наличие или отсутствие самошифровки, противодействие отладчику, внутренние текстовые строки, выбрать эффекты, сопровождающие работу вируса и т. п.

1.2.5. Полиморфные генераторы

Полиморфик-генераторы, как и конструкторы вирусов, не являются вирусами в прямом смысле этого слова, поскольку в их алгоритм не закладываются функции размножения, т. е. открытия, закрытия и записи в файлы, чтения и записи секторов и т. д. Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика. Обычно полиморфные генераторы распространяются в виде файла-архива. Основным файлом в архиве любого генератора является объектный модуль, содержащий этот генератор.

2. Антивирусные программы

Одним из наиболее эффективных способов борьбы с вирусами является использование антивирусного программного обеспечения. **Антивирусная программа** – программа, предназначенная для поиска, обнаружения, классификации и удаления компьютерного вируса и вирусоподобных программ.

Однако не существует антивирусов, гарантирующих стопроцентную защиту от вирусов, поскольку на любой алгоритм антивируса всегда можно предложить новый алгоритм вируса, невидимого для этого антивируса.

При работе с антивирусными программами необходимо знать некоторые понятия:

Ложное срабатывание – детектирование вируса в незараженном объекте (файле, секторе или системной памяти).

Пропуск вируса – недетектирование вируса в зараженном объекте.

Сканирование по запросу – поиск вирусов по запросу пользователя. В этом режиме антивирусная программа неактивна до тех пор, пока не будет вызвана пользователем из командной строки, командного файла или программы-расписания.

Сканирование на лету – постоянная проверка на вирусы объектов, к которым происходит обращение (запуск, открытие, создание и т. п.). В этом режиме антивирус постоянно активен, он присутствует в памяти "резидентно" и проверяет объекты без запроса пользователя.

2.1. Классификация антивирусных программ

Самыми популярными и эффективными антивирусными программами являются *антивирусные сканеры*, *CRC-сканеры* (*ревизоры*). Существуют также антивирусы *блокировщики* и *иммунизаторы*.

Сканеры. Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются так называемые "маски". Маской вируса является некоторая постоянная последовательность кода, специфичная для этого конкретного вируса. Если вирус не содержит постоянной маски или длина этой маски недостаточно велика, то используются другие методы. Примером такого метода является алгоритмический язык, описывающий все возможные варианты кода, которые могут встретиться при заражении подобного типа вирусом. Такой подход используется некоторыми антивирусами для детектирования полиморфик-вирусов.

Во многих сканерах используются также алгоритмы "эвристического сканирования", т. е. анализ последовательности команд в проверяемом объекте, набор некоторой статистики и принятие решения для каждого проверяемого объекта. Поскольку эвристическое сканирование является во многом вероятностным методом поиска вирусов, то на него распространяются многие законы теории вероятностей. Например, чем выше процент обнаруживаемых вирусов, тем больше количество ложных срабатываний.

Сканеры также можно разделить на две категории – *универсальные* и *специализированные*.

Универсальные сканеры рассчитаны на поиск и обезвреживание всех типов вирусов вне зависимости от операционной системы, на работу в которой рассчитан сканер.

Специализированные сканеры предназначены для обезвреживания ограниченного числа вирусов или только одного их класса, например макровирусов.

Сканеры также делятся на:

- *резидентные* (*мониторы*), производящие сканирование "на лету" и обеспечивающие более надежную защиту системы, поскольку они немедленно реагируют на появление вируса;
- *нерезидентные*, обеспечивающие проверку системы только по запросу и способные опознавать вирус только во время своего очередного запуска.

К достоинствам сканеров всех типов относится их универсальность, к недостаткам – размеры антивирусных баз, которые сканерам приходится хранить и пополнять, и относительно небольшая скорость поиска вирусов.

CRC-сканеры. Принцип работы CRC-сканеров основан на подсчете CRC-сумм (контрольных сумм) для присутствующих на диске файлов/системных секторов. Эти CRC-суммы затем сохраняются в базе данных антивируса, как, впрочем, и некоторая другая информация: длины файлов, даты их последней модификации и т. д. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменен или заражен вирусом.

CRC-сканеры, использующие "анти-стелс" алгоритмы реагируют практически на 100 % вирусов сразу после появления изменений на компьютере. Характерный недостаток этих антивирусов заключается в невозможности обнаружения вируса с момента его появления и до тех пор, пока не будут произведены изменения на компьютере. CRC-сканеры не могут определить вирус в новых файлах (в электронной почте, на дискетах, в восстанавливаемых файлах или при распаковке файлов из архива), поскольку в их базах данных отсутствует информация об этих файлах.

Блокировщики. Антивирусные блокировщики – это резидентные программы, перехватывающие "вирусоопасные" ситуации и сообщающие об этом пользователю. К "вирусоопасным" относятся вызовы на открытие для записи в выполняемые файлы, запись в загрузочный сектор диска и др., которые характерны для вирусов в моменты из размножения.

К достоинствам блокировщиков относится их способность обнаруживать и блокировать вирус на самой ранней стадии его размножения, что, кстати, бывает очень полезно в случаях, когда давно известный вирус постоянно активизируется.

Иммунизаторы. Иммунизаторы делятся на два типа: иммунизаторы, сообщающие о заражении, и иммунизаторы, блокирующие заражение каким-либо типом вируса.

2.2. Факторы, определяющие качество антивирусных программ

По степени важности качество антивирусной программы определяется следующими факторами:

1. Надёжность и удобство работы – отсутствие "зависаний" антивируса и прочих технических проблем, требующих от пользователя специальной подготовки.
2. Качество обнаружения вирусов всех распространенных типов, сканирование внутри файлов-документов/таблиц, упакованных и архивированных файлов. Отсутствие "ложных срабатываний". Возможность лечения зараженных объектов.
3. Существование версий антивируса под все популярные платформы (DOS, Windows, Linux и т. д.).
4. Возможность сканирование "налету".
5. Существование серверных версий с возможностью администрирования сети.
6. Скорость работы.

3. Обзор популярных антивирусных программ

Практически все программы, упомянутые в этом обзоре, просты и удобны в пользовании, способны отлавливать практически все существующие сегодня группы вирусов (за исключением «троянцев», отлавливать которых способны лишь немногие антивирусные пакеты).

Большинство антивирусов способны не просто проверять по запросу пользователя диск на наличие вирусов, но и вести незаметную проверку всех запускаемых на компьютере файлов. Наконец, все совре-

менные антивирусы снабжены механизмом автоматического обновления антивирусных баз данных через Интернет.

3.1. Антивирус Касперского

Сайт: http://www.kav.ru
Размер: 12 Мб
Статус: Платная
Цена: $50 (Personal и Lite)
$70 (Personal Pro) (лицензия на 1 год)
$1 в месяц (подписка на Lite)

Это самый популярный и мощный из отечественных антивирусов, да и на мировой антивирусной сцене он котируется весьма высоко. Программа подстроена под российскую «вирусную атмосферу» и способна дать отпор вирусам отечественного производства. Антивирус Касперского способен обезвреживать не только классические вирусы и «троянцев», но и рекламные и шпионские модули. Антивирусная база KAV насчитывает около 53 тысяч вирусов, при этом новые дополнения к программе выпускаются ежедневно и могут быть автоматически скачаны из Интернета.

Версия KAV Personal Pro состоит из нескольких важных модулей:

- *Scanner*, проверяющий жесткие диски на предмет зараженности вирусами. Можно задавать различные режимы проверки: полный поиск, режим проверки архивированных файлов, по формату, маске.
- *Monitor* - программа автоматически загружаемая при запуске Windows и доступная через иконку в левой части Панели задач. Монитор автоматически проверяет все запускаемые на компьютере файлы и открываемые документы и в случае вирусной атаки подает сигнал тревоги. В большинстве случаев Монитор не дает зараженному файлу запуститься, блокируя процесс его выполнения.
- *Инспектор* – модуль, позволяющий отлавливать неизвестные вирусы.
- *Mail Checker* – модуль, отвечающий за проверку «на лету» сообщений электронной почты.
- *Script Checker* – охотник за вирусными и троянскими скриптами.
- *Office Guard* – модуль для проверки каждого загружаемого документа Microsoft Office.
- *Центр управления* – «пульт управления» всеми программами комплекса «Антивирус Касперского».

Однако назвать «Антивирус Касперского» идеальным антивирусом для дома мешает его громоздкость и медлительность.

3.2. NOD32

Сайт: http://www.esetnod32.ru
Размер: 8 Мб
Статус: Платная
Цена: $40

Этот французский антивирус уже давно стал культовым в кругах опытных пользователей – его предпочитают за высокую скорость работы, малый размер, стабильность и надежность работы.

Ключевые возможности программы:

- Простой в использовании графический пользовательский интерфейс.
- Интеграция в контекстные меню Windows Explorer, что обеспечивает возможность быстрой проверки файлов или каталогов с помощью нажатия на правую клавишу мыши.
- Сканирует оперативную память и проверяет собственную целостность.
- Лечит, удаляет и перемещает в карантинную область зараженные объекты.
- Удаляет заражения из заблокированных на запись файлов.
- Удаляет вирусы, червей и «троянцев». Последние версии способны выявлять рекламные и «шпионские» модули (adware и spyware).
- Сканирует почтовые базы Outlook и Outlook Express.
- Имеет возможность запуска по расписанию с помощью различных пользовательских профилей.
- Содержит детальные, интерактивные подсказки.

3.3. AVAST

Сайт: http://www.avast.ru
Размер: 3 Мб
Статус: Бесплатная

Это один из «домашних» вариантов антивирусных пакетов с русским интерфейсом. Он отстает от коммерческих антивирусов лишь в области работы со скриптами, adware и spyware. Но от самых распространенных вирусов он спасает, в том числе и от тех, что распространяются через электронную почту, Интернет-пейджеры и файло-обменные системы. К тому же он быстр и занимает не много места в памяти. Словом - отличная аптечка на тот случай, если более умелого «доктора» по каким-то причинам не найдется под рукой.

3.4. AVG Antivirus

Сайт: http://www.grisoft.com
Размер: 10 Мб
Статус: Бесплатная

Это чешский антивирус, у которого русский интерфейс отсутствует, к тому же базы данных антивируса необходимо обновлять вручную (это сводится к нажатию кнопки «Обновить»). Зато уровень защиты у этой программы достаточно высок: напрочь отсекает от системы классические вирусы, популярные «ирояны» и даже кое-что из spyware-модулей.

AVG Antivirus отличается скромными требованиями, что делает его идеальным антивирусом для ноутбуков.

3.5. Dr.Web

Сайт: http://www.drweb.ru
Размер: 4 Мб
Статус: Платная
Цена: $20-45 (годовая подписка)

Это разработка лаборатории Игоря Данилова. Этот «вечно второй» продукт после «Антивируса Касперского» может предложить не худший уровень защиты.

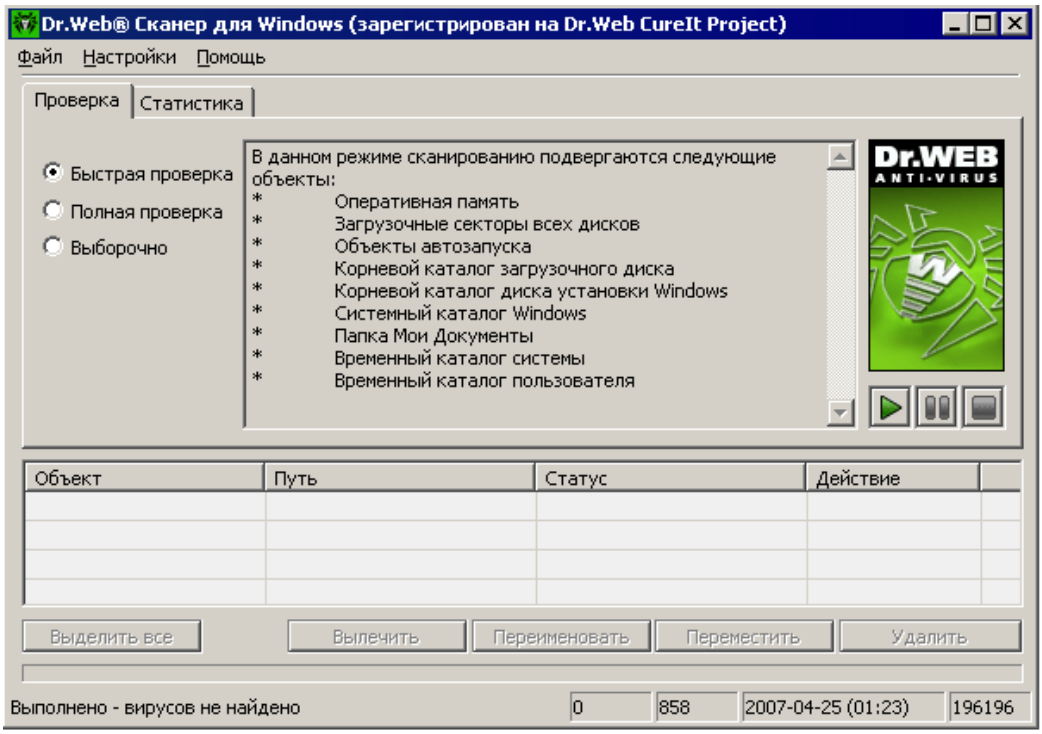
Антивирусная база Dr.Web почти вдвое меньше, чем у KAV (около 30 тысяч записей). Однако на результатах тестирования это не сказывается, поскольку в Dr.Web реализован принципиально иной подход, чем в его коллегах-антивирусах: в программу встроен модуль эвристического анализатора, который позволяет обезвредить не только уже известные программе и занесенные в базу данных, но и новые, еще не опознанные вирусы.

Dr.Web содержит следующие модули:

- *Сканер Dr. Web* (с графическим интерфейсом), запускаемый по запросу пользователя или по расписанию. Сканирует выбранные объекты (определенные файлы, каталоги, диски, сменные носители информации), при этом по умолчанию после своего запуска всегда проверяет оперативную память и файлы автозагрузки.
- *Сканер для среды DOS* и режима командной строки Windows (без графического интерфейса), позволяющий произвести инсталляцию и проверку компьютера даже в случае неработоспособности Windows, обеспечивая при этом еще более высокий уровень обнаружения вирусов.
- *SpIDer Guard* - резидентный монитор антивируса, постоянно находящийся в оперативной памяти и предотвращающий всевозможную вирусную активность. Единственное, нужно сразу заметить, что по умолчанию производится проверка только открываемых файлов.
- *SpIDer Mail* - почтовый антивирусный фильтр, также постоянно находящийся в памяти и контролирующий почтовые сообщения пользователя (поддержка протоколов POP3/SMTP/IMAP4/NNTP). Обнаруживает и обезвреживает почтовые вирусы еще до получения (или отправки) письма почтовым клиентом.
- *Планировщик заданий* - отвечает за регулярные действия (обновления вирусных баз, сканирование дисков компьютера по расписанию).
- *Модуль автоматического обновления* (устанавливается в обязательном порядке) для самостоятельной загрузки и установки дополнений к вирусным базам и обновлений антивирусных компонентов.
- *Карантинное отделение* - папка, куда помещаются все объекты, для которых было выбрано действие "переместить" (по умолчанию это подкаталог 'infected.!!!' в каталоге Dr.WEB).

3.5.1. Сканер Dr.Web

Главное окно сканера. Вкладка проверка



В главном окне сканера (см. рисунок выше) формируется задание на сканирование (вкладка **Проверка**), а также предоставляется доступ к итоговым сведениям о работе сканера (вкладка **Статистика**).

В центральной части окна в зависимости от выбора *режима сканирования* отображается список объектов, которые будут подвергнуты проверке, либо иерархический список файловой системы.

В нижней части окна располагается таблица для отображения сведений о найденных в ходе сканирования зараженных и подозрительных объектах, а также о произведенных программой действиях.

Кроме кнопок и пунктов меню для доступа к различным окнам, настройкам и функциям предусмотрены следующие *клавиши быстрого доступа*:

F1 – открытие справки;
F3 – в главном окне переход на вкладку **Проверка**;
F4 – в главном окне переход на вкладку **Статистика**;
F5 – открытие окна **Путь и маска проверки**;
F7 – запуск процесса сканирования оперативной памяти;

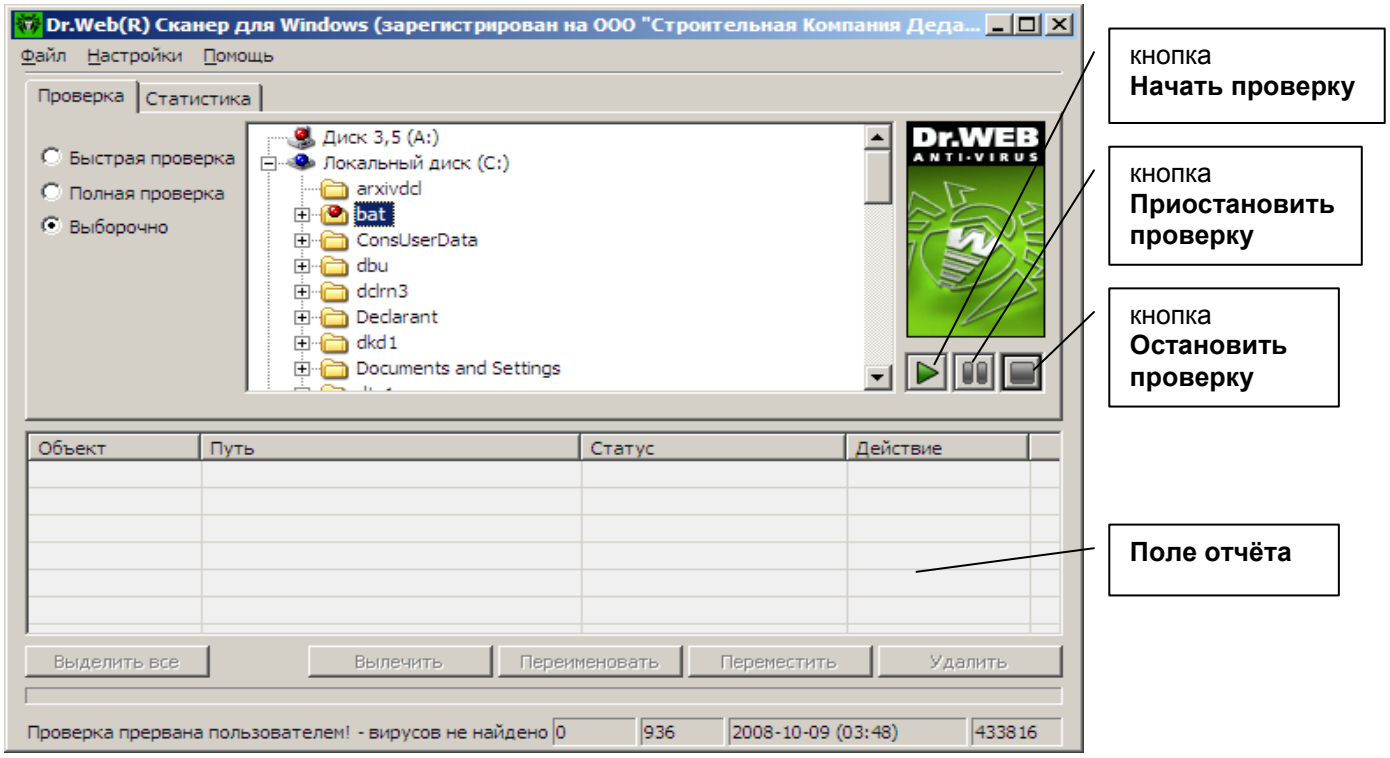
F8 – запуск процесса обновления;
F9 – открытие окна с вкладками настроек сканера;
F10 – перевод фокуса на меню **Файл**;
Ctrl + F5 – запустить процесс сканирования;
Ctrl + F6 – остановить процесс сканирования.

Антивирусная проверка (сканирование) файловой системы

При работе под управлением ОС Windows Vista рекомендуется запускать сканер от имени пользователя, обладающим правами администратора. В противном случае те файлы и папки, к которым непривилегированный пользователь не имеет доступа (в том числе и системные папки) не будут подвергнуты проверке.

Немедленно после запуска программа при настройках по умолчанию проводит антивирусное сканирование оперативной памяти и файлов автозапуска Windows.

Проверка остальных объектов файловой системы производится по вашему запросу. Выберите один из следующих режимов антивирусного сканирования:



Быстрая проверка

В данном режиме производится сканирование следующих объектов:

- оперативной памяти;
- загрузочных секторов всех дисков;
- объектов автозапуска;
- корневого каталога загрузочного диска;
- корневого каталога диска установки Windows;
- системного каталога Windows;
- папки **Мои документы**;
- временного каталога системы;
- временного каталога пользователя.

Полная проверка

В данном режиме производится полное сканирование всех жестких дисков и сменных носителей (включая загрузочные секторы).

Выборочно

Данный режим предоставляет возможность выбрать любые папки и файлы для последующего сканирования.

При выборе данного режима в центральной части вкладки **Проверка** будет представлена файловая система в виде иерархического дерева. При необходимости его можно развернуть вплоть до каталогов любого уровня и файлов в них.

Наряду с выбранными для сканирования в иерархическом списке объектами будут подвергнуты проверке и загрузочные секторы всех дисков.

На рисунке ниже изображена ситуация, в которой в режиме **Выборочно** выбран для сканирования весь логический диск C: и одна из папок на дискете.

Для того чтобы приступить к сканированию, нажмите на кнопку **Начать проверку**  в правой части окна.

Для того чтобы приостановить проверку, нажмите на кнопку **Приостановить проверку**  . Чтобы продолжить проверку нажмите на кнопку  .

Чтобы остановить проверку, нажмите на кнопку **Остановить проверку**  .

По умолчанию программа производит антивирусное сканирование всех файлов с использованием как вирусных баз, так и эвристического анализатора (алгоритм, позволяющий с большой вероятностью обнаруживать неизвестные программе вирусы на основе общих принципов их создания). Исполняемые файлы, упакованные специальными упаковщиками, при проверке распаковываются, проверяются файлы в архивах всех основных распространенных типов (Zip, Arj, Lha, Rar и многих других), файловых контейнерах (PowerPoint, RTF и других), а также файлы в составе писем в почтовых ящиках почтовых программ (формат писем должен соответствовать RFC822).

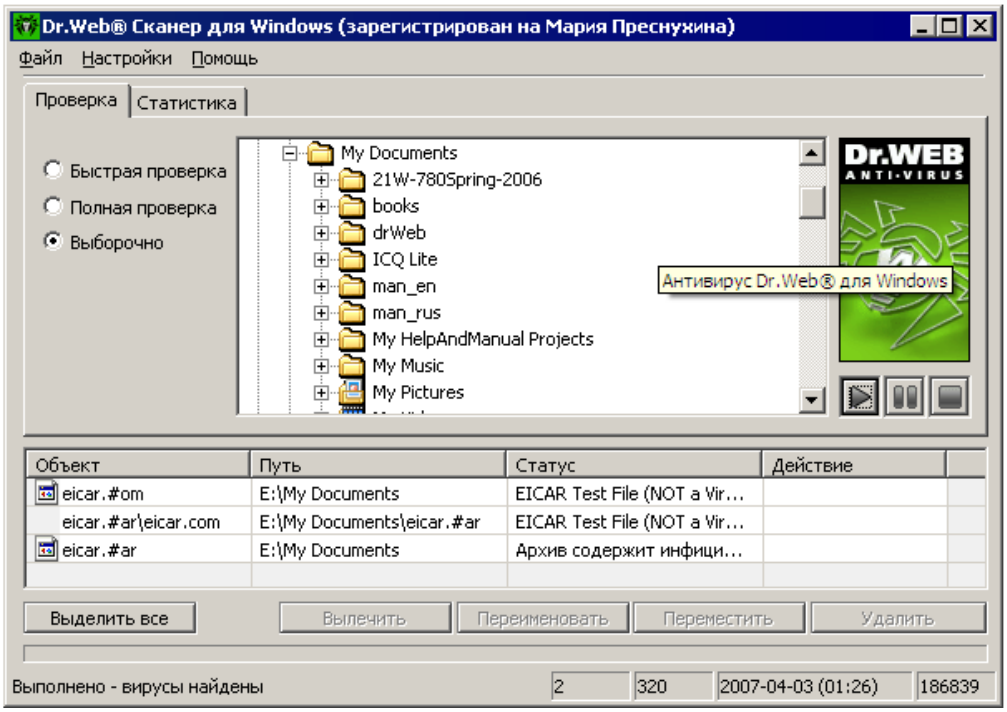
Версия Dr.Web для рабочих станций в случае обнаружения известного вируса или при подозрении на зараженность объекта вирусом по умолчанию информирует пользователя об этом в специальном *поле отчета*, расположенном в нижней части окна (см. рисунок выше).

Dr.Web для серверов Windows по умолчанию предпринимает автоматические действия по предотвращению вирусной угрозы.

Действия при обнаружении вирусов

Версия Dr.Web для рабочих станций в случае обнаружения известного вируса или при подозрении на зараженность объекта вирусом по умолчанию информирует пользователя об этом в специальном поле отчета, расположенном в нижней части окна. Dr.Web для серверов Windows по умолчанию предпринимает автоматические действия по предотвращению вирусной угрозы.

В поле отчета (см. рисунок ниже) в табличной форме представляются сведения о найденных в ходе сканирования зараженных и подозрительных объектах, а также о произведенных программой действиях. Если указанные объекты обнаружены в файловых архивах, почтовых файлах или файловых контейнерах, в таблице приводятся как инфицированные объекты, так и содержащие их архивы.



Колонка таблицы **Объект** содержит наименование инфицированного файла или загрузочного сектора.

Колонка **Путь** содержит путь к инфицированному объекту.

Колонка **Статус** содержит условное наименование вируса (для файлов и загрузочных секторов) или сообщение об инфицированности архива.

Колонка **Действие** содержит сообщение о выполненных действиях (излечении, удалении, переименовании или перемещении объекта).

При обнаружении зараженного или подозрительного файла, используемого другим 32-битным приложением Windows, выбранное вами действие не может быть выполнено немедленно. В поле отчета сканера в колонке **Действие** в этом случае появляется запись "Будет излечен после рестарта", "Будет удален после рестарта" и т. п. в зависимости от выбранного действия. Соответственно только при последующей перезагрузке нужное действие и будет реально выполнено. Поэтому при обнаружении таких объектов рекомендуется провести перезагрузку системы сразу после окончания сканирования.

Вы можете предписать программе действия по устранению вирусной угрозы, отображенной в отчете. Для этого щелкните правой клавишей мыши по строке списка отчета, содержащей описание зараженного объекта. Для выделения объектов в списке отчета дополнительно используются следующие клавиши и комбинации клавиш:

- *Insert* – выделить объект с перемещением курсора на следующую позицию
- *Ctrl+A* – выделить все
- клавиша * на цифровой клавиатуре – инвертировать выделение

Выберите действие, которое вы хотите предпринять, в открывшемся контекстном меню или нажмите на соответствующую кнопку под полем отчета:

Вылечить — восстановить состояние объекта до заражения. Данное действие возможно только при обнаружении известных вирусов, и то не всегда. Действие невозможно при обнаружении вируса в архиве.

Удалить — удалить инфицированный объект. Невозможно, если вирус обнаружен в загрузочном секторе.

Переименовать — изменить расширение имени файла в соответствии с настройками программы. Невозможно, если вирус обнаружен в загрузочном секторе.

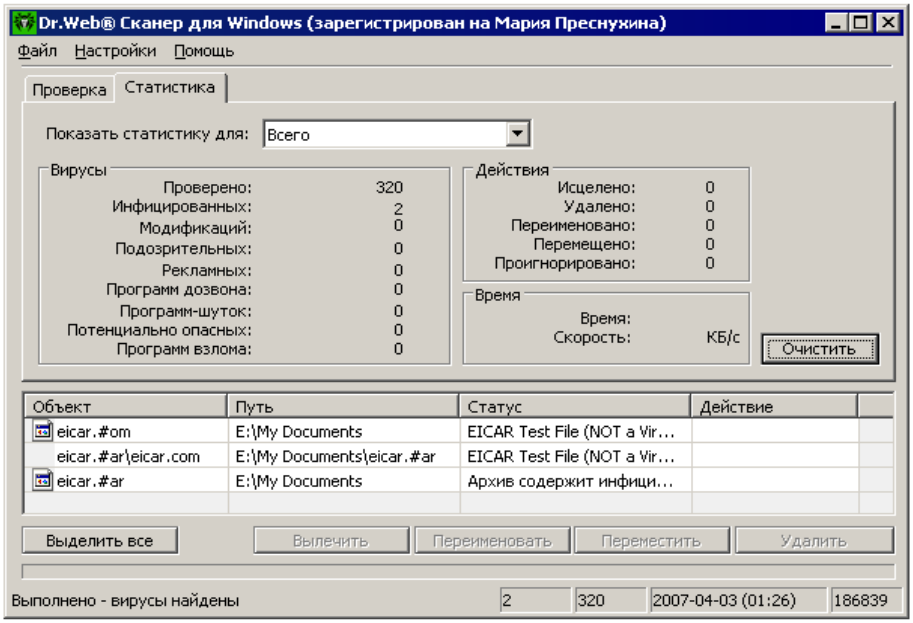
Переместить — переместить инфицированный файл в специальный каталог (карантин). Путь к каталогу задается настройками программы. Невозможно, если вирус обнаружен в загрузочном секторе.

Если вы выбрали вариант **Вылечить**, откроется дополнительное контекстное меню, в котором необходимо выбрать реакцию программы в случае неудачного лечения.

По умолчанию при выборе действия **Удалить** для файловых архивов, контейнеров или почтовых ящиков программа выдает предупреждение о возможной потере данных.

Для файлов внутри архивов никакие действия невозможны. При выборе действия **Удалить** архив будет удален целиком.

Вкладка Статистика



В окне статистики собраны итоговые сведения о работе сканера – общее количество проверенных объектов, обнаружено инфицированных известными вирусами, модификациями известных вирусов, обнаружено подозрительных объектов, а также сведения о действиях программы над зараженными и подозрительными объектами.

Вы также можете получить эти сведения для любого из логических дисков компьютера. Для этого выберите необходимый диск в раскрывающемся списке **Показать статистику дня**, расположенном в верхней части окна.

Для того чтобы обнулить статистические сведения, нажмите на кнопку **Очистить**.

Настройка параметров сканера

Для того чтобы изменить настройки программы:

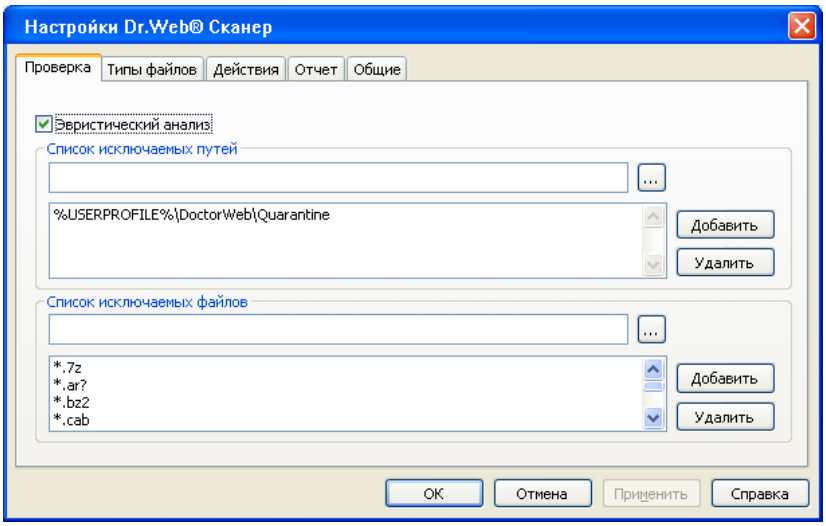
1. Выберите команду меню **Настройки/Изменить настройки**. Откроется окно настроек, содержащее несколько вкладок.

2. Внесите необходимые изменения. При необходимости, нажимайте на кнопку **Применить** перед переходом на другую вкладку.

3. По окончании редактирования настроек нажмите на кнопку **ОК** для сохранения внесенных изменений или на кнопку **Отмена** для отказа от них.

Изменение настроек имеет силу только в данном сеансе работы сканера. При повторном запуске утилиты, все настройки автоматически возвращаются к первоначальным значениям, определенным в ini-файле, поставляемом в комплекте.

Вкладка Проверка



На этой вкладке задаются списки каталогов и файлов, исключаемых из сканирования.

Список исключаемых путей. Здесь можно задать список каталогов, файлы в которых не будут подвергнуты проверке. В таком качестве могут выступать каталоги карантина антивируса, рабочие каталоги некоторых программ и т. п.

Для того чтобы создать список исключаемых путей:

- Введите путь к каталогу, файлы в котором должны быть исключены из проверки. Вы также можете воспользоваться кнопкой … и выбрать объект в стандартном окне операционной системы.
- Нажмите на кнопку **Добавить**, расположенную справа. Каталог будет добавлен в список, расположенный ниже.
- Для того чтобы удалить какой-либо каталог из списка, выберите его в этом списке и нажмите на кнопку **Удалить**. Содержимое каталога будет допущено к последующей проверке.

Список исключаемых файлов. Здесь можно задать список файлов (масок файлов), которые не будут сканироваться. (Из проверки будут исключены все файлы с данным именем.) В таком качестве могут выступать временные файлы (файлы подкачки) и т. п.

Для того чтобы создать список исключаемых файлов:

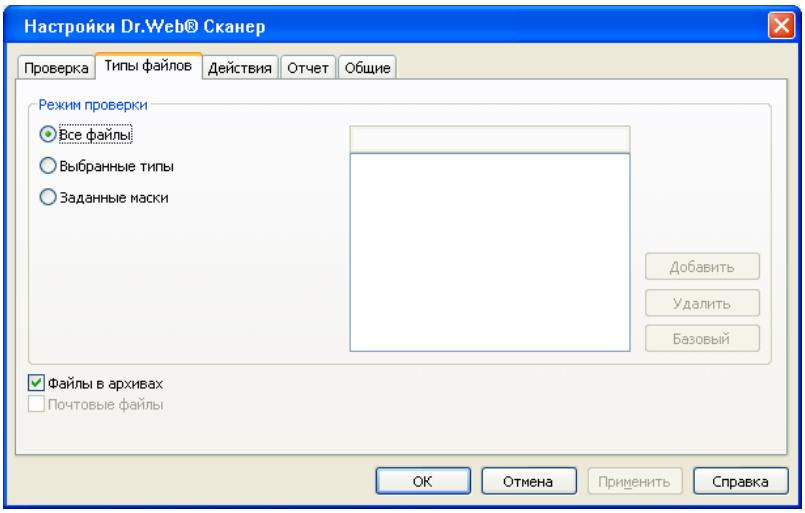
- Введите имя (маску) файла, который должен быть исключен из проверки. Если вводится имя существующего файла, можно воспользоваться кнопкой … и выбрать объект в стандартном окне открытия файла. Вместо части имени файла, допускается использование символов * и ?. Символ * заменяет любую последовательность символов; символ ? заменят один и только один символ (любой).
- Нажмите на кнопку **Добавить**, расположенную справа. Файл (маска файла) будет добавлен в список, расположенный ниже.
- Для того чтобы удалить какой-либо объект из списка, выберите его в списке и нажмите на кнопку **Удалить**.

При необходимости исключения из антивирусной проверки определенного файла, внесите путь к данному файлу (можно воспользоваться кнопкой …) и его имя (имя файла следует прописать вручную) в поле **Список исключаемых путей**.

Также на этой вкладке предоставляется возможность использования **эвристического анализа** (метода, позволяющего выявлять подозрительные объекты, с большой вероятностью зараженные еще неиз-

вестными вирусами). По умолчанию данная настройка включена. Рекомендуется сохранить использование эвристического анализа при сканировании и не менять данную настройку.

Вкладка Типы файлов



На этой вкладке задается дополнительное ограничение на состав файлов, которые должны быть подвергнуты сканированию в соответствии с заданием на сканирование.

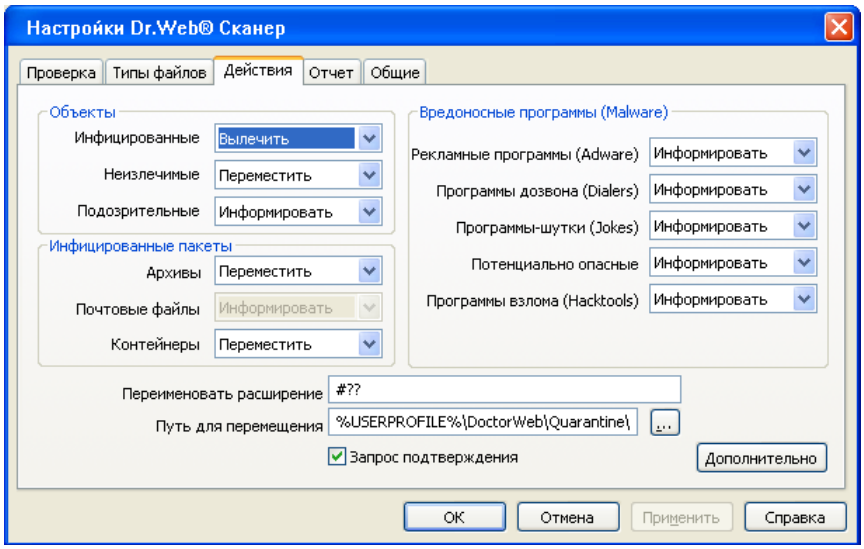
В области **Режим проверки** задается способ отбора проверяемых файлов.

Выбранный по умолчанию вариант **Все файлы** обеспечивает максимальную защиту.

Варианты **Выбранные типы** и **Заданные маски** предписывают проверять только файлы, расширения или имена которых соответственно входят в список, задаваемый в правой части вкладки. По умолчанию список включает расширения основных типов файлов, могущих быть носителями вирусов, и основных типов файловых архивов. Вы можете отредактировать этот список.

На этой вкладке задается также режим проверки файловых архивов и почтовых файлов, который доступен в версии сканера, входящей в полный пакет Антивирус Dr.Web.

Вкладка Действия



На этой вкладке задается реакция программы на обнаружение зараженных или подозрительных файлов, вредоносных программ, а также инфицированных архивов.

Реакция задается отдельно для объектов, зараженных известным и (предположительно) излечимым вирусом, для зараженных неизлечимым вирусом и для предположительно зараженных (подозрительных), а также для отдельных видов вредоносных программ и отдельных типов архивов.

По умолчанию Dr.Web информирует пользователя при подозрении на зараженность объекта вирусом. При этом сведения обо всех подозрительных объектах выводятся в поле отчета, в котором вы можете в дальнейшем предписать программе необходимые действия вручную. В случае обнаружения известного вируса, по умолчанию, Dr.Web пытается излечить объект. Если вирус неизлечим или попытка лече-

ния не была успешной, будет отработана реакция, заданная для неизлечимых вирусов (по умолчанию файл перемещается).

Вы можете выбрать другие реакции:

Вылечить (доступна только при настройке реакции **Для инфицированных**) – предписывает сканеру пытаться излечить объект, зараженный известным вирусом. Если вирус неизлечим или попытка лечения не была успешной, будет отработана реакция, заданная для неизлечимых вирусов.

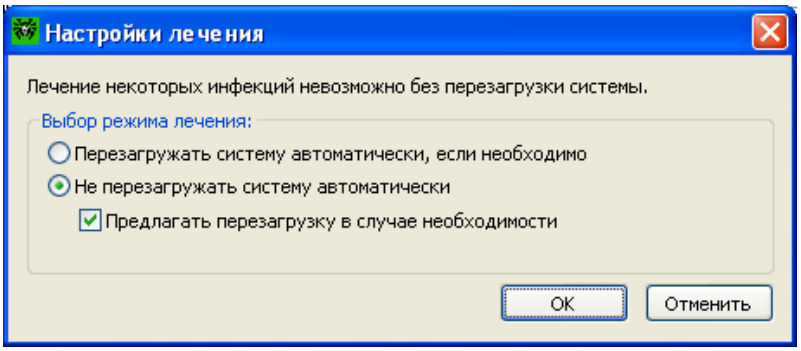
Удалить – предписывает удалить зараженный или подозрительный файл (для загрузочных секторов никаких действий производиться не будет).

Переименовать – предписывает переименовать расширение имени зараженного или подозрительного файла в соответствии с маской, задаваемой в поле **Переименовать расширение** (по умолчанию #??, т. е. заменить первый символ расширения на #).

Переместить – предписывает переместить зараженный или подозрительный файл в каталог карантина, задаваемый в поле **Путь для перемещения** (по умолчанию подкаталог Quarantine, который для Windows 9x/Me располагается в каталоге c:\DoctorWeb\, а для Windows NT/2000/XP/2003 —в каталоге %USERPROFILE%\DoctorWeb\).

Игнорировать – (допускается только для вредоносных программ) — не выводить информацию в окне отчета.

Дополнительные настройки лечения



Это окно вызывается кнопкой **Дополнительно** на вкладке **Действия** окна **Настройки сканера**.

Для успешного завершения лечения некоторых зараженных (инфицированных) файлов требуется перезагрузка ОС Windows. В данном окне задаются дополнительные настройки лечения таких файлов.

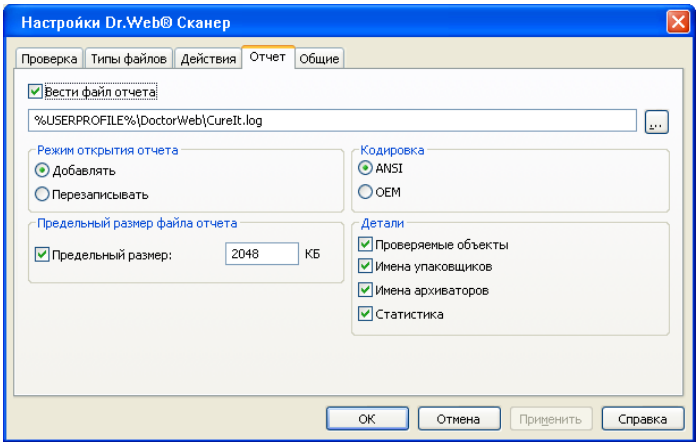
Вариант **Перезагружать систему автоматически, если необходимо** предписывает Dr.Web перезагружать ОС Windows автоматически, без дополнительного диалога с пользователем.

При проведении перезагрузки все несохраненные данные будут утеряны. При выборе пункта **Перезагружать систему автоматически** перед началом лечения рекомендуется завершить работу всех запущенных приложений (кроме Сканера Dr.Web).

Выбранный по умолчанию вариант **Не перезагружать систему автоматически** при установленном флажке **Предлагать перезагрузку в случае необходимости** предписывает Сканеру выдавать запрос на перезагрузку.

Снятие флажка **Предлагать перезагрузку в случае необходимости** отменяет возможность перезагрузки ОС Windows. В этом случае лечение некоторых инфекций может остаться незавершенным.

Вкладка Отчет



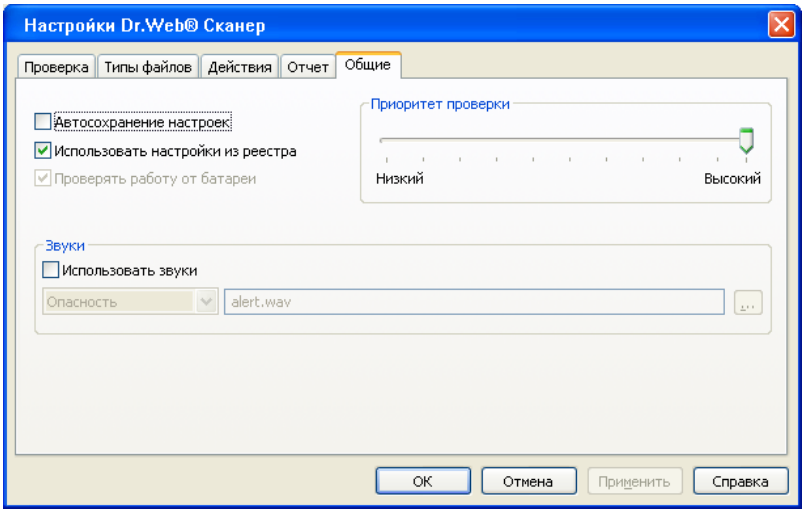
На этой вкладке задается режим ведения файла отчета.

По умолчанию установлен флажок **Вести файл отчета**.

По умолчанию файл отчета CureIt.log для Windows 9x/Me располагается в каталоге c:\DoctorWeb\, а для Windows NT/2000/XP/2003/Vista – в каталоге %USERPROFILE%\DoctorWeb\.

Вы можете настроить наименование и расположение файла отчета, кодировку текста, режим открытия (добавлять ли записи в конец файла отчета или перезаписывать его в начале каждого сеанса), а также степень детальности отчета. Также можно указать, следует ли ограничивать максимальный размер отчета и настроить этот размер.

Вкладка Общие



На этой вкладке задаются параметры взаимодействия программы с ОС а также звуковые реакции программы на различные события.

Параметр **Автосохранение настроек** не используется утилитой Dr.Web.

Флажок **Использовать настройки из реестра** позволяет запоминать в реестре Windows сведения о геометрических параметрах окон программы при последнем запуске.

Флажок **Проверять работу от батареи** позволяет проверять перед началом сканирования, работает ли ноутбук от батареи. Опция доступна только для портативных компьютеров (ноутбуков).

Бегунок **Приоритет проверки** позволяет изменить приоритет процесса сканирования в системе.

Режим звуковых реакций доступен в версии сканера, входящей в полный пакет Антивирус Dr.Web.

Задание

1. Загрузите Сканер Dr.Web.
2. В главном окне Сканера Dr.Web, в режиме **Выборочно** выполните проверку на вирусы своей рабочей папки. Если в ходе проверки были найдены вирусы и информация о них отразилась в *поле отчета*, то выделите все найденные зараженные файлы и попытайтесь вылечить их. Если эти файлы окажутся неизлечимыми, то удалите их.
3. Проверьте на вирусы папки *3 курс* и *4 курс*, находящиеся в папке *Мои документы*. В случае обнаружения инфицированных файлов выполните их лечение, а если необходимо, то и удаление.
4. На вкладке **Статистика** проанализируйте статистику для диска **C:**. Затем обнулите статистические сведения.
5. Измените настройки сканера следующим образом: задайте исключение из проверки папок *Преподаватели*, *3 курс* и *Мои рисунки*, находящихся в папке *Мои документы*; задайте исключение из проверки всех текстовых файлов (используя символы * или ?), находящихся в вашей рабочей папке. Выполните проверку на вирусы папки *Мои документы* с учетом заданных настроек.
6. Удалите настройки, заданные в п.5.
7. На вкладке **Типы файлов** окна настройки сканера выберите режим проверки **Заданные маски** и к уже указанным типам файлов добавьте для проверки расширения файлов: **.doc* и **.rar*. На вкладке **Действия** выберите в области **Объекты**: Инфицированные – *Вылечить*, Неизлечимые – *Переместить*, Подозрительные – *Информировать*. Выполните проверку папки *Мои документы* с учетом выбранных настроек.
8. На вкладке **Действия** в области **Объекты** восстановите прежние настройки (т.е. для инфицированных, неизлечимых и подозрительных объектов выберите *Вылечить*). Сохраните данные настройки.

9. Выполните проверку на вирусы вашей рабочей папки через контекстное меню. Для этого в окне *Проводника* или *Моего компьютера* вызовите контекстное меню на значке вашей папки и выберите из него команду для проверки Сканером Dr.Web.

Контрольные вопросы

1. Опишите характерные черты компьютерных вирусов.
2. Дайте определение программного вируса.
3. Перечислите классификационные признаки компьютерных вирусов.
4. Охарактеризуйте файловый и загрузочный вирусы.
5. В чем особенности резидентных вирусов?
6. Сформулируйте признаки стелс-вирусов.
7. Перечислите деструктивные возможности компьютерных вирусов.
8. Поясните самошифрование и полиморфичность как свойства компьютерных вирусов.
9. Перечислите виды "вирусоподобных" программ.
10. Поясните механизм функционирования "троянской программы" (логической бомбы).
11. В чем заключаются деструктивные свойства логических бомб?
12. Как используются утилиты скрытого администрирования и их деструктивные возможности?
13. Охарактеризуйте "intended"-вирусы и причины их появления.
14. Для чего используются конструкторы вирусов?
15. Для создания каких вирусов используются полиморфик-генераторы?
16. Поясните понятия "сканирование налету" и "сканирование по запросу".
17. Перечислите виды антивирусных программ.
18. Охарактеризуйте антивирусные сканеры.
19. Принципы функционирования блокировщиков и иммунизаторов.
20. Особенности CRC-сканеров.
21. В чем состоят особенности эвристических сканеров?
22. Какие факторы определяют качество антивирусной программы?
23. Какие из перечисленных выше антивирусных программ являются наиболее эффективными?
24. Для чего предназначен Сканер Dr.Web?
25. Что проверяется Сканером Dr.Web в режиме *полной проверки*?
26. Как можно остановить проверку, выполняемую Сканером Dr.Web?
27. Какая информация отображается в *поле отчета* Сканера Dr.Web?
28. Какие действия можно предпринять над инфицированными файлами, отображаемыми в поле отчета главного окна Сканера Dr.Web?
29. Где выполняются настройки параметров Сканера Dr.Web?

Лабораторная работа № 4

Основные признаки присутствия на компьютере вредоносных программ

Цель работы: изучение явных признаков заражения компьютера на примере модификации настроек браузера, исследование возможных мест скрытых проявлений заражения: запущенные процессы, элементы автозапуска, сетевая активность.

Введение

Умение своевременно найти и обезвредить вредоносную программу - один из ключевых навыков компьютерной грамотности. Для этого необходимо знать основные признаки присутствия вируса, уметь оценивать действия, выполняемые той или иной программой на предмет их вредоносности и знать, что в первую очередь следует предпринять, если компьютер все же оказался заражён.

Все виды проявлений вируса на компьютере можно разбить на три группы:

- явные;
- косвенные;
- скрытые.

К ***явным*** относятся менение настроек браузера, всплывающие сообщения и несанкционированный дозвон в Интернет.

К ***косвенным*** можно отнести блокирование работы антивируса, доступа к сайтам антивирусных компаний, сбои в работе системы или других приложений, почтовые уведомления о рассылаемых вами вирусах.

Некоторые вредоносные программы умеют достаточно хорошо скрывать от пользователя свою деятельность - такие проявления, называемые ***скрытыми***, обычно под силу обнаружить только антивирусной программе. Однако в любом случае, если возникло хоть малейшее подозрение на наличие вируса, необходимо уметь провести простейшую диагностику системы, чтобы либо подтвердить заражение, или опровергнуть его.

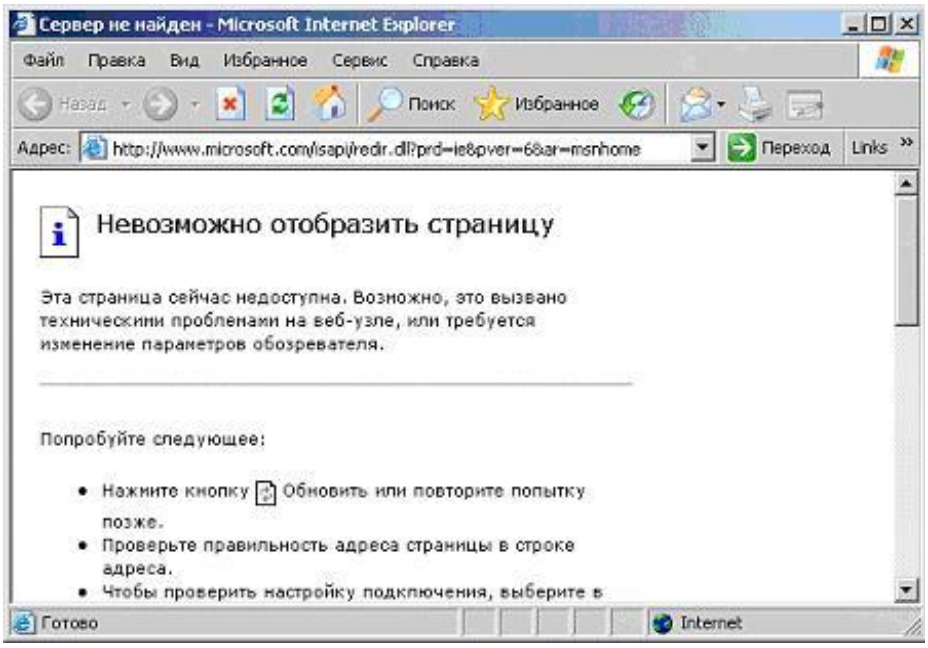


Рис. 1. ***Уведомление, выводимое в окне браузера, если нет доступа в Интернет.***

Задание 1. *Изучение настроек браузера* Internet Explorer

Первое задание этой лабораторной работы посвящено изучению явных признаков проявлений вируса на примере несанкционированного изменения настроек браузера.

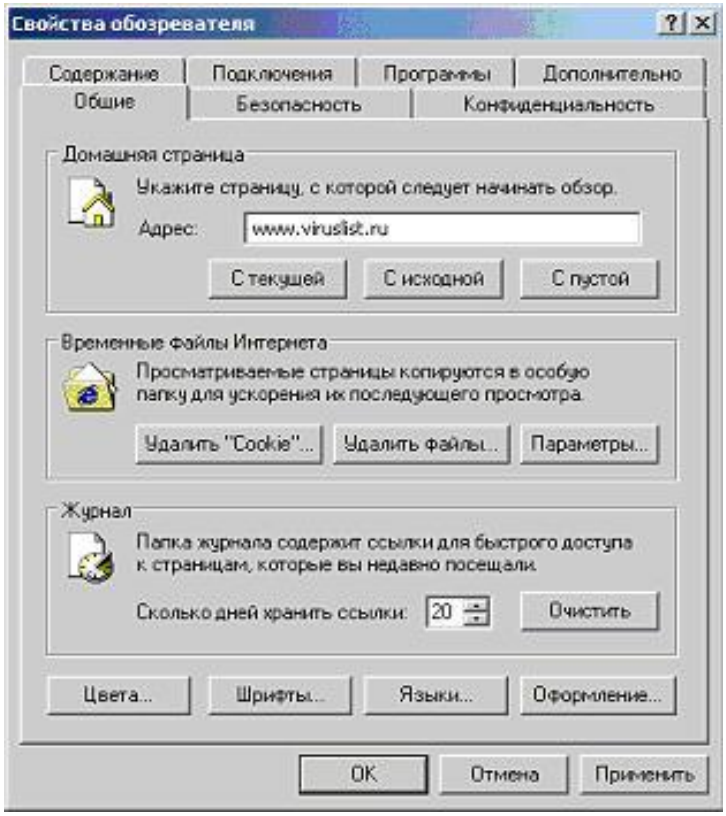


Рис. 2. ***Окно свойств обозревателя.***

Явные проявления обычно выражаются в неожиданно появляющихся рекламных сообщениях и баннерах - обычно это следствие проникновения на компьютер рекламной утилиты. Поскольку их главная цель - это привлечь внимание пользователя к рекламируемой услуге или товару, то им сложно оставаться незаметными. Также явные проявления могут вызывать ряд троянских программ, например утилиты несанкционированного дозвона к платным сервисам. Они вынуждены быть явными, поскольку используемые ими приложения сложно использовать незаметно от пользователя.

Механизм несанкционированного изменения настроек браузера иногда используется для того, чтобы вынудить пользователей зайти на определенный сайт, часто порнографического содержания. Для этого меняется адрес домашней страницы, то есть адрес сайта, который автоматически загружается при каждом открытии браузера.

1. Откройте браузер Internet Explorer, воспользовавшись одноименным ярлыком на рабочем столе или выбрав **Пуск/Все программы/**Internet Explorer.

2. Если у вас открыт и настроен доступ в Интернет и после установки операционной системы стартовая страница изменена не была, должна открыться страница по умолчанию – это может быть http://www.google.com.by или http://www.yandex.ru или какая-либо другая страница. Если доступ в Интернет не настроен, то выведется соответствующее уведомление (см. рис. 1)

3. Проверьте значение параметра, отвечающего за стартовую страницу. Для этого в окне браузера нужно выбрать **Сервис/Свойства обозревателя**/вкладка **Общие**.

4. Адрес стартовой страницы указан в поле **Адрес**. Значение этого поля совпадает с тем адресом, который был автоматически задан при открытии браузера. Измените это поле, удалив имеющийся там адрес и введя новый адрес www.viruslist.ru (см. рис. 2). Далее для подтверждения сделанных изменений щёлкните по кнопке **ОК**.

5. Закройте и снова откройте браузер Internet Explorer.

6. Убедитесь, что теперь первым делом была загружена страница www.viruslist.ru.

7. На загруженной странице ознакомьтесь с рейтингом вредоносных программ.

Таким образом, если ваш браузер начал самостоятельно загружать посторонний сайт, в первую очередь нужно изучить настройки браузера, т.е. какой адрес выставлен в поле домашней страницы.

Ряд вредоносных программ ограничиваются изменением этого параметра и для устранения последствий заражения нужно лишь исправить адрес домашней страницы. Однако это может быть только частью вредоносной нагрузки. Поэтому если вы обнаружили несанкционированное изменение адреса домашней страницы, следует немедленно установить антивирусное программное обеспечение и проверить весь жесткий диск на наличие вирусов.

Задание 2. *Подозрительные процессы*

Второе задание этой лабораторной работы посвящено ознакомлению с основным методом исследования списка запущенных процессов на компьютере (т.е. списка работающих в данный момент программ), получению навыков работы с *Диспетчером задач Windows* и изучению стандартного набора запущенных процессов.

Одним из основных проявлений вредоносных программ является наличие в списке запущенных процессов подозрительных программ. Исследуя этот список и особенно сравнивая его с перечнем процессов, которые были запущены на компьютере до начала работы, можно сделать достаточно достоверные выводы об инфицировании. Это часто помогает при обнаружении вредоносных программ, имеющих лишь только скрытые или косвенные проявления. Однако необходимо чётко понимать и уметь отличать легальные процессы от подозрительных.

Диспетчер задач Windows - это стандартная утилита, входящая в любую Microsoft Windows NT - подобную операционную систему, в том числе Microsoft Windows XP. С ее помощью можно в режиме реального времени отслеживать выполняющиеся приложения и запущенные процессы, оценивать загруженность системных ресурсов компьютера и использование сети.

Познакомимся с интерфейсом Диспетчера и проследим за изменениями в системе на примере запуска программы Paint.

1. Откройте *Диспетчер задач Windows*, нажав одновременно клавиши Ctrl+Shift+Esc. Открывшееся окно содержит четыре вкладки (см. рис. 3), отвечающие четырем видам активности, которые отслеживает Диспетчер: **Приложения**, **Процессы**, **Быстродействие** (использование системных ресурсов) и **Сеть**. По умолчанию у вас должна открыться вкладка **Процессы**.

2. Внимательно изучите ставленный в окне список процессов. Если на компьютере не запущены никакие пользовательские программы, он должен содержать только служебные процессы операционной системы.

3. Для каждого процесса выводятся его параметры (в соответствующем столбце): *имя образа* (может не совпадать с именем запускаемого файла), *имя пользователя*, от чьего имени был запущен процесс, загрузка этим процессом процессора (*ЦП*) и объем занимаемой им оперативной памяти.

Загрузка процессора представлена в процентах от максимальной. Поэтому для удобства пользователя в списке (в столбце *Имя образа*) всегда присутствует пункт "Бездействие системы". С его помощью можно быстро узнать насколько загружен, вернее свободен процессор (см. рис. 3).

4. Отсортируйте все процессы по использованию ресурсов процессора. Для этого нажмите на заголовок поля **ЦП**.

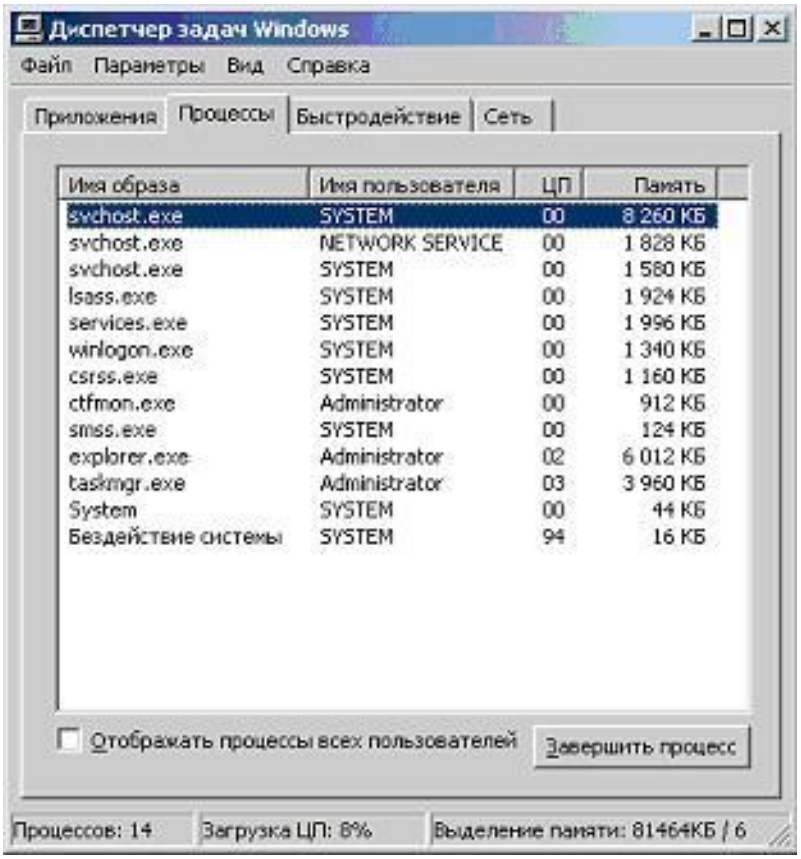


Рис. 3. ***Окно Диспетчера задач*** *Windows.*

5. Поскольку в данный момент не должна быть запущена ни одна пользовательская программа, процессор должен быть свободен. Следовательно, "Бездействие системы" должно оказаться внизу списка с достаточно большим процентом "использования" процессора. На рис. 3 – это 94 %.

Этот метод также можно использовать для того, чтобы в случае заметного снижения производительности определить, какая программа виновна в этом: столбец **ЦП** покажет загрузку процессора, а **Память** - оперативную память.

В ряде случаев может потребоваться вручную завершить некий процесс. Это можно сделать, выделив щелчком мыши имя образа и нажав кнопку **Завершить процесс**.

6. Выпишите все запущенный процессы на лист бумаги или в текстовый файл и перейдите к вкладке **Приложения**.

7. Поскольку в данный момент не запущено ни одно приложение, список запущенных приложений будет пуст.

8. Не закрывая окна Диспетчера задач Windows, откройте программу Paint. Для этого выберите **Пуск/Программы/Стандартные/Paint**.

9. Не закрывая приложение Paint, вернитесь к окну Диспетчера задач Windows и проследите за изменениями на вкладке **Приложения**.

10. Список запущенных приложений должен содержать строку, соответствующую

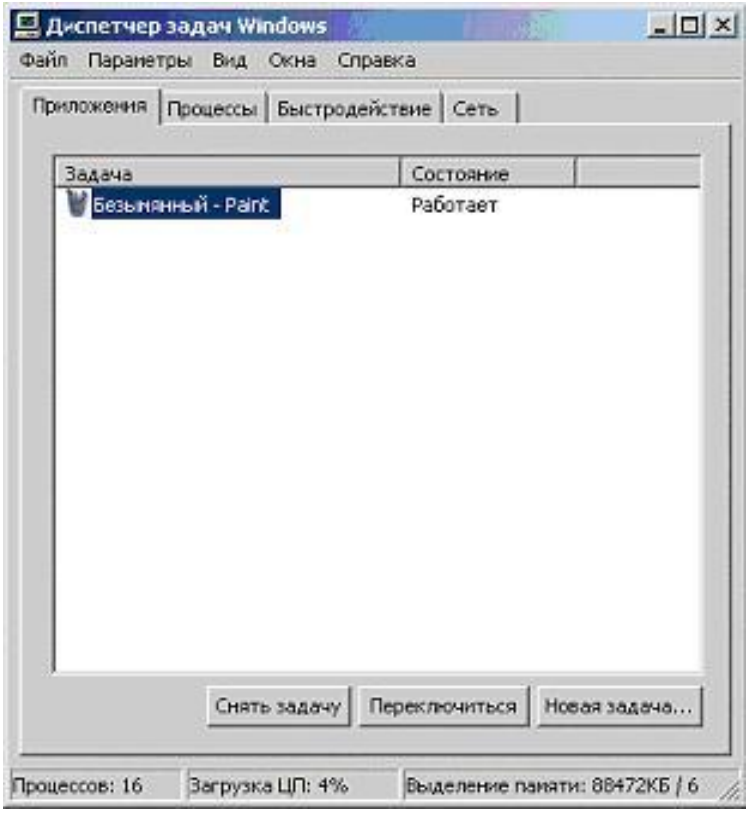


Рис. 4. ***Вкладка*** **Приложения** ***окна Диспетчера задач*** *Windows.*

Paint (см. рис. 4). Поскольку это приложение сейчас работает, это же записано в столбце **Состояние**.

Иногда случается так, что программа вызывает ошибку - тогда в ее состоянии будет написано "Не отвечает". Если некое ранее бесперебойно работающее приложение начало часто без видимых причин переходить в состояние "Не отвечает", это может быть косвенным признаком заражения. Тогда первое, что можно сделать - это воспользоваться кнопкой **Снять задачу** и начать поиски причин. В иных случаях пользоваться этой кнопкой не рекомендуется.

11. Перейдите на вкладку **Процессы**. Сравните список запущенных сейчас процессов с перечнем, составленным на шаге 6 этого задания. Найдите отличие (опишите его в вашем отчёте как ответ на контрольный вопрос 4).
12. Убедитесь, что программе Paint соответствует процесс *mspaint.exe*. Для этого найдите его в списке запущенных процессов, не закрывая и не сворачивая окно Диспетчера задач Windows, вернитесь в окне Paint и закройте его.
13. Проследите, что из списка запущенных процессов пропал *mspaint.exe*.
14. Вернитесь к вкладке **Приложения** и убедитесь, что она снова пуста.
15. Перейдите к вкладке **Быстродействие** (см. рис. 5). Внимательно изучите расположенные тут графики. Любые всплески на них должны по времени соответствовать неким действиям, например запуску требовательной к ресурсам программы. Если ничего похожего сознательно не производилось, это может быть причиной для более детального исследования компьютера.
16. Закройте окно Диспетчера задач Windows.

Задание 3. *Элементы автозапуска*

В третьем задании предлагается изучить элементы операционной системы, отвечающие за автозапуск программ при ее загрузке, а именно: группу **Автозагрузка** в меню **Пуск** и утилиту msconfig.exe.

Для того, чтобы прикладная программа начала выполняться, ее нужно запустить. Следовательно, и вирус нуждается в том, чтобы его запустили. Для этого можно использовать два сценария: либо сделать так, чтобы пользователь сам его стартовал (используются обманные методы), либо внедриться в конфигурационные файлы и запускать одновременно с другой, полезной программой. Оптимальным с точки зрения вируса вариантом служит запуск одновременно с операционной системой - в этом случае запуск практически гарантирован.

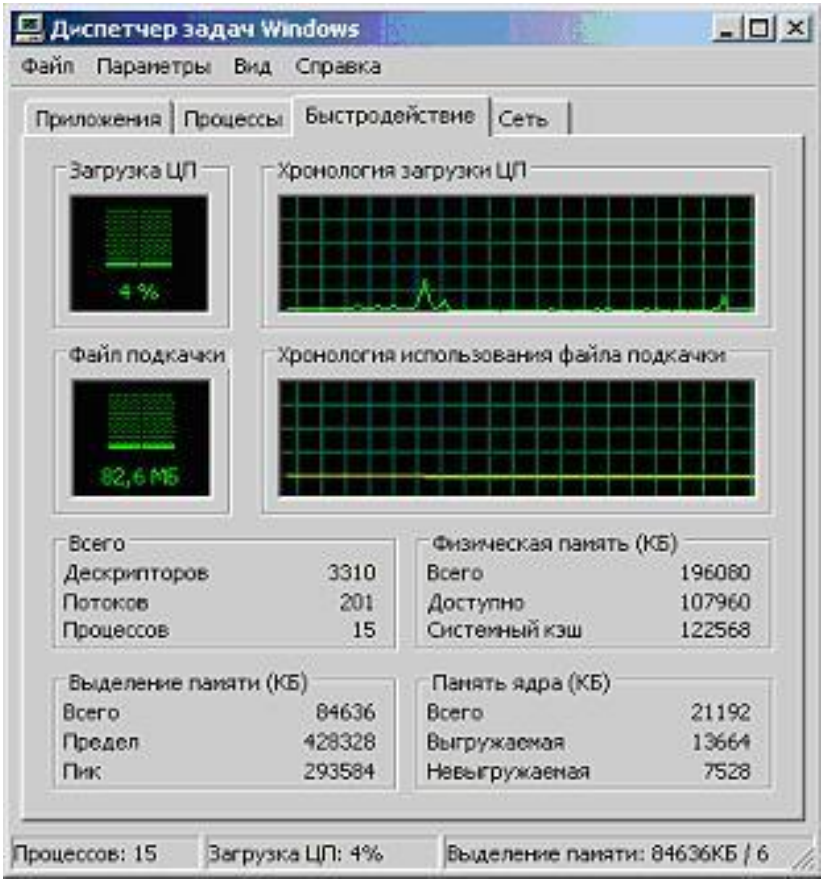


Рис. 5. ***Вкладка*** **Быстродействие** ***окна Диспетчера задач*** *Windows.*

1. Самый простой способ добавить какую-либо программу в автозагрузку - это поместить ее ярлык в раздел **Автозагрузка (Пуск/Все программы/Автозагрузка)**.
2. Проверьте папку **Автозагрузка** на вашем компьютере.
3. Добавьте в список автозагрузки программу *Блокнот* (Notepad). Для этого выберите **Пуск/Все программы/Стандартные**.
4. В открывшемся подменю найдите ярлык программы *Блокнот*. Щелчком правой клавиши мыши на нём откройте контекстное меню и выберите из него команду **Копировать**.
5. Закройте подменю стандартных программ.

6. Выберите **Пуск/Все программы** и дважды щёлкните левой клавишей мыши по названию группы **Автозагрузка** (или щёлкните правой клавишей мыши по названию группы **Автозагрузка** и из контекстного меню выберите команду **Открыть**).

7. В результате откроется соответствующее окно папки автозагрузки (см. рис. 6).

8. В окне автозагрузки щелкните правой клавишей мыши где-нибудь на белом поле окна и в открывшемся контекстном меню выберите команду **Вставить**.

9. В результате этих действий в окне должна появиться копия ярлыка программы *Блокнот* (Notepad).

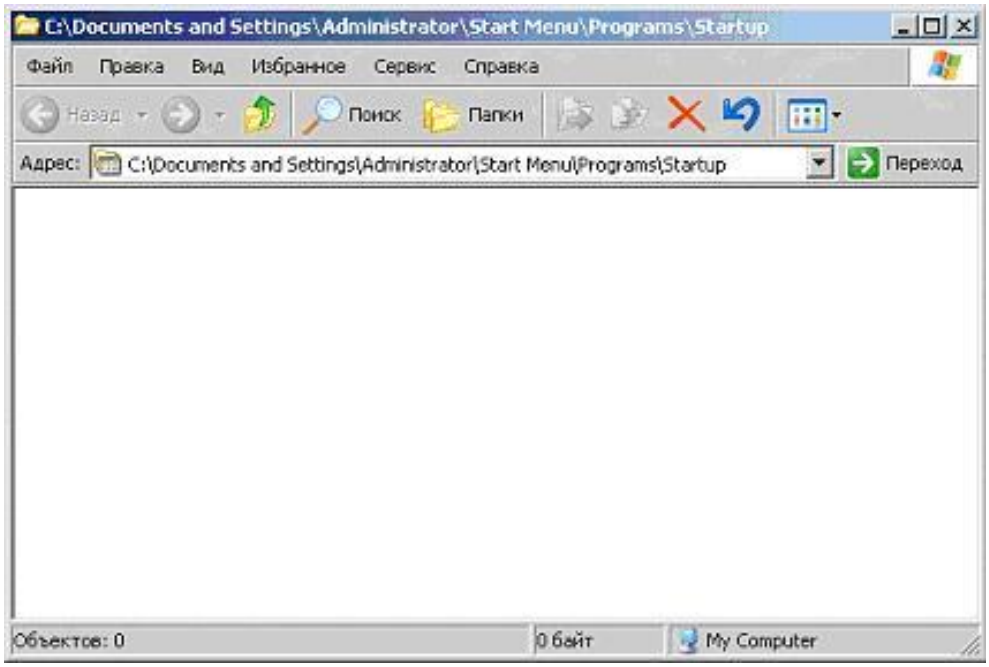


Рис. 6. *Окно папки* Автозагрузка.

10. Закройте окно и убедитесь, что теперь раздел **Автозагрузка** в системном меню **Пуск/Программы** не пуст.

11. Перезагрузите компьютер.

12. Убедитесь, что по завершению загрузки автоматически запустилась программа *Блокнот*.

При обследовании компьютера нужно помнить, что отсутствие подозрительных ярлыков в разделе **Автозагрузка** системного меню **Пуск/Программы** не гарантирует, что ни одно приложение не запускается автоматически. Технически для автозапуска нужно добавить соответствующую запись в системный реестр операционной системы.

Несмотря на то, что реестр Windows очень большой, существует оболочка, позволяющая с ним работать напрямую. Но делать это рекомендуется только в крайнем случае. Для большинства ситуаций, связанных с автозапуском, достаточно использовать системную утилиту **Настройка системы**.

13. Откройте главное меню кнопкой **Пуск** и выберите пункт **Выполнить**. В открывшемся окне **Запуск программы** наберите *msconfig* и нажмите кнопку **ОК**.

14. Ознакомьтесь с внешним видом открывшегося окна утилиты **Настройка системы** (см. рис. 7).

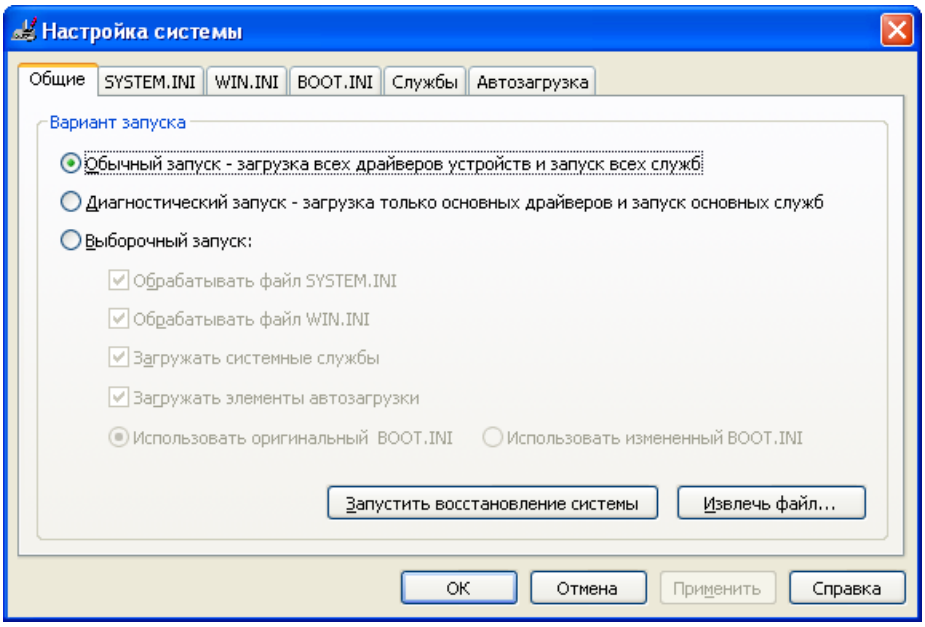


Рис. 7. *Окно утилиты* Настройка системы.

На вкладке **Общие** можно выбрать вариант запуска операционной системы. По умолчанию отмечен **Обычный запуск**. Он обеспечивает максимальную функциональность системы. Остальные два варианта запуска предназначены для диагностики. Второй вариант, **Диагностический запуск**, рекомендуется использовать также при

подтвердившемся вирусном инциденте - если компьютер уже заражен, сразу установить антивирус в ряде случаев нельзя, например, если вирус сознательно блокирует запуск ряда антивирусных программ. Тогда, если нет возможности удалить или хотя бы временно обезвредить вирус вручную, рекомендуется запустить операционную систему в безопасном режиме, инсталлировать антивирус и сразу же проверить весь жесткий диск на наличие вирусов.

Для получения дополнительной информации об этой вкладке и других можно воспользоваться кнопкой **Справка**.

15. Перейдите на вкладку SYSTEM.INI и ознакомьтесь со списком запускаемых драйверов и других параметров операционной системы. Тут отображаются все ссылки, указанные в одноименном системном файле.
16. Перейдите к аналогичной закладке WIN.INI и ознакомьтесь с ее содержимым.
17. Перейдите на вкладку BOOT.INI, которая также отображает данные из одноименного файла. Как и предыдущие две, она также содержит системную информацию. Изменять ее можно только обладая соответствующими знаниями. Однако ознакомиться со стандартным видом и в случае подозрений обнаружить следы вируса под силу и непрофессионалу.
18. Перейдите на вкладку **Службы**. Здесь представлен список всех служб, установленных в системе. Каждая служба представляет собой некое приложение, работающее в фоновом режиме. Например, антивирусный комплекс, обеспечивающий постоянную защиту, также встраивает свою службу, следовательно, она должна присутствовать в этом перечне.
19. Перейдите к вкладке **Автозагрузка** и убедитесь, что в списке приложений, автоматически запускаемых при загрузке системы, есть программа *Блокнот*.

Список в окне **Настройки системы** может содержать дополнительные элементы, не отображаемые в разделе **Пуск/Программы/Автозагрузка**.

20. Отключите автоматическую загрузку *Блокнота*, убрав галочку возле элемента Notepad в столбце **Элемент автозагрузки** и щёлкните по кнопке **ОК**.
21. В открывшемся окне щёлкните по кнопке **Перезагрузка** (см. рис. 8), чтобы провести перезагрузку системы.

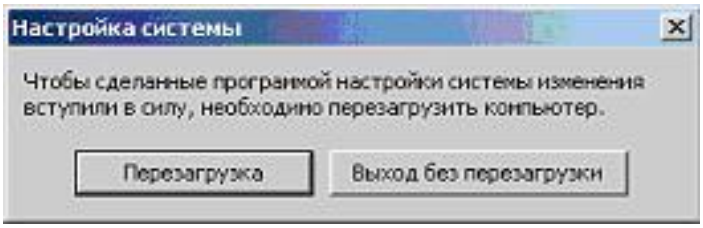


Рис. 8.

22. Дождитесь окончания перезагрузки и войдите в систему опять.
23. Поскольку вы внесли фактически вручную изменения в параметры автозагрузки (отключив запуск *Блокнота)*, система выведет соответствующее уведомление. Внимательно прочитайте текст уведомления и нажмите кнопку **ОК**.
24. Это приведет к открытию окна **Настройка системы**. Обратите внимание, что теперь используется не обычный запуск, а выборочный. При этом полностью обрабатываются все элементы файлов SYSTEM.INI, WIN.INI и BOOT.INI, загружаются все службы (поскольку мы их не трогали), но флаг **Загружать элементы автозагрузки** затенён. Это означает неполную загрузку.
25. Перейдите на вкладку **Автозагрузка** и убедитесь, что её вид не изменился - *Блокнот* всё так же присутствует в списке, но отключён.
26. Не закрывая окна **Настройка системы** проверьте, что *Блокнот* автоматически не запустился и раздел **Пуск/Программы/Автозагрузка** теперь пуст.
27. Вернитесь к закладке **Общие** окна **Настройка системы** и выберите вариант **Выборочный запуск**. Нажмите кнопку **ОК** и в следующем окне щёлкните по кнопке **Перезагрузка**.
28. Дождитесь окончания перезагрузки, войдите в систему и убедитесь, что сообщение о выборочном запуске (как было в пункте 23) не появляется.
29. Однако поскольку флаг, снятый в пункте 20, при переключении в режим **Обычный запуск** вернулся (*Обычный запуск* предполагает загрузку всех зарегистрированных компонентов), приложение *Блокнот* снова автоматически запускается по завершении перезагрузки операционной системы.
30. Убедитесь, что в **Пуск/Программы/Автозагрузка** вернулся ярлык *Блокнота*.
31. Удалите этот ярлык, вызвав контекстное меню (щелчок правой клавишей мыши) и выбрав команду **Удалить**. Для подтверждения своих намерений в появившемся следующем окне нажмите кнопку **Да**.
32. Теперь автозагрузка чиста. Убедитесь в этом, выполнив перезагрузку и войдя заново в систему.

Задание 4. *Сетевая активность*

В четвёртом задании предлагается изучить и проанализировать сетевую активность с помощью Диспетчера задач Windows и встроенной утилиты *netstat*, которая выводит на экран мгновенную статистику сетевых соединений.

Неожиданно возросшая сетевая активность может служить ярким свидетельством работы на компьютере подозрительной программы, производящей несанкционированную рассылку писем, связывающейся со своим автором и передающей ему конфиденциальную информацию или просто загружающую свои дополнительные модули или атакующей соседние компьютеры. Но при этом нужно не забывать, что ряд вполне легальных приложений также имеют свойство иногда связываться с сайтом фирмы-производителя, например для проверки наличия обновлений или более новых версий. Поэтому, прежде чем отключать сеть и выдергивать сетевой шнур, увидев необычно яркое мигание лампочки на сетевой карте, необходимо уметь определять какие программы и приложения вызвали эту подозрительную активность.

Рис. 9.

1. Откройте окно *Диспетчера задач Windows*, нажав одновременно клавиши Ctrl+Shift+Esc, и перейдите на вкладку **Сеть**.

2. В нижней части окна расположен перечень всех установленных в системе сетевых адаптеров. Обычно он один. В столбце **Использование сети** приводится моментальное значение доли используемого канала, а в **Скорость линии** - пропускная способность. В столбце **Состояние** отображается статус.

Если на вашем компьютере нет ни одного активного адаптера, то окно *Диспетчера задач* на вкладке **Сеть** будет выглядеть так, как показано на рис. 9.

3. Инициируйте какое-нибудь сетевое соединение. Например, откройте браузер Internet Explorer и загрузите сайт www.viruslist.ru.

4. Проследите за изменениями на графике *Диспетчера задач*: все ваши действия отобразятся на графике в виде пиков сетевой активности, а значение поля **Использование сети** на время перестанет быть равным нулю.

Таким образом, если вы, закрыв все прикладные программы, которые могут инициировать сетевые соединения, обнаруживаете, что сеть все равно использоваться продолжает, нужно искать причину.

5. *Диспетчер задач Windows* показывает только самую общую информацию. Для получения более подробных данных можно воспользоваться утилитой *netstat*.

Рис. 10. ***Окно утилиты*** **Командная строка**.

6. Закройте окно *Диспетчера задач Windows* и выберите **Пуск/Все программы/Стандартные/Командная строка**.

7. В открывшемся окне (см. рис. 10) нужно набирать команды, оканчивающиеся нажатием клавиши Enter. Такой способ взаимодействия называется работой через командную строку. Утилита *netstat* подразумевает именно такой режим.

Наберите в командной строке

```
netstat/?
```

и нажмите клавишу Enter.

8. Прочитайте описание утилиты *netstat*. Убедитесь, что для вывода самой полной информации нужно использовать ключ – a.

Наберите в командной строке

```
netstat -a
```

и нажмите клавишу Enter.

9. Результатом выполнения команды является список активных подключений, в который входят установленные соединения и открытые порты (см. рис. 11).

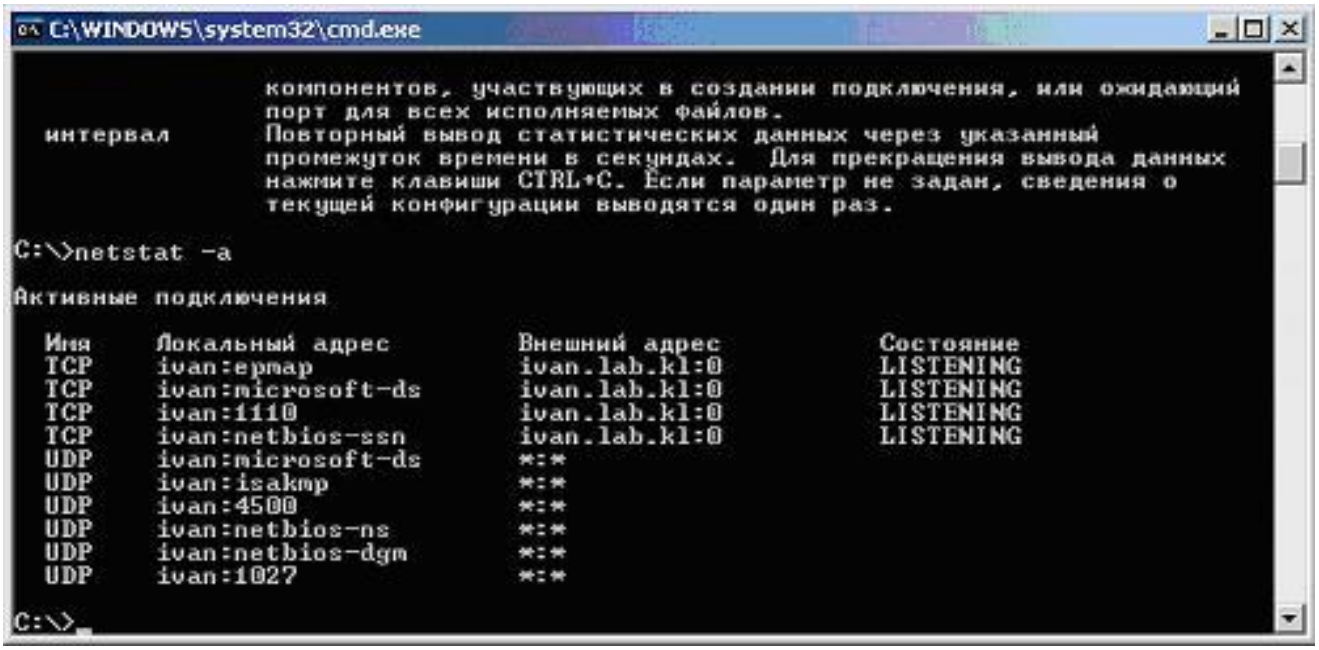


Рис. 11. *Окно утилиты* Командная строка.

Открытые TCP-порты обозначаются строкой "LISTENING" в колонке **Состояние**. Часть портов связана с системными службами Windows и отображается не по номеру, а по названию - epmap, microsoft-ds, netbios-ssn. Порты, не относящиеся к стандартным службам, отображаются по номерам.

UDP-порты обозначаются строкой "UDP" в колонке **Имя**. Они не могут находиться в разных состояниях, поэтому специальная пометка "LISTENING" в их отношении не используется. Как и TCP-порты они могут отображаться по именам или по номерам.

Порты, используемые вредоносными программами, чаще всего являются нестандартными и поэтому отображаются согласно их номерам. Впрочем, могут встречаться троянские программы, использующие для маскировки стандартные для других приложений порты, например 80, 21, 443 - порты, используемые на файловых и веб-серверах.

10. Проверьте, как изменится статистика, отображаемая *netstat* при инициировании новых соединений. Для этого повторите пункт 3 (инициируя новое соединение, например, www.processlibrary.com).

11. Команда *netstat*, в отличие от *Диспетчера задач Windows*, не работает в режиме реального времени, а отображает мгновенную статистику. Следовательно, ее нужно снова запустить.

Вернитесь к окну командной строки, введите

```
netstat –a
```

и нажмите клавишу Enter.

12. Исследуйте полученную статистику.
13. Закройте браузер, повторите команду

```
netstat –a
```

и нажмите клавишу Enter.

14. Убедитесь, что все вызванные ранее сетевые соединения закрыты, а перечень активных соединений не отличается от данных, полученных при выполнении пункта 9.
15. Закройте окно командной строки. Для этого введите команду

```
exit
```

и нажмите клавишу Enter.

Заключение

В этой лабораторной работе были изучены явные признаки заражения компьютера на примере модификации настроек браузера, исследованы возможные места скрытых проявлений: запущенные процессы, элементы автозапуска, сетевая активность. Выполнение практических заданий позволяет получить навыки обнаружения на своём компьютере подозрительных программ вручную, без использования антивирусных средств.

Контрольные вопросы

1. Что относится к *явным* признакам вирусного заражения компьютера ?
2. Как можно изменить адрес домашней страницы, автоматически загружаемой при каждом открытии браузера Internet Explorer ?
3. Каково назначение *Диспетчера задач Windows* ?
4. Какая информация отображается на вкладке **Процессы** окна Диспетчера задач Windows ?
5. Как можно *вручную* завершить некоторый процесс на компьютере и в каких случаях это выполняется ?
6. Опишите найденное вами отличие на вкладке **Процессы** окна Диспетчера задач Windows при выполнении п.11 задания 2 .
7. Что нужно сделать, чтобы какое-либо приложение автоматически загружалось при загрузке операционной системы ?
8. На вкладке **Службы** окна **Настройка системы** найдите названия всех служб, относящихся к антивирусной программе, работающей на вашем компьютере и запишите их в отчёт.
9. О чём свидетельствует увеличение сетевой активности ?
10. Как определить какие программы и приложения вызывают подозрительную сетевую активность ?
11. Какая утилита позволяет более подробно изучить и проанализировать статистику сетевых соединений ? Как запускается эта утилита ?
12. Как можно просмотреть мгновенную статистику сетевых подключений ?

Лабораторная работа № 5

Защита от несанкционированного доступа баз данных Microsoft Access

Цель работы: изучение средств, предоставляемых MS Access для решения задач: архивирования, сжатия и восстановления баз данных; защиты информации с помощью средств шифрования; администрирования баз данных.

Введение

Защитить базы данных MS Access от несанкционированного доступа можно с помощью следующих средств:

- архивирование (создание резервных копий) баз данных;
- сжатие и восстановление баз данных;
- защита информации с помощью средств шифрования;
- установка пароля доступа к базе данных;
- администрирование защищённой базы данных.

1. Архивирование, сжатие и восстановление баз данных

Чтобы застраховаться от потери данных, можно создать резервную копию базы данных Access. Чтобы увеличить производительность базы данных и уменьшить её размер, можно использовать операцию сжатия базы данных Access.

1.1. Создание резервной копии базы данных MS Access

Есть несколько путей создания резервной копии базы данных:

– при наличии достаточного объёма свободного места на диске можно создать резервную копию обычным копированием файла с помощью приложения Проводник (Explorer), входящего в состав операционной системы Windows;

– чтобы сэкономить место на диске, можно создать сжатую копию файла с помощью программы архивирования, например с помощью утилит WinZip или WinRar.

1.2. Сжатие базы данных Access

При удалении данных или объектов файл базы данных становится фрагментированным, это приводит к тому, что дисковое пространство используется неэффективно. Сжатие базы данных позволяет получить копию, в которой данные и объекты сохраняются более рационально, что значительно экономит место на диске.

Чтобы сжать открытую базу данных Access:

1. Загрузите файл базы данных.
2. Выберите команду меню **Сервис/Служебные программы/Сжать и восстановить базу данных**.

Чтобы сжать закрытую в данный момент базу данных или проект Access:

1. Запустите MS Access, не открывая базу данных
2. Выберите команду меню **Сервис/Служебные программы/Сжать и восстановить базу данных**.
3. В появившемся диалоговом окне **База данных для сжатия**, укажите базу данных, которую необходимо сжать, и нажмите кнопку **Сжать**.
4. В появившемся диалоговом окне **Сжатие базы данных под именем** выберите диск и папку и введите имя для сохранения сжатой базы данных, а затем нажмите кнопку **Сохранить**.

В обоих случаях процесс сжатия можно прервать с помощью комбинации клавиш Ctrl+Break или клавиши Esc.

Допускается сжатие файла базы данных Access в файл с тем же именем, что и имя исходного файла, или создание файла с новым именем. При указании того же имени, диска и папки и при успешном сжатии базы данных исходный файл автоматически заменяется на сжатый файл.

Можно настроить MS Access так, чтобы конкретная база данных или проект автоматически сжимались при закрытии.

Чтобы установить автоматическое сжатие базы данных Access:

1. Откройте базу данных, которую нужно сжать.
2. Выберите команду меню **Сервис/Параметры**/вкладка **Общие**/установить флажок **Сжимать при закрытии** и нажмите кнопку **ОК.**

1.3. Восстановление повреждённой базы данных

В большинстве случаев Microsoft Access определяет, что база данных повреждена, при попытке открыть, зашифровать или дешифровать её. Тогда пользователю предоставляется возможность восстановить базу данных, выполнив её сжатие. Но в некоторых ситуациях не удаётся определить, что база данных повреждена. Если база данных ведёт себя непредсказуемым образом, выполните её сжатие.

При серьёзных проблемах, которые приводят к вынужденному завершению работы Access, это приложение перезапускается и автоматически создаётся резервная копия открытой базы данных Access с тем же именем и расширением, что и исходный файл, только с суффиксом _Backup (резервный).

2. Защита информации с помощью шифрования

Защита информации в базе данных Access производится с помощью операции *шифрования*. Операция шифрования в Access приводит к сжатию файла базы данных. После выполнения операции шифрования просмотр данных с помощью специальных программ и текстовых редакторов становится невозможен. Операция *дешифрования* отменяет результаты операции шифрования.

Операция шифрования или дешифрования неприменима к открытой базе данных. Если база данных используется в сети, то, прежде чем приступить к выполнению операции шифрования или дешифрования, убедитесь, что она не открыта ни одним из пользователей.

Чтобы выполнить операцию шифрования или дешифрования:

1. Запустите MS Access, не открывая базу данных.
2. Выберите команду меню **Сервис/Защита/Шифровать/расшифровать**.
3. В появившемся диалоговом окне **База данных для шифрования или дешифрования** укажите имя базы данных, которую требуется зашифровать или дешифровать, и нажмите кнопку **ОК.**
4. Если выбранная на предыдущем шаге база данных не является зашифрованной, появится диалоговое окно **Шифрование базы данных под именем**, в противном случае появится диалоговое окно **Дешифрование базы данных под именем**. Укажите имя, диск и папку для конечной базы данных и нажмите кнопку **Сохранить**.

Можно указать новое имя или имя, совпадающее с именем исходного файла. Если указаны те же имя, диск и папка, а шифрование или дешифрования выполнены успешно, то исходный файл будет заменен на зашифрованный или дешифрованный. Если же операция приводит к ошибке, то исходный файл удалён не будет. Кроме того, исходный файл не будет удалён, пока операция шифрования не завершится. Поэтому необходимо иметь достаточно места на диске для двух версий базы данных — зашифрованной и незашифрованной.

Если для базы данных определена защита на уровне пользователей, то для её шифрования или дешифрования необходимо быть владельцем базы данных или входить в группу Admins и иметь разрешение на монопольное открытие базы данных. В противном случае попытка шифрования или дешифрования окажется неудачной. Шифрование базы данных не препятствует доступу к ней легальных пользователей или групп в Access. Разрешения на доступ к объектам являются частью системы защиты базы данных на уровне пользователей.

3. Администрирование защищённых баз данных

Существует несколько способов защиты базы данных Access от несанкционированного доступа:

- база данных может быть защищена паролем;
- для базы данных Access может быть установлена система защиты на уровне пользователей;
- программный код на VBA может быть защищён паролем.

3.1. Установка и снятие пароля защиты базы данных

Самый простой способ защиты базы данных — с помощью пароля. Можно назначить пароль базе данных Access, и всякий раз, когда пользователь будет открывать базу данных, будет отображаться диалоговое окно с требованием ввести пароль.

Чтобы установить пароль для защиты базы данных:

1. Запустите MS Access, не открывая базу данных.
2. Выберите команду меню **Файл/Открыть**.
3. Выделите файл базы данных.
4. Щелкните по стрелке, расположенной справа от кнопки **Открыть**. В раскрывающемся списке режимов открытия базы данных выделите элемент **Монопольно**. База данных откроется в режиме монопольного доступа.
5. Выберите команду меню **Сервис/Защита/Задать пароль базы данных**.
6. В появившемся диалоговом окне в поле **Пароль** введите пароль для защиты базы данных с учётом регистра символов.
7. Введите пароль ещё раз в поле **Подтверждение**.

8. Нажмите кнопку **ОК.**

Если база данных защищена на уровне пользователей, установить пароль для её открытия может только пользователь, обладающий административными правами. Установка пароля не влияет на систему защиты на уровне пользователя. Эти два способа защиты могут использоваться одновременно. Пароль базы данных сохраняется в базе данных, а не в файле рабочей группы.

Чтобы удалить пароль защиты базы данных:

1. Откройте базу данных в режиме монопольного доступа.
2. В диалоговое окно **Необходимо ввести пароль** ведите пароль.
3. Выберите команду меню **Сервис/Защита/Удалить пароль базы данных**. Появится диалоговое окно **Удаление пароля базы данных**.
4. Введите текущий пароль базы данных.
5. Нажмите кнопку **ОК.**

3.2. Установка связи с таблицами базы данных, защищённой паролем

Чтобы установить связь с таблицами базы данных, защищённой паролем, требуется ввести пароль. Если пароль был указан верно, он сохраняется вместе с другой информацией о ссылках на таблицы. После этого любой пользователь, работающий с базой данных со связанными таблицами, может открыть эти таблицы без указания пароля. Если пароль защищённой базы данных будет изменён, в следующий раз при открытии базы данных, содержащей связанные таблицы, потребуется ввести пароль.

Microsoft Access сохраняет пароль в базе данных, содержащей связанные таблицы защищённой базы данных, в незашифрованном виде. Если это уязвляет систему защиты базы данных, не используйте средство защиты с помощью пароля. Установите систему защиты на уровне пользователей, чтобы ограничить доступ к объектам базы данных.

4. Администрирование баз данных Access, защищённых на уровне пользователей

В задачу администрирования базы данных, защищённой на уровне пользователей, входит выполнение следующих действий:

- подключение файла рабочей группы для работы с защищённой базой данных;
- добавление нового пользователя в рабочую группу и задание для него прав доступа к объектам и прав на владение объектами базы данных (это осуществляется обычно включением его в состав определённых групп внутри рабочей группы);
- добавление новой группы пользователей в рабочую группу и задание для неё прав доступа к объектам базы данных;
- удаление учётной записи пользователя из файла рабочей группы;
- удаление учётной записи группы из файла рабочей группы;
- изменение пароля пользователя;
- восстановление испорченного файла рабочей группы из резервной копии или путём его воссоздания, используя специально сохранённую информацию об учётных записях пользователей и рабочих групп (включающую имена пользователей и групп и их персональные идентификаторы (PID)).

Задачи администрирования, касающиеся защиты приложения на уровне пользователей, может выполнять только пользователь, обладающий административными правами. В Access административными правами автоматически наделяются пользователи встроенной группы Admins. Остальным пользователям разрешено только изменять пароль своей учётной записи и получать отчёт со списком пользователей и групп рабочей группы.

4.1. Использование файла рабочей группы

Рабочей группой в Access называется группа пользователей сети, совместно использующих одну или несколько баз данных Access. Если база данных защищена на уровне пользователей, в файл рабочей группы записываются учётные записи пользователей и групп, входящих в рабочую группу. Пароли пользователей также хранятся в файле рабочей группы. Учётным записям в рабочей группе могут быть назначены права доступа к базе данных и её объектам (таблицам, запросам, формам, отчётам и макросам). Права доступа сохраняются в защищённой базе данных.

Создание и подключение файла рабочей группы производится с помощью служебной программы, которая входит в состав Microsoft Access и называется ***Администратор рабочих групп***. Восстановление файла рабочей группы производится путём его воссоздания по сохранённой информации.

4.1.1. Администратор рабочих групп

Чтобы запустить служебную программу ***Администратор рабочих групп***:

1. Выберите команду меню **Сервис/Защита/Администратор рабочих групп**.
2. Появится диалоговое окно **Администратор рабочих групп**.

4.1.2. Подключение файла рабочей группы к приложению Access

Чтобы использовать базу данных, защищённую на уровне пользователей, присоедините к Access её файл рабочей группы с помощью служебной программы ***Администратор рабочих групп***:

1. Запустите *Администратор рабочих групп*.
2. Появится диалоговое окно **Администратор рабочих групп**.
3. В поле **Рабочая группа** отображается имя текущего присоединённого файла рабочей группы Access. Чтобы присоединить другой файл рабочей группы, нажмите кнопку **Связь**.
4. Появится диалоговое окно **Файл рабочей группы**. Введите в поле **Рабочая группа** полное имя файла рабочих групп или нажмите кнопку **Обзор**, чтобы выбрать нужный файл. Нажмите кнопку **ОК.**
5. Нажмите кнопку **ОК** в окне с сообщением об успешном подключении файла.
6. Нажмите кнопку **ОК,** чтобы закрыть диалоговое окно **Администратор рабочих групп**.

В результате выполнения этих действий путь к файлу рабочей группы записывается в реестр как параметр Access. Это означает, что для всех баз данных, открываемых в Access, будет использована защита на уровне пользователей на основе присоединённого файла рабочей группы. (*По умолчанию к Access присоединён файл рабочей группы с именем* System.mdw*, хранящийся в папке, в которую установлен Office XP, или в папке с личными настройками пользователя Windows. Прежде чем проводить эксперименты с файлом рабочих групп Access, рекомендуется сделать резервную копию этого файла*.)

Если нужно использовать файл рабочей группы для конкретной базы данных, создайте ярлык для открытия этой базы данных, в командной строке которого укажите параметр /wrkgrp и полное имя файла рабочей группы:

"<Путь>\MSACCE.EXE" "<Путь>\<Имя базы данных или проекта Access>" /wrkgrp "<Путь>\<Имя файла рабочей группы>"

.

4.1.3. Создание и восстановление файла рабочей группы

Чтобы создать собственный файл рабочей группы:

1. Запустите Microsoft Access, не открывая базу данных.
2. Запустите программу ***Администратор рабочих групп*** (**Сервис/Защита/Администратор рабочих групп**).
3. В появившемся диалоговом окне **Администратор рабочих групп н**ажмите кнопку **Создать**.
4. Откроется диалоговое окно **Сведения о владельце рабочей группы**. В поля **Имя** и **Организация** введите название рабочей группы и организации.
5. В поле **Код группы** введите уникальный идентификатор группы, состоящий из букв и цифр. Этот идентификатор может включать до 20 символов (см. рис.1).

Внимательно заполняйте поля с информацией о файле рабочей группы. Все три значения — имя, организация и код группы — интерпретируются с учётом регистра символов. Сохраните эту информацию в надёжном месте, чтобы в случае повреждения файла рабочей группы его можно было восстановить. Если эта информация будет утрачена, при повреждении файла рабочей группы его невозможно будет восстановить, а это может привести к безвозвратной потере доступа к защищённым объектам базы данных.

6. Нажмите кнопку **ОК**. Появится диалоговое окно, позволяющее задать имя нового файла рабочей группы. Введите полное имя файла с расширением mdw или нажмите кнопку **Обзор**, чтобы выбрать папку, в которой будет сохранён новый файл, и укажите имя файла. Нажмите кнопку **ОК**.
7. Появится диалоговое окно, позволяющее проверить введённую информацию. Нажмите кнопку **ОК**.

Созданный файл бочей группы ски присоединяется к Access. Присоединённый файл рабочей группы используется при открытии любых баз данных в Access. С этого момента все создаваемые учётные записи будут сохраняться в этом файле рабочей группы.

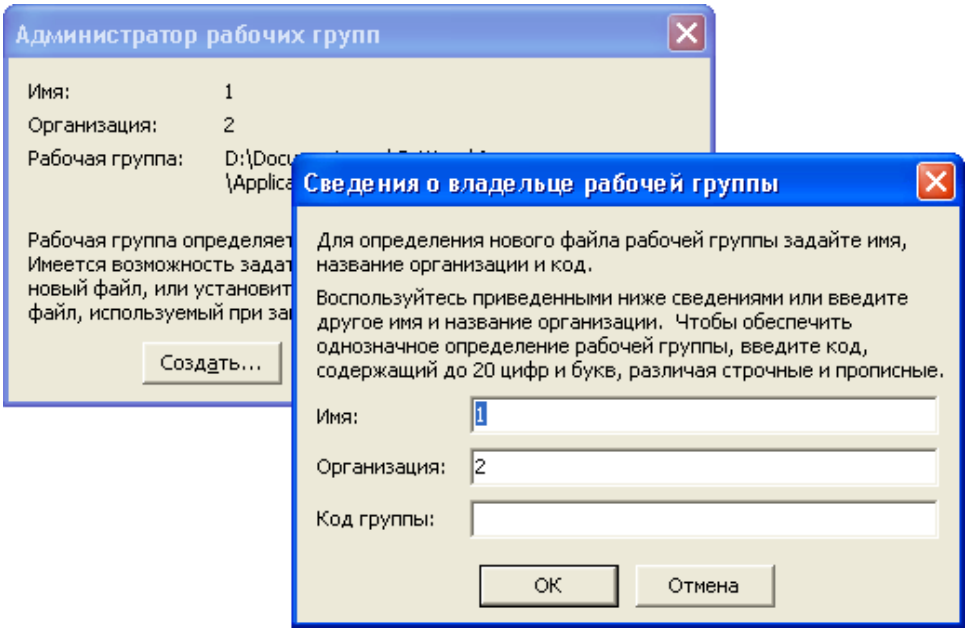


Рис. 1. ***Диалоговое окно*** **Сведения о владельце рабочей группы**.

5. *Управление учётными записями*

Управление учётными записями включает следующие действия:

- добавление или удаление учётной записи пользователя;
- добавление или удаление учётной записи пользователя-администратора;
- добавление или удаление учётной записи группы пользователей;
- добавление пользователя в группу или удаление пользователя из группы;
- изменение пароля учётной записи пользователя.

Все перечисленные действия можно выполнить в Access с помощью диалогового окна **Пользователи и группы**.

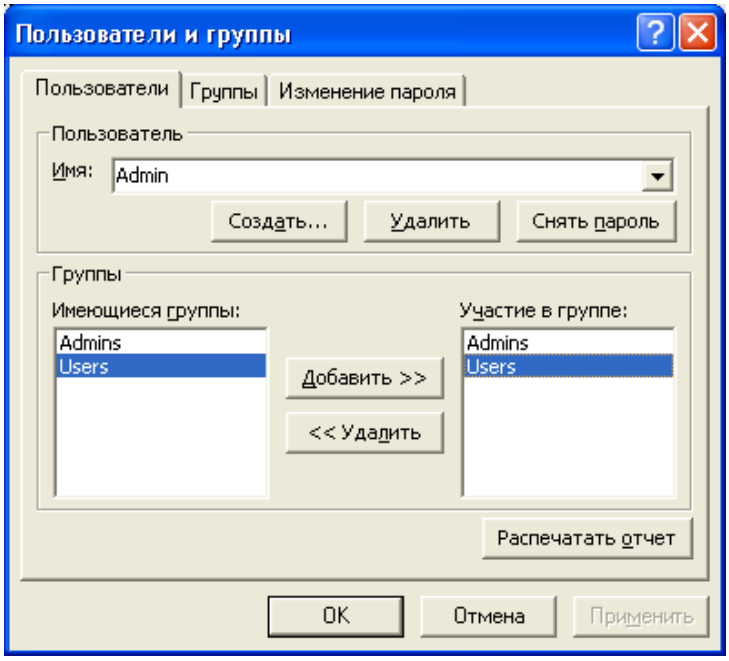


Рис. 2. ***Диалоговое окно*** **Пользователи и группы**.

Чтобы открыть диалоговое окно для управления учётными записями:

1. Удостоверьтесь, что нужный файл рабочей группы присоединён к Access или базе.
2. Откройте базу данных и зарегистрируйтесь с помощью учётной записи, обладающей административными правами (это может быть, например, встроенная учётная запись Admin).
3. Выберите команду меню **Сервис/Защита/Пользователи и группы**. Появится диалоговое окно **Пользователи и группы** (см. рис.2).

Рассмотрим процедуры выполнения ствий с учётными записями с помощью диалогового окна, представленного на рис. 3. Чтобы эти действия повлияли на систему защиты базы данных, после их выполнения необходимо нажать кнопку **ОК** в диалоговом окне **Пользователи и группы**.

Чтобы создать учётную запись пользователя:

1. На вкладке **Пользователи** диалогового окна **Пользователи и группы** нажмите кнопку **Создать**.
2. Появится диалоговое окно **Новый пользователь или группа** (см. рис. 3).
3. В поле **Имя** введите имя пользователя, а в поле **Код** — идентификатор пользователя. Нажмите кнопку **ОК.**

Имя пользователя может включать от одного до двадцати символов. В имени можно использовать буквы, цифры, пробелы и любые другие символы, кроме символов " \ [ ] : | <> + =; , . ? * . Нельзя также использовать ведущие пробелы и управляющие символы.

Необходимо ввести имя пользователя с учётом регистра и запомнить или записать его, поскольку эта информация нужна для успешной регистрации в базе данных и для восстановления файла рабочей группы в случае его повреждения.

Идентификатор пользователя (код) представляет собой последовательность от 4 до 20 символов. Идентификатор пользователя не является паролем пользователя. Вместе с именем пользователя он используется в алгоритме шифрования для вычисления идентификатора защиты учётной записи. Идентификатор пользователя, так же как идентификатор группы, является способом идентификации учётной записи в системе защиты приложения. Если файл рабочей группы будет повреждён, учётные записи в нем можно будет воссоздать если известны их идентификаторы.

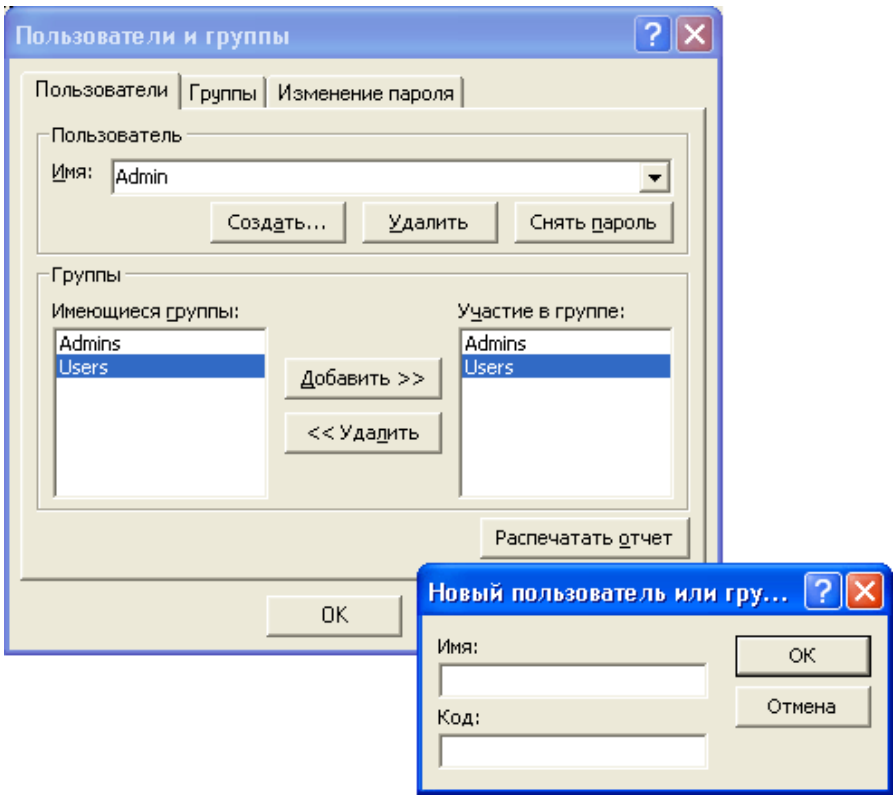


Рис. 3. ***Диалоговое окно*** **Новый пользователь или группа.**

Чтобы удалить учётную запись пользователя:

1. На вкладке **Пользователи** в раскрывающемся списке **Имя** выберите имя пользователя, соответствующее удаляемой учётной записи.
2. Нажмите кнопку **Удалить**. Появится диалоговое окно, требующее подтверждения удаления учётной записи. Нажмите кнопку **Да**.

Чтобы добавить пользователя в группу:

1. На вкладке **Пользователи** в раскрывающемся списке **Имя** выберите имя пользователя, которого нужно добавить в некоторую группу. В списке **Участие в группе** отобразится список групп, в которые включена учётная запись пользователя.
2. В списке **Имеющиеся группы** отображаются все группы, имеющиеся в файле рабочей группы. Выделите в этом списке группу, в которую нужно добавить пользователя.
3. Нажмите кнопку **Добавить** (эта кнопка отмечена двойной стрелкой вправо). Выделенное имя группы появится в списке **Участие в группе**.

Чтобы удалить пользователя из группы:

1. На вкладке **Пользователи** в раскрывающемся списке **Имя** выберите имя пользователя, которого нужно удалить из некоторой группы.
2. В списке **Участие в группе** отобразится список групп, в которые включена учётная запись пользователя. Выделите в этом списке группу, из которой нужно удалить пользователя.
3. Нажмите кнопку **Удалить** (эта кнопка отмечена двойной стрелкой влево). Выделенное имя группы будет удалено из списка **Участие в группе.**

Чтобы добавить учётную запись пользователя-администратора:

1. Создайте новую учётную запись пользователя.
2. Добавьте пользователя в группу Admins.

Чтобы удалить учётную запись пользователя-администратора:

1. Выделите учётную запись пользователя-администратора.
2. Удалите пользователя из группы Admins или удалите учётную запись пользователя.

Чтобы создать учётную запись группы:

1. Раскройте вкладку **Группы** и нажмите кнопку **Создать** (см. рис.4).
2. Появится диалоговое окно **Новый пользователь или группа**.
3. В поле **Имя** введите имя группы, а в поле **Код** (Personal ID) – идентификатор группы. Нажмите кнопку **ОК**.

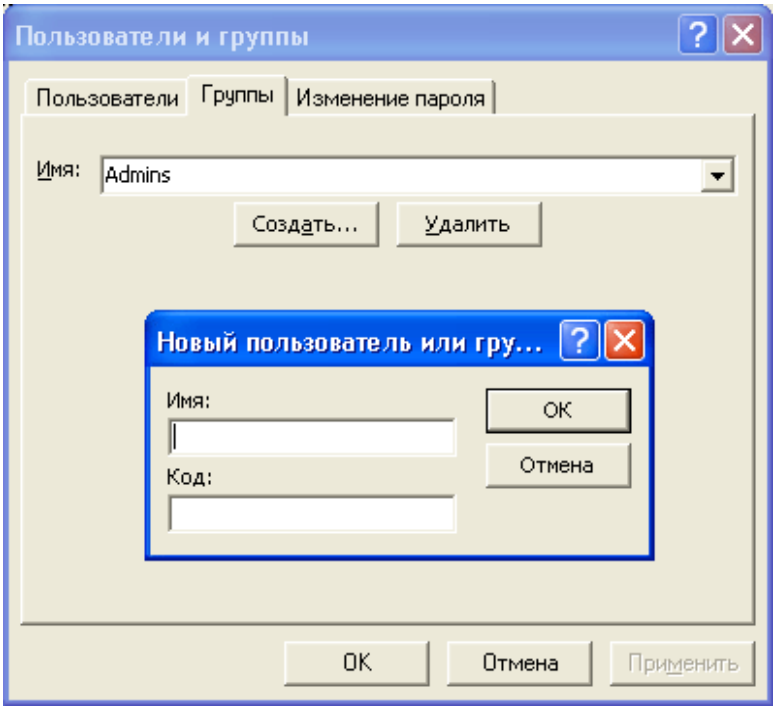


Рис. 4. ***Диалоговое окно*** **Пользователи и группы**.

Чтобы удалить учётную запись группы:

1. На вкладке **Группы** в раскрывающемся списке **Имя** выберите имя группы, которую необходимо удалить.
2. Нажмите кнопку **Удалить**. Появится диалоговое окно, требующее подтверждения удаления учётной записи. Нажмите кнопку **Да**.

Невозможно удалить системные группы Admins и Users и системную учётную запись пользователя Admin, но можно удалить системную учётную запись пользователя Admin из группы Admins. Однако в группе Admins обязательно должен быть хотя бы один пользователь, и из группы Users никакую учётную запись пользователя нельзя удалить.

Чтобы задать или изменить пароль пользователя:

1. Откройте базу данных и зарегистрируйтесь с именем пользователя, пароль которого нужно изменить.
2. Выберите команду меню **Сервис/Защита/Пользователи и группы**. Появится диалоговое окно **Пользователи и группы**.
3. Раскройте вкладку **Изменение пароля**.
4. В поле **Пользователь** отображается имя пользователя, которое было использовано при регистрации. В поле **Текущий пароль** введите текущий пароль пользователя. Если пароль пользователя не был задан, оставьте это поле пустым.
5. В поля **Новый пароль** и **Подтверждение** введите новый пароль пользователя. Нажмите кнопку **ОК.**

Чтобы заменить пароль пользователя пустым паролем:

1. Откройте диалоговое окно **Пользователи и группы**.
2. На вкладке **Пользователи** в раскрывающемся списке **Имя** выберите имя пользователя, пароль которого требуется удалить.
3. Нажмите кнопку **Снять пароль**.

Чтобы получить отчет со списком пользователей и групп рабочей группы:

1. Откройте диалоговое окно **Пользователи и группы**.
2. На вкладке **Пользователи** нажмите кнопку **Распечатать отчёт**.

6. Назначение прав доступа к объектам базы данных

Пользователям и группам пользователей рабочей группы можно назначить разные права для доступа к разным объектам базы данных, защищенной на уровне пользователей. В табл. 1 представлены возможные права доступа, которые могут быть установлены для доступа к объектам базы данных. В столбце *"Дополнительные права"* приведены права доступа, которые необходимы для получения права, указанного в столбце *"Права доступа"*. В результате того, что пользователь или группа наделяется определёнными правами, дополнительные права предоставляются автоматически.

Таблица 1. ***Права доступа, применимые к объектам в Access.***

Права доступа	Разрешенные действия	Объекты	Дополнительные права
Открытие/запуск	Открытие базы данных, формы или отчёта, запуск макроса	Базы данных, формы, отчёты и макросы	
Монопольный доступ	Открытие базы данных для монопольного доступа	Базы данных	
Чтение макета	Просмотр объектов в режиме Конструктора	Таблицы, запросы, формы, отчёты и макросы	
Изменение макета	Просмотр и изменение макета объектов или удаление объектов	Таблицы, запросы, формы, отчёты и макросы	Чтение макета, Чтение данных, Обновление данных, Удаление данных
Администратора	Для баз данных — установка пароля базы данных, репликация базы данных и изменение параметров запуска. Для объектов базы данных — все разрешения на объекты и данные, в том числе предоставление разрешений на доступ	Базы данных, таблицы, запросы, формы, отчёты и макросы	Все остальные права
Чтение данных	Просмотр данных	Таблицы и запросы	Чтение макета
Обновление данных	Просмотр и изменение данных, но без их вставки или удаления	Таблицы и запросы	Чтение макета, Чтение данных
Вставка данных	Просмотр и вставка данных, но без их изменения и удаления	Таблицы и запросы	Чтение макета, Чтение данных
Удаление данных	Просмотр и удаление данных, но без их изменения и вставки	Таблицы и запросы	Чтение макета, Чтение данных

7. Изменение прав доступа к объектам базы данных

Назначение прав доступа к объектам базы данных для учётных записей, хранящихся в файле рабочей группы, выполняется в Access с помощью диалогового окна **Разрешения**.

Чтобы открыть диалоговое окно для назначения прав доступа к объектам базы данных:

1. Откройте защищённую базу данных, подключив необходимый файл рабочей группы.
2. Зарегистрируйтесь с именем пользователя, обладающего административными правами.
3. Выберите команду меню **Сервис/Защита/Разрешения**. Появится диалоговое окно **Разрешения**.

В диалоговом окне **Разрешения** есть две вкладки: **Разрешения** и **Смена владельца**. С помощью вкладки **Разрешения** можно определить права доступа к конкретным объектам базы данных для кон-

кретных пользователей и групп. В поле **Пользователь** отображается имя пользователя, которое было применено для регистрации в момент открытия базы данных. В зависимости от того, обладает ли текущий пользователь административными правами или нет, ему будут позволены или запрещены просмотр и изменение прав доступа к объектам базы данных.

Чтобы назначить права доступа к объектам базы данных конкретной группе:

1. На вкладке **Разрешения** выберите переключатель **группы**.
2. В списке **Пользователи и группы** отобразится список всех групп в рабочей группе. Выделите в этом списке группу, права доступа которой нужно изменить.
3. Измените права доступа к объектам базы данных и нажмите кнопку **ОК.**

Чтобы назначить права доступа к объектам базы данных конкретному пользователю:

1. На вкладке **Разрешения** выберите переключатель **пользователи**.
2. В списке **Пользователи и группы** отобразится список всех пользователей в рабочей группе. Выделите в этом списке пользователя, права доступа которого нужно изменить.
3. Измените права доступа к объектам базы данных и нажмите кнопку **ОК.**

Чтобы назначить выбранному пользователю или группе права доступа к объекту базы данных:

1. На вкладке **Разрешения** в раскрывающемся списке **Тип объекта** выберите тип объекта (**Таблица**, **Запрос**, **Форма**, **Отчет** или **Макрос**).

В списке имен объектов не будут отображаться скрытые объекты, если в диалоговом окне **Параметры** на вкладке **Вид** не установлен флажок **скрытые объекты**, позволяющий отображать скрытые объекты.

2. В списке **Имя объекта** выделите имя объекта, права доступа к которому требуется изменить.
3. Чтобы предоставить определённый вид доступа, установите соответствующий флажок в группе **Разрешения**. Чтобы запретить определенный вид доступа, сбросьте соответствующий флажок в этой группе.
4. Нажмите кнопку **Применить** иначе при выборе другого пользователя, группы или другого объекта появится диалоговое окно, требующее подтверждения сделанных изменений. Чтобы подтвердить изменения, нажмите кнопку **ОК.**

Чтобы назначить пользователю или группе права доступа к базе данных:

1. На вкладке **Разрешения** в раскрывающемся списке **Тип объекта** выберите элемент **База данных**.
2. В списке **Имя** объекта отобразится элемент **<Текущая база данных>**.
3. Установите необходимые разрешения и нажмите кнопку **Применить**.

Чтобы назначить права доступа к создаваемым объектам базы данных, предоставляемые пользователю или группе:

1. На вкладке **Разрешения** в раскрывающемся списке **Тип объекта** выберите тип объекта (например, **Форма**).
2. В списке **Имя объекта** выделите элемент, обозначающий новые объекты заданного типа, права доступа к которым требуется изменить (например, **<Новые формы>**).
3. Установите необходимые разрешения и нажмите кнопку **Применить**.

Установка или сброс флажков некоторых разрешений влечёт установку или сброс других флажков разрешений, поскольку предоставление или отмена определённого вида доступа может привести к предоставлению или отмене другого вида доступа, связанного с измененным. Например, предоставление доступа к таблице вида **Чтение данных** влечёт предоставление доступа **Чтение макета**, а отмена доступа **Обновление данных** влечёт отмену доступа **Изменение макета**.

8. Предоставление права на владение объектами базы данных

Предоставление права на владение объектами базы данных производится с помощью вкладки **Смена владельца** диалогового окна **Разрешения**. Однако изменить владельца всей базы данных с помощью этого диалогового нельзя. Для этого существует отдельная процедура, описанная далее. Предоставление права на владение объектом базы данных пользователю или группе может выполнить лишь

пользователь, обладающий административными правами для этого объекта или правом на владение данным объектом.

Чтобы изменить владельца объекта базы данных (то есть предоставить право на владение этим объектом):

1. Откройте диалоговое окно **Разрешения**, как было описано выше.
2. Раскройте вкладку **Смена владельца** (см. рис. 5).
3. В списке **Тип объекта** выберите тип объекта, право на владение которого нужно предоставить другому пользователю или группе.
4. В списке **Объект** отобразится список всех объектов базы данных заданного типа. Напротив каждого из объектов — в списке **Текущий владелец** — отобразится имя пользователя или группы, которой в настоящее время назначено право на владение объектом.
5. Выделите в списке **Объект** имя объекта, владельца которого нужно изменить.
6. Чтобы назначить в качестве нового владельца объекта конкретного пользователя, выберите переключатель **пользователи**, а затем в раскрывающемся списке **Новый владелец** выберите имя этого пользователя. Чтобы назначить в качестве нового владельца объекта группу, выберите переключатель **группы**, а затем в раскрывающемся списке **Новый владелец** выберите имя этой группы.

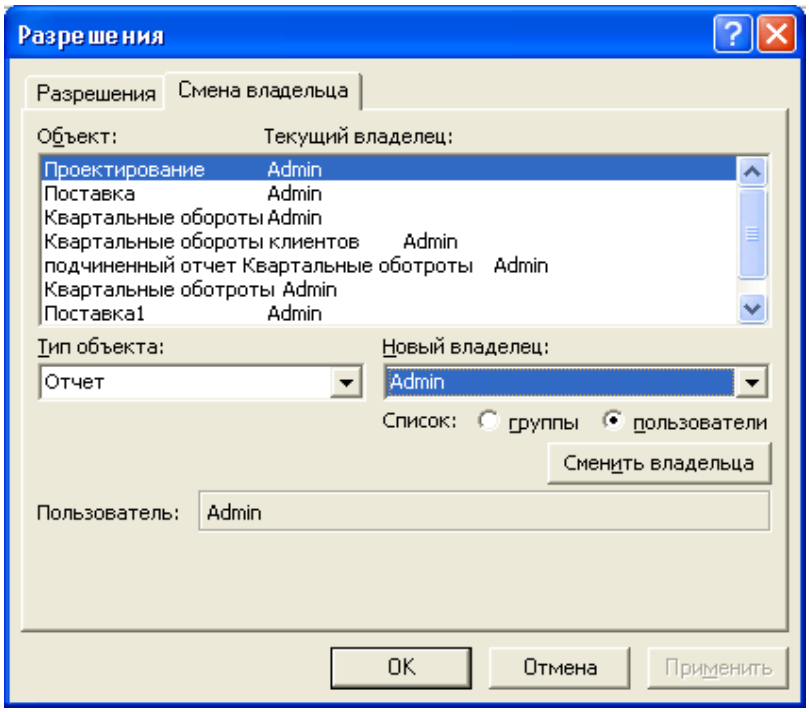


Рис. 5. ***Вкладка*** **Смена владельца** ***диалогового окна*** **Разрешения**.

7. Нажмите кнопку **Сменить владельца**. Напротив имени объекта отобразится имя его нового владельца.
8. Нажмите кнопку **ОК,** чтобы закрыть диалоговое окно **Разрешения**.

Чтобы назначить нового владельца базы данных:

1. Запустите Microsoft Access, подключив файл рабочих групп, содержащий учётную запись нового владельца.
2. Создайте новую базу данных, зарегистрировавшись с именем нового владельца.
3. Импортируйте в созданную базу данных все объекты базы данных, владельца которой нужно изменить.

Для импорта объектов базы данных необходимо обладать правами *Открытие/запуск* для базы данных и *Чтение макета* для всех объектов. В противном случае будут импортированы только те объекты, на которые есть необходимые права доступа. Рекомендуется перед импортированием объектов открыть исходную базу данных, зарегистрировавшись с именем пользователя, обладающего административными правами, и предоставить права на *Чтение макета* для всех объектов в группе Users.

Задание

1. В папке **Мои документы\Преподаватели\Ковалькова\Информационная безопасность** найдите файл базы данных ***Прокат.****mdb* и скопируйте его в свою рабочую папку (после чего окно папки **Информационная безопасность** закройте).
2. Скопированную базу данных переименуйте в ***Прокат1****.mdb*.
3. Чтобы застраховаться от потери данных создайте в своей папке резервную копию базы данных ***Прокат1****.mdb* с помощью обычного копирования. Полученную копию базы данных сохраните под именем ***Прокат1_копия****.mdb*.
4. Запустите MS Access, не открывая базы данных.

5. Выполните сжатие находящейся в вашей папке базы данных ***Прокат1_копия***.mdb, сохранив её под именем ***Прокат1_копия_сжатая***.mdb.

6. Сравните размеры баз данных ***Прокат1_копия***.mdb и ***Прокат1_копия_сжатая***.mdb.

7. Для базы данных ***Прокат1***.mdb установите автоматическое сжатие при каждом её закрытии.

8. Выполните шифрование базы данных ***Прокат1_копия***.mdb, сохранив её под именем ***Прокат1_копия_шифрованная***.mdb.

9. Сравните размеры баз данных ***Прокат1_копия***.mdb и ***Прокат1_копия_шифрованная***.mdb.

10. Отмените автоматическое сжатие базы данных ***Прокат1***.mdb при каждом её закрытии.

11. Установите пароль **777** для защиты базы данных ***Прокат1_копия***.mdb.

12. Закройте базу данных ***Прокат1_копия***.mdb, а затем снова откройте её.

13. Удалите пароль защиты базы данных ***Прокат1_копия***.mdb.

14. В своей папке создайте новую папку с именем **Базы данных** и перенесите в неё файлы баз данных:

- ***Прокат1_копия***.mdb;
- ***Прокат1_копия_сжатая***.mdb;
- ***Прокат1_копия_шифрованная***.mdb.

15. Вернитесь в свою рабочую папку и создайте файл рабочей группы со следующими характеристиками:

а) Имя – **My**;
б) Организация – **BNTU**;
в) Код – **12345**.

16. Сохраните файл рабочей группы в вашей рабочей папке под именем *Security.mdw*.

17. Для базы данных ***Прокат1***.mdb создайте три учётные записи пользователей и добавьте их в группы:

а) **Add** (код – **Add1**, группа *Admins*,) – пользователь-администратор;
б) **Din** (код – **Din2**, группа *Users*) – пользователь;
в) **Den** (код – **Den3**, группа *Users*) – пользователь.

18. Для пользователя **Admin** задайте пароль 111.

19. Закройте базу данных ***Прокат1***.mdb, а затем снова откройте её под именем **Admin**.

20. Закройте базу данных ***Прокат1***.mdb, а затем снова откройте её под именем **Den**.

21. Закройте базу данных ***Прокат1***.mdb, а затем снова откройте её, но уже под именем **Din**.

22. Для пользователя **Din** задайте пароль 222.

23. Закройте базу данных ***Прокат1***.mdb, а затем снова откройте её под именем **Din**. Попробуйте удалить пользователя **Din**, а затем закройте базу данных.

24. Откройте базу данных под именем пользователя-администратора **Add** и снимите пароль с пользователя **Din**, а затем удалите пользователя **Din**.

25. Закройте базу данных ***Прокат1***.mdb, а затем снова откройте её под именем **Admin**.

26. Закройте базу данных ***Прокат1***.mdb, а затем снова откройте её, но уже под именем **Add**.

27. Удалите пользователя **Admin** из группы *Admins*.

28. На Рабочем столе создайте ярлык, который будет запускать вашу базу данных ***Прокат1***.mdb с использованием файла рабочей группы. При создании ярлыка в командную строку введите:

"C:\Program Files\Microsoft Office\Office10\MSACCESS.EXE" "C:\Documents and Settings\Студент\My Documents\3 курс\108616-1\Прокат1.mdb" /WRKGRP "C:\Documents and Settings\Студент\My Documents\3 курс\108616-1\Security.mdw"

Созданный ярлык будет иметь имя *MSACCESS.EXE*.

29. Переименуйте созданный ярлык на Рабочем столе в ***Прокат1***.

В дальнейшем, загружайте базу данных *Прокат1.mdb* с помощью созданного для неё ярлыка на Рабочем столе.

30. С помощью созданного ярлыка на Рабочем столе откройте базу данных ***Прокат1***.mdb под именем пользователя-администратора **Add** и создайте две учётные записи групп со следующими характеристиками:

а) Имя группы – **Hackers** (код – **Hackers1**);
б) Имя группы – **Good** (код – **Good1**).

31. Затем создайте две учётные записи пользователей и добавьте их в группы:

а) **Ann** (код – **Ann4**, группа *Hackers*) – пользователь;

б) **All** (код – **All5**, группа *Good*) – пользователь.

32. Установите отображение скрытых объектов базы данных.
33. Добавьте в группу **Hackers** пользователя **Den**.
34. Добавьте в группу **Good** пользователя **Add**.
35. Отмените группе **Users** следующие права: просмотр любой из таблиц.
36. Назначьте группе **Good** следующие права: просмотр любой из таблиц.
37. Закройте базу данных.
38. С помощью ярлыка загрузите базу данных ***Прокат1.mdb*** под именем **Ann** и попробуйте открывать любые таблицы. Затем закройте базу данных.
39. С помощью ярлыка загрузите базу данных ***Прокат1.mdb*** под именем **All** и попробуйте открывать любые таблицы. Затем закройте базу данных.
40. С помощью ярлыка загрузите базу данных ***Прокат1.mdb*** под именем **Ann**.
41. Удалите пользователя **All**.
42. Удалите пользователя **Add** из группы **Good**.
43. Попробуйте открывать любые таблицы базы данных.
44. Закройте базу данных.
45. Перед завершением работы в классе удалите из вашей папки файл рабочей группы *Security.mdw*.

Контрольные вопросы

1. Какие существуют способы защиты баз данных MS Access от несанкционированного доступа?
2. Для чего осуществляется сжатие базы данных?
3. Можно ли сжать файл базы данных, чтобы при этом остался на диске и первоначальный вариант этого файла (т.е. не сжатый) ? Если можно, то как это сделать?
4. Можно ли зашифровать базу данных, для которой определена защита на уровне пользователей?
5. Что называется *рабочей группой* в Access?
6. Как создаётся файл рабочей группы?
7. Какая информация хранится в файле рабочей группы?
8. Какие действия включает процесс управления учётными записями?
9. Как создаётся/удаляется учётная запись пользователя?
10. Как создаётся/удаляется учётная запись группы?
11. Как добавляется учётная запись в группу?
12. В какую группу добавляется учётная запись пользователя-администратора?
13. Как можно задать или изменить пароль пользователя, для которого создана учётная запись?
14. Как назначаются права доступа к объектам базы данных для конкретной группы?
15. Как назначаются выбранной группе права доступа к объекту базы данных?
16. Как устанавливается отображение скрытых объектов базы данных?
17. Можно ли назначить нового владельца для базы данных. Если можно, то как это сделать?

IV. КОНТРОЛЬ ЗНАНИЙ

Вопросы к зачёту

1. Основные понятия защиты информации и информационной безопасности: основные термины и определения. Основные составляющие информационной безопасности.
2. Виды угроз информационной безопасности. Классификация возможных угроз информационной безопасности АС.
3. Типы атак на компьютерную систему.
4. Наиболее распространённые угрозы безопасности. Каналы утечки информации.
5. Основные способы несанкционированного доступа к информации. Модель нарушителя.
6. Методы защиты от несанкционированного доступа (НСД) в компьютерных системах.
7. Идентификация. Протокол идентификации.
8. Аутентификация. Способы аутентификации пользователя в КС.
9. Аутентификация пользователей на основе паролей и модели «рукопожатия».
10. Аутентификация пользователей на основе PIN-кода.
11. Аутентификация пользователей по их биометрическим характеристикам, клавиатурному почерку и росписи мышью.

12. Программно-аппаратная защита информации от локального НСД.
13. Защита Интернет-подключений.
14. Функции и назначение межсетевых экранов.
15. Виртуальные частные сети (VPN), их назначение и использование в информационных системах.
16. Временные файлы. Методы контроля над временными файлами операционной системы и приложений.
17. Стандарты информационной безопасности.
18. Вредоносные программы и их классификация.
19. Основные каналы распространения компьютерных вирусов и других вредоносных программ. Методы обнаружения и удаления вирусов.
20. Антивирусные программы и комплексы.
21. Программные закладки и методы защиты от них.
22. Анонимное использование Интернет ресурсов. Выбор провайдера. Маскировка IP-адреса.
23. Использование специализированных программ и сервисов.
24. Безопасное использование электронной почты (E-mail), выбор почтового клиента. Защита от спама.
25. Криптография как наука. Основные понятия. Типы криптосистем.
26. Электронная цифровая подпись и её применение.
27. Компьютерная стенография и её применение.
28. Протоколирование и аудит. Задачи и функции аудита.
29. Структура журналов аудита. Активный аудит, методы активного аудита. Средства анализа и аудита.
30. Основные факторы, влияющие на обеспечение информационной безопасности таможенных органов. Основные угрозы информационной безопасности таможенных органов.
31. Модель нарушителя информационной безопасности таможенных органов.
32. Цели, основные задачи и принципы обеспечения информационной безопасности таможенных органов Республики Беларусь.

V. ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Литература

1. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: учеб. Пособие для студ. высш. учеб. заведений / П.Б. Хорев. – 3-е изд., стер. – М.: Издательский центр «Академия», 2007. – 256 с.
2. Леонтьев В.П. Безопасность в сети Интернет. – М.: ОЛМА Медиа Групп, 2008. – 256 с.
3. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. – М.: ИД «ФОРУМ»: ИНФРА-М, 2009. – 416 с.
4. Компьютерная безопасность: Криптогр. методы защиты / Петров А.А.. – М.: ДМК, 2000. - 445 с.
5. Локальные сети и безопасность Microsoft Windows XP. Inside out: [перевод с английского] / Эд Ботт, Карл Зихерт. - Москва: ЭКОМ, 2007. - 941, [2] с.
6. Современная компьютерная безопасность: теоретические основы, практические аспекты: учебное пособие / А. Ю. Щербаков. - Москва: Книжный мир, 2009. - 351, [1] с.
7. Основы защиты сетей: Прил. и стандарты: Пер. с англ. / Вильям Столлингс. - М. и др.: Вильямс, 2002. - 429 с.

Компьютерные программы

1. Операционная система Windows XP
2. Пакет программ MS Office 2003/2007
3. Программы защиты информации от несанкционированного доступа
4. Программы криптографической защиты
5. Программы шифрования данных
6. Антивирусный пакет Dr. Weber (или NOD 32)

Дагестанский гос ударственный технический

университет

Декан
факультета

_____
(подпись) (И.О.Фамилия)

___.___.20___
(дата утверждения)

Р

Информационная безопасность таможенных служб
(наименование дисциплины)

Учебная программа для специальности:
“Таможенное дело”
(код специальности) (Наименование специальности)

(название факультета)

Кафедра «Таможенное дело»
(название кафедры)

Курс (курсы) _____

Семестр (семестры) _____

Лекции _____ Экзамен _____
(количество часов) (семестр)

Практические (семинарские) занятия _____ Зачет _____
(количество часов) (семестр)

Лабораторные занятия _____ Курсовая работа _____
(количество часов) (семестр)

Всего аудиторных часов по дисциплине _____
(количество часов)

Всего часов по дисциплине _____ Форма получения высшего образования дневная
(количество часов)

Составила И. А. Ковалькова, ст. преподаватель

2010 г.

Учебная программа составлена на основе базовой программы по дисциплине «Информационная безопасность таможенных служб».

Рассмотрена и рекомендована к утверждению в качестве варианта УМК на заседании кафедры _____Таможенное дело_____
(название кафедры)

« » _____ 20___ г., протокол № 10
(дата, номер протокола)

Заведующий кафедрой _____ Е.Г.
(подпись) (И.О.Фамилия)

Одобрена и рекомендована к утверждению методической комиссией ДГТУ
(название высшего учебного заведения)

« » июня 20___ г., протокол №
(дата, номер протокола)

Председатель _____
(подпись) (И.О.Фамилия)

I. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Учебная программа дисциплины «Информационная безопасность таможенных служб» разработана для студентов специальности 38.05.02 «Таможенное дело».

Данная программа определяет содержание лекционного материала и тематику лабораторных занятий.

Цель преподавания дисциплины. Целью дисциплины «Информационная безопасность таможенных служб» является ознакомление студентов с фундаментальными понятиями, основными определениями и методами обеспечения информационной безопасности в условиях широкого применения современных информационных технологий. А именно, изучение информационных угроз, их нейтрали-зации, вопросов организации мер защиты информационных ресурсов, норматив-ных документов, регламентирующих информационную деятельность, криптогра-фических методов защиты информации, другие вопросы, связанные с обеспечени-ем безопасности компьютерных сетей.

Основное внимание в рамках дисциплины уделяется рассмотрению методов защиты от несанкционированного доступа к информации в компьютерных сетях с помощью программных и программно-технических средств, базирующихся на криптографических преобразованиях; угроз в коммуникационных сетях и мер по предотвращению попыток реализации этих угроз, основ построения и использования межсетевых экранов, практических вопросов сетевой безопасности, методов обеспечения надёжного хранения информации в компьютерных сетях.

Преподавание дисциплины «Информационная безопасность таможенных служб» должно способствовать повышению уровня подготовки специалистов таможенных органов с целью соответствия профессиональным компетенциям в области информационных технологий.

Задачи изучения дисциплины. Задача дисциплины «Информационная безопасность таможенных служб» состоит в получении студентами основных теоретических знаний по защите информации от несанкционированного доступа в компьютерных системах и сетях: методам обеспечения конфиденциальности, целостности и доступности информации; средствам защиты документов Microsoft Office; средствам обеспечения безопасности баз данных путём разграничения доступа к информации; средствам криптографии; методам и средствам защиты информации от вредоносных программ – компьютерных вирусов и программных закладок. Также студенты должны быть ознакомлены с основными стандартами информационной безопасности.

Полученные теоретические сведения должны быть закреплены на практике в ходе выполнения лабораторных работ.

Перечень дисциплин, усвоение которых необходимо для изучения данной дисциплины. Материал курса «Информационная безопасность таможенных служб» базируется на знаниях по ряду дисциплин:

– «Основы информатики и вычислительной техники»;
– «Технологии организации, хранения и обработки данных»;
– «Делопроизводство в таможенных органах».

В результате освоения курса «Информационная безопасность таможенных служб» студент должен

знать:

– содержание основных понятий обеспечения информационной безопасности;
– основные виды угроз информационной безопасности, методы их выявления и блокирования;
– методы и средства защиты от несанкционированного доступа к информации в компьютерных системах;
– методы защиты информации от несанкционированного доступа в операционных системах;
– криптографические методы обеспечения информационной безопасности;
– способы защиты компьютерных систем от вредоносных программ;

уметь:

– обеспечивать защиту информации штатными средствами операционной системы;
– осуществлять эффективный выбор компьютерных систем защиты;
– применять различные технологии защиты информации в реальных инфраструктурах.

приобрести навыки:

– обеспечения информационной безопасности на рабочем месте, (в т. ч. АРМ).

Знания и умения, полученные студентами при изучении данной дисциплины, необходимы для освоения последующих специальных дисциплин, связанных с информационными технологиями.

Дисциплина излагается в течение одного семестра, курс рассчитан на объём 74 учебных часа, из них – 34( ) аудиторных часа. Примерное распределение аудиторных часов по видам занятий и семестрам:

6 семестр: лекций – 17 ( ) часов, лабораторных работ – 17 ( ) часов.

II. СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема № 1. Основные понятия и анализ угроз информационной безопасности

Основные понятия защиты информации и информационной безопасности: основные термины и определения. Угрозы информационной безопасности и их классификация. Наиболее распространённые угрозы безопасности. Каналы утечки информации.

Тема № 2. Защита информации от несанкционированного доступа

Способы несанкционированного доступа к информации. Методы защиты от НСД в компьютерных системах. Идентификация. Аутентификация. Программно-аппаратная защита информации от локального НСД.

Тема № 3. Безопасное использование информационной среды

Защита Интернет-подключений, функции и назначение межсетевых экранов. Виртуальные частные сети (VPN), их назначение и использование в информационных системах. Временные файлы. Методы контроля над временными файлами операционной системы и приложений. Стандарты информационной безопасности.

Тема № 4. Защита компьютерных систем от вредоносных программ

Вредоносные программы и их классификация. Основные каналы распространения компьютерных вирусов и других вредоносных программ. Методы обнаружения и удаления вирусов. Антивирусные программы и комплексы. Программные закладки и методы защиты от них.

Тема № 5. Безопасное использование интернет-ресурсов

Анонимное использование Интернет ресурсов. Выбор провайдера. Маскировка IP-адреса. Использование специализированных программ и сервисов. Безопасное использование электронной почты (E-mail), выбор почтового клиента. Защита от спама.

Тема № 6. Криптографические методы обеспечения информационной безопасности

Криптография как наука. Основные понятия. Типы криптосистем. Электронная цифровая подпись и её применение. Компьютерная стенография и её применение.

Тема № 7. Анализ защищённости локальной вычислительной сети и её узлов

Протоколирование и аудит. Задачи и функции аудита. Структура журналов аудита. Активный аудит, методы активного аудита. Средства анализа и аудита.

Тема № 8. Защита таможенных информационных систем

Основные факторы, влияющие на обеспечение информационной безопасности таможенных органов. Основные угрозы информационной безопасности таможенных органов. Модель нарушителя информационной безопасности таможенных органов. Цели, основные задачи и принципы обеспечения информационной безопасности таможенных органов Республики Беларусь.

III. УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА

Номер раздела, темы, занятия	Название раздела, темы, занятия, перечень изучаемых вопросов	Количество аудиторных часов				Материальное обеспечение занятия (наглядн., методические пособия и др.)	Литература	Формы контроля знаний
		лекции	практические занятия	лабораторные занятия	СУРС			
1	2	3	4	5	6	7	8	9
1.	**ОСНОВНЫЕ ПОНЯТИЯ И АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. (4 ч.)**							
1.1	Основные понятия защиты информации и информационной безопасности: основные термины и определения. Угрозы информационной безопасности и их классификация. Наиболее распространённые угрозы безопасности. Каналы утечки информации.	2					[1], [4], [6]	
1.2	Программное обеспечение безопасности информационных систем.					Электронный лабораторный практикум		Защита отчета
2.	**ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА**. (4 **ч.**)							
2.1	Способы несанкционированного доступа к информации. Методы защиты от НСД в компьютерных системах. Идентификация. Аутентификация. Программно-аппаратная защита информации от локального НСД.						[1], [3], [4], [5], [6], [9]	
2.2	Основные признаки присутствия на компьютере вредоносных программ.					Электронный лабораторный практикум		Защита отчета
3.	**БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННОЙ СРЕДЫ**. (4 **ч.**)							

3.1	Защита Интернет-подключений, функции и назначение межсетевых экранов. Виртуальные частные сети (VPN), их назначение и использование в информационных системах. Временные файлы. Методы контроля над временными файлами операционной системы и приложений. Стандарты информационной безопасности.						[2], [3], [4], [5], [6], [7]	
3.2	Безопасность компьютера в Сети Интернет.					Электронный лабораторный практикум		Защита отчета
4.	**ЗАЩИТА КОМПЬЮТЕРНЫХ СИСТЕМ ОТ ВРЕДОНОСНЫХ ПРОГРАММ**. (4 **ч**.)							
4.1	Вредоносные программы и их классификация. Основные каналы распространения компьютерных вирусов и других вредоносных программ. Методы обнаружения и удаления вирусов. Антивирусные программы и комплексы. Программные закладки и методы защиты от них.						[2], [3], [4], [5], [6], [7]	
4.2	Компьютерные вирусы и защита от них.					Электронный лабораторный практикум		Защита отчета
5.	**БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ ИНТЕРНЕТ-РЕСУРСОВ**. (6 **ч**.)							
5.1	Анонимное использование Интернет ресурсов. Выбор провайдера. Маскировка IP-адреса. Использование специализированных программ и сервисов. Безопасное использование электронной почты (E-mail), выбор почтового клиента. Защита от спама.						[2], [3], [5], [7], [11]	
5.2	Защита от несанкционированного доступа баз данных Microsoft Access.					Электронный лабораторный практикум		Защита отчета
6.	**КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**. (7 **ч**.)							
6.1	Криптография как наука. Основные понятия. Типы криптосистем. Электронная цифровая подпись и её применение. Компьютерная стенография и её применение.						[3], [4], [7], [10], [12]	

6.2	Криптографические методы и средства защиты информации.					Электронный лабораторный практикум		Защита отчета
7.	**АНАЛИЗ ЗАЩИЩЁННОСТИ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ И ЕЁ УЗЛОВ. (2 ч.)**							
7.1	Протоколирование и аудит. Задачи и функции аудита. Структура журналов аудита. Активный аудит, методы активного аудита. Средства анализа и аудита.						[2], [3], [4], [5], [6], [7]	
8.	**ЗАЩИТА ТАМОЖЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ**. (3 **ч**.)							
8.1	Основные факторы, влияющие на обеспечение информационной безопасности таможенных органов. Основные угрозы информационной безопасности таможенных органов. Модель нарушителя информационной безопасности таможенных органов. Цели, основные задачи и принципы обеспечения информационной безопасности таможенных органов Республики Беларусь.						[2], [3], [4], [5], [6], [7], [14], [15], [16], [17]	

IV. ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

4.1 ОСНОВНАЯ ЛИТЕРАТУРА

8. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: учеб. Пособие для студ. высш. учеб. заведений / П.Б. Хорев. – 3-е изд., стер. – М.: Издательский центр «Академия», 2007. – 256 с.

9. Леонтьев В.П. Безопасность в сети Интернет. – М.: ОЛМА Медиа Групп, 2008. – 256 с.

10. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. – М.: ИД «ФОРУМ»: ИНФРА-М, 2009. – 416 с.

11. Компьютерная безопасность: Криптогр. методы защиты / Петров А.А.. – М.: ДМК, 2000. - 445 с.

12. Локальные сети и безопасность Microsoft Windows XP. Inside out: [перевод с английского] / Эд Ботт, Карл Зихерт. - Москва: ЭКОМ, 2007. - 941, [2] с.

13. Современная компьютерная безопасность: теоретические основы, практические аспекты: учебное пособие / А. Ю. Щербаков. - Москва: Книжный мир, 2009. - 351, [1] с.

14. Основы защиты сетей: Прил. и стандарты: Пер. с англ. / Вильям Столлингс. - М. и др.: Вильямс, 2002. - 429 с.

4.2 ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

15. Информационная безопасность: учебник для вузов: по гуманитарным и социально-экономическим специальностям / В.И.Ярочкин. - Москва: Трикста: Академический проект, 2005. - 542, [1] с.

16. Аутентификация: от паролей до открытых ключей: Пер. с англ. / Ричард Э. Смит. - М. и др.: Вильямс, 2002. - 424 с.

17. Коды и шифры: Юлий Цезарь, "Энигма" и Интернет: перевод с английского / Роберт Черчхаус. - Москва: Весь мир, 2005. - XII, 302 с.

18. Безопасная работа в Internet: эффективный самоучитель: перевод с английского / Уоллес Ванг. - Санкт-Петербург [и др.]: ДиаСофтЮП, 2005. - 397 с.

19. Основы криптографии: учебное пособие для высших учебных заведений по группе специальностей в области информационной безопасности / А.П.Алферов [и др.]. - Москва: Гелиос АРВ, 2005. - 479, [1] с.

20. Основы информационной безопасности: учебное пособие по специальностям "Компьютерная безопасность", "Комплексное обеспечение информационной безопасности автоматизированных систем" и "Информационная безопасность телекоммуникационных систем" / С. П. Расторгуев. - Москва: Академия, 2007. - 186, [1] с.

21. Информационная безопасность в рамках интеграционных процессов: политологический анализ / Габдыжамалов Нурлан Муратказыевич: автореферат диссертации на соискание ученой степени кандидата политических наук: 23.00.02. - Астана, 2010.

22. Информационные технологии. Технологии безопасности. Системы управления защитой информации. Требования: СТБ П ISO/IES 27001-2008. - Минск: Госстандарт: Белорусский государственный институт стандартизации и сертификации, печ. 2008 - VI, 27, [1] с., включая обложку – (Предварительный государственный стандарт Республики Беларусь).

23. Информационные технологии. Методы и средства безопасности. Программные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Оценка качества: СТБ П 34.101.12-2004. - Мн.: Госстандарт: Белорус. гос. ин-т стандартизации и сертификации, 2004. - III, 11 с., включ. обложку. – (Предварительный государственный стандарт Республики Беларусь).

24. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Профиль защиты электронной почты предприятия: СТБ П 34.101.4-2010. - Минск: Госстандарт: Белорусский государственный институт стандартизации и сертификации, печ. 2010 - IV, 33 с. – (Предварительный государственный стандарт Республики Беларусь).

4.3 ТЕМАТИКА ЛАБОРАТОРНЫХ ЗАНЯТИЙ (6 СЕМЕСТР)

ТЕМА 1. Программное обеспечение безопасности информационных систем.

ТЕМА 2. Основные признаки присутствия на компьютере вредоносных программ.

ТЕМА 3. Безопасность компьютера в Сети Интернет.

ТЕМА 4. Компьютерные вирусы и защита от них.

ТЕМА 5. Защита от несанкционированного доступа баз данных Microsoft Access.

ТЕМА 6. Криптографические методы и средства защиты информации.

4.4 КОМПЬЮТЕРНЫЕ ПРОГРАММЫ

7. Операционная система Windows XP
8. Пакет программ MS Office 2003/2007
9. Программы защиты информации от несанкционированного доступа
10. Программы криптографической защиты
11. Программы шифрования данных
12. Антивирусный пакет Dr. Weber (или NOD 32)

4.3 ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ (6 семестр)

33. Основные понятия защиты информации и информационной безопасности: основные термины и определения. Основные составляющие информационной безопасности.

34. Виды угроз информационной безопасности. Классификация возможных угроз информационной безопасности АС.

35. Типы атак на компьютерную систему.

36. Наиболее распространённые угрозы безопасности. Каналы утечки информации.

37. Основные способы несанкционированного доступа к информации. Модель нарушителя.

38. Методы защиты от НСД в компьютерных системах.

39. Идентификация. Протокол идентификации.

40. Аутентификация. Способы аутентификации пользователя в КС.

41. Аутентификация пользователей на основе паролей и модели «рукопожатия».

42. Аутентификация пользователей на основе PIN-кода.

43. Аутентификация пользователей по их биометрическим характеристикам, клавиатурному почерку и росписи мышью.

44. Программно-аппаратная защита информации от локального НСД.

45. Защита Интернет-подключений.

46. Функции и назначение межсетевых экранов.

47. Виртуальные частные сети (VPN), их назначение и использование в информационных системах.

48. Временные файлы. Методы контроля над временными файлами операционной системы и приложений.

49. Стандарты информационной безопасности.

50. Вредоносные программы и их классификация.

51. Основные каналы распространения компьютерных вирусов и других вредоносных программ. Методы обнаружения и удаления вирусов.

52. Антивирусные программы и комплексы.

53. Программные закладки и методы защиты от них.

54. Анонимное использование Интернет ресурсов. Выбор провайдера. Маскировка IP-адреса.

55. Использование специализированных программ и сервисов.

56. Безопасное использование электронной почты (E-mail), выбор почтового клиента. Защита от спама.

57. Криптография как наука. Основные понятия. Типы криптосистем.

58. Электронная цифровая подпись и её применение.

59. Компьютерная стенография и её применение.

60. Протоколирование и аудит. Задачи и функции аудита.

61. Структура журналов аудита. Активный аудит, методы активного аудита. Средства анализа и аудита.

62. Основные факторы, влияющие на обеспечение информационной безопасности таможенных органов. Основные угрозы информационной безопасности таможенных органов.

63. Модель нарушителя информационной безопасности таможенных органов.

64. Цели, основные задачи и принципы обеспечения информационной безопасности таможенных органов ~~РД~~.

V. ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ ПО ИЗУЧАЕМОЙ УЧЕБНОЙ ДИСЦИПЛИНЕ С ДРУГИМИ ДИСЦИПЛИНАМИ СПЕЦИАЛЬНОСТИ

Название дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы по изучаемой учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)

VI. ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ ПО ИЗУЧАЕМОЙ УЧЕБНОЙ ДИСЦИПЛИНЕ

на _____/_____ учебный год

№№ пп	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры
____Таможенное дело_____(протокол № ____ от _____ 20__ г.)
(наименование кафедры)

Заведующий кафедрой

_____ _____ _____
(степень, звание) (подпись) (И.О.Фамилия)

УТВЕРЖДАЮ
Декан факультета

_____ _____ _____
(степень, звание) (подпись) (И.О.Фамилия)

III. УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА

Номер раздела, темы, занятия	Название раздела, темы, занятия, перечень изучаемых вопросов	Количество аудиторных часов				Материальное обеспечение занятия (наглядн., методические пособия и др.)	Литература	Формы контроля знаний
		лекции	практические занятия	лабораторные занятия	СУРС			
1	2	3	4	5	6	7	8	9
1.	**ОСНОВНЫЕ ПОНЯТИЯ И АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**. (6 **ч.)**							
1.1	Основные понятия защиты информации и информационной безопасности: основные термины и определения. Угрозы информационной безопасности и их классификация. Наиболее распространённые угрозы безопасности. Каналы утечки информации.						[1], [4], [6]	
1.2	Программное обеспечение безопасности информационных систем.					Электронный лабораторный практикум		Защита отчета
2.	**ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА**. (6 **ч.**)							
2.1	Способы несанкционированного доступа к информации. Методы защиты от НСД в компьютерных системах. Идентификация. Аутентификация. Программно-аппаратная защита информации от локального НСД.						[1], [3], [4], [5], [6], [9]	
2.2	Основные признаки присутствия на компьютере вредоносных программ.					Электронный лабораторный практикум		Защита отчета
3.	**БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННОЙ СРЕДЫ**. (6 **ч.**)							

3.1	Защита Интернет-подключений, функции и назначение межсетевых экранов. Виртуальные частные сети (VPN), их назначение и использование в информационных системах. Временные файлы. Методы контроля над временными файлами операционной системы и приложений. Стандарты информационной безопасности.						[2], [3], [4], [5], [6], [7]	
3.2	Безопасность компьютера в Сети Интернет.					Электронный лабораторный практикум		Защита отчета
4.	**ЗАЩИТА КОМПЬЮТЕРНЫХ СИСТЕМ ОТ ВРЕДОНОСНЫХ ПРОГРАММ**. (6 **ч**.)							
4.1	Вредоносные программы и их классификация. Основные каналы распространения компьютерных вирусов и других вредоносных программ. Методы обнаружения и удаления вирусов. Антивирусные программы и комплексы. Программные закладки и методы защиты от них.						[2], [3], [4], [5], [6], [7]	
4.2	Компьютерные вирусы и защита от них.					Электронный лабораторный практикум		Защита отчета
5.	**БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ ИНТЕРНЕТ-РЕСУРСОВ**. (8 **ч**.)							
5.1	Анонимное использование Интернет ресурсов. Выбор провайдера. Маскировка IP-адреса. Использование специализированных программ и сервисов. Безопасное использование электронной почты (E-mail), выбор почтового клиента. Защита от спама.						[2], [3], [5], [7], [11]	
5.2	Защита от несанкционированного доступа баз данных Microsoft Access.					Электронный лабораторный практикум		Защита отчета
6.	**КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**. (9 **ч**.)							
6.1	Криптография как наука. Основные понятия. Типы криптосистем. Электронная цифровая подпись и её применение. Компьютерная стенография и её применение.						[3], [4], [7], [10], [12]	

6.2	Криптографические методы и средства защиты информации.					Электронный лабораторный практикум		Защита отчета
7.	**АНАЛИЗ ЗАЩИЩЁННОСТИ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ И ЕЁ УЗЛОВ.** (4 **ч.)**							
7.1	Протоколирование и аудит. Задачи и функции аудита. Структура журналов аудита. Активный аудит, методы активного аудита. Средства анализа и аудита.						[2], [3], [4], [5], [6], [7]	
8.	**ЗАЩИТА ТАМОЖЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ**. (6 **ч**.)							
8.1	Основные факторы, влияющие на обеспечение информационной безопасности таможенных органов. Основные угрозы информационной безопасности таможенных органов. Модель нарушителя информационной безопасности таможенных органов. Цели, основные задачи и принципы обеспечения информационной безопасности таможенных органов Республики Беларусь.						[2], [3], [4], [5], [6], [7], [14], [15], [16], [17]	