Министерство культуры и массовых коммуникаций
Российской Федерации
Федеральное агентство по культуре и кинематографии
Санкт-Петербургский государственный
университет культуры и искусств
Кафедра информатики и информационных технологий

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Практикум

Санкт-Петербург
2008

УДК 004.056(076.5)
ББК 32.81я7
И74

Практикум издается по решению Редакционно-издательского совета Санкт-Петербургского государственного университета культуры и искусств.

Составители практикума:

Ремизов Виктор Сергеевич,
Ремизова Ирина Викторовна

Рецензенты:

доктор технических наук, профессор, заведующая кафедры автоматизации химико-технологических процессов Санкт-Петербургского государственного университета растительных полимеров Г. А. Кондрашкова,

кандидат педагогических наук, доцент кафедры информатики и информационных технологий О. А. Арбатская

И74 Информационная безопасность : практикум / С.-Петерб. гос. ун-т культуры и искусств ; сост. В. С. Ремизов, И. В. Ремизова. – СПб. : СПбГУКИ, 2008. – 68 с.

В учебное пособие вошли задания, связанные с различными видами безопасности информации при работы на ПК. Пособие соответствует Государственному образовательному стандарту по подготовке студентов вузов Практикум предназначен для студентов, обучающихся по всем специальностям.

УДК 004.056(076.5)
ББК 32.81я7

§ 1. Настройки Windows и Office по защите информации

Практическая работа 1

Восстановление зараженных файлов

Краткие теоретические сведения

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

Для анализа макровирусов необходимо получить текст их макросов. Для нешифрованных («не-стелс») вирусов это достигается при помощи меню Сервис/Макрос. Если же вирус шифрует свои макросы или использует «стелс»-приемы, то необходимо воспользоваться специальными утилитами просмотра макросов.

Задание: восстановить файл, зараженный макровирусом.

Алгоритм выполнения работы

Для восстановления документов Word и Excel достаточно сохранить пораженные файлы в текстовый формат **RTF**, содержащий практически всю информацию из первоначальных документов и не содержащий макросы.

Для этого выполните следующие действия.

1. В программе **Word** выберите пункты меню **«Файл» — «Сохранить как».**

2. В открывшемся окне в поле «**Тип файла**» выберите «**Текст в формате RTF»** .

3. Выберите команду **Сохранить**, при этом имя файла оставьте прежним.

4. В результате появится новый файл с именем существующего, но с другим расширением.

5. Далее закройте **Word** и удалите все зараженные **Word** -документы и файл-шаблон **NORMAL.DOT** в папке **Word**.

6. Запустите **Word** и восстановите документы из RTF-файлов в соответствующий формат файла с расширением (.doc).

7. В результате этой процедуры вирус будет удален из системы, а практически вся информация останется без изменений.

Примечание:

а) этот метод рекомендуется использовать, если нет соответствующих антивирусных программ;

б) при конвертировании файлов происходит потеря невирусных макросов, используемых при работе. Поэтому перед запуском описанной процедуры следует сохранить их исходный текст, а после обезвреживания вируса — восстановить необходимые макросы в первоначальном виде.

8. Для последующей защиты файлов от макровирусов включите защиту от запуска макросов.

9. Для этого в **Word** выберите последовательно пункты меню: **Сервис — Макрос — Безопасность** .

6. В открывшемся окне на закладке **Уровень безопасности** отметьте пункт **Высокая**

.

Задания для самостоятельной работы

1. Создайте файл **virus.doc** (содержание — чистый лист) и выполните алгоритм восстановления файла (в предположении его заражения макровирусом).

2. Зафиксируйте этапы работы, используя команду **PrintScreen** клавиатуры (скопированные таким образом файлы вставьте в новый **Word** - документ для отчета преподавателю).

3. Сравните размеры файлов **virus.doc** и **virus.rtf** используя пункт контекстного меню **Свойства** (для этого выделите в **Проводнике** файл, нажмите правую кнопку мыши и выберите пункт **Свойства**).

Контрольные вопросы

1. Какие файлы заражают макровирусы?
2. Как просмотреть код макровируса?
2. Как восстановить файл, зараженный макровирусом?

Практическая работа 2
Профилактика проникновения «троянских программ»

Краткие теоретические сведения

Реестр операционной системы **Windows** — это большая база данных, где хранится информация о конфигурации системы. Этой информацией пользуются как операционная система Windows, так и другие программы. В некоторых случаях восстановить работоспособность системы после сбоя можно, загрузив работоспособную версию реестра, но для этого, естественно, необходимо иметь копию реестра. Основным средством для просмотра и редактирования записей реестра служит специализированная утилита «**Редактор реестра**».

Файл редактора реестра находится в папке **Windows**. Называется он **regedit.exe**. После запуска появится окно редактора реестра. Вы увидите список из 5 разделов:

HKEY_CLASSES_ROOT.
HKEY_CURRES_USER.
HKEY_LOCAL_MACHINE.
HKEY_USERS.
HKEY_CURRENT_CONFIG.

Работа с разделами реестра аналогична работе с папками в Проводнике. Конечным элементом дерева реестра являются ключи или параметры,

делящиеся на три типа:

- строковые (напр. «C:\Windows»);
- двоичные (напр. 10 82 AO 8F);

DWORD — этот тип ключа занимает 4 байта и отображается в шестнадцатеричном и в десятичном виде (например, 0x00000020 (32)).

В Windows системная информация разбита на так называемые ульи (hive). Это обусловлено принципиальным отличием концепции безопасности этих операционных систем. Имена файлов ульев и пути к каталогам, в которых они хранятся, расположены в разделе **HKEY_LOCAL_MACHINE \SYSTEM\CurrenControlSet\ Control\hivelist.**

В таблице 1 даны краткие описания ульев реестра и файлов, в которых хранятся параметры безопасности.

Таблица 1 Характеристика основных разделов системного реестра

HKEY_LOCAL_MACHINE\SAM	Содержит информацию SAM (Security Access Manager), хранящуюся в файлах SAM, SAM.LOG, SAM.SAV в папке %System-root%\System32\Config
HKEY_LOCAL_MACHINBSECURITY	Содержит информацию безопасности в файлах SECURITY, SECURITY.LOG, SECURITY.SAV в папке \%Systemroot%\System32\Co nfig
HKEY_LOCAL_MACHINE\SYSTEM	Содержит информацию об аппаратных профилях этого подраздела. Информация хранится в файлах SYSTEM, SYSTEM.LOG, SYSTEM.SAV в папке \%Systemroot%\System32\Co nfig
HKEY_CURRENT_CONFIG	Содержит информацию о подразделе System этого улья, которая хранится в файлах SYSTEM.SAV и SYSTEM.ALT в папке k%Systemroot%\System32\Co nfig
HKEY_USERS\.DEFAULT	Содержит информацию, которая будет использоваться для создания профиля нового пользователя, впервые регистрирующегося в системе. Информация хранится в файлах DEFAULT, DEFAULT.LOG, DEFAULT.SAV в папке \%Systemroot%\System32\Co nfig

HKEY_CURRENT_USER	Содержит информацию о пользователе, зарегистрированном в системе на текущий момент. Эта информация хранится в файлах NTUSER.DAT и NTUSER.DAT.LOG, расположенных в каталоге v%Systemroot%\Profiies\User name, где User name — имя пользователя, зарегистрированного в системе на данный момент

Задание: проверить потенциальные места записей «троянских программ» в системном реестре операционной системы Windows 2000 (XP).

Алгоритм выполнения работы

Потенциальными местами записей «троянских программ» в системном реестре являются разделы, описывающие программы, запускаемые автоматически при загрузке операционной системы от имени пользователей и системы.

1. Запустите программу **regedit.exe.**

2. В открывшемся окне выберите ветвь **HKEY_ LOCAL_MACHINE** и далее **Software\ Microsoft\ WindowsNT\CurrentVersion\Winlogon**.

3. В правой половине открытого окна программы **regedit.exe** появится список ключей.

4. Найдите ключ **Userinit (REG_SZ)** и проверьте его содержимое.

5. По умолчанию (исходное состояние) 151 этот ключ содержит следующую запись **C:\WINDOWS\ system32\userinit.exe** (рис 1.).

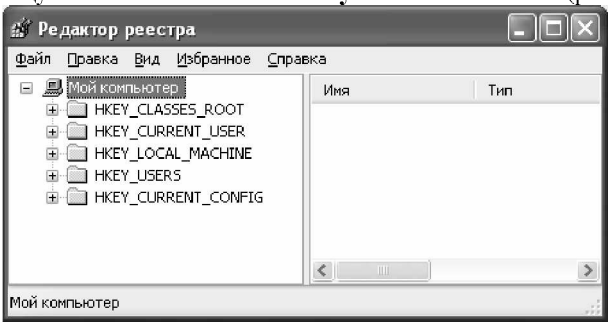


Рис.1

6. Если в указанном ключе содержатся дополнительные записи, то это могут быть «троянские программы».

7. В этом случае проанализируйте место расположения программы, обратите внимание на время создания файла и сопоставьте с Вашими действиями в это время.

8. Если время создания файла, совпадает со временем Вашей работы в Интернете, то возможно, что в это время Ваш компьютер был заражен «троянским конем».

9.Для удаления этой записи необходимо дважды щелкнуть на названии ключа (или при выделенном ключе выбрать команду Изменить из меню Правка программы regedit.exe).

10. В открывшемся окне в поле Значение (рисунок) удалите ссылку на подозрительный файл.

11. Закройте программу regedit.exe.

12. Перейдите в папку с подозрительным файлом и удалите его.

13, Перезагрузите операционную систему и выполните пункты задания 1—4.

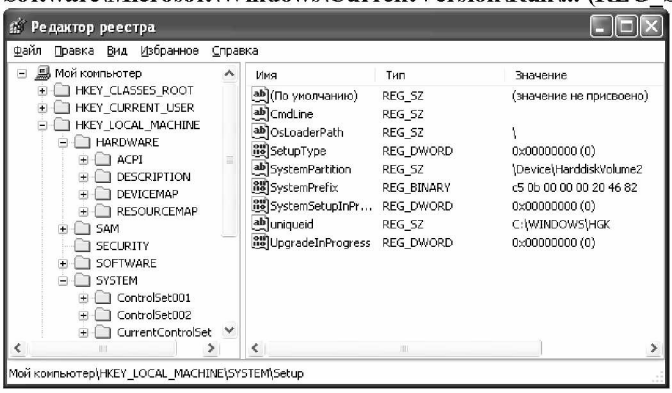
14. Если содержимое рассматриваемого ключа не изменилось, то предполагаемый «троянский конь» удален из Вашей системы.

Еще одним потенциальным местом записей на запуск «троянских программ» является раздел автозапуска **Run.**

Для его проверки выполните следующее.

1. Запустите программу **regedit.exe**.

2.В открывшемся окне выберите ветвь **HKEY_LOCAL_MACHINE** и далее **Software\Microsoft\Windows\CurrentVersion\Run\... (REG_SZ)** (рис.).



3. В рассматриваемом примере автоматически запускается резидентный антивирус и его планировщик заданий, а также утилита, относящаяся к программе **Nero** (запись на CD).

Если в указанном разделе есть записи вызывающие подозрения, то выполните пункты 6—14 предыдущего задания.

Задания для самостоятельной работы

1. Проверьте содержимое ключа HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersi

on\Winlogon\System (REG_SZ)

2, Зафиксируйте этапы работы, используя команду PrintScreen клавиатуры.

1. Составьте отчет о результатах проверки.

Контрольные вопросы

1. Что такое реестр?
2. Поясните особенности «троянских программ».
3. Почему профилактика «троянских программ» связана с системным реестром?
4. Какие разделы и ключи являются потенциальными местами записей «троянских программ»?

Практическая работа 3
Настройка безопасности почтового клиента Outlook Express

Краткие теоретические сведения

Почтовый клиент — это программа, предназначенная для приема и отправки электронной почты. Примером такой программы является программа Outlook Express. Для работы с электронной почтой почтовый клиент должен поддерживать протоколы SMTP (исходящая почта) и POP3 (входящая почта).

Одну из реальных угроз в современных глобальных сетях представляют электронные письма с вложенными программами-вирусами. Именно посредством электронной почты были проведены последние глобальные сетевые атаки. В связи с этим проблема защиты компьютера при работе с электронной почтой приобретает особую актуальность. Аналогично вопрос конфиденциальности и безопасности электронной почты с течением времени не только не теряет своей актуальности, но и ставится все более и более остро. Отправляя конфиденциальную информацию по электронной почте, необходимо иметь уверенность в том, что сообщения не перехватываются и не подделываются.

Outlook Express позволяет использовать цифровые идентификаторы или цифровые удостоверения для защиты электронной почты, в частности, для шифрования почтовых сообщений. По умолчанию Outlook Express автоматически добавляет сертификаты, которые приходят по почте, в адресную книгу Windows.

Цифровой идентификатор состоит из открытого ключа, личного ключа и цифровой подписи. Когда пользователь подписывает отправляемые им сообщения, он добавляет в состав сообщения свою цифровую подпись и открытый ключ. Комбинация цифровой подписи и открытого ключа называется сертификатом.

Цифровая подпись отправителя подтверждает получателю подлинность полученных сообщений. Открытый ключ отправителя получатель может

использовать для отправки ему зашифрованной почты, расшифровать которую он сможет с помощью своего личного ключа. Таким образом, чтобы отправить зашифрованные сообщения в чей-либо адрес, необходимо включить в адресную книгу цифровые идентификаторы, ассоциированные с получателями. Благодаря этому при помощи открытых ключей получателей Вы сможете зашифровывать отправляемые ими сообщения. Каждый получатель расшифрует полученное сообщение с помощью своего личного ключа.

Задание: разработать систему правил по управлению входящими сообщениями в Outlook Express и настроить Outlook Express для передачи сообщений с электронной цифровой подписью.

Алгоритм выполнения работы

А. Создание системы правил по обработке входящих сообщений электронной почты.

Расширенные правила управления сообщениями поддерживают большое количество критериев действий, включая блокирование отправителей сообщения и новые правила для групп новостей.

Для создания правила по обработке входящих сообщений электронной почты выполните следующие действия.

1. Откройте программу **Outlook Express**.
2. Последовательно выполните команды меню **Сервис — Правила для сообщений — Почта.**
3. В результате откроется диалоговое окно (рис. 1) Создать правило для почты.

Создать правило для почты

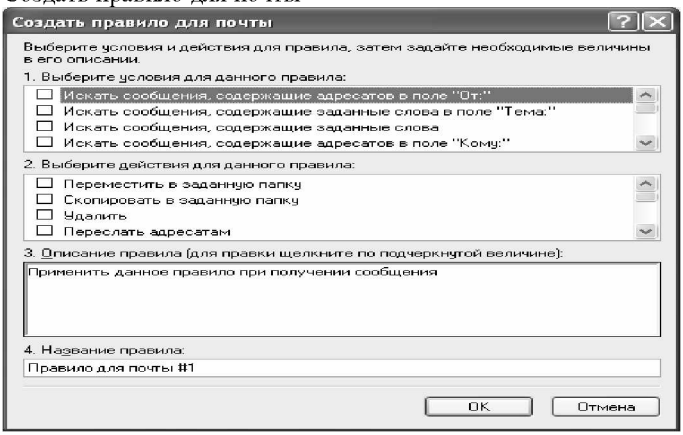


Рис. 1

2. Выберите условие создаваемого правила (например, для защиты от заражения компьютера вложенными в электронное письмо файлами можно

выбрать условие **Искать сообщение с вложениями**, рис. 2).

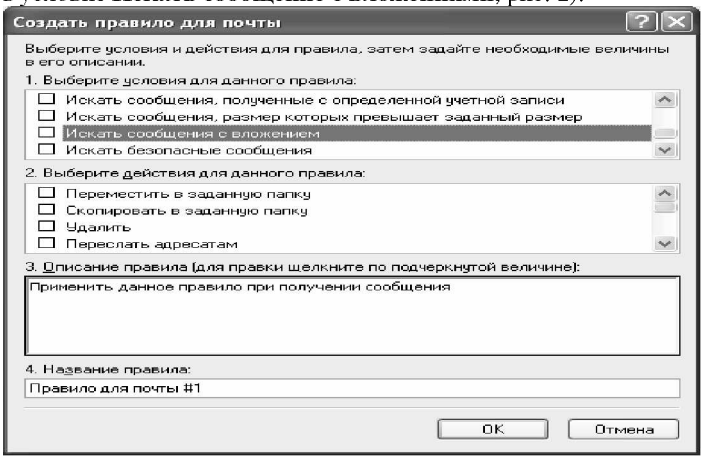


Рис 2

5. Выберите действие для данного правила (например, **Удалить с сервера**, рис. 3).

6. Обратите внимание, что в поле 3 приводится описание созданного правила. После создания этого правила, все письма содержащие вложения будут удалены с сервера.

7. Для завершения создания правила введите его имя в поле 4 — **Название правила**.

8. Для успешного создания правила нужно задать хотя бы одно условие. Если задано составное условие (то есть несколько условий), то по умолчанию должно выполниться хотя бы одно из простых условий; в поле **Описание правила**.

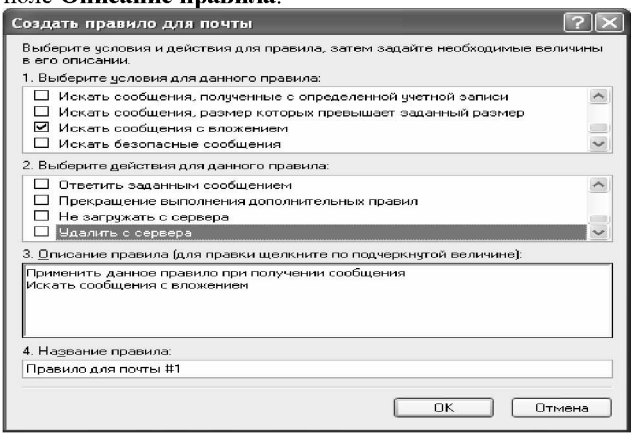


Рис 3

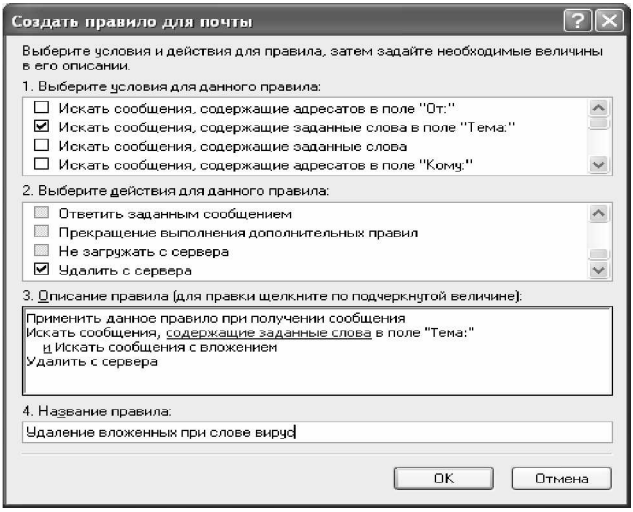


Рис 4

9. Пример составного условия показан на рисунке 4. В результате выполнения этого правила с сервера будут удалены все письма с вложениями, в которых еще в поле «Тема» содержится слово «вирус» (можно задать произвольное слово).

7. Таким образом, комбинируя правила управления входящими сообщениями, можно существенно повысить защищенность компьютера при работе с электронной почтой.

В. Получение цифрового идентификатора.

Прежде чем отправлять сообщения, подписанные цифровой подписью и зашифрованные, необходимо получить цифровой идентификатор.

1. Для получения цифрового идентификатора необходимо заполнить заявку на получение цифрового идентификатора в организации, уполномоченной предоставлять этот сервис.

2. Для этого в окне **Параметры** (меню **Сервис — Параметры**) на вкладке **Безопасность** нажмите кнопку **Получить сертификат**.

3. В результате запустится веб-браузер, который обратится к странице на веб-узле Microsoft, где приводится перечень организаций, уполномоченных предоставлять этот сервис (например, у компании VeriSign можно бесплатно получить временный (на два месяца) цифровой идентификатор, позволяющий опробовать все режимы безопасности программы Outlook Express).

4. После заполнения формы с запросом на предоставление цифрового идентификатора Вы получите (через несколько минут) почтовое сообщение от VeriSign с инструкциями по установке полученного цифрового идентификатора.

5. Раскройте и прочтите письмо. В точности выполните приведенные в нем инструкции.

6 Подтвердите установку цифрового идентификатора.

C. Использование цифровой электронной подписи.

1. Для отправки сообщения, которое требуется подписать цифровой подписью, создайте новое сообщение.

1. Выберите в меню **Сервис** команду **Цифровая подпись**. В результате напротив поля **Кому** появится символ подтверждающий включение электронной цифровой подписи (рис. 5).

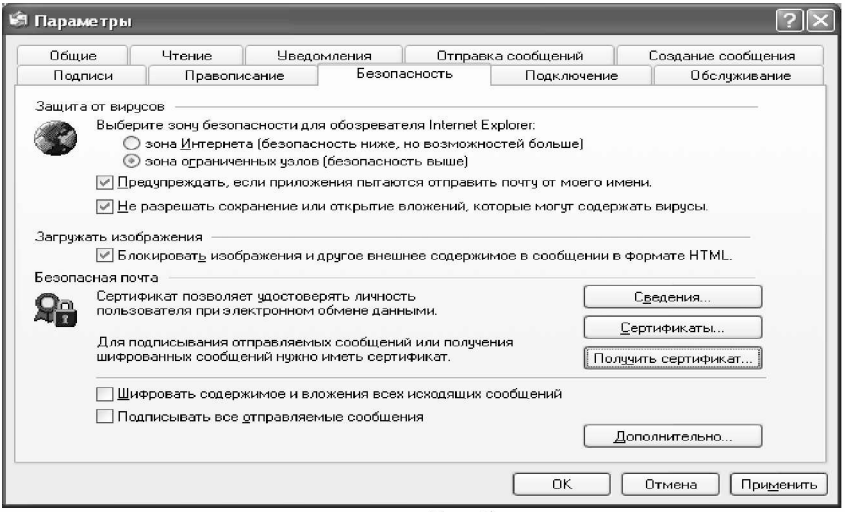


Рис. 5

2. Если отправляемое сообщение требуется также зашифровать, выберите в меню **Сервис** команду **Зашифровать**. В случае включения шифрования появится символ напротив поля **Копия** .

D. Настройка опций обмена защищенной почтой.

1. Чтобы настроить работу с защищенными почтовыми сообщениями, выберите в меню Сервис команду **Параметры** и перейдите на вкладку **Безопасность** (рисунок 5).

1. Параметры, необходимые для настройки обмена защищенной почтой, находятся в группе **Безопасная почта** (рисунок 6).

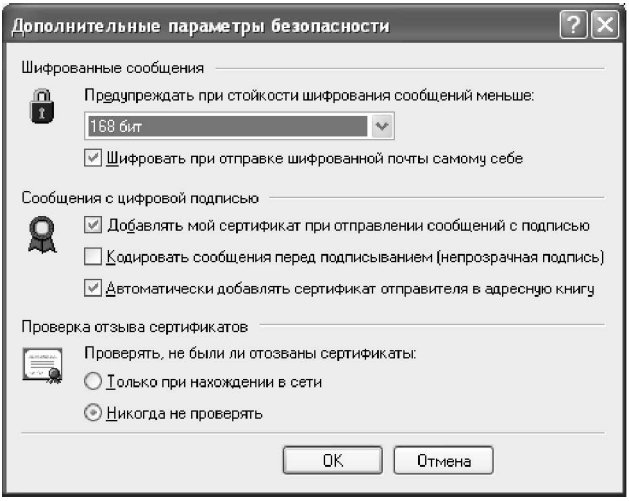


Рис. 6

Задания для самостоятельной работы

1. Выполните задания A — D.

3. Создайте три новых правила (произвольных) управления сообщениями электронной почты и опишите их безопасные свойства, то есть как и от каких угроз можно ими защитить компьютер. Составьте отчет.

Контрольные вопросы

1. Для чего используется механизм электронной цифровой подписи?
2. Что понимается под сертификатом?
3. Какой метод шифрования использует электронная цифровая подпись?

Практическая работа 4
Настройка параметров аутентификации Windows 2000 (XP)

Краткие теоретические сведения

В соответствии с сертификационными требованиями к системам безопасности операционных систем при подключении пользователей должен реализовываться механизм аутентификации и/или идентификации.

Идентификация и аутентификация применяются для ограничения доступа случайных и незаконных субъектов (пользователи, процессы) информационных систем к ее объектам (аппаратные, программные и информационные ресурсы).

Идентификация — присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.

Аутентификация (установление подлинности) — проверка

принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.

Настройка параметров аутентификации рассматриваемых операционных систем выполняется в рамках локальной политики безопасности.

Оснастка «Локальная политика безопасности» используется для изменения политики учетных записей и локальной политики на локальном компьютере. При помощи оснастки «Локальная политика безопасности» можно определить:

- кто имеет доступ к компьютеру;
- какие ресурсы могут использовать пользователи на Вашем компьютере;
- включение и отключение записи действий пользователя или группы в журнале событий.

Задание: настроить параметры локальной политики безопасности операционной системы Windows 2000 (XP).

Алгоритм выполнения работы

Для просмотра и изменения параметров аутентификации пользователей выполните следующие действия:

1. Выберите кнопку **Пуск** панели задач.
2. Откройте меню **Настроить — Панель управления**.
3. В открывшемся окне выберите ярлык Администрирование — Локальная политика безопасности (рис. 1).
4. Выберите пункт Политика учетных записей (этот пункт включает два подпункта: Политика паролей и Политика блокировки учетной записи).
5. Откройте подпункт Политика паролей. В правом окне появится список настраиваемых параметров (рис. 2).
6. В показанном примере политика паролей соответствует исходному состоянию системы безопасности после установки операционной системы, при этом ни один

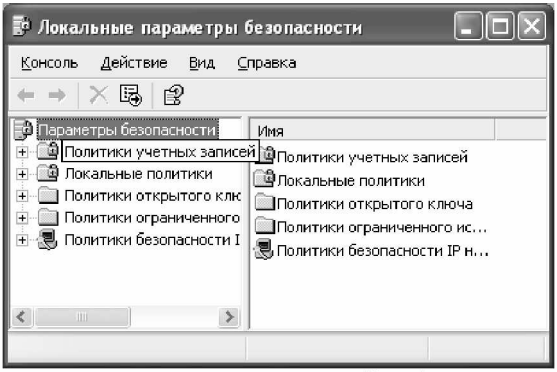


Рис. 1

из параметров не настроен. Значения параметров приведены в таблице 1.

7. Ознакомьтесь со свойствами всех параметров.

8. Для изменения требуемого параметра выделите его и вызовите его свойства из контекстного меню после нажатия правой кнопки мыши (или дважды щелкните на изменяемом параметре).

9. В результате этого действия появится одно из окон, показанных на рисунке 3.

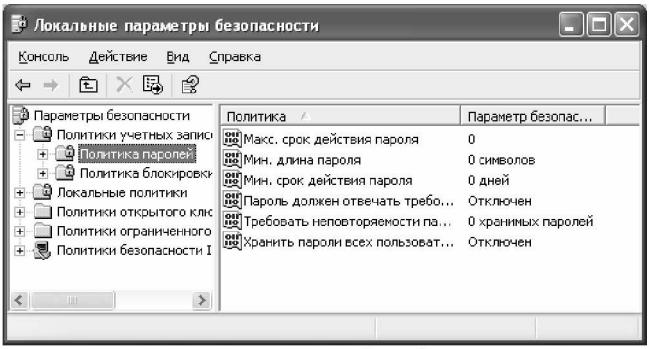


Рис. 2

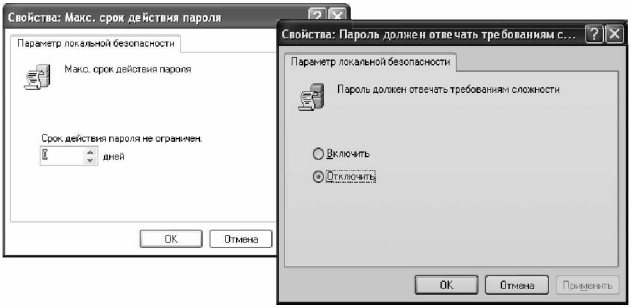


Рис. 3

Значения параметров Политики паролей

Таблица 1

Параметр	Значение
Требовать неповторяемости паролей	Определяет число новых паролей, которые должны быть сопоставлены учетной записи пользователя, прежде чем можно будет снова использовать старый пароль. Это значение должно принадлежать диапазонучлг 0 до 24.
Максимальный срок действия пароля	Определяет период времени (в днях), в течение которого можно использовать пароль, прежде чем система потребует от пользователя заменить его. Можно задать значение в диапазоне от 1 до 999 дней или снять всякие ограничения срока действия, установив число дней равным 0.
Минимальный срок действия пароля	Определяет период времени (в днях), в течение которого необходимо использовать пароль, прежде чем пользователь сможет заменить его. Можно задать значение в диапазоне от 1 до 999 дней или разрешить немедленное изменение, установив число дней равным 0.
Минимальная длина пароля	Определяет наименьшее число символов, которые может содержать пароль учетной записи пользователя. Можно задать значение в диапазоне от 1 до 14 символов или отменить использование пароля, установив число символов равным 0.
Пароль должен отвечать требованиям сложности	Определяет, должны ли пароли отвечать требованиям сложности. Если эта политика включена, пароли должны удовлетворять следующим минимальным требованиям. 5> Пароль не может содержать имя учетной записи пользователя или какую-либо его часть. > Пароль должен состоять не менее чем из шести символов. ^ В пароле должны присутствовать символы трех категорий из числа следующих четырех: 1) прописные буквы английского алфавита от A до Z; 2) строчные буквы английского алфавита от a до z; 3) десятичные цифры (от 0 до 9); 4) символы, не принадлежащие алфавитно-цифровому набору (например, !,$,#, %). Проверка соблюдения этих требований выполняется при изменении или создании паролей.

Окончание табл. 1

Параметр	Значение
Хранить пароли всех пользователей в домене, используя обратимое шифрование	Определяет, следует ли в системах Windows 2000 Server, Windows 2000 Professional и Windows XP хранить пароли, используя обратимое шифрование. Эта политика обеспечивает поддержку приложений, использующих протоколы, которым для проверки подлинности нужно знать пароль пользователя. Хранить пароли, зашифрованные обратимыми методами, - это все равно, что хранить их открытым текстом. Поэтому данную политику следует использовать лишь в исключительных случаях, если потребности приложения оказываются важнее, чем защита пароля.

10. Измените значение параметра и нажмите и сохранить), выберите параметр Требовать неповторяемости паролей и измените Ок.

11. Например (обязательно выполнить его значение на 1.

12. Для настройки Политики блокировки учетной записи выберите этот подпункт и откройте его.

13. Значения параметров данного подпункта Политики учетных записей

приведены в таблице 2.

14. Ознакомьтесь со свойствами всех параметров.

15. Для изменения параметров воспользуйтесь алгоритмом, описанным в пунктах 8-10.

Задания для самостоятельной работы

1. Измените параметр «Пароль должен отвечать требованиям сложности» Политики паролей на «Включен» (рисунок 3) и после этого попробуйте изменить пароль своей учетной записи. Зафиксируйте все сообщения системы, проанализируйте и введите допустимый пароль. Этот пароль является результатом выполнения Вашего задания.

Значения параметров
Политики блокировки учетных записей

Таблица 2

Параметр	Значение
Пороговое значение блокировки	Определяет число неудачных попыток входа **в** систему, после которых учетная запись пользователя блокируется. Блокированную учетную запись нельзя использовать до тех пор, пока она не будет сброшена администратором или пока не истечет ее интервал блокировки. Можно задать значение в диапазоне от 1 до 999 или запретить блокировку данной учетной записи, установив значение 0.
Блокировка учетной записи на	Определяет число минут, в течение которых учетная запись остается блокированной, прежде чем будет автоматически разблокирована. Этот параметр может принимать значения от 1 до 99 999 минут. Если установить значение 0, учетная запись будет блокирована на все время до тех пор, пока администратор не разблокирует ее явным образом. Если пороговое значение блокировки определено, данный интервал блокировки должен быть больше или равен интервалу сброса.
Сброс счетчика блокировки через	Определяет число минут, которые должны пройти после неудачной попытки входа в систему, прежде чем счетчик неудачных попыток будет сброшен в 0. Этот параметр может принимать значения от 1 до 99 999 минут. Если определено пороговое значение блокировки, данный интервал сброса не должен быть больше интервала **Блокировка учетной записи на.**

После успешного выполнения первого задания, измените пароль Вашей учетной записи, а в качестве нового пароля укажите прежний пароль. Все сообщения зафиксируйте, проанализируйте и объясните поведение системы безопасности.

2. Проведите эксперименты с другими параметрами **Политики учетных записей.**

Контрольные вопросы

1 Что такое аутентификация и идентификация?

2 Для чего применяются эти механизмы?

3 Что можно настроить с помощью оснастки **Локальная политика**

безопасности.

Практическая работа 5

Шифрующая файловая система EFS и управление сертификатами в Windows 2000 (XP)

Краткие теоретические сведения

Шифрующая файловая система EFS позволяет пользователям хранить данные на диске в зашифрованном виде.

Шифрование — это процесс преобразования данных в формат, не доступный для чтения другим пользователям. После того как файл был зашифрован, он автоматически остается зашифрованным в любом месте хранения на диске.

Расшифровка — это процесс преобразования данных из зашифрованной формы в его исходный формат.

При работе с шифрующей файловой системой EFS следует учитывать следующие сведения и рекомендации.

1. Могут быть зашифрованы только файлы и папки, находящиеся на томах **NTFS.**

Сжатые файлы и папки не могут быть зашифрованы. Если шифрование выполняется для сжатого файла или папки, файл или папка преобразуются к состоянию без сжатия.

3. Зашифрованные файлы могут стать расшифрованными, если файл копируется или перемещается на том, не являющийся томом **NTFS**.

4. При перемещении незашифрованных файлов в зашифрованную папку они автоматически шифруются в новой папке. Однако обратная операция не приведет к автоматической расшифровке файлов. Файлы необходимо явно расшифровать.

5. Не могут быть зашифрованы файлы с атрибутом «**Системный**» и файлы в структуре папок системный корневой каталог.

6. Шифрование папки или файла не защищает их от удаления. Любой пользователь, имеющий права на удаление, может удалить зашифрованные папки или файлы.

7 Процесс шифрование является прозрачным для пользователя.

Примечание. Прозрачное шифрование означает, что перед использованием файл не нужно расшифровывать. Можно как обычно открыть файл и изменить его. В системах прозрачного шифрования (шифрования «на лету») криптографические преобразования осуществляются в режиме реального времени незаметно для пользователя. Например, пользователь записывает подготовленный в текстовом редакторе документ на защищаемый диск, а система защиты в процессе записи выполняет его шифрование.

Использование **EFS** сходно с использованием разрешений для файлов и

папок. Оба метода используются для ограничения доступа к данным. Но злоумышленник, получивший несанкционированный физический доступ к зашифрованным файлам и папкам, не сможет их прочитать. При его попытке открыть или скопировать зашифрованный файл или папку появится сообщение, что доступа нет.

Шифрование и расшифровывание файлов выполняется установкой свойств шифрования для папок и файлов, как устанавливаются и другие атрибуты, например, «**только чтение**», «**сжатый**» или «**скрытый**». Если шифруется папка, все файлы и подпапки, созданные в зашифрованной папке, автоматически шифруются. Рекомендуется использовать шифрование на уровне папки. Шифрующая файловая система автоматически создает пару ключей шифрования для пользователя, если она отсутствует. Шифрующая файловая система использует алгоритм шифрования Data Encryption Standard (DESX).

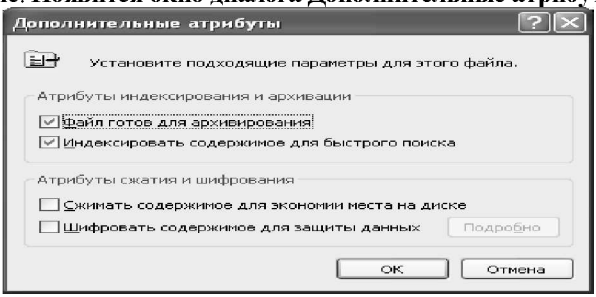
Задание: включить и отключить шифрование файлов шифрующей файловой системой EFS. Экспортировать сертификат с ключами для расшифровки файлов на другом компьютере.

Алгоритм выполнения работы

А. Для включения режима шифрования выполните следующие действия.

1. Укажите файл или папку (например, создайте файл **шифр.doc** в папке **Мои документы**), которую требуется зашифровать, нажмите правую кнопку мыши и выберите в контекстном меню команду **Свойства**.

2. В появившемся окне свойств на вкладке Общие нажмите кнопку Другие. Появится окно диалога Дополнительные атрибуты.



3. В группе **Атрибуты сжатия и шифрования** установите флажок **Шифровать содержимое для защиты данных** и нажмите кнопку «**ОК**».

4. Нажмите кнопку ОК в окне свойств зашифровываемого файла или папки, в появившемся окне диалога укажите режим шифрования: **только к этой папке или к этой папке и всем вложенным папкам и файлам**.

Внимание! После выполнения этих действий файл с Вашей информацией будет автоматически зашифровываться. Просмотр его на другой ПЭВМ будет невозможен.

В. Для выключения режима шифрования выполните следующие действия.

1. Выделите файл шифр.doc в папке **Мои документы**.
2. Нажмите правую клавишу мыши и выберите пункт **Свойства.**
3. На вкладке **Общие** нажмите кнопку **Другие.**
4. В открывшемся окне диалога в группе **Атрибуты сжатия и шифрования** сбросьте флажок **Шифровать содержимое для защиты данных.**

Внимание! После выполнения этих действий файл с Вашей информацией не будет зашифровываться.

С. Создание резервной копии Сертификата средствами Windows 2000 (XP).

Примечание. Резервная копия сертификата необходима для расшифровки данных после переустановки операционной системы или для просмотра зашифрованной информации на другой ПЭВМ.

Внимание! ***Перед переустановкой*** операционной системы обязательно ***создайте копии Сертификатов***, так как после переустановки Вы не сможете расшифровать информацию.

Для создания резервной копии сертификата выполните следующие действия.

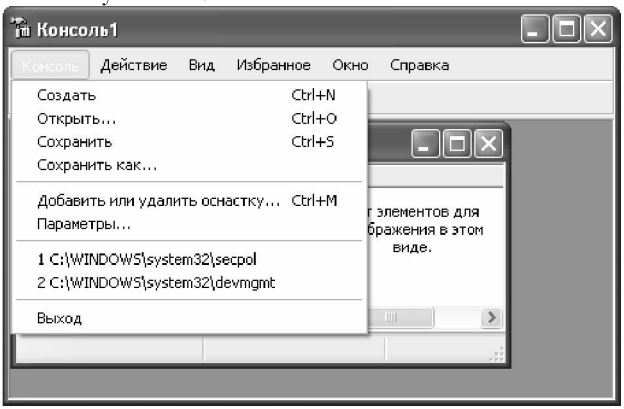
1. Выберите кнопку **Пуск** в панели задач.
2. Перейдите к пункту **Выполнить**.
3. В открывшемся окне в поле ввода введите команду **mmc**.
4. В результате откроется консоль управления **mmc**.

Примечание. Консоль MMC — это средство для создания, сохранения и открытия наборов средств администрирования, называемых консолями. Консоли содержат такие элементы, как оснастки, расширения оснасток, элементы управления, задачи, мастера и документацию, необходимую для управления многими аппаратными, программными и сетевыми компонентами системы Windows. Можно добавлять элементы в существующую консоль MMC, а можно создавать новые консоли и настраивать их для управления конкретными компонентами системы.

5. В меню **Консоль** выберите команду **Добавить или удалить оснастку** (рис. 1) и нажмите кнопку **Добавить**.
6. В поле **Оснастка** дважды щелкните **Сертификаты** (рис. 2), установите переключатель в положение **учетной записи компьютера** и нажмите кнопку **Далее.**
7. Выполните одно из следующих действий.

■ Чтобы управлять сертификатами локального компьютера, установите переключатель в положение **локальным компьютером** и нажмите кнопку **Готово**.

■ Чтобы управлять сертификатами удаленного компьютера, установите переключатель в положение **другим компьютером** и введите имя компьютера или нажмите кнопку **Обзор** для выбора компьютера, затем нажмите кнопку **Готово**.



Рис, 1

8. Нажмите кнопку **Закрыть**.

9. В списке выбранных оснасток для новой консоли появится элемент **Сертификаты** (имя_компьютера).

10. Если на консоль не нужно добавлять другие оснастки, нажмите кнопку **ОК**.

11. Чтобы сохранить эту консоль, в меню **Консоль** выберите команду Сохранить и укажите имя оснастки **Сертификаты**.

12. Закройте окно Консоли и выберите команду Пуск и далее Все программы.

13. Найдите пункт **Администрирование** и выберите подпункт Сертификаты (теперь оснастка с **Сертификатами** доступна в меню **Пуск**).

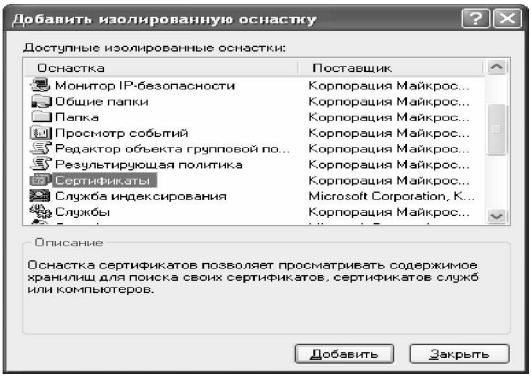


Рис. 2

14. В левом подокне оснастки **Сертификаты** откройте папку **Доверенные корневые сертификаты**, а затем папку **Сертификаты**. В правом подокне появится список сертификатов.

15. Укажите переносимый сертификат (например, первый в списке, рис. 3) и щелкните правой кнопкой мыши. В появившемся контекстном меню выберите команду **Все задачи** и далее выберите команду **Экспорт**.

Рис. 3

16. В результате запустится **Мастер экспорта сертификатов**.

17. Нажмите кнопку **Далее**.

18. В следующем окне мастера выберите опцию **Да**, экспортировать закрытый ключ.

19. Затем нажмите кнопку **Далее**.

20. В следующем окне мастера доступен только один формат (PFX), предназначенный для персонального обмена информацией. Нажмите кнопку Далее.

21. В следующих окнах сообщите пароль (например, **11**), защищающий данные файла сертификатах.pfx а также путь сохранения файла (запишите путь к папке, в которой Вы сохранили копию Сертификата) сертификат.pfx.

22. Нажмите кнопку **Далее**.

23. Отобразится список экспортируемых сертификатов и ключей. Нажмите кнопку **Готово**.

24. Завершите работу Мастера экспорта сертификата нажатием кнопки **ОК** в окне диалога, сообщающем об успешном выполнении процедуры экспорта.

В результате сертификат и секретный ключ будут экспортированы в файл с расширением сертификат.pfx, который может быть скопирован на гибкий диск и перенесен на другой компьютер или использован после переустановки операционной системы.

D. Для восстановления сертификата из резервной копии выполните следующие действия.

1. Перенесите созданный на предыдущем этапе файл с расширением сертификат.pfx на компьютер (**Вам необходимо вспомнить путь к копии Сертификата**).

2. Запустите оснастку **Сертификаты**, для этого выберите кнопку Пуск панели задач и далее **Все программы /Администрирование /Сертификаты.**

3. В окне структуры оснастки **Сертификаты** откройте папку **Доверенные корневые сертификаты**, затем папку **Сертификаты**. В правом подокне появится список Ваших сертификатов.

4. Щелкните правой кнопкой мыши на пустом месте правого подокна.

5. В появившемся контекстном меню выберите команду **Все задачи**.

6. В ее подменю выберите команду **Импорт** (Import).

7. Запустится Мастер импорта сертификатов.

8. Следуйте указаниям мастера — укажите местоположение файла

сертификатах и сообщите пароль защиты данного файла.

9. Для начала операции импорта нажмите кнопки **Готово и ОК.**

10. После завершения процедуры импорта нажмите кнопку ОК и закройте окно Мастера импорта.

В результате Ваших действий текущий пользователь или Вы сами получите возможность работать с зашифрованными данными на этом компьютере.

Задания для самостоятельной работы

1. Экспортируйте сертификат № 2 из папки **Промежуточные центры сертификации RootAgency** (сохраните иллюстрации для отчета).

1. Импортируйте экспортированный сертификат в папку **Личные** (сохраните иллюстрации для отчета).

Контрольные вопросы

1. Что входит в криптосистему?

2. Сравните методы шифрования с открытым и закрытым ключом (асимметричное и симметричное шифрование).

3. Что такое mmc?

1 Назначение шифрующей файловой системы EFS.

Практическая работа 6

Назначение прав пользователей при произвольном управлении доступом в Windows 2000 (XP)

Краткие теоретические сведения

После выполнения идентификации и аутентификации подсистема защиты устанавливает полномочия (совокупность прав) субъекта для последующего контроля санкционированного использования объектов информационной системы.

Обычно полномочия субъекта представляются **списком ресурсов**, доступным пользователю и **правами по доступу** к каждому ресурсу из списка.

При разграничении доступа по спискам задаются соответствия: каждому пользователю — список ресурсов и прав доступа к ним или каждому ресурсу — список пользователей и их прав доступа к данному ресурсу.

Списки позволяют установить права с точностью до пользователя. Списки используются в подсистемах безопасности операционных систем и систем управления базами данных.

Задание: Создать учетную запись и локальную группу, изменить принадлежность пользователя к локальной группе и блокировать учетную

запись пользователя.

Алгоритм выполнения работы

А. Создание учетной записи.

1. Откройте оснастку **Управление компьютером** в разделе **Администрирование Панели управления** (рис. 1).

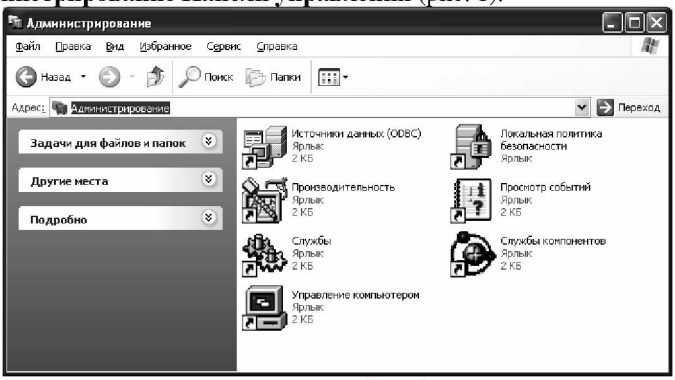


Рис. 1

2. В оснастке **Локальные пользователи и группы** установите указатель мыши на папку **Пользователи** и нажмите правую кнопку.

3. В появившемся контекстном меню выберите команду Новый пользователь (рис. 2). Появится окно диалога **Новый пользователь** (рис. 3).

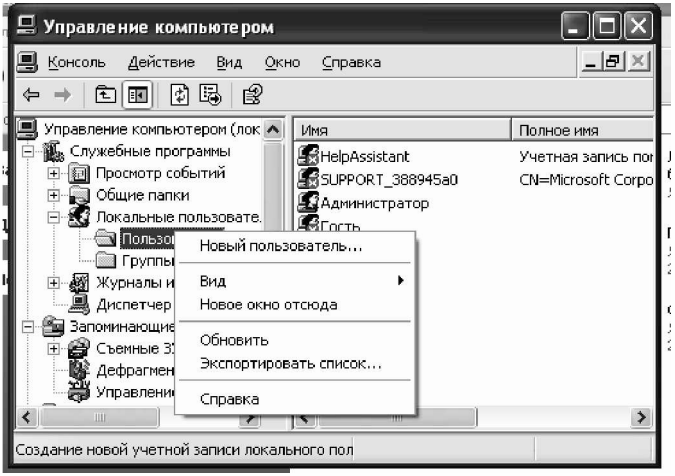


Рис. 2

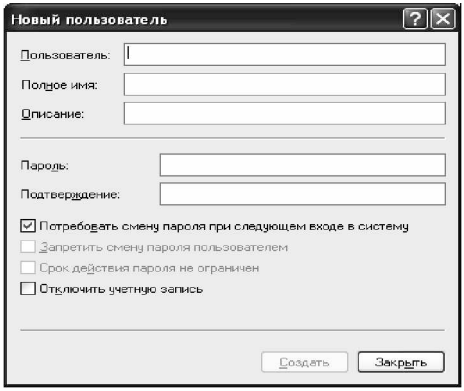


Рис. 3

2. В поле **Пользователь** введите имя создаваемого пользователя, например, свою фамилию.

Примечание. Имя пользователя должно быть уникальным для компьютера. Оно может содержать до 20 символов верхнего и нижнего регистра. Ниже приведены символы, применение которых в имени пользователя недопустимо**:»/ \ []:; =,+*?<>** Имя пользователя не может состоять целиком из точек и пробелов.

5. В поле **Полное имя** введите полное имя создаваемого пользователя.

6. В поле Описание введите описание создаваемого пользователя или его учетной записи, например, «студент.....».

7 В поле **Пароль** введите пароль пользователя и в поле Подтверждение подтвердите его правильность вторичным вводом.

Примечание. Длина пароля не может превышать 14 символов.

8.Установите или снимите флажки:

- потребовать смену пароля при следующем входе в систему;
- запретить смену пароля пользователем;
- срок действия пароля не ограничен;
- отключить учетную запись.

5.Чтобы создать еще одного пользователя, нажмите кнопку **Создать** и повторите шаги с 1 по 8. Для завершения работы нажмите кнопку **Создать** и затем **Закрыть**.

В. Создание локальной группы.

1. В окне оснастки **Локальные пользователи и группы** установите указатель мыши на папке **Группы** и нажмите правую кнопку.

2 В появившемся контекстном меню выберите команду **Новая группа.**

3. В поле **Имя группы** (рисунок 4) введите имя новой группы, например, **Студенты**.

Примечание. Имя локальной группы должно быть уникальным в пределах компьютера. Оно может содержать до 256 символов в верхнем и нижнем регистрах.

4. В поле **Описание** введите описание новой группы.

5. В поле **Члены группы** можно сразу же добавить пользователей и группы, которые войдут в данную группу: для этого нужно нажать кнопку **Добавить** и выбрать их в списке.

Для завершения нажмите кнопку **Создать** и затем **Закрыть**.

C. Изменение членства в локальной группе.

1. В окне оснастки **Локальные пользователи и группы** щелкните на папке **Группы**.

2. В правом подокне установите указатель мыши на модифицируемую группу и нажмите правую кнопку.

3. В появившемся контекстном меню выберите команду **Добавить в группу** или **Свойства**.

4. Для того, чтобы добавить новые учетные записи в группу, нажмите кнопку **Добавить** (рис. 5).

Рис. 5

5. Далее следуйте указаниям окна диалога **Выбор: Пользователи** или **Группы**.

2 Для того, чтобы удалить из группы некоторых пользователей, в поле **Члены группы** (рисунок 5) окна свойств группы выберите одну или несколько учетных записей и нажмите кнопку **Удалить**

Примечание. В локальную группу можно добавлять как локальных пользователей, созданных на компьютере, так и пользователей и глобальные группы, созданные в домене, к которому принадлежит компьютер, или в доверяемых доменах. Встроенные группы не могут быть удалены. Удаленные группы не могут быть восстановлены. Удаление группы не отражается на входящих в нее пользователей.

D. Временная блокировка учетной записи.

1. Откройте оснастку **Управление компьютером**.

2. Для этого либо выберите на **Рабочем столе** ярлык **Мой компьютер** и нажмите правую клавишу мыши, после чего выберите пункт контекстного меню **Управление**, либо воспользуйтесь разделом **Администрирование** в **Панели управления**.

3. В открывшейся оснастке выберите пункты **Служебные программы/Локальные пользователи и группы** (рис. 2).

4. Откройте папку **Пользователи** и выберите учетную запись **Гость**.

5. Нажмите правую клавишу мыши и выберите пункт **Свойства**.

6. В открывшемся окне снимите отметку пункта **Отключить учетную запись** .

7. Нажмите кнопку **ОК** и сделайте вывод о состоянии учетной записи.

3 Выполните пункт 5 и отметьте пункт **Отключить учетную запись**.

Задания для самостоятельной работы

1. Создайте учетную запись с именем ПЗ-6, используя команду Print Screen клавиатуры, сохраните копию экрана со списком пользователей Вашего компьютера (для этого после нажатия клавиши Print Screen вставьте скопированное изображение в новый документ Word) для представления в качестве отчета.

2. Создайте группу **Информационная безопасность** и, как в первом задании, сохраните окно со списком групп Вашего компьютера для отчета.

3. Заблокируйте учетную запись ПЗ-6 и после этого удалите.

Контрольные вопросы

1. Какие методы управления доступом Вам известны?
2. Чем отличается мандатное управление доступом от дискретного?
1.Допустимо ли имя пользователя П38/44? Почему?

Практическая работа 7
Настройка параметров регистрации и аудита в Windows 2000 (XP)

Краткие теоретические сведения

Регистрация является еще одним механизмом обеспечения защищенности информационной системы. Этот механизм основан на подотчетности системы обеспечения безопасности, фиксирует все события, касающиеся безопасности. Эффективность системы безопасности принципиально повышается в случае дополнения механизма регистрации механизмом аудита. Это позволяет оперативно выявлять нарушения, определять слабые места в системе защиты, анализировать закономерности системы, оценивать работу пользователей и т. д.

Аудит — это анализ накопленной информации, проводимый оперативно, в реальном времени или периодически (например, раз в день). Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным.

Практическими средствами регистрации и аудита являются:

- различные системные утилиты и прикладные программы;
- регистрационный (системный или контрольный) журнал.

Первое средство является обычно дополнением к мониторингу, осуществляемому администратором системы. Комплексный подход к

протоколированию и аудиту обеспечивается при использовании регистрационного журнала.

Регистрационный журнал — это хронологически упорядоченная совокупность записей результатов деятельности субъектов системы, достаточная для восстановления, просмотра и анализа последовательности действий, окружающих или приводящих к выполнению операций, процедур или совершению событий при транзакции с целью контроля конечного результата.

Задание: активизировать механизмы регистрации j и аудита операционной системы Windows 2000 (XP) и настроить параметры просмотра аудита папок и файлов.

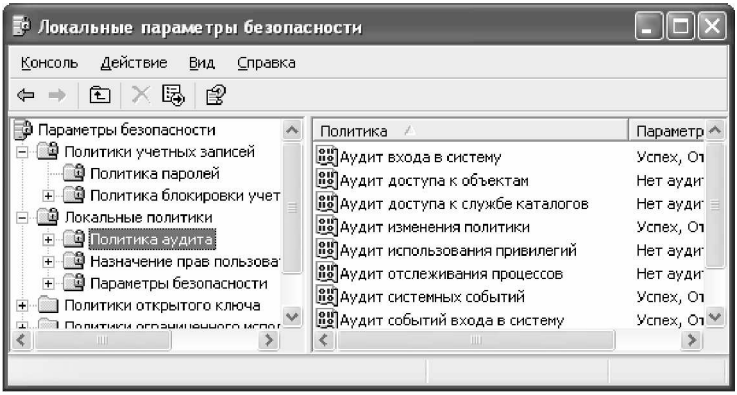
Алгоритм выполнения работы

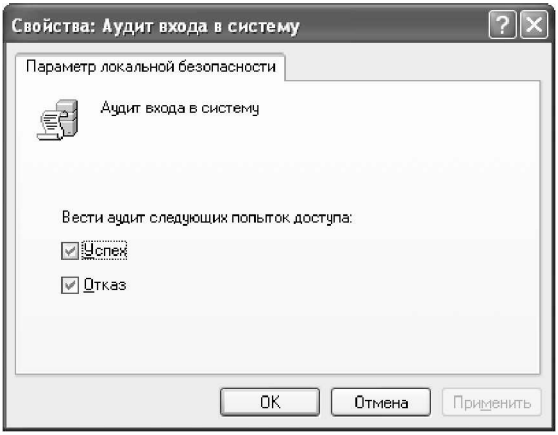
А. Активизация механизма регистрации и аудита с помощью оснастки Локальные политики безопасности.

1. Выберите кнопку **Пуск** панели задач.
2. Откройте меню **Настроить/Панель управления**.
3. В открывшемся окне выберите ярлык **Администрирование /Локальная политика безопасности.**
4. Выберите пункт **Политика аудита** (рис. 1).
5. Для включения или отключения параметров аудита выберите требуемый параметр и дважды щелкните левой клавишей мыши.
6. Для каждого параметра можно задать аудит успехов или отказов, либо вообще отключить аудит событий данного типа (рис. 2).
7. Значения параметров политики аудита приведены в таблице 1.
8. По умолчанию все параметры политики аудита выключены.
9. Включите аудит успеха и отказа для всех параметров.
10. Для этого выполните пункт 5.
8. Нажмите кнопку **ОК**.

Таблица 1 Значение параметров аудита системы

Параметр	Значение
Аудит событий входа в систему	Определяет, подлежит ли аудиту каждая попытка пользователя войти в систему или выйти из нее на другом компьютере при условии, что данный компьютер используется для проверки подлинности учетной записи. Если этот параметр политики определен, можно задать аудит успехов или отказов, либо вообще отключить аудит событий данного типа. Аудит успехов означает создание записи аудита для каждой успешной попытки входа в систему. Аудит отказов означает создание записи аудита для каждой неудачной попытки входа в систему.





Окончание табл. 1

Параметр	Значение
Аудит управления учетными записями	Определяет, подлежат ли аудиту все события, связанные с управлением учетными записями на компьютере. К таким событиям относятся следующие события: ➢ создание, изменение или удаление учетной записи пользователя или группы; ➢ > переименование, отключение или включение учетной записи-пользователя; ➢ ^ задание или изменение пароля.
Аудит доступа к службе каталогов	Определяет, подлежит ли аудиту событие доступа пользователя к объекту каталога Active Directory, для которого задана собственная системная таблица управления доступом.

Аудит входа в систему	Определяет, подлежит ли аудиту каждая попытка пользователя войти в систему или выйти из нее на данном компьютере, или подключиться к нему через сеть.
Аудит доступа к объектам	Определяет, подлежит ли аудиту событие доступа пользователя к объекту — например, к. файлу, папке, разделу реестра, принтеру и т. п. — для которого задана собственная системная таблица управления доступом.
Аудит изменения политики	Определяет, подлежит ли аудиту каждый факт изменения политик назначения прав пользователей, политик аудита или политик доверительных отношений.
Аудит использования привилегий	Определяет, подлежит ли аудиту каждая попытка пользователя воспользоваться предоставленным ему правом.
Аудит отслеживания процессов	Определяет, подлежат ли аудиту такие события, как активизация программы, завершение процесса, повторение дескрипторов и косвенный доступ к объекту.
Аудит системных событий	Определяет, подлежат ли аудиту события перезагрузки или отключения компьютера, а также события, влияющие на системную безопасность или на журнал безопасности.

В. Настройка и просмотр аудита папок и файлов (Доступно только на томах NTFS).

1. Установите указатель мыши на файл или папку, для которой Следует выполнить аудит, и нажмите правую кнопку.

2. В появившемся контекстном меню выберите команду **Свойства**.

3. В окне свойств папки или файла перейдите на вкладку **Безопасность**.

4. На вкладке **Безопасность** нажмите кнопку **Дополнительно** и затем перейдите на вкладку **Аудит**.

5. Если Вы хотите настроить аудит для нового пользователя или группы на вкладке **Аудит** нажмите кнопку **Добавить**.

6. Появится диалоговое окно **Выбор: Пользователь, Компьютер или Группа.**

7. Выберите имя нужного пользователя или группы и нажмите кнопку **ОК**. Откроется окно диалога **Элемент аудита для**. Здесь Вы сможете ввести все необходимые параметры аудита.

8. В списке **Применять** укажите, где следует выполнять аудит (это поле ввода доступно только для папок),

9. В группе **Доступ** следует указать, какие события следует отслеживать: окончившиеся успешно (**Успех**), неудачно (**Отказ**) или оба типа событий.

10. **Применять этот аудит к объектам и контейнерам только внутри этого контейнера** — определяет, распространяются ли введенные Вами настройки аудита на файлы и папки, находящиеся ниже по дереву каталогов файловой системы (флажок не установлен). В обратном случае, установите флажок (или выберите в списке) **Применять** ощию **Только для этой папки**. Это:с позволит не выполнять аудит для тех объектов файловой

системы, которые не представляют интереса.

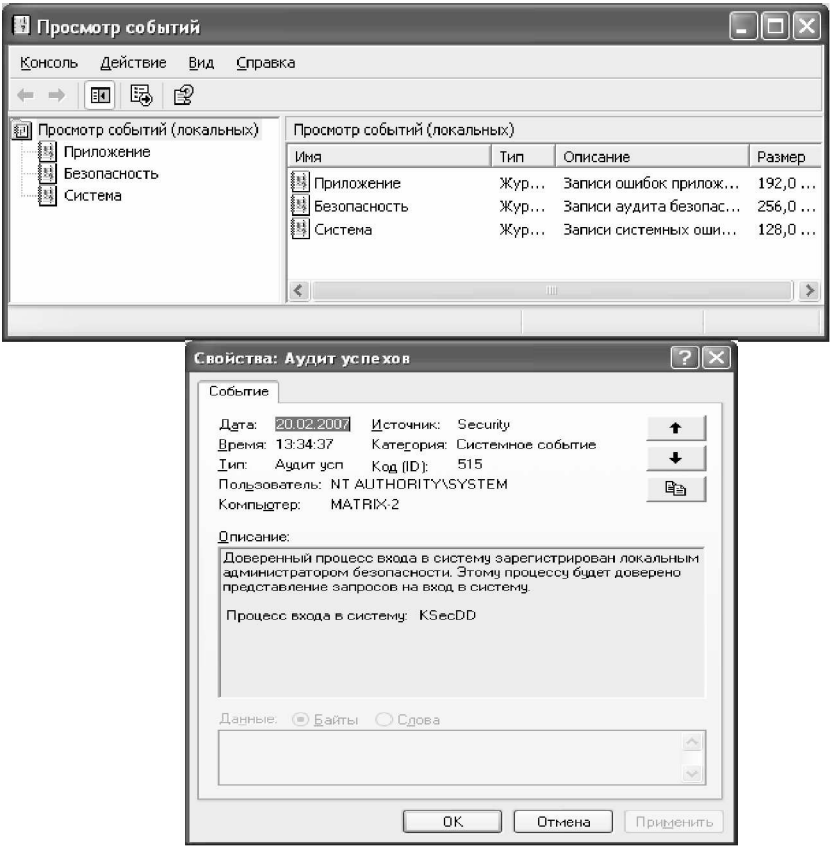
9. После завершения настройки аудита для папки или файла нажмите несколько раз кнопку ОК, чтобы, закрыть все окна диалога.

10.Если Вы хотите просмотреть или изменить настройки аудита для уже существующего пользователя или группы, нажмите кнопку Показать/Изменить. Появится окно диалога Элемент аудита для. Здесь Вы сможете выполнить все необходимые изменения параметров аудита для выбранного Вами пользователя или группы. По окончании внесения изменений нажмите кнопку **ОК**.

Примечание. После включения аудита операционная система Windows 2000 (XP) начинает отслеживать события, связанные с безопасностью. Полученную в результате информацию можно просмотреть с помощью оснастки Просмотр событий. При просмотре журнала событий можно выяснить, кто предпринял попытку выполнения неразрешенного ему действия. Для того чтобы иметь возможность настраивать аудит для файлов и папок, необходимо иметь права администратора.

С. Просмотр событий в журнале событий.

1. Выберите кнопку **Пуск** панели задач.
2. Откройте меню **Настроить/Панель управления**.
3. В открывшемся окне выберите ярлык **Администрирование и далее Просмотр событий.**
4. В открывшемся окне выберите пункт **Безопасность** (рис. 3).
5. В правой половине открытого окна появится список всех зарегистрированных событий.
6. Для просмотра требуемого события вызовите его свойства из контекстного меню или дважды щелкните по его названию левой клавишей мыши.
7. В результате появится окно, как показано на рис. 4.
8. В показанном примере зафиксирован успех **отключения учетной записи Гость** пользователем **Админ** 8.05.04 в 18.28.31.
9. В примере, показанном на рисунке 5, зафиксирован **отказ входа в систему** пользователю **NT AUTHORITY\SYSTEM** (системная учетная запись) 08.05.04 в 17:39:58 по причине «**неизвестное имя** пользователя или **неверный пар**оль».



10. Таким образом, просмотр журнала событий позволяет в полной мере проанализировать действия пользователей и процессов.

Рис. 5

Задания для самостоятельной работы

1. Включите аудит успеха и отказа всех параметров (используйте задание А).
2. Выйдите из системы и предпримите попытку входа в операционную систему с неверным паролем. Откройте журнал событий, найдите соответствующую запись и скопируйте экран в буфер (Print Screen) для отчета.
3. Удалите созданную ранее учетную запись ПЗ-6 и зафиксируйте все события системного журнала, связанные с этим действием для отчета.

Контрольные вопросы

1. Чем отличаются регистрация и аудит?
2. Что является средствами регистрации и аудита?
3. Какие события фиксируются в системном журнале?
4. Что фиксирует система при регистрации событий?

Практическая работа 8
Управление шаблонами безопасности в Windows 2000 (XP)
Краткие теоретические сведения

Управление шаблонами безопасности в **Windows 2000 (XP)** осуществляется с помощью **Редактора шаблонов безопасности**, реализованного в виде оснастки **MMC**.

Он предназначен для создания и редактирования текстовых файлов конфигурации безопасности операционной системы **Windows 2000 (XP)**. Такие файлы значительно легче переносятся с одной системы на другую, чем соответствующие им базы данных безопасности.

Созданные при помощи оснастки **Шаблоны безопасности** текстовые файлы хранятся на жестком диске и при необходимости могут быть импортированы в базу данных безопасности. В этом случае все хранимые настройки безопасности начнут действовать.

Значения параметров обеспечения безопасности заносятся в текстовые файлы с расширением inf, называемые **Шаблонами безопасности**.

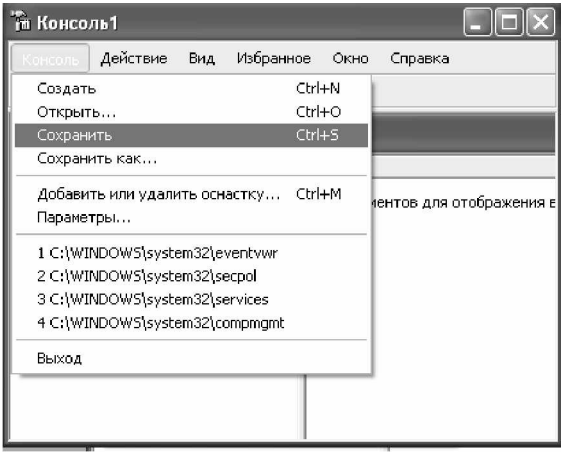
Примечание. Новые **Шаблоны безопасности** не изменяют все старые настройки параметров системы безопасности, они лишь дополняют их, увеличивая (инкрементируя) степень защищенности компьютера. Задание: загрузить редактор Шаблона безопасности, редактировать шаблон безопасности и сохранить его с новым именем.

Алгоритм выполнения работы

А. Загрузка оснастки Шаблоны безопасности.

1. Выберите кнопку **Пуск** в панели задач.
2. Перейдите к пункту **Выполнить**.
3. В открывшемся окне в поле ввода введите команду mmc.
4. В результате откроется консоль управления mmc.
5. В меню **Консоль** выберите команду **Добавить или удалить оснастку** (рис. 6) и нажмите кнопку **Добавить**.
6. В поле **Оснастка** дважды щелкните Шаблоны безопасности.
7. Нажмите кнопку **Закрыть**.

Рис. 6



8. В списке выбранных оснасток для новой консоли появится элемент **Шаблоны безопасности**.

9. Если на консоль не нужно добавлять другие оснастки, нажмите кнопку **ОК**.

10. Чтобы сохранить эту консоль, в меню **Консоль** выберите команду **Сохранить** и укажите имя оснастки **Шаблоны безопасности**.

1L Закройте окно **Консоли** и выберите команду **Пуск** и далее **Все программы.**

12. Найдите пункт **Администрирование** и выберите подпункт **Шаблоны безопасности** (Теперь оснастка с Шаблоны безопасности доступна в меню **Пуск**).

13. Для просмотра значений имеющихся шаблонов в окне оснастки откройте, например, узел **Шаблоны без**опасности, щелчком выберите шаблон безопасности compatws и просмотрите его папки **Политика учетных записей, Локальная поли**тика и др.

14. Помимо раскрытого шаблона безопасности compatws.inf существуют и другие стандартные шаблоны, конфигурации которых позволяют получить различные по надежности системы безопасности.

Б. Редактирование и сохранение шаблона безопасности.

1. Щелкните на одном из стандартных шаблонов безопасности (например, compatws), которые Вы видите в окне оснастки **Шаблоны безопасности.**

2. Если Вы хотите модифицировать какую-либо настройку безопасности, дважды щелкните на ней и отредактируйте значения параметров.

3. Для сохранения откорректированного стандартного шаблона безопасности под другим именем выполните следующие действия.

4. Укажите откорректированный стандартный шаблон (например,

compatws), и нажмите правую кнопку мыши.

5. В появившемся контекстном меню выберите команду **Сохранить как.**

6. Введите с клавиатуры новое имя файла (например, custom). По умолчанию шаблоны безопасности располагаются в каталоге **%SystemRoqt%\Secunfy \Templates**.

7. Пользовательский шаблон будет добавлен в определенную заранее конфигурацию безопасности и сохранен под введенным Вами именем.

Настроив **Шаблон безопасности** для одной ПЭВМ, Вы можете перенести его и на другие ПЭВМ Вашей рабочей группы. **Шаблоны безопасности** являются гибким и удобным инструментом по настройке системы безопасности операционной системы.

Задания для самостоятельной работы

Создайте на базе существующего **Шаблона безопасности** новый шаблон и дайте ему имя ПЗ-8. После этого зафиксируйте список шаблонов, скопировав изображение экрана в буфер и далее в файл для отчета.

Контрольные вопросы

1. Для чего используются **Шаблоны безопасности**?

2. В каком месте на диске хранятся (по умолчанию) шаблоны безопасности?

4 Какие разделы включает стандартный **Шаблон безопасности**?

Практическая работа 9

Настройка и использование межсетевого экрана в Windows 2000 (XP)

Краткие теоретические сведения

Межсетевое экранирование повышает безопасность объектов внутренней сети за счет игнорирования неавторизованных запросов из внешней среды, тем самым обеспечивая все составляющие информационной безопасности. Кроме функций разграничения доступа, экранирование обеспечивает регистрацию информационных обменов.

Функции экранирования выполняет межсетевой экран или брандмауэр (firewall), под которым понимают программную или программно-аппаратную систему, которая выполняет контроль информационных потоков, поступающих в информационную систему и/или выходящих из нее, и обеспечивает защиту информационной системы посредством фильтрации информации. Фильтрация информации состоит в анализе информации по совокупности критериев и принятии решения о ее приеме и/или передаче.

Брандмауэр в **Windows XP** — это система защиты подключения к Интернету (Internet Connection Firewall, ICF), представляет собой программу настройки ограничений, регулирующих обмен данными между Интернетом и небольшой сетью или локальным компьютером. Брандмауэр ICF необходимо установить для любого компьютера, имеющего прямое подключение к

Интернету.

При включении брандмауэра для локального компьютера, подключенного к Интернету с помощью модема удаленного доступа, брандмауэр ICF обеспечивает защиту этого подключения.

Задание: Активизировать встроенный брандмауэр операционной системы Windows XP и настроить его параметры.

Алгоритм выполнения работы

А. Активизация встроенного межсетевого экрана.

1. Откройте компонент **Сетевые подключения**.
2. Для этого выберите последовательно **Пуск — Панель управления — Сетевые подключения.**
3. Выделите подключение удаленного доступа, подключение по локальной сети или высокоскоростное подключение к Интернету, которое требуется защитить брандмауэром, и затем выберите в контекстном меню (при выделенном подключении нажать правую клавишу мыши) команду **Свойства**.
4. На вкладке **Дополнительно** в группе **Брандмауэр подключения к Интернету** (рис. 1) отметьте пункт **Защитить мое подключение к Интернету**.

Примечание. Для отключения брандмауэра достаточно снять флажок **Защитить мое подключение к Интернету**.

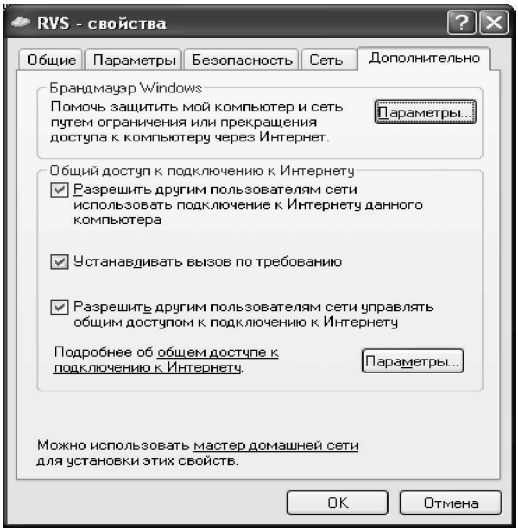


Рис. 1

В. Настройка параметров брандмауэра.

1. Выполните пункты 1-3 предыдущего задания.

2. Выберите кнопку **Параметры** в нижней части открытого окна (рисунок 1).

3. В результате откроется окно **Дополнительные параметры** (рис. 2) с тремя закладками (Службы, Ведение журнала безопасности и ICMP).

5 Выберите закладку **Службы**.

Примечание. На закладке Службы вы можете в явном виде указать службы Интернета, прохождение трафика которых вы допускаете. Например, чтобы обеспечить прохождение веб-страниц из Интернета на компьютер, необходимо включить службу «Веб-сервер HTTP».

5. Отметьте все службы.

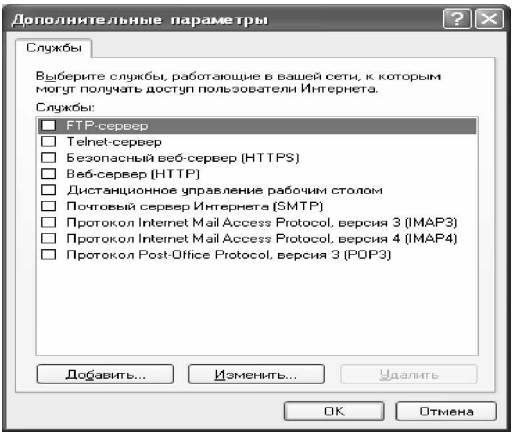


Рис. 2

6 Выберите закладку **Ведение журнала безопасности** .

Примечание. Для брандмауэра подключения к Интернету предусмотрен журнал безопасности для записи событий, связанных с его работой. Журнал безопасности ICF поддерживает следующие возможности.

Запись пропущенных пакетов. Этот параметр задает запись в журнал сведений обо всех потерянных пакетах, исходящих из сети (компьютера) или из Интернета. Если установить флажок **Записывать потерянные па**кеты, будут собираться сведения о каждом пакете, который пытался пройти через ICF, но был обнаружен и отвергнут брандмауэром.

Запись успешных подключений. Этот параметр задает запись в журнал сведений обо всех успешных подключениях, инициированных из сети (компьютера) или из Интернета.

7 Отметь пункты **Записывать пропущенные пакеты и Записывать успешные подключения.** Обратите внимание на расположение журнала безопасности.

Примечание. Журнал безопасности брандмауэра состоит из двух разделов. В заголовке содержатся сведения о версии журнала и полях, в которые можно записывать данные. Содержимое заголовка имеет вид статического списка. Содержимое журнала безопасности представляет собой откомпилированные данные, которые вводятся при обнаружении трафика, пытающегося пройти через брандмауэр. Поля журнала заполняются слева направо, как они расположены на странице. Для того чтобы в журнал вводились данные, необходимо выбрать хотя бы один параметр ведения журнала или оба параметра.

8 Теперь Баш брандмауэр настроен и готов к защите Вашего компьютера от внешних угроз.

Задания для самостоятельной работы

1. Настройте брандмауэр на работу с **Веб-сервером** (HTTP), FTP-сервером и зафиксируйте соответствующее окно для отчета.
2. Включите **журнал безопасности**.
3. После выполнения задания 1 и 2 подключитесь к Интернету и посетите любой веб-сервер.
4. Завершите работу в Интернете и просмотрите **журнал безопасности**.
9 Зафиксируйте записи **журнала безопасности** для отчета.

'Контрольные вопросы

1. Что такое брандмауэр?
2. Какие бывают брандмауэры?

Что фиксирует журнал безопасности брандмауэра?

Практическая работа 10
Создание VPN-подключения средствами Windows 2000 (XP)
Краткие теоретические сведения

Технология виртуальных частных сетей (VPN — Virtual Private Network) является одним из эффективных механизмов обеспечения информационной безопасности при передаче данных в распределенных вычислительных сетях.

Виртуальные частные сети являются комбинацией нескольких самостоятельных сервисов (механизмов) безопасности: шифрования, экранирования и туннелирования.

Задание: Создать VPN-подключение и выполнить его настройку.

Алгоритм выполнения работы

А. Создание VPN-подключения.

1. Откройте компонент **Сетевые подключения**.

2. Для этого выберите последовательно **Пуск — Панель управления — Сетевые подключения.**

3. Выберите пункт **Создание нового подключения** и нажмите кнопку **Далее**.

4. В зависимости от операционной системы выполните следующие действия:

■ для Windows XP — в открывшемся окне выберите пункт **Подключить к сети на рабочем месте** (рис. 1, только для XP) и нажмите Далее. После этого выберите **Подключение к виртуальной частной сети** (рис. 2) и нажмите **Далее**.

■ для Windows 2000 — в открывшемся окне выберите пункт **Подключение к виртуальной частной сети через Интернет** и нажмите **Далее**.

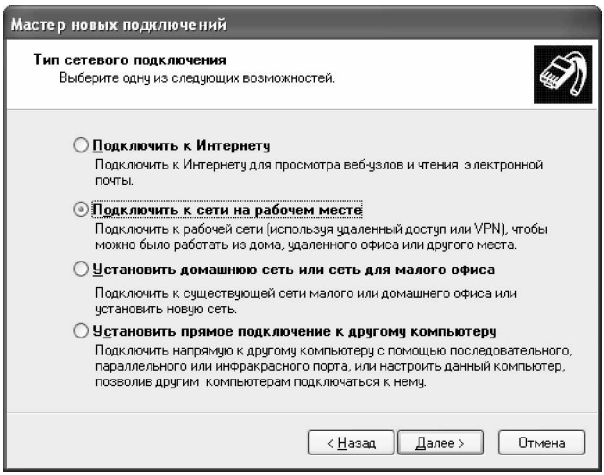


Рис. 1

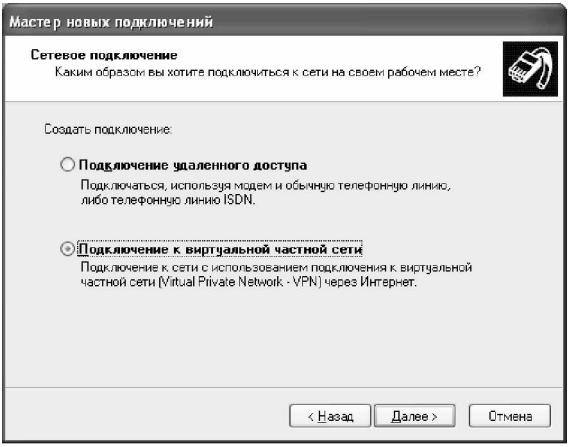


Рис. 2

5. Введите имя подключения и перейдите к следующему шагу командой **Далее**.

6. Если перед установкой «туннельного доступа» требуется подключение к провайдеру услуг Интернета, то выберите (рис. 3) **Набрать номер для следующего предварительного подключения** и, выбрав нужное подключение, нажмите **Далее**. В противном случае, выберите **Не набирать номер для предварительного подключения** и нажмите **Далее**.

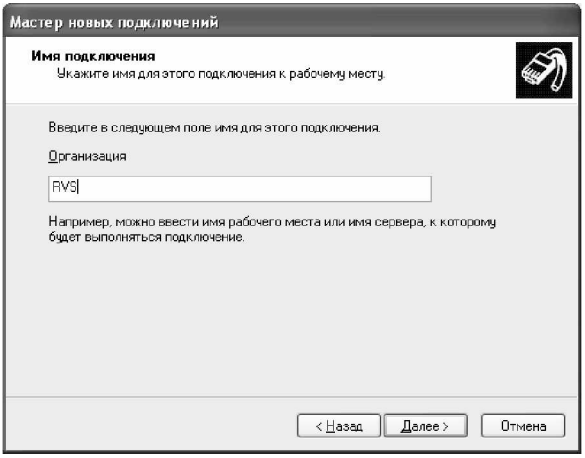
7. Введите имя узла (сети) или его IP-адрес, к которому идет подключение.

8. Завершите работу **Мастера сетевых подключений**.

9. В результате в папке **Подключения** появится новое подключение (рис. 4).

10. Для настройки параметров подключения выделите **подключение VPN** и вызовите его свойства из контекстного меню (нажатие правой клавиши мыши).

Рис. 3



11. Рассмотрите все имеющиеся параметры VPN-подключения (рис. 5) и при необходимости воспользуйтесь соответствующими разделами справки.

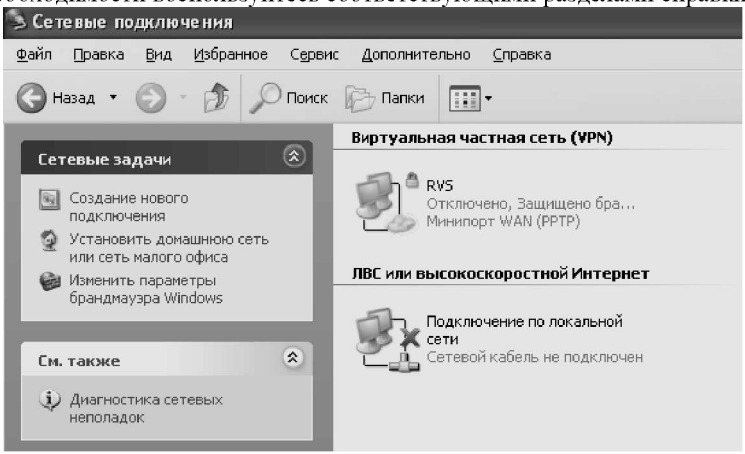


Рис. 4

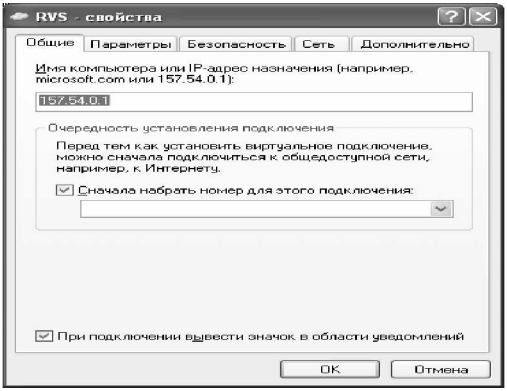


Рис. 5

Задания для самостоятельной работы

Создайте VPN-подключение к узлу с адресом 122.122.122.122 и зафиксируйте окно его свойств (Print Screen) на закладке **Общие** (как показано на рис. 5) в качестве отчета.

Контрольные вопросы

1. Какие механизмы безопасности используются при реализации VPN-подключения?
2. Что такое «туннель» и в чем состоит принцип «туннелирования»?
3 В чем заключаются защитные функции виртуальных частных сетей?

§2.Возможности Windows и Office по защите информации

Служебные программы Windows

Знакомство с программными методами защиты информации начнем с самого простого и важного — рассмотрим возможности операционных систем (ОС) Windows и приложений Office.

В ОС семейства Windows (Windows 95/98/2000/NT/Me/XP), а также в пакеты Office (Office 95/97/2000/XP) встроены некоторые средства, позволяющие во многих случаях избежать потери информации. Основная задача этих средств — диагностика и устранение ошибок в работе компьютера, а также защита информации от несанкционированного доступа. В ОС семейства Windows включена специальная группа программ — Служебные. Программы этой группы позволяют, например, искать и устранять ошибки в работе жесткого или гибкого дисков, оптимизировать их работу, проводить диагностику сети и др.

По рис видно, что в Windows Me и XP среди служебных программ отсутствует проверка диска. Однако это не значит, что в этих системах невозможно осуществить проверку жестких и гибких дисков. Просто нужная программа вызывается не из группы Служебные программы, а другим способом (см. примечания).

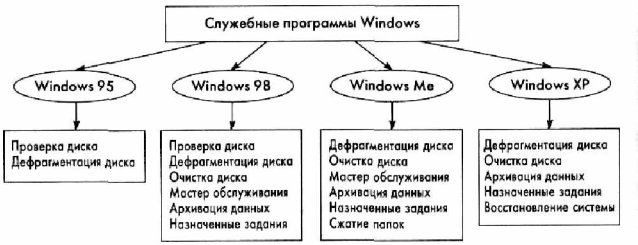


Рис 2.1.Основные программы из группы *Служебные* в Windows 95, 98, Me, XP.

Мы рассмотрим примеры использования некоторых служебных программ для Windows 98 и XP. Выбор операционных систем не случаен. Windows 98, на наш взгляд, сегодня все еще является популярной ОС в России. Windows XP — это система, разработанная на основе технологий, используемых в Windows 2000. Правда, не следует забывать, что Windows XP предъявляет высокие требования к системным ресурсам (не менее 128 Мб оперативной памяти и 2 Гб пространства на жестком диске).

Практическая работа 11.

Дефрагментация диска С
Краткие теоретические сведения

Дефрагментация диска (Defrag) — программа, позволяющая повысить производительность дисков путем оптимизации расположения файлов и папок.

Задача ***дефрагментации***, когда файлы из соседних папок и даже фрагменты одного и того же файла оказываются записанными в разных местах диска. Для того чтобы прочитать или обновить такой файл, компьютеру приходится передвигать головки чтения-записи по всей поверхности диска. А передвижение головок — самая длительная операция при работе с диском. В результате компьютер начинает работать все медленнее, возникают сложности с открытием и сохранением файлов, чаще наблюдаются сбои.

Необходимо принимать какие-то меры. Фирма, конечно, далеко не всегда имеет возможность совместить все свои подразделения в одном большом помещении. Но сделать подобное с файлом или папкой компьютеру очень легко. Для этого и нужна программа дефрагментации. Она располагает файлы на диске так, чтобы оптимизировать доступ к ним, и позволяет значительно ускорить работу компьютера.

Поскольку в процессе работы постоянно происходят запись и удаление информации с диска, через какое-то время расположение файлов вновь становится неудобным для чтения. Поэтому дефрагментацию жестких дисков рекомендуется проводить каждый раз после установки нового программного обеспечения, но не реже одного раза в три месяца .

Практическая работа:

Задание произвести дефрагментацию диска С.

Решение:

Дефрагментация в Windows XP

Программа дефрагментации Windows XP несколько отличается от предыдущих версий Windows .

Алгоритм выполнения работы

1. В Windows XP есть функция анализа, которая не только дает возможность пользователю определить целесообразность проведения дефрагментации, но и определяет список наиболее фрагментированных

(«разорванных») файлов.

Для запуска функции анализа необходимо щелкнуть кнопку ***Анализ*** или выбрать пункт ***Анализ*** в меню ***Действие***.

- После проведения анализа программа выведет на экран подробный отчет (рис. 1.2).

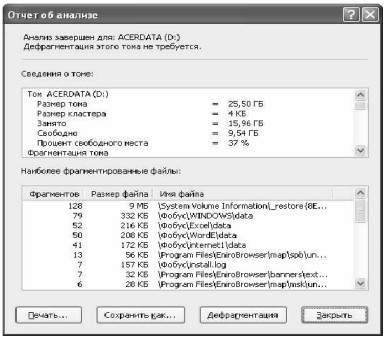


Рис. 2.2.Отчет об анализе диска в программе дефрагментации Windows XP.

2. Запуск процедуры дефрагментации осуществляется с помощью нажатия кнопки ***Дефрагментация*** или выбора соответствующего пункта меню ***Действие***.

- По окончании дефрагментации программа выдает сообщение о завершении операции, ее результатах и предлагает вывести на экран отчет о проделанной работе (рис. 2.3). Отчет о дефрагментации выглядит так же, как отчет об анализе, и предоставляет список файлов, которые невозможно было дефрагментировать.

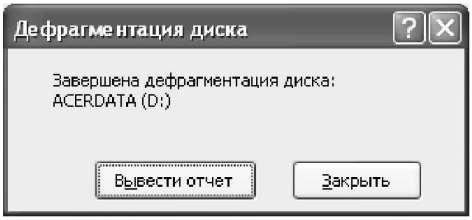


Рис. 2.3. Сообщение о завершении дефрагментации в Windows XP.

3. Windows XP по умолчанию раз в три дня выполняет частичную дефрагментацию (это происходит незаметно для пользователя в процессе записи/чтения файлов и практически не влияет на работу пользователя).

Практическая работа 12

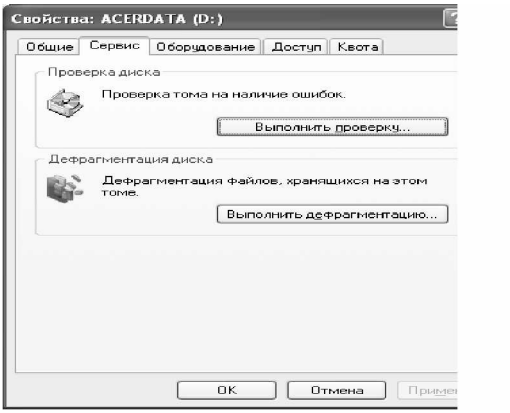
Проверка диска в Windows XP
Краткие теоретические сведения

Проверка диска (Scandisk) — программа, проверяющая корректность длинных имен файлов, структуру папок и системной области, качество поверхности диска и т. д. Программа особенно полезна, когда возникают проблемы при обращении к дискам или обнаруживаются искажения в структуре файлов и папок. Например, если произошел сбой при чтении дискеты, скорее всего, на ней появились поврежденные сектора. Программа проверки диска может переместить информацию из поврежденных участков диска в «здоровые» и пометить поврежденные участки как неиспользуемые. Если программе Scandisk удастся сделать это, по завершении проверки вы сможете прочитать содержимое дискеты.

Задание: произвести проверку диска А.
Алгоритм выполнения работы

1. В Windows XP программу проверки можно запускать только способом, описанным ранее, — нажмите кнопку ***Выполнить проверку*** в окне ***Свойства: Диск***...

Рис, 2.4. Окно программы проверки диска для Windows 98



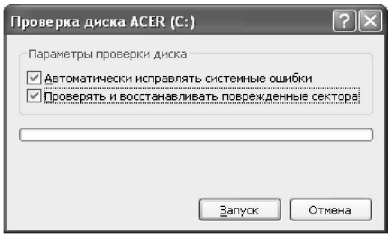


Рис. 2.5 Вкладка Сервис окна Свойства: Дисков Windows XP

- Появится окно ***Проверка диска.***.. (см. рис. 2.4) для диска, выбранного на шаге 2 . В этом окне пользователь может изменить только два параметра (см. рис. 2.5).
- 3. По окончании проверки, в отличие от Windows 98, программа не выдает никаких комментариев. На наш взгляд, это упрощение неудобно для пользователя.

ЗАМЕЧАНИЯ

1. Если ваш компьютер подвержен сбоям а электропитании, то как минимум раз в месяц необходимо запускать программу Проверка диска. Программу Дефрагментация рекомендуется включать каждый раз после установки новых программ.

2. Обе программы для полной проверки требуют достаточно много времени. Их работа может продолжаться час, два и дольше. Время проверки зависит от общего объема дисков, объемов хранящейся на них информации, объемов оперативной памяти данного компьютера и т. д.

3. Обе программы достаточно просты и доступны в применении, но требуют регулярного запуска. К сожалению, как показывает опыт, пользователи в большинстве случаев забывают об этом в потоке текущих дел. В этом случае серьезную помощь может оказать программа Мастер обслуживания.

Практическая работа 13

Работа с программой мастер обслуживания

Краткие теоретические сведения

Эта программа сама возьмет на себя функции по запуску программ обслуживания дисков в определенное пользователем время.

Для того чтобы воспользоваться ***Мастером обслуживания***, необходимо следующее.

1. Составить задание (список программ) на обслуживание в определенное время.

2. На время работы программы оставить включенным системный блок компьютера (монитор, принтер и другие внешние устройства можно отключить).

Задание**: составить задание для программы *Мастер обслуживания*.**

Алгоритм выполнения работы

Запустите программу Мастер обслуживания: ***Пуск > Программы > Стандартные > Служебные > Мастер обслуживания.***

1. В первом окне мастера выберите опцию ***Особый, с выбором параметров***, чтобы самостоятельно установить нужные параметры работы программы

3. Во втором окне мастера установите время проведения обслуживания Не забывайте, что в это время компьютер должен быть включен.

4 В третьем окне мастер выведет список программ, которые автоматически запускаются при загрузке Windows (рис. 2.6.). Любая программа из этого списка увеличивает время загрузки ОС и, работая постоянно, забирает часть оперативной памяти, что, в свою очередь, влияет на общую производительность компьютера. Поэтому снимите флажки с тех программ, запуск которых при каждой загрузке Windows вам не нужен.

5 В четвертом и пятом окнах мастера вам будет предложено выбрать время дефрагментации и проверки диска. Нажав на кнопку ***Расписание***, вы сможете детально настроить время запуска. Кнопка ***Настройка*** открывает окно настройки нужной программы

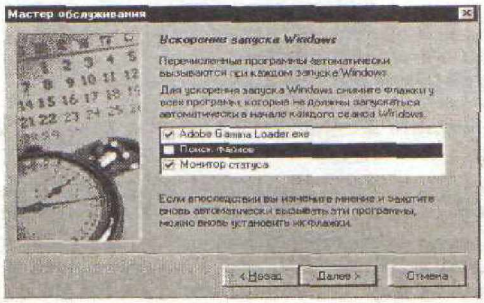
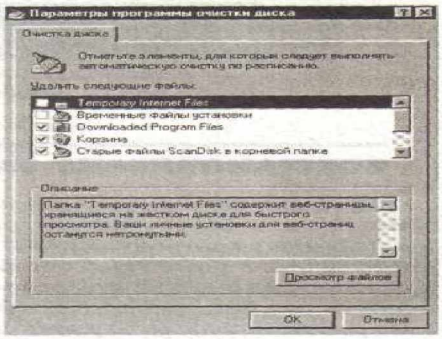


Рис.2.6 Третье окно Мастера обслуживания: настройка списка



программ, запускаемых при каждой загрузке Windows.

Рис. 2.7. Выбор параметров очистки диска.

6 В следующем окне будет выведен ***список папок, в которых хранятся временные файлы. Нажмите кнопку Настройка***.

- Появится окно ***Параметры программы очистки диск***а (рис2.7.).

7. Отметьте в окне ***Параметры программы очистки папки***, которые необходимо очистить. Чтобы ваш компьютер не хранил лишний «мусор», рекомендуем поставить «галочки» напротив всех папок, кроме ***Temporary Internet Files*** и ***Корзина***. Папка ***Temporary Internet Files*** содержит файлы посещенных вами Веб-страниц и позволяет значительно ускорить загрузку этих страниц при их повторном посещении, а часто даже работать со страницами автономно (без подключения к Интернету).

8. В последнем окне (рис. 2.8) мастер покажет, что он будет делать согласно произведенным вами установкам. Если результат вас устраивает, щелкните кнопку ***Готово.***

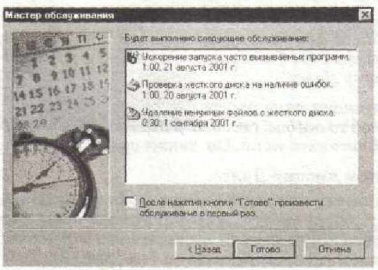


Рис. 2.8. Последнее окно Мастера обслуживания: Информация о произведенных вами настройках.

ПРИМЕЧАНИЕ: отключение Мастера обслуживания

Чтобы отключить ***Мастер обслуживания***, запустите его снова и в соответствующих окнах отметьте пункты ***Не производить дефрагментацию диска, Не выполнять проверку диска и т. д.***

Практическая работа 14

Восстановление конфигурации WINDOWS XP

Краткие теоретические сведения

Функция восстановления конфигурации Windows XP позволяет возвращаться к более ранним параметрам и настройкам системы. Если вы, работая с настройками ОС, сделали что-то неправильно, и после этого система стала работать с ошибками, или, установив новое приложение, вы обнаружили, что его работа приводит к сбоям, вы всегда сможете вернуть конфигурацию системы в предыдущее состояние. Состояние, в которое необходимо вернуть настройки Windows XP, называется ***контрольной точкой восстановления.***

Функция восстановления конфигурации особенно полезна для пользователей, которые осваивают работу с Windows XP. Операционная система ***Windows XP*** предоставляет пользователю широкие возможности по настройкам различных параметров системы, работе с дисками, учетными записями и пр. При этом возможно возникновение ошибок или установка ненужных параметров. Все вновь возникшие проблемы, как правило, можно решить с помощью восстановления системы.

Восстановление системы происходит без потери текущих данных: документов, почтовых сообщений и т. п.

Задание: вернуть конфигурацию Windows XP в предыдущее (рабочее) состояние.

Алгоритм выполнения работы

- Выберите ***Пуск > Программы > Стандартные > Служебные > Восстановление системы.***
- В появившемся окне программы (см. рис. 2.9) отметьте пункт Восстановление более раннего состояния компьютера и нажмите кнопку ***Далее.***

- В следующем окне программы укажите дату и название контрольной точки. Контрольные точки создаются системой автоматически. См. также примечание к этому примеру.
- Нажмите кнопку ***Далее***.
- Начнется процедура восстановления. Процесс занимает несколько минут. Автоматически производится перезагрузка компьютера и выводится на экран окно с подтверждением окончания работы.

ПРИМЕЧАНИЕ: отключение Мастера обслуживания

Чтобы отключить Мастер обслуживания, запустите его снова и в соответствующих окнах отметьте пункты ***Не производить дефрагментацию диска, Не выполнять проверку диска и т. д.***

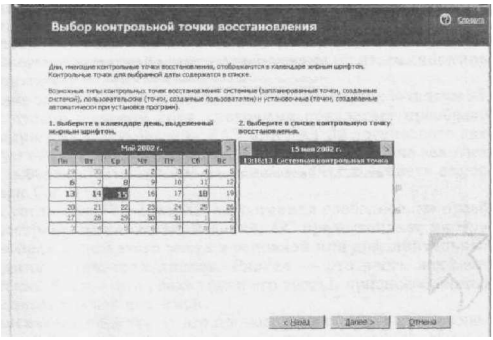


Рис. 2.9. Выбор контрольной точки при восстановлении системы в Windows XP.

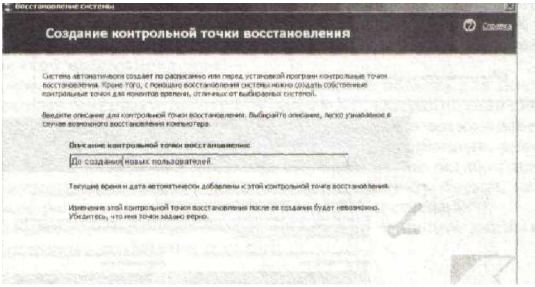
ПРИМЕЧАНИЕ: создание контрольной точки

Windows XP ежедневно автоматически (когда компьютер включается) создает контрольные точки. Но в любое время вы можете создать свою контрольную точку, присвоить ей определенное имя и смело приступать к экспериментам.

1. Откройте окно программы ***Восстановление системы***.

2. Отметьте пункт ***Создать точку восстановления*** и нажмите кнопку ***Далее.***

Рис. 2.10. Ввод имени контрольной точки в ***Windows XP***



3. На завершающем этапе вам будет предложено ввести имя контрольной точки (рис. 2.10).

Практическая работа 15.

Создание логических дисков на компьютере без операционной системы

Краткие теоретические сведения

Файловая система — это метод, который операционная система использует для хранения информации о структуре папок и файлов и доступа к этим файлам на диске. ***Файловой системой*** называют и саму структуру папок и файлов (дерево папок). **Windows 95, 98**, Me работают с файловыми системами ***FAT*** и ***FAT 32***. Как уже говорилось выше, **Windows XP** использует технологии, применяемые в сетевых операционных системах **Windows NT** и **2000**, и работает с файловой системой **NTFS**. Сразу следует отметить некоторые преимущества файловой системы **NTFS перед FAT (FAT 32)** в плане защиты информации:

- при отказе системы (сбоя в питании, ошибки записи на диск) **NTFS** с помощью особых средств во многих случаях обеспечивает возможность восстановления утраченных данных;
- при работе в сети для каждого файла, размещенного на диске с **NTFS**, обеспечивается дополнительная защита от несанкционированного доступа.

При установке операционной системы **Windows XP** поверх **Windows 95/ 98/Me** или на пустой жесткий диск программа предлагает преобразовать действующую файловую **систему FAT** или **FAT 32** логического диска С в файловую систему **NTFS**. Если вы уверены в том, что не захотите впоследствии заменить Windows XP на **Windows 98**, то можете отформатировать **диск С** в **NTFS**.

Если после установки **Windows XP** вы оставили свободное, не

преобразованное пространство на жестком диске, **ОС** предоставляет инструменты для преобразования этого места в основной или дополнительный раздел и создания логических дисков. **Раздел** — это часть жесткого диска. **Логический диск** — это раздел (или его часть), приспособленный для работы с операционной системой.

Создание **логических дисков** — это произвольная (по согласованию с пользователем) разбивка жесткого диска на несколько частей. Каждой части присваивается собственное имя (по буквам латинского алфавита: **C, D, E** и т. д.), и пользователь может работать с этой частью так, как будто это самостоятельный жесткий диск.

Разбивка современных жестких дисков (особенно с учетом их огромной емкости) позволяет:

- быстро создавать резервные копии ;
- использовать на одном компьютере несколько различных операционных систем;
- обеспечить удобство работы на одном компьютере нескольким пользователям и др.

Разбить и переразбить жесткий диск на компьютере с **Windows 98/ Me** или без операционной системы можно при помощи программы ***Fdisk*** (см. пример 2.1). ***Windows XP*** имеет встроенную программу для разбивки дисков (см. пример 2.2).

Замечание. Как правило, когда вы покупаете новый компьютер без операционной системы, его жесткий диск часто состоит из основного раздела DOS (с логическим диском C).

Задание: создать три логических диска на винчестере без ОС, состоящего из одного логического диска C.

ВНИМАНИЕ!

Для выполнения этого примера вам потребуется загрузочная дискета . Без загрузочной дискеты вам не удастся загрузить компьютер, лишенный **ОС**. После того как вы выполните переразбивку жесткого диска способом, представленным в этом примере, все файлы, находящиеся на диске, будут безвозвратно удалены.

Алгоритм выполнения работы

1. Вставьте загрузочную дискету и включите компьютер.
2. Когда загрузка закончится, в командной строке введите ***fdisk***.

- Будет запущена программа ***Fdisk***, и на экране появится вопрос о включении поддержки больших дисков.

3. Нажмите клавишу ***Enter***.

- Появится список параметров программы ***Fdisk*** . Введите цифру 3, чтобы выбрать пункт ***Удаление раздела либо логического диска DOS***, и нажмите ***Enter***.

4. В меню ***Удаление раздела DOS или логического диска DOS*** выберите пункт ***Удаление основного раздела DOS*** (цифра 1 и ***Enter***).

- На экране отобразится информация об основном разделе жесткого диска.

10 Клавиша ***Enter*** запускает процесс удаления, при этом вся информация, находящаяся в разделе (в данном случае на диске С), будет утеряна.

- В результате вы получаете абсолютно чистый жесткий диск, который можно разбивать на любое количество логических дисков. Программа вновь отобразит на экране меню ***Параметры Fdisk***

11.Прежде всего, необходимо вновь создать основной раздел (диск С). Выберите пункт 1 ***Создание раздела DOS либо логического диска DOS.***

*12.*В меню ***Создание раздела DOS либо логического диска DOS*** выберите пункт 1 ***Создание основного раздела DOS.***

13.На следующем шаге программа предлагает ввести размер основного раздела. Укажите объем в мегабайтах. Клавиша ***Enter*** запускает процесс создания основного раздела и нового логического диска С.

- По завершении операции программа вновь возвратит вас к этапу выбора параметров .

9. Другие логические диски можно создавать только в дополнительном разделе. Выберите пункт 1 ***Создание раздела DOS либо логического диска DOS*** и в следующем меню — пункт 2 ***Создание дополнительного раздела DOS***. Для дополнительного раздела укажите размер, равный оставшемуся объему жесткого диска. Нажмите ***Enter***.

- Будет создан дополнительный раздел. Теперь можно приступать к созданию логических дисков.

10.В меню ***Параметры Fdisk*** выберите пункт 1 ***Создание раздела DOS либо логического диска DOS***, затем пункт 3 ***Создание логических дисков***

DOS в дополнительном разделе DOS.

11.Для нового логического диска D введем объем, равный, например, половине объема дополнительного раздела. Аналогично создадим следующий логический диск.

12. По окончании работы над разбивкой жесткого диска можно просмотреть информацию о разделах и логических дисках. В окне ***Параметры Fdisk*** выберите пункт 4 ***Вывод сведений*** об имеющихся разделах — отобразятся сведения о разделах жесткого диска. Нажмите еще раз клавишу Enter для просмотра данных о логических дисках.

Практическая работа 16.

Настройка разделов диска в WINDOWS XP

Задание: создать раздел на жестком диске.

Алгоритм выполнения работы

1. Запустите программу ***Управление компьютером***. Для этого на ***Рабочем столе*** или в ***Главном меню*** щелкните правой кнопкой мыши по значку ***Мой компьютер*** и в появившемся контекстном меню выберите пункт ***Управление.***

2. На панели ***Структура*** (в левой части окна программы) выберите папку ***Управление дисками*** (Рис 2.11).

3. Щелкните правой кнопкой по окошку, отображающему нераспределенную часть диска (в правой нижней части окна, см. рис. 2.11), и выберите пункт ***Создать раздел***... f

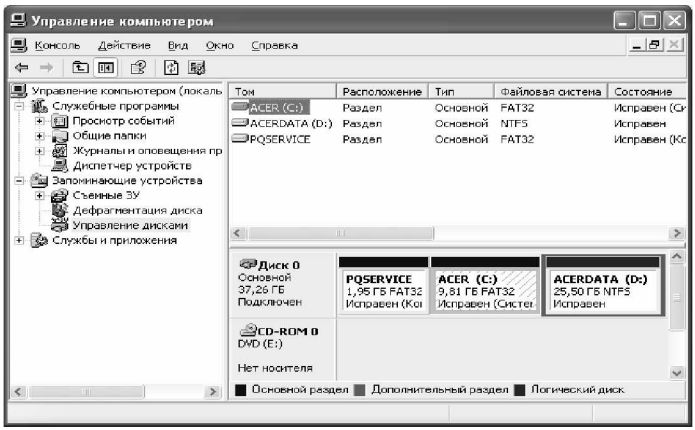


Рис 2.11 Панель Управление компьютером

- Будет запущен мастер создания разделов. Этот мастер на каждом шаге будет выдавать подробное описание каждого действия. Например, при выборе типа раздела (основной или дополнительный) программа выдаст комментарии о каждом из предложенных типов.

4. При создании раздела в нераспределенной области жесткого диска мастер предлагает указать размер нового раздела .

5. После создания раздела мастер предложит создать логический диск. В процессе работы мастера для создания логических дисков необходимо выбрать файловую систему.

Примечания Для некоторых версий Windows XP

- Чтобы открыть оснастку «Управление компьютером», нажмите кнопку **Пуск** и выберите команду **Панель управления**. Дважды щелкните значок **Администрирование**, а затем дважды щелкните значок Управление **компьютером**.
- Для получения сведений об использовании компонента «Управление дисками» выберите команду **Справка** в меню **Действие** окна «Управление компьютером».

ПРИМЕЧАНИЕ 2 : преобразование файловой системы дисков

Если на вашем компьютере существует несколько логических дисков, то программа ***Управление компьютером*** позволяет преобразовывать их файловую систему в FAT 32 или NTFS (за исключением диска, на котором установлена ***Windows XP***, как правило, это диск С).

Установка свойств файлов и папок

Краткие теоретические сведения

Определенный эффект по защите файлов и папок от стирания и порчи может дать работа с окном ***Свойства*** папки или файла (рис. 2.12). Чтобы открыть это окно, щелкните по нужной папке или файлу правой кнопкой мыши и в появившемся контекстном меню выберите пункт ***Свойства.***

Окно ***Свойства*** содержит следующую информацию:

- тип файла;

- местоположение файла или папки в структуре папок;
- объем занимаемого файлом или папкой места на диске;
- количество файлов и папок, которые содержит папка;
- время создания файла или папки.

В окне ***Свойства*** вы можете установить атрибуты файла, отметив соответствующий пункт.

Скрытый. Отметив этот пункт, вы сделаете файл (папку) невидимой для пользователя, если на вкладке ***Вид*** окна ***Вид > Свойства*** папки (в меню папки) выбран пункт ***Не показывать скрытые файлы***. Этот прием поможет избежать случайного удаления важных файлов

4. ***Только чтение***. Если этот флажок установлен, пользователь не сможет изменить содержимое файла, а при попытке его удаления будет выведено дополнительное сообщение о том, что данный файл доступен только для чтения.

Рис. 2.12. Окно свойств папки или файла в Windows 98.

Практическая работа 17.

Установка пароля на заставку

Краткие теоретические сведения

Вы, знаете, что в Windows можно установить режим защиты экрана — заставку. Если вы не хотите, чтобы кто-нибудь мог воспользоваться вашим компьютером, когда вы ненадолго отлучились, установите пароль на

выключение заставки.

Задание**:**

Алгоритм выполнения работы

:

1. Щелкните правой кнопкой мыши в пустом месте ***Рабочего стола*** и в появившемся контекстном меню выберите пункт ***Свойства***.

2. В открывшемся окне ***Свойства: Экран*** перейдите на вкладку ***Заставка*** (рис. 2.13). Если заставка еще не установлена,

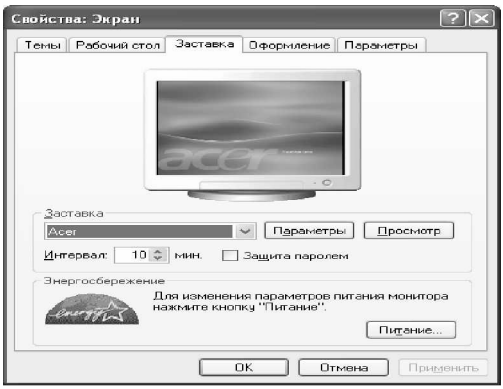


Рис. 2.13. Настройка заставки в Windows .

в поле ***Заставка*** выберите вид заставки. Отметьте пункт ***Пароль*** и нажмите кнопку Изменить.

- Появится окно ***Изменение пароля.***

3. Дважды введите пароль .

- При вводе пароль отображается звездочками или кружочками.

ВНИМАНИЕ!

Для обеспечения достаточного уровня безопасности используйте пароли длиной не менее 8 символов. Лучше, если это будет случайная комбинация букв и цифр, а не существующее в каком-либо языке слово. Помните, что в паролях учитывается регистр букв.

Пароли мешают работе пользователя. Поэтому устанавливайте их

только в том случае, если это действительно необходимо. Обязательно запомните пароль, иначе вы не сможете отключить заставку!

4. В поле ***Интервал*** установите время, через которое будет запущена заставка, если вы не трогаете клавиатуру и мышь. Оптимальное время — 5 минут. Нажмите кнопку ОК.

- Теперь, если в течение заданного времени вы не используете мышь и клавиатуру, будет появляться заставка. При попытке отключить заставку (нажатии клавиши, сдвигании мыши) будет появляться окно Программа-заставка для Windows, в которое необходимо ввести пароль

пароля при отключении заставки.

- Для того чтобы установить новый пароль заставки (или отменить его), не нужно знать старый пароль! Поэтому, уходя, включите заставку вручную (это можно сделать, например, нажав кнопку Просмотр в окне настройки заставки)

.

Пароли. Многопользовательская работа

Операционные системы семейства Windows предоставляют возможность каждому пользователю, работающему с данным компьютером, задавать свои собственные настройки системы.

Практическая работа 18
Создание учетной записи
Краткие теоретические сведения

Windows XP предоставляет большие возможности для защиты от несанкционированного доступа. При установке Windows XP можно создать одну или несколько **учетных записей** пользователей, в том числе и с возможностью администрирования (управления данным компьютером).

На, этапе установки лучше создать только одну учетную запись основного (наиболее опытного) пользователя с функциями администратора. Затем администратор сможет создать учетные записи для других пользователей (с различными возможностями).

Задание: создать учетную запись с функциями администратора.

Алгоритм выполнения работы

11 Откройте программу ***Учетные записи пользователей (Пуск > Панель управления > Учетные записи пользователей)*** и выберите задание ***Создание учетной записи*** (рис. 2.14).

12 Укажите имя создаваемого пользователя, например, ***новый пользователь***. Нажмите кнопку ***Далее***.

13 Установите тип учетной записи. Для пользователя с установленным типом ***Администратор компьютера*** возможности при работе являются неограниченными. Пользователь с типом ***Ограниченная запись*** не имеет возможности устанавливать новые программы, создавать новых пользователей, изменять или удалять системные файлы и т. д.

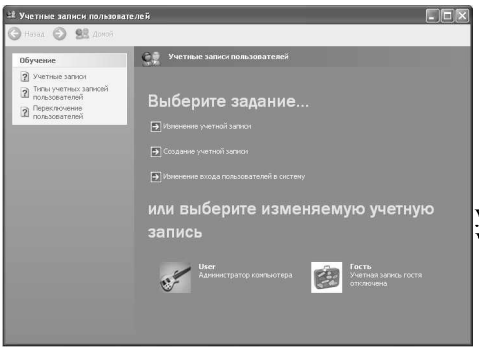


Рис 2.14. Выбор типа учетной записи в Windows XP.

4. Нажмите кнопку ***Создать учетную запись.***

- Имя нового пользователя появится в основном окне ***Учетные записи пользователей***. По умолчанию основная и вновь создаваемые учетные записи не имеют пароля для входа в систему.

5. Чтобы установить для учетной записи пароль, в основном окне ***Учетные записи пользователей*** выделите нужную учетную запись и выберите действие ***Изменение входа пользователей в систему***, а затем команду ***Создание пароля***.

- При загрузке системы в приветственном окне отображаются значки всех зарегистрированных на данном компьютере пользователей. Если для каждой учетной записи установлен пароль на вход в систему, то несанкционированный доступ к компьютеру таким образом практически

исключен.

ПРИМЕЧАНИЕ: гостевой доступ

Иногда возникает необходимость, чтобы к компьютеру имел доступ пользователь, который постоянно на нем не работает. Для этого в Windows XP существует учетная запись Гость. Эта учетная запись имеет тип ***Ограниченная запись***, и пользователь, работающий под этой учетной записью, не имеет возможности изменить системные файлы и настройки, а также не имеет доступа к файлам и папкам других пользователей.

1. В окне ***Учетные записи пользователей*** выделите запись Гость, выберите задание ***Изменить учетную запись*** и в открывшемся окне нажмите кнопку ***Включить учетную запись «Гость».***

Возможности приложений OFFICE

Рассмотрим некоторые возможности по защите информации, заложенные в распространенных офисных приложениях Word, Excel, PowerPoint.

Практическая работа 19

Автосохранение документа

Краткие теоретические сведения

В процессе редактирования документа может произойти сбой в электропитании или «зависание» компьютера. В этом случае вся работа, выполненная вами с момента последнего сохранения файла, будет утеряна. Режим автосохранения позволяет минимизировать такие потери.

Задание: настроить автосохранение в Word.

Алгоритм выполнения работы

14 Выберите в главном меню Word пункт ***Сервис > Параметры***.

15 В открывшемся окне **Параметры** перейдите на вкладку ***Сохранение*** (рис. 2.15).

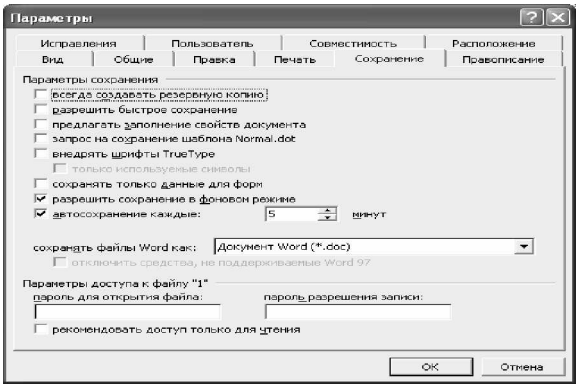


Рис. 2.15. Вкладка ***Сохранение*** окна Параметры Word .

3. Отметьте пункт Авт***осохранение каждые***... и укажите интервал времени, через который необходимо производить автосохранение. Оптимальным является период в 2-3 минуты.

Практическая работа 20.

Защита документа паролем (ДЛЯ OFFICE 97-2000)

В MS Office существует возможность установить пароль для открытия и изменения файла документа.

Задание: установить пароли для чтения и изменения документа Word 97-2000.

Алгоритм выполнения работы

8 **Откройте вкладку *Сохранение* окна Параметры**, как показано в п. 1-2 примера 4.1.

9 В нижней части окна (область ***Параметры доступа к файлу***...) введите в соответствующие поля ***пароль для открытия файла*** и ***пароль разрешения записи***.

- Вводимые пароли будут отображаться звездочками или кружочками.

ВНИМАНИЕ!

Для обеспечения достаточного уровня безопасности используйте пароли длиной не менее 8 символов. Лучше, если это будет случайная

комбинация букв и цифр, а не существующее в каком-либо языке слово. Помните, что в паролях учитывается регистр букв.

Пароли мешают работе пользователя. Поэтому устанавливайте их только в том случае, если это действительно необходимо. Обязательно запомните пароль, иначе вы не сможете открыть документ!

3. Нажмите кнопку ОК.

- На экране дважды появится окно ***Подтверждение пароля***, в котором необходимо будет повторить ввод паролей (сначала — для открытия файла, а затем — для записи).

ПРИМЕЧАНИЕ: **установка пароля в Office XP**

В Office XP пароль задается на вкладке ***Безопасность*** окна ***Параметры*** .

Защит книги или листа EXCEL

Рассмотрим способы защиты, которые предоставляет пользователю меню ***Сервис > Защита*** приложения Excel (рис. 2.16).

Каждый пункт этого меню вызывает соответствующее окно, в котором можно настроить параметры данного вида защиты и при необходимости задать пароль для снятия защиты.

3. ***Защитить лист***. Выбор этого пункта меню позволяет защитить ячейки текущего листа книги от изменений.

4. ***Защитить книгу***. Выбор этого пункта позволяет защитить от изменений всю книгу. Если в появившемся окне ***Защитить книгу*** отметить пункт ***Структуру***, пользователь не сможет перемещать, удалять/добавлять, скрывать/отображать и переименовывать листы. Флажок ***Окна*** позволяет сделать неизменными местоположение и размер окна.

5. ***Защитить книгу и дать общий доступ***. Этот пункт разрешает всем пользователям сети редактировать книгу. При этом запрещается отмена режима исправлений и удаление листов книги.

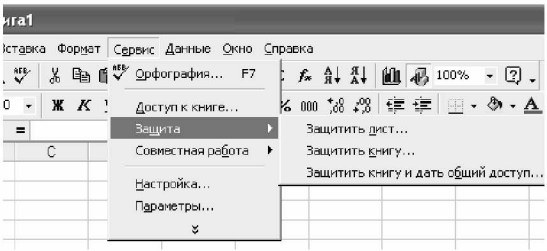
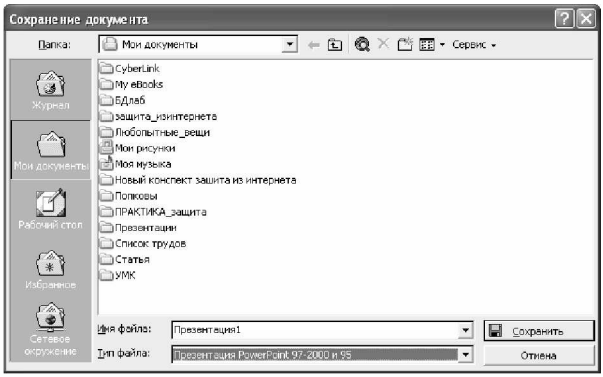


Рис. 2.16 Меню ***Сервис > Защита*** в Excel 97/2000.

Для снятия любого из трех видов защиты необходимо выбрать соответствующий пункт в меню ***Сервис > Защита*** (например, ***Снять защиту листа)*** и ввести пароль, если он был задан.

Выбор типа файла при сохранении
Краткие теоретические сведения

При сохранении рабочих файлов с помощью команд ***Файл > Сохранить и Файл > Сохранить как...*** следует обращать внимание на выбор параметра ***Тип файла***. Например, если вы создаете презентацию в PowerPoint 2002 (Office XP), но предполагаете, что ее придется просматривать на компьютере,



установлен Office 97, в поле Тип файла необходимо выбрать пункт где

Рис. 2.17. Выбор типа файла при сохранении презентации в PowerPoint 2002

Презентация PowerPoint 97-2002 и 95 (рис. 2.17).

Практическая работа 21.

Установка пароля на включение компьютера

Существует довольно простой способ защитить ваш компьютер от несанкционированного доступа — установить пароль на его включение.

Задание: установить пароль на включение компьютера.

1. Включите компьютер. В первые секунды его работы обратите внимание на сообщение:

Press Del to run Setup

(нажмите клавишу Del для запуска режима установок BIOS).

3.Пока видно это сообщение, нажмите клавишу ***Del.***

4.В появившемся меню при помощи клавиш ↑↓ выберите пункт USER PASSWORD и нажмите клавишу Enter.

- Появится окно ***Enter password***.

4. Введите пароль и нажмите клавишу ***Enter***. Лучше, чтобы это была случайная комбинация букв и цифр, а не существующее в каком-либо языке слово. Помните, что в паролях учитывается регистр букв.

- При вводе пароль отображается звездочками.

6.В появившемся окне ***Confirm Password*** повторите ввод пароля и нажмите клавишу ***Enter***.

7.Выберите пункт ***SAVE & EXIT SETUP***.

- Появится окно с сообщением ***SAVE to CMOS and EXIT (Y/N)?*** (сохранить изменения и выйти?).

8.Нажмите клавишу **Y** (ответ «да» — **Yes**), а затем — **Enter**.

- Теперь при включении компьютера будет появляться окно, предлагающее ввести пароль, и если пароля вы не знаете, компьютер не будет загружаться

Содержание

§ 1. Настройки Windows и Office по защите информации

Практическая работа 1
Восстановление зараженных файлов 3

Практическая работа 2
Профилактика проникновения «троянских программ» 4

Практическая работа 3
Настройка безопасности почтового клиента Outlook Express 8

Практическая работа 4
Настройка параметров аутентификации Windows 2000 (XP) 13

Практическая работа 5
Шифрующая файловая система EFS и управление сертификатами в Windows 2000(XP) 18

Практическая работа 6
Назначение прав пользователей при произвольном управлении доступом в Windows 2000 (XP) 23

Практическая работа 7
Настройка параметров регистрации и аудита в Windows 2000 (XP) 27

Практическая работа 8
Управление шаблонами безопасности в Windows 2000 (XP) 33

Практическая работа 9
Настройка и использование межсетевого экрана в Windows 2000 (XP) 35

Практическая работа 10
Создание VPN-подключения средствами Windows 2000 (XP) 38

§ 2. Возможности Windows и Office по защите информации
Служебные программы Windows

Практическая работа 11
Дефрагментация дика С 44

Практическая работа 12
Проверка диска в Windows XP 46

Практическая работа 13
Работа с программой мастер обслуживания 47

Практическая работа 14
Восстановление конфигурации WINDOWS XP 50

Практическая работа 15
Создание логических дисков на компьютере без операционной системы 52

Практическая работа 16
Настройка разделов диска в WINDOWS XP 55
Практическая работа 17
Установка пароля на заставку 57
Практическая работа 18
Создание учетной записи 59
Практическая работа 19
Автосохранение документа 61
Практическая работа 20
Защита документа паролем (ДЛЯ OFFICE 97-2000) 62
Практическая работа 21
Установка пароля на включение компьютера 64

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Практикум

Печать офсетная. Бумага «Canon Office». Гарнитура «Times New Roman».
Подписано в печать 21.04.2008. Формат 60×90/16
Печ. л. 4,25. Тир. 50. Зак. 91

ФГОУВПО «Санкт-Петербургский гос. ун-т культуры и искусств»
191186, Санкт-Петербург, Дворцовая наб., 2. Тел. 312 85 73