|  |
| --- |
| имени-вострухина |
| **115172, Москва, ул. Б.Каменщики, д. 7; тел., факс: (495) 911-20-77; e-mail:**  [**spo-54@edu.mos.ru**](mailto:spo-54@edu.mos.ru) |

**ОТДЕЛЕНИЕ «Автоматизации, радиоэлектроники и ИКТ»**

**ПЦК ( КМК) 090305 Информационная безопасность автоматизированных систем**

**УТВЕРЖДАЮ**

**Зам. директора по УМР**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Бозрова И.Г.

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОВЕДЕНИЮ**

**ПРАКТИЧЕСКИХ ЗАНЯТИЙ**

для специальности **090305 Информационная безопасность автоматизированных систем**

*(по программе углубленной подготовки)*

по МДК.02.01. Программно-аппаратные средства обеспечения информационной безопасности

ПМ.02. Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах

**Разработчик:**

преподаватель ГБПОУ Колледж связи №54имени П.М Вострухина Агаян А. А.

**Методические рекомендации рассмотрены и одобрены на заседании ПЦК ( КМК)** спец.090305 Информационная безопасность автоматизированных систем

протокол №\_\_\_ от «\_\_»\_\_\_\_\_\_\_. 2014 г.

Председатель ПЦК \_\_\_\_\_\_\_\_\_\_\_\_ В. С. Колесников

**Содержание**

[1. Общие положения](#__RefHeading___Toc306010771) 3-5

[2. Методика и средства выполнения практических работ](#__RefHeading___Toc306010772) 6-8

[3. Этапы выполнения практических работ](#__RefHeading___Toc306010773) 6

[4. Тематика практических работ и задания к ним](#__RefHeading___Toc306010774) 8-124

[5. Учебно-методическое и информационное обеспечение дисциплины](#__RefHeading___Toc306010775) 125-126

# Общие положения

**Цель и задачи выполнения практических работ**

Данные методические указания предназначены для закрепления теоретических знаний, полученных в рамках лекционного курса, и приобретения необходимых практических навыков и умений в решении профессиональных задач по программе междисциплинарного курса по МДК.02.01. «Программно-аппаратные средства обеспечения информационной безопасности» специальности 090305 «Информационная безопасность автоматизированных систем».

В результате выполнения вышеназванных практических работ, предполагается достичь следующих результатов:

**уметь:**

* применять программно-аппаратные средства обеспечения информационной безопасности;
* диагностировать, устранять отказы и обеспечивать работоспособность программно-аппаратных средств обеспечения информационной безопасности;
* оценивать эффективность применяемых программно-аппаратных средств обеспечения информационной безопасности;
* участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации;
* решать частные технические задачи, возникающие при аттестации объектов, помещений, программ, алгоритмов;
* использовать типовые криптографические средства и методы защиты информации, в том числе и электронную цифровую подпись;
* применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности программно-аппаратными средствами;

**знать:**

* методы и формы применения программно-аппаратных средств обеспечения информационной безопасности;
* особенности применения программно-аппаратных средств обеспечения информационной безопасности в операционных системах, компьютерных сетях, базах данных;
* типовые модели управления доступом;
* типовые средства, методы и протоколы идентификации, аутентификации и авторизации;
* типовые средства и методы ведения аудита и обнаружения вторжений;
* типовые средства и методы обеспечения информационной безопасности в локальных и глобальных вычислительных сетях;
* основные понятия криптографии и типовые криптографические методы защиты информации.

|  |  |
| --- | --- |
| **Код** | **Наименование результата обучения** |
| ПК 2.1. | Применять программно-аппаратные средства обеспечения информационной безопасности в автоматизированных системах. |
| ПК 2.2. | Участвовать в эксплуатации программно-аппаратных средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности. |
| ПК 2.3. | Участвовать в мониторинге эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах. |
| ПК 2.4. | Участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации. |
| ПК 2.5. | Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, программ, алгоритмов. |
|  |
| ПК 2.6 | Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности программно-аппаратными средствами. |
| ОК 1. | Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности. |
| ОК 2. | Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество |
| ОК 3. | Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность |
| ОК 4. | Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития |
| ОК 5. | Использовать информационно-коммуникационные технологии в профессиональной деятельности |
| ОК 6. | Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями |
| ОК 7. | Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий |
| ОК 8. | Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации |
| ОК 9. | Ориентироваться в условиях частой смены технологий в профессиональной деятельности |
| ОК 10. | Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей). |
| ОК 11. | Формулировать задачи логического характера и применять средства математической логики для их решения. |
| ОК 12. | Владеть основными методами и средствами разработки программного обеспечения. |
| ОК 13. | Производить инсталляцию и настройку автоматизированных информационных систем, выполнять в автоматизированных информационных системах регламентные работы по обновлению, техническому сопровождению и восстановлению при отказах. |

# Методика и средства выполнения практических работ

Выбор содержания и объем конкретной практической работы обусловлен сложностью учебного материала для усвоения, междисциплинарными связями и учетом значения конкретной практической работы для приобретения обучающимися соответствующих умений и компетенций, предусмотренных ФГОС.

Методика выполнения каждой практической работы определяется моделью соответствующей задачи, решаемой студентом на занятии по заданию преподавателя.

Средством проведения практических работ являются:

* Комплект персональных ЭВМ в компьютерных классах, с выходом в Интернет;

Комплекс программного обеспечения:

* операционная система Windows ХР;
* виртуальная машина VM Virtual Box

Практические работы проводятся в компьютерных классах, расположенных на учебных площадках

Процедурным обеспечением практических работ является:

* настоящие Методические указания

# Этапы выполнения практических работ

Выполнение каждой из практических работ включает в себя пять (5) основных этапов.

1. Постановка задачи практической работы

На первом практическом занятии со студентами проводится общая постановка задач практических работ. Преподаватель может давать необходимые пояснения по методике предстоящих практических работ. После ознакомления с программным комплексом преподаватель проводит постановку задачи конкретного практического занятия. Здесь разъясняется группе студентов содержание и объем работ, предусмотренных конкретной практической работы. Прежде всего, формулируется цели, задачи, основные этапы работы, последовательность и ход решения задачи практической работы. Определяются содержание и форма представления результатов работы. Необходимо пояснить, что каждая практическая работа студента должна быть оформлена в виде отчета о практической работе. Поясняется методика составления и оформления отчета по практической работе. Проводится инструктаж по Охране труда с записью в журнал.

1. Ознакомление студента с содержанием и объемом практической работы.

На этом этапе студент должен тщательно изучить содержание и объем предстоящей практической работы. Если постановка задачи недостаточно ясна, он может обратиться к преподавателю за дополнительными разъяснениями. Затем студент приступает к выполнению задания практической работы.

Порядок выполнения практической работы.

Студент включает ПК и, при необходимости, запускает соответствующую программу. В соответствии с установленной последовательностью этапов работы студент выполняет объем работ, предусмотренных заданием практической работы.

При условии выполнения полного объема практической работы студент проверяет правильность результатов и предъявляет преподавателю результаты работы, выведенные на монитор. В случае замеченных ошибок, студент принимает меры к их исправлению и затем снова предъявляет результаты преподавателю для контроля и приема результатов работы. Если в работе ошибок не содержится, то приступает к составлению и оформлению отчета по практической работе.

1. Регистрация результатов и оформление отчета по практической работе.

По мере того, как выполняются этапы практической работы, студент регистрирует все результаты своей работы в собственном файле или в рабочей тетради для выполнения практических работ. Этот файл в будущем должен быть оформлен как отчет студента по практической работе. Файл должен храниться в папке соответствующего студента. На основе полученных результатов практической работы, составить соответствующий отчет и сдать его преподавателю. Оформление отчета выполнить по следующим правилам. Отчет по практической работе должен содержать следующие обязательные разделы – номер и тема ПР, цель, задание, методика работы, основные этапы практической работы, выводы по выполненной работе.

Отчет по каждой практической работе составляется по следующей обобщенной структуре:

* Наименование идентифицирующих признаков: «Отчет по практической работе №\_\_\_\_\_ по теме (наименование темы)».
* Студента (указываются фамилия и инициалы, курс, группа).
* Цель работы. Формулируется в соответствии с содержанием раздела «Цель работы», соответствующей практической работы.
* Необходимые принадлежности; задание; методика работы. Определяется в соответствии с указанной выше формулировкой и при необходимости уточняется в зависимости от содержания конкретной практической работы.
* Этапы выполнения работы. Приводятся номера и наименования этапов работы, указанные выше. Последовательно по каждому из этапов приводится характеристика содержания выполненных по этапу работ.
* Выводы по работе. К этой части работы студент должен быть особенно внимательным. Формулируются выводы теоретического и практического характера о выполненной практической работе. Обычно выводы излагаются последовательно по каждому из этапов работы (отчета) – 1-2 вывода. Выводы формулируются в сжатой и четкой форме. Вывод должен содержать сжатую мысль о выполненном этапе работы, как результат аналитико-синтетической переработки содержания выполненного этапа. Не следует указывать в выводах содержание и объем выполненных работ.

Текст отчета должен быть изложен лаконично и вместе с тем информативно с соблюдением правил грамматики. В конце отчета может быть указана литература, которую студент применил в практической работе. Библиографические описания литературных источников должны быть оформлены в соответствии с ГОСТ 7.1-84. Правила библиографического описания документации.

1. Заключительная часть практической работы.

После окончания составления отчета студент проверяет его правильность и устраняет ошибки. При условии отсутствия ошибок предъявляет экранный отчет преподавателю. Преподаватель читает текст отчета и принимает его. При условии замеченных ошибок преподаватель указывает студенту на эти ошибки. После этого студент исправляет ошибки и повторно предъявляет отчет преподавателю.

После завершения полного объема работ, исправления ошибок по замечаниям преподавателя, сохраняет отчет, выходит из системы и выключает компьютер.

# Тематика практических занятий и задания к ним

**Практическое занятие 1**

|  |  |
| --- | --- |
| Защита от несанкционированного доступа и сетевых атак | |
|  |  |

1. Цель занятия:

Познакомиться с настройками встроенного брандмауэра и Центра обеспечения безопасности системы Microsoft Windows XP

1. Задания и краткие теоретические сведения:

#### Брандмауэр Windows

Задачу защиты от несанкционированного доступа и *сетевых атак* домашнего компьютера успешно решает *брандмауэр* (или *межсетевой экран*). Он может быть как встроенным в операционную систему (например, *брандмауэр* Windows), так и устанавливаемым отдельно.

**Брандмауэр или межсетевой экран** — это программное или аппаратное обеспечение, которое помогает отражать сетевые атаки вирусов пытающихся попасть на компьютер через Интернет. *Брандмауэр* является одним из наиболее популярных средств защиты.

*Брандмауэр* Windows контролирует входящий и исходящий сетевой трафик подключений. *Брандмауэр* следит за информацией, отправляемой с компьютера, и предотвращает попадание в него ненужных данных из сети. При необходимости *брандмауэр* динамически открывает порты и позволяет компьютеру принимать запрошенный трафик, например сайт, адрес которого Вы набрали в браузере.

**"Порт"** — это сетевой термин, обозначающий точку, через которую сетевой трафик поступает на компьютер. Открываемые порты зависят от типа трафика, который нужно отправить или получить.

Если вы не запрашивали входящий трафик, *брандмауэр* подключения к интернету блокирует его до того, как он достигнет компьютера. В некоторых случаях, таких как работа в сети, установка онлайновых игр или собственного сервера, можно открыть некоторые порты. Это позволит другим пользователям подключаться к компьютеру, но может также снизить уровень безопасности.

Windows XP является одной из самых популярных клиентских операционных систем Windows и содержит в себе встроенный *брандмауэр*. Ранние версии операционных систем Windows (до Windows XP) не содержали встроенный *брандмауэр*. Более поздние версии - Vista и Seven - содержат в себе дополнительные компоненты защиты от несанкционированного доступа и шпионских программ, например Windows Defender.

Встроенные брандмауэры, в отличие от брандмауэров сторонних производителей, отличаются скромной функциональностью, но при этом работают без конфликтов с операционной системой. Еще одним существенным преимуществом является их бесплатность.

|  |
| --- |
| 1. Для того чтобы открыть *брандмауэр* Windows XP выполните следующие действия:Пуск –>Настройка->Панель управления –>*Брандмауэр* Windows 2. На экране появится меню *Брандмауэр* Windows   3_2   1. Вкладка **Общие** позволяет менять режим работы *Брандмауэра* Windows. Можно **Включить брандмауэр** или **Выключить** его. Отключите *Брандмауэр* Windows, а затем вновь включите его. 2. Вкладка **Исключения** позволяет создавать исключения для нужных служб и программ. Если Вы точно уверены в легитимности программы, например, игры, а *брандмауэр* заблокировал ей сетевой доступ, добавьте ее в список исключения. Для этого нажмите на кнопку **Добавить программу**3_k1 и в появившемся списке выберите любое приложение.   3_3    3_4  На рис. в список будет добавлена программа *iTunes* для работы с плеером *Ipod*. После выбора программы нажмите на кнопку ОК.   1. Вкладка **Дополнительно** позволяет включить или отключить *Брандмауэр* Windows для конкретных сетевых подключений, заблокировать или разблокировать *сетевые службы*. Выберите нужное сетевое **Подключение** и нажмите кнопку **Параметры**3_k2   3_5   1. При устранении неполадок, можно воспользоваться **Журналом Безопасности**, для того, чтобы выяснить, когда произошла неполадка и при каких обстоятельствах. Нажмите кнопку **Параметры**3_k2 в блоке **Ведение журнала безопасности**. В появившемся окне произведите настройки, согласно предложенному и нажмите ОК.   3_4v1   1. Блок **Протокол ICMP** служит для приема и отправки сообщений об ошибках и состоянии компьютеров в сети. Так же этот протокол используют некоторые *вредоносные программы*, с периодичностью показывая различные сообщения о якобы произошедших ошибках в операционной системе.   3_6   1. Блок **Параметры по умолчанию** служит для восстановления исходных настроек *Брандмауэра* Windows.   3_7 Центр Обеспечения безопасности Windows Для безопасной работы в сети Интернет, необходимо, что на компьютере постоянно функционировал *межсетевой экран* и антивирусная программа. Кроме того, необходимо чтобы все последние обновления ПО и ОС были установлены на Вашем компьютере. Отслеживание обновления антивирусных баз, программного обеспечения и т.п. является достаточно трудоемкой задачей, и пользователь не всегда компетентен в этих вопросах. Более того, это требует значительных временных затрат. Для решения вышеизложенных задач компания Microsoft включила в состав SP2 и SP3 для Windows XP инструмент под названием **Центр обеспечения безопасности Windows (Windows Security Center)**.   1. Для того чтобы открыть Центр обеспечения безопасности Windows нажмите Пуск –>Настройка->Панель управления –>Центр обеспечения безопасности   3_8   1. Для включения Центра обеспечения безопасности Windows нажмите Пуск –>Настройка->Панель управления –>Администрирование –>Службы.   3_9  В открывшемся окне среди списка служб выберите **Центр обеспечения безопасности**.  3_10  Кликните на службе мышью два раза. В открывшемся окне выберите тип запуска **Авто**. В строке **Состояние** указано состояние службы. Если она остановлена, нажмите на Пуск. После этого **Состояние** изменится на **Работает**. Нажмите на кнопки Применить и ОК и перезагрузите компьютер.  3_11   1. На экране появится меню **Центра обеспечения безопасности Windows.**   3_12  Как видно из рис. **Центр обеспечения безопасности** контролирует три основные компонента для защиты – *брандмауэр*, *антивирус* и систему автоматического обновления. В случае, если компонент будет отключен или параметры одного из компонентов будут настроены не верно, система выдаст предупреждение пользователю (рис.  3_13   1. Основное окно Центра обеспечения безопасности Windows можно разделить на 3 части   3_14   * + **Ресурсы**. С помощью данной части меню можно получить доступ локальным и Интернет-ресурсам: последним сведениям о безопасности и вирусах от Microsoft, проверить наличие последних обновлений от Windows Update, вызвать справку о Центре обеспечения безопасности, получить поддержку по вопросам безопасности и изменить способ оповещения Центром обеспечения безопасности.   + **Компоненты безопасности**. Здесь отображаются параметры настройки трех основных компонентов безопасности: *брандмауэра*, автоматического обновления, антивирусной защиты.   + **Параметры безопасности**. Отсюда можно перейти к настройкам безопасности обозревателя Internet Explorer, автоматического обновления, *брандмауэра*Windows. Рассмотрим меню окна Центр обеспечения безопасности более подробно.  1. В меню **Ресурсы** первые три ссылки предназначены для перехода на соответствующие страницы на сайте Microsoft. Предпоследняя ссылка предназначена для открытия справочной службы Windows на странице "Общие сведения о центре обеспечения безопасности Windows". Последняя ссылка предназначена для открытия окна "Параметры оповещений". Нажмите на последнюю ссылку. Появится окно для настроек параметров системы оповещений.   3_15  Вы можете отключить любое из оповещений Центра обеспечения безопасности. В частности, если установлен *антивирус*, который Центр обеспечения безопасности не обнаруживает, удалите галочку напротив "Защита от вирусов".   1. В меню **Компоненты безопасности** напротив каждого компонента отображается его текущее состояние. На рис. представлены возможные состояния.   3_16  Состояния A-C понятны без комментариев. Состояние D - "Не найдено" - соответствует невозможности определить присутствие соответствующего ПО (например, *антивирус* или *брандмауэр*). Состояние E - "Срок истек" - возможно для антивирусной защиты, когда обновления антивирусных баз устарели. Состояние F - "Не наблюдается" - соответствует отключенному контролю над соответствующим компонентом.   1. Выключите один из компонентов защиты. Состояние этого компоненты примет вид, показанный на рис. (например, если отключить *Брандмауэр* Windows).   3_17   1. Включите отключенный компоненты защиты, на экране появится сообщение о том, что Ваш компонент успешно запущен.   3_18   1. Если один из компонентов не может выполнить нужное действие (например, автоматические обновления устанавливаются по выбору пользователя), статус компонента примет вид, показанный на рис.   3_19   1. Как уже отмечалось ранее, в меню Параметры безопасности расположены кнопки перехода к настройкам безопасности следующих компонентов: обозреватель Internet Explorer, автоматическое обновление, *брандмауэр* Windows,нажав на кнопку **Свойства обозревателя**,вы попадете на закладку **Безопасность** в окне настроек обозревателя Internet Explorer.   3_20   1. Нажав кнопку **Автоматическое обновление**, вы откроете окно настроек "Автоматического обновления".   3_21  Здесь возможны несколько вариантов настройки обновлений:   * + **автоматически**. Операционная система будет в указанное время загружать обновления и самостоятельно устанавливать их. Это рекомендуемый режим.   + **загружать обновления, пользователь сам назначает время установки**. В данном варианте обновления загружаются, выводится соответствующее сообщение. Далее пользователь сам решает, когда их нужно установить.   + **уведомлять, но не загружать и не устанавливать их автоматически**. Операционная система проверяет наличие уведомлений и оповещает пользователя в случае, если таковые имеются. Пользователь вручную загружает их и устанавливает.   + **отключение автоматических обновлений**.   Поставьте автоматическую установку обновлений каждый день в 16:00.   1. Нажав кнопку **Брандмауэр Windows**, вы попадете в окно настроек *брандмауэра* Windows, рассмотренное нами ранее.   3_22 |
| empty |
| empty |
|  |
|  |

**Оформите и сдайте отчет**

7. *Содержание отчета:*

1. Номер и тема лабораторной работы;
2. Цель работы;
3. Необходимое оборудование;
4. Ход выполнения лабораторной работы (этапы);
5. Выводы по выполненной работе.

8. *Контрольные вопросы:*

1. 1. Дайте определение межсетевого экрана?
2. Функции брандмауэра?

**Практическое занятие 2**

## Резервное копирование данных. Работа с подсистемой безопасности

1. Цель занятия:

Получение практических навыков работы с о служебными программами в Windows XP.

***Задание:***

* + Изучить теоретический материал.
  + Проделать описанные по ходу текста команды (сделать скриншоты).
* Выполнить дефрагментацию диска
* Очистку диска
* Архивацию данных
* Восстановление системы
  + Оформить отчет

2.Краткие теоретические сведения и ход выполнения работы

## ****Работа со служебными программами****

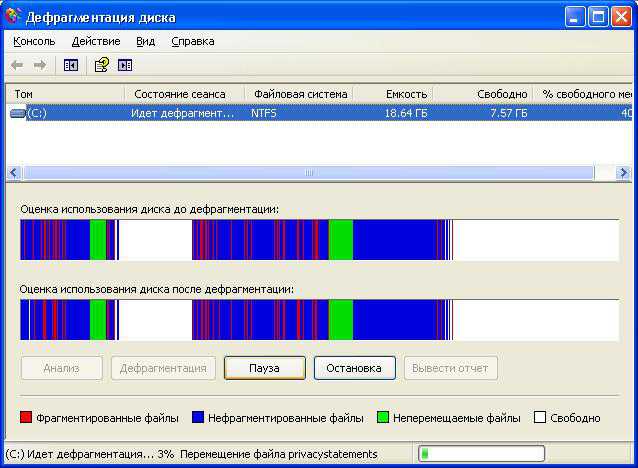
В состав операционных систем обычно входят программы настройки и обслуживания компьютера, а также программы, позволяющие получать информацию о работе компьютера.

1. Восстановление системы
2. Дефрагментация диска
3. Очистка диска
4. Сведения о системе
5. Архивация данных

**Дефрагментация диска**

«Дефрагментация диска» — это системная служебная программа, выполняющая анализ локальных томов с последующим поиском и объединением фрагментированных файлов и папок. Процесс перезаписи частей файла в соседние сектора на жестком диске для ускорения доступа и загрузки. При обновлении файла компьютер стремится сохранить изменения в наибольшей свободной области на жестком диске. Программа анализирует и объединяет фрагментированные файлы и папки таким образом, чтобы каждый файл или папка тома занимали единое непрерывное пространство. В результате чтение и запись файлов и папок выполняется эффективнее.

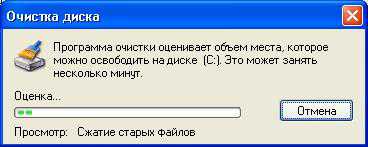
Объединяя отдельные части файлов и папок, программа дефрагментации также объединяет в единое целое свободное место на томе, что делает менее вероятной фрагментацию новых файлов. Процесс объединения фрагментированных файлов и папок называется дефрагментацией.

Отчетное окно дефрагментации

**Очистка диска**

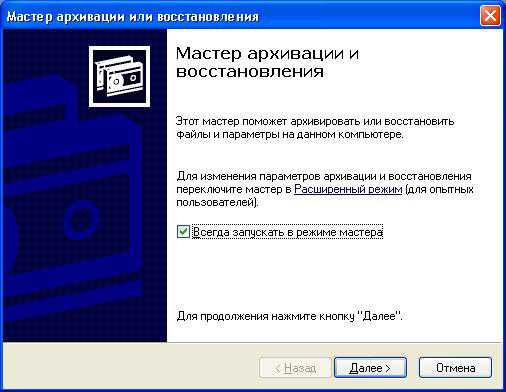
Во время работы за компьютером на жестком диске накапливается большое количество ненужной информации. Это всевозможные временные файлы, скачанные из Интернет веб-страницы, а также не используемые файлы приложений. Чем больше программ вы устанавливаете и запускаете, чем чаще выходите в Интернет - тем больше шансов появления на жестком диске разного бесполезного мусора, который занимает драгоценное свободное место. Для поддержания порядка на своем ПК необходимо периодически устраивать уборку. Операционная система Windows XP предоставляет множество полезных утилит, среди которых есть программа под названием "Очистка диска".

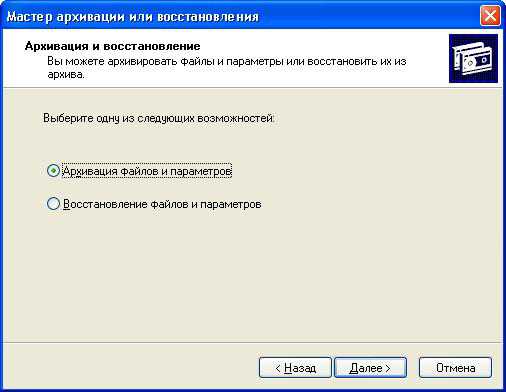
Утилита "Очистка диска" располагается в стандартном наборе служебных программ Windows XP. Для ее запуска активируйте Пуск (Start), Программы (Programs), Стандартные (Accessories), Служебные (System Tools), Очистка диска (Disk Cleanup). Иначе программу можно запустить из командной строки, набрав ее название: cleanmgr. После запуска утилиты на экране появится рабочее окно программы

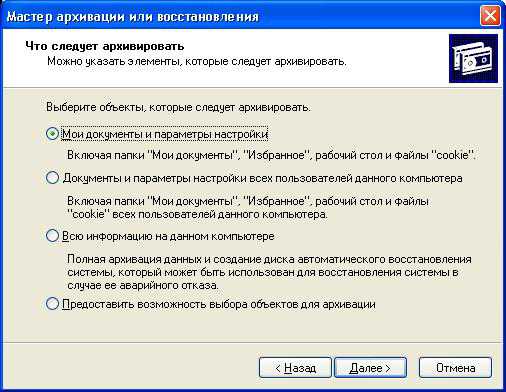


**Архивация данных**

Один из вариантов восстановления системы: создание резервной копию всех файлов и папок своей системы припомощи стандартной утилиты «Архивация данных». Для этого,в «Свойствах» (Properties) жёсткого диска выберите закладку «Сервис »(Tools) и нажмите на кнопку «Выполнить архивацию...» (Backup now...), или (Меню Пуск(Start) —> Программы(Programs) —> Стандартные(Accessories) —> Служебные(System Tools) —> Архивация(Backup)). В открывшемся окне выберите закладку «Архивация» (Backup), и отметьте архивацию всего содержимого данного компьютера.



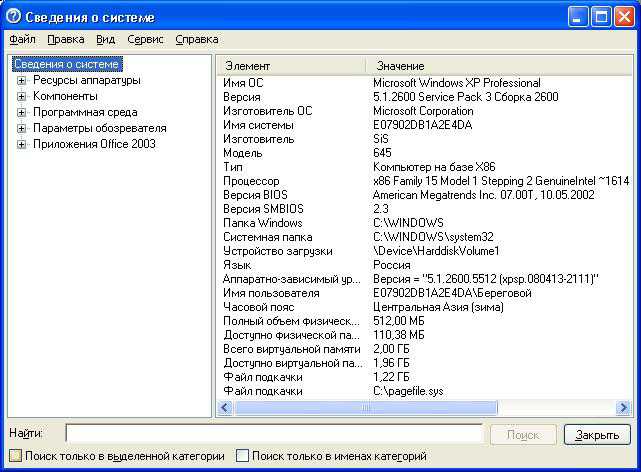
  
Выбор предлагаемой операции

  
Выбираем элементы, которые следует заархивировать

**Сведения о системе**

Программа «Сведения о системе» собирает и отображает данные о конфигурации системы. Такие данные можно получить как для локального компьютера, так и для удаленного компьютера, с которым установлено соединение.

Сюда входит информация о конфигурации оборудования, компонентах компьютера, а также программном обеспечении, в том числе о подписанных и неподписанных драйверах. При устранении неполадок, связанных с конфигурацией системы, сотрудникам службы технической поддержки необходимы определенные данные о компьютере. Программа «Сведения о системе» позволяет быстро собрать необходимые данные

  
Все сведения о системе, находящейся на компьютере

**Восстановление системы**

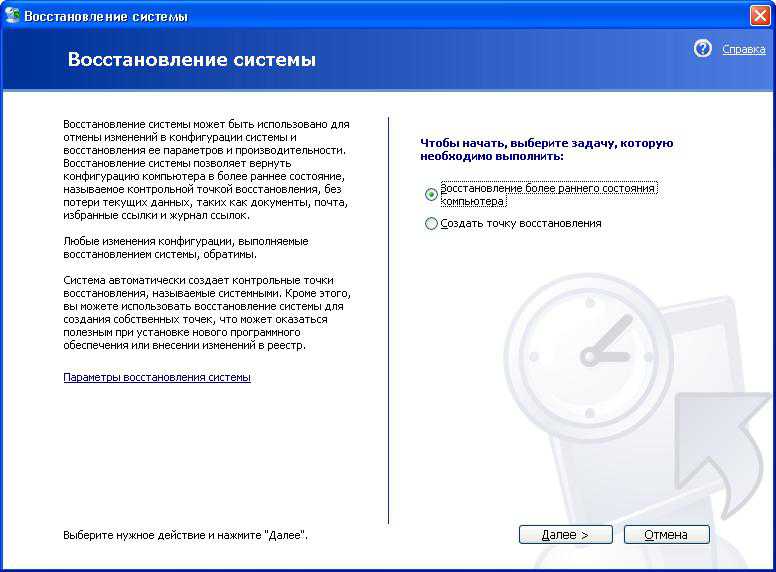
Служба восстановления системы (System Restore Service) Выполняет функции восстановления системы

В состав «Windows XP» входит компонент «System Restore»(Восстановление системы):

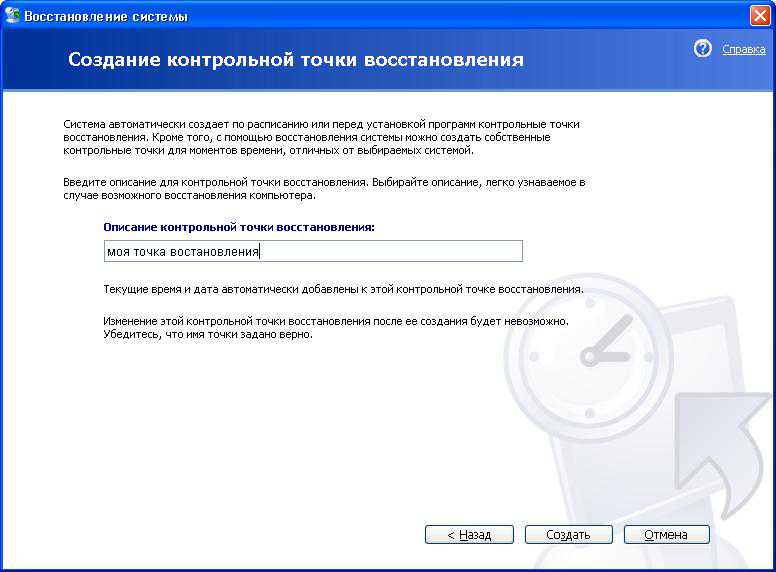
(Меню «Start» (Пуск) —> All Programs (Все программы) —> Accessories (Стандартные) —> System Tools (Служебные) —> System Restore (Восстановление системы)).

С его помощью можно вернуть систему в состояние, предшествовавшее её краху, не прибегая к переустановке операционной системы. «System Restore» восстанавливает реестр, локальные профили, системные базы данных, а также системные файлы, которые она копирует по умолчанию в архив «Restore». При этом нельзя восстановить что-либо одно — восстановлению подлежит либо всё, либо ничего

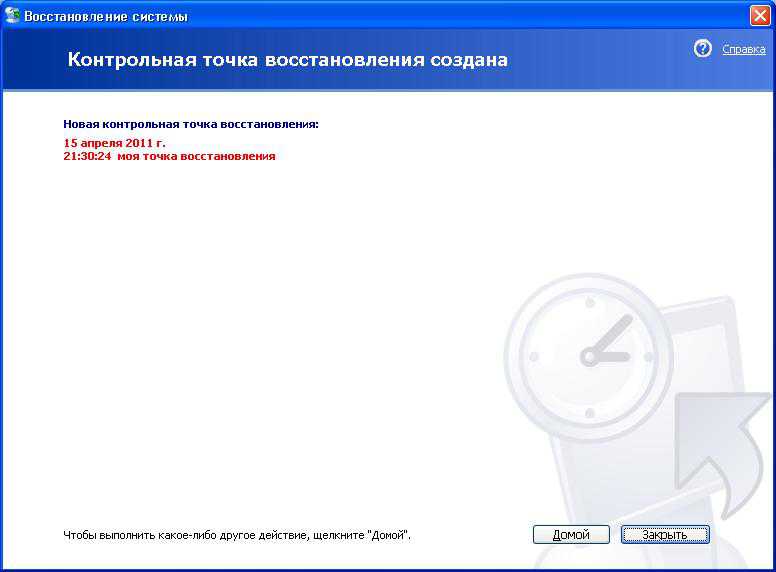
Контрольная точка



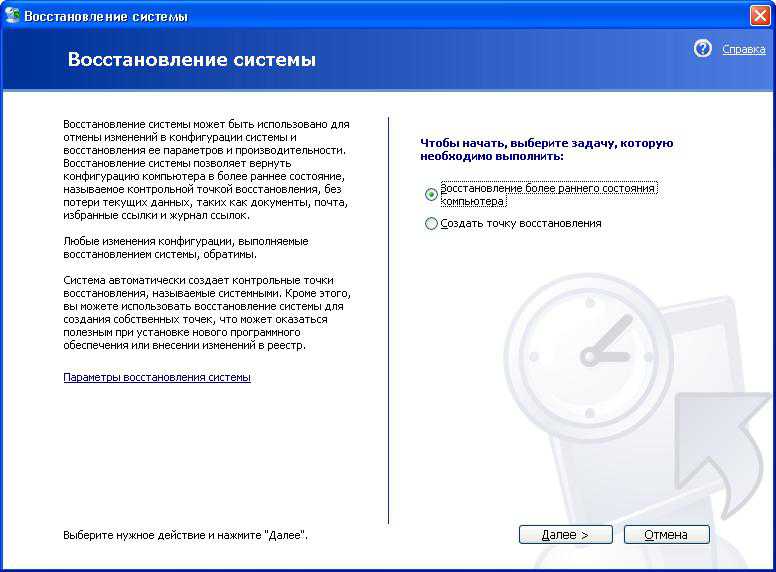
Создание контрольной точки восстановления



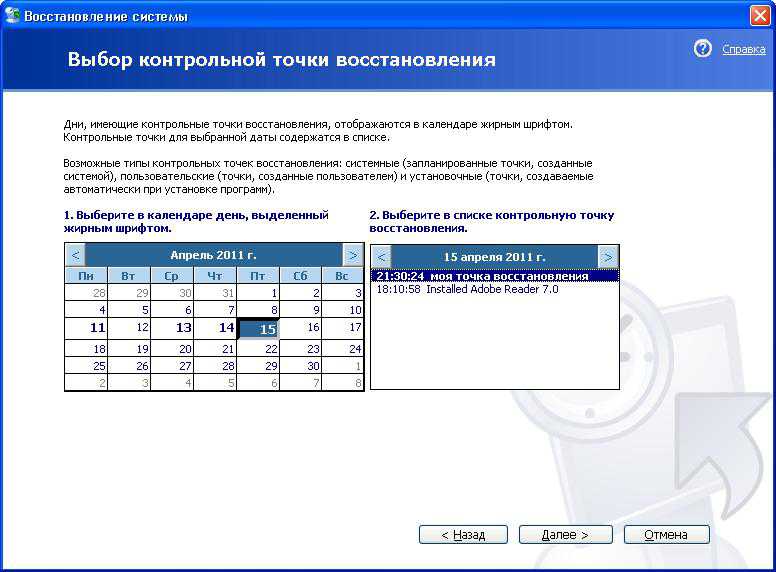
Контрольная точка- это время, когда произошло резервное копирование.



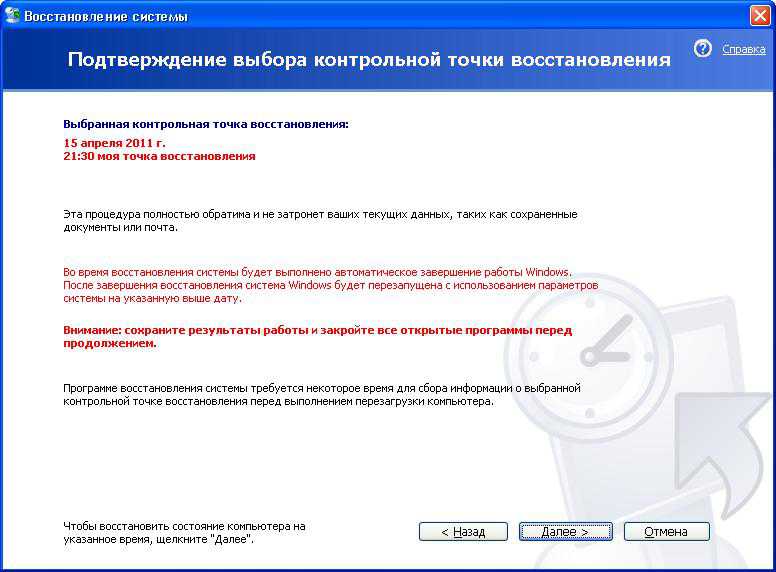
Начинаем восстановление.



Выбираем дату, на момент, который создали нашу точку восстановления.



Подтверждаем выбор контрольной точки восстановления.



3. Содержание отчета

1. Номер и тема практической работы;
2. Цель работы;
3. Необходимые оборудование;
4. Ход выполнения практической работы (этапы);
5. Выводы по выполненной работе.

4.Контрольные вопросы

1. Какие служебные программы входят в состав Windows XP?

2. Какие программы позволяют получать информацию о работе системы?

**Практическое занятие 3**

**Работа с реестром Windows**

**Цель работы:** выявление вредоносных программ с помощью реестра Windows.

**Задание:**

* Изучить и законспектировать теоретический материал.
* Запустить свою виртуальную машину.
* Править реестр с помощью редактора реестра.
* Править реестр с помощью специальных программ сторонних производителей (CCleaner).
* Оформить протокол.

**Теоретическийматериал**

**Реестр операционной системы Windows** - это иерархически построенная 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.

Реестр формируется из различных данных. Чтобы получилось то, что видит пользователь, редактируя реестр, происходит следующее.

Вначале, в процессе установки и настройки Windows, на диске формируются файлы, в которых хранится часть данных относительно конфигурации системы.

Затем, в процессе каждой загрузки системы, а также в процессе каждого входа и выхода каждого из пользователей, формируется некая виртуальная сущность, называемая "реестром" — объект *REGISTRY*\. Данные для формирования "реестра" частично берутся из тех самых файлов (*Software, System* …), частично из информации, собранной ntdetect при загрузке (HKLM\Hardware\Description).

То есть часть данных реестра хранится в файлах, а часть данных формируется в процессе загрузки Windows.

Характеристики *основных разделов* реестра представлены в таблице :

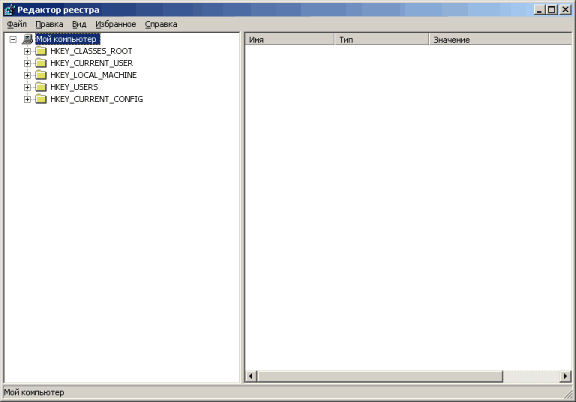
|  |  |
| --- | --- |
|  | |
| **HKEY\_LOCAL\_MACHINE\SAM** | Содержит информацию *SAM* (Security *Access Manager*), хранящуюся в файлах *SAM*,*SAM*.LOG, *SAM*.SAV в папке \%System-root%\System32\Confiq |
| **HKEY\_LOCAL\_MACHINE\SECURITY** | Содержит информацию безопасности в файлах SECURITY.SECURITY.LOG, SECURITY.SAV в папке \%Systemroot%\System32\Confiq |
| **HKEY\_LOCAL\_MACHINE\SYSTEM** | Содержит информацию об аппаратных профилях этого подраздела. Информация хранится в файлахSYSTEM.SYSTEM.*LOG, SYSTEM*.SAV в папке \%Systemroot%\System32\Config |
| **HKEY\_CURRENT\_CONFIG** | Содержит информацию о подразделе System этого улья, которая хранится в файлах SYSTEM.SAV и SYSTEM.ALT в папке \%Systemroot%\System32\Config |
| **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\Confiq |
| **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 \%Systemroot%\Profiles\User name, где User name — имя пользователя, зарегистрированного в системе на данный момент |

Основным средством для просмотра и редактирования записей реестра служит специализированная утилита **"Редактор реестра"**.

Для того чтобы открыть редактор реестра откройте Пуск->Выполнить. В окне введите **regedit**.



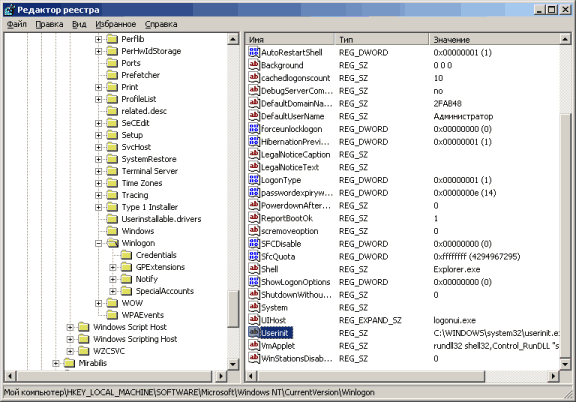
Откроется окно редактора реестра.



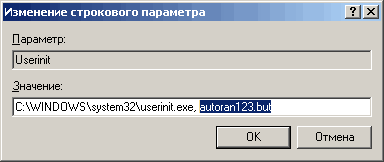
В левой части окна находится дерево ключей реестра, ключи изображены в виде папок. В правой части окна отображаются записи, относящиеся к выбранному ключу. В ключе могут находиться и записи — параметры настройки, и другие ключи — группы параметров настройки.

*Вредоносные программы*, как и любые программы, для работы нуждаются в запуске. Поэтом они часто используют реестр, в частности, его разделы, отвечающие за автоматический запуск программ при загрузке операционной системы.

1. Откройте Редактор реестра.
2. В ветви **HKEY\_LOCAL\_MACHINE** выберите **Software\ Microsoft\WindowsNT\CurrentVersion\Winlogon.**
3. В правой половине окна появится список ключей для данной ветви. Найдите ключ **Userinit** и проверьте его содержимое.



Нормальным значением данного ключа является запись **C:\WINDOWS\system32\userinit.exe**. Наличие в ключе других записей может свидетельствовать о наличии на компьютере вредоносных программ. Для удаления из ключа подозрительной записи щелкните на нем два раза левой кнопкой мыши. После редактирования нажмите ОК.



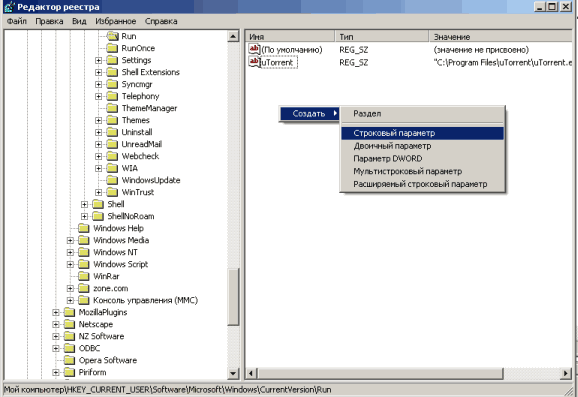
Далее перейдите в папку, где находится подозрительный файл и удалите его вручную. После этого перезагрузите систему. Если после перезагрузки в ключе удаленное значение не появилось снова – система вылечена.

Как уже говорилось выше, любимым местом вредоносных программ являются разделы реестра, отвечающие за автозапуск.

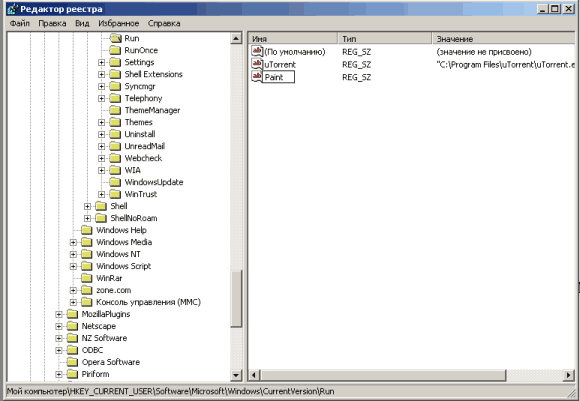
В реестре автозагрузка представлена в нескольких местах:

* + **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**- программы, которые запускаются при входе в систему. Данный раздел отвечает за запуск программ для всех пользователей системы.
  + **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce**- программы, которые запускаются только один раз при входе пользователя в систему. После этого ключи программ автоматически удаляются из данного раздела реестра. Данный раздел отвечает за запуск программ для всех пользователей системы.
  + **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx**- программы, которые запускаются только один раз, когда загружается система. Этот раздел используется при инсталляции программ, например для запуска настроечных модулей. После этого ключи программ автоматически удаляются из данного раздела реестра. Данный раздел отвечает за запуск программ для всех пользователей системы.
  + **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run** - программы, которые запускаются при входе текущего пользователя в систему
  + **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce** - программы, которые запускаются только один раз при входе текущего пользователя в систему. После этого ключи программ автоматически удаляются из данного раздела реестра.
  + **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices** - программы, которые загружаются при старте системы до входа пользователя в Windows.
  + **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce** - программы отсюда загружаются только один раз, когда загружается система.

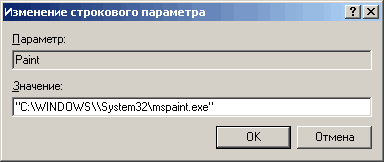
1. Откройте Редактор реестра
2. Откройте следующий раздел HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run
3. В правой части окна вызовите правой кнопкой мыши контекстное меню и выберите Создать->Строковый параметр



1. Задайте имя для создаваемого параметра.



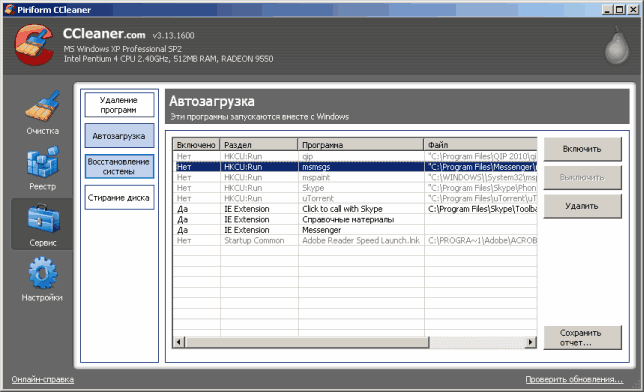
1. Откройте вновь созданный параметр и задайте ему значение в виде пути к исполняемому файлу Paint - **C:\WINDOWS\\System32\mspaint.exe**



1. Нажмите ОК и перезагрузите компьютер. Paint загрузится автоматически после загрузки операционной системы.

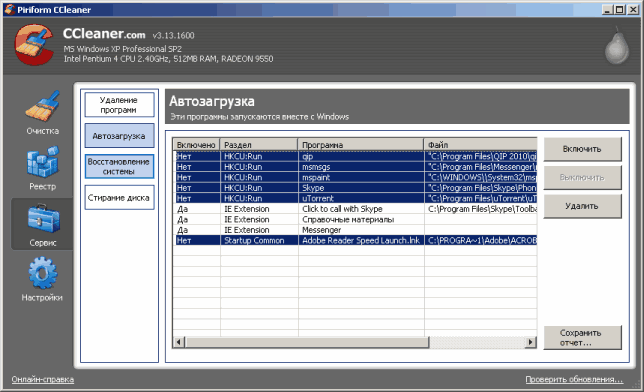
Помимо **regedit** реестр можно править с помощью специальных программ сторонних производителей. Одна из наиболее распространенных программ называется **CCleaner.**

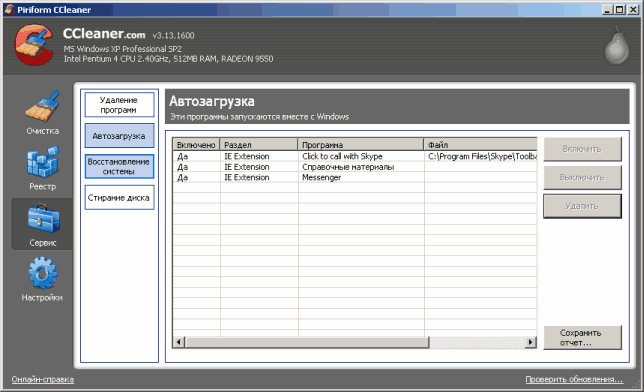
Откройте программу CCleaner. В левом меню выберите **Сервис** и откройте вкладку **Автозагрузка**.



Здесь показаны программы, которые запускаются или запускались вместе с Windows. В столбце "Включено" отображен статус программы на данный момент. Если Вы хотите удалить программу из автозагрузки, выберите ее и нажмите на кнопку Удалить.

Можно выбрать несколько программ сразу.





Здесь также можно включить и выключить программы с помощью соответствующих кнопок на правой панели. Попробуйте самостоятельно добавить программу "Блокнот" в автозагрузку (поместив ярлык в папку Автозагрузки) и удалить ее с помощью CCLeaner.

Оформите отчет, сделайте выводы по работе.

*Содержание отчета*

1. Номер и тема практической работы;
2. Цель работы;
3. Необходимые оборудование;
4. Ход выполнения практической работы (этапы);
5. Выводы по выполненной работе.

*Контрольные вопросы*

1 Определение реестра Windows?

2.Характеристики *основных разделов* реестра?

**Практическое занятие 4**

Работа с файловой системой операционной системы Windows

**Цель:**

Получение практических навыков работы в файловой системе NTFS.

***Задание:***

* + Изучить теоретический материал.
  + Проделать описанные по ходу текста команды (сделать скриншоты).
* Сжать том
* Сжать отдельные файлы и папки с командной строки
* Зашифровать папку в системе EFS.
  + Оформить протокол.

**Теоретический материал**

**Обеспечение безопасности в файловой системе NTFS**

NTFS обеспечивает безопасность на уровне файлов, в отличие от общей безопасности файловой системы FAT. При использовании FAT вы можете запретить или разрешить доступ из сети к части дискового пространства. А с помощью NTFS можно установить доступ к конкретным папкам и файлам. При работе с FAT любой пользователь, расположившийся за компьютером, независимо от способа его регистрации, имеет доступ ко всем вашим файлам.

NTFS является частью сетевой и Windows XP Professional-систем безопасности. Рассмотрим методы обеспечения безопасности и использование системы NTFS в Windows XP Professional. Сначала мы рассмотрим отличительные черты NTFS, затем применение разрешений NTFS, а о конвертации FAT в NTFS на вашем жестком диске.

**Отличительные черты NTFS**

Термины FAT и NTFS являются общими названиями, каждое из которых заключает в себе несколько различных версий этих форматов. Например, существует несколько разновидностей FAT: FAT12, FAT16 и FAT32. Для простоты изложения в этом курсе мы будем их называть просто FAT. С другой стороны, существуют две версии NTFS, а именно версия 4.0 и 5.0.

В этом разделе мы поговорим об отличительных особенностях NTFS. Мы рассмотрим сжатие, шифрование, квоты, а также работу системы в целом. Но сначала давайте разберемся, в чем состоит отличие версии 4.0 файловой системы NTFS от версии 5.0.

**4.0 и 5.0**

Windows XP Professional предлагает самую свежую версию NTFS. В Windows NT использовалась версия 4.0 NTFS. Система Windows XP Professional пользуется версией 5.0, представленной в Windows 2000. Хотя файловые системы обеих версий приспособлены к взаимному чтению и записи, в Windows XP Professional есть ряд новых качеств, которыми Windows NT не может пользоваться при доступе к жесткому диску с NTFS 5.0.

* Reparse points (Точки повторной обработки). Windows NT не может пользоваться этими точками.
* Disk Quotas (Квотирование диска). Windows NT будет игнорировать квоты на дисковое пространство, установленные Windows XP Professional.
* Encryption (Шифрование). Windows NT не может ни читать, ни делать запись в шифрованных файлах.
* Sparse files (Разреженный файлы). Windows NT не может пользоваться разреженными файлами.
* Change journal (Журнал изменений). Windows NT игнорирует журнал изменений.

Эти добавления делают NTFS v.5.0 мощным инструментом со встроенными возможностями управления, который при правильном применении сделает организацию более продуктивной и эффективной.

**Сжатие**

Жесткие диски компьютеров становятся все более вместительными. Это происходит потому, что цены на жесткие диски падают, а потребность в дисковом пространстве для хранения файлов растет. Что бы вы ни сохраняли, будь то приложения или мультимедийные файлы, всегда требуется дополнительное место на диске. Но вместо добавления или обновления жестких дисков Windows XP Professional предлагает механизм, который поможет использовать пространство жесткого диска самым оптимальным образом. Это - сжатие папок.

**Типы сжатия Windows XP Professional**

Windows XP Professional предлагает два типа сжатия папок: NTFS-сжатие и ZIP-сжатие. Выбор метода сжатия будет зависеть от цели, которую вы преследуете, применяя этот метод. Если надо заархивировать данные, то лучше всего применить zip-сжатие. С другой стороны, если файлы, которые вы постоянно используете, захватывают все большее пространство (или есть файлы, которые вы хотите сохранять на жестком диске, но редко ими пользуетесь), то следует обратиться к NTFS-компрессии. Ниже мы рассмотрим особенности этих двух видов сжатия.

ZIP. ZIP-компрессия является популярным форматом сжатия, который годами реализовывался с помощью инструмента от сторонних разработчиков. При ZIP-сжатии несколько файлов архивируются в одной большой ZIP-папке. Для выполнения компрессии или декомпрессии папки пользователь должен явно выполнить это действие. Поэтому такой тип компрессии нельзя применить незаметно. Более того, в связи с тем, что ZIP-файлы выглядят как файлы уникального типа, приложения не могут получить к ним доступ. ZIP-компрессия подходит для тех случаев, когда вы хотите переслать несколько файлов во вложении к письму и надо учитывать размер вложения, или при создании архива данных.

NTFS. Сейчас нас больше интересует NTFS-сжатие. Этот вид компрессии подходит как для папок, так и для файлов, но работает только при NTFS-делении дискового пространства (еще один повод конвертировать диск в NTFS). Кроме того, NTFS-компрессия совершенно "прозрачна" (незаметна) для приложений и пользователей. Когда приложение открывает сжатый файл, то NTFS выполняет декомпрессию только той части файла, которая читается в данный момент, и копирует ее в память. Так как порция данных в памяти находится в сжатом состоянии, то работе системы ничто не мешает. Если данные нужно сохранить в файле, то компьютер должен сжать файл. В NTFS это выполняется достаточно легко. Просто включите компрессию в меню Properties (Свойства) файла или папки.

Размер сжатого файла или папки будет зависеть от типа файла. Например, при сжатии документа Word можно ожидать довольно значительного сжатия - со 120 Кб до 50 Кб. С другой стороны, при сжатии графического файла вы не достигнете такого же уровня компрессии.

Обращаясь к компрессии, вы также должны подумать о том, что она затронет процесс доступа к файлу (хотя и не так сильно, как об этом упоминалось ранее в связи с NTFS-сжатыми файлами). Это особенно заметно, когда сжат весь диск целиком, а не отдельный файл или папка. Компьютеру приходится выполнять задание по сжатию и декомпрессии файла, так что, если таких файлов много, то система будет загружена работой.

**Тома**

Если вы хотите выжать из своего жесткого диска все пространство "до последней капли", то можете подвергнуть сжатию весь том. В зависимости от величины тома, количества файлов, содержащихся в нем, и скорости компьютера процесс может занять несколько минут. По сравнению со сжатием файлов или папок выполнение этого задания занимает больше времени, потому что Windows XP Professional должна пройтись по всем папкам и изменить уровень сжатия, а затем сжать (или наоборот) каждый файл в папке.

Для сжатия полного тома проделайте следующие шаги.

1. Используя Windows Explorer или через меню My Computer (Мой компьютер), найдите том, который надо сжать.
2. Щелкните правой кнопкой мыши на томе и выберите Properties (Свойства).
3. На вкладке General (Общи) отметьте (или снимите отметку, если вы хотите декомпрессировать том) флажок Compress drive to save disk space (Сжать диск для экономии места).
4. Нажмите на ОК.
5. Далее вы увидите диалоговое окно Confirm Attribute Changes (Подтверждение изменения атрибутов). Выберите либо сжатие всего тома, либо корневой папки.

**Файлы и папки**

В зависимости от потребностей и желаний вы можете выбрать только несколько папок или файлов, которые надо компрессировать. Система NTFS позволяет сжимать отдельные папки и файлы. Для выполнения компрессии отдельных файлов и папок проделайте следующие действия.

1. Используя Windows Explorer или через меню My Computer (Мой компьютер), найдите файл или папку, который вы хотите компрессировать.
2. Щелкните правой кнопкой мыши на объекте и выберите Properties (Свойства).
3. На вкладке General (Общие) щелкните на кнопке Advanced (Дополнительно).
4. В диалоговом окне Advanced Attributes (Дополнительные атрибуты) выберите (или очистите, если вы хотите провести декомпрессию раздела) флажок Compress contents to save disk space (Сжать содержимое для экономии места).
5. Щелкните на ОК.
6. В окне свойств щелкните на ОК.
7. При сжатии папки Windows XP Professional спросит, нужно ли сжать только папку или сжать папку со всеми подкаталогами и файлами. Сделайте свой выбор и нажмите на ОК.

Когда вы посмотрите на Windows Explorer, то заметите, что сжатые файлы и папки выглядят несколько иначе. Имена сжатых файлов и папок напечатаны синим шрифтом. Это служит напоминанием о том, какие папки и файлы являются сжатыми, а какие нет.

**COMPACT.EXE**

Как и при работе с другими инструментами Windows XP Professional, вы можете сжимать файлы и папки из командной строки. Командная строка бывает предпочтительнее, если нужно провести пакетное сжатие. Команда COMPACT записывается следующим образом:

Compact /c

COMPACT.EXE содержит несколько ключей, которые помогают модифицировать сжатие. Помимо ключа /c (который означает простое сжатие файла), вы можете воспользоваться ключом /f на случай сбоя в работе компьютера во время проведения сжатия, так как этот ключ позволяет закончить компрессию.

Более того, команда COMPACT пригодится для сжатия файла определенного типа по шаблону. Например, если требуется сжать все Adobe Acrobat файлы, то команда выглядит следующим образом:

Compact /c\*.pdf

Из корневой папки вы можете сжать полный том:

Compact /c/I s:\

В данном случае ключ /I не позволяет посылать сообщения об ошибке, прерывающие процесс сжатия. Полный список ключей команды COMPACT можно получить, введя в командную строку следующее:

Compact /?

**Выполнение**

Компьютеры-клиенты являются подходящим местом для проведения сжатия, так как компрессия и декомпрессия должны проводиться локально. И наоборот, при размещении сжатых файлов на сервере он будет тратить дополнительное время на компрессию и декомпрессию файлов. Это вызовет перебои в работе сервера, которые распространятся по всей сети, так как пакеты не будут передаваться с положенной им скоростью.

С другой стороны, серверы, на которых размещена информация только для чтения (или файлы, которые редко требуются) будут приемлемыми кандидатами для проведения компрессии из-за их редкой посещаемости.

**Квоты на дисковое пространство**

В системе NTFS можно устанавливать квоты для пользователей на пространство жесткого диска. Если свободное пространство на диске ограничено, квоты помогут избежать потери исключительно важных данных, которые просто могут не уместиться на заполненный до отказа диск.

В системе Windows XP Professional квотирование дискового пространства позволяет выполнять следующие действия.

* Уведомлять пользователей о том, что они превысили порог выдачи предупреждения (но еще не израсходовали свою квоту).
* Не допускать запись на диск после того, как пользователи исчерпали свои квоты.

Квотирование диска в Windows XP Professional работает индивидуально в отношении каждого пользователя и каждого тома. Дисковое пространство выделяется каждому пользователю, чье право собственности на файл отслеживается по его идентификатору безопасности (SID). Если пользователь переносит данные из одной папки в другую папку на том же томе, то количество пространства на жестком диске, которое занимает пользователь, не меняется. Если пользователь копирует файлы одной папки в другую в одном и том же томе, то ему придется дважды платить за эти данные, так как они существуют в двух местах одного тома.

Квоты диска "прозрачны" для пользователя. Когда он смотрит на доступное пространство диска, то видит, сколько осталось от выделенной ему части. Как и для полностью заполненного диска, после того как квота исчерпана, на диске нельзя сохранить ни одного файла. Если пользователю требуется больше пространства на жестком диске, то он может проделать следующее.

* Удалить файлы.
* Передать файлы в собственность другого пользователя.
* Попросить администратора об увеличении квоты.

Примечание. Пользователи не могут схитрить, применяя компрессию файлов в надежде получить больше дискового пространства.

При установлении квот следует помнить о двух величинах.

* Порог выдачи предупреждения. Создает точку, при прохождении которой в журнале регистрации событий делается запись о том, что пользователь превысил порог выдачи предупреждения.
* Предел квоты. Устанавливает объем пространства диска, который выделяется для работы данному пользователю. При выходе за эту границу Windows XP Professional может сделать запись в журнале регистрации событий о том, что квота исчерпана, или вы просто можете лишить пользователя возможности сохранять информацию в его томе. Размер квоты можно ограничить 1 Кб, но все же лучше довести его до 2 Мб. Это позволит Windows XP Professional создавать профиль пользователя при входе пользователя в систему.

Например, если вы решите, что квота каждого пользователя должна составлять 1 Гб, и установите порог выдачи предупреждения на 900 Мб, то, когда пользователь израсходует 900 Мб объема, в регистрационном журнале будет сделана запись. Когда пользователь превысит порог в 1 Гб, вы посредством инструмента квотирования можете запретить пользователю получение дополнительного пространства на жестком диске, сделать запись в журнале регистрации, или выполнить и то, и другое.

**Включение квотирования**

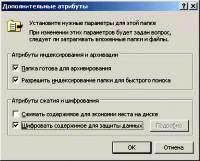
Для установки квот диск должен быть отформатирован под NTFS, и квоты должны устанавливаться лицом, имеющим полномочия администратора. Для включения квот проделайте следующие шаги.

1. Щелкните правой кнопкой мыши на томе, для которого вы хотите установит квоты.
2. Выберите Properties (Свойства).
3. Щелкните на вкладке Quota (Квота) Вы можете ввести следующие настройки.
   * Включить или выключить квотирование диска.
   * Запретить использование диска лицам, израсходовавшим свои квоты.
   * Установить по умолчанию порог выдачи предупреждения и границу квоты для новых пользователей объема.
   * Делать запись в журнале регистации событий о том, что пользователь превысил квоту или порог выдачи предупреждения.
4. В заключение нажмите на ОК, чтобы установить квоты.

**EFS**

Microsoft Windows XP и шифрованная файловая система (EFS) дает возможность хранить данные на диске в зашифрованном формате, однако при переустановке системы или удалении учетной записи пользователя его зашифрованные данные будут безвозвратно утеряны, если не позаботиться о сохранении сертификата и ключей, создании учетной записи агента восстановления*.*

Шифрованная файловая система EFS используется для хранения шифрованных файлов на томах файловой системы NTFS 5.0. После того как файл или папка зашифрованы, с ними можно работать так же, как и с другими файлами или папками, т.е. шифрование прозрачно для пользователя, зашифровавшего файл. Это означает, что перед использованием файл не нужно расшифровывать. Можно, как обычно, открыть файл и изменить его.   
  
Работа с EFS аналогична использованию разрешений для файлов и папок. Задача обоих методов — ограничение доступа к данным. Однако разрешения для файлов и папок не защитят вас, если злоумышленник получит физический доступ к вашим данным, например, подключит ваш жесткий диск к другому компьютеру или загрузится с помощью другой операционной системы, имеющей доступ к томам NTFS. При попытке же открыть или скопировать зашифрованный файл или папку он получит исчерпывающий ответ: «Нет доступа».   
  
Шифрование и расшифровывание файлов выполняется путем установки атрибута файла или папки**Свойства папки или файла > Общие > Другие > Шифровать содержимое для защиты данных** ( рис. 1).



Как только мы зашифруем какую-нибудь папку или файл, Windows создаст для нас сертификат и связанную с ним пару ключей (открытый и секретный ключ), на основании которых будет происходить шифрование и дешифрование файлов. Сертификат — цифровой документ, используемый для проверки подлинности и безопасной передачи данных в общедоступных сетях (Интернет), он связывает открытый ключ с объектом, содержащим соответствующий закрытый ключ.   
  
Наша задача — провести резервное копирование ключей. Это можно сделать с помощью оснастки консоли управления **Сертификаты**. По умолчанию при установке системы она отсутствует, поэтому мы ее добавим, проделав ряд шагов.   
  
Нажмите кнопку **Пуск**, выберите команду **Выполнить**, введите **mmc** и нажмите кнопку **OK**. В меню**Консоль** выберите команду **Добавить или удалить оснастку** и нажмите кнопку **Добавить.** В поле**Оснастка** дважды щелкните **Сертификаты**. Далее установите флажок *Моей учетной записи пользователя*и нажмите кнопку **Готово**. В меню **Консоль > Параметры** установите режим консоли **Пользовательский — огр. доступ, одно окно**, нажмите Применить. Теперь консоль готова к работе ( рис. 2).



Если вы уже зашифровали какой-нибудь файл или папку, то в **Корень консоли > Сертификаты-текущий пользователь > Личные >Сертификаты** вы должны увидеть сертификат, который связан с секретным ключом и который нам нужно экспортировать в файл. Перейдем к нему и вызовем контекстное меню, выберем **Все задачи**, а потом **Экспорт**. На предложение *Экспортировать закрытый ключ вместе с сертификатом ответим* «**Да**», формат файла оставим без изменений, введем пароль, знание которого нам будет нужно для обратной процедуры — импорта сертификата. Полученный файл с расширением .pfx необходимо спрятать, так как любой пользователь, который импортирует данный сертификат для своей учетной записи, получит доступ к вашим файлам, конечно, если узнает или угадает пароль, необходимый для импорта сертификата.   
  
Рекомендуется использовать шифрование на уровне папки. Если шифруется папка, все файлы и подпапки, созданные в зашифрованной директории, автоматически шифруются. Эта процедура позволяет создавать зашифрованные файлы, данные которых никогда не появятся на диске в виде обычного текста — даже временные файлы, создаваемые программами в процессе редактирования, также будут зашифрованы.   
  
При работе с зашифрованными файлами и папками следует учитывать ряд моментов.   
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.   
  
Зашифрованные файлы могут стать расшифрованными, если файл копируется или перемещается на том, не являющийся томом NTFS. 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. Не могут быть зашифрованы файлы с атрибутом Системный и файлы в системном каталоге. Шифрование папки или файла не защищает их от удаления — любой пользователь, имеющий права на удаление, может удалить зашифрованные папки или файлы. По этой причине рекомендуется использование EFS в комбинации с разрешениями системы NTFS. Могут быть зашифрованы или расшифрованы файлы и папки на удаленном компьютере, для которого разрешено удаленное шифрование. Однако если зашифрованный файл открывается по сети, передаваемые при этом по сети данные не будут зашифрованы. Для шифрования данных, передаваемых по сети, должны использоваться другие протоколы, например SSL/TLS или IPSec.   
  
Теперь давайте рассмотрим процесс шифрования в Microsoft Windows XP на более низком уровне, чтобы обезопасить себя от издержек шифрования, а именно — потери данных.   
  
Для начала вспомним две основные криптографические системы. Наиболее простая — шифрование с использованием секретного (симметричного) ключа, т.е. для шифровки и расшифровки данных используется один и тот же ключ. Преимущества: высокая скорость шифрования; недостатки: проблема передачи секретного ключа, а именно возможность его перехвата. Представители: DES, 3DES, DESX, AES. Отличие шифрования с открытым ключом (асимметричное шифрование) заключается в том, что данные шифруются одним ключом, а расшифровываются другим, с помощью одного и того же ключа нельзя осуществить обратное преобразование. Эта технология шифрования предполагает, что каждый пользователь имеет в своем распоряжении пару ключей — открытый ключ (public key) и личный или закрытый ключ (private key). Таким образом, свободно распространяя открытый ключ, вы предоставляете другим пользователям возможность шифровать свои сообщения, направленные вам, которые сможете расшифровать только вы. Если открытый ключ и попадет в «плохие руки», то он не даст возможности определить секретный ключ и расшифровать данные. Отсюда и основное преимущество систем с открытым ключом: не нужно передавать секретный ключ, однако есть и недостаток — низкая скорость шифрования. Представители: RSA, алгоритм Эль-Гамаля, алгоритм Диффи-Хелмана.   
  
В EFS для шифрования используются все преимущества вышеперечисленных систем. Данные шифруются с помощью симметричного алгоритма с применением ключа шифрования файла (File Encryption Key, FEK). FEK — сгенерированный EFS случайным образом ключ. На следующем этапе FEK шифруется с помощью открытого ключа пользователя и сохраняется в пределах атрибута, называемого полем расшифровки данных (Data Decryption Field, DDF) непосредственно внутри самого файла. Кроме того, EFS шифрует FEK, используя открытый ключ агента восстановления, и помещает его в атрибут Data Recovery Field — DRF. DRF может содержать данные для множества агентов восстановления.   
  
Агент восстановления данных (Data Recovery Agent, DRA) — пользователь, который имеет доступ ко всем зашифрованным данным других пользователей. Это актуально в случае утраты пользователями ключей или других непредвиденных ситуациях. Агентом восстановления данных назначается обычно администратор. Для создания агента восстановления нужно сначала создать сертификат восстановления данных и определить политику восстановления, а затем назначить одного из пользователей таким агентом. Политика восстановления играет важную роль в системе шифрования Windows XP, она определяет агентов восстановления, а их отсутствие или удаление политики вообще запрещает использование пользователями шифрования.   
  
Чтобы настроить политику восстановления, необходимо запустить консоль **Пуск > Настройка > Панель управления > Администрирование >Локальная политика безопасности**, в которой перейти к пункту**Политики открытого ключа > Файловые системы EFS** ( рис. 3). По умолчанию политика восстановления такова, что права агента восстановления принадлежат администратору. Если сертификат агента восстановления по умолчанию удален, а другого агента в политике нет, компьютер будет иметь пустую политику восстановления. Пустая политика восстановления означает, что агента восстановления не существует. Это отключает EFS, следовательно, запрещает пользователям шифровать файлы на этом компьютере. Мы можем создать учетную запись администратора с помощью агента восстановления и провести для надежности операцию экспорта его ключа, а можем создать новый сертификат восстановления и назначить другого пользователя в качестве агента.



Чтобы создать сертификат восстановления, необходимо воспользоваться утилитой командной строки cipher, которая предназначена для управления шифрованием (подробную информацию об этой утилите можно прочитать в справке операционной системы). Нужно войти в систему с полномочиями администратора, ввести в командной строке:   
**cipher /R: имя файла сертификата**  
  
Далее введите пароль, который понадобится в случае импортирования. Файлы сертификата имеют расширение .**pfx** (содержит сертификат и связанный с ним открытый и закрытый ключ) или .**cer**(сертификат и связанный с ним открытый ключ) и указанное вами имя. Эти файлы позволяют любому пользователю системы стать агентом восстановления, поэтому наша задача — сохранить их в надежном месте, а главное, не забыть добавить сертификат агента восстановления в политику открытого ключа.   
  
Чтобы создать этого самого агента, необходимо проделать следующие шаги: войти в систему под учетной записью, которая должна стать агентом восстановления данных; в консоли **Сертификаты**перейдите в раздел **Сертификаты - Текущий пользователь > Личные > Сертификаты**; далее **Действие >Все задачи > Импорт для запуска мастера импорта сертификатов**, затем проведите импорт сертификата восстановления. Причем учтите: чтобы расшифровывать файлы, необходимо импортировать закрытый ключ, поэтому при выборе файла для импорта используйте файл **.pfx**.   
  
Часто недостатком шифрования с помощью EFS считают невозможность транспортировки зашифрованных данных, т.е. записать данные на «болванку», не потеряв их секретность, не удастся. Но это не совсем так — действительно, просто записать их нельзя, но можно воспользоваться программой архивации для Windows XP — **NTBackup**, в этом случае данные будут скопированы на указанный носитель без дешифрования, причем носитель может не поддерживать NTFS 5.0. После восстановления зашифрованные данные остаются в зашифрованном виде.   
  
И еще несколько советов. Всегда включайте шифрование для папок, так как это защитит временные файлы. Экспортируйте закрытый ключ учетной записи агента восстановления, сохраните его в надежном месте, после чего удалите с компьютера. При смене политик восстановления не спешите удалять старые сертификаты, пока не будете уверены, что все файлы, зашифрованные с помощью этих сертификатов, не будут обновлены.

Когда вы стираете файл с жесткого диска, на самом деле вы не удаляете его, а просто сообщаете компьютеру о том, что часть диска, на которой находится файл, теперь доступна для использования. Файл исчезает только тогда, когда вы что-то записываете поверх него. Однако пока этого не произошло, файл продолжает существовать на диске и может быть легко восстановлен.

Использование файловой системы EFS (Encrypting File System - шифрованная файловая система) в Windows XP Professional позволяет защитить данные. При применении EFS сохраняемые на диске файлы шифруются, и их нельзя прочитать, пока к ним не будет корректного доступа.

Примечание. EFS можно применять только в NTFS-томе.

EFS представляет собой трехступенчатый процесс.

1. Для шифрования и расшифровки данных применяется пара ключей: открытый/закрытый и ключ шифрования файлов. Когда пользователь в первый раз шифрует файл, EFS создает ключ шифрования файлов (FEK). FEK шифруется с помощью открытого ключа пользователя и в зашифрованном состоянии хранится вместе с файлом.
2. Существует несколько способов пометить файл, предназначенный для шифрования:
   * вручную настроить EFS путем изменения расширенных свойств файла;
   * сохранить файл в папке, предназначенной для шифрования;
   * использовать команду CIPHER.EXE в командной строке.
3. Для расшифровки файла пользователь должен открыть его и удалить шифрование, используя команду CIPHER.EXE. При дешифровке файла система EFS сначала декодирует FEK с помощью закрытого ключа пользователя, а затем расшифровывает данные, используя FEK.

**EFS в Windows XP Professional**

Система EFS известна со времени появления Windows 2000, но Windows XP Professional добавила в нее новые свойства, повысив ее функциональность. Эти новые качества включают в себя следующее.

* Возможность шифровать файлы в режиме офлайн.
* Наличие агентов восстановления данных (Data Recovery Agents).
* Возможность использования алгоритма 3DES (triple-DES) вместо DESX (Data Encryption Standard XORed).
* Дискета сброса пароля может быть использована для переустановки пароля пользователя.
* Зашифрованные файлы можно хранить в веб-папках.

В Windows XP Professional система EFS включается по умолчанию. Однако тут надо соблюсти некоторые предварительные условия. Во-первых, пользователи должны иметь открытый и закрытый ключи и открытый сертификат шифрования. Однако EFS может использовать самоподписываемые сертификаты, которым для работы не нужна подпись администратора.

**Шифрование и расшифровка**

При работе с EFS лучше всего зашифровывать целую папку, а не отдельные файлы. Это ускоряет процесс и делает его более эффективным. Вместо шифрования разрозненных файлов вы сможете одним движением руки создать защиту множества файлов. Более того, при шифровании папки целиком все запасные копии файлов тоже шифруются.

Примечание. Разумеется, будут зашифрованы только те копии, которые хранятся в зашифрованной папке.

Для шифрования файла или папки проделайте следующие шаги.

1. В My Computer (Мой компьютер) выберите файл или папку, которые нужно зашифровать.
2. Щелкните правой кнопкой мыши на файле или папке и выберите Properties (Свойства).
3. На вкладке General (Общие) щелкните на кнопке Advanced (Дополнительно).
4. Отметьте флажок Encrypt contents to secure data (Шифровать содержимое для защиты данных) и затем нажмите ОК.

Если вы решили зашифровать только файл, то Windows XP Professional выдаст запрос, хотите ли вы зашифровать один этот файл или всю папку. Как упоминалось ранее, лучше зашифровать целую папку, но, тем не менее, можно зашифровать и отдельный файл. После шифрования имя файла будет показано зеленым цветом.

Примечание. Сжатые файлы представлены шрифтом синего цвета. Файл не может быть одновременно зашифрованным и сжатым.

Дешифрование файлов и папок проводится аналогичным образом. В данном случае вам потребуется очистить флажок Encrypt contents to secure data.

**Оптимизация NTFS**

Хотя Windows XP Professional и NTFS включают в себя множество функций, облегчающих хранение и управление файлами, за всю эту легкость приходится платить. Если вы хотите повысить эффективность работы своего жесткого диска, то проверьте ряд элементов.

**Размер кластеров**

Решение конвертировать свой жесткий диск в NTFS требует некоторого планирования (о чем мы будем говорить в разделе "Конвертирование/Форматирование жесткого диска с помощью NTFS"). Необходимо заранее обдумать величину кластеров. Если все файлы будут преимущественно одного размера, меньше размера кластера по умолчанию, равного 4Кб, то, возможно, вы сочтете нужным изменить размер кластеров по умолчанию при конвертировании жесткого диска.

Представьте себе, что жесткий диск составлен из миллиардов крошечных блоков. Это - кластеры. Допустим, что каждый кластер содержит 4 Кб информации. Если файл вмещает в себя только 3 Кб данных, то в каждом кластере будет напрасно расходоваться пространство. Конечно, это только 1 Кб, но в сумме получится много. В таблице содержатся размеры кластеров по умолчанию для NTFS-дисков различного размера.

С другой стороны, уменьшение размера кластеров приводит к увеличению фрагментации. Этот означает, что после удаления информации из блока кластеров, если вы хотите снова им воспользоваться для записи файла, то он должен быть равен (или меньше) файла, ранее располагавшегося в этом блоке. При добавлении новых файлов, записываемых на неиспользованные кластеры, начинает проявляться фрагментация, поскольку, хотя на диске и есть свободное пространство, оно разбито на такие мелкие кусочки, что им нельзя воспользоваться. Если вы сохраняете большие файлы, или они имеют тенденцию к росту, лучше по умолчанию установить величину кластеров, равную 16 - 32 Кб.

|  |  |
| --- | --- |
| Таблица 1 Размер NTFS кластеров по умолчанию | |
| **Размер жесткого диска** | **Размер кластера** |
| 512 Мб или меньше | 512 б |
| 513 Мб - 1 Гб | 1 024 б |
| 1 Гб - 2 Гб | 2 048 б |
| 2 Гб и больше | 4 069 б |

О размере кластеров следует подумать и при преобразовании томов из формата FAT в NTFS в Windows 2000 и в более ранних версиях. Это связано с тем, что по умолчанию размер кластеров составляет 512 байтов, что, естественно, ведет к фрагментации. Лучше всего скопировать все содержимое жесткого диска, переформатировать его, указать нужный размер кластеров, и затем вернуть все данные на том.

Если жесткий диск стал фрагментированным, то было бы хорошо провести дефрагментацию с помощью инструмента, предоставляемого Windows XP Professional.

**Организация**

Файловая система. Хотя NTFS поддерживает папки с огромным количеством файлов, будет неразумно складывать все документы в одну папку. Это особенно актуально, если вы часто читаете и удаляете файлы из этой папки. При каждом открывании папки Windows XP Professional тратит время на поиск имени и статистики каждого файла. Наилучшим решением в этом случае будет создание подкаталогов всегда, когда это возможно, чтобы свести количество считываний к минимуму.

Индексация. Если пользователи регулярно просматривают жесткие диски в поисках файлов и папок, то вам следует подключить службу индексации - Indexing Service. Это в значительной степени сократит время поиска. Indexing Service также помогает сократить время поиска внутри документа.

При подключенной службе индексации NTFS заносит все изменения файловой системы в журнал изменений. Необходимость проводить обновления журнала изменений неизбежно вызывает замедление в работе системы, но эти издержки полностью покрываются за счет конечного повышения скорости поиска файлов и папок.

**Разрешения NTFS**

NTFS обеспечивает такой уровень детализации отбора, что пропускает только тех, кому вы хотите предоставить доступ, и отсеивает всех остальных.

Новым качеством в Windows XP Professional является простое совместное использование файла (simple file sharing). Эта функция включается при первичной инсталляции Windows XP Professional или при совместном использовании тома или папки. Чтобы подключить большее количество инструментов управления доступами пользователей, простое совместное использование файла надо отключить.

Вы можете задать вопрос, зачем же нужно простое совместное использование файлов, если эту функцию надо отключать. Только затем, чтобы облегчить процесс совместного использования файлов и папок. При включенном простом совместном использование файлов нет и множества конфигураций для осуществления доступа пользователей к файлам, принтерам и т. д. Этим обеспечивается легкий способ совместного использования файлов. Однако если вы хотите управлять тем, кто именно может получать право доступа к файлам, то простое совместное использование файлов следует отключить. Для этого проделайте следующие шаги.

1. Выберите Start\My Computer (Пуск\Мой компьютер), затем щелкните на Tools (Сервис) и выберите Folder Options (Свойства папки) .
2. В диалоговом окне Folder Options щелкните на вкладке View (Просмотр).
3. Просмотрите до конца перечень настроек в окне Advanced Settings (Дополнительные параметры) и либо установите, либо очистите флажок Use simple file sharing (Использовать простой общий доступ к файлам).
4. Нажмите на ОК.

Примечание. Само по себе отключение простого совместного использования файла не позволит вам устанавливать разрешения для файлов. Вы должны также разместить все свои файлы и папки в NTFS-томе или разделе.

**Разрешения для папок и томов**

Разрешения осуществляют контроль над тем, что пользователь или группа могут делать с объектом в сети или на своем локальном компьютере. Разрешения поддерживаются только при отключении простого совместного использования файла и на жестком диске в формате NTFS. В [таблице 2](http://helpwinxp.narod.ru/helpwinxp-10.html#table.10.2) перечислены разрешения, назначаемые для папок, а в [таблице 3](http://helpwinxp.narod.ru/helpwinxp-10.html#table.10.3) - для файлов.

|  |  |  |
| --- | --- | --- |
| Таблица 2. Разрешения папок | | |
| **Разрешение** | | **Разрешает или запрещает это действие** |
| Change Permissions | | Изменение разрешений папки. |
| Create Files | | Создание новых файлов в данной папке. |
| Create Folders | | Создание подкаталогов в данной папке. |
| Delete | | Удаление папки. |
| Delete subfolders and files | | Удаление файлов и подкаталогов, даже если у вас нет разрешения на их создание. |
| List Folder | | Просмотр содержимого папки. |
| Read Attributes | | Просмотр атрибутов папки. |
| Read Permissions | | Просмотр разрешений папки. |
| Take Ownership | | Присвоение себе прав другого пользователя на владение папкой. |
| Traverse Folder | | Открытие папки для просмотра подкаталогов и родительских папок. |
| Write Attributes | | Внесение изменений в свойства папки. |
| Таблица 3. Разрешения файла | | | |
| **Разрешение** | **Разрешает или запрещает это действие** | | |
| Append Data | Добавление информации в конец файла без изменения существующей информации. | | |
| Change Permissions | Внесение изменений в разрешения файла. | | |
| Delete | Удаление файла. | | |
| Execute File | Запуск программы, содержащейся в файле. | | |
| Read Attributes | Просмотр атрибутов файла. | | |
| Read Data | Просмотр содержимого файла. | | |
| Read Permissions | Просмотр разрешений файла. | | |
| Take Ownership | Присвоение себе прав собственности на этот файл у другого владельца. | | |
| Write Attributes | Изменение атрибутов файла. | | |
| Write Data | Изменение содержания файла. | | |

**Создание и управление разрешениями**

Создавая разрешения для отдельных файлов, папок и NTFS-томов, вы можете воспользоваться гораздо большим количеством опций безопасности, чем предлагает файловая система FAT. Вкладка Properties (Свойства) выбранной папки или тома включает в себя вкладку Security (Безопасность). Щелкнув на ней, вы можете увидеть ряд опций для управления доступом.

Для настройки разрешений данной папки или тома проделайте следующие шаги.

1. Укажите том или папку, для которых вы собираетесь устанавливать разрешения.
2. Щелкните правой кнопкой мыши на нем и выберите Properties (Свойства).
3. Выберите вкладку Security (Безопасность).

Примечание. Если NTFS-том находится в совместном использовании, то необходимо устанавливать разрешения посредством вкладки Security (Безопасность), а не используя для этого кнопку Permissions (Разрешения) на вкладке Sharing (Общий доступ).

В появившемся окне свойств вы увидите два окна. В верхнем окне содержится список пользователей и групп В нижнем - список разрешений для пользователя, которые можно устанавливать и регулировать. Опять же, эта вкладка доступна только для томов в формате NTFS.

Оформите отчет, сделайте выводы по работе.

3. Содержание отчета

1. Номер и тема практической работы;
2. Цель работы;
3. Необходимые оборудование;
4. Ход выполнения практической работы (этапы);
5. Выводы по выполненной работе.

4.Контрольные вопросы

* 1. Назовите отличительные черты NTFS?
* Для чего необходимо использование файловой системы EFS?
* Назовите основные виды разрешений в NTFS?

**Практическое занятие 5.**

Настройка BIOS

***Цель работы:***

Знакомство с основными настройками BIOS. Получение практических навыков оптимизации работы BIOS.

***Задание:***

·     Изучить и законспектировать теоретический материал.

·     Войти в BIOS Setup.

·     Задать пароль на вход в BIOS.

·     Изменить порядок загрузки.

·     Рассмотреть все возможности настройки BIOS.

·     Сделать файл справки по настройкам BIOS

**Теоретический материал**

***BIOS***

*Общая информация*

Важным элементом системной платы является *BIOS* (*Basic Input/Output System* ‑ базовая система ввода-вывода). Так называют аппаратно встроенное в компьютер программное обеспечение, которое доступно без обращения к диску. В микросхеме *BIOS* содержится программный код, необходимый для управления клавиатурой, видеокартой, дисками, портами и другими компонентами. Обычно *BIOS* размещается в микросхеме *ПЗУ* (*ROM, Read Only Memory*), расположенной на материнской плате компьютера (этот узел часто называют *ROM BIOS*). Такая технология позволяет обеспечить постоянную доступность *BIOS* независимо от работоспособности внешних по отношению к материнской плате компонентов (например, загрузочных дисков). Поскольку доступ к *RAM* (оперативной памяти) осуществляется значительно быстрее, чем к *ROM*, многие изготовители предусматривают при включении питания автоматическое копирование *BIOS* из *ROM* в оперативную память. Задействованная при этом область памяти называется теневой (*Shadow RAM*). В микросхемах *BIOS* используют различные типы памяти для хранения программного кода. *PROM* (*Programmable Read-Only Memory*) ‑ это тип памяти, данные в которую могут быть записаны только однократно. Отличие*PROM* от *ROM* в том, что *PROM* изначально производятся «чистыми», в то время как в *ROM* данные заносятся в процессе производства. А для записи данных в микросхемы *PROM* применяют устройства, называемые программаторами. *EPROM* (*Erasable Programmable Read-Only Memory* ‑ стираемое программируемое *ПЗУ*) ‑ специальный тип *PROM*, который может очищаться (и записываться) с использованием ультрафиолетовых лучей. Память типа *EEPROM* похожа на *EPROM*, но операции стирания-записи производятся электрическими сигналами.

В настоящее время большинство современных материнских плат комплектуется микросхемами *FLASH BIOS*, код в которых может перезаписываться при помощи специальной программы. Такой подход облегчает модернизацию *BIOS* при появлении новых компонентов, которым нужно обеспечить поддержку (например, новейших типов микросхем оперативной памяти). Так как львиная доля программного кода *BIOS* стандартизирована, то есть является одинаковой и обязательной для всех компьютеров *PC*, в принципе, менять его нет особой необходимости. Перезапись *BIOS* ‑ крайне ответственная и весьма непростая задача. Браться за нее следует только в самом крайнем случае ‑ если проблема не решается никакими другими способами. При этом надо ясно отдавать себе отчет в необходимости и последствиях каждого шага этой операции. Современные типы *BIOS*, выполненные по технологии *Plug- and-Play*, называют *PnP BIOS*, при этом поддержка такой архитектуры обеспечивается только микросхемами *Flash ROM*. Вообще полная поддержка технологии *Plug-and-Play* со стороны *Windows* возможна только в случае применения *PnP BIOS*. Обычно это обстоятельство служит веским основанием для принятия решения о перезаписи *BIOS*. Кроме вышеуказанного, в новых версиях *BIOS* часто исправляются мелкие ошибки и недоработки. Новые версии обычно содержат и новые возможности.

*Назначение и функции BIOS*

В современных компьютерах BIOS выполняет несколько функций:

* Запуск компьютера и процедура самотестирования (*Power-On Self Test* ‑ *POST*). Программа, расположенная в микросхеме *BIOS*, загружается первой после включения питания компьютера. Она детектирует и проверяет установленное оборудование, настраивает его и готовит к работе. Если обнаруживается неисправность оборудования, процедура *POST* останавливается с выводом соответствующего сообщения или звукового сигнала. Настройка параметров системы с помощью программы *BIOS Setup*. Во время процедуры *POST* оборудование определяется в соответствии с параметрами *BIOS*, хранящимися в специальной *CMOS-памяти.* Изменяя эти параметры, пользователь может настроить работу отдельных устройств и системы в целом по своим потребностям. Редактируются они в специальной программе, которую также называют *BIOS Setup* или *CMOS Setup*.
* Поддержка функций ввода-вывода с помощью программных прерываний *BIOS*. В составе системной *BIOS* есть встроенные функции для работы с клавиатурой, видеоадаптером, дисководами, жесткими дисками, портами ввода-вывода и др. Эти функции широко используются в операционных системах, подобных *MS-DOS*, и практически не применяются в современных версиях *Windows*.

*Процедура POST*

Первое устройство, которое запускается после нажатия кнопки включения компьютера ‑ блок питания. Если все питающие напряжения окажутся в норме, вступает в работу центральный процессор, который считывает содержимое микросхемы *BIOS* и начинает выполнять записанную в ней процедуру самотестирования, или *POST*. *POST* решает несколько основных задач:

1)    Инициализирует и настраивает основные системные компоненты: процессор, оперативную память, чипсет и видеоадаптер.

2)    Проверяет контрольную сумму *CMOS* и состояние батареи. Если контрольная сумма *CMOS* ошибочная, будут загружены значения по умолчанию.

3)    Тестирует процессор и оперативную память. Результаты обычно выводятся на экран.

4)    Инициализирует и настраивает периферийные устройства: клавиатуру, мышь, дисководы, жесткие диски и др. Сведения об обнаруженных накопителях также выводятся на экран.

5)    Распределяет ресурсы между устройствами и выводит таблицу с обнаруженными устройствами и назначенными для них ресурсами.

6)    Ищет и инициализирует устройства с собственной *BIOS*.

7)    Вызывает загрузчик операционной системы.

После того, как успешно завершилась процедура *POST*, запускается поиск загрузочного сектора, который может находиться на жестком диске или сменном носителе. Порядок опроса устройств устанавливается с помощью параметров *BIOS: First Boot Device, Second Boot Device, Third Boot Device*.

*Основные разработчики BIOS*

Раньше ‑ примерно в начале-середине 90-х годов прошлого века ‑ можно было встретить версии *BIOS*, целиком разработанные производителями системных (материнских) плат или ноутбуков ‑ например *Intel*, *IBM*, *Compaq*, *Toshiba*, *Dell*. В результате эволюции компьютерного оборудования все лучшие наработки были воплощены в продукции таких брэндов, как *Award*, *AMI*, *Phoenix*, которые сейчас являются основными производителями программного кода *BIOS*. Поэтому версии*BIOS* различаются незначительно. Рассмотрим подробнее каждого производителя базовой версии *BIOS*.

*AwardBIOS* компании *Award Software (phoenix.com)* ‑ наиболее известный производитель *BIOS*. В свое время очень популярной была версия 4.51, позже появилась версия 6.0, которая установлена на львиной доле современных материнских плат. В далеком 1998 году фирма *Award* была куплена компанией *Phoenix*, однако все последующие разработки выходят под торговой маркой *AwardBIOS* или *Phoenix-Award BIOS*.

*AMIBIOS* компании *American Megatrends (ami.com)*. В настоящее время данный производитель занимает второе место по популярности среди производителей материнских плат. В основном данную версию BIOS на свою продукцию устанавливают такие компании, как *ASUStec*, *ASRock*, *MSI*.

*PhoenixBIOS* компании *Phoenix Technologies (phoenix.com)* чаще всего встречается на ноутбуках.

*Версии BIOS*

Для того, чтобы использовать все возможности чипсета, установленного на материнской плате, а также особенности работы со всем периферийным оборудованием (жесткие диски, карты расширения и пр.), необходима своя версия *BIOS*. Но для того, чтобы создать необходимую версию, нужно обеспечить полный цикл разработки программы. Но фирмам-производителям невыгодно содержать специальный отдел, тратить время и ресурсы. Поэтому создание *BIOS*обычно разделяют на два этапа:

1)    Производитель *BIOS* разрабатывает базовую версию, в которой реализованы все функции, не зависящие от особенностей чипсета.

2)    Производитель материнской платы совместно с компанией ‑ разработчиком *BIOS*, так сказать, подгоняют версию под особенности платы. Со временем появляется новое периферийное оборудование, и *BIOS* может неоднократно изменяться после выпуска платы, получая новые функции и возможности. Новые версии BIOS выкладываются для скачивания на сайтах компаний ‑ производителей материнских плат с точным указанием модели этой самой платы.

Таким образом, понятие *«версия BIOS»* можно обозначить как версию базового кода (обычно обозначается как *AwardBIOS 6.0* ‑ шестая версия *BIOS*компании *Award*) либо версию *BIOS* для конкретной модели материнской платы, название которой обычно состоит из сокращенного названия модели платы и номера обновления.

*Вход в BIOS Setup*

Вход в *BIOS Setup* возможен только при включении компьютера. При первоначальном тестировании *POST* (слышен один короткий сигнал из системного динамика) необходимо нажать определенную клавишу или сочетание клавиш. Обычно на экранной заставке при тестировании отображается надпись типа *«PressDEL to enter Setup»* ‑ это означает, что для входа в *BIOS Setup* необходимо нажать клавишу *DEL*. Узнать, за которой клавишей закреплен вход в *BIOS*, можно из инструкции к материнской плате. Если инструкции нет, а экранная заставка не отображает подсказки, можно опробовать наиболее известные варианты комбинаций:

*Delete*

*F1, F2, F3, F10, F11, F12*

*Esc*

*Ctrl + Shift + S или Ctrl + Alt + S*

*Ctrl + Alt + Esc*

*Ctrl + Alt + Delete*

*Интерфейс BIOS и приемы работы с параметрами*

Наиболее распространенные версии *BIOS* имеют схожий текстовый интерфейс, и изменение всех значений параметров осуществляется при помощи клавиатуры. При входе в *BIOS Setup* пользователь попадает в главное окно, где расположены все основные разделы. Внутри раздела также может быть расположен еще один раздел (подраздел). Все разделы имеют одинаковую структуру:

·     В верхней части окна выводится название текущего раздела или подраздела.

·     В левой части находится список доступных параметров выбранного раздела (либо вызывается выпадающий список при нажатии на клавишу

Enter).

·     Справа от названий параметров выводятся их текущие значения. Если какой-либо из параметров и его значение отображается бледным цветом ‑ значит, либо он предназначен только для чтения и не может изменяться, либо для его редактирования необходимо изменить другой связанный с ним параметр.

·     В правой части окна обычно выводится краткая справка по выбранному параметру, в нижней части ‑ подсказка по использованию функциональных клавиш.

После входа в BIOS Setup и появления главного окна будут доступны следующие клавиши для управления:

·     (клавиши управления курсором) — перемещение по разделам и параметрам.

·     *Enter* ‑ вход в выбранный раздел или выполнение команды, также в современных *BIOS* появляется выпадающий список доступных параметров. *Page Up/PageDown* или *+/-* на дополнительном цифровом блоке клавиатуры ‑ изменение значения выбранного параметра: нажимая указанные клавиши несколько раз, можно перебрать все доступные значения изменяемого параметра. Обычно, по отображении последнего параметра указатель перемещается на первое значение списка (т.н. зацикленный список).

·     *ESC* ‑ выход из раздела в главное меню, а при нажатии в главном окне ‑ выход из *BIOS Setup* с отменой всех изменений.

·     *F1* ‑ вызов справки по работе с *BIOS Setup*.

·     *F2* ‑ смена цветовой палитры программы *BIOS Setup* (доступна не во всех версиях).

·     *F5* ‑ восстановление предыдущих значений для выбранного раздела: будут возвращены те значения, которые были на момент входа в программу *BIOS Setup*, либо (в некоторых версиях) установлены значения по умолчанию.

·     *F6* ‑ установка для выбранного раздела значений по умолчанию (команда *Load Fail-Safe Defaults*); также в различных версиях могут использоваться клавиши*F5* или *F9* (*AMI BIOS*).

·     *F7* ‑ установка для выбранного раздела оптимизированных значений (команда *Load Optimized Defaults*).

·     *F10* ‑ выход из *BIOS Setup* с сохранением всех внесенных изменений, при этом нужно подтвердить действия с помощью клавиш *Y* или *Enter*. *Y/N* ‑ *Yes/No* (*Да/Нет*) ‑ согласиться или отказаться от выполнения команды или изменения параметра. *BIOS* также может предупреждать о том, что изменение параметра может повлечь нестабильную работу всей системы. Пользователь может либо согласиться и не изменять данный параметр, либо отказаться и продолжить редактировать параметр на свое усмотрение.

*Основные разделы BIOS*

В большинстве случаев производители *BIOS* используют классический вид первой страницы *BIOS Setup* размещения основных разделов и команд в два столбца. Как было оговорено ранее, каждая материнская плата имеет свои особенности, названия основных разделов *BIOS*, как правило, не меняются. Рассмотрим кратко названия основных разделов, дабы легче ориентироваться в местонахождении требуемого параметра.

·     *Standard CMOS Features (Standard CMOS Setup)* ‑ здесь собраны стандартные настройки компьютера, к которым относятся параметры дисковых накопителей, настройки даты, времени. Здесь также можно узнать о количестве установленной оперативной памяти и другие сведения о системе.

·     *Advanced BIOS Features (BIOS Features Setup)* ‑ «расширенные настройки *BIOS*», к которым относятся параметры загрузки, параметры работы компьютера,чипсета, периферии и кэш-памяти.

·     *Advanced Chipset Features (Chipset features Setup)* ‑ настройки работы чипсета материнской платы ‑ в частности, настройка северного моста (определяющих работу оперативной памяти, процессора, видеосистемы, шин *AGP*, *PCI-Express* и других устройств).

·     *Integrated Peripherals* ‑ настройка параметров интегрированных периферийных устройств, которые поддерживаются южным мостом ‑ таких, как гибкие и жесткие диски, адаптеры, порты и др.

·     *Power Management Setup* ‑ установка параметров электропитания и режимов энергосбережения, а также параметров изменения рабочего состояния при наступлении определенного события.

·     *PnP/PCI Configurations* ‑ управление способом распределения ресурсов между периферийными устройствами. Обычно данной функцией не пользуются, оставляя по умолчанию автоматическое распределение ресурсов.

·     *PC Health Status или H/W Monitor* ‑ отображение текущего значения, получаемого со встроенных датчиков, температур, напряжений и скорости вращения вентиляторов, а также установка значений для срабатывания защиты от перегрева.

·     Frequency/Voltage Control ‑ установка рабочих частот и напряжений для процессора, чипсета, оперативной памяти, видеоадаптера и других значений.

·     *Load Fail-Safe Defaults (Load BIOS Setup Defaults)* ‑ команда, сбрасывающая все настройки BIOS до значения по умолчанию, при этом устанавливаются безопасные значения всех параметров, частот и напряжений.

·     *Load Optimized Defaults (Load High Performance)* ‑ команда устанавливает настройки BIOS, которые обеспечивают оптимальную производительность системы, сохраняя ее стабильность. Ускоряется процедура POST, режимы работы оперативной памяти, шин и другие

параметры.

·     *Set Supervisor Password, Set User Password* ‑ команды для установки административного и пользовательского пароля на вход в *BIOS Setup* или загрузку компьютера.

*Диагностические средства BIOS*

Чтобы выдать сообщение пользователю, *BIOS* имеет возможность подать звуковой сигнал либо сообщить в текстовом виде на экране монитора. Первоначальное тестирование компьютера сопровождается подачей одного короткого звукового сигнала, что свидетельствует об успешном завершении процедуры *POST* и готовности к загрузке операционной системы. Если при прохождении *POST* обнаружена серьезная ошибка, работа системы будет остановлена с выдачей звуковых сигналов и/или текстового сообщения на экран монитора.

*Обновление BIOS*

Практически во всех современных материнских платах код *BIOS* записан в энергонезависимую микросхему *Flash-памяти*, что делает процедуру обновления*BIOS* достаточно простой. Тем не менее, перезапись *BIOS* ‑ операция достаточно ответственная, и выполнять ее необходимо лишь в том случае, если другими средствами устранить какую-либо проблему не представляется возможным либо если возникает одна из перечисленных причин:

·     В материнскую плату нужно установить новый процессор, поддержка которого появилась лишь в новой версии *BIOS*.

·     К материнской плате необходимо подключить жесткий диск большего объема, чем предусматривает имеющаяся версия *BIOS*.

·     Активация дополнительных функций, реализованных в чипсете, но недоступная в более ранних версиях *BIOS*.

·     Если компьютер работает нестабильно (хотя на стабильность влияет и множество других параметров) либо версия *BIOS* повреждена.

Следует принять во внимание, что, если веских причин для обновления *BIOS’а* нет, то лучше отказаться от этой процедуры. Ведь после перезаписи придется заново редактировать все настройки *BIOS*, а также операционной системы, и даже переустанавливать ее. Если все-таки было принято решение об обновлении*BIOS*, то необходимо выполнить несколько подготовительных действий:

·     Изучить производителя и модель материнской платы ‑ это можно сделать либо просто осмотрев материнскую плату, либо посмотрев ее название и модель в инструкции, а можно использовать одну из диагностических утилит (*SiSoftware Sandra*, *sisoftware.co.uk* либо *EVEREST*, lavales.com).

·     Скачать с сайта производителя материнской платы новую версию *BIOS* для вашей модели (обычно файл с расширением *\*.bin*) и программу- прошивальщик, а также инструкцию к программе-прошивальщику и изучить все ключи и команды либо распечатать, дабы при неудачной прошивке иметь возможность воспользоваться всеми ее возможностями.

·     Создать загрузочную дискету с программой-прошивальщиком и новой версией *BIOS*.

·     Обязательно сделать резервную копию работающего *BIOS* вашей материнской платы, чтобы иметь возможность выполнить откат.

·     Позаботится о стабильности системы на время прошивки *BIOS*, отключив дополнительную периферию и оставив необходимый минимум устройств для загрузки системы.

При несоблюдении описанных выше основных правил обновления код *BIOS* может быть поврежден, вследствие чего компьютер может не загружаться. Однако признаки жизни компьютер все же подает: загорается индикатор питания, запускаются вентиляторы, мигают индикаторы дисков и на клавиатуре. В таком случае прежде, чем приступать к процедуре восстановления *BIOS*, нужно отключить на некоторое время компьютер от сети, обнулить *CMOS* при помощи перемычки на компьютере и попытаться включить его снова.

*Разгон компьютера средствами BIOS*

Скорость работы таких компонентов, как процессор, оперативная память, видеоадаптер и чипсет, зависит от установленных тактовых частот, интервалов и рабочих напряжений. Изменяя эти параметры, можно заставить систему работать на повышенной или пониженной частоте. Превышение рабочих частот по сравнению со значениями, заданными производителем устройства, называется разгоном. Так, при работе на повышенной частоте/напряжении срок службы микросхемы снижается вдвое при сроке службы, заявленном производителем примерно 15-20 лет. Вот теперь представьте ваш домашний компьютер без апгрейда хотя бы 5-7 лет. Часто ли можно встретить в домашней системе видеоадаптер или процессор пятилетней давности? В конечном итоге решение принимать пользователю.

Почему же вообще возможен разгон? Производители всегда оставляют так называемый запас прочности для своего оборудования, что необходимо для его надежности в течение всего срока эксплуатации. Для процессора, оперативной памяти, видеоадаптера, чипсета и других компонентов рабочие частоты устанавливаются с помощью тактового генератора на материнской плате. Во многих материнских платах предусмотрено изменение частоты в *BIOS*, разгон выполняется простым изменением нескольких параметров. Вместе с тем, при разгоне могут проявиться отрицательные эффекты:

·     нестабильная работа компьютера, сбои или зависания, связанные с повышенными частотами разогнанных компонентов;

·     невозможность включить компьютер или загрузить операционную систему из-за слишком высоких рабочих частот;

·     сокращение срока службы компонентов;

·     выход из строя процессора, оперативной памяти, материнской платы или видеоадаптера при чрезмерном завышении питающих напряжений или по другим причинам.

К процессу разгона компонентов следует подходить очень ответственно: будучи повреждены из-за разгона, гарантийному обмену они не подлежат. Существует два основных способа разгона компьютера. Разгон с помощью специализированных утилит ‑ на компакт-дисках с драйверами к материнской плате часто поставляется специализированная утилита для разгона непосредственно из операционной системы. *Разгон с помощью BIOS* ‑ используются специализированные настройки *BIOS*. *Разгон с помощью BIOS* предполагает установку рабочих частот и напряжений пользователем. Следует сразу же заметить, что неосторожное изменение рабочих частот и напряжений может привести к тому, что система может самостоятельно перезагружаться или не загружаться вовсе, а в самом пессимистичном случае даже выходят из строя отдельные компоненты. Данный способ довольно трудоемок по сравнению со способом использования утилит, но позволяет достичь выдающихся результатов. Традиционно раздел для рабочих частот и напряжений называется *frequency/Voltage Control*, но производители материнских плат стремятся дать этому разделу свое уникальное и броское название. Вот несколько примеров: *MB Intelligent Tweaker (M.I.T.)* ‑*Gigabyte*, *Cell Menu* ‑ *MSI*, *Genie BIOS Setting* ‑ *DFI*.Названия и местоположение некоторых параметров может изменяться даже в продукции одного производителя. Некоторые производители материнских плат пытаются скрыть критичные для разгона характеристики ‑ данное решение позволяет уменьшить число звонков в службу технической поддержки при неумелом разгоне. Например, *Gigabyte в BIOS Setup* открывает некоторые настройки только при нажатии на *Ctrl+F1*. Однако встречаются так называемые бюджетные варианты материнских плат, в которых возможности разгона напрочь отсутствуют. Этим производитель добивается стабильной работы, удешевления проектирования, разработки и производства и как результат низкой цены конечного продукта. Тем не менее, следует очень ответственно подходить к изменению известных настроек и еще более тщательно изучать неизвестные.

Оформите отчет, сделайте выводы по работе.

3. Содержание отчета

1. Номер и тема практической работы;
2. Цель работы;
3. Необходимое оборудование;
4. Ход выполнения практической работы (этапы);
5. Выводы по выполненной работе.

4.Контрольные вопросы

* 1. Что такое POST?
  2. Какие задачи решает POST?
  3. Перечислите основные разделы BIOS.
  4. Как изменить порядок опроса устройств для поиска загрузочного сектора?
  5. Каким образом установить оптимизированные значения для BIOS?
  6. Каким образом осуществляется выход из раздела в главное меню?
  7. Для чего необходимо обновление BIOS?
  8. Как обновить BIOS?
  9. Каким образом выйти из BIOS сохранив изменения?
  10. Перечислите основные клавиши для управления меню BIOS.

1. **Практическое занятие 6.**

Управление логическими разделами жёсткого диска.

***Цель работы:*** Получение практических навыков работы с программой позволяющей управлять разделами жесткого диска Wondershare Disk Manager.

***Задание:***

* + Изучить теоретический материал.
  + Установить программу Wondershare Disk Manager на виртуальную машину.
  + Проделать описанные по ходу текста команды (сделать скриншоты).
* Создайте новый логический раздел.
* Удалите созданный раздел.
* Воспользуйтесь мастером восстановления разделов.
  + Оформить протокол.

**Теоретический материал**

Раньше, когда емкость жестких дисков измерялась мегабайтами, для накопления приличного пространства приходилось подключать к компьютеру по несколько накопителей. Операционная система распознавала их и именовала поочередно буквами латинского алфавита. Все было просто: сколько винчестеров стоит — столько отображается и букв дисков.

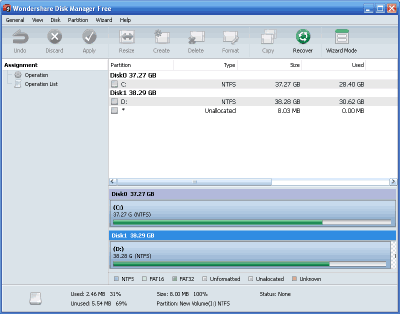
Однако с появлением емких носителей ситуация стала кардинально меняться. Теперь почти в каждом современном ПК реальный жесткий диск всего один, но система определяет его как два и более! Все дело в том, что современные винчестеры можно «разбивать» на несколько разделов, каждому из которых присваивается отдельная буква, и с которыми можно работать отдельно, не затрагивая файловой системы секторов соседних логических дисков. Речь пойдет о программе, которая позволяет управлять разделами жесткого диска. И называется она Wondershare Disk Manager. Это небольшое приложение под Windows позволяет создавать, удалять, перемещать, изменять размер разделов жесткого диска. В ней присутствуют все самые необходимые инструменты, которые есть в платных пакетах, поэтому Wondershare Disk Manager вполне можно сравнить с Windows-версией Acronis Disk Director:

Сравнение Wondershare Disk Manager с платным аналогом Acronis Disk Director

|  |  |  |
| --- | --- | --- |
| Особенности | Wondershare Disk Manager | Acronis Disk Director |
| Основные операции с разделами | + | + |
| Поддержка файловых систем Linux | - | + |
| Восстановление разделов | + | + |
| Резервное копирование разделов | + | + |
| Управление буквами и именами томов | + | + |
| Конвертирование файловой системы | только из FAT в NTFS | + |
| Проверка целостности тома | + | + |

**Интерфейс Wondershare Disk Manager**

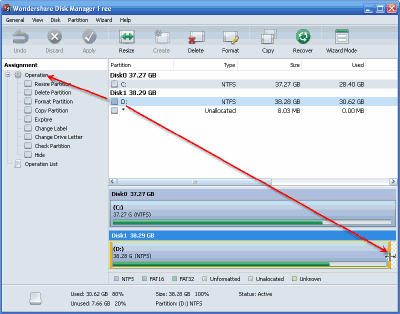
главное окно Wondershare Disk Manager:

[](http://files.gold-free.ru/soft/sys/WondershareDiskManager.gif)

В самом верху окна находится панель меню, к которой касаться мы практически не будем, поскольку все функции вынесены на панель инструментов (ниже) . Под панелью инструментов мы видим непосредственную рабочую область, разбитую на три части: слева — панель событий, справа вверху — список жестких дисков с подробной информацией о них, а внизу — схематическое изображение дискового пространства. В самом низу окна находится статусная строка с обобщенной информацией о разделах жестких дисков.

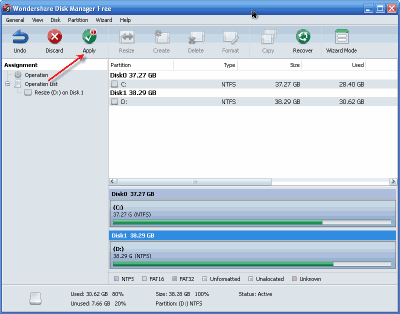
**Работа с диском**

Для начала работы с разделами достаточно выбрать один из них в списке или на схеме:

[](http://files.gold-free.ru/soft/sys/WondershareDiskManager_3.gif)

После этого на панели операций слева высветится список всех возможных действий над данным томом, а на схеме активируются планки управления размером раздела.

В Wondershare Disk Manager, можно изменять размеры разделов простым перетаскиванием мыши без необходимости вызывать дополнительные диалоговые окна. Вот простой пример: как видите, на диске D есть 8 мегабайт неразмеченного пространства. Чтобы добавить его к основному разделу достаточно просто выделить его и потянуть за правую планку управления размером до упора.

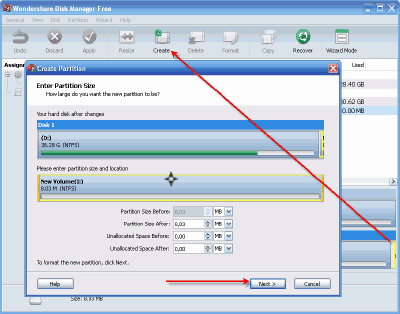
[](http://files.gold-free.ru/soft/sys/WondershareDiskManager_4.gif)

После этого в списке операций появится запись о совершенном нами действии, а на панели инструментов активируется три кнопки, позволяющие отменить, удалить или подтвердить данное действие. В нашем случае для подтверждения нужно нажать кнопку «Apply». Появится окошко подтверждения, в котором нас в последний раз спросят действительно ли мы подтверждаем свое действие. Снова кликаем «Apply» и ждем завершения процедуры.

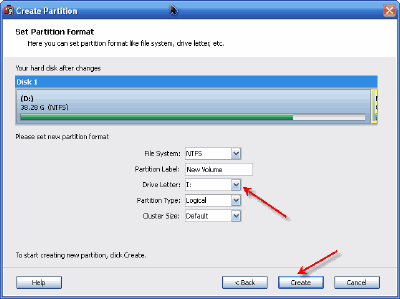
Стоит заметить, что если Вам нужно задать точный размер раздела, то для переразмеривания воспользуйтесь мастером, который вызывается нажатием кнопки «Resize» на панели инструментов.

**Создание нового логического диска**

В предыдущем примере неразмеченное пространство мы присоединили к основному разделу, однако мы могли бы поступить и по-другому: отобрать пару гигабайт от основного тома и создать на получившейся пустой области новый логический диск

[](http://files.gold-free.ru/soft/sys/WondershareDiskManager_5.gif)

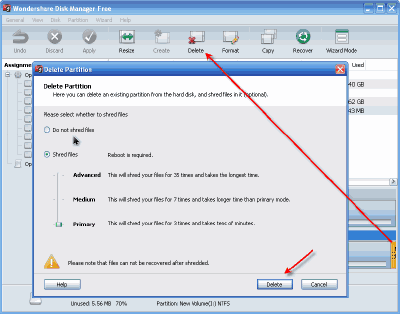
Для этого нужно выбрать неразмеченную область и вызвать мастер создания раздела, кликнув кнопку «Create». В первом окне мастера мы можем точно уменьшить размер нового тома, после чего нужно будет перейти к следующему окну, нажав кнопку «Next»:

[](http://files.gold-free.ru/soft/sys/WondershareDiskManager_6.gif)

Вы сможете выбрать файловую систему для нового логического диска, задать ему название, букву, тип и размер кластеров (стандартные настройки можно и не менять). После этого достаточно будет нажать кнопку «Create» и мы получим новый раздел (правда, после процедуры подтверждения описанной выше).

**Удаление ненужных разделов**

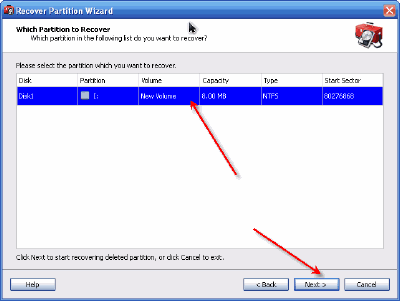
Иногда случаются случаи, когда мы больше не нуждаемся в том или ином разделе и его нужно удалить (например, для увеличения места на основном томе). В таком случае мы можем воспользоваться мастером удаления разделов Wondershare Disk Manager:

[](http://files.gold-free.ru/soft/sys/WondershareDiskManager_7.gif)

Выбираем раздел, который подлежит уничтожению, и жмем кнопку «Delete» на панели инструментов. Откроется окно, в котором мы сможем выбрать тип удаления тома. А доступно их два: без уничтожения файлов и с их полным стиранием (последний режим требует перезагрузки). В первом случае мы в будущем при желании легко сможем восстановить практически все файлы, хранившиеся на разделе до его удаления при помощи функции «Recover». Второй же вариант позволяет полностью очистить содержимое выбранного раздела без возможности его восстановления. В режиме «Shred files» мы можем установить количество проходов перезаписи данных на выбранном разделе от 3 (Primary) до 35 (Advanced). После выбора типа удаления раздела достаточно будет нажать кнопку «Delete» и подтвердить свое действие.

**Восстановление разделов**

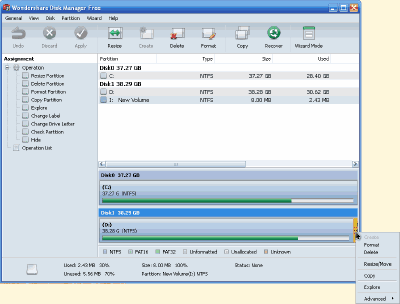
Следующим инструментом Wondershare Disk Manager является мастер восстановление разделов:

[](http://files.gold-free.ru/soft/sys/WondershareDiskManager_8.gif)

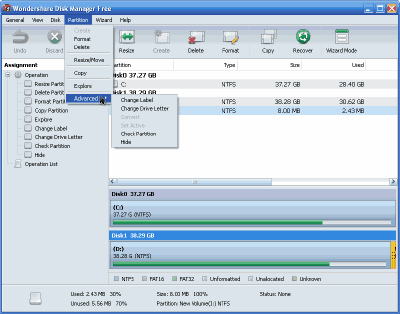
Вызывается он нажатием кнопки «Recover». В первом окне мастера мы можем выбрать автоматическое или ручное сканирование жесткого диска (рекомендуется автоматическое). В следующем окне программа, просканировав пространство винчестера, выдаст список доступных для восстановления томов. Выбираем один из них и жмем «Next». После подтверждения действия мы получим полную копию удаленного ранее раздела жесткого диска со всеми файлами, хранившимися на нем (если конечно Вы не стирали их при удалении тома).

**Работа через контекстное меню**

Ко всем основным и дополнительным функциям Wondershare Disk Manager можно получить доступ несколькими способами. Мы уже работали с панелью инструментов и рассматривали панель событий, однако, как и во многих других приложениях, порой очень удобным способом управления является контекстное меню:

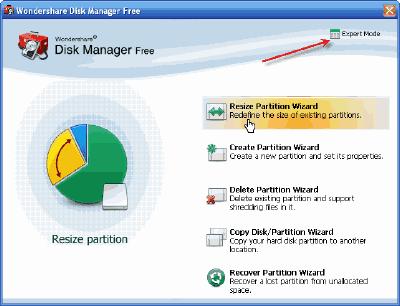
[](http://files.gold-free.ru/soft/sys/WondershareDiskManager_9.gif)

Здесь, как и на панели событий, собраны все возможные действия над выбранным разделом, которых нет на панели инструментов. Например, пункт «Explore» позволяет быстро открыть корневой каталог выбранного логического диска, а в разделе «Advanced» собраны дополнительные инструменты по работе с разделом:

[](http://files.gold-free.ru/soft/sys/WondershareDiskManager_10.gif)

К таким инструментам относятся «Изменение названия диска», «Изменение буквы диска», «Конвертирование файловой системы», «Установка активности», «Проверка целостности диска» и «Скрытие раздела».

Также существует специальный режим мастера, в который можно переключиться, нажав кнопку«Wizard Mode» (крайняя справа кнопка на панели инструментов):

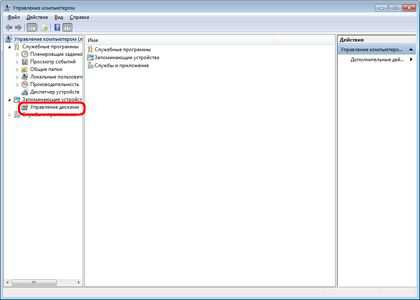
[](http://files.gold-free.ru/soft/sys/WondershareDiskManager_11.gif)

В этом режиме мы имеем доступ только к самым основным инструментам для работы с разделами (переразмеривание, создание, удаление, копирование и восстановление томов). Они представлены в виде кнопок с небольшим пояснением, нажатие которых вызывает соответствующий мастер, описанный выше.

**Примечание**

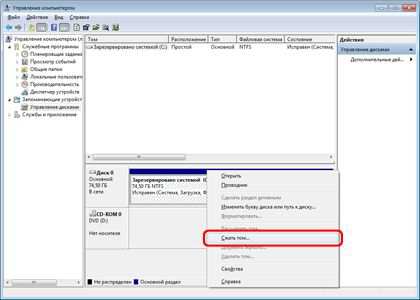
Операционная система Windows 7 оснащена встроенной утилитой для разбивки дисков. Для того чтобы запустить ее пройдите по пути: Пуск – Панель управления -  Система – Администрирование – Управления компьютером – Управление дисками.

В диалоговом окне "управление компьютером", в разделе "запоминающие устройства", выберете элемент "управление дисками"



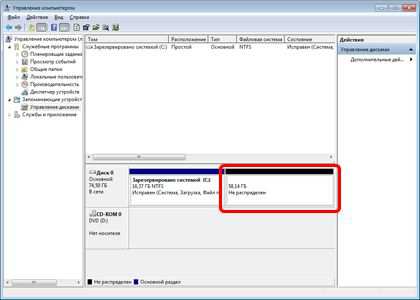
В списке томов, разделов, кликните правой кнопкой мыши диск,

содержимое которого хотите сжать и выберете команду **сжать** **том**.

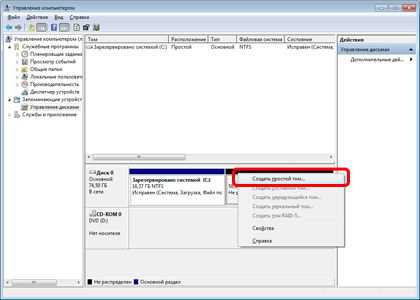


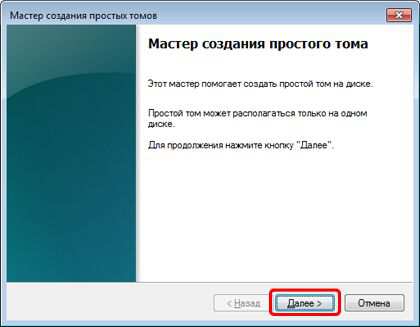
Понятно. Таким образом за счет сжатия содержимого на существующем жестком диске создается свободное место.

Незанятое пространство это объем свободного пространства, который только что был создан.

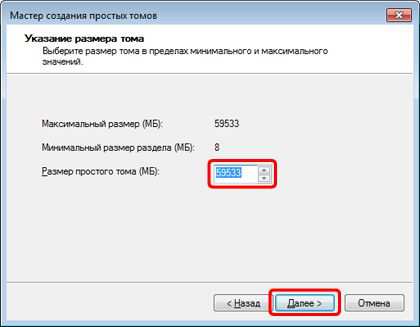


**Инструкции по преобразованию раздела в новый том в системе Windows 7**

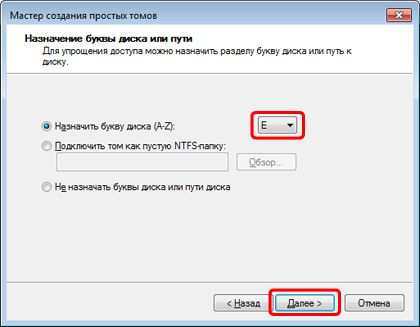
Щелкните правой кнопкой мыши незанятое пространство на диске, где хотите создать раздел, и нажмите кнопку **Создать простой том**. Запустится мастер **создания простого тома**.  




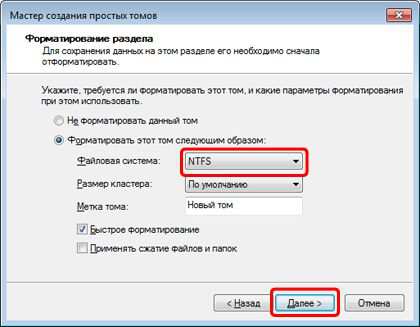
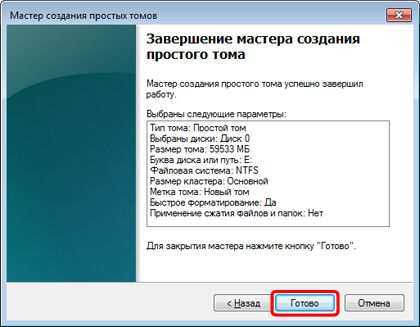
Проверьте будущий размер нового тома и нажмите кнопку **Далее**.



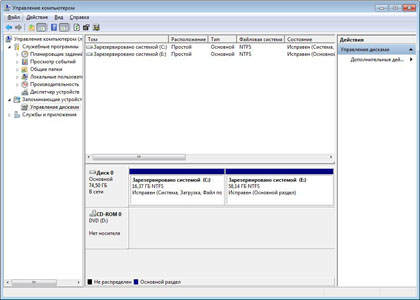
Проверьте букву диска, которая будет назначена новому тому, и нажмите кнопку **Далее**.



Убедитесь, что в качестве файловой системы указан формат NTFS, и нажмите кнопку **Далее**.



Начнется форматирование тома, и все параметры будут применены после его завершения.



Оформите отчет, сделайте выводы по работе.

*Содержание отчета*

1. Номер и тема практической работы;
2. Цель работы;
3. Необходимые оборудование;
4. Ход выполнения практической работы (этапы);
5. Выводы по выполненной работе.

*Контрольные вопросы*

* В каких случая необходима разметка жесткого диска?
* Какие программы позволяют разметить диск?
* Возможна ли разметка диска без специальных утилит?

**Практическое занятие 7.**

Управлениеправами пользователей в Windows XP

**Цель работы:** Ознакомиться с процедурами создания учетных записей пользователей и управления их правами.

**Задание:**

* Изучить теоретический материал.
* Запустить свою виртуальную машину.
* Настроить учетные записи пользователя.
* Ознакомиться с настройками управления группами пользователей.
* Оформить отчет.

**Теоретическийматериал.**

|  |  |
| --- | --- |
| В операционной системе Windows XP на одном и том же компьютере могут работать разные пользователи, каждый под своим именем. При входе в ОС запрашиваются имя и пароль, на основе которых происходит аутентификация пользователя.  Компьютер может работать автономно, а может быть рабочей станцией в сети. Если компьютер загружается для автономной работы или для работы в *одноранговой сети*, то пользователь регистрируется, используя внутренний (локальный) список имен пользователей системы.  Если компьютер загружается для работы в *сети с выделенным сервером*, то пользователь регистрируется, используя имя, которое ему выдал администратор сети. Список с этими именами хранится на сервере.  Данные о пользователе находятся в специальной базе данных на локальных компьютерах и на сервере. На каждого пользователя заводится отдельная учетная карточка, которая носит название учетная запись.  Windows XP использует три типа учетных записей пользователей:   1. Локальные учетные записи для регистрации пользователей локального компьютера. База локальных учетных записей хранится на каждом компьютере своя, и содержит информацию о пользователях только данного компьютера. Создаются учетные записи администратором этого компьютера. 2. Встроенные учетные записи пользователей создаются автоматически при установке Windows XP. Встроенных учетных записей две — Администратор и Гость. Встроенные учетные записи хранятся в той же базе, что и локальные учетные записи. 3. Учетные записи пользователей домена хранятся на выделенном сервере и содержат данные о пользователях локальной сети.   Локальная учетная запись - это учетная запись, которой могут быть предоставлены разрешения и права на вашем компьютере. Для удобства управления локальными пользователями, их можно объединять в группы и управлять группами, чтобы не устанавливать одни и те же настройки для каждого пользователя в отдельности. Ограничения, установленные для группы, распространяются на всех пользователей этой группы.  Домен или глобальные пользователи и группы управляются *сетевым администратором*. Имеется возможность добавить локальных пользователей, глобальных пользователей и глобальные группы в локальные группы. Однако невозможно добавить локальных пользователей и локальные группы в глобальные группы.  Пользователи и группы важны для безопасности Windows XP поскольку позволяют ограничить возможность пользователей и групп выполнять определенные действия путем назначения им прав и разрешений. Право дает возможность пользователю выполнять на компьютере определенные действия, такие как *архивирование* файлов и папок или завершение работы компьютера. Разрешение представляет собой правило, связанное с объектом (например, файлом, папкой или принтером), которое определяет, каким пользователям и какого типа доступ к объекту разрешен.  Операционная система содержит несколько встроенных учетных записей пользователей и групп, которые не могут быть удалены:   * **Учетная запись администратора**   *Учетная запись пользователя* с именем "Администратор" используется при первой установке рабочей станции или рядового сервера. Эта учетная запись позволяет выполнять необходимые действия до того, как пользователь создаст свою собственную учетную запись. Администратор является членом группы администраторов на рабочей станции или рядовом сервере.  Учетную запись "Администратор" нельзя удалить, отключить или вывести из группы администраторов, что исключает возможность случайной потери доступа к компьютеру после уничтожения всех учетных записей администраторов. Это свойство отличает пользователя "Администратор" от остальных членов локальной группы "Администраторы".   * **Учетная запись гостя**   Учетная запись гостя предназначена для тех, кто не имеет реальной учетной записи на компьютере. Учетную запись "Гость" нельзя удалить, но можно переименовать или отключить. Учетной записи пользователя "Гость", как и любой другой учетной записи, можно предоставлять права и разрешения на доступ к объектам. Учетная запись "Гость" по умолчанию входит во встроенную группу "Гости", что позволяет пользователю войти в систему с рабочей станции или рядового сервера. Дополнительные права, как любые разрешения, могут быть присвоены группе "Гости" членом группы администраторов.  К стандартным группам Windows XP относятся следующие группы:   * **Администраторы**   Пользователи, входящие в группу "Администраторы", имеют полный доступ на управление компьютером. Это единственная встроенная группа, которой автоматически предоставляются все встроенные права и возможности в системе. По умолчанию туда входит учетная запись "Администратор".   * **Операторы архива**   *Члены группы* "Операторы архива" могут архивировать и восстанавливать файлы на компьютере, независимо от всех разрешений, которыми защищены эти файлы. Также они могут входить на компьютер и выключать его, но не могут изменять параметры безопасности.   * **Опытные пользователи**   *Члены группы* опытных пользователей могут создавать учетные записи пользователей, но могут изменять и удалять только созданные ими учетные записи. Они могут создавать локальные группы и удалять пользователей из локальных групп, которые они создали. Они также могут удалять пользователей из групп "Опытные пользователи", "Пользователи" и "Гости".  Они не могут изменять группы "Администраторы" и "Операторы архива", не могут являться владельцами файлов, не могут выполнять *архивирование* и восстановление каталогов, не могут загружать и выгружать драйверы устройств или управлять журналами безопасности и аудита.   * **Пользователи**   *Члены группы* пользователей могут выполнять наиболее распространенные задачи, например запуск приложений, использование локальных и *сетевых принтеров*, завершение работы и блокировка рабочих станций. Пользователи могут создавать локальные группы, но изменять могут только те, которые они создали. Пользователи не могут организовывать общий доступ к каталогам или создавать *локальные принтеры*.   * **Гости**   Группа "Гости" позволяет случайным или разовым пользователям войти в систему со встроенной учетной записью гостя рабочей станции и получить ограниченные возможности. *Члены группы* "Гости" могут только прекратить работу компьютера.  *Управление учетными записями* пользователей и группами осуществляется пользователями, входящими в группу Администраторы. | |
|  |  |

#### Задание 1. Управление учетными записями пользователя

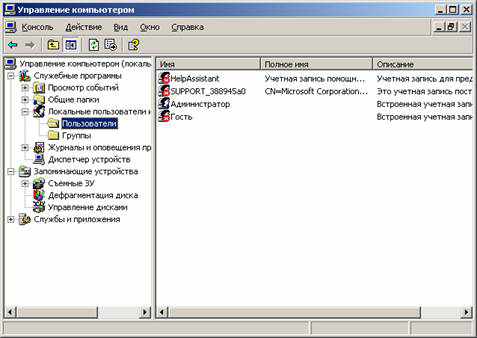
Для *управления учетными записями* используется компонент "Управление компьютером". Чтобы его открыть выберите Пуск->Настройка->Панель управления.

Дважды щелкните значок Администрирование 4_k1 затем дважды щелкните значок Управление компьютером 4_k2.

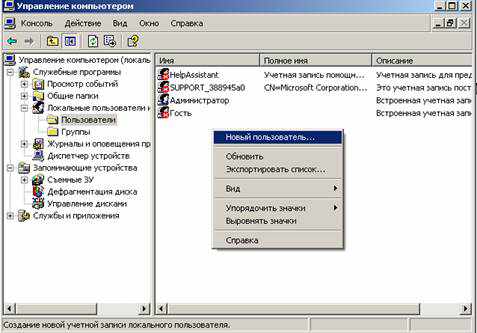
Второй способ открыть "Управление компьютером" нажать правой кнопкой на значке "Мой компьютер" и в появившемся контекстном меню выбрать "Управление".

##### Создание новой учетной записи пользователя

1. Откройте компонент "Управление компьютером" одним из описанных выше способов.
2. В дереве консоли выберите компонент "Локальные пользователи и группы" и щелкните в нем узел Пользователи.



Нажмите правой кнопкой мыши в окне со списком пользователей и в появившемся меню выберите команду Новый пользователь.



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| В появившемся окне заполните поля по аналогии  4_3  По умолчанию стоит опция "потребовать смену пароля при следующем входе в систему". То есть система при первом входе пользователя в ОС потребует от него сменить пароль. Если убрать галочку с этого пункта, появится возможность выбрать следующие опции:   * + запретить смену пароля пользователем. То есть пользователь будет использовать пароль, заданный при создании учетной записи;   + срок действия пароля не ограничен – то есть пароль никогда не истекает.   Опция "Отключить учетную запись" делает вход в систему данного пользователя невозможным.  Чтобы завершить работу, нажмите кнопку Создать, а затем Закрыть.  Если есть необходимость в создании сразу нескольких пользователей нужно нажать на Создать и повторить все предыдущие шаги. После заведения последнего пользователя нажать на Создать и затем сразу на Закрыть.  После этого заведенные пользователи появляются в списке.  4_4 Изменение учетной записи пользователя 1. Откройте компонент "Управление компьютером".  2. В дереве консоли выберите компонент "Локальные пользователи и группы" и перейдите к Пользователям.  3. Выберите учетную запись, которую требуется изменить.  4_5    4. Нажмите на учетную запись правой кнопкой мыши и в контекстном меню выберите "Свойства".  4_6  5. Внесите нужные изменения и нажмите кнопку ОК.  4_7 Изменение пароля для пользователя 1. Откройте компонент "Управление компьютером".  2. В дереве консоли выберите компонент "Локальные пользователи и группы" и щелкните в нем узел Пользователи.  3. Выберите учетную запись, которую требуется изменить.  4_8  4. В контекстном меню выберите пункт "Задать пароль".  4_9  5. Выйдет окно, извещающее о том, что принудительная смена пароля администратором является крайней мерой. Нажмите кнопку "Продолжить".  4_10  6. В появившемся окне задайте новый пароль для пользователя и нажмите на ОК. Теперь пользователь сможет войти в систему только с новым паролем.  4_11 Отключение и активизации учетной записи пользователи 1. Откройте компонент "Управление компьютером".  2. В дереве консоли выберите компонент "Локальные пользователи и группы" и щелкните в нем узел Пользователи.  3. Выберите учетную запись, которую требуется изменить.  4_12  4. В меню контекстном меню выберите Свойства.  5. Чтобы отключить выбранную *учетную запись пользователя*, установите флажок "Отключить учетную запись".  4_13   Удаление учетной записи пользователи 1. Откройте компонент "Управление компьютером".  2. В дереве консоли выберите компонент "Локальные пользователи и группы" и щелкните в нем узел Пользователи.  3. Выберите учетную запись, которую требуется удалить.  4. В контекстном меню учетном записи выберите Удалить.  5. Появится окно, предупреждающее о последствиях удаления пользователя. Выберите ДА.  4_14  6. Пользователь исчезнет из списка.   |  |  | | --- | --- | | Задание 2. Управление группами пользователей Пользователь, принадлежащий группе, имеет все права на разрешения, предоставленные этой Группе. Пользователь, являющийся членом нескольких групп, имеет все права и разрешения, предоставленные каждой из этих групп.  При удалении локальной группы удаляется учетная запись группы. Учетные записи пользователей и глобальных групп, являющихся членами удаленной группы, при этом не удаляются. Создание новой локальной группы  1. Откройте компонент "Управление компьютером". 2. В дереве консоли выберите компонент "Локальные пользователи и группы" и щелкните в нем узел Группы.   4_15   1. Правой кнопкой вызовите контекстное меню и выберите Создать группу   4_16  Заполните поле *Имя группы*. При желании можно заполнить поле Описание.  4_17   1. Выполните одно из следующих действий. Чтобы создать еще одну группу, нажмите кнопку Создать и заполните поля. Чтобы завершить работу, нажмите кнопку Создать, а затем Закрыть. Новая группа появится в списке групп.   4_18 Добавление пользователя в группу  1. Откроите компонент "Управление компьютером". 2. В дереве консоли выберите компонент "Локальные пользователи и группы" и выберите в нем узел Группы. 3. Выберите нужную группу. 4. В контекстном меню выберите Свойства или Добавить в группу.   4_19   1. В открывшееся окне нажмите кнопку Добавить. 2. В нижнее поле введите имя пользователя, которого хотите добавить.   4_20   1. Если необходимо проверить имена добавляемых пользователей или групп. Нажмите кнопку Проверить имена. Нажмите на ОК.   4_21   1. Добавив имена всех требуемых пользователей, нажмите кнопку ОК. Отобразится окно с членами данной группы. В списке появятся добавленные пользователи.   4_22 Удаление локальной группы  1. Откройте компонент "Управление компьютером". 2. В дереве консоли выберите компонент "Локальные пользователи и группы" и щелкните в нем узел Группы. 3. Выберите Группу, которую следует удалить. 4. В контекстном меню группы выберите Удалить.   4_23     1. Появится окно, предупреждающее о последствиях удаления. Выберите ДА.   4_24   1. Удаленная группа исчезнет из списка групп данного компьютера.   4_25 | | | empty | | |  |  | | |
| empty | |
| empty | |
|  |  |

*Содержание отчета*

1. Номер и тема практической работы;
2. Цель работы;
3. Необходимые оборудование;
4. Ход выполнения практической работы (этапы);
5. Выводы по выполненной работе.

*Контрольные вопросы*

1. Основные типы учетных записей?
2. Стандартные группы Windows XP?

**Практическое занятие 8.**

Управление процессами в операционной системе Windows

**Цель работы:** Получение практических навыков управления процессами и самостоятельной работы с документацией команд.

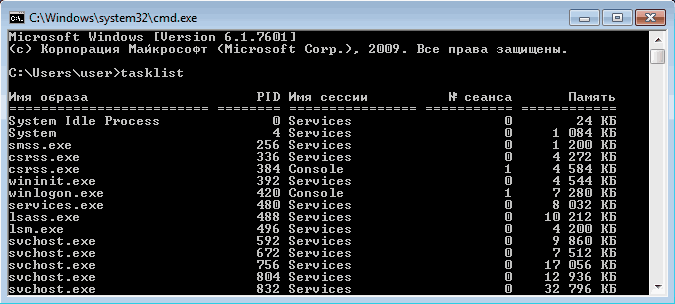
**Задание**

1. Запустите Windows
2. Составьте справочник для приведенных команд, расписав какие параметры для чего нужны.
3. Установите PSTools
4. Поработайте с этими командами: запуская, запуская по времени, меняя приоритеты, уничтожая процессы.
5. Разберитесь как работать с диспетчером задач, и что означает информация в столбцах (кроме информации о памяти).
6. Что нужно уметь (с командной строки):  
   - задавать задание на запуск процессов в определенное время, показывать этот список, удалять из списка, изменять задания  
   - запускает определенную программу или команду в отдельном окне.  
   - завершать процесс  
   - выводить (и понимать) информацию (исключая память и ввод/вывод) о работающих процессах и потоках  
   - выводить (и понимать) информацию (исключая память и ввод/вывод) о работающих процессах и потоках
7. Отправьте примеры использования на проверку.
8. В своей виртуальной машине сделать:  
   - создать задание на запуск программы, минута,час,день месяца, месяц - последняя цифра в номере зачетки

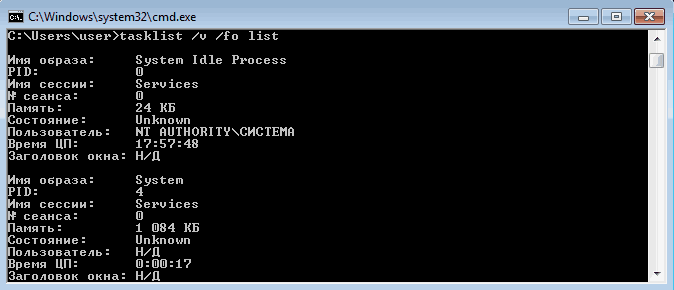
Управление процессами из командной строки

Бывают ситуации, когда все остальные инструменты кроме командной строки недоступны, например некоторые вредоносные программы могут блокировать запуск Task Manager и подобных ему программ. Для управления процессами в командной строке есть две утилиты — tasklist и taskkill. Первая показывает список процессов на локальном или удаленном компьютере, вторая позволяет их завершить.

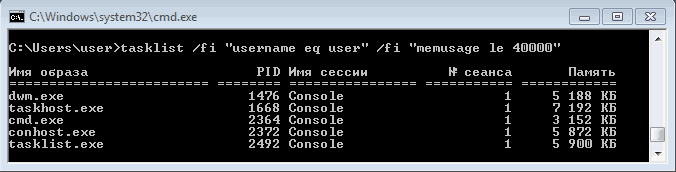
Если просто набрать команду tasklist в командной строке, то она выдаст список процессов на локальном компьютере

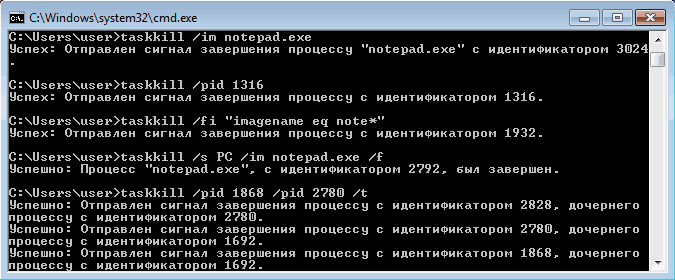
[](http://windowsnotes.ru/wp-content/uploads/2012/01/cmd1.gif)

По умолчанию информация выводится в виде таблицы, однако ключ /fo позволяет задать вывод в виде списка или в формате CSV, а ключ /v  показывает более подробную информацию о процессах, например команда tasklist /v /fo list выведет подробное описание всех процессов в виде списка

[](http://windowsnotes.ru/wp-content/uploads/2012/01/cmd2.gif)

Список получится довольно большой, поэтому попробуем уточнить запрос.  Для этого используем ключ /fi , который позволяет использовать фильтры для вывода данных, например команда tasklist /fi «username eq user» /fi «memusage le 40000″ выводит список процессов пользователя user, которые потребляют не больше 40Мб памяти

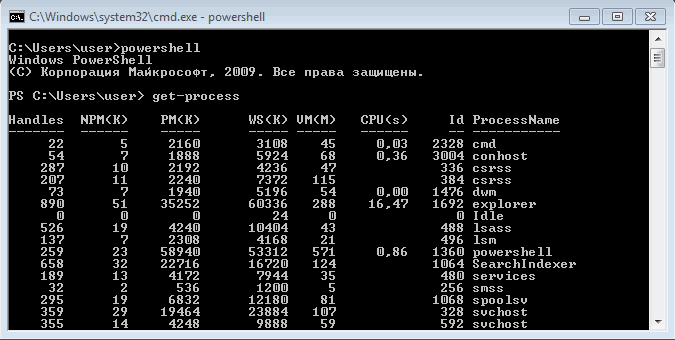
[](http://windowsnotes.ru/wp-content/uploads/2012/01/cmd3.gif)

Найдя процессы, которые необходимо завершить, воспользуемся командой taskkill.Завершать процессы можно по имени, идентификатору процесса (PID) или задав условия с помощью фильтров. Для примера запустим несколько экземпляров «блокнота» (notepad) и попробуем завершить его разными способами[](http://windowsnotes.ru/wp-content/uploads/2012/01/cmd5.gif)

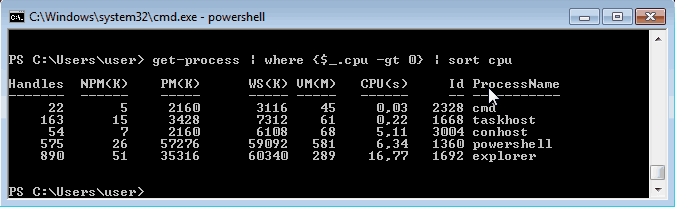
Ключ /f завершает процесс принудительно, а /t завершает все дочерние процессы.

 Полную справку по командам tasklist и taskkill можно получить, введя их с ключом/?

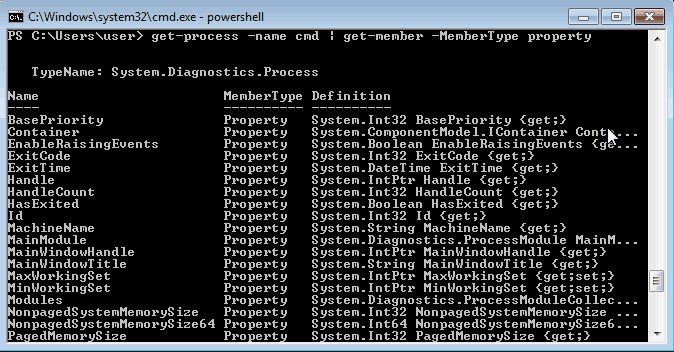
Также можно запустить — PowerShell. Windows PowerShell — расширяемое средство автоматизации от [Microsoft](http://ru.wikipedia.org/wiki/Microsoft), состоящее из [оболочки](http://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D0%BE%D0%BB%D0%BE%D1%87%D0%BA%D0%B0_%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B9_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B) с [интерфейсом командной строки](http://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D1%84%D0%B5%D0%B9%D1%81_%D0%BA%D0%BE%D0%BC%D0%B0%D0%BD%D0%B4%D0%BD%D0%BE%D0%B9_%D1%81%D1%82%D1%80%D0%BE%D0%BA%D0%B8) и сопутствующего [языка сценариев](http://ru.wikipedia.org/wiki/%D0%A1%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B2%D1%8B%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA), задачи обычно выполняются с помощью [командлетов](http://ru.wikipedia.org/w/index.php?title=%D0%9A%D0%BE%D0%BC%D0%B0%D0%BD%D0%B4%D0%BB%D0%B5%D1%82&action=edit&redlink=1) (в оригинале cmdlets), которые являются специализированными [классами](http://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D0%B0%D1%81%D1%81_(%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5)) .NET. Powershell можно запустить не выходя из командной строки. Для управления процессами используем командлет Get-Process

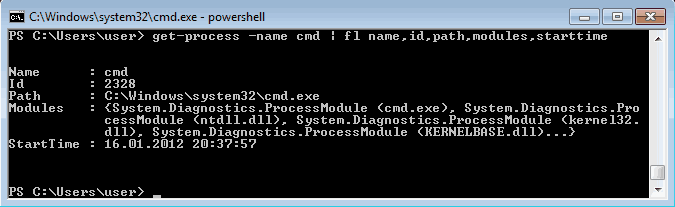
[](http://windowsnotes.ru/wp-content/uploads/2012/01/cmd6.gif)

Чтобы не выводить весь список процессов можем воспользоваться командлетом Where-Object, который задает фильтр для выводимой информации, например с помощью командыget-process | where {$\_.cpu -gt 0} | sort cpu выведем список процессов, которые загружают процессор и отсортируем их по возрастанию нагрузки

[](http://windowsnotes.ru/wp-content/uploads/2012/01/cmd9.gif)

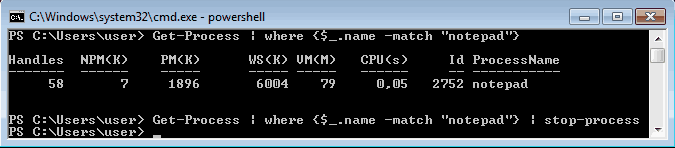
С помощью PowerShell мы можем получить любую информацию о любом процессе. В качестве примера возьмем процесс cmd и выведем список его свойств командой    
get-process -name cmd | get-member -membertype property

[](http://windowsnotes.ru/wp-content/uploads/2012/01/cmd7.gif)

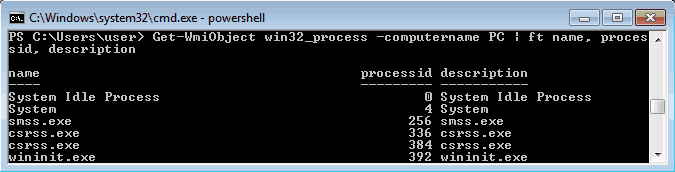
Выбираем те свойства, что нам интересны ( в примере имя и ID процесса, путь к файлу, используемые модули и время запуска) и выводим их в виде списка командой   
get-process -name cmd | format-list name, id, path, modules, starttime [](http://windowsnotes.ru/wp-content/uploads/2012/01/cmd8.gif)

Таким образом мы можем посмотреть когда и кем был запущен процесс, сколько он потребляет ресурсов, где находится исполняемый файл и еще много различной информации.

Для завершения процесса в PowerShell есть командлет Stop-Process. Он завершает указанный процесс по его имени или идентификатору. Однако мы поступим по другому и передадим результат выполнения командлета Get-Process по конвейеру   
get-process | where {$\_.name -match «notepad»}  | stop-process

[](http://windowsnotes.ru/wp-content/uploads/2012/01/cmd10.gif)

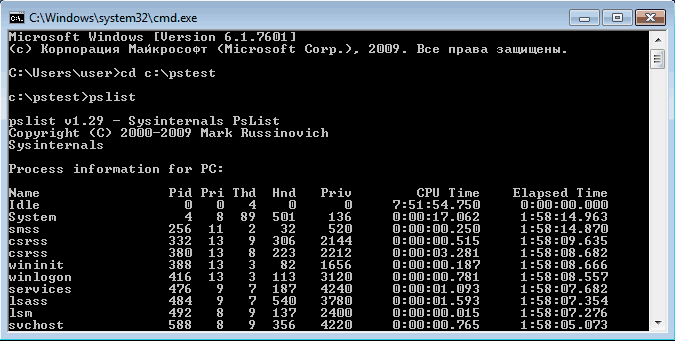
Get-Process не может показать процессы на удаленном компьютере, для этого воспользуемся командлетом Get-WmiObject , например командой Get-WmiObject win32\_process -computername PC | ft name, processid, description смотрим процессы на удаленном компьютере PC

[](http://windowsnotes.ru/wp-content/uploads/2012/01/cmd11.gif)

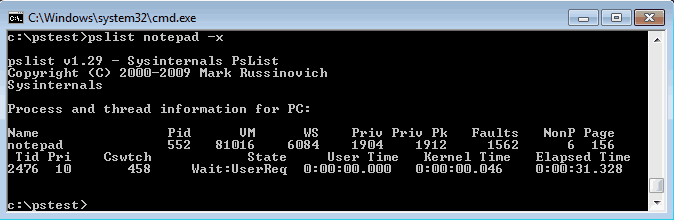
Для боле полного ознакомления с PowerShell можно воспользоваться встроенной справкой, для вызова справки нужно набрать Get-Help «имя командлета»

Рассмотрим еще одно средство для управления процессами из командной строки. Это утилиты Pslist и Pskill входящие в состав пакета [PSTools](http://technet.microsoft.com/ru-ru/sysinternals/bb896649.aspx)от компанииSysinternals.

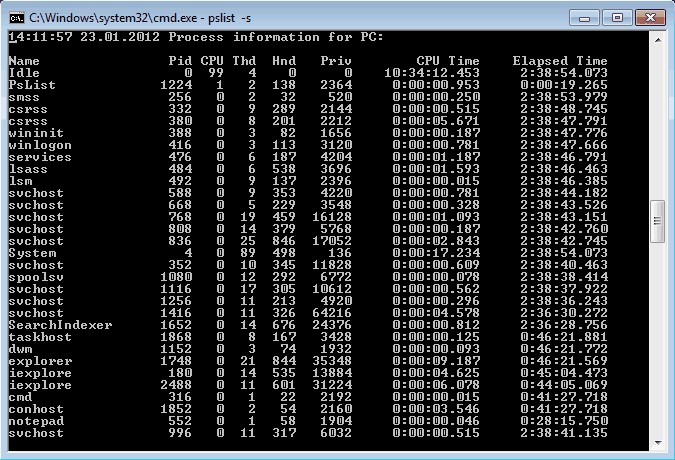
Эти утилиты не требуют специальной установки, достаточно просто скопировать их на диск. Для запуска нужно зайти в папку с утилитами и ввести в командной строке необходимую команду

[](http://windowsnotes.ru/wp-content/uploads/2012/01/cmd12.gif)

Pslist может выводить информацию о процессах по имени или ID, например командой pslist notepad -x выведем подробную информацию например о блокноте

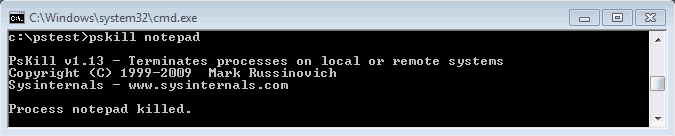
[](http://windowsnotes.ru/wp-content/uploads/2012/01/cmd13.gif)

Особенностью утилиты Pslist является режим task-manager. В  этом режиме информация автоматически обновляется, причем можно задать время работы и интервал обновления. Запускается режим ключом -s , например командой tasklist -s -r 10 запускаем режим программу в режиме task-manager с обновлением раз в 10 сек.

[](http://windowsnotes.ru/wp-content/uploads/2012/01/cmd14.gif)

Завершение процесса программой pskill предельно просто, вводим команду и имя (или ID) процесса и все

|  |
| --- |
| Для каждого приложения, запускаемого под управлением Microsoft Windows, операционная система создает собственную задачу, иными словами, отводит определенный объем оперативной памяти для выполнения этой программы и контролирует работу загруженного в память приложения с ресурсами компьютера. Помимо задач в Windows XP имеются также процессы - виртуальное адресное пространство памяти, отведенное для выполнения программой или самой операционной системой каких-либо процедур. Одна задача может активизировать в Windows несколько различных процессов: например, web-браузер может одновременно обращаться к порту модема для получения и отправки каких-либо данных и отображать на экране результат работы встроенного в web-страницу апплета Java. Каждому процессу автоматически назначается индивидуальный опознавательный номер, так называемый Process ID или PID, предназначенный для однозначной идентификации процесса в системе.  Если запущенная вами программа неожиданно вызвала «зависание» компьютера, в большинстве случаев нет необходимости прибегать к аварийной перезагрузке: вполне достаточно отыскать в памяти вызвавшую сбой задачу и снять ее, то есть принудительно прекратить ее дальнейшее выполнение. Возможна и другая ситуация: закрыв неожиданно «зависшую» программу путем снятия задачи, вы не сможете продолжить прерванную работу с каким-либо файлом или документом. Например, удалив из памяти компьютера Microsoft Word, вы не сможете снова загрузить в него текст, который только что редактировали, поскольку операционная система считает, что этот документ уже используется другой программой. Подобные явления происходят потому, что после снятия задачи в памяти все еще остался инициированный этой задачей процесс - в нашем случае это процесс обработки документа Word. Прекратив выполнение вызывающего сбои процесса, вы сможете продолжить работу с Windows XP в обычном режиме.  Для управления задачами и процессами в Microsoft Windows XP предусмотрена специальная системная утилита, называемая Диспетчер задач (Windows Task Manager), окно которой появляется на экране при нажатии сочетания клавиш Ctrl+Alt+Del  Диспетчер задач Windows  **Рис.** Диспетчер задач Windows  Окно утилиты Диспетчер задач Windows имеет пять функциональных вкладок. Вкладка Приложения (Applications) содержит список всех запущенных в системе задач: в поле Задача (Task) отображается название задачи, в поле Состояние (Status) - ее текущее состояние. Нормальным статусом задачи является состояние Работает (Running). Если задача «зависла» и не отвечает на системные запросы, ее состояние будет определено как Не отвечает (Not responding). Чтобы снять одну из задач, выделите ее щелчком мыши в меню Задача (Task) и нажмите на кнопку Снять задачу (End Task). Чтобы переключиться к какой-либо задаче, то есть открыть на экране ее окно, выделите в списке нужную задачу и щелкните мышью на кнопке Переключиться (Switch To). Вы можете инициировать новую задачу, нажав на кнопку Новая задача (New Task) и указав полное имя и путь к запускаемой программе в соответствующем поле открывшегося окна либо определив эту программу визуально при помощи кнопки Обзор (Browse).  Вкладка Процессы (Processes) дает возможность управлять запущенными в системе процессами.  В меню на данной вкладке отображаются названия процессов - Имя образа (Image Name), определители инициаторов процессов - Имя пользователя (User Name), характеристики аппаратной обработки процессов - ЦП (CPU) и занимаемый процессами объем оперативной памяти - Память (Memory Usage). Вы можете включить отображение других характеристик процессов (например, PID, диапазон ввода-вывода, объем используемого процессом кэша и т. д.), воспользовавшись функцией Выбрать столбцы (Select Columns) командного меню Вид (View). Чтобы прекратить выполнение процесса, выделите его заголовок щелчком мыши и нажмите на кнопку Завершить процесс (End Process). Если вы хотите, чтобы в данном меню отображались процессы, инициированные всеми пользователями вашей системы, установите флажок рядом с пунктом Отображать процессы всех пользователей (Show processes from all users). Вы можете также установить приоритет процесса, если щелкните на его заголовке правой кнопкой мыши, выберите в появившемся меню пункт Приоритет (Set Priority) и укажете назначаемый для данного процесса режим выполнения:   * Реального времени (Realtime)- режим реального времени (все инициируемые процессом запросы выполняются системой по мере поступления); * Высокий (High)- высочайший приоритет; * Выше среднего (AboveNormal)- высокий приоритет; * Средний (Normal)- стандартный приоритет; * Ниже среднего (BelowNormal)- низкий приоритет; * Низкий (Low)- наиболее низкий приоритет.   Чем выше приоритет процесса, тем быстрее выполняются инициированные им запросы. Процессам с высоким приоритетом система предоставляет аппаратные и программные ресурсы в первую очередь. При перераспределении приоритетов процессов следует помнить, что если вы установите высокий приоритет какому-либо второстепенному процессу, приоритет одного из жизненно важных для Windows системных процессов может автоматически стать низким, в результате чего скорость работы системы в целом заметно снизится или выполнение этого процесса будет полностью блокировано, что приведет к «зависанию» компьютера. Устанавливать высокий приоритет одному из процессов следует только в том случае, если его выполнение с «нормальным» приоритетом по каким-то причинам затруднено или невозможно.  Вкладка Быстродействие (Performance) окна Диспетчера задач Windows содержит информацию о загрузке процессора, оперативной памяти и об использовании других аппаратных ресурсов компьютера .  В частности, индикаторы Загрузка ЦП (CPU Usage) и Хронология загрузки ЦП (CPU Usage History) показывают нагрузку на процессор вашего компьютера, индикаторы Файл подкачки (PF Usage) и Хронология использования файла подкачки (PF Usage History) - использование файла подкачки при системном кэшировании данных, индикатор Физическая память (Physical Memory) - степень загрузки оперативной памяти в килобайтах.  Аналогичным образом вкладка Сеть (Networking) демонстрирует нагрузку на вашу локальную сеть. И наконец, если вы хотите просмотреть список всех работающих в настоящее время с вашей системой пользователей, перейдите ко вкладке Пользователи (Users).  Вкладка Быстродействие окна Диспетчер задач Window  **Рис.** Вкладка Быстродействие окна Диспетчер задач Windows  Если вы зарегистрированы в системе как администратор данного компьютера, то можете отключить одного из пользователей, выделив в меню название его сеанса работы с Windows щелчком мыши и нажав на кнопку Отключить (Disconnect). Помимо этого вы можете отправить ему сообщение нажатием на кнопку Отправить сообщение (Send Message). Чтобы завершить текущий сеанс работы с Windows, щелкните мышью на кнопке Выйти из системы (Logoff). |

[](http://windowsnotes.ru/wp-content/uploads/2012/01/cmd15.gif)

 Справку по утилитам Pslist и Pskill можно посмотреть, введя команду с ключом /?

Все манипуляции с процессами необходимо выполнять с правами администратора, для этого командную строку требуется запускать с повышением привилегий.

Оформите отчет, сделайте выводы по работе.

Содержание отчета

1. Номер и тема практической работы;
2. Цель работы;
3. Необходимые оборудование;
4. Ход выполнения практической работы (этапы);
5. Выводы по выполненной работе.

Контрольные вопросы

1. Что такое процесс?
2. Каким образом можно вывести все процессы из командной строки?

**Практическая работа № 9**

Сканирование сети на наличие уязвимостей

***Цель***

Получение практических навыков управления сетевыми подключениями, средствами встроенных утилит, стороннего программного обеспечения.

***Задание****:*

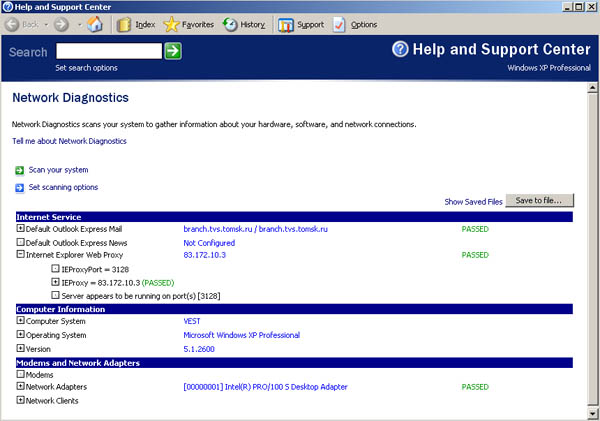
1. Проверьте работоспособность сетевого подключения с помощью встроенных утилит Windows XP
2. Создайте профиль для сканирования Моѐ сканирование
3. Укажите свой диапазон адресов
4. Просканируйте сеть
5. Ответьте на контрольные вопросы в тетради
6. Оформите отчет.

### Диагностика IP-протокола

### Проверка работоспособности сетевого подключения

**Теоретическая часть:** Существуют различные утилиты, позволяющие быстро продиагностировать IP-подключение. Однако большинство операций легко может быть выполнено с использованием команд самой операционной системы.

Пользователи Windows XP для диагностики сетевого подключения могут воспользоваться специальным мастером. Эта программа вызывается из меню задачи *Сведения о системе* (*Пуск > Все программы > Стандартные > Служебные > Сведения о системе > меню Сервис > Диагностика сети*):



В ходе выполнения лабораторной работы Вы познакомитесь с утилитами, запускаемыми из командной строки, позволяющими детально продиагностировать работоспособность подключения Вашего компьютера к сети.

**Ход работы:**

**Ipconfig**

Для отображения параметров IP-протокола используются утилиты *ipconfig* (Windows NT/2000/XP) и *winipcfg* (Windows 9x). Эта утилита выводит на экран основные параметры настройки протокола TCP/IP: значения адреса, маски, шлюза.

1. Нажмите кнопку *Пуск*, выберите строку меню *Выполнить*, наберите символы cmd и нажмите клавишу *Enter* на клавиатуре.
2. В открывшемся окне наберите *ipconfig /all*. При нормальной работе компьютера на экран должен вывестись примерно такой листинг:

Windows IP Configuration

Host Name . . . . . . . . . . . . : vest

Primary Dns Suffix . . . . . . . : tvs.tomsk.ru

Node Type . . . . . . . . . . . . : Hybrid

IP Routing Enabled. . . . . . . . : No

WINS Proxy Enabled. . . . . . . . : No

DNS Suffix Search List. . . . . . : tvs.tomsk.ru

tomsk.ru

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : tvs.tomsk.ru

Description . . . . . . . . . . . : Intel(R) PRO/100 S Desktop Adapter

Physical Address. . . . . . . . . : 00-02-B3-8D-44-53

Dhcp Enabled. . . . . . . . . . . : Yes

Autoconfiguration Enabled . . . . : Yes

IP Address. . . . . . . . . . . . : 83.172.10.54

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Default Gateway . . . . . . . . . : 83.172.10.254

DHCP Server . . . . . . . . . . . : 83.172.10.2

DNS Servers . . . . . . . . . . . : 192.168.0.1

83.172.10.2

Primary WINS Server . . . . . . . : 83.172.10.2

Secondary WINS Server . . . . . . : 213.183.109.3

Lease Obtained. . . . . . . . . . : 24 августа 2004 г. 9:40:41

Lease Expires . . . . . . . . . . : 27 октября 2004 г. 9:40:41

Отключите сетевое подключение, повторите команду. При отсутствующем соединении на экран выводится примерно такой листинг:

Windows IP Configuration

Host Name . . . . . . . . . . . . : vest

Primary Dns Suffix . . . . . . . : tvs.tomsk.ru

Node Type . . . . . . . . . . . . : Hybrid

IP Routing Enabled. . . . . . . . : No

WINS Proxy Enabled. . . . . . . . : No

DNS Suffix Search List. . . . . . : tvs.tomsk.ru

tomsk.ru

Ethernet adapter Local Area Connection:

Media State . . . . . . . . . . . : Media disconnected

Description . . . . . . . . . . . : Intel(R) PRO/100 S Desktop Adapter

Physical Address. . . . . . . . . : 00-02-B3-8D-44-53

Обратите внимание, что программа вывела на экран только данные о "физических" параметрах сетевой карты и указала, что отсутствует подключение сетевого кабеля (*Media disconnected*).

**Ping**

Команда используется для проверки протокола TCP/IP и достижимости удаленного компьютера. Она выводит на экран время, за которое пакеты данных достигают заданного в ее параметрах компьютера.

1. Проверка правильности установки протокола TCP/IP. Откройте командную строку и выполните команду:

ping 127.0.0.1

Адрес 127.0.0.1 — это личный адрес любого компьютера. Таким образом, эта команда проверяет прохождение сигнала "на самого себя". Она может быть выполнена без наличия какого-либо сетевого подключения. Вы должны увидеть приблизительно следующие строки:

Pinging 127.0.0.1 with 32 bytes of data:

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

По умолчанию команда посылает пакет 32 байта. Размер пакета может быть увеличен до 65 кбайт. Так можно обнаружить ошибки при пересылке пакетов больших размеров. За размером тестового пакета отображается время отклика удаленной системы (в нашем случае — меньше 1 миллисекунды). Потом показывается еще один параметр протокола — значение TTL. TTL — "время жизни" пакета. На практике это число маршрутизаторов, через которые может пройти пакет. каждый маршрутизатор уменьшает значение TTL на единицу. При достижении нулевого значения пакет уничтожается. Такой механизм введен для исключения случаев зацикливания пакетов.

Если будет показано сообщение о недостижимости адресата, то это означает ошибку установки протокола IP. В этом случае целесообразно удалить протокол из системы, перезагрузить компьютер и вновь установить поддержку протокола TCP/IP.

1. Проверка видимости локального компьютера и ближайшего компьютера сети. Выполните команду

ping 192.168.0.19

На экран должны быть выведены примерно такие строки:

Pinging 212.73.124.100 with 32 bytes of data:

Reply from 192.168.0.19: bytes=32 time=5ms TTL=60

Reply from 192.168.0.19: bytes=32 time=5ms TTL=60

Reply from 192.168.0.19: bytes=32 time=4ms TTL=60

Reply from 192.168.0.19: bytes=32 time=4ms TTL=60

Ping statistics for 212.73.124.100:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 4ms, Maximum = 5ms, Average = 4ms

Наличие отклика свидетельствует о том, что канал связи установлен и работает.

**Tracert**

При работе в Сети одни информационные серверы откликаются быстрее, другие медленнее, бывают случаи недостижимости желаемого хоста. Для выяснения причин подобных ситуаций можно использовать специальные утилиты.

Например, команда *tracert*, которая обычно используется для показа пути прохождения сигнала до желаемого хоста. Зачастую это позволяет выяснить причины плохой работоспособности канала. Точка, после которой время отклика резко увеличено, свидетельствует о наличии в этом месте "узкого горлышка", не справляющегося с нагрузкой.

1. В командной строке введите команду:

tracert 192.168.0.19

Вы должны увидеть примерно такой листинг:

Tracing route to 192.168.0.19

over a maximum of 30 hops:

1 <1 ms <1 ms <1 ms 192.168.0.19

Trace complete.

**Route**

Команда **Route** позволяет просматривать маршруты прохождения сетевых пакетов при передаче информации.

1. Выведите на экран таблицу маршрутов TCP/IP, для этого в командной строке введите команду **route print**.

**Net view**

Выводит список доменов, компьютеров или общих ресурсов на данном компьютере. Вызванная без параметров, команда **net view** выводит список компьютеров в текущем домене.

1. В командной строке введите команду **net view** и вы увидите список компьютеров своей рабочей группы.
2. В командной строке введите команду **net view \\192.168.0.250**  для просмотра общих ресурсов расположенных на компьютере **192.168.0.250**
3. **Сканирование локальной сети с программой LanSurfer**

**Задание для самостоятельной работы**

**1. Создайте профиль для сканирования Моѐ сканирование**

**2. Укажите свой диапазон адресов**

**3. Просканируйте сеть**

Краткие теоретические сведения

LanSurfer предназначен для:

1. быстрого многопоточного сканирования компьютеров, расшаренных папок и серверов в локальной сети и составления списка сети, содержащего исчерпывающую информацию и компьютерах и ресурсах сети.

2. открытия ресурсов сети указанными пользователем приложениями.

3. вывода ресурсов сети, сходных по содержанию, вместе. (напр. видео или аудио папки)

4. быстрого многопоточного поиска файлов/папок в локальной сети (доступен расширенный поиск)

5. управления локальными расшаренными папками (на своем компьютере)

6. мониторинга и управления подключениями к локальным расшаренным папкам Полностью настраиваемый интерфейс с многоязычной поддержкой (с русским). Для удобной работы широко используются профили (для хранения настроек). Например, можно создать профили сети, сканирования, поиска один раз и потом одним кликом переключаться между ними.

**Порядок выполнения работы**

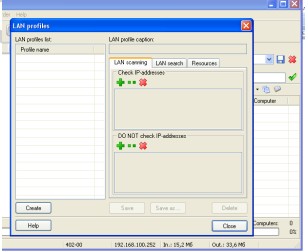
1. Установите программу LanSurfer;

2. После установки запустите программу.

3. Создайте LANprofiles. Для этого выберите пункт меню Options



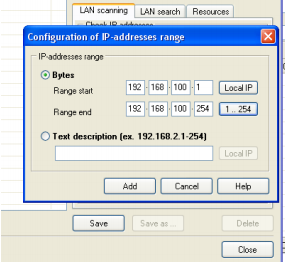
4. В раскрывшемся окне выберите пункт LANprofiles



5. Щелкните мышкой по кнопке Greate

6. Вверху справа активируется строка ввода диапазона адресов для сканирования.7. Щелкните кнопкой мыши по зеленому плюсу

8. Появиться окно, в котором необходимо ввести начальный IP-адрес и последний адрес диапазона IP-адресов



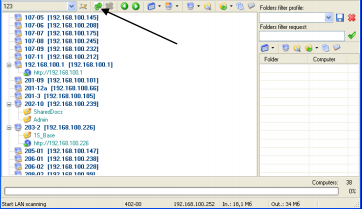
9. Введите диапазон адресов вручную или используя кнопки Local IP или 1..254

10. Нажмите кнопку ADD

11. Вверху в пункте Lanprofile caption введите имя вашего профиля и нажмите Save

12. После этого выйдите из режима настройки профиля нажав кнопку Close

13. Выполните сканирование сети. Для этого нажмите кнопку StartLanScaning



14. После сканирования на экран выведется список ПК, серверов, маршрутизаторов, общедоступных папок.

Оформите отчет, сделайте выводы по работе.

Содержание отчета

1. Номер и тема практической работы;
2. Цель работы;
3. Необходимые оборудование;
4. Ход выполнения практической работы (этапы);
5. Выводы по выполненной работе.

Контрольные вопросы

1. Перечислите основные консольные утилиты проверки сетевых подключений, перечислите их основные функции.
2. Перечислите основные функции программы сканирования сети LanSurfer.

# Учебно-методическое и информационное обеспечение дисциплины (ПМ)

**1. Основная литература**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Наименование | Авторы | Место издания | Год издания | Наличие | |
| в библиотеке, экз | в ЭБС, адрес в сети Интернет |
| 1. | Методы и средства защиты информации в компьютерных системах | Хорев П. Б. | М.: Академия | 2010 |  | + |
| 2. | Информационная безопасность: 3-е издание | Мельников В.П. | М.: Академия | 2010 |  | + |
| 3. | Программно-аппаратная защита информации: учебное пособие | Хорев П.Б. | М.: Форум | 2009 |  | + |

**2. Дополнительная литература**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Наименование | Авторы | Место издания | Год издания | Наличие | |
| в научно-технической библиотеке, экз | в ЭБС, адрес в сети Интернет |
| 1. | Комплексная система защиты информации на предприятии | Гришина Н. В. | М.: Форум | 2009 |  | + |
| 2. | Защита информации в персональном компьютере: учебное пособие | Емельянова Н.З., Партыка Т.Л., Попов И.И. | М.: Форум | 2009 |  |  |
| 3. | Основы информационной безопасности: учебное пособие | Галатенко В.А. | Интернет-Университет Информационных Технологий, www.intuit.ru | 2010 |  |  |