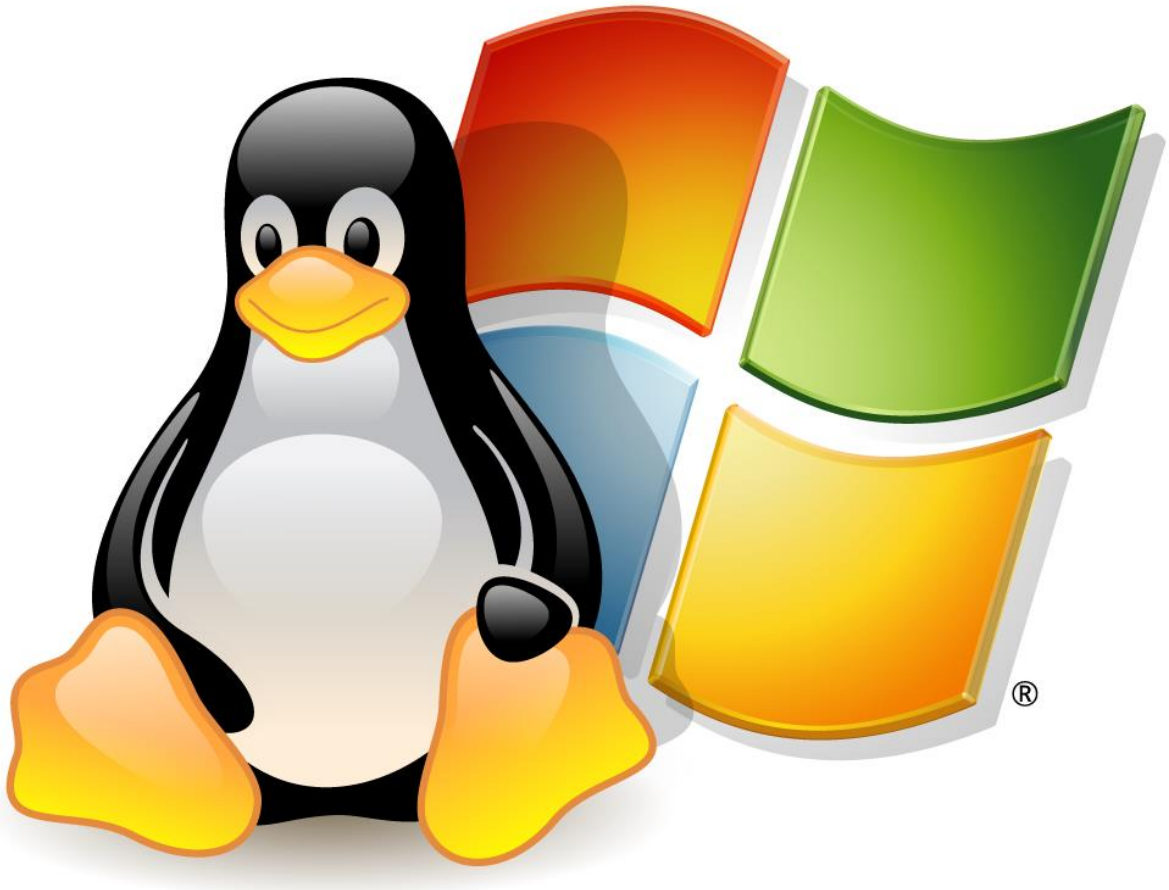
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

Д.О. Пахмурин

ОПЕРАЦИОННЫЕ СИСТЕМЫ ЭВМ

Учебно-методическое пособие к практическим занятиям



Томск – 2015

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

Кафедра промышленной электроники

Д.О. Пахмурин

ОПЕРАЦИОННЫЕ СИСТЕМЫ ЭВМ

Учебно-методическое пособие
к практическим занятиям для студентов
очно-заочной формы обучения по направлению
11.03.04 – Электроника и наноэлектроника
(профиль "Промышленная электроника")

2015

Пахмурин Д.О.
Операционные системы ЭВМ: Учебно-методическое пособие к практическим занятиям. – Томск: Томский государственный университет систем управления и радиоэлектроники, 2015. – 55 с.

Приведены методические указания для выполнения практических занятий по дисциплине "Операционные системы ЭВМ", определена тематика и порядок их выполнения.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Данные методические указания являются дополнением к учебному пособию "Операционные системы ЭВМ" для студентов очно-заочной формы обучения. Они являются необходимыми для практической подготовки современного инженера к деятельности по администрированию операционных систем.

Целью методических указаний является познакомить студентов с основными моментами в управлении операционными системами и привитие им соответствующих практических знаний в сфере компьютерных технологий. В современном мире без достаточно полноценного обучения работе с информацией, с принципами функционирования компьютерного оборудования не возможна качественная разработка каких-либо серьезных технических проектов.

Более глубокие практические знания будут даны студентам в рамках лабораторных работ, руководство по выполнению которых будет издано в виде отдельного учебно-методического пособия в ближайшее время.

1. Виртуальная машина. Настройка сетевого интерфейса. Основные сетевые команды. Работа с протоколом TCP/IP в ОС Windows XP.

Цель работы: Изучить основные сетевые команды и принципы работы с протоколом TCP/IP в ОС Windows XP.

1.1. Краткие теоретические сведения

1.1.1. Виртуальная машина

Технология виртуализации предназначена для осуществления возможности одновременного запуска на одном компьютере нескольких (в том числе, различных) ОС. Это позволяет пользователям (и/или системным администраторам) иметь ряд преимуществ при одновременной работе в альтернативных средах без перезапуска самого компьютера. Причем, работая с альтернативной ОС, пользователь не чувствует никаких ограничений в использовании ее возможностей, получая полную иллюзию работы с реальной системой. При этом в такой системе имеется возможность выполнять различные малоизученные или потенциально опасные для нее операции, не беспокоясь о последствиях: поскольку система является виртуальной, ее крах или частичное повреждение не скажется на работе реальной ОС.

Основные преимущества такого подхода состоят в следующем:

– появляется возможность инсталляции на одном компьютере нескольких ОС без необходимости соответствующего конфигурирования физических жестких дисков;

– можно осуществлять работу с несколькими ОС одновременно с динамическим переключением между ними без перезагрузки реальной системы;

– сокращается время изменения состава и конфигурации установленных виртуальных ОС;

– осуществляется изоляция реального оборудования от нежелательного воздействия программного обеспечения, работающего в среде виртуальной ОС;

– появляется возможность моделирования вычислительной сети на единственном автономном компьютере.

Благодаря этим преимуществам существенно расширяется круг задач, которые можно решать без перезагрузки системы и без опасения нанести ей какой-либо ущерб. Основные из них:

– освоение новой, альтернативной ОС;

– запуск специализированных приложений, предназначенных для работы в среде конкретной ОС;

– тестирование одного приложения под управлением различных ОС;

– установка и удаление оценочных или демонстрационных версий новых приложений;

– тестирование потенциально опасного программного обеспечения, относительно которого имеется подозрение на вирусное заражение;

– управление правами доступа пользователей к данным и программам в пределах виртуальной среды.

Все сказанное выше реализуется посредством применения специализированных инструментов, позволяющих организовывать виртуальную вычислительную среду. Иными словами, этот класс приложений ориентирован на развертывание, так называемых, виртуальных машин.

С точки зрения пользователя, *виртуальная машина* (ВМ) – это конкретный экземпляр некой виртуальной вычислительной среды ("виртуального компьютера"), созданный с помощью специального программного инструмента. Обычно такие инструменты позволяют создавать и запускать произвольное число виртуальных машин, ограничиваемое лишь физическими ресурсами реального компьютера.

Собственно инструмент для создания ВМ (его иногда называют *приложением виртуальных машин*) – это обычное приложение, устанавливаемое, как и любое другое, в рамках реальной ОС, именуемой *хостовой* или *ведущей*.

В рамках ВМ пользователь устанавливает, как и на реальном компьютере, нужную ему ОС. Такая ОС, принадлежащая конкретной ВМ, называется *гостевой*. Перечень поддерживаемых гостевых ОС является одной из наиболее важных характеристик ВМ. Наиболее мощные из современных ВМ обеспечивают поддержку более десятка популярных версий ОС семейств Windows, Linux и MacOS.

Виртуальные машины могут быть построены на базе различных платформ и при помощи разных технологий. Используемая схема виртуализации зависит как от аппаратной платформы, так и от особенностей взаимодействия *хостовой* и поддерживаемых *гостевых* ОС. Некоторые архитектуры обеспечивают возможность виртуализации на аппаратном уровне, другие, напротив, требуют применения дополнительных программных средств.

В настоящее время наибольшее распространение получили три схемы виртуализации:

– эмуляция API гостевой ОС;

– полная эмуляция гостевой ОС;

– квазиэмуляция гостевой ОС

В первом случае, приложение работает в изолированном адресном пространстве и взаимодействует с оборудованием при помощи интерфейса прикладного программирования API, предоставляемого *хостовой* ОС. Если две ОС совместимы по интерфейсу API (например, Windows 98 и Windows ME), то приложение, разработанное для одной из них, будет работать и на другой. Если, напротив, две ОС несовместимы по интерфейсу API (Windows 2000 и Linux), то необходимо обеспечить перехват обращений приложений к API *гостевой* ОС и имитировать ее поведение средствами *хостовой*. При таком подходе можно установить одну ОС и работать одновременно как с ее приложениями, так и с приложениями альтернативной ОС.

Поскольку весь код приложения исполняется без эмуляции, а эмулируются лишь вызовы API, такая схема виртуализации приводит к незначительной потере в производительности ВМ. Однако, из-за того, что многие приложения используют недокументированные функции API или обращаются к ОС в обход API, даже очень мощные эмуляторы API имеют проблемы совместимости и позволяют запускать не более 70% от общего числа приложений. Кроме того, поддерживать эмуляцию API бурно развивающейся системы, типа Windows, очень нелегко, и большинство эмуляторов API так и остаются эмуляторами какой-то конкретной версии ОС.

Примеры продуктов, выполненных по данной технологии:

– проект Wine, позволяющий запускать DOS-, Win16- и Win32-приложения под управлением ОС Linux и ОС Unix;

– продукт Win4Lin компании Netraverse, позволяющий запускать ОС семейства Windows под управлением ОС Linux:

– проект DOSEMU, позволяющий запускать DOS-приложения под управлением ОС Linux;

– проект UML, позволяющий запускать несколько копий ОС Linux на одном компьютере;

– российский проект Virtuozzo, также позволяющий запускать несколько копий ОС Linux на одном компьютере.

Второй случай – это проекты, поддерживающие технологию полной эмуляции, работают по принципу интерпретации инструкций системы команд *гостевой* ОС. Поскольку при этом полностью эмулируется поведение как центрального процессора, так и всех внешних устройств, то существует возможность эмулировать компьютер с архитектурой Intel x86 на компьютерах с совершенно другой архитектурой, например на рабочих станциях Mac или на серверах Sun, реализуемых на RISC-процессорах.

Главный недостаток полной эмуляции заключается в существенной потере производительности *гостевой* ОС. Поэтому до недавнего времени ВМ с полной эмуляцией чаще всего использовались в качестве низкоуровневых отладчиков для исследования и трассировки ОС. Однако благодаря значительному росту вычислительной мощности в последнее время этот недостаток становится все менее значимым. Наиболее яркий представитель этого вида ВМ – продукт Virtual PC от Microsoft. В качестве других примеров можно привести:

– проект Bochs, позволяющий запускать различные ОС, ориентиро-ванные на архитектуру Intel x86, под ОС Linux, Windows и Mac OS;

– продукт Simics, позволяющий запускать различные ОС архитектуры Intel x86 под управлением ОС семейства Windows и других ОС;

– проект Qemu – эмулятор различных архитектур на компьютере.

Технология квазиэмуляции *гостевой* ОС основана на том обстоятельстве, что далеко не все инструкции *гостевой* ОС нуждаются в прямой эмуляции средствами *хостовой* ОС. Многие из инструкций, необходимых для корректной работы *гостевых* приложений, могут быть непосредственно адресованы *хостовой* ОС. Исключение составляют инструкции для управления, например, такими устройствами, как видеокарта, некоторые контроллеры, таймер.

Таким образом, в процессе работы ВМ с квазиэмуляцией происходит выборочная эмуляция инструкций *гостевой* ОС. Очевидно, что производительность такой ВМ должна быть выше, чем в предыдущем случае.

Примеры проектов, выполненных по технологии квазиэмуляции:

– технология Virtual Platform, на базе которой компания VMware предлагает ряд продуктов, в том числе приложение для рабочих станций VMware Workstation;

– российские продукты Serenity Virtual Station и Parallels Workstation от компании Параллели (англ. Parallels);

– проект Plex86, позволяющий запускать различные ОС архитектуры Intel x86 под управлением ОС Linux.

– проект L4Ka, использующий микроядерную архитектуру ОС;

– проект Xen, позволяющий запускать модифицированные ОС Linux, FreeBSD, NetBSD и Windows XP под управлением ОС Linux, FreeBSD, NetBSD, а также, при соблюдении некоторых условий, обеспечивающий даже прирост производительности.

В рамках практических и лабораторных работ дальнейшее изучение технологии виртуализации будет реализовано на примере Microsoft Virtual PC.

Перечень *гостевых* ОС, которые могут быть установлены с применением продуктов семейства VMware, охватывает только операционные системы семейства Windows – начиная с Windows 98 и закан-чивая Windows Vista, а также серверные операционные системы Windows Server 2003 и 2008.

В качестве *хостовой* ОС могут использоваться также только ОС из семейства Windows: Windows 2000 Professional, Windows 2000 Server и Advanced Server, Windows XP (Home или Professional), семейства Windows Server 2003 и Windows Server 2008.

1.1.2. Настройка сетевого интерфейса. Основные сетевые команды

TCP/IP (Transmission Control Protocol / Internet Protocol) является самым популярным сетевым протоколом, служащим основой глобальной сети Интернет. Предлагаемые им средства маршрутизации обеспечивают максимальную гибкость функционирования локальных сетей предприятий. В ОС Windows XP протокол **TCP/IP** устанавливается автоматически. В сетях протокола **TCP/IP** каждому клиенту должен быть назначен соответствующий **IP**-адрес, представляющий собой 32-разрядное число, разделенное точками (например, 192.168.1.255). Кроме того, клиенту может потребоваться служба имен или алгоритм разрешения имен. В комплект протокола **TCP/IP** входят служебные программы **FTP** (File Transfer Protocol) и **Telnet**. **FTP** – это приложение с текстовым интерфейсом, позволяющее подключаться к FTP-серверам и передавать файлы. **Telnet** обладает графическим интерфейсом и позволяет входить на удаленный компьютер и выполнять команды так же, как если бы пользователь находился за клавиатурой этого компьютера.

В стеке TCP/IP используются три типа адресов: **локальные** (называемые также **аппаратными**), **IP-адреса** и **символьные доменные** имена.

В терминологии TCP/IP под **локальным адресом** понимается такой тип адреса, который используется средствами базовой технологии для доставки данных в пределах подсети, являющейся элементом составной интерсети. В разных подсетях допустимы разные сетевые технологии, разные стеки протоколов, поэтому при создании стека TCP/IP предполагалось наличие разных типов локальных адресов. Если подсетью интерсети является локальная сеть, то локальный адрес – это **MAC-адрес**. MAC-адрес назначается сетевым адаптерам и сетевым интерфейсам маршрутизаторов. MAC-адреса назначаются производителями оборудования и являются уникальными, так как управляются централизованно. Для всех существующих технологий локальных сетей MAC-адрес имеет формат 6 байт, например 11-A0-17-3D-BC-01. Однако протокол IP может работать и над протоколами более высокого уровня, например над протоколом IPX или X.25. В этом случае локальными адресами для протокола IP соответственно будут адреса IPX и X.25. Следует учесть, что компьютер в локальной сети может иметь несколько локальных адресов даже при одном сетевом адаптере. Некоторые сетевые устройства не имеют локальных адресов. Например, к таким устройствам относятся глобальные порты маршрутизаторов, предназначенные для соединений типа "точка-точка".

IP-адреса представляют собой основной тип адресов, на основании которых сетевой уровень передает пакеты между сетями. Эти адреса состоят из 4 байт, например 109.26.17.100. IP-адрес назначается администратором во время конфигурирования компьютеров и маршрутизаторов. IP-адрес состоит из двух частей: номера сети и номера узла. Номер сети может быть выбран администратором произвольно, либо назначен по рекомендации специального подразделения Internet (Internet Network Information Center, InterNIC), если сеть должна работать как составная часть Internet. Обычно поставщики услуг Internet получают диапазоны адресов у подразделений InterNIC, а затем распределяют их между своими абонентами. Номер узла в протоколе IP назначается независимо от локального адреса узла. Маршрутизатор по определению входит сразу в несколько сетей. Поэтому каждый порт маршрутизатора имеет собственный IP-адрес. Конечный узел также может входить в несколько IP-сетей. В этом случае компьютер должен иметь несколько IP-адресов, по числу сетевых связей. Таким образом, IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

Символьные доменные имена. Символьные имена в IP-сетях называются доменными и строятся по иерархическому признаку. Составляющие полного символьного имени в IP-сетях разделяются точкой и перечисляются в следующем порядке: сначала простое имя конечного узла, затем имя группы узлов (например, имя организации), затем имя более крупной группы (поддомена) и так до имени домена самого высокого уровня (например, домена объединяющего организации по географическому принципу: RU - Россия, UK - Великобритания, US - США), Примеров доменного имени может служить имя base2.sales.zil.ru. Между доменным именем и IP-адресом узла нет никакого алгоритмического соответствия, поэтому необходимо использовать какие-то дополнительные таблицы или службы, чтобы узел сети однозначно определялся как по доменному имени, так и по IP-адресу. В сетях TCP/IP используется специальная распределенная служба Domain Name System (**DNS**), которая устанавливает это соответствие на основании создаваемых администраторами сети таблиц соответствия. Поэтому доменные имена называют также **DNS-именами**.

Для выделения в IP-адресах адресов сети и адресов узла применяется **маска подсети**. *Маска* – это число, которое используется в паре с IP-адресом; двоичная запись маски содержит единицы в тех разрядах, которые должны в IP-адресе интерпретироваться как номер сети. Поскольку номер сети является цельной частью адреса, единицы в маске также должны представлять непрерывную последовательность.

В масках количество единиц в последовательности, определяющей границу номера сети, не обязательно должно быть кратным 8, чтобы повторять деление адреса на байты. Пусть, например, для IP-адреса 129.64.134.5 указана маска 255.255.128.0, то есть в двоичном виде:

IP-адрес 129.64.134.5 - 10000001. 01000000.10000110. 00000101

Маска 255.255.128.0 - 11111111.11111111.10000000. 00000000

То есть в десятичной форме записи - номер сети 129.64.128.0, а номер узла 0.0.6.5.

Механизм масок широко распространен в IP-маршрутизации, причем маски могут использоваться для самых разных целей. С их помощью администратор может структурировать свою сеть, не требуя от поставщика услуг дополнительных номеров сетей. На основе этого же механизма поставщики услуг могут объединять адресные пространства нескольких сетей путем введения так называемых

"префиксов" с целью уменьшения объема таблиц маршрутизации и повышения за счет этого производительности маршрутизаторов.

1.1.3. Работа с протоколом TCP/IP в ОС Windows XP

Служебные программы и утилиты протокола **TCP/IP** обеспечивают подключение к различным современным сетям. При этом чтобы использовать эти утилиты, на компьютере должна быть установлена поддержка протокола **TCP/IP**. К числу поддерживаемых протоколом **TCP/IP** служебных команд и утилит относятся следующие: **Finger, Ping, Ftp, Rcp, Hostname, Rexec, Ipconfig, Route, Lpq, Rsh, Lpr, Tftp, Nbtstat, Tracert, Netstat, Getmac,** а также целый ряд команд с приставкой **Net [accounts | computer | config | continue | file | group | help | helpmsg | localgroup | name | pause | print | send | session | share | start | statistics | stop | time | use | user | view]** и другие**.** Дополнительные сведения о запуске служб **TCP\IP** из командной строки находятся в разделе **Net start**.

В настоящей практической работе предполагается ознакомление с основным набором команд протокола **TCP/IP** и выполнение нескольких учебных заданий с применением командной оболочки.

1.2. Порядок выполнения практической работы

На данном занятии вам необходимо будет осуществить настройку Microsoft Virtual PC на работу с виртуальной машиной, на которой будет эмулирована Windows XP Professional sp3. Эта операционная система сейчас остается самой востребованной в мире и в России, хотя ее догоняет Windows 7.

Ваша работа будет заключаться в следующем. Запустив ярлык Virtual PC, необходимо выбрать создать новую виртуальную машину (**New…**). При этом необходимо выбрать уже имеющуюся виртуальную машину, расположенную в папке C:\Documents and Settings\student\OS.

После того, как новая виртуальная машина подключена, необходимо осуществить ее настройку – подключить два диска. В левом окне диалога настройки выбираем **Hard Disc 1**. В правом окне жмем кнопку **Brose**. Выбираем файл виртуального диска (**WinXPsp3.vhd**), расположенный в той же папке, что и сама виртуальная машина. Повторяем эту операцию для второго диска (файл **WinXPsp3_Disc_D.vhd**). После этого запускаем вновь созданную ВМ. При старте ВМ в окне будет отображаться процесс, аналогичный запуску компьютере. Чтобы

переключиться в полноэкранный режим, необходимо нажать одновременно правую кнопку **ALT и Enter**.

После завершения запуска ОС необходимо выполнить следующие действия:

1. Установить разрешение экрана 1024x768 пикселей;
2. Вызвать свойства сетевого окружения (щелчок правой кнопкой "мыши" на ярлыке "Сетевое окружение" – "Свойства").
3. На закладке "Общие" выбираем **Internet Protocol (TCP/IP)** – "Свойства" и задать следующие параметры сетевого интерфейса:

IP-адрес:	192.168.220.20*№варианта*
Маска подсети:	255.255.255.0
Шлюз по умолчанию:	192.168.220.2
DNS-серверы:	192.168.220.10
	192.168.220.11

4. Подтвердить выполненные настройки.
5. Выполнить проверку настроек. Для этого необходимо проделать следующее:

– запустить консоль командной строки;

– изучить синтаксис команды **ipconfig**;

– выполнить проверку настроек, выписав локальный адрес (адрес физической машины) и IP-адрес виртуальной машины.

6. Выполнить проверку связи с другими узлами. Для этого необходимо проделать следующее:

– запустить консоль командной строки (если после выполнения предыдущего пункта консоль была закрыта);

– изучить синтаксис команды **ping**;

– выполнить проверку связи с физической локальной машиной, используя ip-адреса узлов.

7. Исследовать содержимое кэша **ARP**. Для этого в окне командной оболочки выполните следующие действия:

– наберите команду **Arp** с необходимыми ключами;

– нажмите **Enter** для ввода;

– самостоятельно осуществите добавление в кэш **ARP** статической записи со следующими параметрами:

ip-адрес 192.168.220.13,

MAC-адрес 00-04-23-e2-ac-a7;

– повторно исследуйте содержимое кэша **ARP**,

8. Вывести список интерфейсов и их индексов. Для этого в окне командной оболочки выполните следующие действия:

– наберите команду **Route** с необходимыми ключами,

– нажмите **Enter** для ввода,

9. Проверить наличие соединения с узлом сети по заданному **IP**-адресу или имени узла. Для этого в окне командной оболочки выполните следующие действия:

– наберите команду **Ping** с необходимыми ключами согласно условиям:

число отправляемых сообщений с эхо-запросом – 10,

длина поля данных – 4096 байт;

– нажав **Enter** для ввода, проверьте наличие соединения с узлом сети, имеющего:

IP-адрес петли обратной связи,

IP-адрес собственного узла пользователя,

IP-адрес основного шлюза (по умолчанию),

IP-адрес сайта www.mail.ru,

10. Выполнить трассировку маршрута до определенной точки назначения, заданной **IP**-адресом или именем узла. Исследовать статистику переходов и потерь **TCP/IP**-пакетов в процессе трассировки. Для этого в окне командной оболочки выполните следующие действия:

– наберите команду **Tracert** с необходимыми ключами,

– нажав **Enter** для ввода, выполните трассировку маршрута, имеющего:

IP-адрес шлюза (маршрутизатора) внешнего сетевого интерфейса,

IP-адрес физического локального узла,

имя удаленного узла внешней сети, принадлежащего томскому сегменту сети Интернет,

– наберите команду **Pathping** с необходимыми ключами,

– нажав **Enter** для ввода, выполните трассировку маршрута, имеющего тот же **IP**-адрес или имя удаленного узла внешней сети, принадлежащего томскому сегменту сети Интернет,

11. Исследовать статистические данные **TCP/IP**-подключений с помощью команды **Netstat** на конкретных примерах:

а) Выведите **Ethernet** статистику**.**

б) Выведите статистику по всем активным протоколам.

в) Выведите статистику только по **TCP**-протоколу.

г) Выводите статистику всех активных **TCP/IP**-подключений и **PID**-кодов процессов каждые 10 секунд.

12. Изучить статистику протокола и текущих соединений **TCP/IP** с использованием **NetBIOS over TCP/IP** на конкретных примерах:

а) Выведите таблицу имен **NetBIOS** физической рабочей станции;

б) Отобразите содержимое кэша имен **NetBIOS** собственного узла пользователя.

в) Выводите статистику сеанса **NetBIOS** по **IP**-адресу удаленного узла сети (192.168.220.13) через каждые 15 секунд.

В настоящей практической работе были рассмотрены команды и служебные утилиты, позволяющие посредством командного интерпретатора иметь доступ к основным функциям протокола **TCP/IP** с целью тестирования сетевого оборудования, взаимодействия узлов (маршрутизаторов) в сети, а также настройки программного обеспечения для обеспечения коммутации компьютеров в глобальной сети Интернет. Основным преимуществом данного набора команд является их универсальность в применении, а их принадлежность к протоколу **TCP/IP** обеспечивет возможность взаимной связи различного сетевого оборудования и компьютеров с разными операционными системами. Изученные команды и утилиты являются базовыми инструментами системного администратора и специалиста в области информационных технологий. Эти знания являются необходимыми в развивающихся условиях современного информационного пространства. Они создают основу для дальнейшего изучения принципов сетевого взаимодействия и развития навыков в области обеспечения сетевой безопасности.

2. Изучение основных принципов организации и построения консоли администрирования MMC в ОС Windows XP.

Цель работы: Изучить основные принципы организации и построения консоли администрирования, а также базовые возможности некоторых инструментов системного администратора ОС Windows XP.

2.1. Краткие теоретические сведения

Консоль управления Microsoft Management Console, сокращенно MMC является инструментом создания, сохранения и открытия средств администрирования (называемых консолями MMC), которые управляют оборудованием, программными и сетевыми компонентами операционной системы (ОС), иными словами, это основа администрирования любой ОС, в частности ОС Windows XP.

Консоль MMC непосредственно не выполняет административные функции, однако предоставляет возможности интеграции в нее компонентов или системных приложений, выполняющие эти функции. Основной тип интегрируемых на консоль компонентов называется **оснасткой**, которые не могут выполняться отдельно без консоли. Среди других добавляемых элементов могут быть элементы управления ActiveX, ссылки на Web-страницы, папки, виды панели задач и собственно задачи для выполнения. Дополнительные теоретические сведения об оснастках и других используемых для интеграции на консоль элементах будут добавлены в дальнейшем, в соответствующих разделах практических и лабораторных работ по применению различных оснасток.

Базовое окно консоли MMC представляет собой графическую форму с контекстными меню, реализующие дружественный пользовательский интерфейс. Имеется панель инструментов с командами создания, открытия и сохранения консолей и, кроме того, область описания и строка состояния в нижней части окна. Чтобы увидеть базовое окно, а также непосредственно саму консоль MMC, необходимо выполнить следующие действия:

- нажмите **Пуск | Выполнить**,
- наберите в появившемся окне **MMC.exe** (или просто **mmc**),
- нажмите **Enter** для ввода.

Новая консоль MMC представляет собой отдельное окно, разделенное на две вертикальные области, в левой из которых отображается дерево консоли с его

корнем. Дерево консоли показывает доступные элементы и компоненты консоли. Правая область является областью сведений, которая содержит описания элементов и выполняемых ими функций. Содержание области сведений соответствует выбранному элементу в дереве консоли и может включать Web-страницы, графики, диаграммы, таблицы и столбцы.

Создавая надежные средства управления компьютерами сети, можно собрать и настроить собственную консоль MMC, выполняющую заданные функции администрирования. После того как добавлены все необходимые элементы и компоненты консоли, панель главного меню, панель инструментов, а также область описания и строка состояния могут быть скрыты для предотвращения в дальнейшем нежелательных изменений. Созданные таким образом управляющие системы сохраняются в файлах с расширением **.msc** (Management Saved Console, сохраненная консоль управления) и могут быть, в частности, распространены в пределах всей системы посредством задания к ним доступа с помощью ярлыков или элементов меню **Пуск**.

Чтобы увидеть консоль управления локальным компьютером в качестве примера готовой и отлаженной консоли MMC, необходимо выполнить:

- нажмите **Пуск | Выполнить**,
- наберите в появившемся окне **compmgmt.msc**,
- нажмите **Enter** для ввода.

Существует два основных режима доступа консоли администрирования, задающиеся непосредственно при ее создании: **пользовательский**, в котором можно администрировать систему, работая с уже существующими консолями, и **авторский**, в котором можно создавать новые консоли или изменять существующие. В свою очередь, имеется три уровня режима пользователя, что обусловливает всего четыре варианта предустановленного режима доступа:

- авторский режим;
- режим пользователя – полный доступ;
- режим пользователя – ограниченный доступ, многооконный;
- режим пользователя – ограниченный доступ, однооконный.

Консоль MMC, инициализированная в авторском режиме, предоставляет полный доступ ко всем ее возможностям, включая добавление и удаление оснасток, создание новых окон и панелей задач, а также просмотр любых частей дерева консоли и другие. Однако при выборе одного из трех режимов пользователя

авторские возможности исключаются. В частности, если для консоли установлен параметр "пользовательский режим – полный доступ", то предоставляются все команды управления окном консоли и полный доступ к ее дереву, но запрещается добавление, удаление оснасток и изменение свойств консоли администрирования.

Изменения консоли ММС в авторском и пользовательском режимах сохраняются по-разному. При закрытии консоли в авторском режиме выводится диалоговое окно с предложением сохранить изменения. Однако в пользовательском режиме и снятом флажке "Не сохранять изменения для этой консоли" изменения будут сохранены автоматически при закрытии.

Если консоль открыта при соблюдении одного из следующих условий:

– в базовом окне при загрузке,
– с помощью команды контекстного меню **Автор**,
– в командной строке с параметром **/а**,

то предустановленный режим игнорируется, а открытие консоли осуществляется в авторском режиме.

Очевидно, что загрузка консоли ММС в авторском режиме не требуется рядовым пользователям. Системный администратор может настроить профили пользователей так, чтобы запретить им переход в авторский режим, как из командной строки, так и через контекстное меню. Кроме того, запрет перехода в авторский режим может быть организован при использовании возможностей групповой политики, при которой, в частности, осуществляется ограничение доступа к определенным оснасткам. Рассмотрению базовых возможностей оснастки групповой политики будет посвящена соответствующая работа.

Прежде чем создавать новую консоль ММС, необходимо определить действия, для которых предназначена эта консоль, список администрируемых компонентов, оснасток и других элементов, которые потребуются для выполнения поставленных задач. Следует также рассмотреть необходимость создания видов панели задач. После принятия этих решений можно открыть новую консоль и начать добавлять элементы к дереву консоли. Полное руководство по созданию и настройке консолей ММС находится на Web-узле корпорации Майкрософт (http://www.microsoft.com).

В практической работе предполагается ознакомление с основными принципами организации и построения консоли администрирования ММС.

2.2. Подготовка к выполнению практической работы

Перед началом выполнения практической работы в среде ОС Windows XP необходимо выполнить следующее:

1) загрузить ОС Windows XP и активировать справочное меню (**Пуск |Справка и поддержка**);

2) ознакомиться с описанием и возможностями запуска и применения консоли администрирования MMC;

3) ознакомиться с возможностью получения сведений пункта 2 из альтернативного источника информации, доступного непосредственно в справке консоли администрирования MMC (**Справка | Вызов справки**);

4) ознакомиться с описанием и возможностями оснасток "Локальные пользователи и группы" и "Редактор объекта групповой политики" ("Групповая политика").

2.3. Порядок выполнения практической работы

Для выполнения практической работы необходимо запустить виртуальную машину с гостевой ОС Windows XP.

Порядок выполнения:

I. Создание консоли администрирования MMC в авторском режиме требует выполнения следующих действий:

- нажмите **Пуск | Выполнить**,
- наберите в появившемся окне **MMC.exe** (или просто **mmc**),
- нажмите **Enter** для ввода.

Возможны следующие альтернативные варианты авторского запуска созданной ранее консоли администрирования:

A. запуск из командной строки, используя синтаксис:

Mmc *путь\имя_файла.msc* /**a**,

где параметр:

путь\имя_файла.msc – запускает консоль MMC с одновременным открытием файла сохраненной консоли с именем имя_файла.msc (Таблица 2.1). Если файл консоли не указан, будет открыта новая консоль MMC.

/a — открывает консоль MMC в авторском режиме.

Дополнительными параметрами команды могут быть:

/64 — открывает 64-разрядную версию консоли MMC (MMC64). Этот параметр используется только при работе в ОС Windows XP 64-Bit Edition.

/32 — открывает 32-разрядную версию консоли MMC (MMC32). При работе в ОС Windows XP 64-Bit Edition в окне консоли MMC, запущенной с этим параметром, открываются 32-разрядные оснастки.

Дополнительная информация по данной команде доступна одноименном разделе справки ОС Windows XP (**Пуск | Справка и поддержка**). Справку также можно получить, набрав в окне командной оболочки строку **Mmc /?** и нажав **Enter** для ввода.

Таблица 2.1. Список штатных консолей MMC, применяемых в ОС Windows XP с целью администрирования, мониторинга, оптимизации и аудита

№ п/п.	Файл консоли MMC	Описание
1.	dfrg.msc	Дефрагментация дисков
2.	devmgmt.msc	Диспетчер устройств
3.	gpedit.msc	Групповая политика
4.	ntmsoprq.msc	Запрос операторов съемных ОЗУ
5.	wmimgmt.msc	Инфраструктура управления
6.	secpol.msc	Локальные параметры безопасности
7.	lusrmgr.msc	Локальные пользователи и группы
8.	fsmgmt.msc	Общие папки
9.	perfmon.msc	Производительность
10.	eventvwr.msc	Просмотр событий
11.	rsop.msc	Результирующая политика
12.	certmgr.msc	Сертификаты
13.	services.msc	Службы
14.	ciadv.msc	Служба индексирования
15.	ntmsmgr.msc	Съемные ЗУ
16.	diskmgmt.msc	Управление дисками
17.	compmgmt.msc	Управление компьютером

Примечание. Файлы консоли MMC расположены в системном каталоге C:\WINDOWS\system32\ или %Systemroot%\system32\. Пример запуска консоли **dfrg.msc** из командной строки: **mmc** %Systemroot%\system32\dfrg.msc.

B. Запуск из файлового менеджера Проводник ОС Windows XP:

– наведите манипулятор мышь на файл с расширением .msc, находящийся в системной папке ОС (%systemroot%\system32\),

– кликните правой кнопкой мыши на файле и из контекстного меню выберите **Автор**.

II. Настройка параметров консоли администрирования ММС предназначена для ее конфигурирования с целью придания ей уникального вида.

Задание № 2.1. Изучить возможности изменения параметров и способы настройки консоли администрирования ММС на конкретных примерах.

Для придания уникального вида сохраненной (новой) консоли администрирования ММС в авторском режиме выполните следующие действия:

1. В меню **Консоль** выберите команду **Параметры**.

2. На вкладке **Консоль** в поле названия введите новый заголовок, содержащий **номер группы и фамилии студентов**, выполняющих данную работу.

3. На вкладке **Консоль** выполните следующие действия:

– нажмите кнопку **Сменить значок**,

– в поле **Имя файла** введите путь к файлу, содержащему значки (например, %systemroot%\system32\shell32.dll),

– в поле **Текущий значок** выберите необходимый значок,

– кликните **Применить** для подтверждения.

4. На вкладке **Консоль** из списка **Режим консоли** выберите пользовательский режим с полным доступом, в котором будет открываться консоль ММС при ее непосредственном запуске.

5. Для установленного в предыдущем пункте режима выполните указанные ниже действия:

– запретите изменение консоли ММС при ее непосредственном запуске, установив флажок "**Не сохранять изменения для этой консоли**",

– сделайте активным диалоговое окно **Вид | Настройка вида** консоли ММС при запуске, установив флажок **"Разрешить пользователю настраивать вид консоли"**.

6. Если необходимо удалить файлы, содержащие параметры отображения файлов консоли, на вкладке **Очистка диска** нажмите кнопку **Удалить файлы**.

7. Сохраните окончательно сконфигурированную консоль администрирования ММС, выбрав самостоятельно ее имя и путь к месту расположения в меню **Консоль | Сохранить как...** При сохранении обратите внимание на то, что файлы консоли по умолчанию размещаются в папке

«Администрирование», имеющей полный путь C:\Documents and Settings\student\Главное меню\Программы\Администрирование\.

8. Закройте сконфигурированную и сохраненную консоль администрирования MMC.

В файловом менеджере Проводник ОС Windows XP выполните следующие инструкции:

– наведите манипулятором мышь на сохраненный файл консоли администрирования MMC и, дважды кликнув на нем, запустите консоль,

– откройте диалоговое окно **Вид | Настроить** и, изменяя положение флажков, обратите внимание на получаемый результат,

– изменив вид консоли MMC приемлемым образом, кликните **ОК** для подтверждения полученного результата,

– в контекстном меню **Консоль** кликните **Выход**,

– снова запустите консоль администрирования MMC, кликнув манипулятором мышь на сохраненном файле консоли,

– изучите полученный результат.

III. Добавление различных элементов и компонентов к дереву консоли администрирования MMC предназначено для конфигурирования консоли с целью придания ей уникальных функций и оптимизации ее работы в целом.

Основным, интегрируемым на консоль компонентом, как уже упоминалось, является оснастка. Оснастки существуют двух видов: **изолированные** и **расширения**. Изолированная оснастка (или просто оснастка) добавляется к дереву консоли MMC без предварительного добавления других элементов, то есть непосредственно в корень дерева консоли. Оснастка расширения (или просто расширение) всегда добавляется к другой изолированной оснастке или расширению, которые уже имеются в дереве консоли MMC. Если для определенной оснастки разрешены расширения, то, как правило, они работают с объектами, управляемыми непосредственно этой оснасткой, например с компьютером, принтером, модемом или другим внешним устройством.

В дереве консоли оснастки и расширения располагаются для удобства иерархически или по группам. При добавлении новой оснастки или расширения, они появляются в виде нового элемента в дереве консоли MMC или в виде нового пункта контекстного меню, дополнительной панели инструментов, страницы свойств, а

также возможно мастера, организующего определенную последовательность действий, к уже установленной оснастке.

Другими элементами, по необходимости применимыми для интеграции на консоль администрирования MMC, являются виды панели задач и собственно задачи, которые могут включать в себя команды меню для элементов консоли и команды, запускаемые из командной строки. Кроме того, могут быть созданы команды, действующие как часть дерева консоли или открывающие другой компонент.

Прежде всего, перед добавлением указанных элементов к консоли MMC, необходимо определить их число. Если, в частности, требуется добавить несколько видов панели задач, то наряду с этим необходимо определить тип каждой панели (для отображения списка и задач или только задач), а также разделить задачи по интегрированным видам панели. Добавление видов панели задач и собственно задач осуществляется посредством работы мастера создания этих элементов. При этом важно помнить, что консоль MMC должна содержать, по крайней мере, одну оснастку, чтобы возможность интеграции появилась в принципе.

Отдельной возможностью, иногда необходимой при администрировании сетей, является добавление элементов и компонентов дерева консоли администрирования MMC в виде списка ярлыков в меню "Избранное".

Дополнительные сведения о добавлении различных элементов в дерево консоли администрирования MMC можно получить, воспользовавшись справкой ОС Windows XP (**Пуск | Справка и поддержка**) в разделе **Общее представление о MMC \ Консоль MMC в авторском режиме \ Оснастки \ Создание консолей**.

Задание № 2.2. Исследовать процесс добавления различных элементов и компонентов к дереву консоли администрирования MMC на конкретных примерах.

Первым необходимым компонентом, добавляемым к дереву консоли администрирования MMC при ее организации и построении, является оснастка. Для добавления оснастки в авторском режиме выполните следующие действия:

1. Создайте новую **Консоль** управления MMC одним из описанных в **пункте I** текущего учебного задания способов.

2. Задайте данной консоли новый заголовок, содержащий **номер группы и фамилии студентов**, выполняющих данную работу.

3. В меню **Консоль** выберите команду **Добавить или удалить оснастку**.

4. В диалоговом окне **Добавить/удалить оснастку** нажмите кнопку **Добавить** вкладки **Изолированная оснастка**. Список **Оснастки** в диалоговом окне **Добавить/удалить оснастку** определяет элемент дерева консоли, к которому выполняется добавление элементов. В этом списке можно найти любой элемент дерева консоли. Обратите внимание на то, что по умолчанию это **Корень консоли**.

5. В диалоговом окне **Добавить изолированную оснастку**, выберите оснастки **Службы** из списка доступных в системе, кликнув на ней манипулятором мышь и нажав кнопку **Добавить**. Для добавления другой оснастки из списка, повторите указанные действия настоящего пункта повторно.

6. Для некоторых оснасток в процессе их инсталляции выводится диалоговое окно **Выбор целевого компьютера**, определяющее, чем, устанавливаемая оснастка будет управлять в дальнейшем – локальным или сетевым компьютером. Выберите **Локальный компьютер**, установив переключатель в соответствующее положение.

7. Нажмите **Готово**, **Закрыть** и затем кликните **ОК** для подтверждения ввода.

8. Скройте меню и панель инструментов оснастки **Службы**, выполнив действия указанные ниже:

- В меню **Вид** выберите команду **Настроить**,
- В группе **Оснастка** снимите флажок **Меню**,
- В группе **Оснастка** снимите флажок **Панели инструментов**,
- Нажмите **ОК**.

При устанавливании или снятии флажков, соответствующие им меню и панели инструментов отображаются или скрываются, причем, для всех оснасток консоли, включая текущую. Если переключение флажков не приводит к изменению вида консоли, тогда текущая оснастка не имеет специальных меню или панелей инструментов.

9. Не закрывая консоль администрирования ММС, сохраните ее, выбрав команду **Сохранить** в меню **Консоль**.

Для добавления расширений к уже установленной в предыдущем задании оснастке **Службы** выполните следующее:

10. В меню **Консоль** выберите команду **Добавить или удалить оснастку**.

11. В диалоговом окне **Добавить/удалить оснастку** выберите вкладку **Расширение**. На этой вкладке можно выбрать любой элемент дерева консоли из списка **Оснастки**, которые могут быть расширены, и просмотреть **Доступные расширения**, которые могут быть включены или отключены. После подключения расширение автоматически размещается в дереве консоли под оснасткой, к которой оно относится. Если дерево консоли содержит больше одного экземпляра оснастки, к которой подключено расширение, все остальные экземпляры автоматически получают это расширение.

12. Среди **Доступных расширений** оснастки **Службы** удалите флажок с расширения **Расширенный вид** (предварительно сняв флажок **Добавить все разрешения**) и отметьте, к чему привело это действие. Повторите аналогичные действия с другими расширениями данной оснастки и изучите получаемый результат.

13. Не закрывая консоль администрирования MMC, сохраните ее.

В окне консоли администрирования выполните следующие инструкции:

– последовательно перебирая доступные в системе оснастки, найдите те из них, которые обладают дополнительным меню, панелью инструментов или расширениями,

– изучите полученный результат и сделайте вывод о проделанной работе.

Следующим элементом, необходимым в ряде случаев администрирования и предназначенным, в том числе, для удобства отображения информации, является новый вид панели задач. Для добавления видов панелей задач и собственно задач в авторском режиме выполните следующее:

1. Создайте новую **Консоль** управления MMC одним из описанных в **пункте I** текущего учебного задания способов.

2. Задайте данной консоли новый заголовок, содержащий **номер группы и фамилии студентов**, выполняющих данную работу.

3. Добавьте оснастку **Службы** в корень консоли MMC.

4. В дереве консоли кликните манипулятором мышь на этой оснастке.

5. В меню **Действие** или кликнув правой кнопкой манипулятора на оснастке, выберите команду **Новый вид панели задач**.

6. Следуйте инструкциям **"Мастера создания вида панели задач"**, чтобы добавить на консоль новую панель вида.

7. Если сразу после создания вида панели задач необходимо создать задачи, установите флажок **"Запустить мастер создания новой задачи"** на последнем экране **"Мастера создания вида панели задач"**.

8. Следуйте инструкциям "**Мастера создания новой задачи"**, чтобы добавить на консоль новую задачу к существующей панели вида.

9. В дереве консоли кликните элемент или компонент (в нашем случае это оснастка), связанный с видом панели задач, затем в меню **Действие** выберите команду **Правка вида панели задач**.

10. На вкладке **Задачи** нажмите кнопку **Создать**.

11. Повторите инструкции пункта 7 настоящего задания.

12. Не закрывая консоль администрирования ММС, сохраните ее.

Измените вид панели задач сохраненной консоли администрирования ММС, выполнив следующие действия:

– введите новое имя,

– введите новое описание,

– установите переключатель **Стиль для области сведений** в положение, соответствующее новому формату списка,

– удалите соответствующий флажок, чтобы отобразить стандартную вкладку,

– установите переключатель **Стиль для описания задачи** в положение, соответствующее новому стилю задачи,

– выберите новое значение ширины для вертикального списка или высоты для горизонтального списка,

– нажмите кнопку **Параметры** и установите переключатель в одно из необходимых положений,

– нажмите **ОК** для подтверждения ввода,

– изучите полученный результат,

– сделайте вывод о проделанной.

Важной особенностью при построении и организации консоли администрирования ММС является возможность добавления элементов и компонентов дерева консоли в виде списка ярлыков в меню **"Избранное"**. Для добавления элемента или компонента в авторском режиме выполните следующее:

1. Создайте новую Консоль управления ММС одним из описанных в **пункте I** текущего учебного задания способов.

2. Задайте данной консоли новый заголовок, содержащий **номер группы и фамилии студентов**, выполняющих данную работу.

3. В дереве консоли кликните элемент или компонент (в нашем случае это оснастка), который нужно добавить в список "Избранное".

4. В области сведений выберите вкладку вида панели задач, которую нужно добавить, в случае, если для элемента или компонента, указанного в дереве консоли, настроен вид панели задач. В противном случае в области сведений вкладки не видны.

5. Выберите в меню **Избранное** команду **Добавить в избранное**.

6. В поле **Создать в:** диалогового окна **Добавление в папку "Избранное"** выполните указанные ниже действия:

- создайте новую папку с названием, выбранным самостоятельно, кликнув папку, которая будет выступать в качестве родительской для создаваемой папки и нажав кнопку **Создать папку**,
- нажмите кнопку **ОК** для ввода,
- в поле **Имя папки** введите имя, под которым будет добавлен элемент, кликните **ОК** для подтверждения ввода.

7. Не закрывая консоль администрирования ММС, сохраните ее.

Упорядочите "Избранное" сохраненной консоли администрирования ММС, выполнив следующие действия:

- добавьте новую папку, введя ее имя в соответствующее поле и кликнув **ОК** для подтверждения ввода,
- переместите элемент, созданный в **пункте 5** настоящего задания, в новую, только что созданную, папку и кликните **ОК** для ввода,
- переименуйте выбранный элемент и нажмите клавишу **Enter** для подтверждения ввода,
- удалите все элементы, расположенные ниже папки "Избранное",
- нажмите **Закрыть** для завершения задания,
- изучите полученный результат,
- сделайте вывод о проделанной работе.

3. Работа с подсистемой безопасности в ОС Windows XP

Цель работы: Изучение основных возможностей подсистемы безопасности и способы защиты данных в среде ОС Windows XP и создание пользовательской консоли администрирования MMC, предназначенной для организации и управления локальными политиками безопасности в среде ОС Windows XP

3.1. Подготовка к выполнению практической работы

Возможность управления политикой безопасности (на локальном компьютере или в сети) осуществляется посредством создания консоли администрирования MMC и добавления на нее соответствующих, предназначенных для этих целей средств управления (оснасток и расширений). При этом возможно использование оснасток, изученных ранее и ориентированных на управление правами доступа и разрешениями, имеющимися у пользователя в процессе работы с локальными ресурсам системы. В случае необходимости, применение других системных инструментов и программных модулей сторонних разработчиков (например, ориентированных на аудит и мониторинг ОС) также может быть полезным с целью расширения функционала консоли администрирования. Средства управления политикой безопасности локального узла, подразделения или домена представлены в табл. 3.1.

Отдельно следует отметить еще одно программное средство **Secedit.exe**, представляющее собой исполняемый файл, запускаемый из командной строки, в рамках пакетного файла или посредством автоматического планировщика заданий. Данное средство используется для автоматизации задач настройки системы безопасности группы компьютеров локальной сети. Для применения данного средства в повседневной практике необходимо иметь навыки использования командного интерпретатора и опыт написания пакетных файлов и сценариев.

Таблица 3.1. Средства управления политикой безопасности ОС

№ п/п.	Средство управления политикой безопасности	Описание
1.	Средство «Локальная политика безопасности»	Данное средство используется для прямого изменения политик учетных записей и локальных политик, политик открытого ключа, а также политик безопасности IP локального компьютера.
2.	Шаблоны безопасности	Шаблон безопасности является файлом, представляющим конфигурацию безопасности или политику безопасности. Подобные шаблоны могут применяться к политике локального компьютера или импортироваться в объект **«Групповая политика»**
3.	Средство «Анализ и настройка безопасности»	Данное средство используется для анализа и настройки безопасности локального узла с помощью шаблона безопасности.
4.	Расширение «Параметры безопасности» для групповой политики	Данное средство может использоваться для изменения отдельных параметров безопасности локального узла, подразделения или домена.

В настоящей практической работе предполагается ознакомление с основными принципами организации локальной и сетевой политик безопасности на основе консоли администрирования MMC с применением базовых возможностей указанных выше программных средств и оснасток «Редактор объекта групповой политики» («Групповая политика»), «Шаблоны безопасности», «Анализ и настройка безопасности», а также «Политики безопасности IP на «Локальный компьютер» и «Монитор IP-безопасности». При этом для детального изучения принципов создания и настройки консоли администрирования MMC с применением отмеченных средств целесообразно воспользоваться полным руководством, находящимся на Web-узле корпорации Майкрософт (http://www.microsoft.com).

Перед началом выполнения практической работы в среде ОС Windows XP необходимо выполнить следующее:

1) загрузить ОС Windows XP и активировать справочное меню (**Пуск | Справка и поддержка**);

2) ознакомиться с описанием и возможностями запуска и применения консоли администрирования MMC;

3) ознакомиться с описанием и возможностями оснасток, предназначенных для организации и администрирования локальной и сетевой политиками безопасности в среде ОС Windows XP: **«Редактор объекта групповой политики» («Групповая политика»), «Шаблоны безопасности», «Анализ и настройка безопасности»,** а также **«Политики безопасности IP на «Локальный компьютер»** и **«Монитор IP-безопасности»**.

3.2. Порядок выполнения практической работы

Практическая работа выполняется последовательно в соответствии с определенным порядком и включает в себя четыре учебных задания.

Практическая работа выполняется в виртуальной машине.

Порядок выполнения

Как было ранее отмечено, локальные политики безопасности применяются на отдельных узлах сети. В состав этих политик входят следующие:

– *Назначение прав пользователя* определяет, какие пользователи и группы обладают правами на вход в систему и авторизованы на выполнение соответствующих задач.

– *Политики аудита* определяют события безопасности, которые, в свою очередь, заносятся в Журнал безопасности данного компьютера. При этом в журнал могут заноситься успешные, неудачные или те и другие попытки. Журнал безопасности является частью оснастки «Просмотр событий».

– *Параметры безопасности* определяют действия ОС, направленные на обеспечение безопасности вычислительной системы. Например, к их числу относятся включение или отключение таких параметров безопасности как цифровая подпись данных, доступ оптическим накопителям, установка определенных драйверов или приглашение на вход в систему. Конфигурирование локальной политики посредством изменения некоторых параметров безопасности будет рассмотрено в ходе выполнения текущей практической работы. При этом необходимо иметь ввиду, что приоритет имеют политики следующих объектов в указанном порядке: подразделение, домен и только затем локальный компьютер.

Это обусловлено тем, что бесконтрольное применение нескольких политик к одному локальному узлу может породить конфликт между параметрами безопасности.

На основе полученных в предыдущих практических работах знаний и навыков по организации и построению консоли администрирования ММС необходимо выполнить следующее:

1. Создайте новую консоль администрирования в авторском режиме, задав ей в качестве имени **фамилию и номер группы студента, выполняющего работу**.

2. При необходимости сконфигурируйте параметры созданной консоли должным образом с целью придания ей уникального вида.

3. Добавьте на консоль новую панель вида задач, следуя инструкциям **«Мастера создания вида панели задач»**. В процессе работы **«Мастера»** введите новое имя **«Политика безопасности»** и описание **«Оснастки и расширения»** для данной панели задач; в появившемся окне **«Завершение мастера создания вида панели задач»** уберите флажок **«Добавить новые задачи на эту панель задач после закрытия мастера»** и нажмите кнопку **«Готово»** для подтверждения операции.

4. Добавьте в корень дерева консоли ММС оснастку **«Локальные пользователи и группы»** и одним из ранее изученных способов создайте новую учетную запись с правами группы **«Пользователи»**. Имя пользователя, описание и пароль выберите самостоятельно. В процессе создания учетной записи пользователя оставьте флажок **«Потребовать смену пароля при следующем входе в систему»**.

5. Не закрывая консоль, сохраните ее.

Последовательность выполненных действий позволяет создать консоль администрирования ММС, придать ей уникальный вид и удобный интерфейс для дальнейшего использования в рамках настоящей практической работы.

Задание №3.1. Изучение основных возможностей программного средства **«Локальная политика безопасности»** в среде ОС Windows XP на конкретных примерах.

Прежде, чем интегрировать инструмент **«Локальная политика безопасности»** на созданную заранее консоль администрирования MMC и осуществить его детальное рассмотрение, необходимо отметить, что в ОС Windows XP данный инструмент существует автономно в виде штатного программного средства и может быть использован на локальном компьютере вне рамок оснастки **«Редактор объекта групповой политики»**. В частности, для просмотра локальной политики безопасности им можно воспользоваться, вызвав его посредством команды **Выполнить** в меню **Пуск**, набрав **secpol.msc** и нажав **Enter** для подтверждения. Кроме того, поскольку модуль **«Локальная политика безопасности»** является штатным средством администрирования, он находится в группе соответствующих программных средств, расположенных в меню **«Пуск | Панель управления | Администрирование»**.

Несмотря на сказанное выше, дальнейшее изучение локальной политики безопасности будет осуществляться в предположении, что имеется системная необходимость создания собственной консоли MMC с включенным внутрь набором необходимых для администрирования инструментов, в том числе модуля **«Локальная политика безопасности»**. Для ознакомления с возможностями локальной политики безопасности в ОС Windows XP с использованием одноименной оснастки, прежде всего, необходимо выполнить следующие подготовительные действия:

1. Откройте только что созданную консоль администрирования MMC, в которой к этому моменту должна быть уже добавлена оснастка **«Локальные пользователи и группы»**.

2. Воспользовавшись оснасткой **«Редактор объекта групповой политики»**, добавьте политику **«Локальный компьютер»** в корень консоли, как было показано в предыдущих практических работах.

3. С одной стороны, в окне дерева консоли MMC откройте ветвь **«Конфигурация компьютера | Конфигурация Windows | Параметры безопасности»** в **«Политике «Локальный компьютер»»**. С другой стороны, в

отдельном окне ОС откройте инструмент **«Локальная политика безопасности»** одним из выше описанных способов и, сравнив содержимое открытых окон, обратите внимание на то, что **«Параметры безопасности»** локальной политики абсолютно идентичны тем, которые отображаются в оснастке **«Политика «Локальный компьютер»**.

Таким образом, у системного администратора появляется возможность в случае необходимости интегрировать базовый инструмент локальной безопасности во вновь создаваемую и конфигурируемую консоль ММС.

4. Сохраните и закройте консоль администрирования ММС.

С целью обучения и ознакомления с **«Локальной политикой безопасности»** интерес в дальнейшем будут представлять **«Политики учетных записей»**, а также некоторые **«Локальные политики»** при **«Назначении прав пользователя»** и общих **«Параметров безопасности»**.

Секция А. Ознакомление с основными возможностями **«Политики учетных записей»** в ОС Windows XP.

Политики учетных записей (**«Конфигурация компьютера | Конфигу-рация Windows | Параметры безопасности | Политики учетных записей»**) применяются на локальных компьютерах сети и определяют взаимодействие учетных записей с данным компьютером или доменом. Существует три политики учетных записей:

– *Политика паролей* определяет параметры паролей, в частности, соответствие набору обязательных условий и сроку их действия.

– *Политика блокировки учетной записи* определяет условия и период времени блокировки учетной записи.

– *Политика Kerberos* определяет параметры протокола сетевой аутентификации Kerberos, такие как срок жизни сеансового билета и соответствие обязательным условиям. Данный протокол обеспечивает взаимно-секретную аутентификацию компьютеров в сети на основе клиент-серверной модели. Политика Kerberos не входит в состав политики локального компьютера, она используется только для учетных записей пользователей домена.

Дополнительная информация по данной тематике доступна в справочных разделах **«Локальная политика безопасности»** и **«Параметры безопасности»** оснастки **«Групповая политика»**, а также в разделе **«Методы проверки**

подлинности» справки ОС Windows XP (**Пуск | Справка и поддержка**) или на сайте **www.oszone.net**.

Для ознакомления с базовыми возможностями **«Политики учетных записей»** в ОС Windows XP выполните следующее:

1. Разверните окно созданной ранее консоли администрирования MMC, если оно находится в свернутом состоянии на панели задач, или загрузите консоль снова. В оснастке **«Локальные пользователи и группы»** наведите манипулятором мышь на нового пользователя и задайте ему любой пароль, выбрав команду **«Задать пароль...»** из контекстного меню.

2. Найдите подраздел **«Политика паролей»** в разделе **«Политики учетных записей»** оснастки **«Политика «Локальный компьютер»**.

3. Последовательно просмотрите все политики паролей с целью их дальнейшего применения на практике. Для этого дважды щелкните на каждой из них и на вкладке **«Объяснение параметра»** изучите их сущность.

4. Включите политику **«Пароль должен отвечать требованиям сложности»**, изменив положение соответствующего переключателя на вкладке **«Параметр локальной безопасности»**.

5. Установите минимальную длину пароля в 10 символов, осуществив необходимые действия в соответствующей политике паролей.

6. Перейдите в подраздел **«Политика блокировки учетной записи»** и аналогично изучите сущность расположенных здесь политик безопасности.

7. Установите **«Пороговое значение блокировки»** на три ошибки входа в систему и осуществите блокировку учетной записи на 2 минуты в случае совершенных ошибок ввода.

8. Сохраните и закройте консоль администрирования MMC.

При выполнении заданий секции используйте следующие инструкции:

– перенесите последовательность выполняемых действий в отчет (возможно приведение графических фрагментов, сделанных с экрана, в качестве демонстрационного материала),

– войдите в систему под созданной учетной записью и проверьте влияние новых значений системных параметров политик безопасности на процесс аутентификации,

– сделайте вывод о проделанной работе и запишите его в отчет.

Секция В. Ознакомление с основными возможностями **«Локальных политик»** при **«Назначении прав пользователя»** в ОС Windows XP.

Локальные политики безопасности, применяемые при назначении прав пользователя (**«Конфигурация компьютера | Конфигурация Windows | Параметры безопасности | Локальные политики | Назначение прав пользователя»**), позволяют системному администратору определить, какие пользователи и группы будут обладать правами на вход в ОС и какие будут при этом авторизованы на выполнение соответствующих задач. Особенностью данных локальных политик является то, что они могут быть применены к любому пользователю или группе в системе простым их (пользователей) добавлением в число тех, на которые рассматриваемая политика распространяется. Это позволяет, тем самым, иметь пользователям возможность влиять на политику безопасности ОС. Для иллюстрации сказанного и ознакомления с базовыми возможностями локальных политик безопасности при **«Назначении прав пользователя»** в ОС Windows XP выполните следующее:

1. Разверните окно созданной ранее консоли администрирования MMC, если оно находится в свернутом состоянии на панели задач, или загрузите консоль снова. В оснастке **«Политика «Локальный компьютер»** найдите подраздел **«Назначение прав пользователя»** в разделе **«Локальные политики»**.

2. Последовательно просмотрите все политики для назначения прав пользователям с целью их дальнейшего применения на практике. Для этого дважды щелкните на каждой из них и на вкладке **«Объяснение параметра»** изучите их сущность.

3. Добавьте созданного ранее пользователя в число тех, которым позволено производить операции архивирования файлов и каталогов в системе. Для этого воспользовавшись одноименной политикой безопасности, **«Добавьте пользователя или группу»** стандартным способом на вкладке **«Параметр локальной безопасности»** и удалите группы, обладающие этим правом по умолчанию.

4. Запретите группам **«Пользователи»** и **«Операторы архива»** доступ к компьютеру из сети. Для этого внимательно изучите политики **«Доступ к компьютеру из сети»** и **«Отказ в доступе к компьютеру из сети»**.

5. Добавьте созданного ранее пользователя в число тех, которым позволено осуществлять **«Изменение системного времени»**.

6. Добавьте созданного ранее пользователя в число тех, которым позволено осуществлять **«Создание страничного файла»**.

7. Добавьте созданного ранее пользователя в число тех, которым позволено осуществлять **«Управление аудитом и журналом безопасности»**.

8. Сохраните и закройте консоль администрирования MMC.

При выполнении заданий секции используйте следующие инструкции:

– перенесите последовательность выполняемых действий в отчет (возможно приведение графических фрагментов, сделанных с экрана, в качестве демонстрационного материала),

– войдите в систему под созданной учетной записью и проверьте влияние новых значений системных параметров политик безопасности на процесс авторизации,

– сделайте вывод о проделанной работе и запишите его в отчет.

Секция С. Ознакомление с основными возможностями **«Локальных политик»** при настройке **«Параметров безопасности»** в ОС Windows XP.

Основные политики, применяемые для обеспечения локальной или сетевой безопасности и представленные в виде набора соответствующих параметров (**«Конфигурация компьютера | Конфигурация Windows | Параметры безопасности | Локальные политики | Параметры безопасности»**), позволяют системному администратору, наряду с политиками учетных записей и базовыми методами авторизации, организовать первый уровень защиты данных от несанкционированного доступа из сети или же, напротив, позволить уполномоченным пользователям иметь определенные права при обращении к информации.

Для ознакомления с базовыми возможностями рассматриваемого набора политик безопасности в ОС Windows XP выполните следующее.

1. Разверните окно созданной ранее консоли администрирования MMC, если оно находится в свернутом состоянии на панели задач, или загрузите консоль снова.

В оснастке **«Политика «Локальный компьютер»** найдите подраздел **«Параметры безопасности»** в разделе **«Локальные политики»**.

2. Последовательно просмотрите все политики безопасности данного подраздела с целью их дальнейшего применения на практике. Для этого дважды щелкните на каждой из них и на вкладке **«Объяснение параметра»** изучите их сущность.

3. Включите возможность очистки страничного файла виртуальной памяти при завершении работы системы, воспользовавшись соответствующей политикой безопасности. Это позволит при определенных условиях избежать перехвата данных из виртуальной памяти.

4. Следующие несколько настроек данного пункта задания реализуют концепцию «безопасного входа в систему», которая может быть практически использована на серверах домена или отдельных узлах локальной сети.

Прежде всего, следует отметить, что некоторым пользователям новый механизм входа в систему с использованием окна приветствия в ОС Windows XP может показаться неудобным или непривычным. Для устранения данного дискомфорта в системе имеется вариант переключения данного механизма в «классический» режим. Для этого необходимо осуществить **«Изменение входа пользователей в систему»** в меню **«Пуск | Панель управления | Учетные записи пользователей»**. В появившемся окне необходимо убрать флажки **«Использовать страницу приветствия»** и **«Использовать быстрое переключение пользователей»** и подтвердить изменения, щелкнув манипулятором мышь по кнопке **«Применение параметров»**.

Данное изменение приводит к тому, что после перезагрузки ОС появляется «классическое» окно входа в систему с двумя полями: «Пользователь», в котором следует набрать имя учетной записи, и «Пароль» – для ввода пароля, назначенного этой учетной записи.

Внимание! При переключении механизма входа в «классический» режим утрачивается возможность использования технологии быстрого переключения пользователей. Поэтому, в случае обратного перехода (в положение с использованием окна приветствия) для возврата данной технологии в активное состояние необходимо войти в ОС с правами администратора и установить соответствующий флажок **«Использовать быстрое переключение пользователей»**.

Далее переведите в положение **«Отключено»** параметр безопасности локальной политики **«Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL»**, как это делается на рабочих станциях и серверах домена. Эта настройка обеспечивает пользователей необходимостью одновременно нажимать кнопки CTRL, ALT и DEL каждый раз при входе в ОС, что делает процедуру входа более защищенной.

Отключите возможность отображения имени пользователя (в поле **«Пользователь»**), выполнившего последним вход в систему, воспользовавшись соответствующей политикой безопасности **«Интерактивный вход в систему: не отображать последнего имени пользователя»**. Данная политика исключает возможность несанкционированного манипулирования именем пользователя в сети.

Концепция **«безопасного входа в систему»** реализована полностью.

5. С целью уведомления пользователей локальной сети включите возможность отображения текста сообщения следующего содержания: **«ВНИМАНИЕ!!! Вы входите в корпоративную сеть компании. Причинение вреда аппаратно-программному обеспечению компании преследуется в административном порядке. Будьте аккуратны, это Ваше имущество!!!»**, воспользовавшись локальными политиками **«Интерактивный вход в систему: заголовок сообщения для пользователей при входе в систему»** и **«Интерактивный вход в систему: текст сообщения для пользователей при входе в систему»**.

6. Практический смысл следующего задания заключается в активации так называемой модели «гостевого доступа», позволяющей организовать беспрепятственный общий доступ к объектам (файлам и каталогам) файловой системы из локальной сети. Эта модель является оптимальным выбором для домашнего применения, хотя обладает ослабленной безопасностью в процессе эксплуатации. В этой связи, критически необходимо использовать дополнительные аппаратно-программные средства для защиты клиентских компьютеров от несанкционированного доступа, вирусов и внешних атак.

Кроме модели «гостевого доступа», существует еще одна, классическая модель доступа, называемая «обычной», имеющая место при организации общих сетевых ресурсов. Модель «обычного доступа» обладает повышенным уровнем

безопасности и гибкостью при настройке прав. Поэтому применение данной модели целесообразно в корпоративных условиях.

Чтобы активировать модель «гостевого доступа», во-первых, необходимо включить встроенную учетную запись «Гость». Для этого следует найти политику безопасности **«Учетные записи: Состояние учетной записи «Гость»** и перевести соответствующий системный параметр безопасности в положение **«Включено»**.

Во-вторых, в локальной политике **«Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей»** следует изменить значение параметра модели совместного доступа в положение **«Гостевая – локальные пользователи удостоверяются как гости»**.

В-третьих, в локальной политике **«Учетные записи: ограничить использование пустых паролей только для консольного входа»**, регламентирующей использование пустых паролей, необходимо перевести параметр безопасности в состояние **«Отключено»**. Это позволит пользователям с учетной записью **«Гость»** и пустым паролем иметь возможность беспрепятственного доступа в систему из локальной сети. По умолчанию, во включенном состоянии этого параметра, использование пустых паролей допускается только для консольного входа, то есть для входа в систему с клавиатуры компьютера.

Очевидно, что данная политика в состоянии **«Отключено»** также ослабляет системную безопасность настраиваемой среды при доступе к так называемым «административным» ресурсам, если учетные записи последних надежно не защищены парольной защитой.

Наконец, следует проверить наличие пользователя «Гость» в числе тех, кому в принципе разрешен доступ из локальной сети. Для этого откройте изученную ранее (**секция В** текущего задания) ветвь **«Параметры безопасности | Локальные политики | Назначение прав пользователя»** и в локальной политике **«Отказ в доступе к компьютеру из сети»** убедитесь в отсутствии учетной записи «Гость» среди запрещенных. Если пользователю «Гость» доступ из сети запрещен, то удалите учетную запись.

Таким образом, последние четыре политики позволяют организовать «гостевой доступ» из локальной сети к тому компьютеру, на котором данные настройки были применены. Как следствие, реализованная конфигурация при

использовании на каждом локальном узле в рабочей группе или домене обеспечивает беспрепятственный взаимный доступ к общим локальным ресурсам.

8. Сохраните и закройте консоль администрирования MMC.

При выполнении заданий секции используйте следующие инструкции:

– перенесите последовательность выполняемых действий в отчет (возможно приведение графических фрагментов, сделанных с экрана, в качестве демонстрационного материала),

– выйдите из системы, снова войдите в нее и проверьте влияние новых значений системных параметров политик безопасности,

– сделайте вывод о проделанной работе и запишите его в отчет.

Задание №3.2. Изучение основных возможностей программного средства **«Шаблоны безопасности»** в среде ОС Windows XP на конкретных примерах.

В предыдущих заданиях практической работы были рассмотрены отдельные политики безопасности и принадлежащие им системные параметры, изменяемые при конфигурировании безопасности ОС. Однако гораздо эффективней конфигурировать ОС в процессе ее загрузки посредством единовременного применения группы параметров безопасности. Для этих целей в среде ОС Windows XP существует специализированное программное средство **«Шаблоны безопасности»**, представляющее собой оснастку, как и прежде добавляемую к дереву консоли администрирования MMC. В рамках данной оснастки имеется возможность создавать и применять в системе текстовые файлы, содержащие в себе все необходимые настройки безопасности для безопасных областей, поддерживаемых локальной политикой. Именно данные текстовые файлы в ОС принято называть шаблонами безопасности. В ОС Windows XP существует ряд штатных шаблонов безопасности, определяющих конфигурацию безопасности по семи категориям:

1) Политики учетных записей – это набор параметров аутентификации учетных записей. Для учетных записей домена параметры учетной политики должны быть одинаковы по всему домену. Данные политики подразделяются на:

– *Политика паролей* – ограничения на пароль, его минимальную длину, хранение старых паролей, минимальный и максимальный срок действия пароля, сложность пароля и, возможно, обратимое шифрование хранимых данных.

– *Политика блокировки учетной записи* отвечает за действие, которое должно выполняться при вводе неверного пароля, включая пороговое число неудачных попыток входа в ОС, при котором происходит блокировка учетной записи или ответные действия, включая частоту сброса счетчиков попыток входа.

– *Политика Kerberos* – набор параметров протокола сетевой аутентификации Kerberos v.5, в частности, включающего время жизни для билетов на их выдачу, билетов службы, максимальное расхождение часов и проверку членства в группе и статуса блокировки учетных записей.

2) Локальные политики – параметры безопасности только для компьютера, на котором применяется шаблон безопасности. Они применяются к базе данных учетной записи локального узла и делятся на три категории.

– *Политика аудита* – набор отслеживаемых событий, которые будут храниться в журнале безопасности локального компьютера.

– *Назначение прав пользователя* определяет участников безопасности, которым будут даны права пользователей на локальном компьютере. Эти права приоритетнее любых разрешений ФС NTFS, назначенных объекту (файлу или каталогу).

– *Параметры безопасности* – спектр параметров, заданных в Реестре ОС. Обычно они указывают, отображать ли имя последнего пользователя, под которым входили в компьютер, или изменять ли имя учетной записи «Администратор».

3) Журнал событий – набор свойств журналов приложений, безопасности и системы, включая максимальный размер журнала, пользователей, которые могут его просматривать, срок хранения событий в журналах и действия, которые надо предпринять, если журналы безопасности достигли заданного максимального размера.

4) Группы с ограниченным доступом позволяют зафиксировать членство в группах безопасности. Допустимые группы безопасности выбирает создатель шаблонов безопасности. Обычно в эту группу включаются «Опытные пользователи», «Администраторы предприятия» и «Администраторы схемы». В результате можно явно указать, какие участники безопасности могут быть членами группы с

ограниченным доступом. Данная политика также определяет, членом каких групп может быть сама группа с ограниченным доступом.

5) Системные службы позволяют задать ограничения для служб, установленных на компьютере, в том числе их статус (активизирована или отключена) и какие участники вправе ее запустить или остановить. В частности, например, можно настроить данную политику таким образом, чтобы была отключена служба **«Routing and Remote Access»** (**«Маршрутизация и удаленный доступ»**) на всех клиентских рабочих станциях. Это обеспечит запрет пользователям настраивать свои персональные компьютеры в качестве серверов удаленного доступа.

6) Реестр определяет безопасность разделов Реестра ОС и их кустов: какие участники безопасности вправе изменять параметры безопасности и аудит каких действий по модификации Реестра следует вести.

7) Файловая система определяет параметры избирательного списка управления доступом (DACL) и системного списка управления доступом (SACL) для любых каталогов, включенных в эту политику. Эти каталоги должны располагаться на носителе с ФС NTFS.

Известно, что компьютеры в сети могут выступать в разных ролях, то есть иметь различное назначение. Это обстоятельство влияет на выработку решения по тому, какие параметры следует применять для формирования политики безопасности для того или иного узла. Это приводит к тому, что перед определением шаблонов безопасности необходимо выявить компьютеры в сети, для которых нужно создать одинаковые параметры безопасности. Обычно для этого достаточно определить роль, которую каждый компьютер выполняет в сети, и уникальные требования безопасности для каждой роли.

Каждая роль, в конечном итоге, будет связана с шаблоном безопасности, определяющим типовую или требуемую безопасность для этого класса компьютеров. Наиболее распространенные роли компьютеров в сети следующие.

Контроллеры домена хранят базу данных Active Directory, требования безопасности для защиты которой являются самыми строгими.

Серверы приложений содержат клиентские серверные приложения, например, Web-приложения, базы данных SQL или почтовые серверные приложения. В каждой из указанных выше категорий можно определить соответствующие параметры безопасности для серверного приложения.

Файловые серверы хранят данные, совместно используемые в сети. В рамках определения безопасности можно создать специальные списки DACL для определенных хранилищ данных.

Серверы печати предназначены для организации печати на принтерах, находящихся в общем доступе для компьютеров локальной сети. Для каждого сетевого принтера могут быть установлены различные права доступа для разных пользователей.

Серверы экстрасети – компьютеры с любой сетевой ОС, не являющиеся членами Active Directory. Хотя они могут проводить аутентификацию, но, как правило, располагаются в нейтральной (демилитаризованной DMZ-зоне) и имеют ограниченный доступ к ресурсам внутренней локальной сети.

Рабочие станции – клиентские компьютеры с сетевой ОС, не покидающие территориально офис предприятия. Их можно подразделять в зависимости от отдела или филиала, где они установлены.

Портативные компьютеры – клиентские узлы, имеющие возможность мобильного перемещения. Пользователи этих компьютеров могут обладать особыми привилегиями для выполнения некоторых задач вне корпоративной локальной сети.

Киоски устанавливаются в общественных местах и выполняют одно общедоступное приложение. В шаблоне безопасности киоска можно настроить автоматическую регистрацию на входе с использованием предварительно созданной учетной записи, позволяющей работать со специализированным инсталлированным приложением.

Нетрудно заметить, что такое структурирование узлов по ролям способствует выработке решения по разделению параметров безопасности на группы для их дальнейшей интеграции в соответствующие шаблоны безопасности. Анализ безопасности, выработка решений с подбором соответствующих параметров безопасности, а также примеры реального внедрения принятых решений подробно описываются в практическом курсе MCSE по безопасности сети от корпорации Microsoft.

В рамках настоящей практической работы для ознакомления с базовыми возможностями рассматриваемого программного средства **«Шаблоны безопасности»** в среде ОС Windows XP выполните следующее:

1. Разверните окно созданной ранее консоли администрирования MMC, если оно находится в свернутом состоянии на панели задач, или загрузите консоль снова.

2. Добавьте в корень дерева консоли MMC новую оснастку **«Шаблоны безопасности»** способом, изученным ранее, и разверните ее, чтобы были видны все ее элементы.

3. Создайте новый шаблон безопасности. Для этого выберите манипулятором мышь строку **«C:\WINDOWS\security\templates»**, показывающую локальное место хранения шаблонов безопасности в системе, и далее команду **«Создать шаблон…»** либо из выпадающего контекстного меню, либо из меню **«Действие»** на панели инструментов.

4. Откройте только что созданный шаблон безопасности и обратите внимание на то, что он включает в себя все семь категорий, описанных выше. Кроме того, просмотрите содержащиеся в нем политики безопасности и убедитесь, что все они находятся в состоянии **«Не определено»**.

Таким образом, создается пустой шаблон безопасности, в который можно внести все необходимые параметры, относящиеся к организуемой политике безопасности.

5. Сохраните созданный шаблон, открыв контекстное меню **«Действие»** и выбрав команду **«Сохранить как…»**. Имя шаблону присвойте, например, **MyFirstShablon** или определите его самостоятельно.

Как утверждалось ранее, ОС Windows XP изначально включает в себя ряд шаблонов безопасности, которые могут быть взяты в качестве основы для построения собственной политики безопасности. В частности, в распоряжении администратора может быть готовая политика безопасности, которая, в свою очередь, может быть улучшена и применена позже в системе.

По степени безопасности существуют четыре типа шаблонов:

- основной (Basic),
- безопасный (Secure),
- высокой степени безопасности (High secure),
- смешанный (Miscellaneous).

В качестве примера, среди штатных шаблонов безопасности находятся такие, как **Hisecdc** (сокр. **High secure domain controller**), который устанавливает самый высокий уровень безопасности для контроллера домена, или **Securews** (сокр. **Secure work station**) – устанавливает средний уровень безопасности для рабочих станций.

Любой из доступных шаблонов может быть использован для разработки собственной политики безопасности.

Внимание! Перед модификацией штатного шаблона безопасности его следует предварительно сохранить под другим именем, чтобы он не был испорчен перезаписью.

6. Для создания шаблона безопасности, обладающего стандартной функциональностью, возьмите за основу системный шаблон **Setup security**, обеспечивающий уровень безопасности по умолчанию, и сохраните его с другим именем, выбранным самостоятельно или, например, **MySecondShablon**.

7. В только что сохраненном шаблоне выберите самостоятельно и измените несколько политик безопасности. При необходимости воспользуйтесь теми системными политиками, которые уже изменялись в предыдущих заданиях, например, при организации модели «гостевого доступа». Сохраните сконфигурированный таким образом шаблон безопасности.

8. Примените созданный шаблон безопасности в системе. Для этого в оснастке **«Политика «Локальный компьютер»** щелкните дважды на разделе **«Конфигурация компьютера»** и разверните подраздел **«Конфигурация Windows»**. Щелкните правой кнопкой мыши по строке **«Параметры безопасности»**, а затем – по команде **«Импорт политики»**. Выберите созданный шаблон безопасности и импортируйте его в систему, нажав **ОК**.

Примечание. Для возврата системных параметров безопасности в состояние **«по умолчанию»** примените в системе штатный, неизмененный шаблон безопасности **Setup security**. Уровень безопасности ОС Windows XP будет приведен к начальному состоянию.

9. Сохраните и закройте консоль администрирования MMC.

При выполнении задания используйте следующие инструкции:

– перенесите последовательность выполняемых действий в отчет (возможно приведение графических фрагментов, сделанных с экрана, в качестве демонстрационного материала),

– перезагрузите компьютер и проверьте влияние новых значений системных параметров политик безопасности,

– сделайте вывод о проделанной работе и запишите его в отчет.

Задание №3.3. Изучение основных возможностей программного средства **«Анализ и настройка безопасности»** в среде ОС Windows XP на конкретных примерах.

Другим, не менее важным, штатным программным средством, предназначенным для анализа настроек некоторого шаблона безопасности и сравнения их с текущими настройками безопасности действующего в системе шаблона, является оснастка **«Анализ и настройка безопасности»**. Учитывая то, что в ОС Windows XP имеется огромное количество политик безопасности, отслеживать каждую из них по отдельности представляется проблематичным. Однако анализ безопасности системы посредством рассматриваемого инструмента позволяет обнаруживать «дыры» в системе, тестировать влияние группового изменения настроек безопасности в ОС без их непосредственного применения, а также выявлять любые отклонения в политике безопасности сети.

Для ознакомления с базовыми возможностями изучаемого инструмента **«Анализ и настройка безопасности»** в среде ОС Windows XP выполните следующее:

1. Разверните окно созданной ранее консоли администрирования MMC, если оно находится в свернутом состоянии на панели задач, или загрузите консоль снова.

2. Добавьте в корень дерева консоли MMC новую оснастку **«Анализ и настройка безопасности»** способом, изученным ранее, и выберите ее.

После этого шага инструмент **«Анализ и настройка безопасности»** будет доступен, но нефункционален. Для получения необходимой функциональности его предстоит предварительно сконфигурировать.

3. Поскольку работа данного инструмента основана на использовании базы данных, сначала ее необходимо создать. Инструмент позволяет создать базу данных конфигураций и анализа безопасности, также называемую локальной базой данных политики компьютера.

В идеальном случае, база данных должна создаваться сразу же после инсталляции ОС. В этих условиях в ней будут содержаться настройки параметров безопасности в состоянии «по умолчанию». Поэтому при необходимости данная база может быть экспортирована сразу после загрузки системы и быть всегда доступной на случай «отката» к первоначальным настройкам.

Создайте новую базу данных. Для этого в меню **«Действие»** выберите команду **«Открыть базу данных...»**, введите в появившемся диалоговом окне новое

имя базы данных (имя выберите самостоятельно) и щелкните на кнопке **«Открыть»**. В следующем окне выберите созданный ранее шаблон безопасности с именем **MyFirstShablon** и импортируйте его в базу данных, подтвердив намерение командой **«Открыть»**.

Если все сделано без ошибок, то при выборе оснастки **«Анализ и настройка безопасности»** в верхней части области сведений консоли администрирования MMC будет отображаться системный путь, где хранится только что созданная база данных системы безопасности ОС Windows XP.

4. Для анализа сформированной базы данных необходимо выбрать манипулятором мышь оснастку **«Анализ и настройка безопасности»**, а затем – команду **«Анализ компьютера…»** в контекстном меню **«Действие»** (альтернативным способом данную команду можно выбрать из выпадающего контекстного меню, если щелкнуть правой кнопкой мыши по выбранной оснастке). В появившемся диалоговом окне обратите внимание на системный путь и имя файла журнала ошибок, в котором будут сохраняться результаты анализа. При необходимости путь по умолчанию и имя файла могут быть заменены на более подходящие для организации удобного доступа.

Нажмите **ОК** для подтверждения операции анализа безопасности. В процессе проверки безопасности системы в окне состояния будет отображаться ход выполнения задания. По окончании анализа результаты отображаются справа, в области сведений, и появляется возможность просмотра и изменения необходимых настроек политик безопасности.

Если необходимо, просмотр файла журнала ошибок может быть осуществлен посредством выбора соответствующей команды **«Показать файл журнала»** в меню **«Действие»** на панели инструментов.

5. Последовательно проанализируйте параметры безопасности двух разделов **«Политики паролей»** и **«Локальные политики»**, щелкнув манипулятором мышь по каждому из включенных подразделов. Обратите внимание, что в области сведений справа отображаются теперь три колонки с названиями **«Политика»**, **«Параметр базы данных»** и **«Параметр компьютера»**, то есть имеется возможность сравнения действующих в системе и настраиваемых системных параметров политик безопасности.

6. Измените в базе данных несколько выбранных самостоятельно параметров безопасности анализируемых политик. Для этого щелкните манипулятором мышь

на выбранной политике и измените системное значение параметра в появившемся диалоговом окне **«Свойства»**, предварительно установив флажок **«Определить следующую политику в базе данных»**. Описание сущности изменяемого параметра безопасности доступно на соответствующей вкладке **«Объяснение параметра»** окна **«Свойства»**.

Внимание! Имейте ввиду, что изменяемые системные параметры влияют только на базу данных, а не на текущие параметры компьютера.

Таким образом, сравнивая текущие параметры действующей в системе политики безопасности можно настроить необходимые системные параметры с целью их экспортирования в новый шаблон безопасности и дальнейшего использования в ОС Windows XP.

7. Экспортируйте базу данных только что измененных параметров в новый шаблон безопасности с именем **MyThirdShablon**. Сохраните консоль ММС, выгрузите и загрузите ее снова. Проверьте наличие шаблона **MyThirdShablon** в оснастке **«Шаблоны безопасности»** и действительность изменения выбранных параметров политик безопасности внутри шаблона.

Таким образом, созданный шаблон безопасности теперь может быть, при необходимости, применен в системе способом, изученным в предыдущем задании практической работы.

8. Закройте консоль администрирования ММС, сохранив ее.

При выполнении задания используйте следующие инструкции:

– перенесите последовательность выполняемых действий в отчет (возможно приведение графических фрагментов, сделанных с экрана, в качестве демонстрационного материала),

– сделайте вывод о проделанной работе и запишите его в отчет.

Задание №3.4. Изучение основных возможностей программного средства **«Брандмауэр подключения к Интернету»** в среде ОС Windows XP на конкретных примерах.

Теперь, когда основные действия по предотвращению несанкционированного локального проникновения определены, необходимо обеспечить дополнительный уровень защиты от потенциальных атак извне. Одним самых важных, штатных компонентов защиты ОС Windows XP от внешних угроз является инструмент, ограничивающий обмен информацией между локальной средой и сетью Интернет, **«Брандмауэр подключения к Интернету»** (Internet Connection Firewall, **ICF**), коротко брандмауэр или сетевой экран.

ICF представляет собой достаточно мощную систему защиты, которая отслеживает все аспекты работы линий связи и проверяет исходные и конечные адреса информационных пакетов. Для предотвращения попадания нежелательного трафика в локальную сеть из Интернета **ICF** содержит список всех соединений контролируемого компьютера, располагающихся в специальной таблице. Входящий трафик сравнивается с данными из этой таблицы и при несовпадении входящие пакеты блокируются. В частности, это препятствует атакам в виде сканирования портов из сети Интернет. При этом стоит помнить, что **ICF** блокирует любой пакет, неожиданно приходящий в локальную сеть, включая те, которые могут быть полезны пользователю, например, пакеты электронной почты. Поэтому **ICF** необходимо сконфигурировать таким образом, чтобы исключить подобные коллизии и пропускать сообщения, направляя их соответствующему адресату.

Для ознакомления с базовыми возможностями брандмауэра ICF в среде ОС Windows XP выполните следующее:

1. Включите **ICF** в среде ОС Windows XP. Для этого необходимо выбрать сетевое подключение (**«Пуск | Панель управления | Сетевые подключения»**), предполагаемое к защите посредством **ICF**. Затем, либо из контекстного меню выбрать команду **«Свойства»**, либо щелкнуть по команде **«Изменение настроек подключения»** слева в группе команд **«Сетевые задачи»**. В окне **«Свойства сетевого подключения»** на вкладке **«Дополнительно»** необходимо щелкнуть по кнопке **«Параметры»** брандмауэра Windows и закрыть несанкционированный

доступ из сети, выбрав **«Включить (рекомендуется)»** на появившейся вкладке **«Общие»**.

2. Для обеспечения контроля за действиями **ICF** в системе предусмотрен механизм ведения журнала безопасности, который позволяет создавать список действий системы защиты, а именно установку запрета или разрешения на трафик со стороны **ICF**. Это бывает весьма полезно при организации безопасной среды. Включение процесса документирования за действиями **ICF** осуществляется на вкладке **«Дополнительно»** брандмауэра Windows. Для этого необходимо щелкнуть по кнопке **«Параметры»** в разделе **«Ведение журнала безопасности»**, поставить опциональные флажки напротив **«Записывать пропущенные пакеты»** и **«Записывать успешные подключения»**. Подтвердите операцию, нажав **ОК**.

Кроме того, имеется возможность регулировать дополнительную функциональность по протоколу управляющих сообщений Интернета ICPM (в частности, позволяющего компьютерам в сети обмениваться информацией об ошибках). Список запросов из сети Интернет, на которые будет отвечать конфигурируемый компьютер, представлен в виде набора параметров в разделе **«Протокол ICMP»** на вкладке **«Дополнительно»**.

Включите протоколирование следующих сообщений:

- входящих эхо-запросов;
- входящих меток времени;
- входящих запросов маршрутизатора;
- переадресацию.

Уместно отметить, что по своей сути журнал **ICF** является программным средством, также предназначенным для аудита системы безопасности наряду с теми, которые изучаются в соответствующей практической работе. К числу подобных средств также следует отнести автономную оснастку **«Просмотр событий»**, расширение **«Политика аудита»** в рамках оснастки **«Политика «Локальный компьютер»**, а также рассмотренную в предыдущем задании оснастку **«Анализ и настройка безопасности»**.

В частности, посредством расширения **«Политика аудита»** можно осуществлять проверку и регистрацию событий в следующих категориях:

- управление учетной записью,
- ввод-вывод данных в сети,
- доступ к конкретному объекту (файлу или каталогу),

- изменение политик сети,
- попытки использования специальных привилегий,
- загрузка пользовательских процессов,
- другие системные действия.

Поскольку аудит в значительной степени расходует системные ресурсы, необходимо заранее определиться с элементами, требующими контроля (иными словами, надо четко представлять себе, что необходимо контролировать, чтобы излишне не нагружать систему).

3. Журнал **ICF** имеет свой уникальный формат. В заголовке указываются версия используемого межсетевого экрана **ICF**, имя журнала безопасности, примечание о том, что вход в систему регистрируется по локальному времени, и список доступных полей для регистрационных записей (табл. 3.2).

Польза журнала безопасности **ICF** состоит в том, что после его просмотра можно обнаружить попытки несанкционированного доступа к сети. Изучив поля **action**, **scr-ip** и **dst-ip**, в частности, можно определить, пытается ли кто-то повредить сеть в целом или вывести из строя какое-то определенное устройство.

В любой текстовый редактор загрузите журнал безопасности **ICF**, располагающийся в системном каталоге **C:\Windows\pfirewall.log** и найдите все его отмеченные атрибуты, поля и изучите содержимое журнала в целом, воспользовавшись таблицей 3.2. Вероятно, может оказаться, что осуществленных записей в журнале ICF будет не слишком много – это связано с тем, что журнал безопасности был активирован сравнительно недавно.

Дополнительно журнал безопасности ICF может быть переименован и сохранен в место, путь к которому системный администратор определяет самостоятельно. Это удобно в том случае, когда имеется необходимость вести несколько отчетов, например, по дням недели или времени дня. Размер файла журнала безопасности ICF может быть изменен на вкладке **«Параметры журнала»** с установленного в 4Мб по умолчанию до 32Мб по необходимости.

Таблица 3.2. Поля ввода данных в журнале безопасности **ICF**

№ п/п.	Поле журнала безопас-ности ICF	Описание поля
1.	**Action**	Операция, перехваченная брандмауэром Windows. Входящие данные включают в себя: **OPEN**, **CLOSE**, **DROP**, **INFO-EVENTS-LOST** (указывается количество произошедших событий, не сохраненных в журнале).
2.	**Date**	Дата ввода файла в формате **YY-MM-DD** (год-месяц-день).
3.	**Dst-ip**	**IP**-адрес конечного пункта доставки пакета.
4.	**Dst-port**	Номер порта конечного пункта доставки пакета.
5.	**Icmpcode**	Число, обозначающее поле кода в **ICMP**-сообщении.
6.	**Icmptype**	Число, обозначающее поле ввода текста в **ICMP**-сообщении.
7.	**Info**	Поле для ввода информации о событии, которое зависит от типа действия.
8.	**Protocol**	Протокол связи. Если это не **TCP**, **UDP** или **ICMP**, то здесь указывается цифра.
9.	**Size**	Размер пакета (байт).
10.	**Scr-ip**	**IP**-адрес устройства-отправителя.
11.	**Scr-port**	Номер порта отправителя.
12.	**Tcpack**	**TCP**-номер подтверждения пакета.
13.	**tcp-flags**	**TCP**-флаг, указываемый в начале пакета: **A** – Ack (важность поля подтверждения), **F** – Fin (последний пакет), **P** – Psh (функция «проталкивания» пакета), **S** – Syn (синхронизация последовательности номеров), **U** – Urg (важность поля указателя срочности).
14.	**Tcpsyn**	**TCP**-последовательность номеров пакетов.
15.	**Tcpwin**	**TCP**-размер окна (байт).
16.	**Time**	Время регистрации файла в формате **HH:MM:SS** (часы:минуты:секунды).

4. Иногда в процессе работы возникает необходимость не контролировать брандмауэром ICF трафик, проходящий в сети через доверенные специализированные приложения, например, приложения контроля информационных пакетов, торрент-клиенты или трафик, проходящий через

определенные открытые порты, например, настроенные под так называемый «портфорвардинг». Для этих целей в **ICF** предусмотрена возможность исключений.

Для активации данной возможности по отношению к программам на вкладке **«Исключения»** брандмауэра Windows добавьте, для примера, выбранное приложение, генерируемый трафик которого не будет контролироваться впредь. Закройте окно **«Добавление программы»** и обратите внимание на то, что только что выбранная программа появилась в области исключений **«Программы и службы»** на исследуемой вкладке (напротив неконтролируемого приложения стоит флажок активации, снятие которого обратно приводит к контролю трафика этого приложения).

При выполнении задания используйте следующие инструкции:

– перенесите последовательность выполняемых действий в отчет (возможно приведение графических фрагментов, сделанных с экрана, в качестве демонстрационного материала),

– сделайте вывод о проделанной работе и запишите его в отчет.

Изученные в первом задании практической работы инструменты и возможности не являются исчерпывающими для всеобъемлющей организации сетевой безопасности в ОС (спектр специализированных программных средств, предназначенных для локальной и сетевой защиты компьютера, достаточно широк, а его детальное рассмотрение в практикуме не представляется возможным), однако в первом приближении они позволяют обезопасить локальную рабочую среду и в некоторой степени защитить ее от сетевого проникновения извне.

ЗАКЛЮЧЕНИЕ

Методические указания для выполнения практических работ по дисциплине "Операционные системы ЭВМ" позволяет изучить практические основы настройки и администрирования операционных систем Windows семейства NT и UNIX. После выполнения всех практических работ студенты получают достаточный уровень в области работы с операционными системами. Для получения более углубленных знаний в этой сфере предлагается использовать руководство к выполнению лабораторных работ по данной дисциплине.

ЛИТЕРАТУРА

1. Танненбаум Э. Современные операционные системы. 3-е изд. – СПб.:Питер, 2010. – 1120 с.: ил. – (Серия "Классика Computer Science").

2. Олифер В.Г., Олифер Н.А. Сетевые операционные системы. – СПб.: Питер, 2002. – 544 с.: ил.

3. Руссинович М., Соломон Д. Внутреннее устройство Microsoft Windows: Windows Server 2003, Windows XP и Windows 2000. Мастер-класс. / Пер. с англ. – 4-е изд. – М.: Издательско-торговый дом "Русская Редакция"; СПб.: Питер, 2005. – 992 с.: ил.

4. Пахмурин Д.О. Операционные системы ЭВМ: Учебное пособие. – Томск: Томский государственный университет систем управления и радиоэлектроники, 2013. – 254 с.: ил.

5. Пахмурин Д.О. Операционные системы ЭВМ: Учебно-методическое пособие. – Томск: Томский государственный университет систем управления и радиоэлектроники, 2015. – 155 с.: ил.