Московский государственный технический университет
имени. Н.Э.Баумана

В.М. Постников, С.Б. Спиридонов

Эксплуатация АСОИиУ

Методические указания
к лабораторному практикуму по курсу
“Эксплуатация автоматизированных систем
обработки информации и управления”

Москва
Издательство МГТУ им.. Н.Э. Баумана
2019 г.

Оглавление

Работа № 2 Администрирование сервера АСОИиУ, построенных на основе ЛВС с операционной системой Windows Server

Часть 1. Администрирование сервера АСОИиУ, построенных на основе ЛВС с ОС Windows Server

Цель работы: Изучение задач, решаемых администратором сети, и средств для их решения, освоение принципов администрирования сетей и получение начальных навыков работы в качестве администратора сети, управляемой сетевой ОС Windows Server.

Продолжительность работы: - 4 часа.

1. Особенности операционной системы Microsoft Windows Server.

Microsoft Windows Server — это операционная система, которая помогает ИТ-специалистам полностью контролировать инфраструктуру, обеспечивая доступность, управляемость, функциональность, гибкость, безопасность, надежность и устойчивость серверной среды.

Microsoft Windows Server позволяет:

- оптимизировать и упростить процесс установки сетевой ОС;
- использовать эффективные средства группового администрирования;.
-обнаруживать и устранять неполадки с помощью эффективных и мощных средств диагностики.

Современные АСОИиУ, как правило, строят на базе кластеров серверов, которые могут объединять до 8 серверов. Мастер настройки сервера позволяет устанавливать или удалять роли сервера, среди которых следует выделить следующие: веб-сервер, сервер печати, сервер факсов, сервер удаленного доступа, сервер доменных имен и т.д.

Microsoft Windows Server является многозадачной операционной системой, способной централизовано или распределено управлять различными наборами ролей, в зависимости от потребностей пользователей.

2. Основные теоретические сведения

Важным моментом в деятельности администратора сети является настройка политики безопасности сети, состоящей из домена (набора взаимодействующих серверов, входящих в его состав), отдельных серверов и локальных компьютеров. Политика безопасности домена или одного сервера представляет собой сочетание всех тех параметров, которые регулируют его безопасность и позволяют администратору сети решать следующие задачи:

- обеспечить только санкционированный доступ пользователей к серверу;
- задать ресурсы, которые может использовать каждый пользователь;
- управлять ведением журнала событий, т.е. включить или отключить запись действий пользователя (или группы) в журнал событий.

Политика безопасности каждого компьютера определяется политикой безопасности домена и сервера. Параметры безопасности группы имеют приоритет над параметрами локального компьютера. При изменении любого параметра политика безопасности обновляется не сразу. Параметры безопасности обновляются каждые 90 минут на компьютере или сервере и каждые 5 минут на контроллере домена. Кроме того, независимо от наличия изменений эти параметры обновляются каждые 16 часов. Для немедленного вступления изменений в силу следует в командной строке соответствующего сервера набрать: grupgrade.exe.

Для изменения локальной политики безопасности следует набрать команду: Пуск\ Администрирование\ Локальная политика безопасности.

На экране монитора появляется окно для настройки рабочих параметров локальной политики безопасности. В частности, используя информацию, приведенную в этом окне, можно: задать политику аудита, присвоить права пользователям, установить параметры безопасности для защиты сервера.

Шаблон политики безопасности домена аналогичен шаблону локальной политики безопасности. Он отличаются тем, что политика безопасности домена применяется ко всем серверам в домене, а не только к одному

локальному серверу, на котором он установлен. Политика безопасности домена настраивается с консоли следующим образом

Пуск\ Администрирование \Политика безопасности домена

Политика ограничения программ позволяет администратору задать программы, которые можно запускать на компьютере, и учетные записи пользователей, имеющих доступ к этим программам.

Файловую систему сервера отличают следующие особенности:

- надежность (или усовершенствованная отказоустойчивость), поскольку введен механизм транзакций, при котором незавершенные файловые операции отменяютя;.
- гибкость, поскольку размер кластера может изменяться в широких пределах от 512 байт. до 64 Кбайт;
- поддерживает длинные имена файлов;
- поддерживает шифрование и прозрачное сжатие файлов;.
- мощная модель безопасности, включающая до 13 атрибутов файлов;

Для ограничения доступа локальных и удаленных пользователей к каталогам (папкам) и файлам, расположенных на сервере, администратор сети устанавливает для них разрешения. Для каждого файла или папки можно назначить или запретить до семи основных разрешений, которые приведены в табл.2.1:

При большом количестве пользователей их следует разбить на локальные группы, которые представляют собой наборы пользователей, которым предоставляются одинаковые и вполне определенные права доступа к одним и тем же ресурсам сервера.

Для упрощения процесса администрирования разрешения на доступ к определенным папкам и файлам можно назначить каждой локальной группе пользователей отдельно, а в дальнейшем следует просто добавить в эту группу (или исключить из нее) новых пользователей без изменения набора разрешений.

Таблица 2.1

Основные типы разрешений для работы с файловой системой сервера

№	Разрешение	Описание
1	Full Control (Полный доступ)	Обеспечивает полное управление папками и файлами, в том числе позволяет назначать разрешения
2	Modify (Изменить)	Предоставляет все разрешения, кроме возможности присвоить владение и назначать разрешения. Позволяет читать, удалять, изменять и перезаписывать файлы и папки
3	Read & Execute (Чтение и выполнение)	Чтение разрешений и запуск программных файлов
4	List (Folders Only) (Чтение содержимого папки)	Позволяет просматривать имена файлов и подпапок внутри папки
5	Read (Чтение)	Обеспечивает просмотр, копирование, печать и переименование файлов, папок и объектов. Не позволяет запускать выполняемые программы, кроме файлов сценариев. Позволяет считывать разрешения объектов, атрибуты объектов и расширенные атрибуты (например, бит Archive, EFS). Позволяет составить список файлов и подпапок папки
6	Write (Запись)	Разрешения чтения, плюс создание и перезапись файлов и папок
7	Special Permissions (Особые разрешения)	Позволяет составлять комбинации из 14 более детальных разрешений, которые не входят ни в одно из остальных 6 основных разрешений.

Сетевая ОС имеет системный монитор, который содержит много объектов и счетчиков, позволяющих собирать статистику по работе основных ресурсов сервера: процессора, памяти, физических дисков и т.д. Ниже для объектов процессор, физический диск и система приведены счетчики, которые используются администратором сети наиболее часто.

Объект процессор имеет счетчики:

- % времени С1, - доля времени, в течение которого процессор простаивает

- % времени прерываний, доля времени, которое процессор тратит на получение и обслуживание аппаратных прерываний.

- % загруженности процессора, доля времени, которую процессор тратит на обработку всех потоков команд.

Объект физический диск имеет счетчики:

- процент активности диска, процент времени, затраченного выбранным дисковым устройством на обработку запросов на чтение и запись данных.

- обращений записи на диск/сек, частота выполнения операций записи на этот диск.

- обращений чтения с диска/сек, частота выполнения операций чтения с этого диска.

- обращений к диску/сек, частота выполнения операций чтения и записи на этот диск.

- скорость записи на диск (байт/сек), скорость, с которой происходит передача данных на этот диск при выполнении операций записи.

- скорость чтения с диска (байт/сек), скорость, с которой происходит передача данных с этого диска при выполнении операций чтения.

-скорость обмена с диском (байт/сек) , скорость, с которой происходит обмен данными с этим диском при выполнении операций чтения или записи.

- среднее время записи на диск, время в секундах, затрачиваемое в среднем на одну операцию записи данных на диск.

- среднее время чтения с диска, время в секундах, затрачиваемое в среднем на одну операцию чтения данных с диска.

- среднее время обращения к диску, время в секундах, затрачиваемое в среднем на один обмен данными с диском.

- средний размер одной записи на диск (байт) , среднее количество байт данных, переданных на диск при выполнении операций записи.

- средний размер одного чтения с диска (байт) , среднее количество байт данных, полученных с диска при выполнении операций чтения.

- средний размер одного обмена с диском (байт), среднее количество байт данных, переданных при выполнении операций чтения или записи.

-средняя длина очереди записи на диск, среднее количество запросов на запись, которые были поставлены в очередь для соответствующего диска в течение интервала измерения.

-средняя длина очереди чтения диска, среднее количество запросов на чтение, которые были поставлены в очередь для соответствующего диска в течение интервала измерения.

- средняя длина очереди диска, это среднее общее количество запросов на чтение и на запись, которые были поставлены в очередь для соответствующего диска в течение интервала измерения.

-текущая длина очереди диска, количество невыполненных запросов к диску во время сбора сведений о загруженности.

Объект система: имеет счетчики:

- операций чтения файлов/сек, среднее число всех операций чтения файловой системы данного компьютера.

- системных вызовов/сек - это частота обращений к процедурам системных служб операционной системы.

-счетчик потоков, количество потоков в компьютере в момент сбора информации.

- счетчик процессов, количество процессов в компьютере в момент сбора информации.

Сетевая ОС имеет также компоненту “Журналы и оповещения производительности”, которая позволяет собирать данные о производительности компьютеров и их компонент в автоматическом режиме. Данные этих журналов и счетчиков можно просмотреть в системном мониторе в виде диаграмм или гистограмм. Ведение журналов является наиболее распространенным способом наблюдения за работой сети. Это наблюдение следует осуществлять с интервалом не менее 15 минут.

При наблюдении за большим числом объектов и счетчиков записываются большие объемы данных, занимающих дисковое пространство и существенно снижающих производительность сети. Администратор должен определить оптимальное соотношение между числом наблюдаемых объектов и частотой обновления данных, чтобы размер файла журнала был не слишком большим.

Наблюдения за работой сети позволяют администратору обнаружить избыточный спрос на определенные ресурсы сети, который приводит к возникновению узких мест в работе сети. Основные причины возникновения узких мест и рекомендации по их устранению следующие:

- если недостаточно ресурсов (например, производительности процессора или объема оперативной памяти), то требуется их наращивание или модернизация, т.е. замена на более производительные;
- если ресурсы используются неравномерно (например, диски), то требуется перераспределение информации, находящейся на них;
- если ресурс частично неисправен (например, диск с большим количеством неисправных секторов), то требуется его замена;
- если ресурс используется программой в монопольном режиме, то требуется замена или корректировка этой программы;
- если ресурс неправильно настроен (например, размер кадра передаваемого по сети отличного качества составляет всего 512 байт), то требуется перенастройка этого параметра на 1500 байт.

3. Порядок выполнения лабораторной работы

Задание включает последовательное выполнение следующих работ.

3.1. Исследование процесса подключения к серверу с правами администратора.

3.2. Создание пользователей, установка и исследование режима их работы.

3.3. Установка и исследование политики безопасности

3.4 .Установка и исследование процесса сбора статистических данных о работе основных ресурсов сервера: процессора, памяти, дисков. Построение графиков загрузки и использования основных ресурсов сервера.

3.5 Определение узких мест сервера, выработка рекомендаций по их устранению. Устранение узких мест сервера (под руководством преподавателя).

3.1 Исследование процесса подключения к серверу с правами администратора

3.11. Для подключения выберите файл-сервер с именем «Windows server 2003». В меню для разрешения подключения пользователя к этому файл-серверу последовательно задайте имя и пароль пользователя, в данном случае администратора. Имя и пароль дает преподаватель.

3.1.2 Если указанные параметры введены правильно, то Вы подключились к серверу, на экране появится главное меню администратора системы «Управление данным сервером». Если это меню не появилось, то допущена ошибка при вводе исходных данных, следует повторно набрать имя и пароль администратора

3.1.3 Допустите ошибки (по указанию преподавателя) при наборе имени и пароля администратора, а также их комбинаций, Исследуйте и зафиксируйте реакции системы на допущенные ошибки.

3.2 Создание пользователей, установка и исследование режима их работы.

3.2.1. Выберите в меню «Управление данным сервером», которое находится на экране монитора, режим администрирования. На экране монитора появится список функций, которые разрешены администратору системы.

3.2.2 Исследуйте, под руководством преподавателя, набор функциональных возможностей администратора системы, их назначение и особенности использования.

3.2.3 Выберите функцию «локальная политика безопасности». На экране монитора появится набор функций политики безопасности.

3.2.4 Используя функцию «политика учетных записей», под руководством преподавателя, исследуйте функциональные возможности администратора системы по созданию нового пользователя и установке режима его работы.

3.2.5 Создайте нового пользователя и установите режим его работы по данным, указанным преподавателем.

3.2.6 С помощью функции «политика паролей» установите для созданного пользователя пароль по данным, указанным преподавателем.

3.2.7.Выйдите из системы. Подключитесь снова к серверу, но под именем созданного вами нового пользователя и его пароля.

3.2.8 Исследуйте особенности режима работы, установленные для нового пользователя, и зафиксируйте ответы ОС на все ваши действия.

3.3 Установка и исследование политики безопасности

3.3.1 Подключитесь к серверу с правами администратора. Выберите в меню «Управление данным сервером», которое находится на экране монитора, режим администрирования. Выберите функцию администратора «локальная политика безопасности». На экране монитора появится набор функций политики безопасности.

3.3.2 Исследуйте возможности функции «политика паролей»: установка граничных значений для длины пароля, срока его действия и требования, которые предъявляются к сложности пароля.

3.3.3 Изучите и исследуйте возможности функции «политика блокировки учетных записей» и выделите основные режимы блокировки.

3.3.4. Исследуйте возможности функции «локальная политика», направленные на назначение пользователям прав доступа к ресурсам системы.

3.3.5 Изучите и исследуйте возможности функции «политика аудита» и виды возможного аудита.

3.4 Установка и исследование процесса сбора статистических данных о работе основных ресурсов сервера:

3.4.1 Выберите в наборе функций администрирования функцию «производительность», а в ней выберите функцию «журналы и оповещения производительности». В состав последней функции входит функция «журналы счетчиков», в которой следует указать все счетчики, которые будут использованы для сбора статистических данных о работе аппаратно-программных ресурсов файл-сервера.

3.4.2. Сформируйте и запустите на решение набор рабочих задач по согласованию с преподаавателем.

3.4.3 Используя функцию «системный монитор» получите для таких ресурсов файл-сервера, как процессор, память и накопитель на жестком диске, основные их рабочие характеристики: коэффициент загрузки ресурса, средняя длина очереди к ресурсу в зависимости от набора решаемых задач.

3.4.4 Исследуйте графики загрузки ресурсов файл-сервера в зависимости от набора решаемых задач.

3.4.5 Определите, в зависимости от набора решаемых задач, средние длины очередей к ресурсам файл-сервера, которые указаны в следующих счетчиках:

Для процессора: Processor Queue Length

Для физического диска: Avg. Disk Queue Length

3.5 Определение узких мест сервера, выработка рекомендаций по их устранению. Устранение узких мест файл-сервера.

3.5.1. По данным, приведенным в пп.3.4.5, определите узкое место файл-сервера, т. е. ресурсы файл-сервера, к которым наибольшая очередь

3.5.2 Дайте обоснованные рекомендации по устранению узких мест файл-сервера.

3.5.3 Укажите дополнительные аппаратные или программные компоненты, необходимые для устранения узких мест файл-сервера.

4. Содержание отчета

Отчет о работе должен включать:

1. Краткую последовательность выполнения работы.
2. Таблицы и рисунки, иллюстрирующие режим работы пользователя.
3. Рекомендации по организации защиты информации на файл-сервере.
4. Таблицы и рисунки, иллюстрирующие работу основных ресурсов файл-сервера;
5. Исследования по выявлению узких мест файл-сервера и рекомендации по их устранению.

5. Контрольные вопросы

1. Какие функции включает политика безопасности файл-сервера.?

2 .Перечислите основные типы разрешений для работы с папками и файлами файл-сервера и дайте пояснения по их использованию?

3. Перечислите основные атрибуты файлов и дайте пояснения по их использованию?

4. Какие счетчики и объекты следует использовать для сбора информации, позволяющей оценить эффективность работы файл-сервера сети?

5. Поясните, когда следует применять методику определения узких мест файл-сервера сети?

5.1. Вопросы категории **«Помнить».**

1. Какие функции включает политика безопасности файл-сервера.?

2. Перечислите основные атрибуты файлов и дайте пояснения по их использованию?

5.2. Вопросы категории **« Понимать».**

1 Перечислите основные типы разрешений для работы с папками и файлами файл-сервера и дайте пояснения по их использованию?

2. Поясните принцип назначения разрешений пользователям на доступ к общим ресурсам, при работе в сети под управлением Windows Server 2003.

3. Какие из перечисленных ниже защитных политик в Windows Server 2003 позволят заставить пользователей применить пароли определённой длины?:

- политики аудита; - групповые политики;
- политики проверки подлинности; - списки управления доступом.

5.3. Вопросы категории **« Применять».**

1. Какие счетчики и объекты следует использовать администратору для сбора информации и оценки эффективности работы дисков файл-сервера?

2. Поясните, когда администратору следует применять методику определения узких мест файл-сервера сети.

3. Поясните, когда администратору следует объединять пользователей в группы.

6. Практические навыки и компетенции, получаемые студентом после выполнения лабораторной работы

6.1. Студент должен **помнить:**

- перечень задач, решаемых администратором сети;
- особенности сетевых ОС семейства Windows;

- назначение и функциональные различия между понятиями: веб-сервер, сервер печати, сервер факсов, сервер файловый, сервер удалённого доступа.

6.2. Студент должен **понимать**:

- назначение политики безопасности, реализуемой в рамках возможностей сетевых ОС семейства Windows;
- суть основных (типовых) принципов администрирования сетей архитектуры «клиент-сервер»;
- влияние параметров настройки серверов на производительность сетей;
- возможности типов разрешений для работы с файловой системой сервера.

6.3. Студент должен научиться **применять**:

- средства администрирования сетевых ОС семейства Windows;
- настройки политики безопасности сервера, работающего под управлением ОС Windows Server, для разграничения прав доступа пользователей к его ресурсам;
- технологию групповых политик при настройке доступа большого числа пользователей к ресурсам сервера, работающего под управлением ОС Windows Server;
- настройки утилиты Performance Monitor с целью оценки характеристик производительности сервера, работающего под управлением ОС Windows Server.

7. Правила безопасности при выполнении работы

Запрещается без разрешения преподавателя:

- подключать компьютеры и сетевое оборудование к розеточной сети;
- открывать системные блоки серверов и стационарных компьютеров;
- подключать к розеточной сети дополнительное оборудование, не входящее в комплект средств, используемых в работе;
- подключать к портам коммутаторов оборудование, не входящее в комплект средств, используемых в работе;
- развинчивать коммутаторы, мониторы и мыши.

8. Рекомендуемые источники информации.

1.Постников В.М. Основы эксплуатации автоматизированных систем обработки информации и управления. Краткий курс: учеб. пособие. М.: Изд- во МГТУ им. Н.Э. Баумана, 2013. 180 с.
2. Постников В.М. , Черненький В.М. Методы принятия решений в системах организационного управления: учеб. пособие./ В.М. Постников, В.М. Черненький. М.: Изд-во МГТУ им. Н.Э. Баумана, 2014. 205 с.
3. .Постников В.М. Основы эксплуатации АСОИиУ. Часть 1. Техническое обслуживание: учеб. пособие. М.: Изд- во МГТУ им. Н.Э. Баумана, 2015. 192 с.
4. Постников В.М. Основы эксплуатации АСОИиУ. Часть 2. Администрирование и развитие: учеб. пособие. М.: Изд- во МГТУ им. Н.Э. Баумана, 2015. 190 с.
5. Поляк- Брагинский А. Администрирование сети на примерах: пер. с англ. СПб.: БХВ Петербург 2005.
6. Беленькая Н.М. Администрирование в информационных системах. М.: Горячая линия. Телеком. 2011.
7. Щепка П., Microsoft Windows Server 2003 Практическое руководство по настройке сети: пер. с англ. СПб.: НИТ 2006.

Часть 2. Исследование и настройка параметров реестра сетевых ОС семейства Windows

Цель работы: Изучение задач, решаемых администратором сети с помощью реестра сетевых ОС семейства Windows, освоение принципов администрирования сетей с помощью реестра и получение начальных навыков работы с реестром.

Продолжительность работы: - 4 часа.

1. Назначение реестра сетевых ОС семейства Windows

Реестр сетевых ОС семейства Windows администратор системы использует для настройки рабочих параметров системы с целью обеспечения эффективного функционирования АСОИиУ.

Системный реестр - база данных для хранения сведений о конфигурации компьютера и настроек его ОС. Системный реестр не имеет ограничений по объему.

2. Основные теоретические сведения

Любая ОС семейства Windows постоянно обращается во время ее загрузки и работы к системному реестру, который содержит следующие данные:

- профили всех пользователей, т. е. настройки режима их работы;
- конфигурацию оборудования, установленного на компьютере;
- данные об установленных программах и типах документов, создаваемых каждой программой;
- свойства папок;
- данные об используемых портах.

Для работы с системным реестром в ОС имеется встроенная утилита, которая называется Редактор реестра (Registry Editor). Утилита имеет небольшой размер, так в Windows XP – 133 Кбайта. Редактор реестра находится в файле regedit.exe. Запуск редактора реестра выполняется следующим образом:

Команды «пуск», «выполнить». На экране монитора появится окно, в этом окне в поле «открыть» введите команду: regedit.exe.

Системный реестр содержит пять основных разделов. Каждый раздел имеет собственное место хранения и файл журнала. При необходимости любой раздел реестра можно восстановить, не затрагивая остальные разделы. Основные разделы системного реестра приведены в табл.2.2:

Основные разделы реестра Таблица 2.2

№	Раздел системного реестра	Описание
1	HKEY_CURRENT_USER	В разделе хранятся настройки пользователя, вошедшего в систему, т.е. папки пользователя и настройки панели управления. Эти данные называются профилем пользователя.
2	HKEY_USERS	Раздел содержит все профили пользователей компьютера.
3	HKEY_LOCAL_MACHINE	Раздел включает все настройки, относящиеся к локальному компьютеру (для всех пользователей).
4	HKEY_CLASSES_ROOT	Раздел является подразделом HKEY_LOCAL_MACHINE\Software. Хранящиеся в разделе сведения обеспечивают открытие необходимой программы при открытии файла с помощью проводника.
5	HKEY_CURRENT_CONFIG	Раздел включает сведения о профиле оборудования, используемом локальным компьютером при запуске системы

При запуске утилиты Редактора реестра появляется окно, напоминающее стандартную программу Проводник системы Windows. В левом поле окна этой программы находятся названия разделов, подразделов и параметров, а в правом - их значения Основные типы данных системного реестра приведены в табл.2.3:

Основные типы данных системного реестра Таблица 2.3

№	Тип данных	Описание
1	REG_BINARY	Включает в себя двоичные данные; информация хранится в двоичном виде и отображается в шестнадцатеричном формате
2	REG_DWORD	Представляет собой целые числа размером в 4 байт, и отображается в двоичном, шестнадцатеричном или десятичном форматах.
3	REG_EXPAND_SZ	Представляет собой строку данных переменной длины.
4	REG_MULTI_SZ	Содержит многострочный текст, удобный для чтения.
5	REG_FULL_RESOURCE_DESCRIPTOR	Представляет собой последовательность вложенных массивов, с помощью которой хранятся списки ресурсов оборудования или драйверов

Некоторые важные параметры системного реестра, касающиеся сетевой безопасности, приведены в табл 2.4

Параметры реестра, касающиеся сетевой безопасности, Таблица 2.4

№	Параметр системного реестра	Описание
1	[HKEY_LOCAL_MACHINE\Software\Microsoft\ Windows\CurrentVersion\Policies\Network] AlphanumPwds=1	Позволяет требовать пароли только из букв и цифр. Может обязать пользователя всегда комбинировать в паролях буквы и цифры
2	[HKEY_LOCAL_MACHINE\SOFTWARE\Micro soft\Windows\CurrentVersion\Policies\Network] MinPwdLen=hex:6	Обеспечивает установку минимального количества символов в паролях
3	[HKEY_CURRENT_USER\Software\Microsoft\W indows\CurrentVersion\Internet Settings] DisablePasswordCaching=1	Запрещает кэширование паролей..
4	[HKEY_LOCAL_MACHINE\Software\Microsoft\ Windows\CurrentVersion\Policies\Network] HideSharePwds=1	Не показывает пароли при вводе. При попытке доступа к защищенному паролем ресурсу Windows не скрывает пароль, который вводят. Позволяет заменять символы пароля звездочками:
5	[HKEY_LOCAL_MACHINE\SYSTEM\CurrentC ontrolSet\Services\LanmanServer\Parameters] Hidden=1	Позволяет включить режим, при котором в режиме обзора сети другие пользователи не будут видеть вашего компьютера:
6	[HKEY_LOCAL_MACHINE\SOFTWARE\Micro soft\Windows\CurrentVersion\Internet Settings\Cache] Persistent=0	Автоматически удаляет временные файлы после работы в Интернет. При значении, равном нулю, заставит Internet Explorer удалять все временные файлы, оставшиеся после работы в Интернет, а при значении равном единице1, позволит оставить эти файлы на диске.
7	[HKEY_LOCAL_MACHINE\Software\Microsoft\ Windows\CurrentVersion\Policies\Explorer] NoInstrumentation=1	Запрещает записывать, с какими приложениями недавно работал пользователь и к каким документам получал доступ:

Основные действия с системным реестром следующие: импорт, экспорт, создание разделов, создание строкового параметра, создание двоичного параметра.

Для управления записями системного реестра нужно открыть соответствующую ветвь реестра и щелчком правой кнопки мыши вызвать контекстное меню. В нем можно выбрать один из следующих пунктов:

переименовать, изменить, изменить двоичные данные, удалить . Также для каждого параметра и ветви системного реестра можно задавать разрешения на чтение/запись каждому пользователю или группе пользователей. Для этого следует выбрать конкретную ветвь и выбрать пункт меню «правка – разрешения»

3. Порядок выполнения работы

Задание включает последовательное выполнение следующих работ.

3.1. Анализ способов запуска редактора системного реестра.

3.2 Анализ состава и структуры редактора системного реестра.

3.3 Анализ состава и структуры системного реестра.

3.4 Анализ процессов задания параметров реестра с помощью редактора.

3.5 Исследование влияния параметров реестра на временные характеристики функционирования компьютеров рабочей группы.

3.6 Исследование возможного наличия записей вредоносных программ в системном реестре (на примере «троянских программ»).

3.1. Анализ способов запуска редактора системного реестра.

Проведите сравнительный анализ пяти способов запуска редактора реестра в ОС Windows.:

3.1.1 Вход в редактор реестра через клавишу «Пуск» из диалогового окна «Выполнить»:

- нажмите на клавиатуре на клавиши «Пуск»;
- в появившемся окне выберите строку «Выполнить»;
- в поле «Открыть» введите выражение: «regedit» (без кавычек);
- нажмите на кнопку «Enter». После этого на экране монитора компьютера появится окно Редактора реестра.

3.1.2 Вход в редактор реестра из папки Windows:

- откройте Проводник на своем компьютере:.
- войдите на диск «C:», откройте папку «Windows»;.

- найдите, а затем кликните два раза левой кнопкой мыши по приложению «regedit», появится окно редактора реестра.

3.1.3 Вход в редактор реестра из командной строки:

- запустите командную строку от имени администратора;.
- в окне интерпретатора командной строки введите: «regedit» (без кавычек);
- нажмите на клавишу «Enter» появится окно редактора реестра.

3.1.4 Вход в редактор реестра с помощью Windows Power Shell:

- запустите Windows PowerShell от имени администратора;.
- в окне PowerShell введите: «regedit» (без кавычек), а потом нажмите «Enter», появится окно редактора реестра.

3.1.5 Вход в редактор реестра с помощью клавиши «Win»:

- нажмите одновременно на клавиатуре на клавиши «Win» + «R».;
- в появившемся окне «Выполнить» в поле «Открыть» введите выражение: «regedit» (без кавычек);
- нажмите на кнопку «Enter». Появится окно редактора реестра.

3.2 Анализ состава и структуры редактора системного реестра.

3.2.1 Запустите любым из рассмотренных ранее способов редактор реестра. Появится окно редактора реестра, состоящее из четырех областей:

- строка меню (вверху окна), содержит пункты меню, изучите назначение этих пунктов и их функциональные возможности;
- строка состояния (внизу окна), содержит полный путь к разделу реестра, в составе которого содержится выбранный (выделенный) параметр;
- в левой панели отображается иерархия разделов и подразделов реестра;
- в правой панели показаны текущие значения параметров выбранного раздела или подраздела реестра.

Изучите назначение и функциональные возможности команд строки меню.

. 3.2.2 Изучите и исследуйте функциональные возможности команд modify (изменить), new (создать), rename (переименовать), delete (удалить),

входящих в состав пункта меню edit (редактирование), расположенного в строке меню

3.3 Анализ состава и структуры системного реестра.

3.3.1 Перед исследованием состава и структуры реестра, а тем более при изменении его отдельных параметров, обязательно следует создать копию реестра. Для создания копии реестра следует выполнить следующие действия:

- в левой панели в структуре реестра выбираем раздел «Компьютер»;
- щелкаем правой кнопкой мышки по этому разделу и в появившемся контекстном меню выбираем строку «экспорт»;
- задаем имя для копии файла реестра, а также указываем диапазон экспорта (должно быть выбрано «весь реестр»);
- указываем имя папки, в которой будет находиться копия файла реестра), и выполняем команду «Enter»;

После указанных действий появляется файл с заданным нами именем и расширением (.reg). Теперь, чтобы после проведения исследований вернуть реестр в исходное состояние, следует выбрать этот файл с расширением (.reg) и выполнить для него команду «импорт» , не забудьте нажать «Открыть»..

3.3.2 В левой панели редактора реестра находятся названия пяти основных разделов реестра. Используя команды меню редактора ре ра, исследуйте структуру и состав каждого из этих разделов. Выберите наиболее важные параметры реестра, изменение значений которых, с вашей точки зрения, может существенно влиять на производительность и информационную безопасность системы.

3.3.3 Изучите и исследуйте права доступа: no access (нет доступа), full control (полный доступ), read (только чтение), которые администратор может давать пользователям к разделам реестра.

3.3.4 Нарисуйте структурную схему разделов и наиболее важных подразделов реестра.

3.4 Анализ процессов задания параметров реестра с помощью редактора реестра.

3.4.1 Войдите в раздел реестра «HKEY_USERS» и отобразите все профили текущего пользователя, которые содержит этот раздел.

3.4.2 Получите у преподавателя значение рабочего параметра протокола TCP/IP (размер окна кадров, передаваемых по сети без подтверждения) и задайте его в реестре с помощью команды:

HKEY_LOCAL_MACHINE/ System/Current Control Set/Services/TCPIP/ Parameters.

3.4.3 Получите у преподавателя численное значение времени завершения работы Windows. По умолчанию оно равно 20 с., но многие приложения требуют гораздо меньше времени. Для уменьшения времени, отводимого на закрытие программы в ОС Windows, выполните следующие действия:

- в основном окне редактора реестра выберите раздел HkEY_LOCAL_MACHINE
- внутри этого раздела последовательно выберите подразделы SYSTEM и CurrentControl Set
- выделите подраздел CurrentControl Set и щелкните по нему. Справа появятся все параметры, входящие в состав этого подразделаэ
- выберите параметр WaitToKillServiceTimeout и выполните двойной щелчок по этому параметру;
- откроется окно, в котором будет указано текущее значение этого параметра;
- установите значение этого параметра согласно указания преподавателя и проверьте корректность внесенных изменений в реестр после перезапуска компьютера.

(Следует строго соблюдать размерность и правила задания параметра, так, например, для времени 4 с значение этого параметра равно 4000)

3.5 Исследование влияния параметров реестра на временные характеристики функционирования компьютеров рабочей группы.

3.5.1 Получите у преподавателя размеры окна кадров протокола TCP/IP и размеры набора передаваемых данных между компьютерами рабочей группы..

3.5.2. Для каждого размера окна кадров и набора данных определите время и скорость передачи этого набора данных между двумя компьютерами сети

3.5.3 Оцените влияние на время передачи набора данных характеристик этого набора данных и размера окна кадров. Дайте рекомендации по организации передачи набора данных между компьютерами сети по рассматриваемой среде передачи данных.

3.6 Исследование возможного наличия записей вредоносных программ в системном реестре (на примере «троянских программ»).

3.6.1 «Троянский конь» - это вредоносная программ, полученная путем явного изменения или добавления команд в пользовательскую программу. Проведите анализ содержимого следующего параметра реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Windows\CurrentVersion\ Winlogon

По умолчанию этот параметр имеет значение:

C^\Windows\system32\userinit.exe

Если в значении параметра содержатся дополнительные записи, то это могут быть «троянские программы».

3.6.2 При наличии «троянских программ». Проведите анализ места их расположения, особое внимание обратите на время создания файла.

4. Содержание отчета

Отчет о работе должен включать:

1.Набор функциональных задач, решаемых администратором системы с помощь реестра.

2. Состав и структуру системного реестра сетевых ОС Windows.

3. Структуру редактора реестра, правила и принципы работы с редактором реестра.

4. Перечень параметров системного реестра, влияющих на временные характеристики функционирования компьютера в сети.

5. Рекомендации по настройке параметров реестра для увеличения производительности и информационной безопасности системы.

6. Экранные формы, иллюстрирующие работу администратора с редактором реестра ОС Windows.

7. Результаты проведенных исследований, оформленные в виде графиков и таблиц

5. Контрольные вопросы

5.1 Вопросы категории «**Помнить»:**

1.Сформулируйте назначение и основные правила работы с редактором реестра сетевых ОС Windows.

2. Перечислите основные разделы реестра ОС Windows и их назначение.

3. Перечислите основные параметры реестра ОС Windows, влияющие на производительность компьютера при работе в сети.

5.2 Вопросы категории «**Понимать»**:

1. Поясните порядок действий по изменению параметров реестра ОС Windows с помощью редактора реестра

2. Поясните принципы задания численных значений параметрам реестра ОС Windows.

5.3 Вопросы категории «**Применять»**:

1. Как изменить содержимое реестра ОС Windows.

2. Как изменить значение параметра реестра ОС Windows

6. Практические навыки и компетенции, получаемые студентом после выполнения лабораторной работы

6.1. Студент должен **помнить:**

- перечень задач, решаемых администратором системы с помощью реестра ОС Windows;
- назначение реестра сетевых ОС семейства Windows;
- состав и структуру реестра сетевых ОС семейства Windows;

- принципы и правила задания параметров реестра сетевых ОС семейства Windows, используя редактор реестра.

6.2. Студент должен **понимать**:
- принципы и правила задания параметров реестра сетевых ОС семейства Windows с помощью редактора реестра;
- принципы работы реестра сетевых ОС семейства Windows.

6.3. Студент должен научиться **применять**
- редактор реестра для настройки параметров реестра сетевых ОС семейства Windows.

7. Правила безопасности при выполнении работы

Запрещается без разрешения преподавателя:
- подключать компьютеры и сетевое оборудование к розеточной сети;
- открывать системные блоки серверов и стационарных компьютеров;
- подключать к розеточной сети дополнительное оборудование, не входящее в комплект средств, используемых в работе;
- подключать к портам коммутаторов оборудование, не входящее в комплект средств, используемых в работе;
- развинчивать коммутаторы, мониторы и мыши.

8. Рекомендуемые источники информации.

1.Постников В.М. Основы эксплуатации автоматизированных систем обработки информации и управления. Краткий курс: учеб. пособие. М.: Изд- во МГТУ им. Н.Э. Баумана, 2013. 180 с.
2. Постников В.М. , Черненький В.М. Методы принятия решений в системах организационного управления: учеб. пособие./ В.М. Постников, В.М. Черненький. М.: Изд-во МГТУ им. Н.Э. Баумана, 2014. 205 с.
3. .Постников В.М. Основы эксплуатации АСОИиУ. Часть 1. Техническое обслуживание: учеб. пособие. М.: Изд- во МГТУ им. Н.Э. Баумана, 2015. 192 с.
4. Постников В.М. Основы эксплуатации АСОИиУ. Часть 2. Администрирование и развитие: учеб. пособие. М.: Изд- во МГТУ им. Н.Э. Баумана, 2015. 190 с.
5. Щепка П., Microsoft Windows Server 2003 Практическое руководство по настройке сети: пер. с англ. СПб.: НИТ 2006.