Министерство образования XXX

Государственное бюджетное профессиональное образовательное учреждение

XXX «Колледж «XXX»

09.02.07

ОТЧЕТ

По лабораторным работам

МДК 04.02 Обеспечение качества функционирования компьютерных систем

ККОО.ПМ.XXX.000

Студент XXX

Преподаватель XXX

Дата защиты_____ Оценка_____

2022

Лабораторная работа №7.

«Настройка политики безопасности»

Цель работы: «получение навыков работы с редактором групповой политики, изучение конфигурации групп пользователей и компьютеров»

Материально-техническое обеспечение: Компьютер, операционная система Windows 7

Краткие теоретические сведения:

Групповая политика – это набор правил, в соответствии с которыми производится настройка рабочей среды Windows. Групповые политики создаются в домене и реплицируются в рамках домена. Объект групповой политики (Group Policy Object, GPO) состоит из двух физически раздельных составляющих: контейнера групповой политики (Group Policy Container, GPC) и шаблона групповой политики (Group Policy Template, GPT). Эти два компонента содержат в себе всю информацию о параметрах рабочей среды, которая включается в состав объекта групповой политики. Продуманное применение объектов GPO к объектам каталога Active Directory позволяет создавать эффективную и легко управляемую компьютерную рабочую среду на базе ОС Windows.

Групповая политика в Windows XP предназначена для определения конфигурации групп пользователей и компьютеров. Конфигурация для группы пользователей и компьютеров создаётся с помощью оснастки «Групповая политика» консоли управления (MMC). Параметры групповой политики хранятся в объекте групповой политики, который в свою очередь связан с выбранными контейнерами Active Directory, например сайтами, доменами или подразделениями. Оснастка «Групповая политика» позволяет определить параметры политики для следующих элементов:

1 Политики из системного реестра;

К ним относятся групповые политики для операционной системы Windows 7 и её компонентов, а также для приложений. Для управления

этими параметрами используется узел «Административные шаблоны» оснастки «Групповая политика».

2 Параметры безопасности;

В эту категорию входят параметры безопасности для локального компьютера, домена и сети.

3 Параметры установки и обслуживания программ;

Служат для централизованного управления установкой, обновлением и удалением программ.

4 Параметры сценариев;

Сценарии для запуска компьютера и завершения его работы, входа пользователей в систему и окончания сеансов.

5 Параметры перенаправления папок;

Позволяют администратору перенаправлять специальные папки пользователей в сеть.

Благодаря групповой политике можно один раз определить конфигурацию рабочей среды пользователя, после чего операционная система будет применять заданные политики.

Порядок выполнения лабораторной работы:

1. Изучить теоретический материал.
2. Выполнить предлагаемые задания.
3. Ответить на контрольные вопросы и предоставить в тетради в виде отчета. Отчет должен включать:

- номер, наименование лабораторной работы и тему;
- ответы на контрольные вопросы;
- выводы.

4. Выполненную работу и отчет по проделанной работе предъявить преподавателю.

Задания для выполнения лабораторной работы:

Задание 1

Чтобы запустить редактор групповой политики, выполните следующие действия:

Примечание. Чтобы использовать редактор групповой политики, необходимо войти в систему с учётной записью, обладающей привилегиями администратора.

1. Откройте «Консоль управления MMC». Для этого нажмите на кнопку «Пуск», в поле поиска введите mmc , а затем нажмите на кнопку Enter.

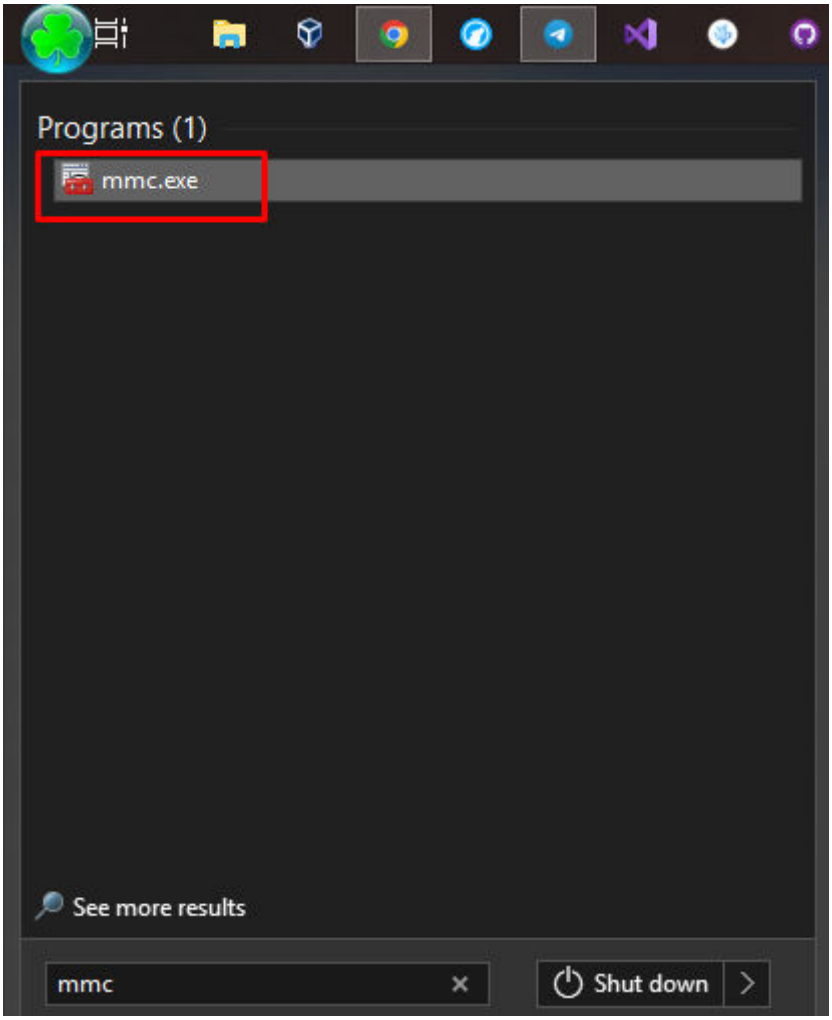

Рисунок 1 Поиск «mmc.exe»

2. Откроется пустая консоль MMC. В меню «Консоль» выберите команду «Добавить или удалить оснастку» или воспользуйтесь комбинацией клавиш Ctrl+M.

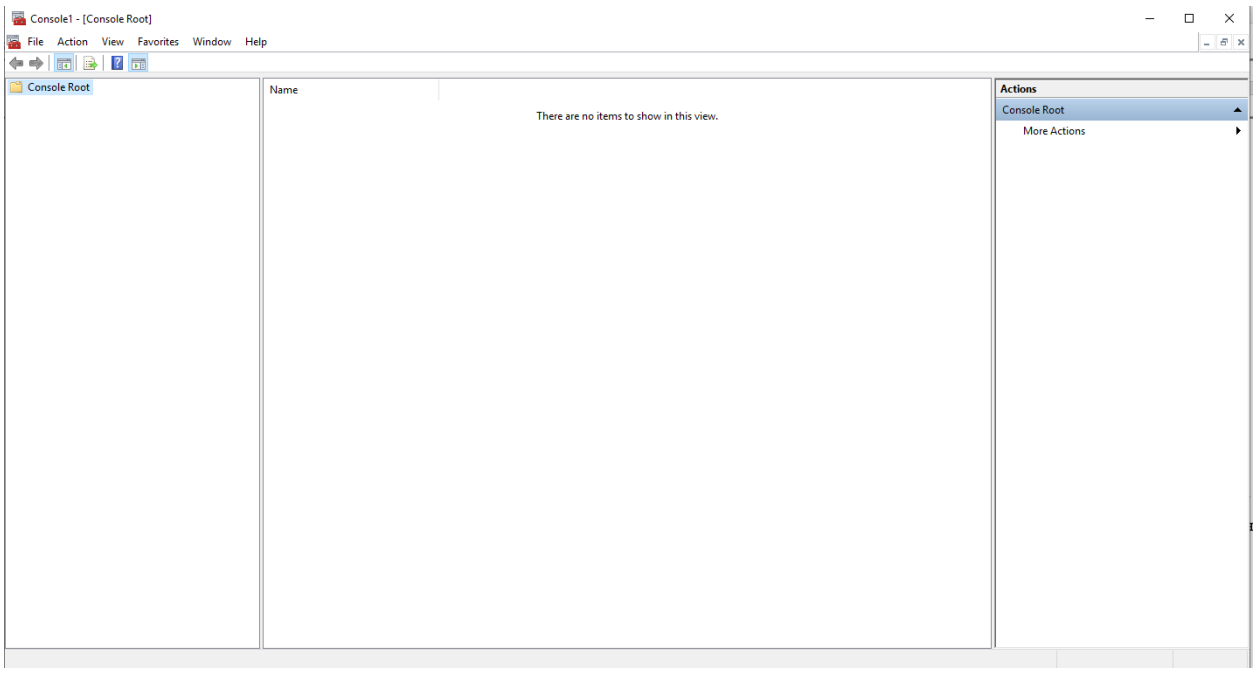

Рисунок 2 Открытая консоль

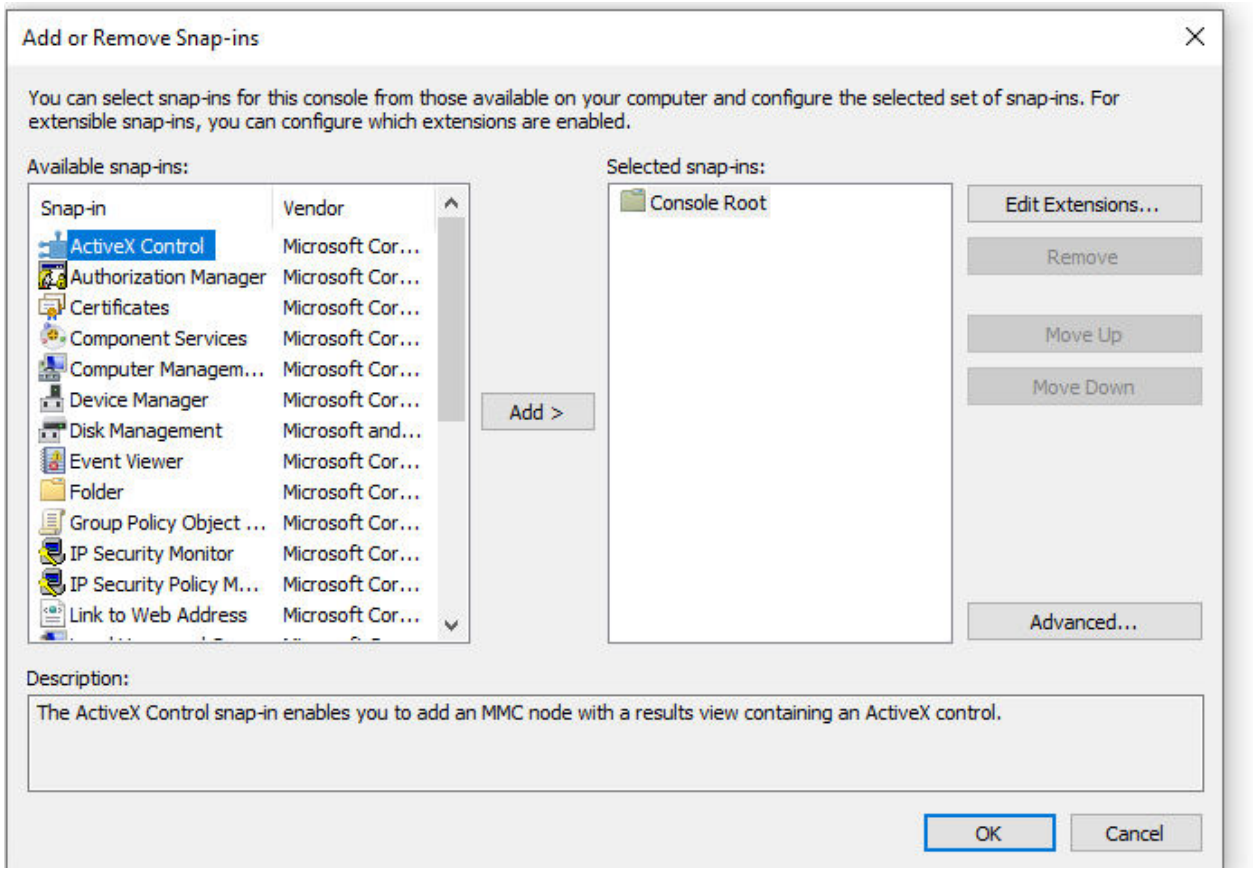

Рисунок 3 Добавление оснастки

3. В диалоге «Добавление и удаление оснасток» выберите оснастку «Редактор объектов групповой политики» и нажмите на кнопку «Добавить».

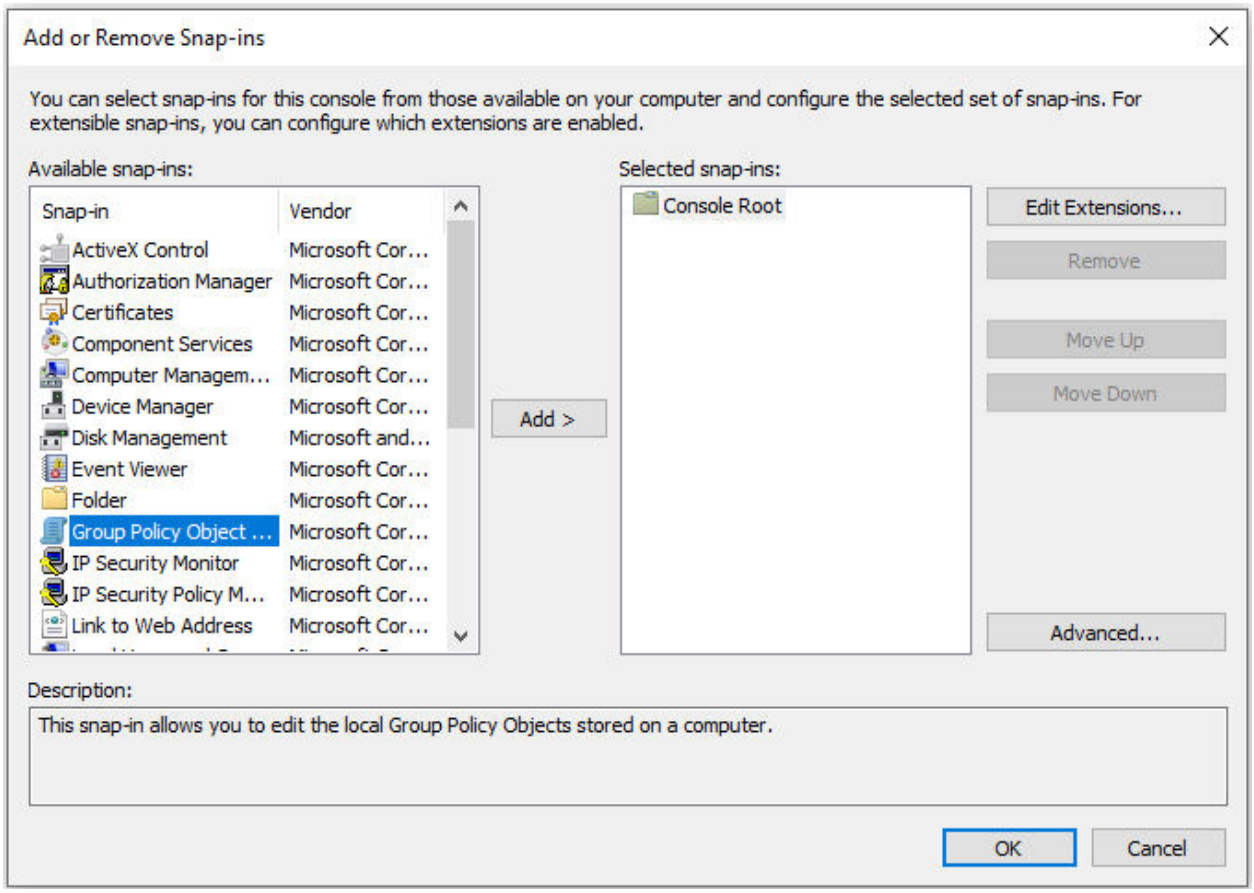

Рисунок 4 Добавление оснастки «Редактор объектов групповой политики»»

4. Для того чтобы выбрать нужный объект групповой политики, в появившемся диалоге «Выбор объекта групповой политики» нажмите на кнопку «Обзор».

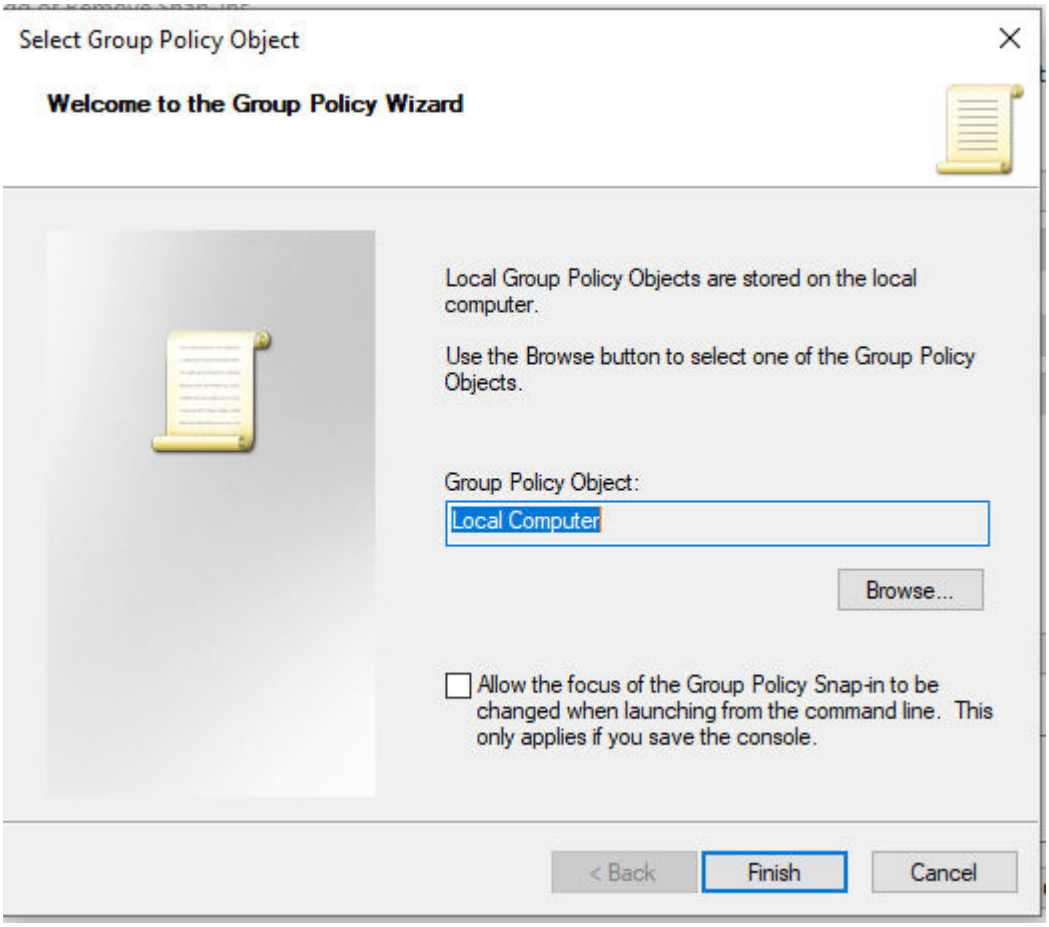

Рисунок 5 Обзор

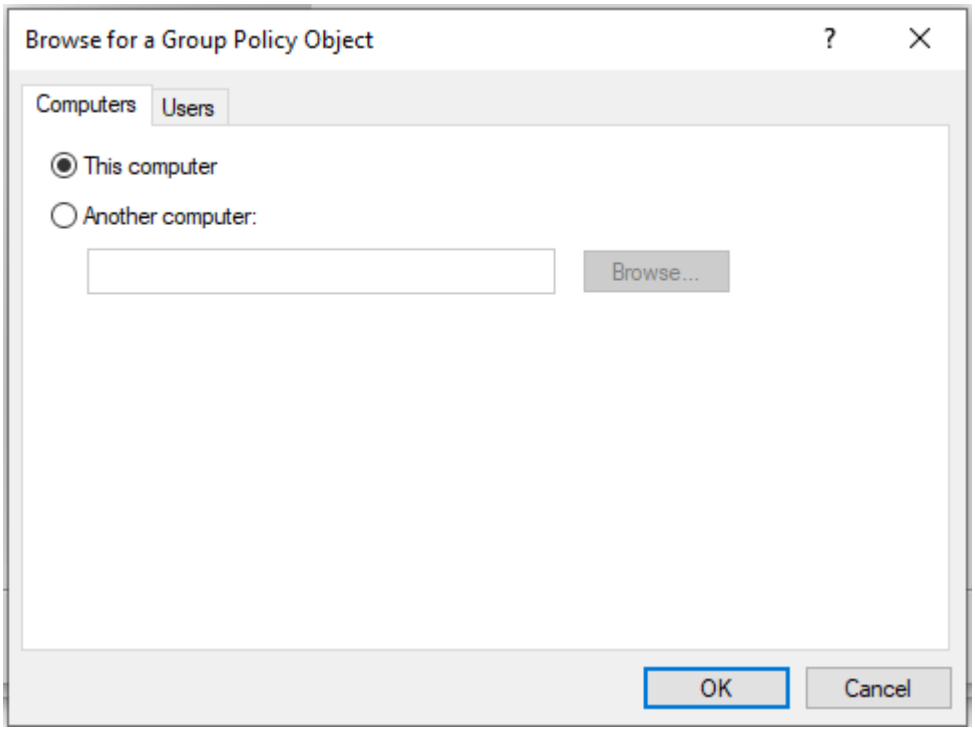

Рисунок 6 Обзор

5. В диалоге «Поиска объекта групповой политики» можно перейти на вкладку «Пользователи» и выбрать объект, над которым будут проводиться настройки групповой политики, например «Не администраторы».

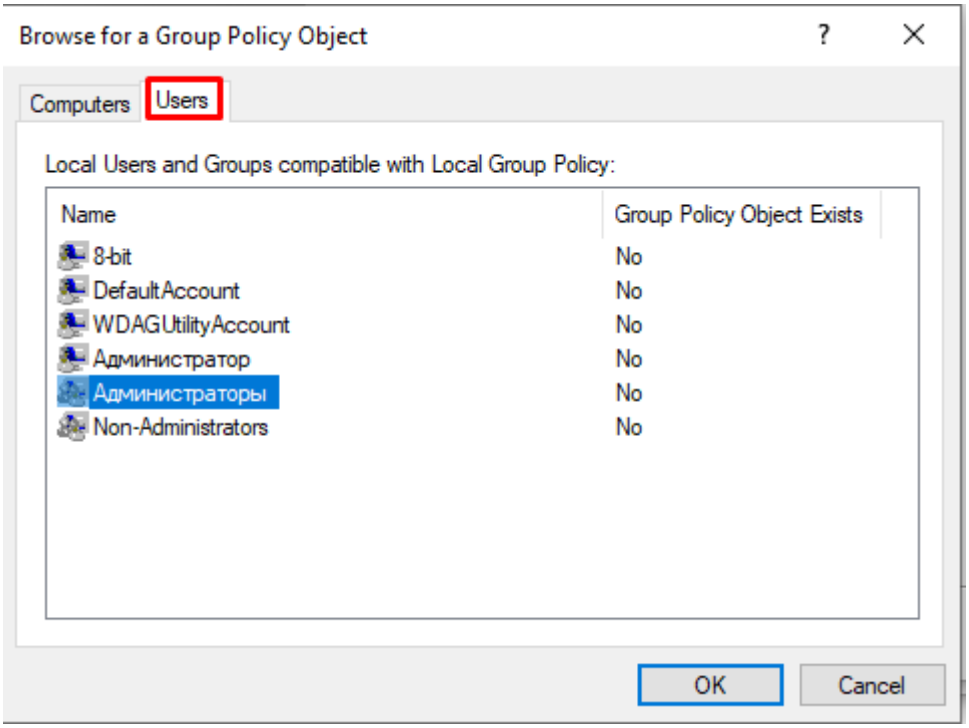

Рисунок 7 Вкладка пользователи

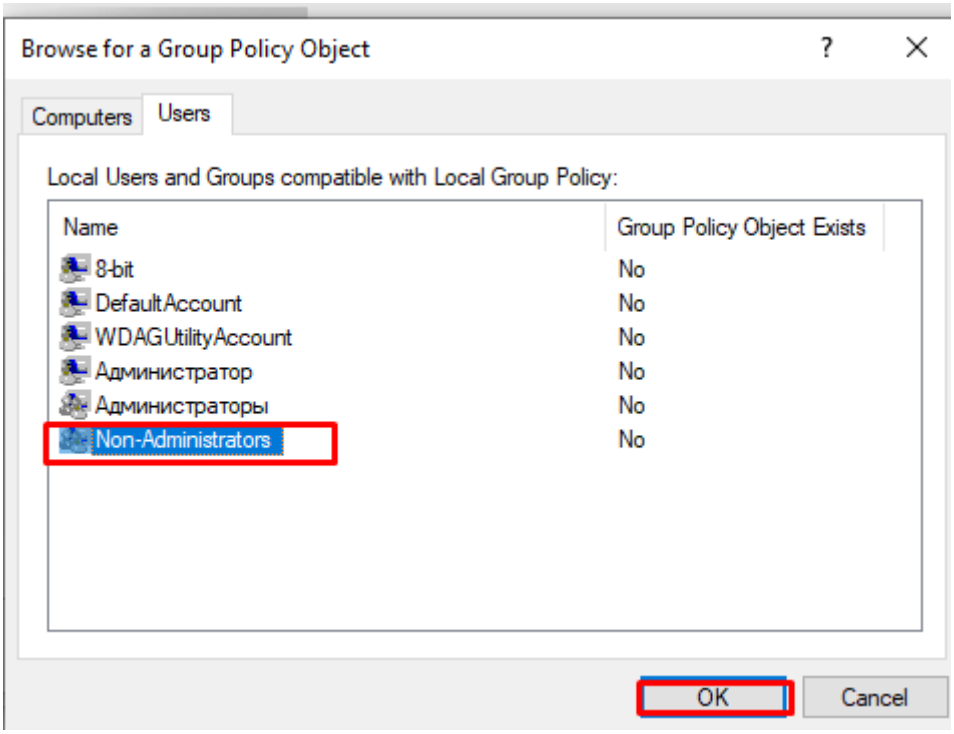

Рисунок 8 Выбор объекта, над которым будут проводиться настройки «Групповой политики»»

6. Нажмите на кнопку «ОК» в диалоге «Поиск объекта групповой политики», в диалоге «Выбор объекта групповой политики» нажмите на кнопку «Готово», а после этого нажмите на кнопку «ОК» диалога «Добавление и удаление оснасток».

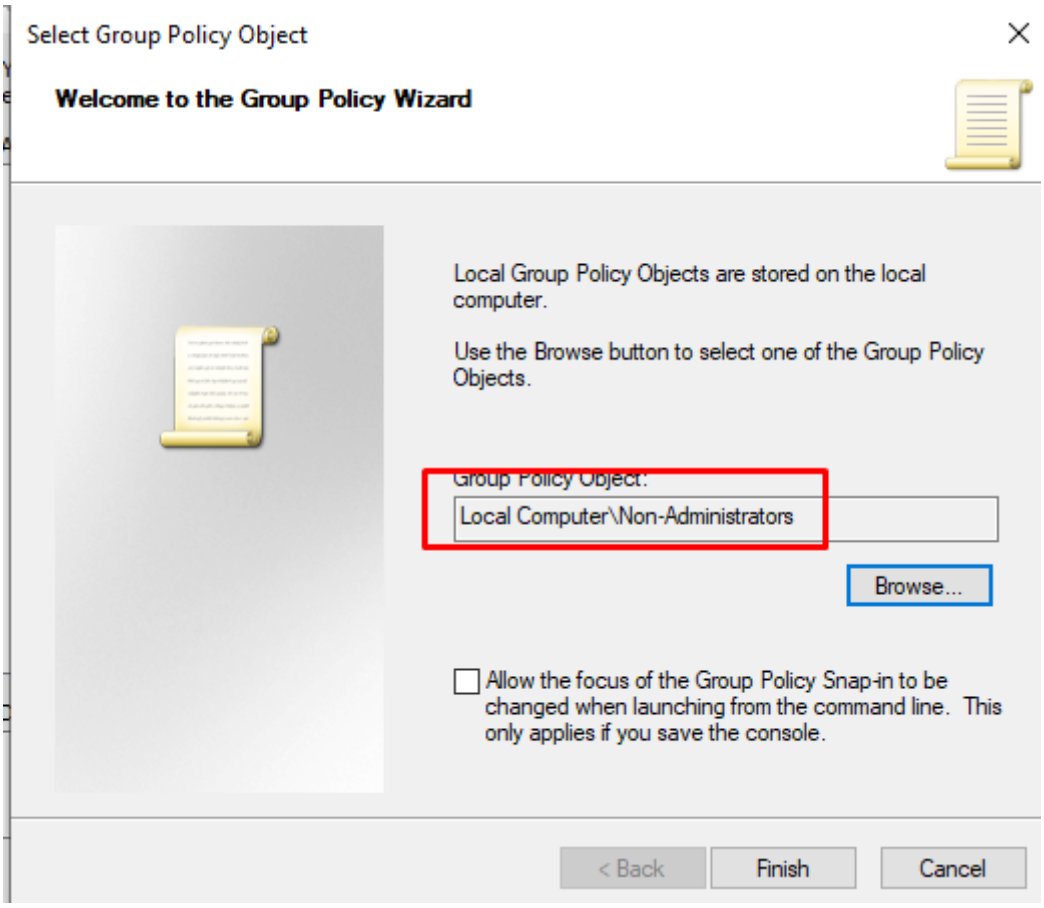

Рисунок 9 Выбор объекта групповой политики

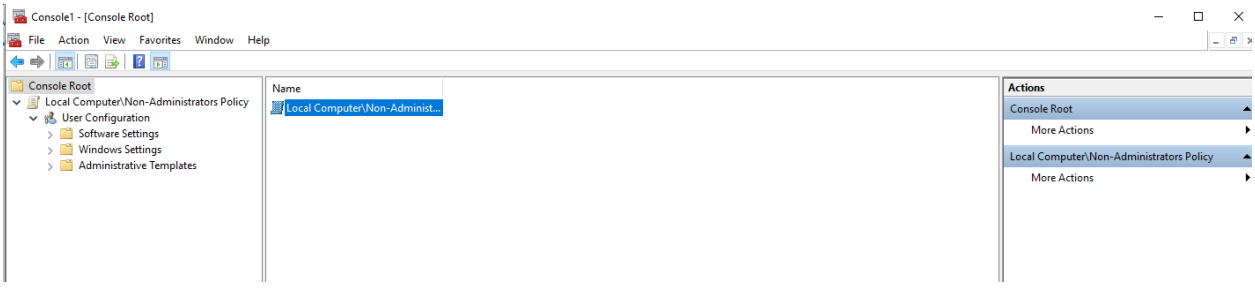

Рисунок 10 Добавление и удаление оснасток

Задание №2

Чтобы использовать редактор групповой политики, выполните следующие действия:

1. Разверните нужный объект групповой политики, например «Политика «Локальный компьютер»;

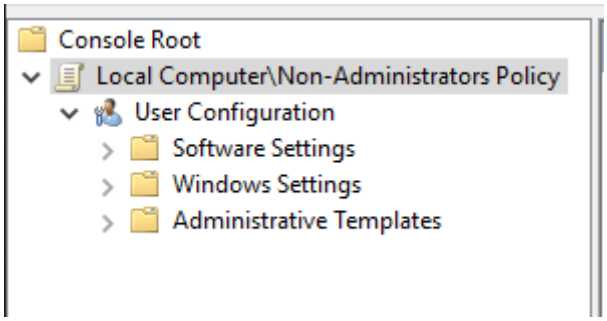

Рисунок 11 Политика «Локальный компьютер»

2. Разверните нужный узел, например, «Конфигурация компьютера»;

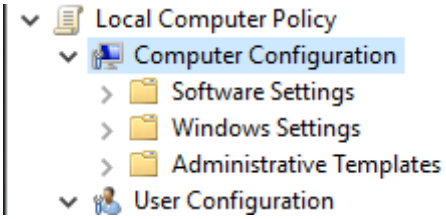

Рисунок 12 Конфигурация компьютера

3. Разверните нужный вложенный элемент, например, «Конфигурация Windows»;

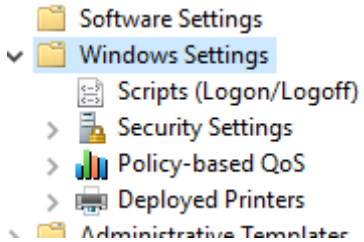

Рисунок 13 Конфигурация Windows

4. Откройте папку, которая содержит нужный параметр политики. «Элементы политики» отображаются на правой панели оснастки в редакторе групповой политики;

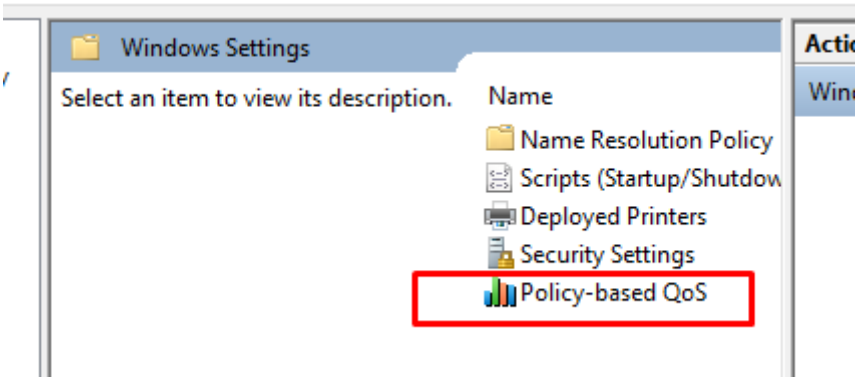

Рисунок 14 Конфигурация Windows

5. В списке «Параметр» два раза щёлкните нужный элемент политики;

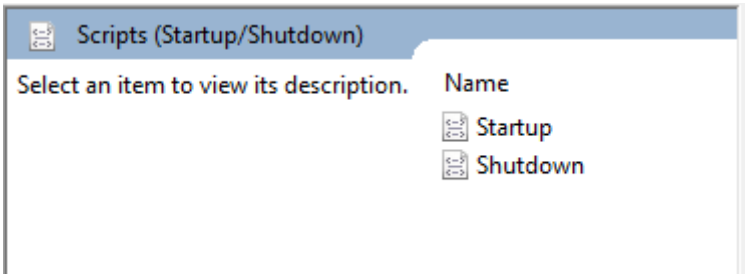

Рисунок 15 Список параметров

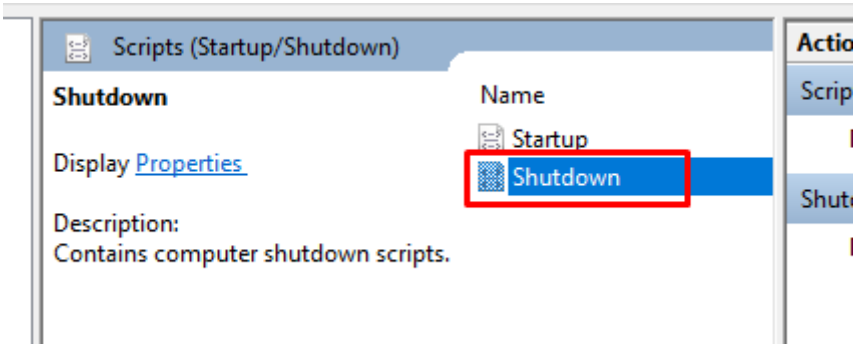

Рисунок 16 Параметр «Завершение работы»

6. Настройте параметры политики в открывшемся диалоговом окне и нажмите кнопку «Ок»;

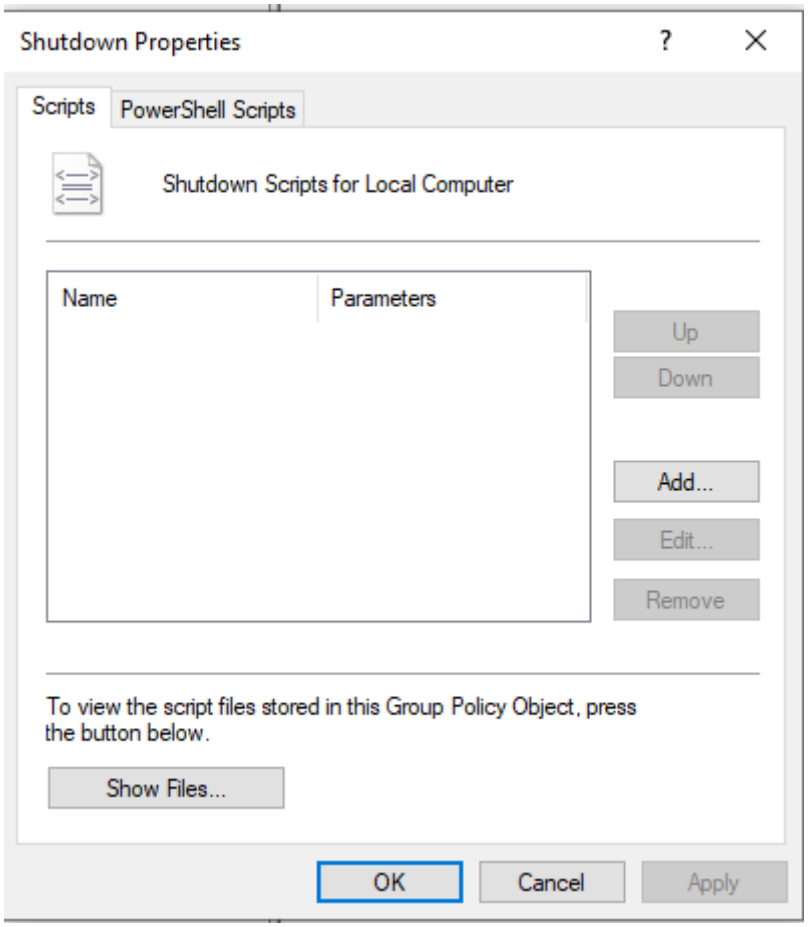

Рисунок 16 Свойства параметра завершения работы

7. Выполнив необходимые действия, закройте консоль управления;

Конфигурация компьютера

Этот узел служит для настройки политик, применяемых к компьютеру независимо от того, кто входит в систему. Узел «Конфигурация компьютера», как правило, содержит вложенные элементы для параметров программ, параметров Windows и административных шаблонов.

Конфигурация Windows

Узел, расположенный в дереве \Конфигурация компьютера \ Конфигурация Windows, содержит параметры, применяющиеся ко всем пользователям, входящим в систему на данном компьютере. Он включает две подпапки: «Параметры безопасности» и «Сценарии».

Сценарии запуск/завершение

Администраторы используют это расширение для указания сценариев, которые выполняются при запуске или завершении работы системы. Сценарии выполняются в контексте локального компьютера.

- Автозагрузка – содержит сценарии загрузки компьютера;
- Завершение работы – содержит сценарии завершения работы компьютера.

Параметры безопасности

С помощью параметров безопасности можно изменить политику безопасности для подразделения, домена или узла с любого компьютера, присоединённого к домену. Администратор безопасности с помощью компонента «Параметры безопасности» может изменить параметры безопасности, назначенные объекту групповой политики.

Политика учётных записей

Представляет собой набор параметров для настройки политики паролей и блокировки учётных записей.

Параметры безопасности были рассмотрены в предыдущей лабораторной работе.

Задание №3

1. Откройте оснастку «Групповая политика».

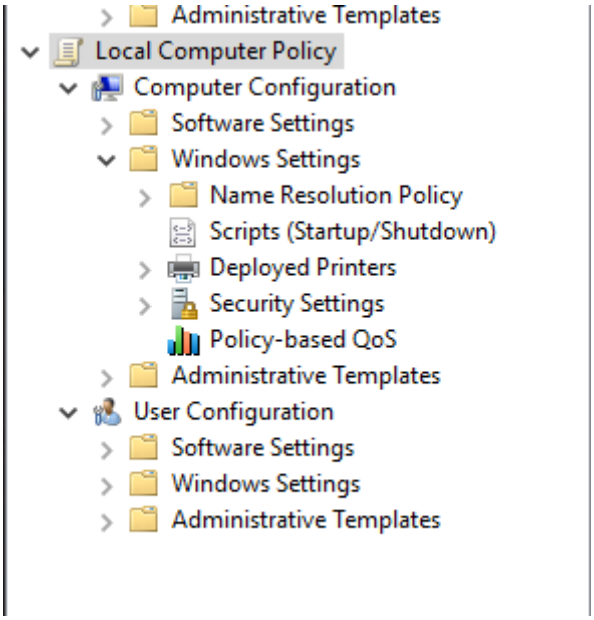

Рисунок 17 Оснастка «Групповая политика»

2. В дереве консоли щёлкнуть «Сценарии (запуск/завершение)».

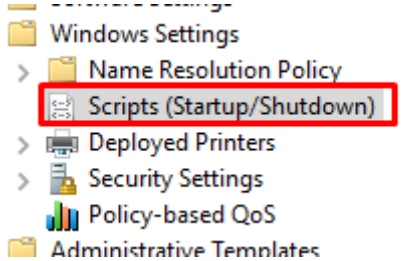

Рисунок 18 Сценарии

3. Дважды щёлкнуть «Автозагрузка».

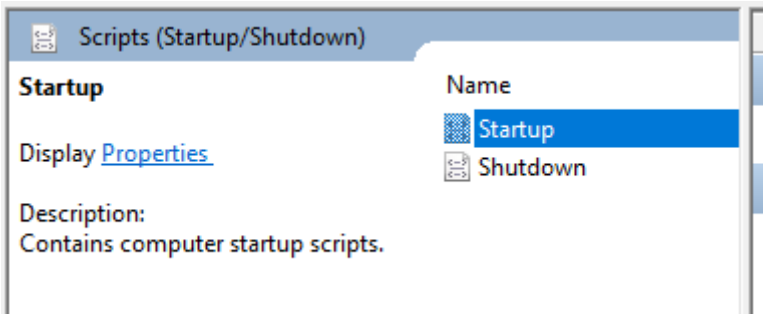

Рисунок 19. Параметр «Автозагрузка»

4. В диалоговом окне «Свойства: Автозагрузка» нажать кнопку «Добавить».

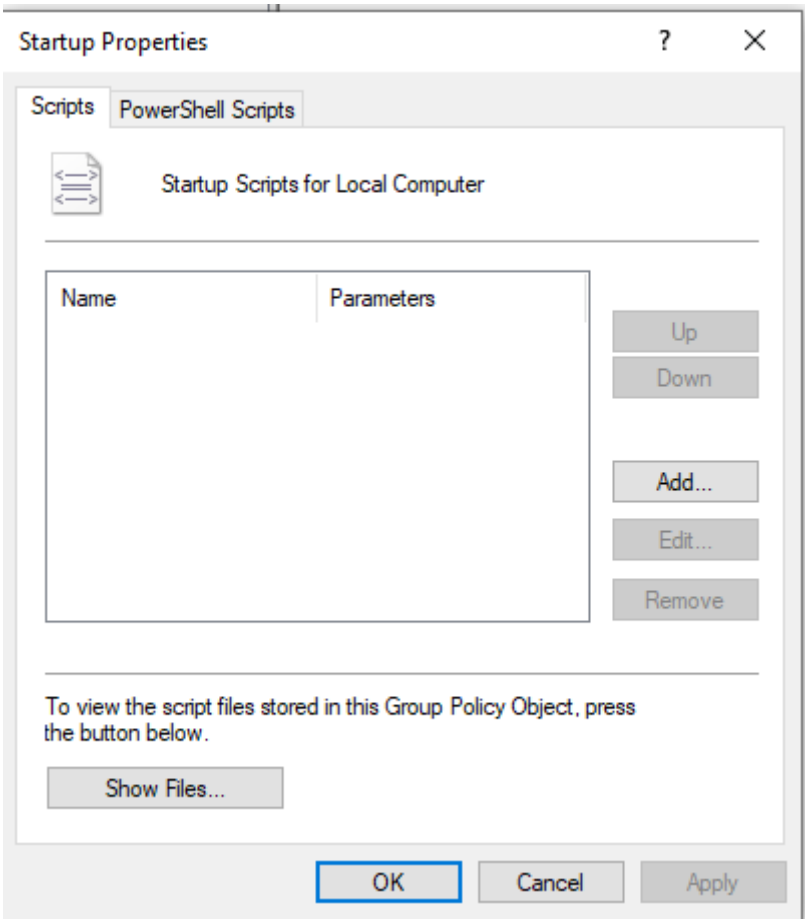

Рисунок 20 Свойства «Автозагрузки»

5. В диалоговом окне «Добавление сценария» ввести «Имя сценария» и «Параметры», нажать кнопку «ОК».

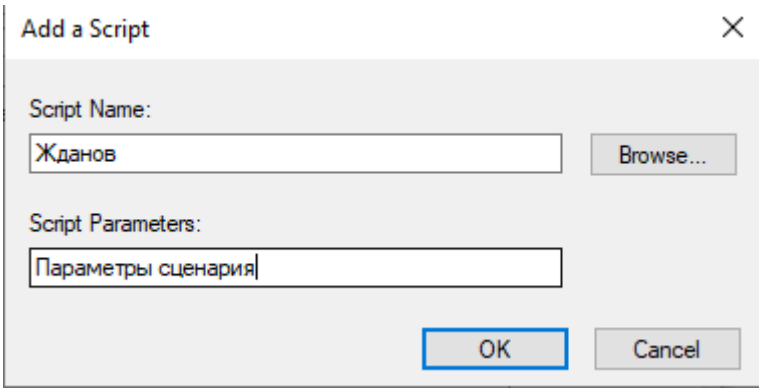

Рисунок 21 Добавление сценария

Административные шаблоны

Узел «Административные шаблоны» содержит всю информацию о политиках системного реестра.

Компоненты Windows – содержат параметры для компонентов операционной системы.

а) Пересылка событий;

- диспетчер подписки – позволяет настроить адрес сервера, интервал обновления и центр сертификации, выдающий сертификаты для диспетчера подписки. Диспетчер подписки – это компьютер, которому пересылаются события;

- ForwarderResourceUsage – управляет использованием ресурсов сервера пересылки. Каждый параметр применяется ко всем подпискам сервера пересылки.

б) Каналы RSS;

- отключить синхронизацию каналов в фоновом режиме – определяет, включена ли синхронизация каналов в фоновом режиме. Если параметр включён, то возможность синхронизации каналов в фоновом режиме отключена. При отключённом или ненастроенном параметре пользователям будет позволено синхронизировать их каналы в фоновом режиме;

- отключить добавление и удаление каналов – запрещает пользователям подписываться на канал и удалять каналы, на которые они уже подписаны;

- отключить загрузку вложений – запрещает загрузку вложений (вложенных файлов) из канала на компьютер;

- отключить обнаружение каналов – запрещает пользователям включать автоматическое обнаружение доступных на соответствующей веб-странице каналов обозревателем Internet Explorer;

- отключить список каналов – запрещает пользователям использовать Internet Explorer в качестве средства чтения каналов. Этот параметр не влияет на платформу RSS.

в) Internet Explorer – содержит параметры политики для IE:

- отключить отображение меню «Справка» в IE – позволяет отключить меню «Справка» в Internet Explorer;

- включение полноэкранного режима – панель навигации содержит средства просмотра веб-страниц, поиска в сети с помощью выбранных инструментов поиска, просмотра журнала, печати и доступа к почте и группам новостей. Строка меню содержит меню с раскрывающимися списками соответствующих функций. Среди них печать, настройка Internet Explorer, копирование и вставка текста, управление избранным и справка. С помощью панели команд осуществляется управление и доступ к избранному, веб-каналам, закладкам и т. д. Полноэкранный режим отключает эти три панели, и обозреватель переходит в полноэкранный режим. Ярлыки этих панелей перестают работать;

- настроить строку обозревателя – позволяет задавать строку, которую Internet Explorer будет отправлять веб-серверам в заголовке запроса HTTP User Agent в качестве версии обозревателя;

- отключить проверку настроек безопасности – отключает функцию проверки безопасности параметров, которая определяет, когда параметры ставят безопасность Internet Explorer под угрозу;

- отключить управление фильтром фишинга – позволяет пользователям включить фильтр фишинга, предупреждающий о попытках незаконного сбора персональной информации с помощью фишинга при посещении веб-узла;

- задать параметры прокси для компьютера – применяет параметры прокси ко всем пользователям на данном компьютере;

- отключить изменение параметров подключений – запрещает пользователям изменять параметры удалённого доступа;

- отключить изменение параметров прокси – задаёт подключение к Интернету с указанными параметрами прокси-сервера. Прокси-сервер действует как посредник между внутренней сетью (интрасетью) и Интернетом, получая файлы с удалённых веб-серверов. Этот параметр указывает, хочет ли пользователь подключаться к адресам локальной

интрасети с помощью прокси-сервера или в обход него для адресов интрасети;

- отключить настройку журнала – задаёт, сколько дней Internet Explorer отслеживает просмотренные страницы в списке журнала. Получить доступ к параметру «Удалить журнал обозревателя» можно, выбрав «Служебные программы», «Параметры обозревателя» и вкладку «Общие». В Internet Explorer 7 он доступен также как параметр «Удалить историю» прямо в «Служебных программах», «Удалить историю просмотра»;

- запретить удаление временных файлов Интернета и файлов cookies – используется для управления временными файлами Интернета и файлами cookie, связанными с историей просмотра Интернета и доступными при выборе в Internet Explorer 7 команд «Средства», «Параметры Интернета», «Удалить историю просмотра»;

- отключить возможность «Удаление паролей» – запрещает пользователям очищать пароли. Эта возможность доступна через параметр «Удалить пароли» в диалоговом окне «Удалить журнал обозревателя» в Internet Explorer 7, кроме того, можно щёлкнуть кнопку «Очистить пароли» в группе «Очистка журнала автозаполнения» диалогового окна «Настройка автозаполнения», вызываемого на вкладке «Содержание» в свойствах обозревателя.

г) Совместимость приложений:

- процессы IE – позволяет избегать запросов на разрешение, когда сценарии, запущенные внутри процесса Internet Explorer, пытаются выполнять операции с буфером обмена (например, вырезание, копирование, вставку), а также действия для URL в зоне, настроенной на отображение запроса;

- список процессов – позволяет администраторам задавать приложения, для которых это средство запрещено или разрешено;

- все процессы – позволяет запретить или разрешить эту функцию для всех процессов, запущенных на компьютере. Если включить этот параметр политики, сценарий любого процесса компьютера сможет выполнять операции с буфером обмена без запроса на разрешение. Т.е. если поведение зоны настроено на запрос разрешения, эта настройка не будет учитываться, а операция будет разрешена. Если отключить этот параметр политики, сценарий любого процесса компьютера не сможет выполнять операции вырезания, копирования или вставки из буфера обмена без запроса на разрешение.

д) Панель управления браузером:

Содержит параметры для добавления или удаления вкладок диалогового окна свойств обозревателя:

- отключить страницу «Общие» – удаляет вкладку «Общие» из диалогового окна свойств обозревателя;
- отключить страницу «Безопасность» – удаляет вкладку «Безопасность» из диалогового окна свойств обозревателя;
- отключить страницу «Содержание», «Подключение», «Программы», «Конфиденциальность», «Дополнительно» – удаляет одноимённые вкладки из диалогового окна свойств обозревателя;
- отправлять международные доменные имена – разрешает Internet Explorer преобразовывать имена доменов в формате Unicode в формат IDN (Punycode) перед посылкой на серверы службы доменных имён (DNS) или прокси-серверы;
- использовать кодировку UTF-8 для почтовых ссылок – позволяет задать, использует ли Internet Explorer кодировку UTF-8 для почтовых ссылок;
- запретить пропуск ошибок сертификата – Internet Explorer обрабатывает как критические любые ошибки сертификатов SSL/TLS (Secure

Socket Layer/Transport Layer Security), прерывающие переход (такие как «истёк срок действия», «сертификат отозван», «несоответствие имён»).

е) Панели инструментов:

- средство обновления панели инструментов проверяет установленные панели инструментов и вспомогательные объекты обозревателя на совместимость при запуске Internet Explorer. При обнаружении несовместимой панели инструментов пользователь получит запрос на её обновление или отключение. Отдельные панели инструментов и вспомогательные объекты обозревателя, включённые или отключённые политикой, не будут подвергнуты этой проверке.

Задание №4

1. Откройте оснастку «Групповая политика».

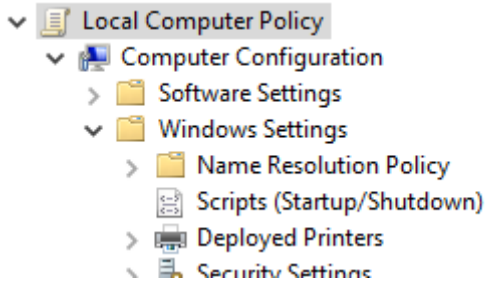

Рисунок 22 Оснастка «Групповая политика»

2. В узле «Конфигурация компьютера» выберите «Административные шаблоны».

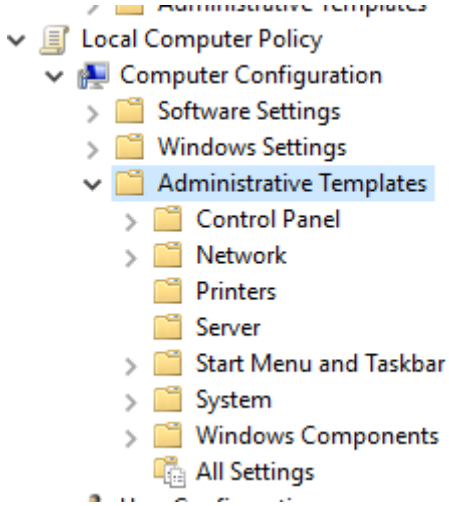

Рисунок 23 Административные шаблоны

3. Далее выберите «Компоненты Windows» – «Internet Explorer» – «Удалить журнал браузера» – «Запретить удаление временных файлов Интернета и файлов cookies».

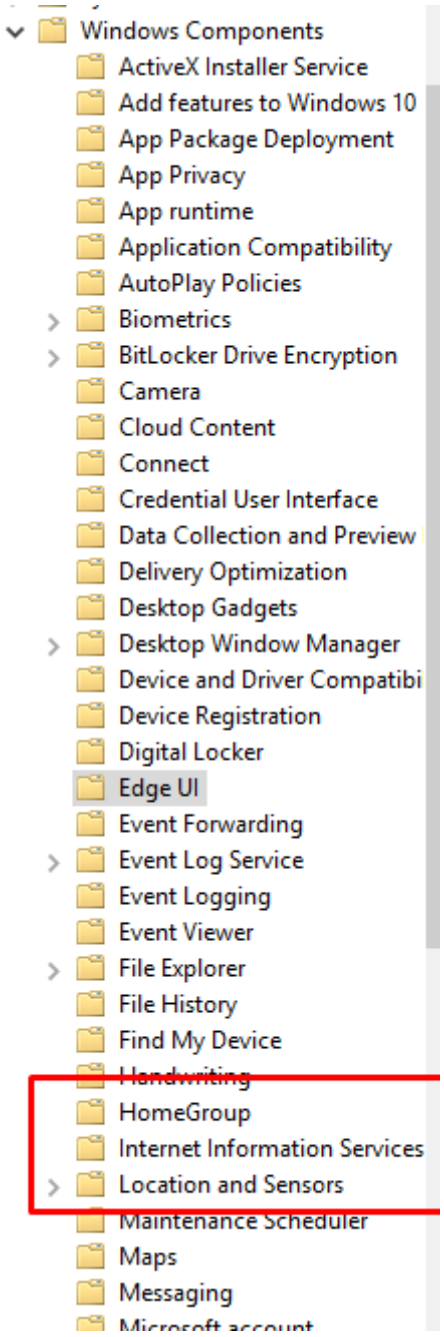

Рисунок 24 Отсутствие компонента

4. В завершении установите необходимые параметры

ж) Совместимость приложений:

- включить обработчик совместимости приложений – управляет состоянием обработчика совместимости приложений на компьютере. Обработчик, являющийся частью загрузчика, просматривает базу данных

совместимости при каждом запуске приложения на компьютере. Если обнаружено соответствие для приложения, оно обеспечивает либо исполняемые решения или исправления совместимости, либо отображается справочное сообщение приложения, если известна причина неполадок;

 включить мастер совместимости программ – управляет состоянием мастера совместимости программ. Когда эта политика включена, она отключает начальную страницу мастера в центре справки и поддержки и в меню «Пуск».

з) Просмотр событий:

 URL-адрес EVANTS.ASP – это URL-адрес, передаваемый в область описания события в диалоговом окне свойств события. Измените это значение, если хотите использовать другой веб-сервер для обработки запросов дополнительной информации о событиях;

 программа EVANTS.ASP – это программа, которая будет вызвана, если пользователь щёлкнет ссылку EVENTS.ASP;

 параметры командной строки программы EVANTS.ASP – задаёт параметры командной строки, передаваемые программе EVENTS.ASP.

и) Службы IIS:

 запрет установки IIS – когда этот параметр включён, запрещается установка служб IIS, а также установка компонентов Windows или приложений, которым требуется IIS. Пользователи, устанавливающие компоненты Windows или приложений, которым требуется IIS, могут не получить предупреждение о невозможности установки IIS из-за данной групповой политики. Включение данного параметра не влияет на IIS, если службы IIS уже установлены на компьютере.

к) Центр обеспечения безопасности:

 включить «Центр обеспечения безопасности» (только для компьютеров в домене) – указывает, включён ли «Центр обеспечения безопасности» на пользовательских компьютерах, которые присоединены к

домену Active Directory. Когда «Центр обеспечения безопасности» включён, он наблюдает за основными параметрами безопасности (брандмауэр, антивирус, автоматическое обновление), и уведомляет пользователей, если их компьютеры подвержены опасности. Категория «Центр обеспечения безопасности» в панели управления также содержит секцию состояния, где пользователи могут найти рекомендации по повышению безопасности своего компьютера. Если «Центр обеспечения безопасности» отключён, то ни уведомления, ни раздел состояния не отображаются.

л) Планировщик заданий (управляет возможностью пользователей управлять заданиями).

 скрывать страницы свойств – запрещает пользователям просматривать и изменять свойства существующего задания. Эта политика удаляет команду «Свойства» из меню «Файл» в окне «Назначенные задания» и из контекстного меню, которое появляется при выполнении правого щелчка на задании. В результате пользователи не могут изменять свойства заданий. Они могут просматривать только те свойства, которые отображаются в окне назначенных заданий при использовании команды «Таблица» в меню «Вид»;

 запретить запуск и завершение задач – запрещает пользователям запускать или останавливать задания вручную. Эта политика удаляет команды «Выполнить» и «Завершить задание» из контекстного меню, которое появляется при выполнении правого щелчка мышью на задании. В результате пользователи не могут запускать задания вручную или принудительно завершать задания до окончания их выполнения;

 запретить перетаскивание с помощью мыши – запрещает пользователям добавлять и удалять задания с помощью перемещения или копирования программ в папку «Назначенные задания». Эта политика отключает команды «Вырезать», «Копировать», «Вставить» и «Вставить ярлык» в контекстном меню и в меню «Правка» в папке «Назначенные

задания». Она также отключает возможности перетаскивания объектов с помощью мыши в эту папку;

 запретить создание новых заданий – удаляет элемент «Добавить задание» из папки назначенных заданий, которая запускает «Мастер планирования заданий». Кроме того, система не позволяет переместить или скопировать с помощью буфера обмена или мыши программы или документы в папку «Назначенные задания»;

 запретить удаление заданий – удаляет команду «Удалить задание» из меню «Правка» папки назначенных заданий и из контекстных меню, которые открываются правым щелчком мыши на задании. Кроме того, система не позволяет удалить задание из папки «Назначенные задания» с помощью вырезания существующего задания в буфер обмена или перетаскивания его мышью;

 скрыть флажок дополнительных свойств в мастере планирования заданий удаляет флажок «Установить дополнительные параметры» после нажатия кнопки «Готово» с последней страницы мастера планирования заданий. Она предназначена для того, чтобы упростить создание заданий для начинающих пользователей;

 запретить обзор – ограничивает выбор назначаемых для выполнения по расписанию программ теми, которые указаны в меню «Пуск» пользователя, и запрещает пользователю изменять расписание выполнения уже назначенных заданий. Эта политика удаляет кнопку «Обзор» из мастера назначения заданий и вкладки «Задание» диалогового окна свойств задания. Кроме того, пользователи не могут изменять значение поля «Выполнить» и «Рабочая папка», которые определяют программу и путь для выполняемого задания.

Задание №5

1 Откройте оснастку «Групповая политика».

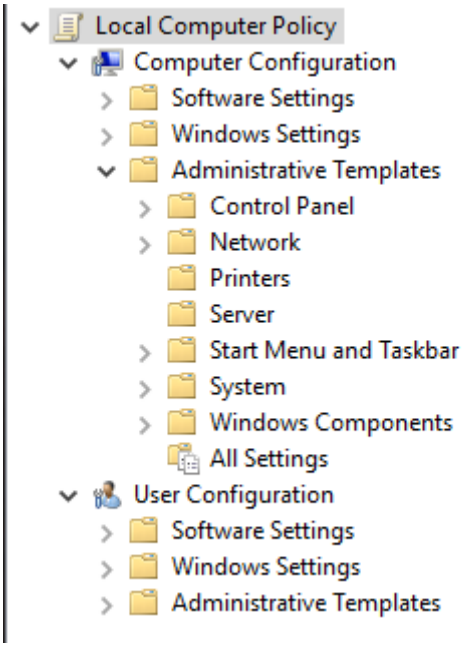

Рисунок 26 Оснастка «Групповая политика»

2 В узле «Конфигурация компьютера» выберите «Административные шаблоны».

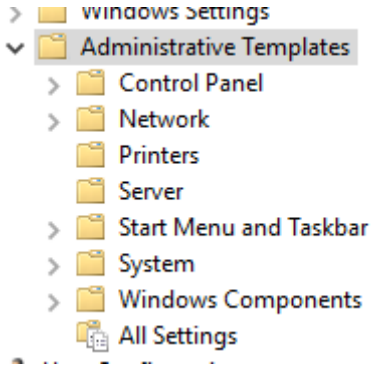

Рисунок 27 Административные шаблоны

3 Далее выберите «Компоненты Windows» – «Все параметры» – «Удалить элемент «Отключение сеанса» из диалога завершения работы.

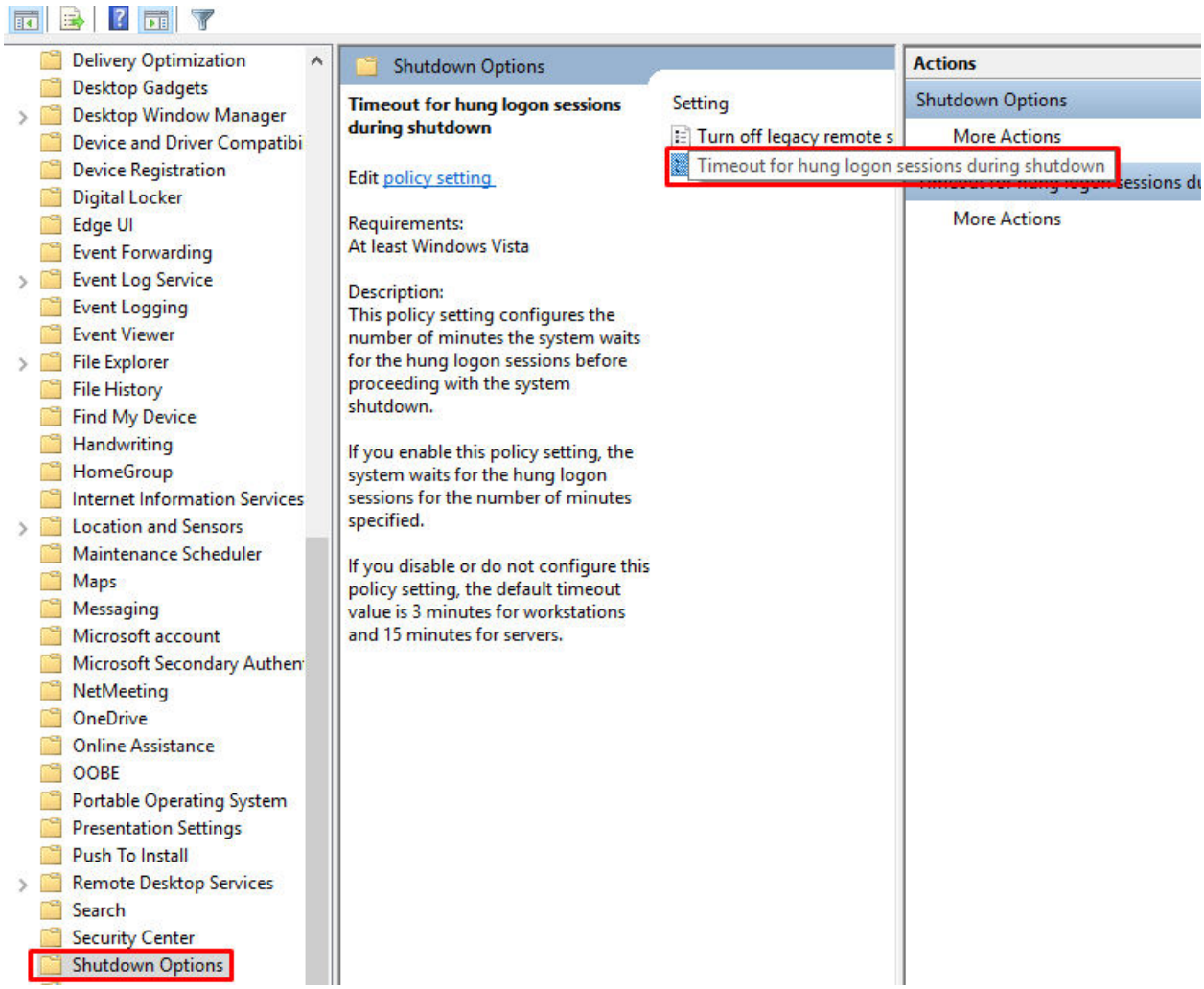

Рисунок 28 Таймаут для зависших сеансов

4 В завершении установите необходимые параметры.

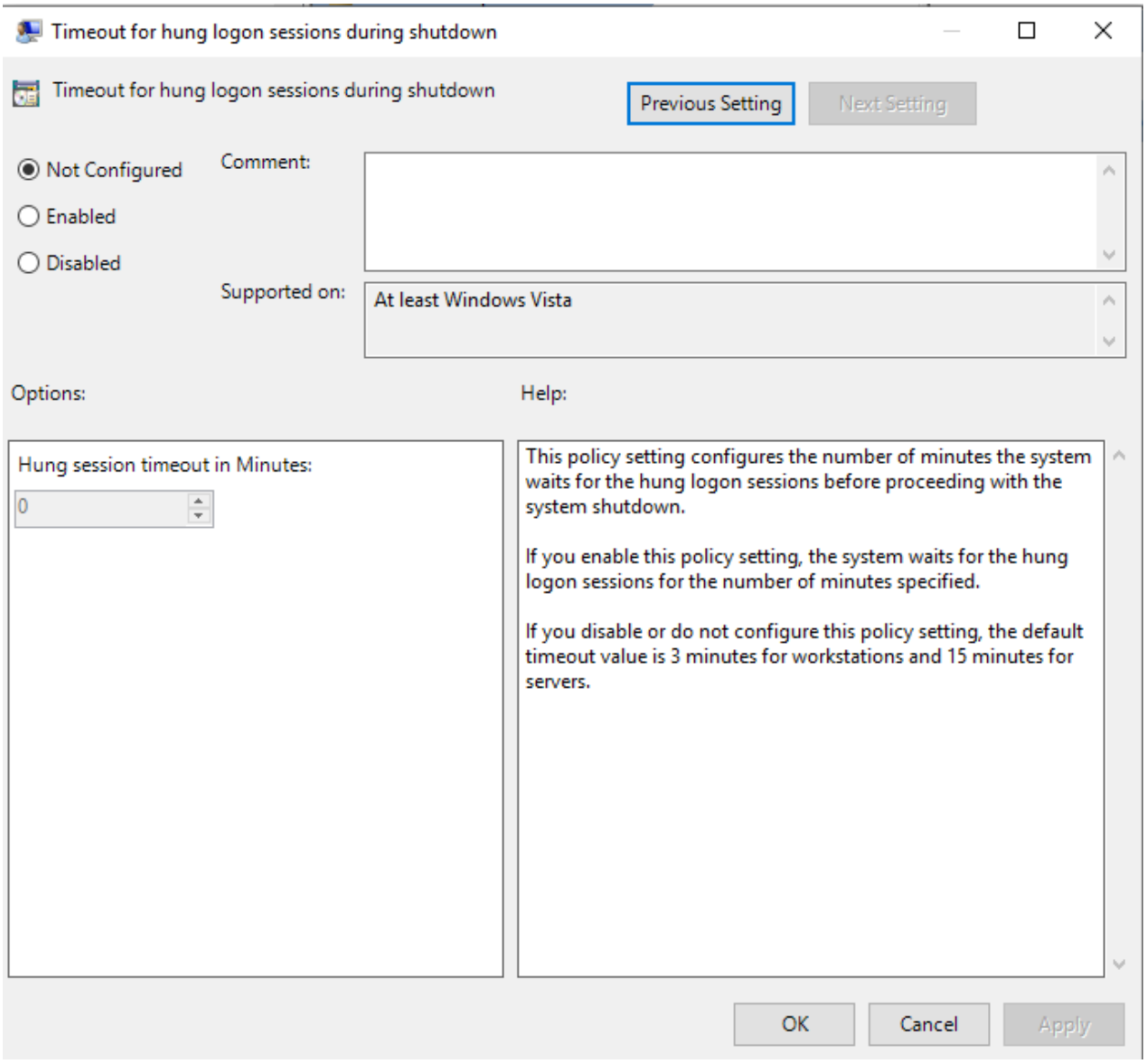

Рисунок 29 Установка необходимых параметров

м) Смарт-карта:

- разрешить перенаправление часового пояса – разрешено ли клиентским компьютерам перенаправлять их параметры часового пояса в сеанс службы терминалов;
- не разрешать перенаправление буфера обмена – указывает, следует ли отключать совместное использование содержимого буфера обмена (перенаправление буфера обмена) удалёнными компьютерами и клиентскими компьютерами для сеанса служб терминалов;
- не разрешать перенаправление устройства чтения смарт-карт – указывает, следует ли предотвращать сопоставление устройств чтения смарт-

карт (перенаправление устройства смарт-карт) в сеансе службы терминалов. Компьютер клиента должен работать под управлением Windows 2000 Server, Windows XP Professional или семейства Windows Server 2003;

- разрешать перенаправление звука – указывает, могут ли пользователи выбирать, где будет воспроизводиться звук с удалённого компьютера в сеансе службы терминалов (перенаправление звука);
- не разрешать перенаправление клиентских принтеров – эта политика может использоваться для запрещения пользователям перенаправление заданий на печать с удалённого компьютера на принтер, подключённый к их локальному (клиентскому) компьютеру.

н) Шифрование и безопасность:

- всегда запрашивать пароль у клиента при подключении – указывает, всегда ли службы терминалов запрашивают пароль клиента при подключении.
- установить уровень шифрования для клиентских подключений – указывает службам терминалов на необходимость применения указанного уровня шифрования для всех данных, передаваемых между клиентом и удалённым компьютером во время сеанса работы со службами терминалов;
- безопасный сервер – указывает, требует ли сервер терминалов безопасные подключения RPC от всех клиентов либо допускает небезопасные подключения.

о) Лицензирование:

- группа безопасности сервера лицензий – указывает серверы терминалов и серверы лицензий, которым сервер лицензирования сервера терминалов предоставляет лицензии. С помощью этого параметра можно определять, каким серверам будут выдаваться лицензии. По умолчанию сервер лицензирования служб терминалов выдаёт лицензию любому запросившему её компьютеру;

- запретить повышение лицензий – управляет тем, как сервер лицензий распределяет обновления лицензий для серверов терминалов, работающих под управлением Windows 2000. Сервер лицензий пытается предоставлять наиболее подходящие клиентские лицензии (CAL) для подключения.

п) Временные папки:

- не использовать временные папки для сеанса – указывает, следует ли службам терминалов создавать временные папки сеансов. Используя этот параметр, можно запретить создание на удалённом компьютере отдельных временных папок для каждого сеанса;
- не удалять временные папки при выходе – указывает, сохраняются ли временные папки служб терминалов после завершения сеансов пользователями. Этот параметр позволяет управлять временными папками сеансов пользователей на удалённом компьютере, даже если пользователь завершает сеанс.

р) Клиент:

- запретить сохранение паролей – указывает, могут ли сохраняться на этом компьютере пароли клиентов сервера терминалов.

с) Каталог сеансов:

- задать ограничение по времени для отключённых сеансов – этот параметр можно использовать для указания наибольшего количество времени, в течение которого отключённый сеанс остаётся открытым на сервере;
- задать ограничение по времени для активных сеансов – используя этот параметр, можно задать наибольший интервал времени, в течение которого сеанс служб терминалов может быть активен до автоматического отключения;
- задать ограничение по времени для бездействующих сеансов – параметр можно использовать для указания наибольшего количество

времени, в течение которого активный сеанс может оставаться бездействующим (без участия пользователя) до автоматического отключения;

- разрешать переподключение только от исходного клиента – указывает, могут ли пользователи переподключаться к отключённому сеансу служб терминалов, используя другой компьютер (не тот, с которого был начат сеанс);
- завершать сеанс при достижении ограничения по времени – этот параметр используется, чтобы указать, что при достижении ограничений по времени для активных или бездействующих сеансов эти сеансы следует завершать (то есть выполнить выход пользователя, а сеанс удалить с сервера).

Задание №6

1 Откройте оснастку «Групповая политика».

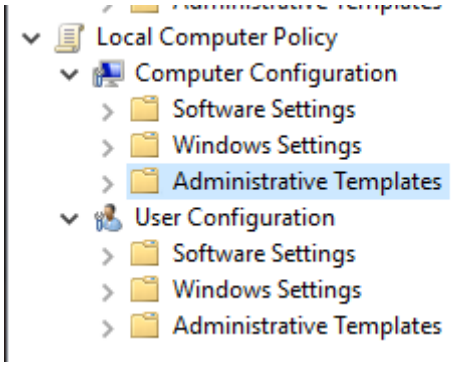

Рисунок 30 Оснастка «Групповая политика»

2 В узле «Конфигурация компьютера» выберите Административные шаблоны.

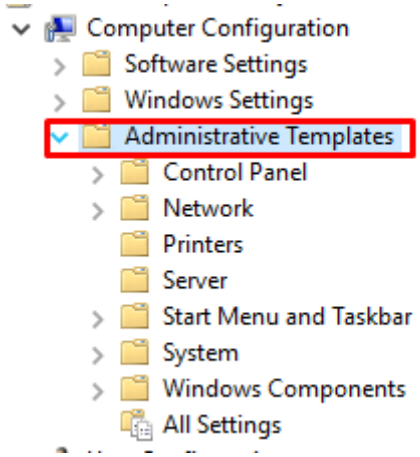

Рисунок 31 Административные шаблоны

3 Далее выберите «Все параметры» – «Запретить сохранение паролей».

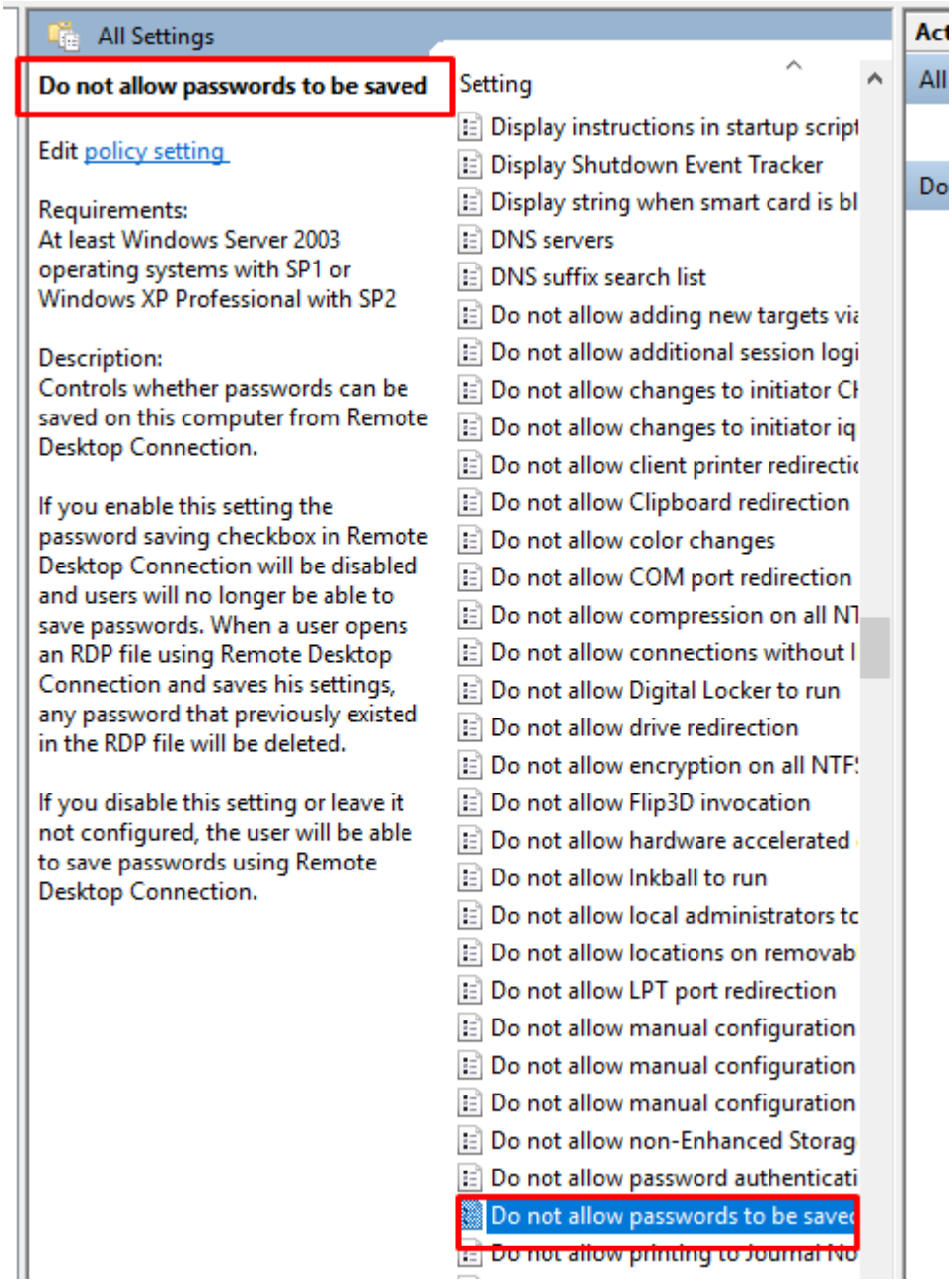

Рисунок 32 Запрет на сохранение паролей

4 В завершении установите необходимые параметры.

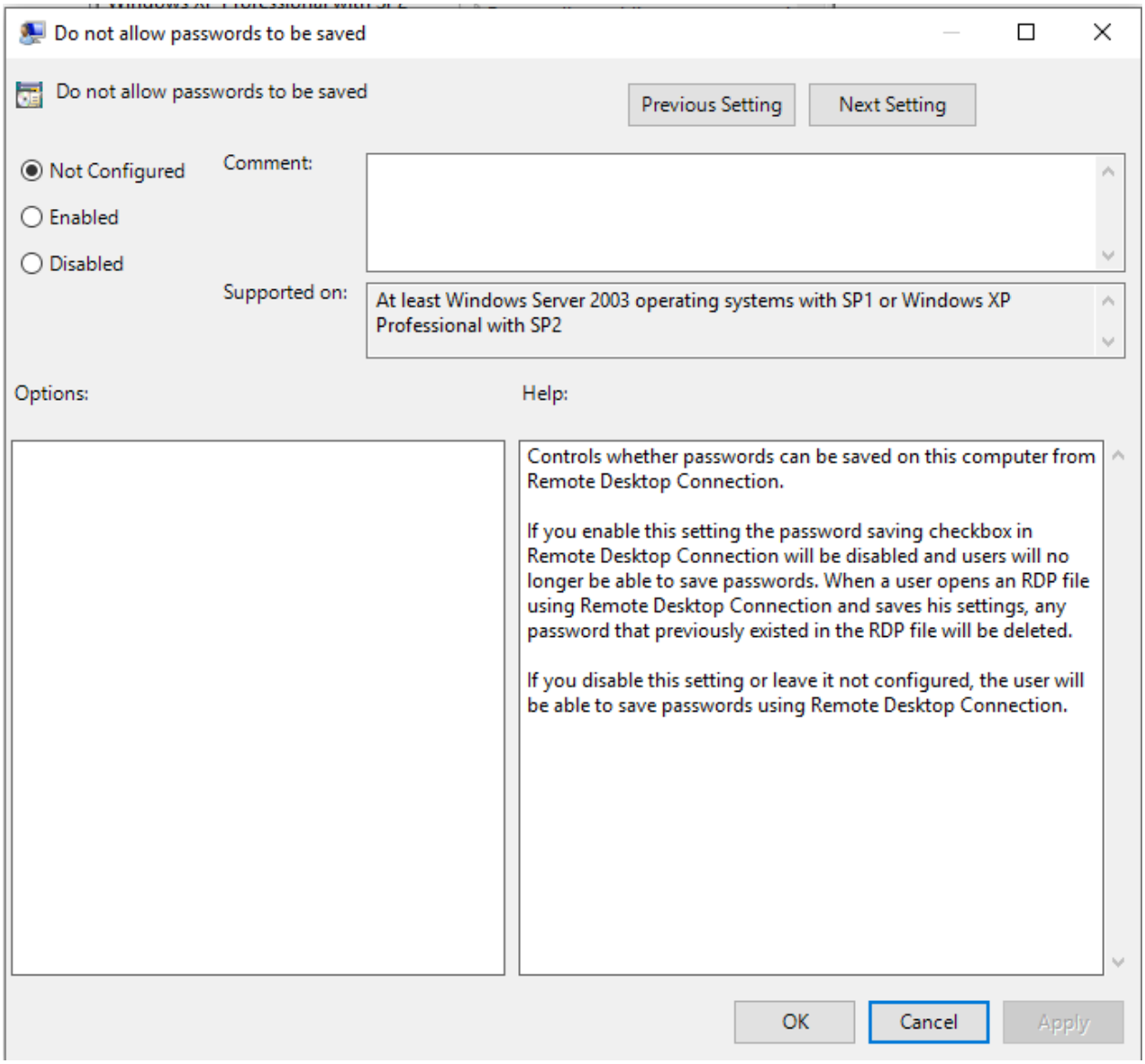

Рисунок 33 Установка необходимых параметров

т) Проводник:

- отключить защищённый режим протокола оболочки – позволяет настраивать функциональные возможности протокола оболочки. При использовании всех возможностей протокола приложения могут открывать папки и запускать файлы. Защищённый режим уменьшает возможности протокола, позволяя приложениям открывать только некоторые папки. Приложения не смогут запускать файлы в защищённом режиме. Рекомендуется использовать протокол в защищённом режиме для повышения безопасности Windows.

у) Установщик Windows:

- запретить использование установщика – эта политика может запретить пользователям устанавливать программы или разрешить устанавливать только программы, предложенные администратором;
- ведение журнала – указывает типы событий, записываемых установщиком Windows в журнал транзакций для каждой установки. Журнал, Msi.log, находится в папке Temp на системном томе;
- запретить установки для пользователей – позволяет настраивать установки для пользователей. Для этого следует включить эту политику и выбрать в раскрывающемся списке желаемое поведение;
- отключить создание контрольных точек восстановления системы – восстановление системы позволяет пользователям, в случае возникновения проблем, восстанавливать состояние своего компьютера на некоторый предшествующий момент, не теряя при этом личных файлов с данными. По умолчанию, установщик Windows Installer автоматически создает контрольную точку восстановления системы всякий раз при установке приложения, так что пользователи могут восстановить состояние компьютера до состояния, предшествовавшего установке этого приложения;
- запретить удаление обновлений – эта политика управляет тем, имеют ли право обычные пользователи или администраторы удалять обновления, установленные с помощью установщика Windows;
- максимальный размер кэша базисных файлов – эта политика задаёт процент свободного места на диске, доступного для кэша базисных файлов установщика Windows.

ф) Windows Messenger:

- запретить выполнение Windows Messenger – позволяет отключить Windows Messenger;
- не запускать Windows Messenger автоматически при входе – Windows Messenger автоматически загружается и начинает выполняться при входе пользователя в Windows XP. Эта политика может использоваться для

того, чтобы отменить автоматический запуск Windows Messenger при входе в систему.

х) Windows Update:

 не отображать параметр «Установить обновления и завершить работу» в диалоговом окне завершения работы Windows – позволяет выбрать, будет ли отображаться параметр «Установить обновления и завершить работу» в диалоговом окне завершения работы Windows;

 настройка автоматического обновления – указывает, будет ли данный компьютер получать обновления системы безопасности и другие важные обновления с помощью службы автоматического обновления Windows. Этот параметр позволяет указать, разрешается ли автоматическое обновление для данного компьютера;

 указать размещение службы обновлений Microsoft в интрасети – указывает сервер интрасети, на котором находятся обновления, полученные с веб-узлов обновлений Microsoft. Затем эту службу обновления можно использовать для автоматического обновления системы на всех компьютерах сети. Эта политика позволяет указать сервер в сети, на котором будет работать внутренняя служба обновлений. Клиентская программа автоматического обновления будет искать в этой службе обновлений, применимые для компьютеров сети;

 не выполнять автоматическую перезагрузку при автоматической установке обновлений, если в системе работают пользователи – указывает, что для завершения запланированной установки программа автоматических обновлений подождёт перезагрузки компьютера кем-либо из пользователей вместо принудительного автоматического перезапуска.

ц) Удалённое управление Windows:

 разрешить обычную проверку подлинности – позволяет определить, будет ли клиент службы удалённого управления Windows (WinRM) использовать обычную проверку подлинности;

- разрешить незашифрованный трафик – позволяет определить, будет ли клиент службы удалённого управления Windows посылать и принимать через сеть незашифрованные сообщения;
- надёжные сайты – позволяет определить, будет ли клиент службы удалённого управления Windows использовать список, заданный в списке надёжных сайтов, чтобы определить степень надёжности целевого сайта;
- запретить проверку подлинности согласованием – позволяет указать, что клиент службы удалённого управления Windows (WinRM) не будет использовать проверку подлинности согласованием;
- запретить проверку подлинности по протоколу Kerberos – позволяет указать, что клиент службы удалённого управления Windows (WinRM) не будет использовать проверку подлинности Kerberos непосредственно;
- запретить краткую проверку подлинности – позволяет указать, что клиент службы удалённого управления Windows (WinRM) не будет использовать краткую проверку подлинности.

ч) Удалённая оболочка Windows:

- тайм-аут простоя – задаёт в миллисекундах максимальное время, в течение которого удалённая оболочка при отсутствии активности пользователей остаётся открытой, а затем удаляется;
- тайм-аут оболочки – определяет максимальное время в миллисекундах, которое отводится на выполнение удалённой команды или сценария;
- разрешить доступ к удалённой оболочке – настраивает доступ к удалённым оболочкам;
- максимальный объём памяти в мегабайтах для одной оболочки – задаёт максимальный общий объём памяти, которую можно выделить для любой активной удалённой оболочки и её дочерних процессов;

- максимальное число удалённых оболочек для одного пользователя – задаёт максимальное количество одновременно запущенных оболочек, которые любой пользователь может удалённо открыть на одном компьютере;
- максимальное количество процессов для одной оболочки – задаёт максимальное количество процессов, разрешенное к запуску для удалённой оболочки;
- MaxConcurrentUsers – задаёт максимальное количество пользователей, которые могут параллельно выполнять удалённые операции в одной системе с помощью удалённой оболочки CMD.

ш) Проигрыватель Windows Media:

- не создавать ярлык на рабочем столе – запрещает добавление значка ярлыка проигрывателя на рабочий стол пользователя;
- не создавать ярлык на панели быстрого запуска – запрещает добавление ярлыка проигрывателя на панель быстрого запуска;
- не отображать диалоговые окна первого пользования – запрещает отображение диалоговых окон «Параметры конфиденциальности» и «Параметры установки» при первом запуске проигрывателя Windows Media;
- запрещение предоставления общего доступа к библиотеке – запрещает общий доступ к любой библиотеке проигрывателя Windows Media на этом компьютере с других компьютеров и устройств в домашней сети. Кроме того, флажок «Общий доступ по умолчанию» и кнопка «Запретить доступ» будут недоступны;
- запретить сглаживание изображения – запрещает сглаживание изображения, в результате чего улучшается качество воспроизведения на компьютерах с ограниченными ресурсами. Кроме того, флажок «Использовать сглаживание изображения» в диалоговом окне «Настройка ускорения видео» в проигрывателе снят и недоступен;

 запретить автоматическое обновление – запрещает обновление проигрывателя и отключает запросы на обновление для пользователей с правами администратора, когда появляется новая версия. Команда «Проверка наличия обновлений» в меню «Справка» в проигрывателе недоступна. Кроме того, ни один из временных интервалов не выбран и не доступен в разделе «Проверка обновлений» на вкладке «Проигрыватель».

Задание №7

1 Необходимо открыть оснастку «Групповая политика».

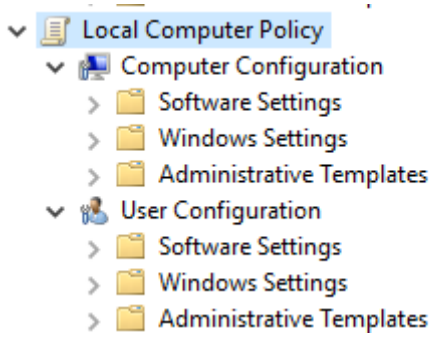

Рисунок 34 Оснастка «Групповая политика»

2 В дереве консоли выбрать Конфигурация компьютера – Административные шаблоны – Компоненты Windows – Проигрыватель Windows Media.

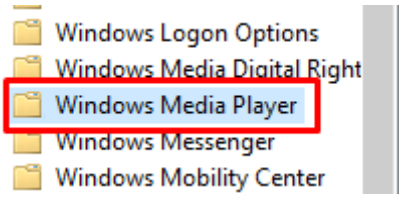

Рисунок 35 Проигрыватель Windows Media

3 Далее дважды щёлкнуть в правой части окна по пункту «Не создавать ярлык на рабочем столе».

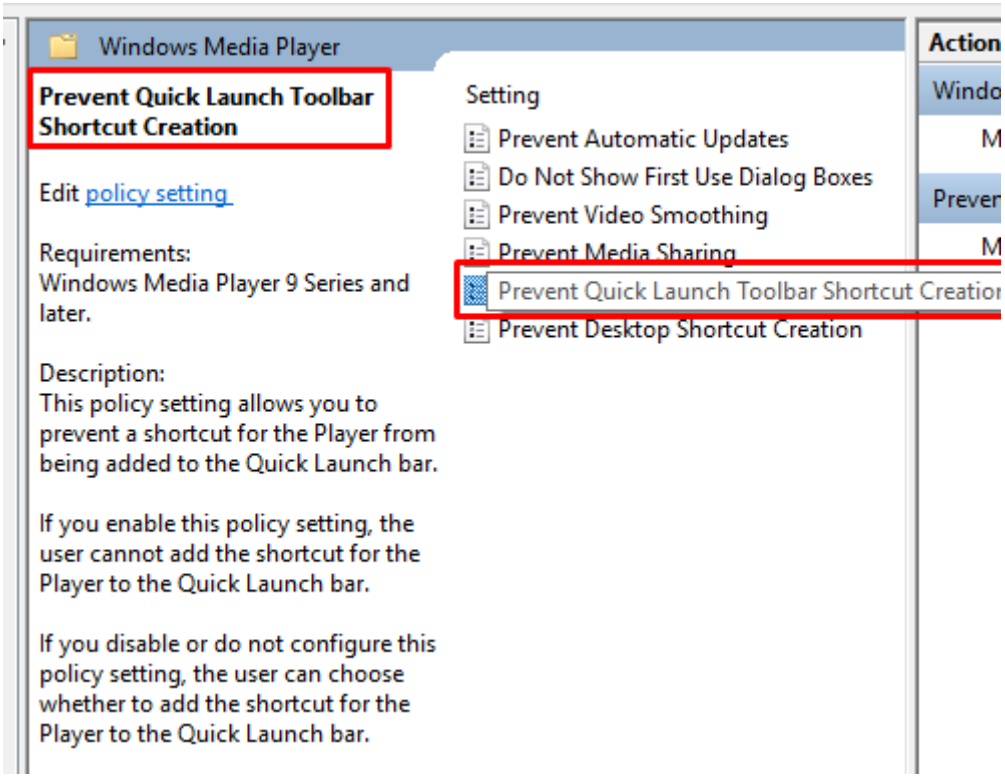

Рисунок 36 Проигрыватель Windows Media

4 Установить флажок «Включён».

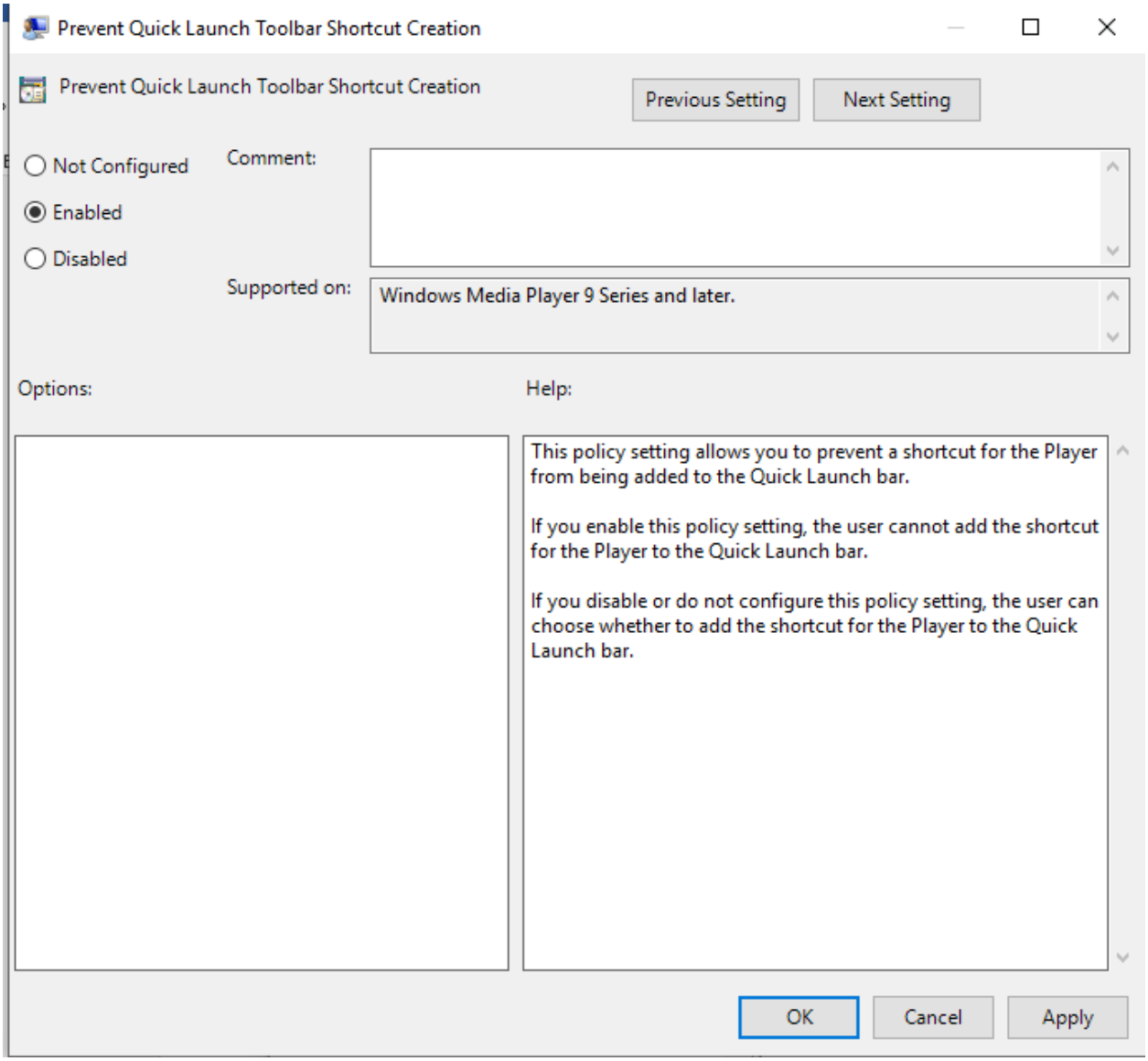

Рисунок 37 Флажок «Включён»

Система

Разрешает настройку параметров различных компонентов системы:

- предотвращение доступа к потенциально небезопасным функциям справки HTML для указанных папок – можно ограничить выполнение определённых команд справки HTML, чтобы они выполнялись только для файлов справки HTML (.chm) в указанных папках и их подпапках. Можно также отключить выполнение этих команд для всей системы. Настоятельно рекомендуется добавлять в эту политику только папки, требующие административных привилегий;

- не отображать страницу «Управление данным сервером» при входе – указывает, следует ли отключить автоматическое отображение страницы «Управление данным сервером»;
- отображать диалог слежения за завершением работы – диалог слежения за событиями завершения работы может отображаться при завершении работы рабочей станции или сервера. В нем содержится ряд вопросов, которые отображаются при вызове завершения работы компьютера, что используется для сбора сведений о том, почему выполняется завершение работы компьютера;
- включить постоянную временную метку – постоянный штамп времени позволяет системе обнаруживать время неожиданного отключения за счет записи на диск текущего времени по расписанию, которое определяется интервалом штампа времени;
- указать расположение установочных файлов Windows – указывает другое размещение для установочных файлов Windows;
- указать размещение установочных файлов пакета обновления Windows – указывает другое размещение для установочных файлов пакета обновления Windows;
- отключить сообщения о состоянии загрузки, завершения работы, входа и выхода из сети – подавляет сообщения о состоянии системы;
- подробные сообщения о состоянии – указывает системе, что следует отображать наиболее подробные сообщения о состоянии;
- отключить автозапуск – отключает возможность автозапуска. Автозапуск приводит к тому, что система приступает к чтению данных с устройства сразу же после того, как носитель вставлен в это устройство. В результате немедленно запускается файл программы установки для программных дисков или начинается воспроизведение музыки для звуковых носителей;

- не выключайте питание компьютера после завершения работы Windows – позволяет настроить автоматическое выключение питания компьютера после завершения работы Windows. Она не влияет на поведение завершения работы Windows, когда работа завершается вручную из меню Пуск или из диспетчера задач. Некоторые приложения, такие как программа обеспечения поддержки источника бесперебойного питания (ИБП), могут зависеть от поведения завершения работы Windows;
- отключить запрос на использование Windows Update при поиске драйверов – указывает, будет ли выдаваться запрос администратору о выполнении поиска драйверов на узле Windows Update через Интернет.

а) Сценарии:

- синхронное выполнение сценариев входа в систему – указывает, что системе следует дождаться завершения работы сценариев входа перед тем, как будет запущен интерфейс «Проводника Windows» и создан рабочий стол;
- асинхронное выполнение сценариев загрузки – позволяет системе асинхронное, одновременное выполнение сценариев загрузки. Сценарии загрузки представляют собой пакетные файлы, состоящие из команд, выполняемых системой при загрузке системы, перед тем как будет выдано приглашение для входа пользователя в систему. По умолчанию, система ожидает завершения выполнения каждого из сценариев загрузки перед запуском следующего сценария загрузки;
- выполнять сценарии загрузки с отображением команд – отображает команды сценариев загрузки во время их выполнения;
- выполнять сценарии завершения работы с отображением команд – отображает команды сценариев завершения работы во время их выполнения;

 максимальное время выполнения сценариев групповой политики – определяет, как долго система ожидает выполнения сценария, применяемого групповой политикой.

б) Вход в систему:

 всегда использовать классический вход в систему – вынуждает пользователя выполнять вход в систему с помощью классического окна входа в систему;

 запускать указанные программы при входе – указывает дополнительные программы или документы, которые Windows будет автоматически запускать или открывать при входе пользователя в систему.

в) Дисковые квоты:

 включить дисковые квоты – включает и отключает управление дисковыми квотами на всех NTFS-томах этого компьютера и запрещает пользователям изменять этот параметр;

 задать предел дисковой квоты – задаёт обязательное применение дисковых квот и запрещает пользователям изменять этот параметр;

 предел квоты по умолчанию и уровень предупреждения – указывает значение предела дисковой квоты и уровня предупреждения по умолчанию для новых пользователей тома;

 применять политику к съемным носителям – распространяет политики дисковой квоты из этой папки на все тома с файловой системой NTFS на съемных носителях.

г) Групповая политика:

 отключить фоновое обновление групповой политики – предотвращает обновление групповой политики во время использования компьютера. Эта политика применима к групповым политикам для компьютеров, пользователей и контроллеров домена;

 интервал обновления групповой политики для компьютеров – определяет частоту обновления групповой политики для компьютеров во

время работы (в фоновом режиме). Эта политика указывает частоту фонового обновления только для групповых политик в папке «Конфигурация компьютера»;

- обнаружение медленных подключений для групповой политики – определяет медленное подключение для применения или обновления групповой политики;
- обработка политики реестра – определяет порядок обновления политик работы с реестром;
- обработка политики настройки IE –определяет порядок обновления политик настройки Internet Explorer;
- обработка политики установки программ – определяет порядок обновления политик установки программ. Оказывает влияние на все политики, использующие компонент установки программ из групповой политики, в том числе, политики, находящиеся в разделе «Конфигурация программ \ Установка программ»;
- обработка политики сценариев – определяет, когда обновляются политики, которые назначают выполнение общих сценариев;
- всегда использовать локальные файлы ADM для редактора объектов групповой политики – разрешение использовать локальные ADM-файлы для оснастки групповой политики. По умолчанию при редактировании объекта групповой политики используется оснастка редактора объекта групповой политики; ADM-файлы загружаются из объекта групповой политики в оснастку редактора.

д) Удалённый помощник:

- запрошенная удалённая помощь – определяет, можно ли пользователю запрашивать удалённую помощь с этого компьютера;
- разрешить предложение удалённой помощи – определяет, может ли персонал службы поддержки или сетевой администратор (в дальнейшем «эксперт») предлагать удалённую помощь для пользователя этого

компьютера, если пользователь первым явно не запросил помощь через канал связи, электронную почту или службу мгновенных сообщений.

е) Восстановление системы:

- отключить восстановление системы – восстановление системы позволяет пользователям, в случае возникновения проблем, восстанавливать состояние своего компьютера на некоторый предшествующий момент, не теряя при этом личных файлов с данными;
- отключить конфигурацию – позволяет отключать интерфейс конфигурации для восстановления системы.

Задание №8

1. В дереве консоли выбрать «Конфигурация компьютера» – «Административные шаблоны» – «Система» – «Восстановление системы».

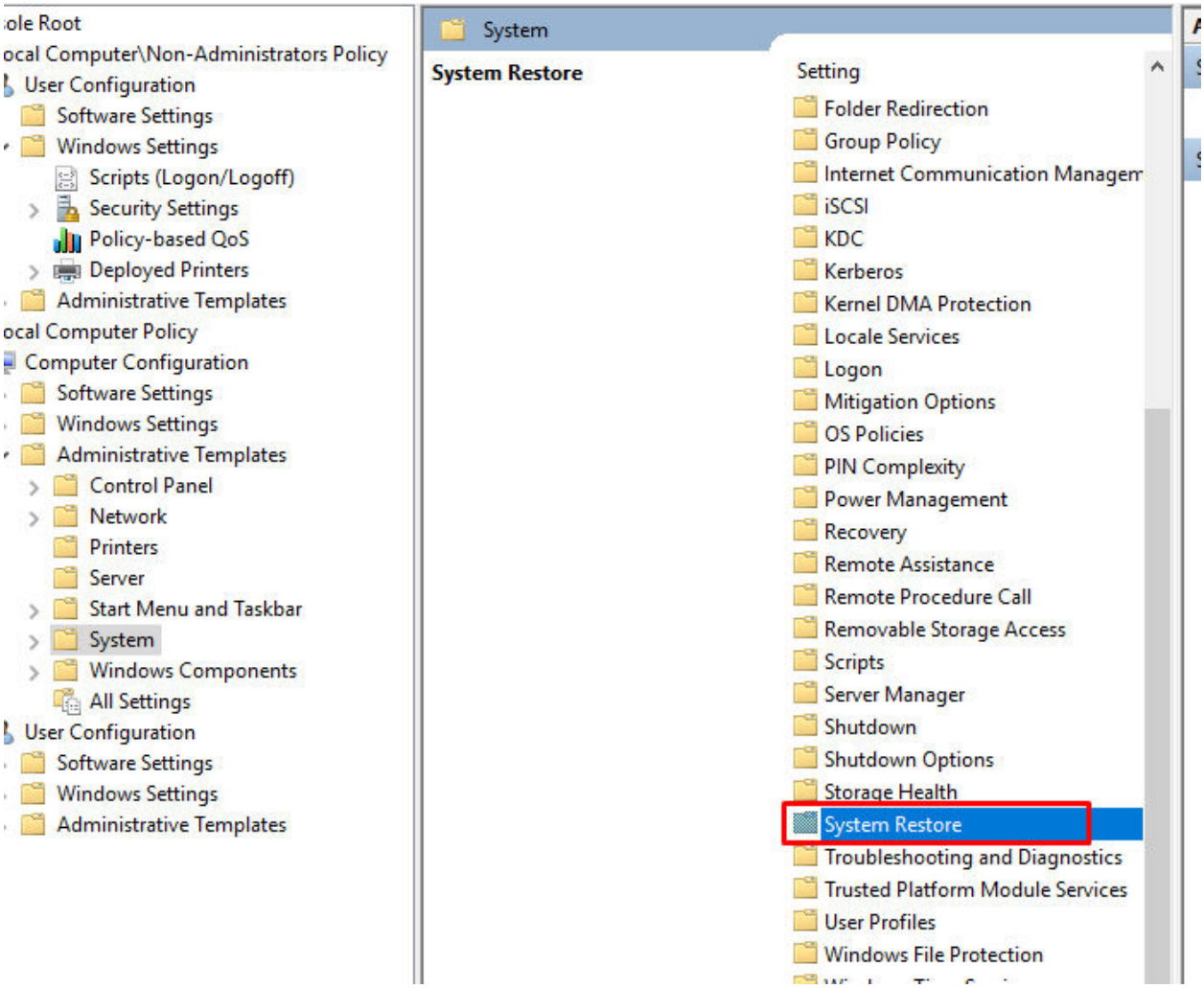

Рисунок 38 «Восстановление системы»

2. Далее дважды щёлкнуть в правой части окна по пункту «Отключить конфигурацию».

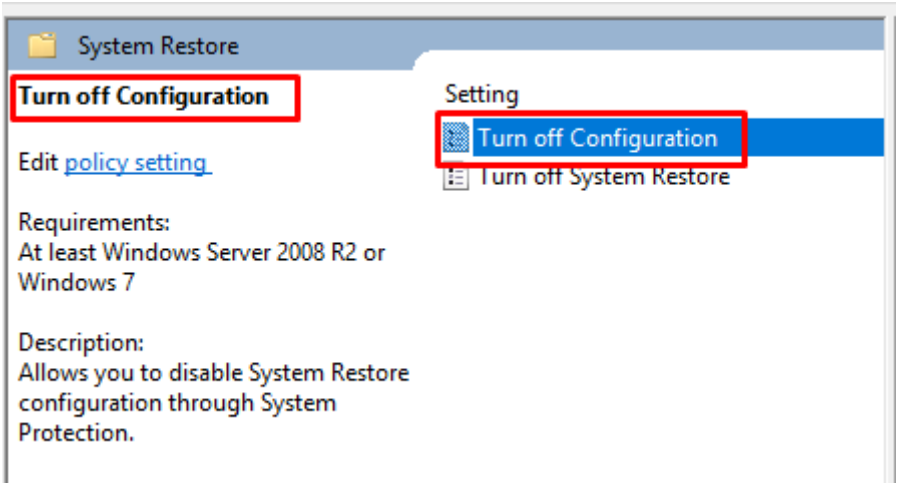

Рисунок 39 «Отключить конфигурацию»

3. Задать параметр «Включён».

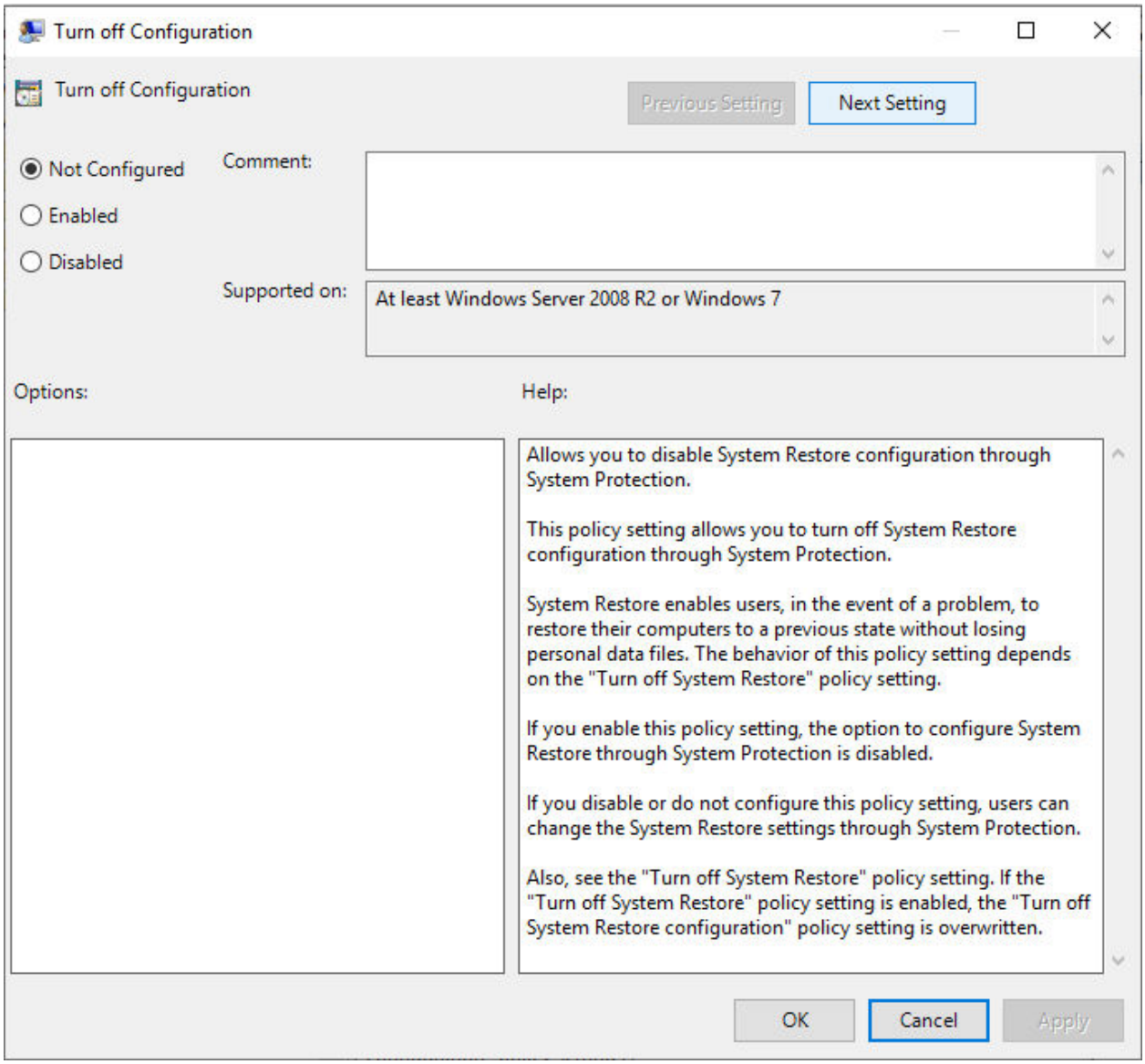

Рисунок 40 Параметр «Включён»

ж) Отчёт об ошибках:

- отображать уведомления об ошибках – используется для управления тем, будет ли пользователь иметь возможность отправлять отчёт об ошибках;
- настроить отчёты об ошибках – задаёт параметры отправки отчёта об ошибках и того, какая информация отправляется в этих отчётах, если включена отправка отчётов об ошибках. Эта политика не включает и не отключает отправку отчётов об ошибках, для этого следует использовать политику «Отключить отчёты об ошибках Windows» в папке «Конфигурация

компьютера/Административные шаблоны/Система/Управление связью через Интернет/Параметры связи через Интернет»;

- сообщать о системных ошибках – эта политика управляет тем, следует ли добавлять сообщения об ошибках в работе операционной системы в отчёт, если включена отправка отчётов об ошибках;
- список приложений, для которых нужно отправлять отчёт об ошибках – задаёт приложения, для которых всегда нужно отправлять отчёт об ошибках;
- список приложений, для которых не нужно отправлять отчёт об ошибках – управляет рапортованием об ошибках для обычных приложений, когда рапортование об ошибках включено.

з) Защита файлов Windows:

- установить частоту сканирования защиты файлов – определяет, когда средство защиты файлов Windows сканирует защищённые файлы. Этот параметр заставляет средство защиты файлов Windows выполнять перечисление и сканирование всех системных файлов с целью обнаружения изменений;
- скрывать окно индикации сканирования файлов – скрывает окно индикации выполнения сканирования файлов. Это окно обеспечивает дополнительную информацию о состоянии, которая может потребоваться только опытным пользователям;
- ограничить размер кэша защиты файлов – указывает наибольший объём места на диске, который может использоваться для файлового кэша защиты файлов Windows.

и) Служба времени Windows:

- глобальные параметры конфигурации – задаёт набор параметров для всех поставщиков времени, установленных на компьютере;

- включить Windows NTP-клиента – указывает, включён ли NTP-клиент Windows. Включение NTP-клиента Windows позволяет компьютеру выполнять синхронизацию часов компьютера с другими NTP-серверами;
- настроить Windows NTP-клиента – указывает, выполняет ли NTP-клиент Windows синхронизацию времени с доменной иерархией или настроенным вручную NTP-сервером. Указывает, может ли клиент синхронизовать время из источника, находящегося за пределами своего сайта, как долго NTP-клиент Windows ожидает перед тем, как попытаться заново разрешить не разрешенное ранее имя NTP-сервера, и степень подробности протоколирования событий NTP-клиента;
- включить Windows NTP-сервер – указывает, включён ли NTP-сервер Windows. Включение NTP-сервера Windows позволяет компьютеру обслуживать NTP-запросы от других компьютеров.

к) Управление связью через Интернет:

- ограничить связь через Интернет – указывает, может ли Windows использовать доступ к Интернету для выполнения задач, требующих обращения к ресурсам Интернета;
- отключить веб-публикацию в списке задач для файлов и папок – указывает, отображаются ли задачи «Опубликовать файл в вебе», «Опубликовать эту папку в вебе», «Опубликовать выделенные объекты в вебе» в разделе задач для файлов и папок в окне Проводника Windows. «Мастер веб-публикаций» используется для загрузки списка поставщиков услуг и позволяет публиковать информацию на вебе;
- отключить загрузку из Интернета для мастеров веб-публикаций и заказа отпечатков – указывает, нужно ли загружать список поставщиков услуг для мастеров веб-публикации и заказа отпечатков;
- отключить заказ отпечатков через Интернет в списке задач для изображений – указывает, надо ли отображать «Заказ отпечатков через Интернет» в списке задач для изображений;

- отключить участие в программе улучшения поддержки пользователей Windows Messenger – указывает, выполняет ли Windows Messenger сбор анонимной информации о том, как используется программное обеспечение и служба Windows Messenger;
- отключить службу сопоставления файлов Интернета – указывает, нужно ли использовать веб-службу Майкрософт для поиска приложений, подходящих для открытия файлов, которым ещё не сопоставлено приложение. Когда пользователь открывает файл, расширение имени которого не сопоставлено ни одному из приложений на этом компьютере, имеется возможность выбрать либо одно из локальных приложений, либо обратиться в веб-службу для поиска подходящего приложения;
- отключить выполнение печати через HTTP-протокол – указывает, следует ли разрешить выполнение печати от этого клиента через HTTP-протокол. Выполнение печати через HTTP позволяет клиентам выполнять печать на принтерах, находящихся как в интрасети, так и в Интернете.

л) DCOM (параметры совместимости приложений):

- разрешать локальные исключения проверки безопасности при активации – позволяет указать, что локальные администраторы компьютера могут предоставлять список для политики «Задать исключения проверки безопасности при активации»;
- задать исключения проверки безопасности при активации – позволяет просматривать и изменять список кодов приложения DCOM-сервера (appid), исключённых из проверки безопасности при активации DCOM. DCOM использует два списка: один настроен через групповую политику с использованием этой политики; другой – действиями локальных администраторов компьютера.

Конфигурация пользователя

Этот узел служит для настройки политик, применяемых к пользователям независимо от того, на каком компьютере они входят в

систему. Узел «Конфигурация пользователя», как правило, содержит вложенные элементы для параметров программ, параметров Windows и административных шаблонов.

Конфигурация Windows

Узел, расположенный в дереве \Конфигурация пользователя \Конфигурация Windows, содержит параметры, применяющиеся к пользователям вне зависимости от того, с какого компьютера они входят в систему. Он включает три подпапки: «Перенаправление папки», «Параметры безопасности» и «Сценарии».

Сценарии вход/выход из системы

Администраторы используют это расширение для указания сценариев, которые выполняются при входе пользователя в систему или выходе из неё. Сценарии выполняются в пользовательском контексте.

- Вход в систему – содержит сценарии входа в систему пользователя.
- Выход из системы – содержит сценарии выхода пользователя.

Параметры безопасности

Параметры безопасности были рассмотрены в предыдущей лабораторной работе.

Административные шаблоны

Узел «Административные шаблоны» содержит всю информацию о политиках системного реестра.

Как правило, узел «Административные шаблоны» не всегда содержит полный перечень политик. Для того чтобы получить полный доступ к политикам данной категории необходимо подключить файл, содержащий административные шаблоны. Сделать это можно следующим образом:

- разверните узел «Конфигурация пользователя» (если он не развёрнут);

- в узле «Конфигурация пользователя» нажмите ПКМ на элемент «Административные шаблоны»;
- выберите пункт меню «Добавление и удаление шаблонов»;
- нажмите кнопку «Добавить»;
- выберите файл system.adm;
- нажмите кнопку «Открыть».

Теперь, имея доступ ко всем административным шаблонам, рассмотрим принцип работы некоторых из них.

Компоненты Windows

а) NetMeeting. Общий доступ к приложениям;

- открыть общий доступ к приложениям – запрещает общий доступ к приложениям с помощью NetMeeting. Пользователи не смогут предоставлять общий доступ к своим приложениям или пользоваться доступом к чужим приложениям;
- запретить предоставление общего доступа – запрещает пользователям предоставлять общин доступ. Однако они смогут пользоваться общим доступом к чужим приложениям или рабочему столу;
- запретить предоставление общего доступа к рабочему столу – запрещает пользователям предоставлять общин доступ к рабочему столу. Однако они смогут предоставлять общин доступ к отдельным приложениям;
- запретить предоставление общего доступа к командной строке – запрещает пользователям предоставлять общин доступ к командной строке. Таким образом, предотвращается возможность непредусмотренного предоставления доступа к другим приложениям, поскольку командная строка может использоваться для запуска других приложений;
- запретить предоставление общего доступа к окнам Проводника – запрещает пользователям предоставлять общин доступ к окнам Проводника. Таким образом, предотвращается возможность непредусмотренного

предоставления доступа к другим приложениям, поскольку окно Проводника может использоваться для запуска других приложений;

 запретить общий доступ к приложениям в режиме True Color – запрещает пользователям предоставлять общий доступ к приложениям в режиме True Color. В этом режиме приложение требует большей пропускной способности канала связи.

Контрольные вопросы:

1. Что подразумевается под «параметрами» Групповой политики?

Параметры политики безопасности — это правила, которые администраторы настраивают на компьютере или нескольких устройствах с целью защиты ресурсов на устройстве или сети.

2. Какой узел используют администраторы для задания политик, применяемых к компьютерам, независимо от того, кто осуществил вход в систему и каким образом?

Конфигурация компьютера;

3. Какой узел используется для задания политик, применяемых к пользователям, независимо от того, с какого компьютера ими осуществлён вход в систему?

Конфигурация пользователя;

4. Чем отличается содержание папки «Конфигурация программ», расположенная в узле \Конфигурация компьютера\ Конфигурация программ от содержания папки, расположенной в узле \ Конфигурация пользователя\ Конфигурация программ.

Содержание папки «Конфигурация программ», расположенная в узле \Конфигурация компьютера\ Конфигурация программ ничем не отличается от содержания папки, расположенной в узле \ Конфигурация пользователя\ Конфигурация программ