**Цель работы:** изучить редактор локальной групповой политики и научиться настраивать групповые политики безопасности на АРМ пользователя с установленной на нем ОС Windows для защиты информации от несанкционированного доступа (НСД).

Используемое программное обеспечение: ОС версии не ниже Windows XP.

## 1. Теоретические сведения:

*1.1. Введение в групповые политики Windows*

Групповые политики – это совокупность параметров, используемых для конфигурирования рабочего окружения пользователя или компьютера. Механизм групповых политик – основа централизованного управления конфигурациями пользователей (для разделения ресурсов между несколькими пользователями, использующих один компьютер) и компьютеров в корпоративной сети. В домашних условиях вы можете просто применить к своему компьютеру и необходимым учетным записям реестра, при помощи которых большинство настроек будут применены после перезагрузки компьютера или настраивать его вручную, что может занять очень много времени. Но как же быть, если вы работаете администратором в крупной организации, где нужно настроить десятки, а может и сотни компьютеров? Причем, в вашей организации, скорее всего, существует несколько отделов, у каждого из которых должны быть индивидуальные настройки. Например, компьютеры, расположенные в конференц-залах, предназначенные для проведения презентаций должны быть оснащены обоями рабочего стола с корпоративным логотипом. Или сотрудники отдела маркетинга не должны иметь права на запуск оснастки служб системы или редактора системного реестра. Большинство настроек локального компьютера или автоматизированного рабочего места (АРМ) пользователя, а также сетевых АРМ, которые входят в состав доменной сети, настраиваются при помощи групповых политик.

Групповые политики - это набор правил, обеспечивающих инфраструктуру, в которой администраторы локальных компьютеров и доменных служб Active Directory могут централизовано развертывать и управлять настройками пользователей и компьютеров в организации. Все настройки учетных записей, операционной системы, аудита, системного реестра, параметров безопасности, установки программного обеспечения и прочие параметры развертываются и обновляются в рамках домена при помощи параметров объектов групповой политики GPO (Group Policy Object). Объект групповой политики (англ. Group Policy Object, GPO) состоит из двух физически раздельных составляющих: контейнера групповой политики (англ. Group Policy Container, GPC) и шаблона групповой политики (англ. Group Policy Template, GPT). Эти два компонента содержат в себе все данные 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. Политики применяются сверху вниз по иерархии каталога Active Directory.

Групповые политики являются компонентом операционной системы Windows и основываются на тысячах отдельных параметров политик, иначе говоря, политик, определяющих определённую конфигурацию для своего применения.

*1.2. История групповых политик*

Структура многопользовательских операционных систем предполагает возможность создания для отдельного пользователя индивидуального окружения. В окружение пользователя могут входить: конфигурации рабочего стола и индивидуальные настройки оболочки; доступные пользователю приложения; сценарии, выполняющиеся при входе пользователя в системе или выходе из нее; ассоциированные с пользователем права и разрешения на доступ к локальным и сетевым информационным ресурсам. Для управления

правами пользователей в доменах Windows и применяются механизмы групповых политик.

Для операционных систем Windows концепция групповых политик не является инновационным шагом в области системной безопасности и настройки операционных систем. Первые политики появились еще в Windows NT 4.0 и назывались системными политиками. Эти политики предназначались только для изменения данных системного реестра и основывались на файлах, которые назывались шаблонами adm. Для создания этих политик использовался специальный редактор системных политик. На то время системные политики были значительным шагом в обеспечении безопасности операционных систем Windows, несмотря на то, что объекты локальной политики не использовались, и система Windows NT 4.0 не поддерживала службы Active Directory.

Групповые политики появились в операционной системе Windows 2000 и включали в себя около 900 настроек для пользователей и компьютеров, которые могли в полной мере применяться к клиентским компьютерам. Из утилиты, предназначенной для изменения данных системного реестра, групповые политики операционной системы Windows 2000 превратились в компонент, предназначенный для изменения параметров конфигурации операционной системы. Групповые политики по-прежнему расположены в шаблонах ADM. Система Windows 2000 Server уже позволяет распространять объекты групповых политик для компьютеров, расположенных в домене и подразделениях (OU) в Active Directory.

В операционных системах Windows XP и Windows Server 2003 возможности групповых политик были расширены. С появлением этих систем у администраторов появилась возможность управлять параметрами безопасности и установкой приложений, а количество политик увеличилось до 1400. Локальные объекты групповой политики существовали независимо от того, входит ли компьютер в состав домена, рабочей группы или вовсе не принадлежит к сетевой среде. Политики распространялись только на тот

компьютер, где хранятся сами GPO. В том случае, если компьютер не принадлежал к домену, локальная политика использовалась только для настройки конфигурации локального компьютера. Но если он входил в состав домена Active Directory, то параметры, привязанные к инфраструктурной единице домена (домен, лес, сайт) заменяли параметры локального объекта групповой политики.

Операционные системы Windows Vista и Windows Server 2008 уже поддерживают около 2500 настроек групповых политик. Новые категории управления политиками теперь уже обеспечивают управление питанием, возможность блокировки установки устройств, улучшенные параметры безопасности, расширение настроек Internet Explorer, а также возможность делегировать пользователям право устанавливать драйверы принтеров. В этих операционных системах было создано расширение для формата шаблонов политик. У форматов adm был значительный недостаток - для реализации локализации групповых политик нужно было создавать отдельный adm-файл для каждого языка. Теперь административные шаблоны представляют собой пару XML-файлов - *.admx файл, который определяет изменения в реестре, а также adml файл, который отвечает за языковые настройки указанной политики. Несмотря на эти изменения, в одной системе могут сосуществовать как adm, так и admx/adml шаблоны без всяких проблем. В операционной системе Windows Server 2008 можно создавать стартовые объекты групповой политики. Использование стартового объекта групповой политики позволяет хранить набор параметров административных шаблонов политик в одном объекте и включать эти параметры в новые объекты групповой политики. Также для каждого объекта групповых политик появились возможности добавления комментариев, а сведения о подключенных сетях обеспечивают улучшение отклика групповой политики на изменение сетевых условий.

В операционных системах Windows 7 и Windows Server 2008 R2 уже насчитывается около 3200 настроек групповых политик.

*1.3. Оснастка «Редактор локальной групповой политики»*

Объекты групповых политик делятся на две категории:

«Доменные объекты групповых политик», которые используются для централизованного управления конфигурацией компьютеров и пользователей, входящих в состав домена Active Directory. Эти объекты хранятся только на контроллере домена.

«Локальные объекты групповых политик», которые позволяют настраивать конфигурацию локального компьютера, а также всех пользователей, созданных на этом компьютере. Эти объекты хранятся только в локальной системе. Локальные объекты групповых политик могут применяться, даже если компьютер входит в состав домена. Для управления локальными объектами групповых политик в операционных системах Windows используется оснастка консоли управления «Редактор локальной групповой политики». При помощи данной оснастки вы можете настраивать большинство системных компонентов и приложений.

В оснастке редактора локальных объектов групповой политики присутствуют два основных узла:

*1.3.1. Узел «Конфигурация компьютера».*

Узел «Конфигурация компьютера» предназначен для настройки параметров компьютера. В этом узле расположены параметры, которые применяются к компьютеру, невзирая на то, под какой учетной записью пользователь вошел в систему. Эти параметры применяются при запуске операционной системы и обновляются в фоновом режиме каждые 90-120 минут. Узел «Конфигурация компьютера» содержит три дочерних узла, при помощи которых настраиваются все параметры локальных объектов групповых политик: «Конфигурация программ», «Конфигурация Windows», «Административные шаблоны».

*1.3.2. Узел «Конфигурация пользователя»*

Узел «Конфигурация пользователя» предназначен для настроек параметров пользователей. Параметры, которые находятся в этом узле,

применяются при входе конкретного пользователя в систему. Так же, как и параметры, расположенные в узле конфигурации компьютера, параметры, расположенные в узле конфигурации пользователя обновляются в фоновом режиме каждые 90-120 минут. Узел «Конфигурация пользователя» также содержит три дочерних узла, при помощи которых настраиваются все параметры локальных объектов групповых политик: «Конфигурация программ», «Конфигурация Windows», «Административные шаблоны».

В дочернем узле «Конфигурация программ» расположено только одно расширение клиентской стороны «Установка программ», благодаря которому, вы можете указать определенную процедуру установки программного обеспечения. Расширения клиентской стороны (Client-Side-Extension, CSE) преобразовывает указанные параметры в объект групповой политики и вносит изменения в конфигурацию пользователя или компьютера. Создавать объекты групповой политики для развертывания программного обеспечения можно только в операционной системе Windows Server 2008/2008R2.

Дочерний узел «Конфигурация Windows» в основном предназначен для обеспечения безопасности компьютера и учетной записи, для которой применяются данные политики. В нем вы можете найти несколько опций безопасности «Политика разрешения имен», «Сценарии», «Развернутые принтеры», «Параметры безопасности». Особый интерес представляет опция «Параметры безопасности». Эта опция позволяет настраивать политики безопасности средствами GPO. В этой опции для конфигурации безопасности компьютера доступны следующие настройки политик:

Политики учетных записей (позволяют устанавливать политику паролей и блокировки учетных записей).

Локальные политики (отвечают за политику аудита, параметры безопасности и назначения прав пользователя).

Политики открытого ключа (позволяют: настраивать компьютеры на автоматическую отправку запросов в центр сертификации предприятия и установку выдаваемых сертификатов; создавать и распространять список

доверия сертификатов (CTL); добавлять агенты восстановления шифрованных данных и изменение параметров политики восстановления шифрованных данных; добавлять агенты восстановления данных шифрования диска BitLocker).

Политики ограниченного использования программ (позволяют осуществлять идентификацию программ и управлять возможностью их выполнения на локальном компьютере, в подразделении, домене и узле).

Политики управления приложениями (отвечают за создание и управления правилами и свойствами функционала AppLocker, который позволяет управлять установкой приложений и сценариев).

Политики IP-безопасности на «Локальный компьютер» (позволяют создавать политику IP-безопасности локального компьютера и управлять списками IP–фильтров).

Дочерний узел «Административные шаблоны» является крупнейшим из всех возможных расширений групповой политики и включает тысячи параметров для приложений и компонентов операционной системы Windows. Каждому параметру политики административных шаблонов соответствует определенный параметр системного реестра.

Политики в дочернем узле «Административные шаблоны» узла «Конфигурация компьютера» изменяют значения реестра в ключе HKEY_LOCAL_MACHINE (или просто HKLM), а политики в дочернем узле «Административные шаблоны» узла «Конфигурация пользователя» - HKEY_CURRENT_USER (HKCU). В некоторых источниках административные шаблоны могут называться политиками на основе реестра. В рамках этой работы должен быть рассмотрен дочерний узел «Административные шаблоны» для локального компьютера. О применении настроек административных шаблонов для нескольких компьютеров или пользователей, входящих в домен, в данной работе не обсуждается. Для системных администраторов дочерний узел «Административные шаблоны» предоставляет возможности динамического управления операционной

системой. Несмотря на то, что администратору понадобится немало времени на настройку этого узла, все изменения, примененные при помощи групповых политик, невозможно будет изменить средствами пользовательского интерфейса.

## 2. Ход выполнения лабораторной работы.

По исходным данным варианта № 4, проводится настройка АРМ в ИС типа 1Б.

Требования к классу защищенности 1Б:

Подсистема управления доступом:

должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю временного действия длиной не менее восьми буквенно-цифровых символов;

- должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по физическим адресам (номерам);

- должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;

- должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;

- должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на него информации.

Подсистема регистрации и учета:

должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС.

В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;

- результат попытки входа: успешный или неуспешный - несанкционированный;

- идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;

- код или пароль, предъявленный при неуспешной попытке;

- должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа его последовательным номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). Вместе с выдачей документа должна автоматически оформляться учетная карточка документа с указанием даты выдачи документа, учетных реквизитов документа, краткого содержания (наименования, вида, шифра, кода) и уровня конфиденциальности документа, фамилии лица, выдавшего документ, количества страниц и копий документа (при неполной выдаче документа - фактически выданного количества листов в графе «Брак»).

В параметрах регистрации указываются:

- дата и время выдачи (обращения к подсистеме вывода);

- спецификация устройства выдачи [логическое имя (номер) внешнего устройства];

- краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;

- идентификатор субъекта доступа, запросившего документ;

- объем фактически выданного документа (количество страниц, листов, копий) и результат выдачи успешный (весь объем), неуспешный;

- должна осуществляться регистрация запуска (завершения) всех программ и процессов (заданий, задач) в АС. В параметрах регистрации указываются:

- дата и время запуска;

- имя (идентификатор) программы (процесса, задания);

- идентификатор субъекта доступа, запросившего программу (процесс, задание);

- результат запуска (успешный, неуспешный - несанкционированный);

- должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам.

В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная;

- идентификатор субъекта доступа;

- спецификация защищаемого файла;

- имя программы (процесса, задания, задачи), осуществляющей доступ к файлу;

- вид запрашиваемой операции (чтение, запись, удаление, выполнение, расширение и т.п.);

- должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей.

В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная;

- идентификатор субъекта доступа;

- спецификация защищаемого объекта [логическое имя (номер)];

- имя программы (процесса, задания, задачи), осуществляющей доступ к защищаемому объекту;

- вид запрашиваемой операции (чтение, запись, монтирование, захват и т.п.);

- должна осуществляться регистрация изменений полномочий субъектов доступа и статуса объектов доступа. В параметрах регистрации указываются:

- дата и время изменения полномочий;

- идентификатор субъекта доступа (администратора), осуществившего изменения;

- идентификатор субъекта, у которого проведено изменение полномочий и вид изменения (пароль, код, профиль и т.п.);

- спецификация объекта, у которого проведено изменение статуса защиты и вид изменения (код защиты, уровень конфиденциальности);

- должен осуществляться автоматический учет создаваемых защищаемых файлов, инициируемых защищаемых томов, каталогов, областей оперативной памяти ЭВМ, выделяемых для обработки защищаемых файлов, внешних устройств ЭВМ, каналов связи, ЭВМ, узлов сети ЭВМ, фрагментов сети с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;

- должен проводиться учет всех защищаемых носителей информации с помощью их маркировки;

- учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);

- должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации;

- должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей.

Очистка осуществляется двукратной произвольной записью в любую освобождаемую область памяти, использованную для хранения защищаемой информации;

- должна осуществляться сигнализация попыток нарушения защиты на терминал администратора и нарушителя.

Криптографическая подсистема:

должно осуществляться шифрование всей конфиденциальной информации, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, в каналах связи, а также на съемные портативные носители данных (дискеты, микрокассеты и т.п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа. При этом должна выполняться принудительная очистка областей внешней памяти, содержавших ранее незашифрованную информацию;

- доступ субъектов к операциям шифрования и к соответствующим криптографическим ключам должен дополнительно контролироваться посредством подсистемы управления доступом;

- должны использоваться сертифицированные средства криптографической защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации криптографических средств защиты.

Подсистема обеспечения целостности:

должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды. При этом:

- целостность СЗИ НСД проверяется по контрольным суммам всех

компонент СЗИ как в процессе загрузки, так и динамически в процессе работы АС;

- целостность программной среды обеспечивается качеством приемки программных средств в АС, предназначенных для обработки защищенных файлов;

- должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС;

- должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД. Администратор должен иметь свой терминал и необходимые средства оперативного контроля и воздействия на безопасность АС;

- должно проводиться периодическое тестирование всех функций СЗИ НСД с помощью специальных программных средств не реже одного раза в квартал;

- должны быть в наличии средства восстановления СЗИ НСД, редусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности, а также оперативное восстановление функций СЗИ НСД при сбоях;

- должны использоваться сертифицированные средства защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации средств защиты СЗИ НСД.

### *2.1. Выбрать оснастку «Редактора локальной групповой политики»*

Использование системного окна «Выполнить».

Воспользуйтесь комбинацией клавиш «WIN+R» для открытия диалога «Выполнить». В диалоговом окне «Выполнить», в поле «Открыть» введите gpedit.msc и нажмите на кнопку «ОК».

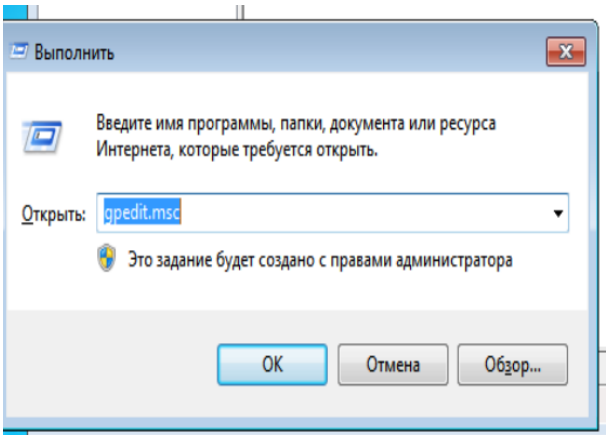


Рисунок 1 - Переход к редактору локальной групповой политики

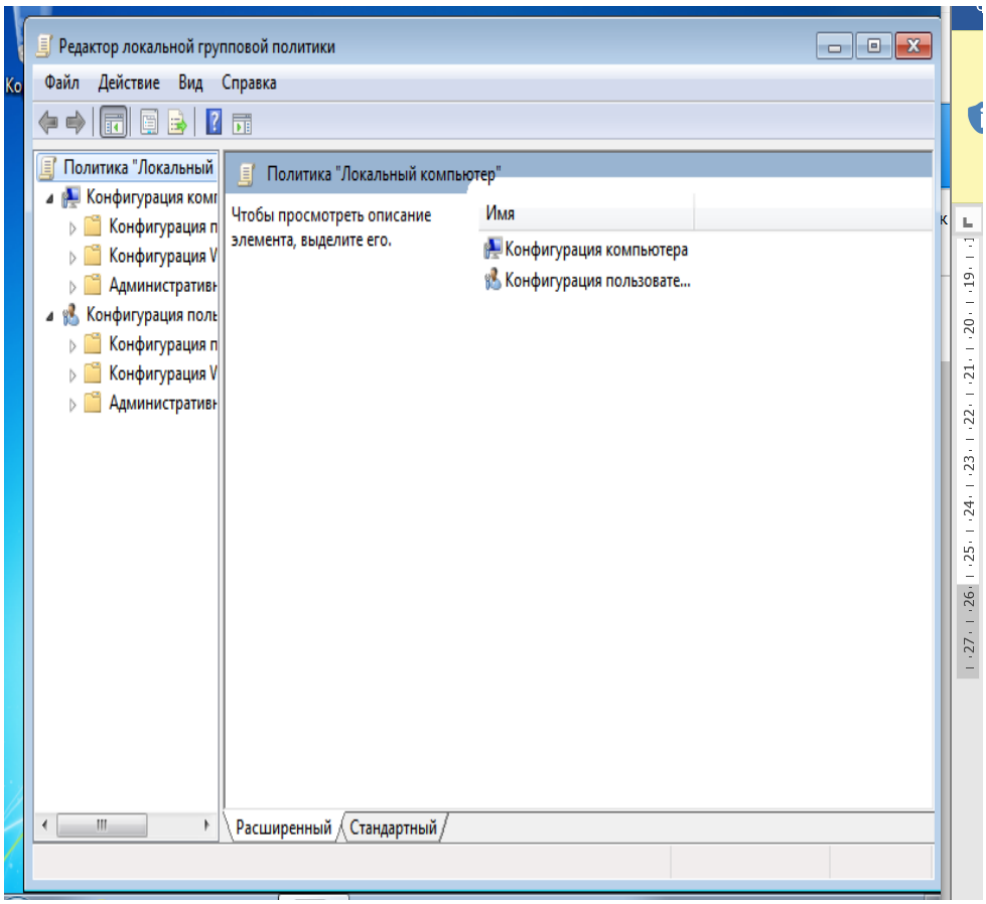


Рисунок 2 – Редактор локальной групповой политики

*Использование консоли управления оснастками MMC*

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

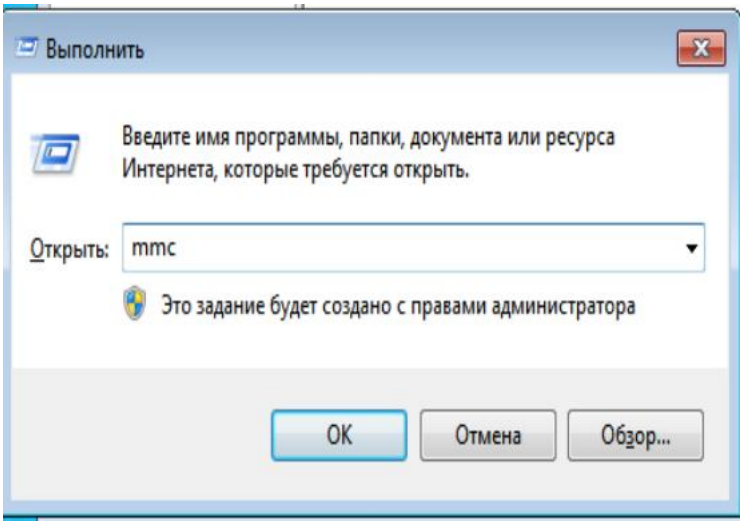


Рисунок 3 - Переход к консоли mmc

В меню «Консоль» выберите команду «Добавить или удалить оснастку» или воспользуйтесь комбинацией клавиш Ctrl+M. В диалоге «Добавление и удаление оснасток» выберите оснастку «Редактор объектов групповой политики» и нажмите на кнопку «Добавить». В появившемся диалоге «Выбор объекта групповой политики» нажмите на кнопку «Обзор» для выбора компьютера или нажмите на кнопку «Готово» (по умолчанию установлен объект «Локальный компьютер»). В диалоге «Добавление или удаление оснасток» нажмите на кнопку «ОК».

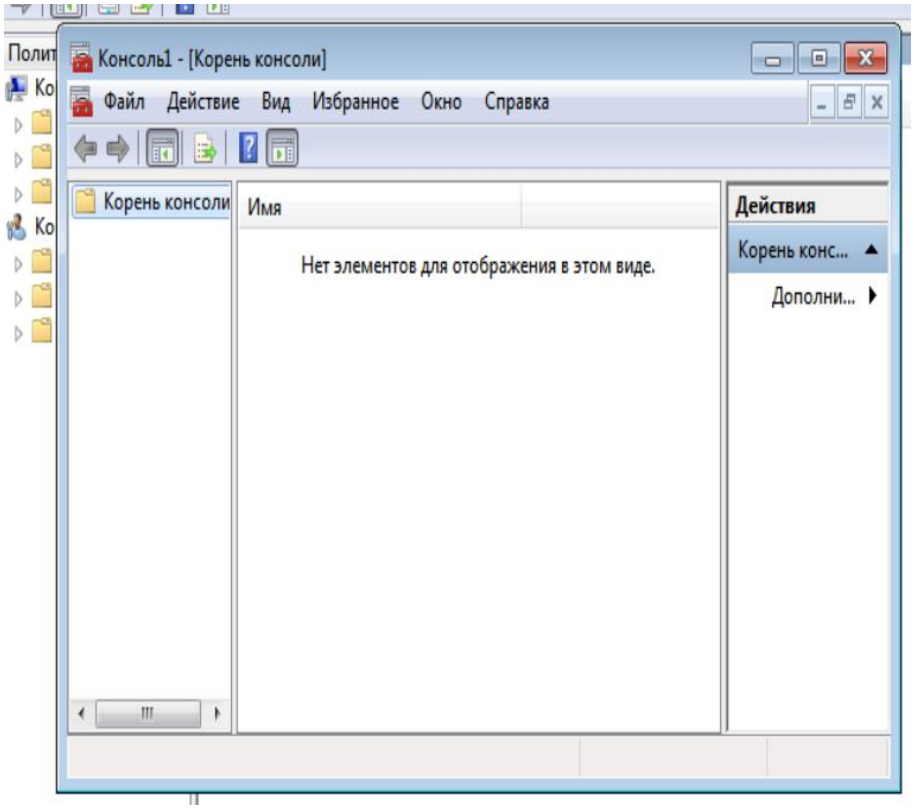


Рисунок 4 – Корень консоли

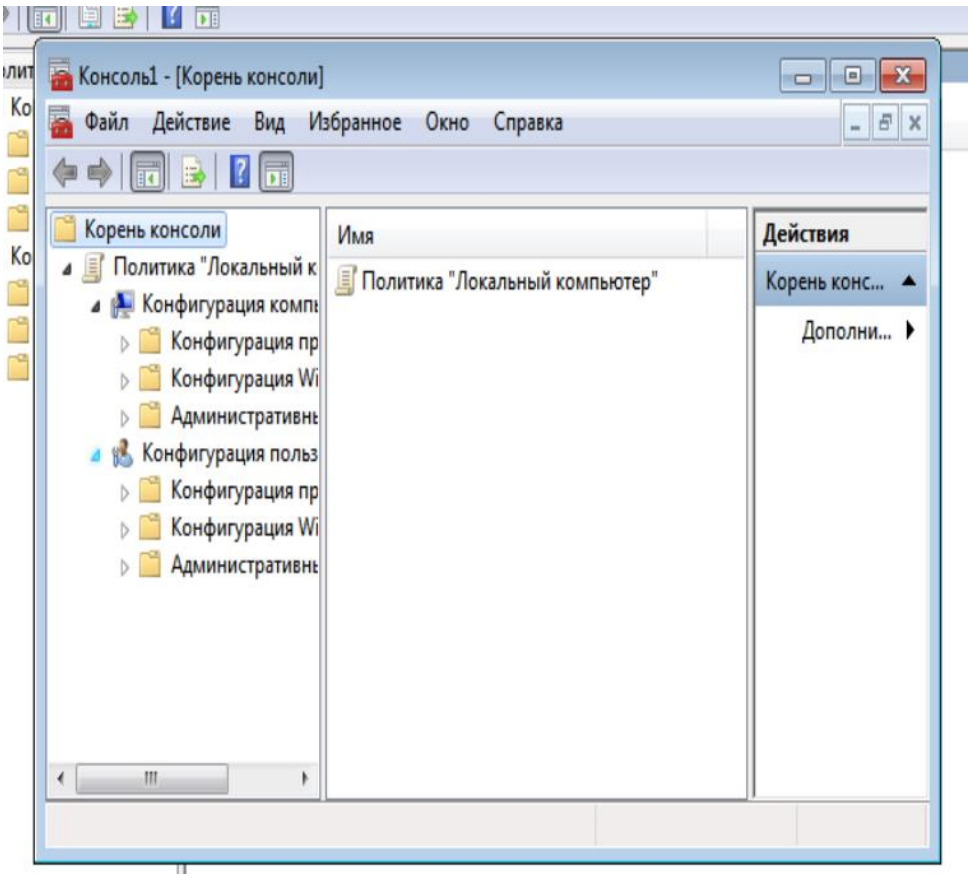


Рисунок 5 – Редактор локальной групповой политики, открытый с помощью использования консоли управления оснастками MMC

### *2.2. Узел «Конфигурация компьютера»*

Настройка дочернего узла «Конфигурация Windows» в «Конфигурации компьютера»

Открыть оснастку «Конфигурация Windows», перейдя по адресу: WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел «Конфигурация Windows».

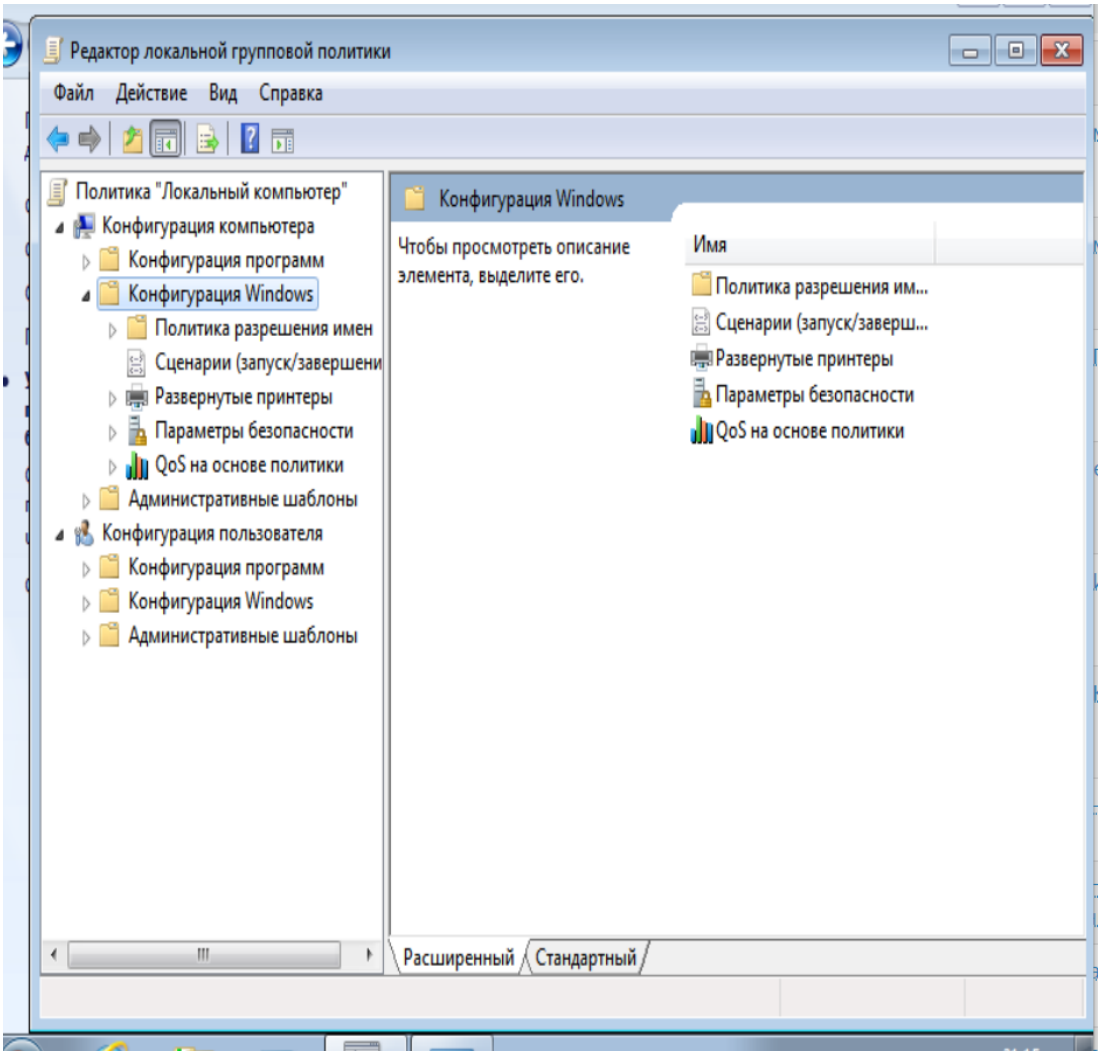


Рисунок 6 - Содержимое узла «Конфигурация Windows» до внесения изменений

Перейдем к настройке узла «Сценарии» в дочернем узле «Конфигурация Windows» приложения «Групповые политики». Для этого откроем оснастку «Сценарии», перейдя по адресу: *WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел «Конфигурация Windows» → узел «Сценарии».*

Групповые политики Windows позволяют запускать различные файлы скриптов при загрузке/ завершении работы компьютера, входе/выходе пользователя. С помощью «Групповых политик» можно исполнять на компьютерах домена не только классические файлы скриптов (.bat, .cmd, ,vbs), но скрипты PowerShell (.ps1).

Windows Powershell - оснастка командной строки и скриптовый язык для различной автоматизации задач и администрирования в Windows. Скрипты Windows направлены на автоматизацию рабочего процесса.

Поскольку АРМ расположено в «закрытом» контуре, напишем скрипт с названием «GetAllFiles.ps1» на языке PowerShell, который будет выводить на экран и в файл C:\CountFiles.csv информацию о том, сколько содержит файлов каждая папка и подпапки в директории C:\, а также размер этих папок и подпапок. CountFiles.csv файл можно импортировать в Microsoft Excel или в другое удобное приложения для работы с таблицами, и отсортировать столбцы файла по возрастанию или спаданию.

```
$source="C:"
Get-ChildItem $source -recurse -force | where {$_.psIscontainer} | foreach {
    $count = Get-ChildItem $_.fullname -recurse | where {$_.length} | Measure-Object -property length -Sum
    Write-Host($_.FullName)
    $FilesSize = '{0:F}' -f ((($count.Sum)/1024)/1024)
    Write-Host("Files: " + $count.count )
    Write-Host("Size: " + $FilesSize + " MB")
    '"' + $_.FullName + '",' + $count.count + '",' + $FilesSize + '"' | Out-File C:\CountFiles.csv -Append
}
```

Рисунок 7 – Содержимое скрипта «GetAllFiles.ps1»

Добавим скрипт «GetAllFiles.ps1» в сценарии автозагрузки.

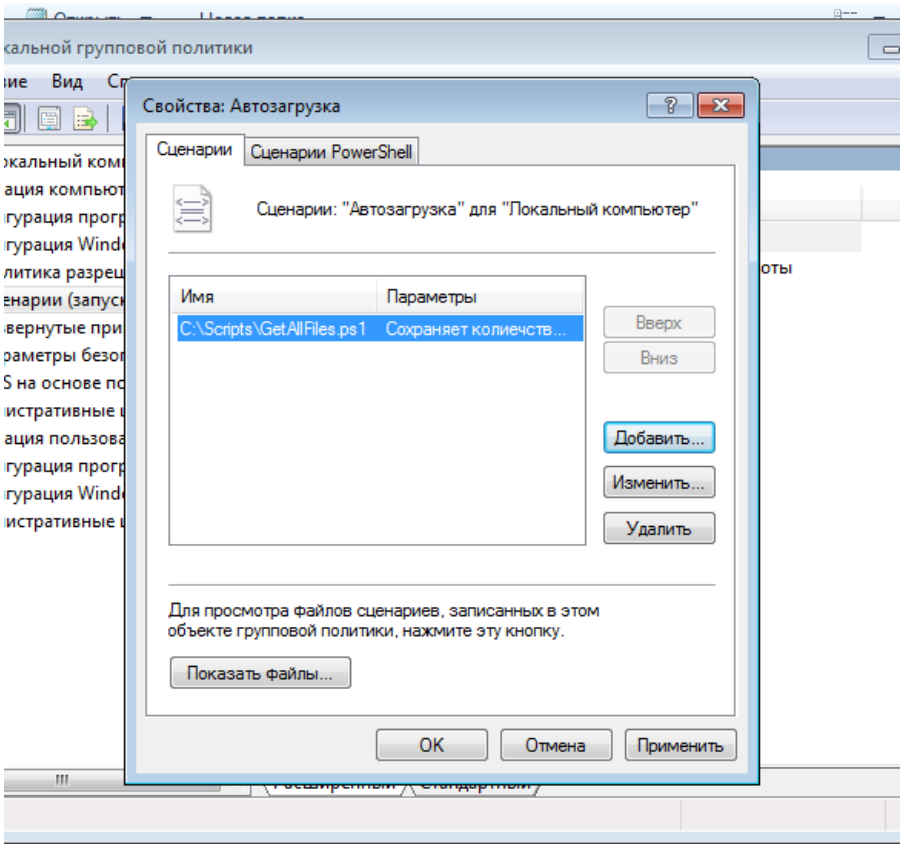


Рисунок 8 – Добавление скрипта в автозагрузку

«Сценарии» политики «Конфигурация Windows» успешно настроены.

Перейдем к настройке опций «Параметры безопасности» в дочернем узле «Конфигурация Windows» приложения «Групповые политики».

Дочерний узел «Конфигурация Windows» в основном предназначен для обеспечения безопасности компьютера и учетной записи, для которой применяются данные политики. В нем вы можете найти несколько опций безопасности, но особый интерес представляет опция «Параметры безопасности». Она позволяет настраивать политики безопасности средствами «Групповой политики». В этой опции для конфигурации безопасности компьютера доступны следующие настройки политик:

- Политики учетных записей, которые позволяют устанавливать политику паролей и блокировки учетных записей.
- Локальные политики (можно не настраивать см. здесь ЛАБ№1), отвечающие за политику аудита, параметры безопасности и назначения прав пользователя.
- Политики открытого ключа, которые позволяют:

- настраивать компьютеры на автоматическую отправку запросов в центр сертификации предприятия и установку выдаваемых сертификатов;
- создавать и распространять список доверия сертификатов (CTL);
- добавлять агенты восстановления шифрованных данных и изменение параметров политики восстановления шифрованных данных;
- добавлять агенты восстановления данных шифрования диска BitLocker.

• Политики ограниченного использования программ, позволяющие осуществлять идентификацию программ и управлять возможностью их выполнения на локальном компьютере, в подразделении, домене и узле.

• Политики управления приложениями, отвечающие за создание и управления правилами и свойствами функционала AppLocker, который позволяет управлять установкой приложений и сценариев.

• Политики IP-безопасности на «Локальный компьютер», которые позволяют создавать политику IP-безопасности локального компьютера и управлять списками IP-фильтров.

Напомним, что наше АРМ расположено в «закрытом» контуре ИС. Исходя из этого, настроим «Политики учетных записей».

Откроем оснастку «Политика паролей», перейдя по адресу: WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел «Конфигурация Windows» → узел «Параметры безопасности» → узел «Политики учетных записей» → узел «Политики паролей».

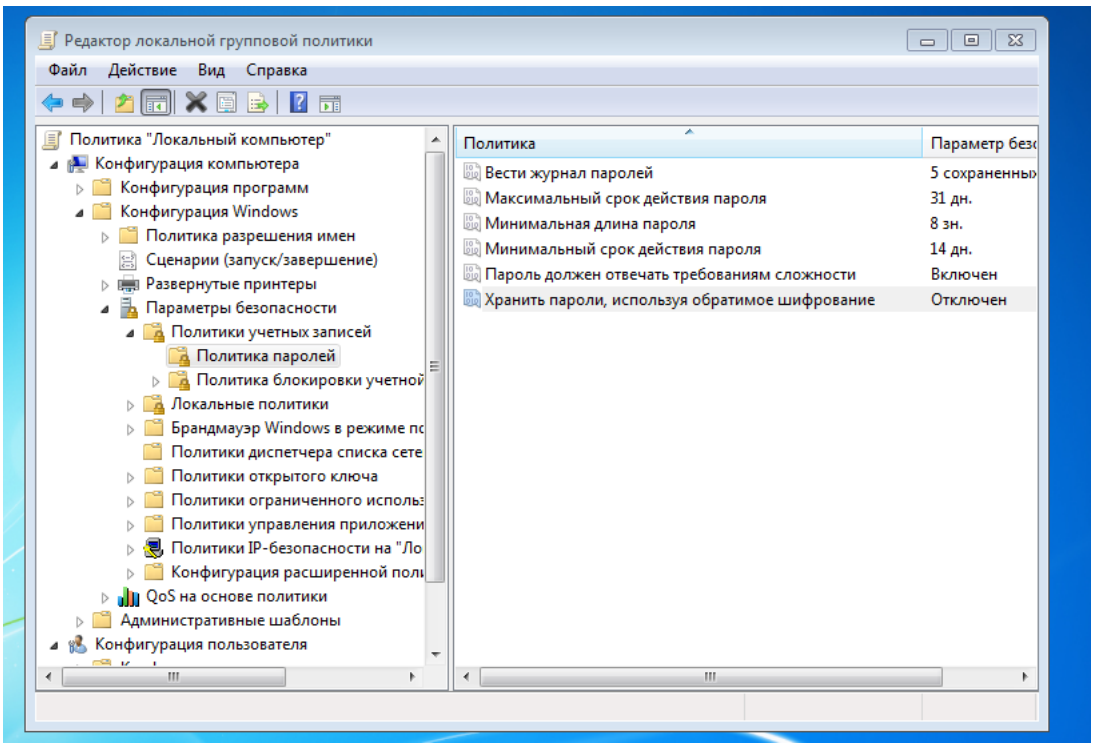


Рисунок 9 – Узел «Политика паролей»

«Политика учетных записей» аналогична локальным политикам безопасности. Поэтому используем ранее применяемые настройки для настройки политики «Политика паролей» из лабораторной работы №1.

Теперь настроим узел «Политика блокировки учетных записей».

Перейдем по адресу: WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел «Конфигурация Windows» → узел «Параметры безопасности» → узел «Политики учетных записей» → узел «Политика блокировки учетных записей».

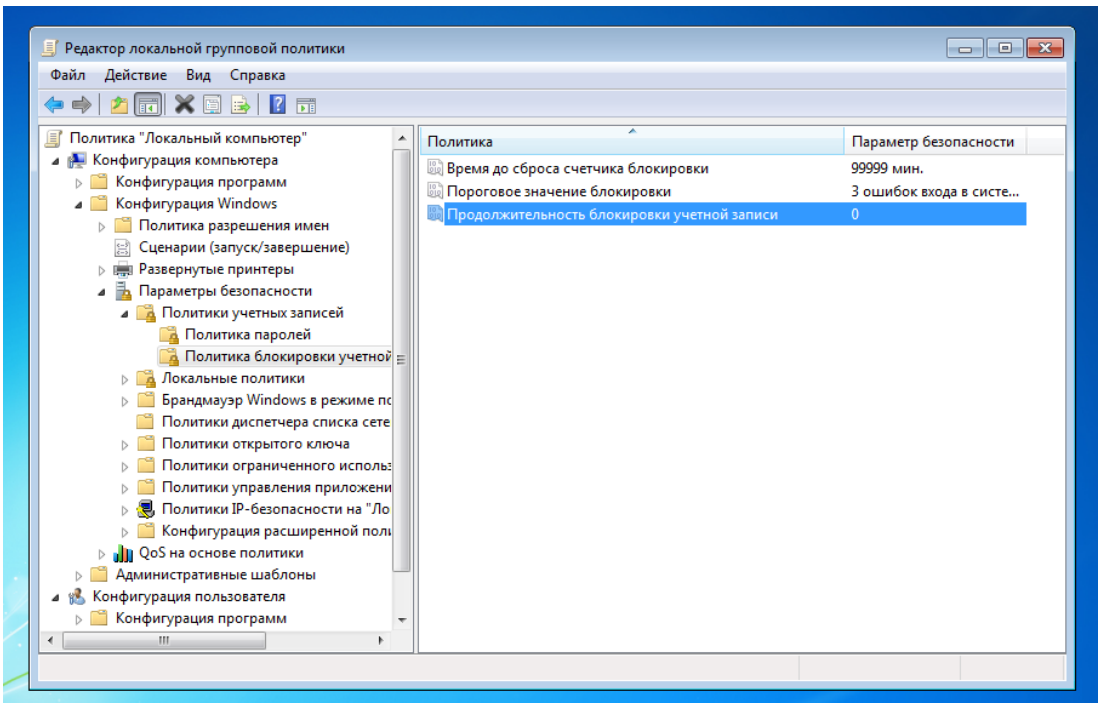


Рисунок 10 - Узел «Политика блокировки учетных записей»

Блокировка учетной записи.

Поскольку АРМ, которое рассматривается в данной лабораторной работе, расположено в «закрытом» контуре, то данный параметр разумно установить в значение 0: в этом случае учетная запись будет заблокирована до тех пор, пока администратор не разблокирует ее вручную. Эта мера предосторожности повысит защищенность АРМ: если будет превышено количество попыток входа (речь о которых идет далее), то этот случай уже вызывает подозрения – не действия ли это злоумышленника. Поэтому для сохранения безопасности АРМ учетная запись, для которой было превышено количество попыток входа, будет заблокирована до тех пор, пока с данной проблемой не разберется системный администратор.

Пороговое значение счетчика блокировки.

Поскольку АРМ расположено в «закрытом» контуре, установим значение данного параметра на 3 возможные попытки входа в учетную запись. Это рекомендуемое стандартное значение, и, с точки зрения безопасности, трех попыток хватит легальному пользователю, чтобы получить доступ к АРМ, а нелегальному – не хватит времени, чтобы подобрать правильный пароль до того, как учетная запись будет заблокирована.

Сброс счетчика блокировки через – 99999 минут.

Поскольку для рассматриваемого АРМ значение параметра «Продолжительность блокировки учетной записи» было выбрано 0, то есть учетная запись будет заблокирована до тех пор, пока ее не разблокирует системный администратор, для данного параметра можно выбрать любое значение. Автоматическая разблокировка учетной записи не произойдет в любом случае, однако для дополнительной защищенности АРМ установим значение параметра «Сброс счетчика блокировки» на максимальное значение 99999. Теперь в случае, если по какой-то причине предыдущая политика не вступит в силу, учетная запись все равно будет заблокирована на достаточно длительный срок, чтобы с причинами блокировки успел разобраться системный администратор и, при необходимости, предупредить действия злоумышленника.

Настроим «Локальные политики».

«Локальные политики», отвечающие за политику аудита, параметры безопасности и назначения прав пользователя, в соответствии с пояснениями к выполнению данной лабораторной работы настраиваются аналогично тому, как это было выполнено в «Лабораторной работе №1: Локальные политики безопасности АРМ».

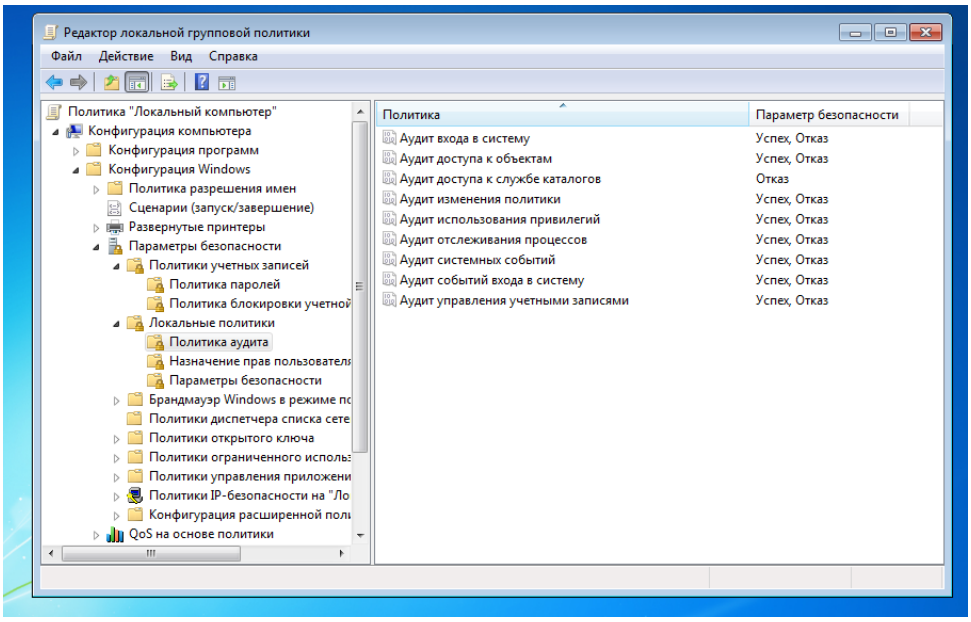


Рисунок 11 - «Локальные политики», отвечающие за политику аудита.

Откроем оснастку «Политики безопасности IP на «Локальный компьютер», перейдя по адресу: WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел «Конфигурация Windows» → узел «Параметры безопасности» → узел «Политики открытого ключа» → узел «Политики безопасности IP на «Локальный компьютер». Ниже можно увидеть содержимое политики после применения изменений.

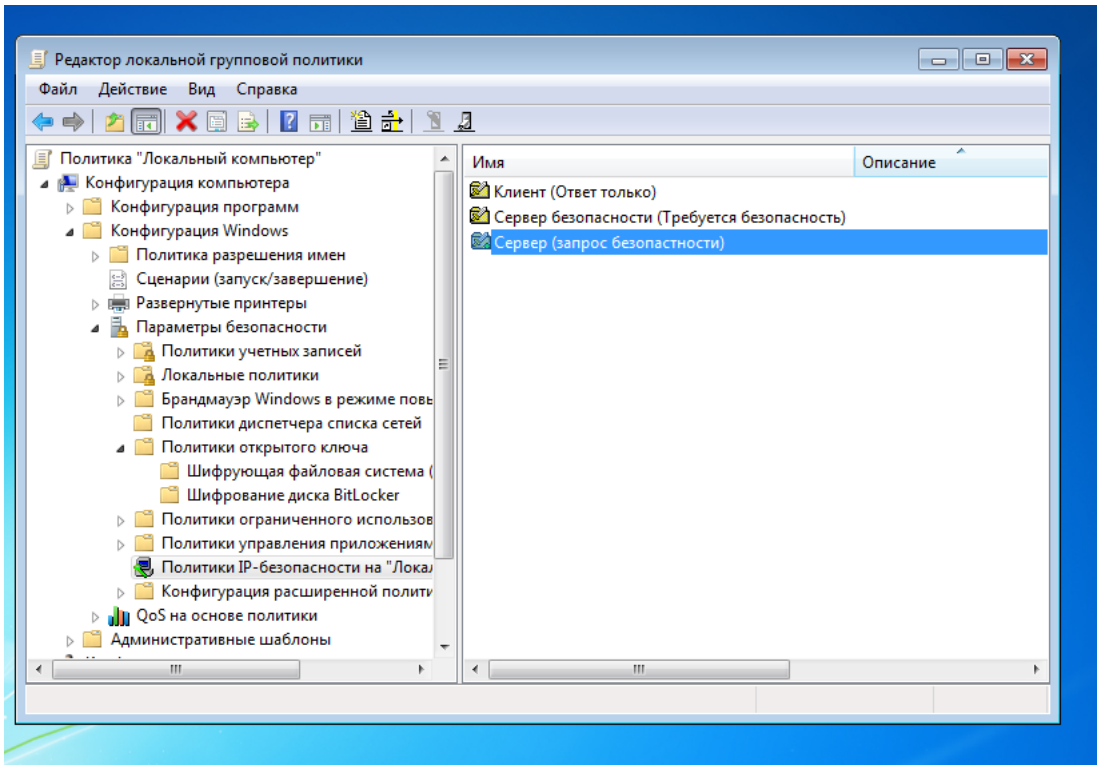


Рисунок 12 – Содержимое политики после применения изменений

Поясним смысл настройки каждого пункта:

- Клиент (Ответ только)

Поскольку АРМ расположено в «закрытом» контуре, то в целях повышения безопасности пользователям не следует выходить в сеть Internet. Поэтому в соответствии с этой политикой запрещаются все запросы пользователя и разрешено только отправлять ответы (серверам предприятия). Также в целях повышения безопасности используется протокол проверки подлинности Kerberos:

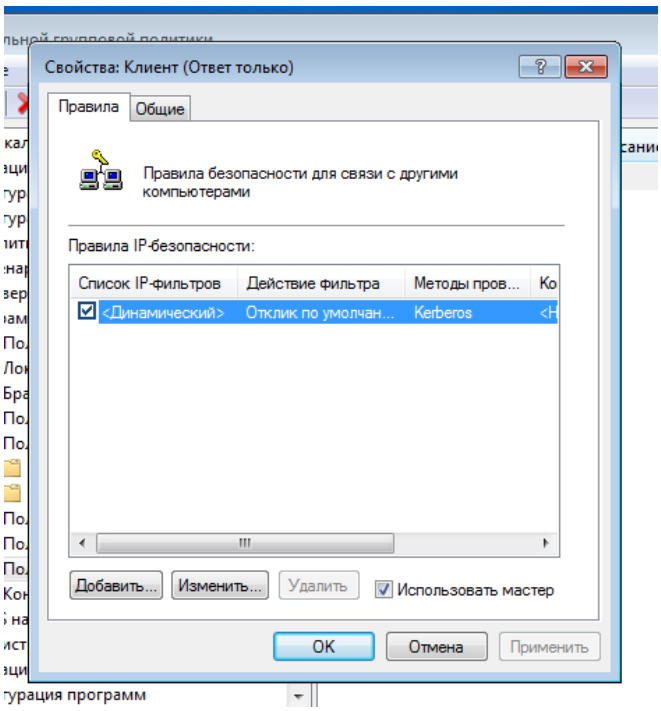


Рисунок 13 – Использование протокола Kerberos для проверки подлинности

- Сервер (запрос безопасности)

При обращении к серверу вначале передается запрос безопасности.

Также в целях повышения безопасности для всех видов трафика требуется использование проверки подлинности с помощью протокола Kerberos:

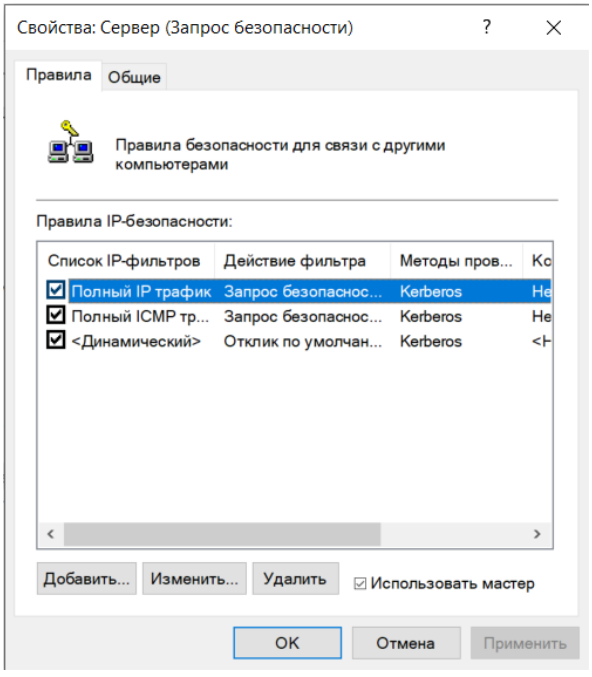


Рисунок 14 - Использование протокола Kerberos для проверки подлинности

Сервер безопасности (Требуется безопасность)

Настраивается аналогично с пунктом «Сервер», с учетом всех требований к безопасности.

«Политики безопасности IP на «Локальный компьютер» успешно настроена.

Настройка дочернего узла «Административные шаблоны» в «Конфигурации компьютера»

Перейдем к настройке узла «Административные шаблоны» в дочернем узле «Конфигурация Windows» приложения «Групповые политики».

Дочерний узел «Административные шаблоны» является крупнейшим из всех возможных расширений групповой политики и включает тысячи параметров для приложений и компонентов операционной системы Windows. Каждому параметру политики административных шаблонов соответствует определенный параметр системного реестра.

Политики в дочернем узле «Административные шаблоны» узла «Конфигурация компьютера» изменяют значения реестра в ключе HKEY_LOCAL_MACHINE (или просто HKLM). В рамках этой работы будет рассматриваться дочерний узел «Административные шаблоны» для локального компьютера.

Поскольку политика «Административные шаблоны» включает в себя тысячи приложений и компонентов для гибкой настройки групповой политики безопасности под самые разные цели, нет смысла перечислять настройку всех компонентов. Вспомним, что рассматриваемое АРМ представляет ценность для предприятия, и в целях безопасности пользователям запрещается выходить в сеть Internet, разрешается отвечать на запросы серверов, а каждую неделю системный администратор проверяет состояние АРМ. Исходя из того, что АРМ расположено в «закрытом» контуре, настроим важные для безопасной его работы компоненты:

1) Запрет удаленного управления рабочим столом

Откроем оснастку «Запретить удаленное управление рабочим столом», перейдя по адресу: *WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел «Административные шаблоны» → узел «Компоненты Windows» → узел «NetMeeting» → узел «Запретить удаленное управление рабочим столом»*.

Поскольку предполагается, что рассматриваемая АРМ находится в защищенном контуре, то к ней могут подключаться только системный администратор и пользователь АРМ. Поэтому важно обязательно включить запрет на удаленное управление рабочим столом.

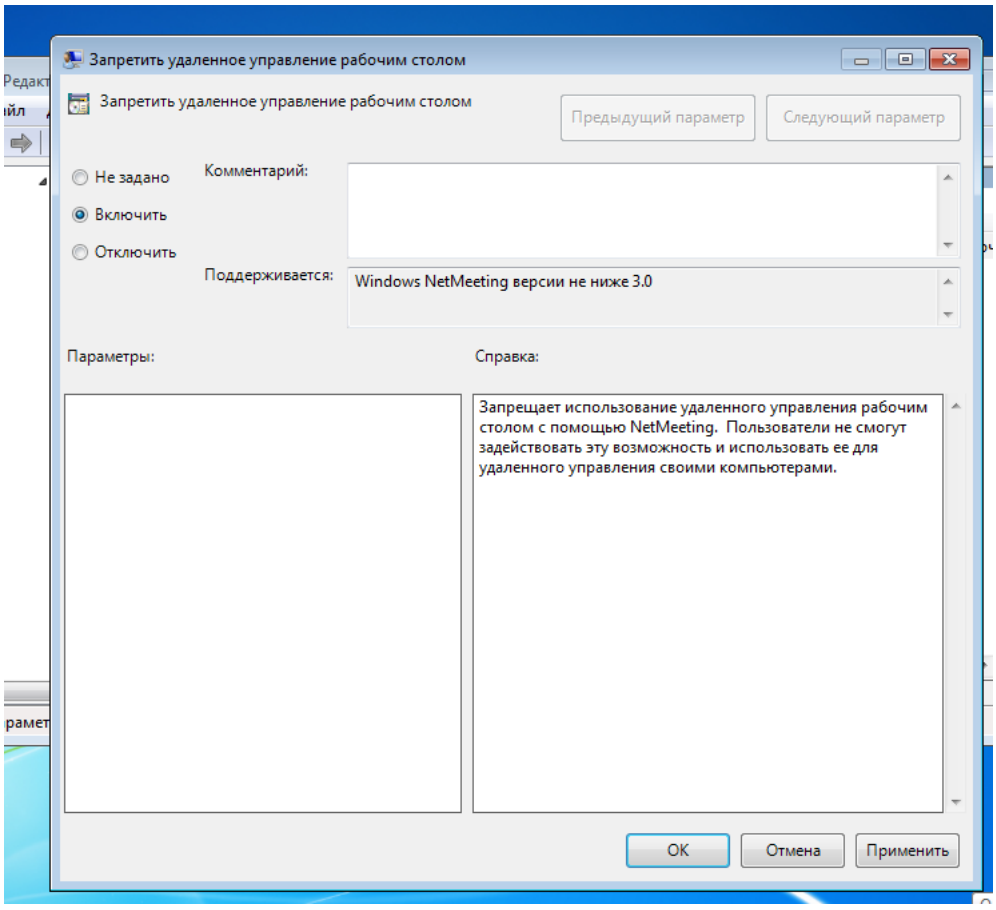


Рисунок 15 - Запрет на удаленное управление рабочим столом

Этот же параметр регулируется из оснастки «Разрешать удаленное подключение с использованием службы терминалов», расположенной по адресу: WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел «Административные шаблоны» → узел «Компоненты Windows» → узел «Службы удаленных рабочих столов» → узел

«Сеансов удаленных рабочих столов» → узел «Подключения» → узел «Разрешать удаленное подключение с использованием служб удаленных рабочих столов». Запретим удаленное подключение, т.е. отключим разрешение на подключение.

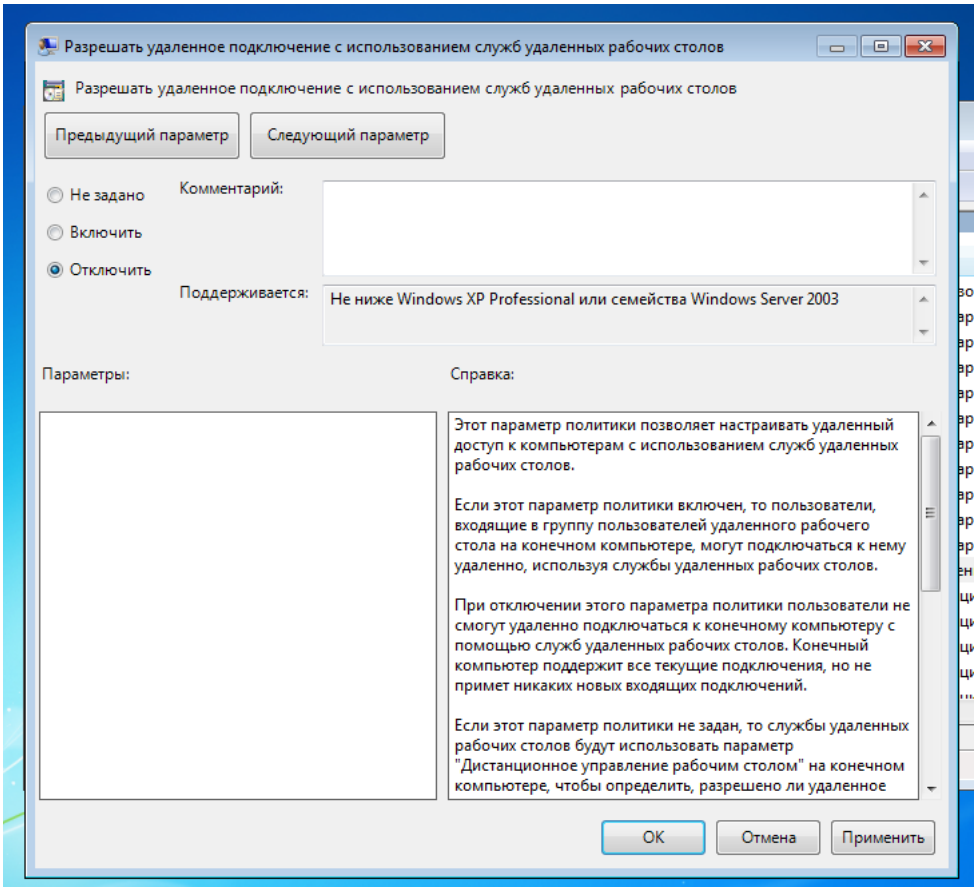


Рисунок 16 – Отключение разрешения на удаленное подключение

2) Выключить журнал событий справки приложения

Откроем оснастку «Выключить журнал событий справки приложения», перейдя по адресу: WIN+R →services.msc → «Журнал событий Windows».

Поскольку предполагается, что рассматриваемая АРМ не имеет доступа к интернету, то пользователь имеет возможность запускать только предустановленные программы и/или те, которые пользователь загружает непосредственно на АРМ с носителя. Последний случай представляет для системного администратора особый интерес: предполагается, что, в соответствии с политикой безопасности компании, личные носители информации, не прошедшие проверку, запрещены. Поэтому ведение журнала

запуска приложений позволит отследить, из какого источника был запущен процесс, и отследить нарушителей

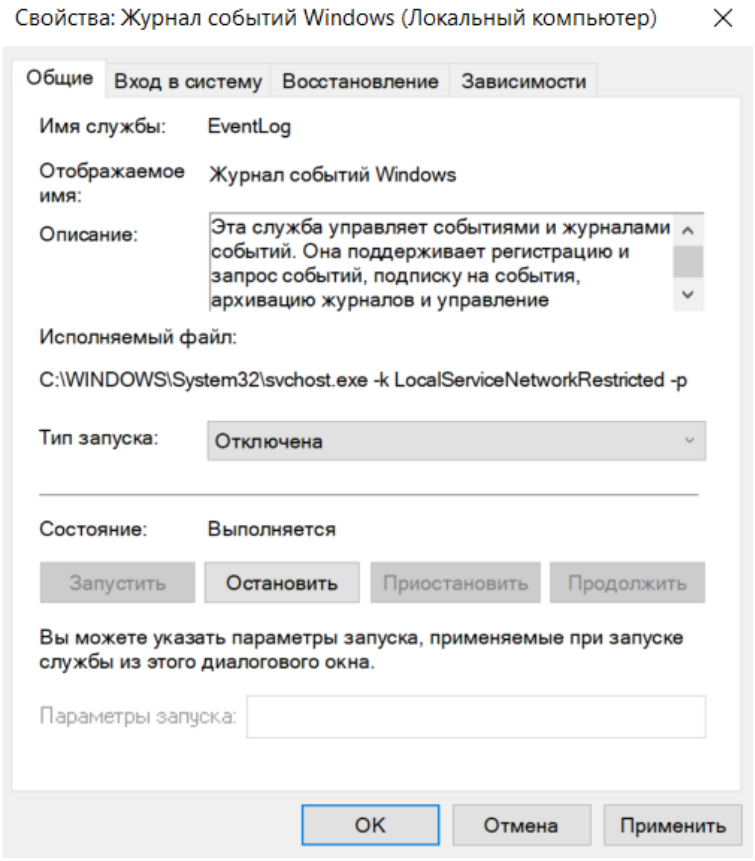


Рисунок 17 – Отключение журнала событий

3) Предотвращение доступа к 16-разрядным приложениям

Откроем оснастку «Предотвращение доступа к 16-разрядным приложениям», перейдя по адресу: WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел «Административные шаблоны» → узел «Компоненты Windows» → узел «Совместимость приложений» → узел «Предотвращение доступа к 16-разрядным приложениям».

Современные операционные системы семейства Windows являются 32-х битными и 64-х битными. Рассматриваемая АРМ имеет операционную систему Windows XP 32 бита, поэтому, с точки зрения логики, нет смысла разрешать запуск приложений меньшей разрядности: это может вызвать проблемы совместимости.

Кроме того, 16-ти битные приложения не безопасны, и, если вдруг пользователь запустит подобное приложение, злоумышленник теоретически может попытаться получить доступ к операционной системе жертвы через это уязвимое небезопасное приложение. Несмотря на то, что в нашем случае на АРМ недопустимо устанавливать и запускать сторонние приложения, следует предотвратить вероятность такой уязвимости.

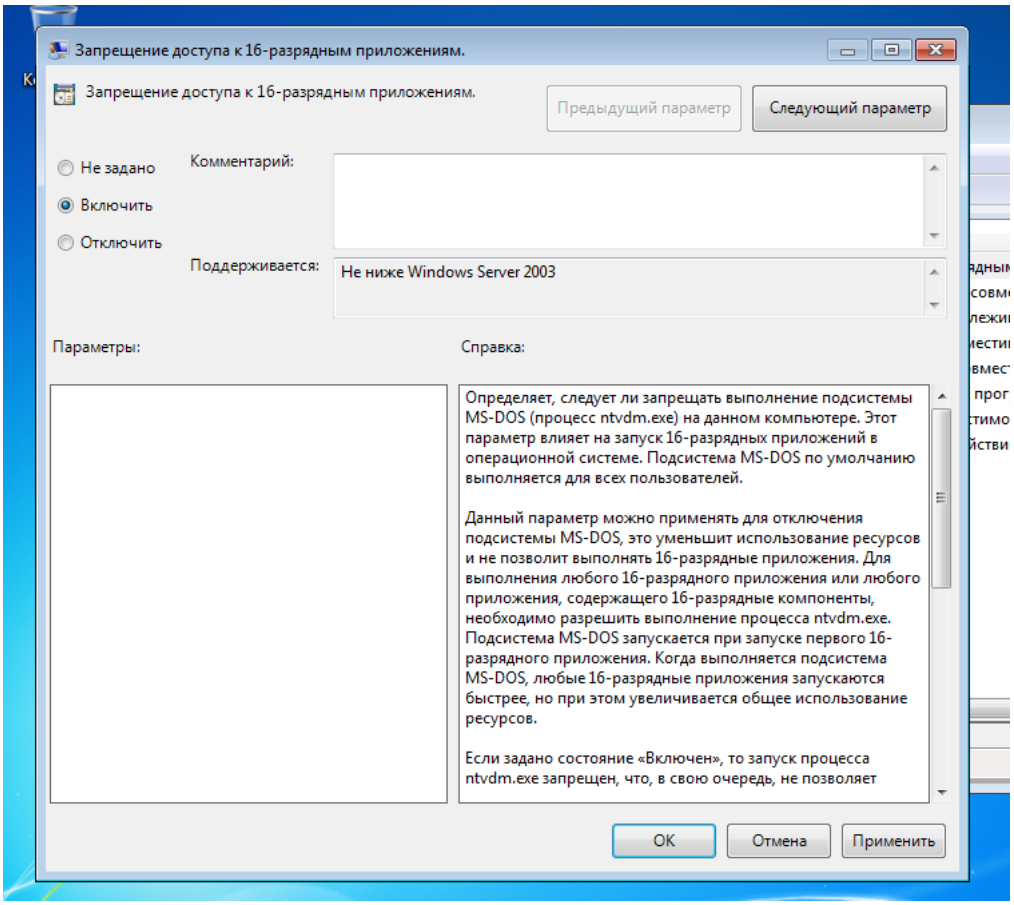


Рисунок 18 -Предотвращение доступа к 16-разрядным приложениям

4) Включение «Центра обеспечения безопасности»

Откроем оснастку «Включить центр обеспечения безопасности», перейдя по адресу: WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел «Административные шаблоны» → узел «Компоненты Windows» → узел «Центр обеспечения безопасности» → параметр «Включить центр обеспечения безопасности».

При подключении АРМ к серверу необходимо использовать все доступные механизмы обеспечения безопасности. В частности – «Центр обеспечения безопасности»

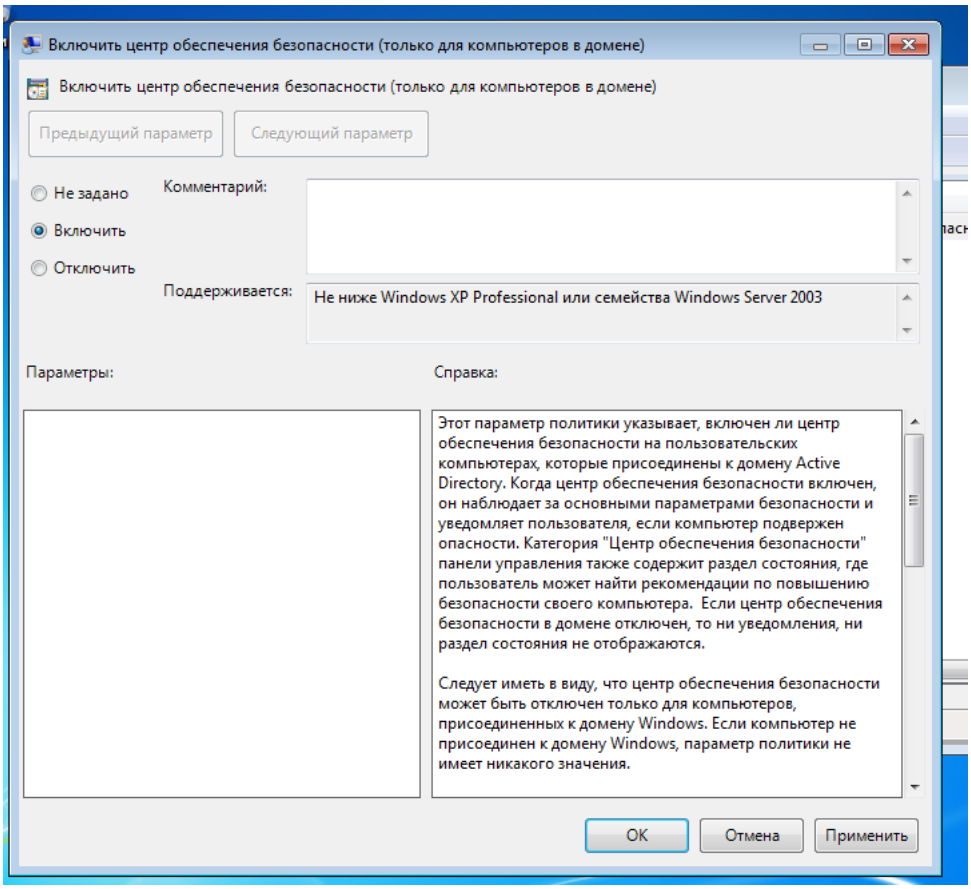


Рисунок 19 – Включение «Центра обеспечения безопасности»

5) Запрет удаления заданий

Откроем оснастку «Запретить удаление заданий», перейдя по адресу: WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел «Административные шаблоны» → узел «Компоненты Windows» → узел «Планировщик заданий» → параметр «Запретить удаление заданий».

Поскольку АРМ представляет ценность, для обеспечения ее безопасности системный администратор может устанавливать определенные задания: например, сбор статистики использования программ, журналирование событий и т.д. Эти задачи являются компонентом комплекса по обеспечению безопасности АРМ, и нельзя допустить, чтобы пользователь

мог их изменять. Поэтому требуется установить запрет на удаление уже установленных для АРМ заданий

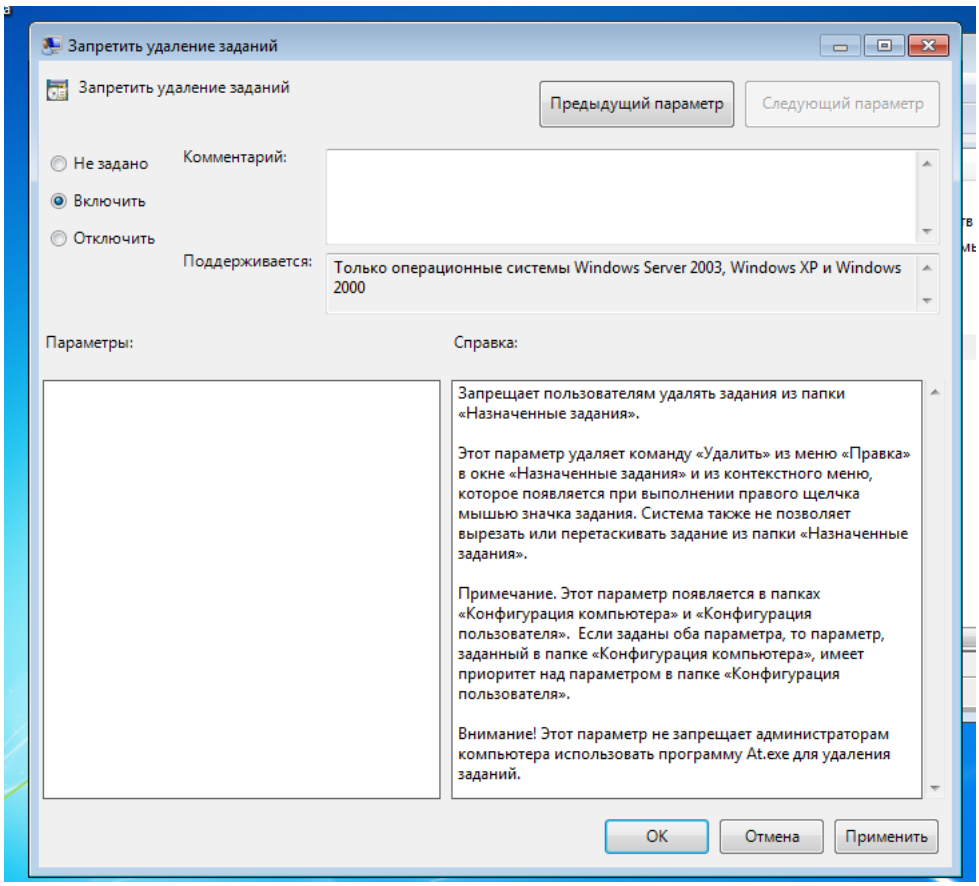


Рисунок 20 -Запрет удаления заданий

6) Удаление элемента «Безопасность Windows» из меню «Пуск»

Откроем оснастку «Удалить элемент «Безопасность Windows» из меню «Пуск», перейдя по адресу: WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел «Административные шаблоны» → «Компоненты Windows» → узел «Службы удаленных рабочих столов» → узел «Сеансов удаленных рабочих столов» → узел «Среда удаленных сеансов» → параметр «Удалить элемент «Безопасность Windows» из меню «Пуск».

Рассматриваемая АРМ представляет ценность для предприятия, поэтому разумно будет убрать компонент «Безопасность Windows» из меню «Пуск», чтобы пользователь не имел доступа к настройкам безопасности в принципе

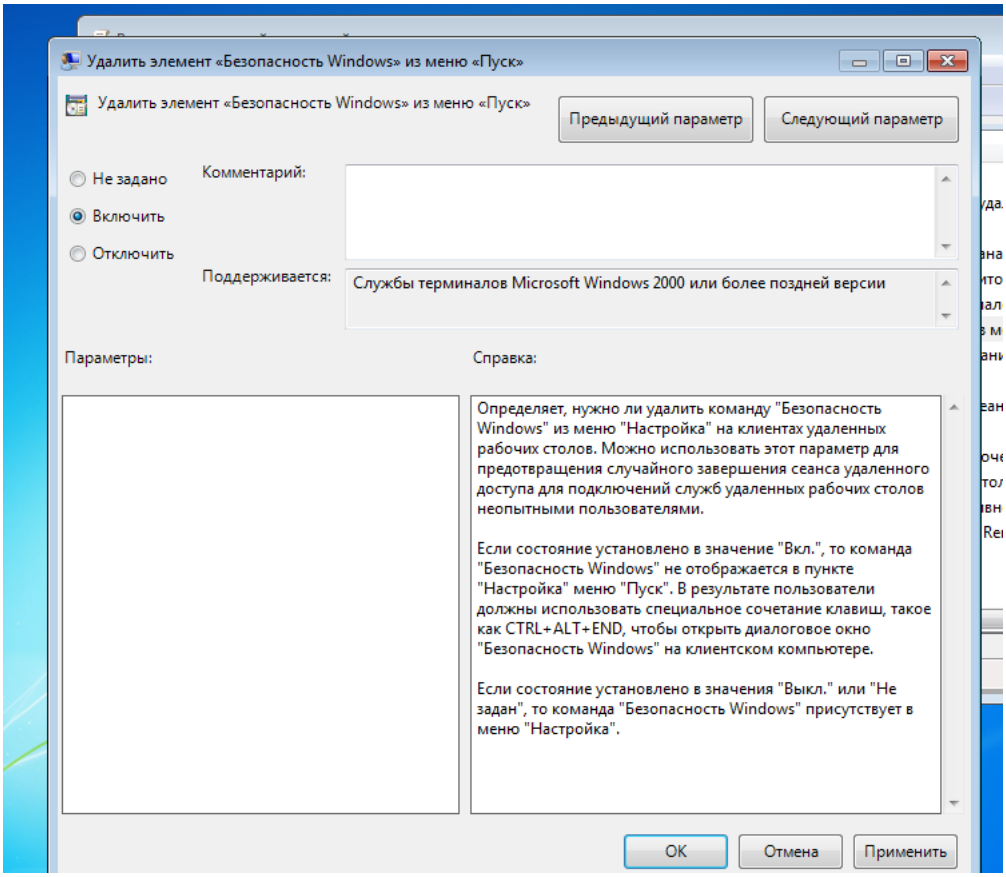


Рисунок 21 – Удаление элемента «Безопасность Windows» из меню «Пуск»

7) Включение защищенного режима протокола оболочки

Откроем оснастку «Отключить защищенный режим протокола оболочки», перейдя по адресу: WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел «Административные шаблоны» → «Компоненты Windows» → узел «Проводник» → параметр «Отключить защищенный режим протокола оболочки».

Данный параметр регулирует возможность доступа к папкам и файлам, если используется защищенный режим, то приложения не могут запускать файлы, находящиеся под защитой. Для блокировки доступа пользователя к файлам и папкам, изменение которых может повредить работоспособности ОС и безопасности АРМ в частности, следует отключить этот параметр политики: в таком случае протокол оболочки используется в защищенном режиме, позволяя приложениям открывать только разрешенные папки

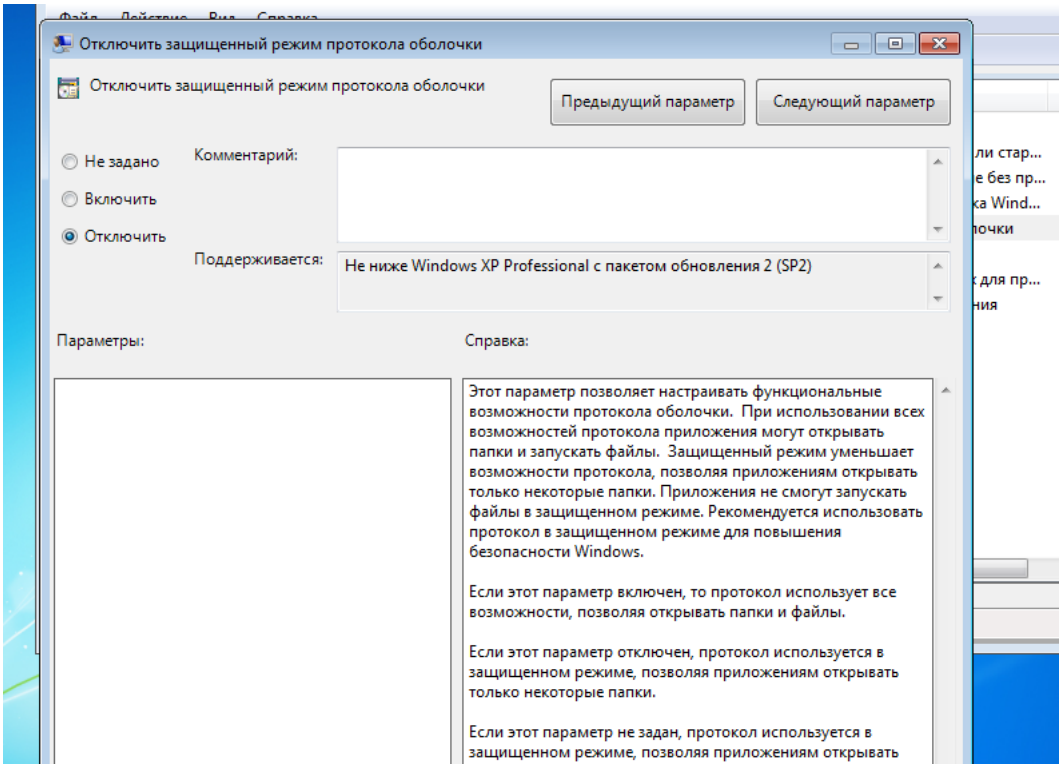


Рисунок 22 – Включение защищённого режима протокола оболочки

8) Ведение журнала запуска и установки приложений

Откроем оснастку «Ведение журнала», перейдя по адресу: WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел «Административные шаблоны» → «Компоненты Windows» → узел «Ведение журнала событий» → параметр «».

АРМ представляет ценность для предприятия, поэтому следует вести журнал всех процессов, генерируемых приложениями. Это позволит отследить, с чем и когда работает пользователь АРМ, а также определить, пытается ли он нарушить политику безопасности предприятия, устанавливая и запуская те приложения, которые не были предустановленны на его АРМ. Следовательно, необходимо включить «Ведение журнала», а в параметрах записи указать все события (ошибки, состояние, действия и т.д.) – если системный администратор будет располагать всеми сведениями о происходящем на АРМ, ему будет проще регулировать события

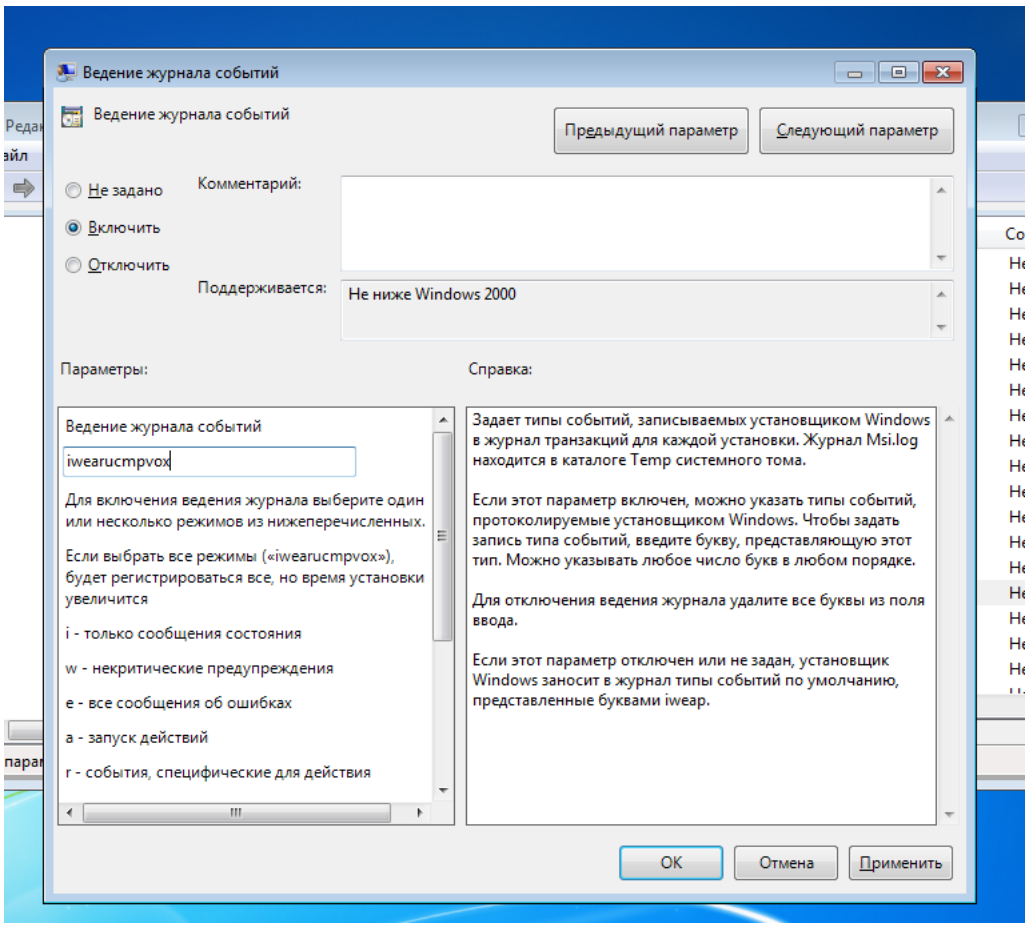


Рисунок 23 -Ведение журнала запуска и установки приложений

9) Настройка автоматического обновления системы

Откроем оснастку «Настройка автоматического обновления», перейдя по адресу: WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел «Административные шаблоны» → «Компоненты Windows» → узел «Центр обновления Windows» → параметр «Настройка автоматического обновления».

Обновление системы важно: зачастую именно они повышают безопасность ОС, исправляя багги и ошибки, сделанные разработчиками ОС, и не применение обновлений, по сути, оставляет открытой уязвимость, которую пытаются исправить. Следовательно, этой уязвимостью может воспользоваться злоумышленник – значит, нужно своевременно обновлять ОС.

Однако обновление ОС занимает время и ресурсы АРМ, во время обновления невозможно пользоваться АРМ – а значит, происходит потеря

человекочасов и средств, которые можно было заработать за вынужденное время простоя. Поэтом необходимо настроить автоматическое обновление системы.

Предположим, что у пользователя, рассматриваемого АРМ 5-дневный 8-ми часовой рабочий день с 9:00 до 17:00, а пятница – сокращенный день, с 9:00 до 16:30. Значит, можно выбрать пятницу днем, когда разрешено автоматическое обновление системы: в 17:00 АРМ уже не будет нужно пользователю, т.е. все его ресурсы можно отдать обновлениям. В соответствии с этим настроим политику.

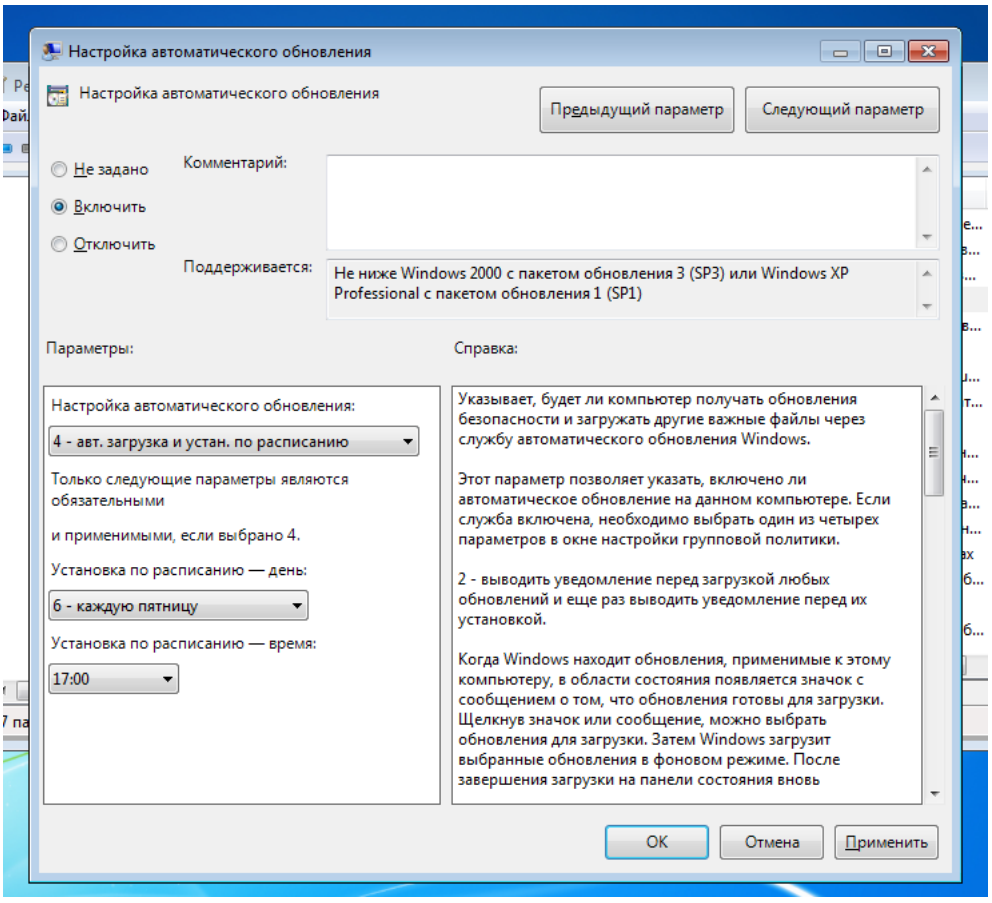


Рисунок 24 – Настройка автоматического обновления

«Административные шаблоны» оснастки «Конфигурация компьютера» успешно настроены.

На этом настройка узла «Конфигурация компьютера» закончена.

Вывод по пункту: в данной части лабораторной работе были настроены политики, относящиеся к узлу «Конфигурация компьютера»,

предназначенному для настройки параметров компьютера. В этом узле расположены параметры, которые применяются к компьютеру, невзирая на то, под какой учетной записью пользователь вошел в систему.

Дочерний узел «Конфигурация программ» позволяет указать определенную процедуру установки программного обеспечения.

Дочерний узел «Конфигурация Windows» в основном предназначен для обеспечения безопасности компьютера и учетной записи, для которой применяются данные политики.

Дочерний узел «Административные шаблоны» является крупнейшим из всех возможных расширений групповой политики и включает тысячи параметров для приложений и компонентов операционной системы Windows.

В частности, в процессе выполнения данного задания были настроены:

- Конфигурация Windows, включая сценарии для автозагрузки и выключения АРМ и параметры безопасности Windows (политика паролей и блокировки учетных записей)
- Локальные политики и политики безопасности IP на «Локальный компьютер
- Административные шаблоны, включающие в себя компоненты для безопасной работы Windows

Настройка каждого параметра политик и журналов была обоснована.

### 2.3. Настройка дочерних узлов «Конфигурации пользователя»

Для выполнения данного пункта задания требуется настроить опции и политики безопасности дочерних узлов «Конфигурация Windows» и «Административные шаблоны» для узла «Конфигурация компьютера».

Политика паролей зависит от того, для каких целей предполагается использовать АРМ: она будет серьезнее или слабее. Предположим, что АРМ, о котором речь пойдет далее, находится в закрытом контуре некоторого предприятия, и на нем происходит обработка каких-то данных, касающихся работы предприятия и собранных в открытом контуре. Раз в неделю системный администратор проверяет данное АРМ, просматривает журналы и

логии работы пользователя за прошедшую неделю и, при необходимости, вносит корректировки.

Предполагается, что у пользователя, рассматриваемого АРМ 5-дневный 8-ми часовой рабочий день с 9:00 до 17:00, а пятница – сокращенный день, с 9:00 до 16:30. В конце каждого месяца все сотрудники составляют отчеты о проделанной работе.

АРМ имеет в домене IP-адрес 172.168.13.16, сервер, с которым связан АРМ – 172.168.13.1.

Настройка дочернего узла «Конфигурация Windows» в «Конфигурации пользователя»

Откроем оснастку «Конфигурация Windows», перейдя по адресу: WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация пользователя» → узел «Конфигурация Windows». Ниже можно увидеть содержимое узла «Конфигурация Windows» до внесения изменений

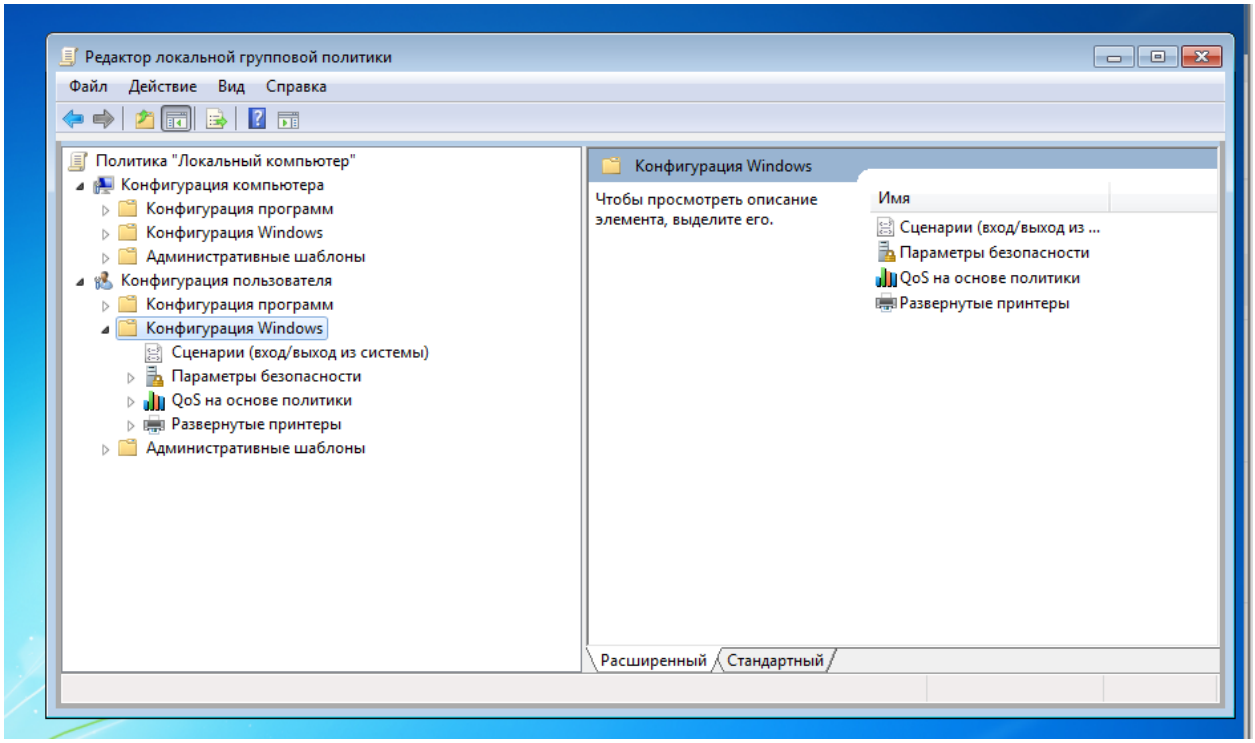


Рисунок 25 - Содержание узла «Конфигурация Windows» до внесения изменений

Перейдем к настройке узла «Сценарии» в дочернем узле «Конфигурация Windows» приложения «Групповые политики». Для этого откроем оснастку «Сценарии», перейдя по адресу: WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел «Конфигурация пользователя» → узел «Сценарии».

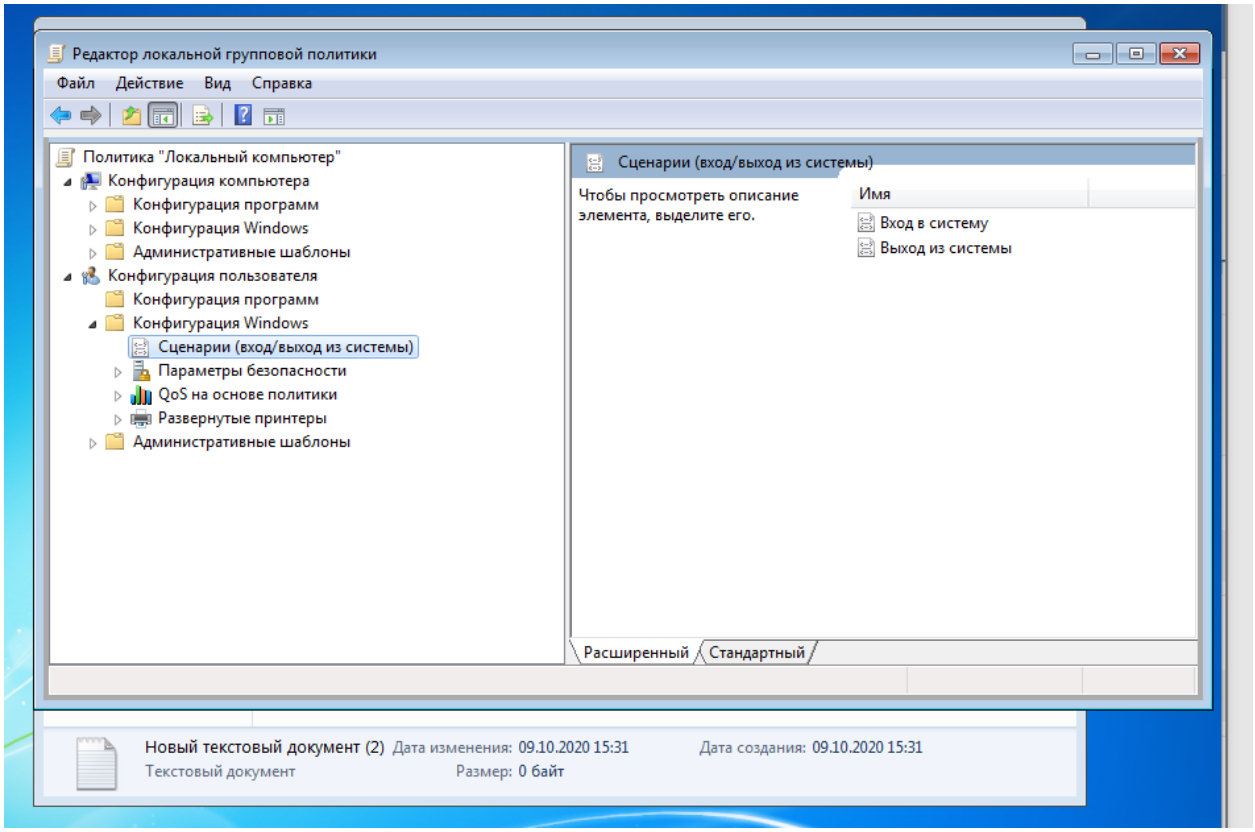


Рисунок 26 – Содержание узла «Сценарии»

Групповые политики Windows позволяют запускать различные файлы скриптов при загрузке/ завершении работы компьютера, входе/выходе пользователя. С помощью «Групповых политик» можно исполнять на компьютерах домена не только классические файлы скриптов (.bat, .cmd, ,vbs), но скрипты PowerShell (.ps1).

Windows Powershell - оснастка командной строки и скриптовый язык для различной автоматизации задач и администрирования в Windows. Скрипты Windows направлены на автоматизацию рабочего процесса.

Поскольку текущее АРМ представляет ценность для компании, напишем скрипт с названием «GetBackup.ps1» на языке PowerShell, который

будет делать бэкап системы при каждом выходе пользователя из системы. Ниже представлена часть содержимого скрипта, расположенного по адресу «C:\Scripts».

Предполагается, что упользователя рассматриваемого АРМ 5-дневный 8-ми часовой рабочий день с 9:00 до 17:00, а пятница – сокращенный день, с 9:00 до 16:30. Если PowerShell скрипт запущен в определенное время и определенный день, а именно: в понедельник, среду и пятницу, на 17 часов вечера, – то он начинает копировать файлы из указанных папок:

- \\172.168.13.16\Backups\Other, которая предположительно содержит информацию, которую пользователь считает важной для своей работы и желает сделать для нее резервную копию;
- \\172.168.13.16\Backups\WindowsImageBackup, которая предположительно содержит все резервные копии системы.

Здесь 172.168.13.16 – присвоенный данному компьютеру IP-адрес в домене. Копирование происходит на сервер, расположенный по адресу 172.168.13.1 в аналогичные папки. Ход процесса записывается в лог файл.

После окончания работы на e-mail системного администратора присылается письмо, в котором указано: свободное место на локальных дисках (до старта и после окончания), объем резервной копии, время старта и окончания, средняя скорость копирования. После этого компьютер выключается (для резервного копирования он автоматически включается в соответствии с настройками BIOS, поэтому его следует повторно выключить).

Этот скрипт будет запускаться при выходе пользователя из системы, а запуск раз в два дня позволит обезопасить пользователя от потери информации и вызванных этим простоев. Также письмо, генерируемое скриптом и отправляемое системному администратору, позволит последнему быть в курсе происходящего на АРМ.

Добавим скрипт «GetBackup.ps1» в сценарии событий выхода из системы

Рисунок 27 – Добавление скрипта к событиям выхода из системы

Теперь при каждом выходе пользователя из системы в понедельник, среду и пятницу в 17:00 часов вечера будет создаваться резервная копия всей важной информации.

Однако большое количество создаваемых каждую неделю копий (3 в неделю, 12 в месяц) может пагубно сказаться на памяти АРМ: в скрипте выделяет минимум 1 ГБ на создание копии, а в предприятии целесообразно экономить ресурсы. Поэтому напишем скрипт «KillOldBackups.ps1», который будет запускаться при каждом входе пользователя в систему в понедельник в 9:00 утра. Этот скрипт будет сканировать папку «C:\Backups», которая содержит резервные копии, создаваемые скриптом «GetBackup.ps1», и смотреть на дату находящихся там резервных копий и удалять все бэкапы старше месяца.

Предполагается, что в конце каждого месяца все сотрудники составляют отчеты о проделанной работе, поэтому все резервные копии, дата создания которых старше текущей более чем на 1 месяц, уже не актуальны. Ниже представлено содержимое скрипта, расположенного по адресу «C:\Scripts»

```
1  if ((($Day_of_week -eq 1)-and($StartTimeHour -eq 9))
2  $date = (Get-Date).AddMonths(-1)
3  Remove-Item "C:\Backups\*" -force -recurse
4  Get-ChildItem -Path C:\Backups\ | where {!$_.PSIsContainer} |
5  foreach {
6      if ($_.LastWriteTime -lt $date) { Remove-Item $_ -whatif }
7          }
8  }
```

Рисунок 31 - Содержимое скрипта, удаляющего старые резервные копии backup

Этот скрипт будет запускаться при входе пользователя в систему и регулировать количество занимаемой уже не нужными резервными копиями памяти АРМ.

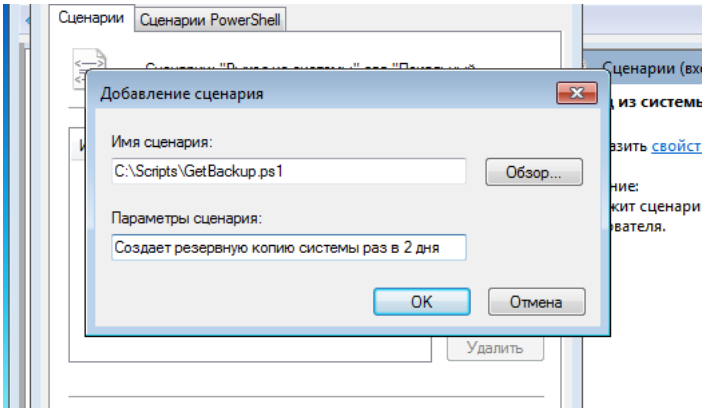


Рисунок 28 - Добавление скрипта к событиям выхода из системы

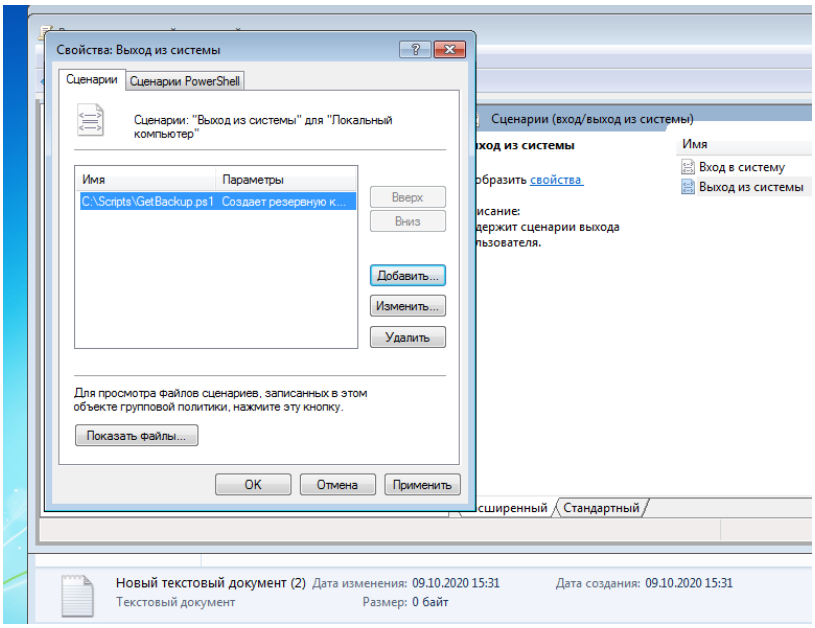


Рисунок 29 - Добавление скрипта к событиям выхода из системы

Добавим скрипт «KillOldBackups.ps1» в сценарии событий выхода из системы.

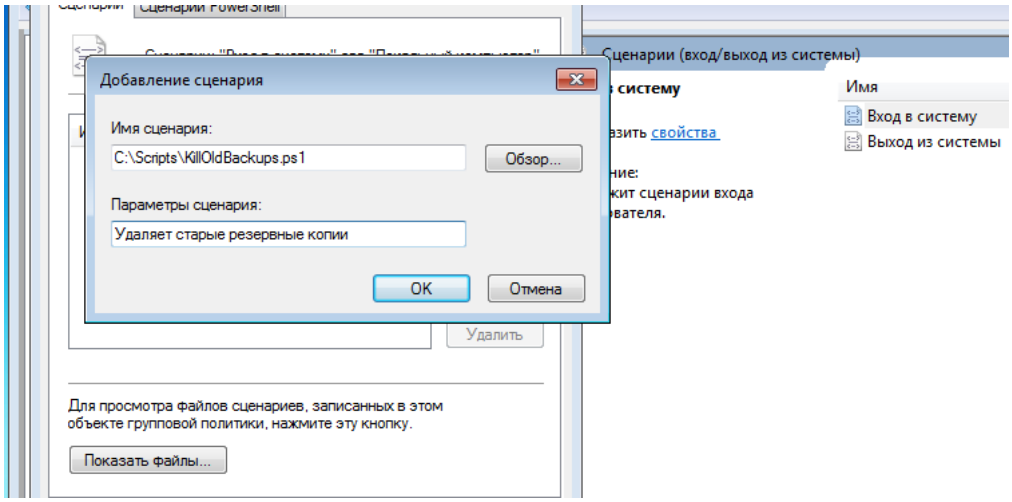


Рисунок 30 – Добавление скрипта к событиям выхода из системы

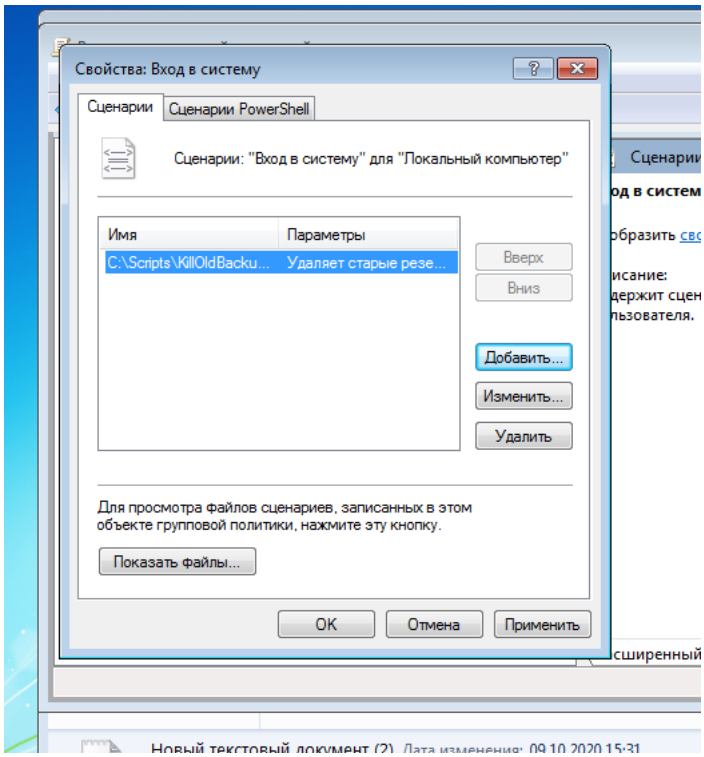


Рисунок 31 - Добавление скрипта к событиям выхода из системы

Таким образом, специально для целей, выполняемых АРМ и в соответствии с рабочим графиком пользователя, были написаны два скрипта, выполняющих резервное копирование системы и содержащейся на ней важной информации и регулирующие количество занимаемой этими скриптами памяти. «Сценарии» политики «Конфигурация пользователя» успешно настроены.

Перейдем к настройке узла «Настройки Internet Explorer» в дочернем узле «Конфигурация пользователя» приложения «Групповые политики».

Поскольку АРМ представляет ценность, то в интересах предприятия запретить пользователям доступ в интернет. Осуществим это с помощью «Групповой политики», настроив параметры используемого прокси-сервера.

Для этого откроем оснастку «Параметры прокси-сервера», перейдя по адресу: WIN+R → inetcpl.cpl → вкладка «Подключения» → «Настройка сети»

Для того, чтобы запретить пользователям доступ в интернет, достаточно указать в качестве обязательно используемого несуществующий IP-адрес прокси-сервера. Используем адрес «0.0.0.0», установим обязательным

использование данного прокси-сервера для всех адресов, по которым пытаются обратиться пользователи.

Но, поскольку АРМ все еще требуется связь с сервером, который располагается предположительно по адресу 172.168.13.1, разрешим соединения с ним, записав его адрес в графу исключений.

С учетом вышеописанных параметров, настройки данной политики выглядят следующим образом

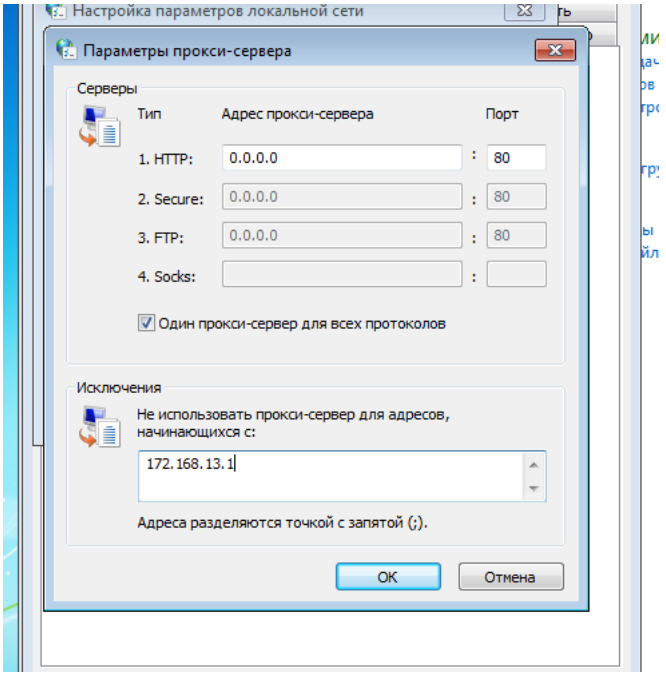


Рисунок 32 -Настройка прокси-сервера

«Настройки Internet Explorer» успешно настроена.

В качестве исключения указан адрес сервера, с которым связывается АРМ: это сделано для того, чтобы АРМ имел возможность отправлять резервные копии серверу.

Настройка дочернего узла «Административные шаблоны» в «Конфигурации пользователя»

Перейдем к настройке узла «Административные шаблоны» в дочернем узле «Конфигурация пользователя» приложения «Групповые политики».

Дочерний узел «Административные шаблоны» является крупнейшим из всех возможных расширений групповой политики и включает тысячи параметров для приложений и компонентов операционной системы Windows.

Каждому параметру политики административных шаблонов соответствует определенный параметр системного реестра.

Политики в дочернем узле «Административные шаблоны» узла «Конфигурация пользователя» изменяют значения реестра в ключе HKEY_CURRENT_USER (HKCU). Для пользователя «Административные шаблоны» представляют собой настройки, связанные с интерфейсом АРМ.

Поскольку политика «Административные шаблоны» включает в себя тысячи приложений и компонентов для гибкой настройки групповой политики безопасности под самые разные цели, нет смысла перечислять настройку всех компонентов. Следует определить, к каким компонентам пользователь АРМ, исходя из предназначения АРМ, может иметь доступ, а к каким – нет. Главным образом это касается доступа к настройкам АРМ, использование которых может нарушить работу АРМ (а, соответственно, и работу пользователя, что влечет за собой простой и финансовые убытки для предприятия).

1) Предотвращение доступа к 16-разрядным приложениям

Откроем оснастку «Предотвращение доступа к 16-разрядным приложениям», перейдя по адресу: WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация пользователя» → узел «Административные шаблоны» → узел «Компоненты Windows»→ узел «Совместимость приложений» → узел «Запрещение доступа к 16-разрядным приложениям».

Современные операционные системы семейства Windows являются 32-х битными и 64-х битными. Рассматриваемая АРМ имеет операционную систему Windows XP 32 бита, поэтому, с точки зрения логики, нет смысла разрешать запуск приложений меньшей разрядности: это может вызвать проблемы совместимости.

Кроме того, 16-ти битные приложения не безопасны, и, если вдруг пользователь запустит подобное приложение, злоумышленник теоретически может попытаться получить доступ к операционной системе жертвы через это уязвимое небезопасное приложение. Несмотря на то, что в нашем случае на

АРМ недопустимо устанавливать и запускать сторонние приложения, следует предотвратить вероятность такой уязвимости.

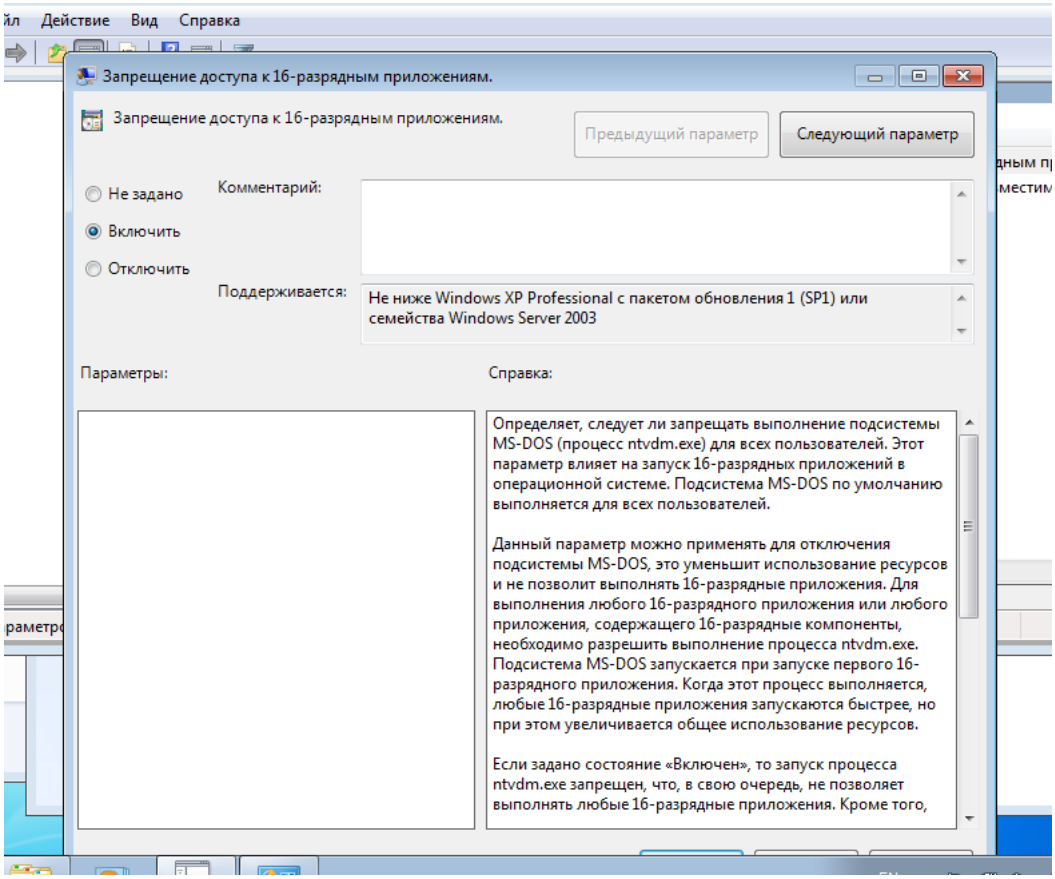


Рисунок 33 - Запрещение доступа к 16-разрядным приложениям

2) Удаление команды «Свойства папки» из меню «Сервис»

Откроем оснастку «Удалить команду «Свойства папки» из меню «Сервис», перейдя по адресу: WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация пользователя» → узел «Административные шаблоны» → узел «Компоненты Windows» → узел «Проводник» → узел «Удалить команду «Свойства папки» из меню «Сервис».

Следует запрещать пользователю доступ к команде «Свойства папки», поскольку, с ее использованием, можно настроить разрешение на отображение скрытых и системных файлов. Поскольку изменение системных файлов влечет ошибки в работе системы, их нельзя изменять обычным пользователям, не имеющим представления о том, как правильно настраивать систему. В целях безопасности уберем возможность обращения к свойствам папок

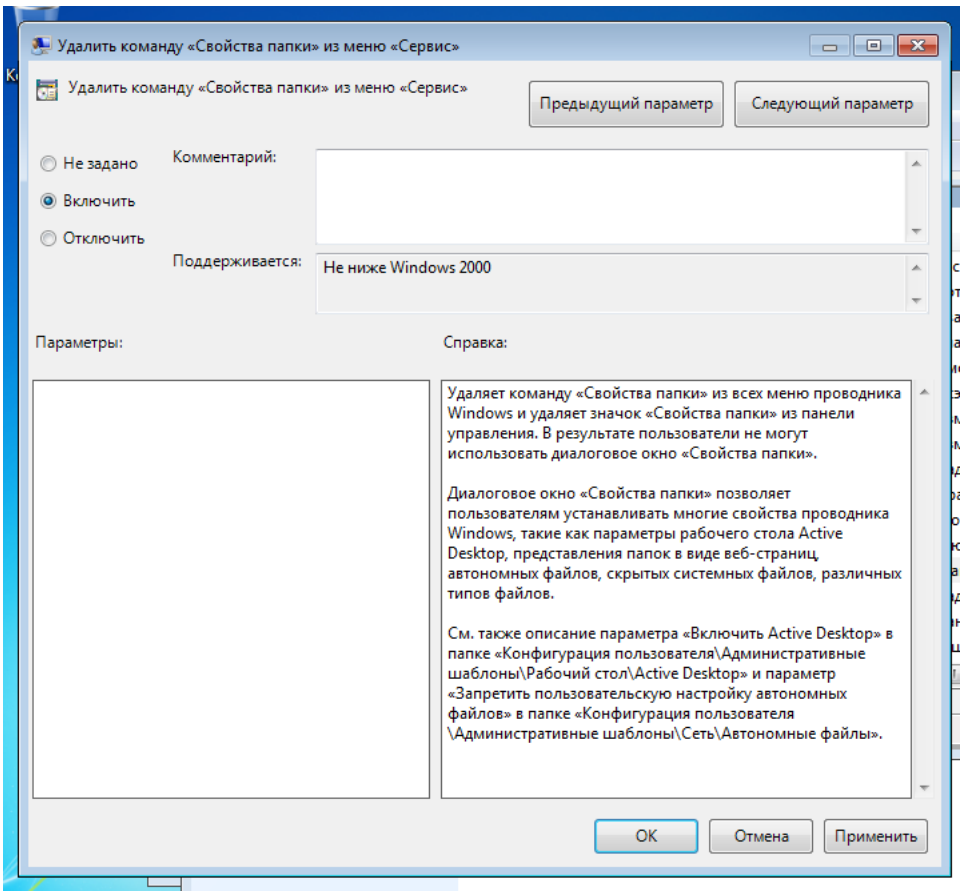


Рисунок 34 - Удалить команду «Свойства папки» из меню «Сервис»

3) Удаление вкладки «Безопасность»

Откроем оснастку «Удалить вкладку «Безопасность», перейдя по адресу: WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация пользователя» → узел «Административные шаблоны» → узел «Компоненты Windows» → узел «Проводник» → узел «Удалить вкладку «Безопасность».

Политика безопасности для пользователя и АРМ настраивается системным администратором, в целях сохранения безопасности на должном уровне, нельзя допускать возможность изменения каких-то настроек из системы самим пользователем. Во избежание такой возможности уберем вкладку «Безопасность»

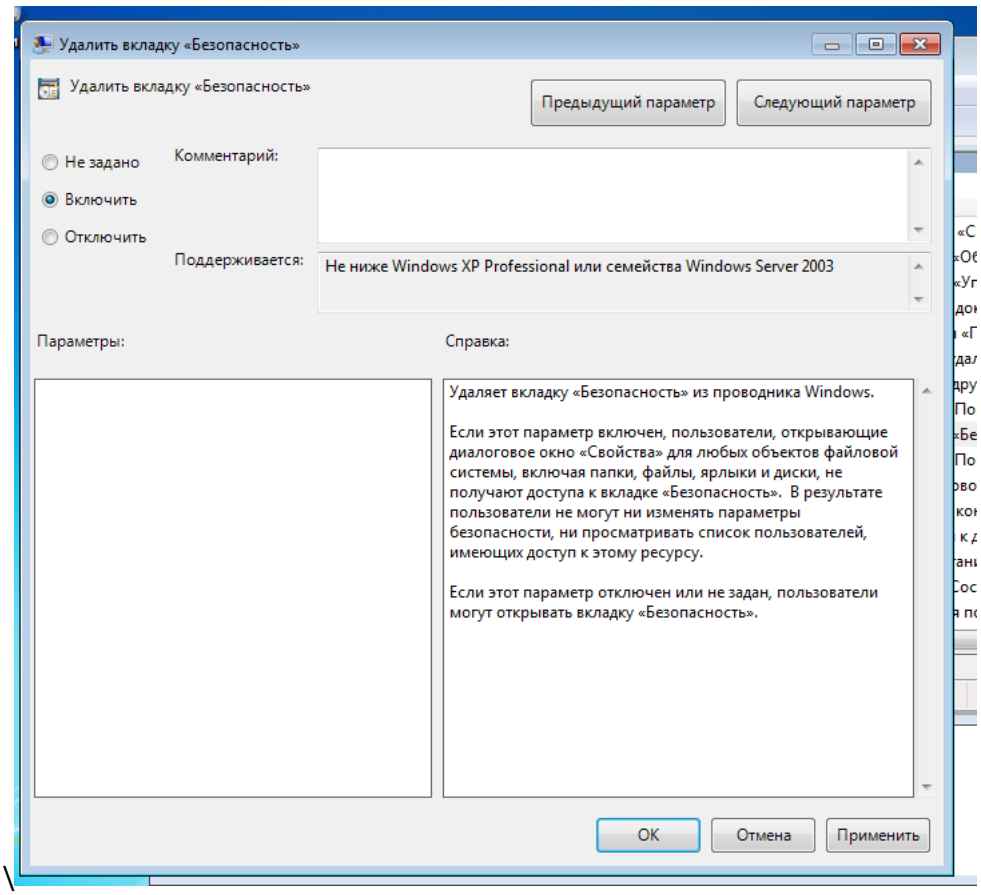


Рисунок 35 -Удаление вкладки «Безопасность»

4) Скрытие значка «Вся сеть» в папке «Сетевое окружение»

Откроем оснастку «Скрыть значок «Вся сеть» в папке «Сетевое окружение», перейдя по адресу: WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация пользователя» → узел «Административные шаблоны» → узел «Компоненты Windows» → узел «Проводник» → узел «Скрыть значок «Вся сеть» в папке «Сетевое окружение».

Знание топологии сети для обычного пользователя не должно представлять интереса, однако в случае, если к данному АРМ получит доступ злоумышленник, это облегчит ему понимание того, как следует действовать дальше. Поэтому в целях безопасности следует убрать возможность просмотра полной топологии сети

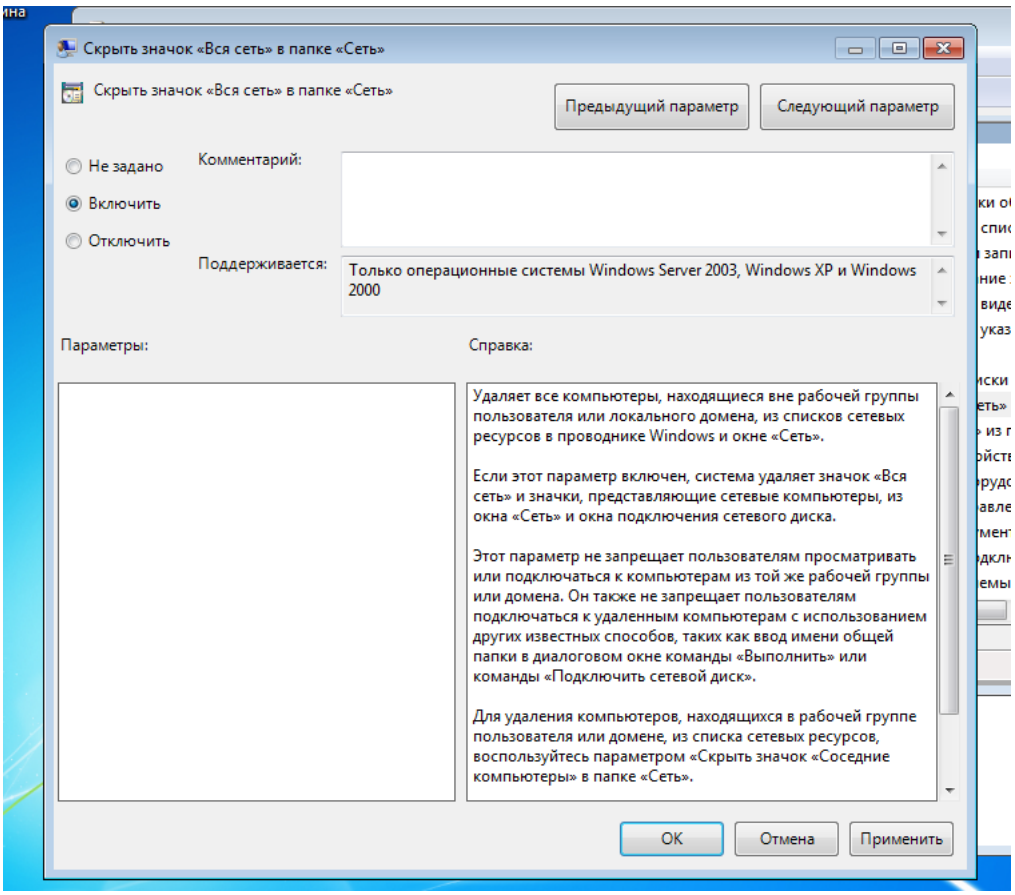


Рисунок 36 - Скрытие значка «Вся сеть» в папке «Сетевое окружение»

5) Запретить создание новых заданий

Откроем оснастку «Запретить создание новых заданий», перейдя по адресу: WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация пользователя» → узел «Административные шаблоны» → узел «Компоненты Windows» → узел «Планировщик заданий» → узел «Запретить создание новых заданий».

Все задания, которые запланированы в системе, задаются системным администратором. Следует запретить возможность создания новых заданий самим пользователем

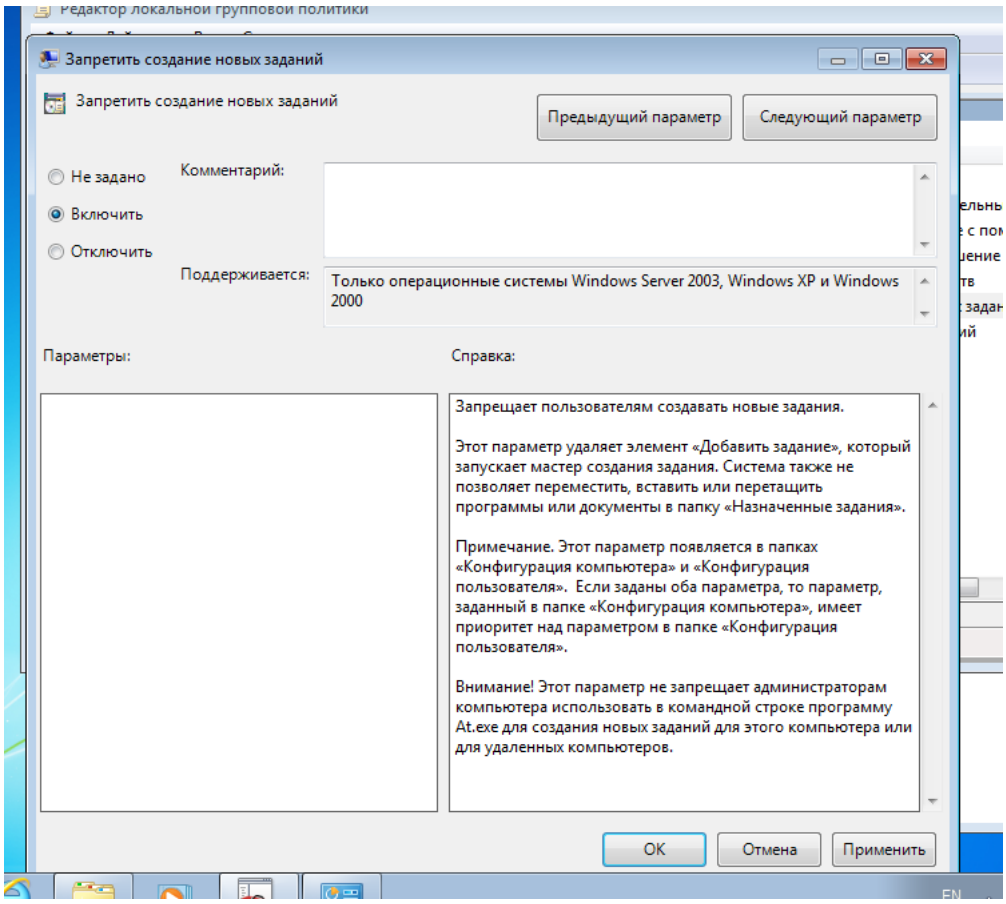


Рисунок 37 – Запретить создание новых заданий

6) Запретить удаление заданий

Откроем оснастку «Запретить удаление заданий», перейдя по адресу: WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация пользователя» → узел «Административные шаблоны» → узел «Компоненты Windows» → узел «Планировщик заданий» → узел «Запретить удаление заданий».

Все задания, которые запланированы в системе, задаются системным администратором. Следует запретить возможность удаления уже установленных заданий самим пользователем

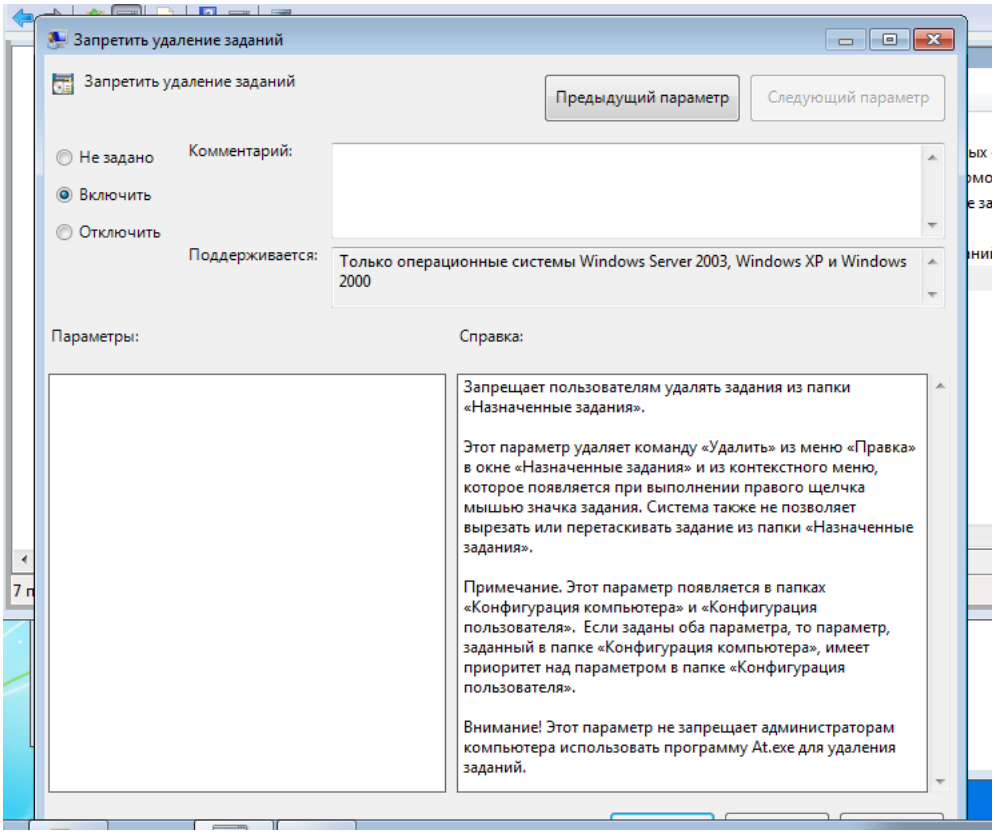


Рисунок 38 – Запретить удаление заданий

7) Запрет использования съемных носителей при установке

Откроем оснастку «Запретить установку со съемных носителей», перейдя по адресу: WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация пользователя» → узел «Административные шаблоны» → узел «Компоненты Windows» → узел «Установщик Windows» → узел «Запретить установку со съемных носителей».

Политика безопасности предприятия подразумевает, что пользователям нельзя использовать личные съемные носители. В целях повышения безопасности следует запретить использование любых съемных носителей для установки каких бы то ни было приложений

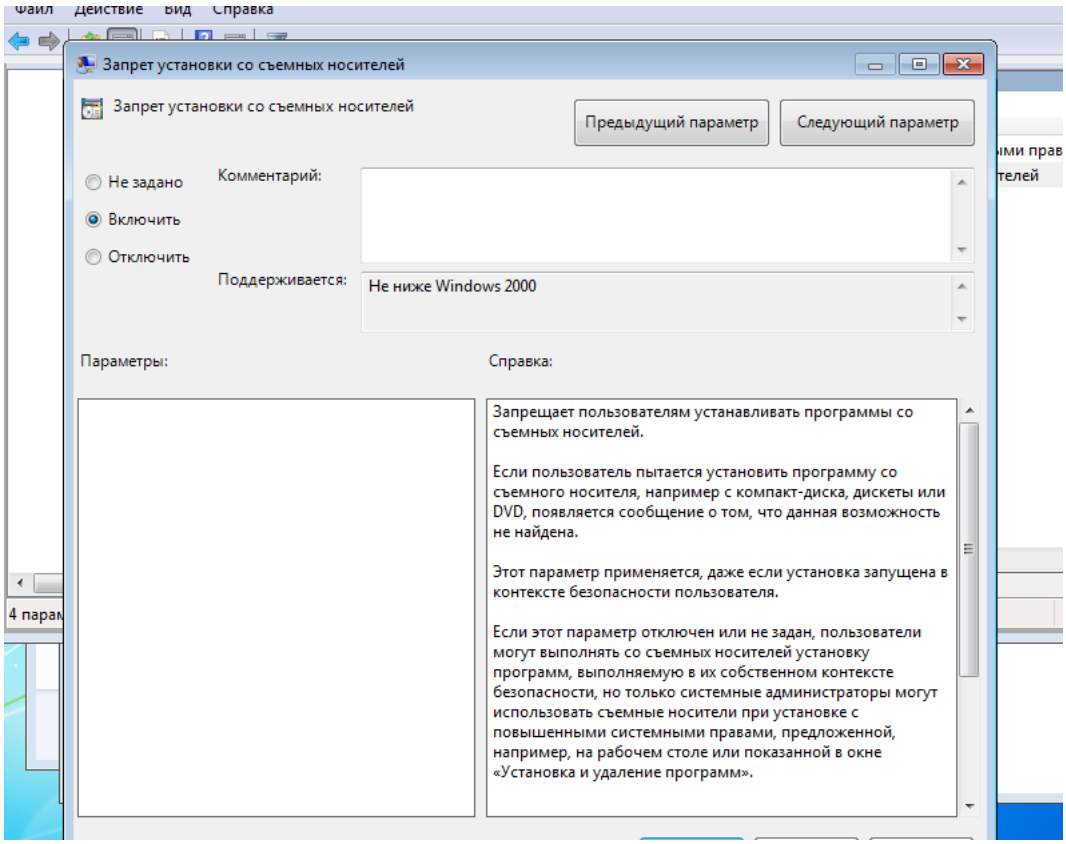


Рисунок 39 -Запрет использования съемных носителей при установке

8) Удаление «Сетевых подключений» из меню «Пуск»

Откроем оснастку «Удалить «Сетевые подключения из меню «Пуск», перейдя по адресу: WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация пользователя» → узел «Административные шаблоны» → узел «Панель задач и меню «Пуск» → узел «Удалить «Сетевые подключения из меню «Пуск».

Ранее в политике «Конфигурация Windows» был настроен запрет возможности выхода в сеть для пользователей: был выбран неправильный прокси-сервер, чтобы запросы пользователя оставались без ответа и, соответственно, доступ в интернет не работал. Теперь для увеличения безопасности следует убрать вкладку «Сетевые подключения» из меню «Пуск», чтобы пользователь не имел возможности выбрать другой прокси-сервер и восстановить подключение к интернету

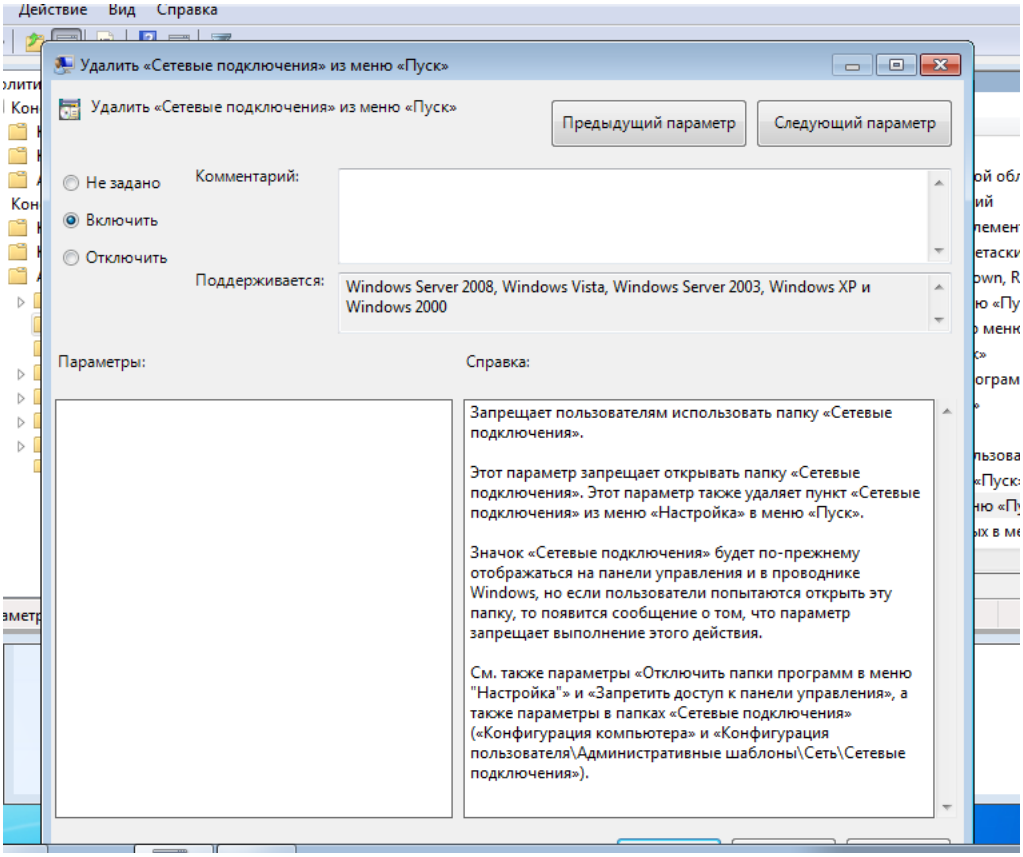


Рисунок 40 - Удаление «Сетевых подключений» из меню «Пуск»

9) Действия при отключении от сервера

Откроем оснастку «Действия при отключении от сервера», перейдя по адресу: WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация пользователя» → узел «Административные шаблоны» → узел «Сеть» → узел «Автономные файлы» → узел «Действия при отключении от сервера».

Поскольку синхронизация с сервером важна для АРМ и, соответственно, для пользователя, работающего за ней, следует предусмотреть порядок работы в случае, если сервер окажется недоступен. Для этого включим параметр «Действия при отключении сервера» и укажем реакцию системы, когда сервер становится недоступен: система будет работать автономно, т.е. файлы сервера будут доступны локальному компьютеру. Эта настройка позволит избежать простоев и финансовых убытков, связанных с ними

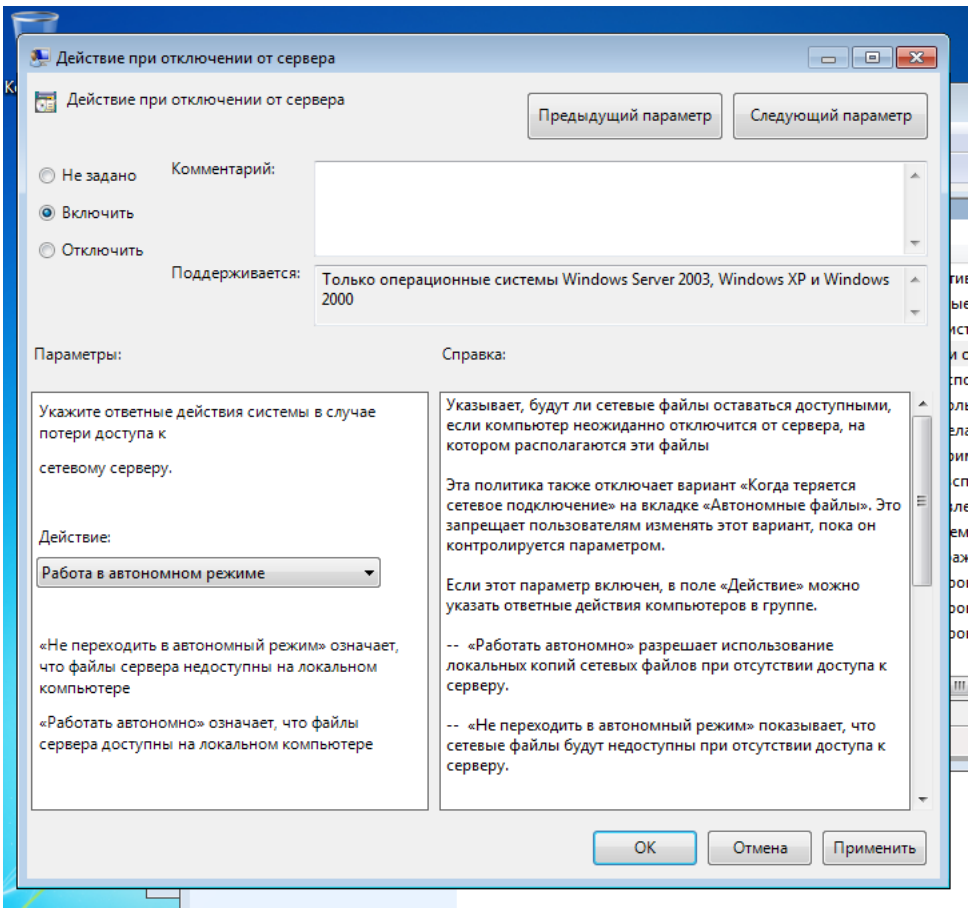


Рисунок 41 - - Действия при отключении от сервера

«Административные шаблоны» оснастки «Конфигурация пользователя» успешно настроена.

Промежуточный вывод: в процессе выполнения данного этапа задания были настроены «Административные шаблоны» с учетом места расположения АРМ. Приведены обоснования настроек параметров для каждого пункта политики безопасности. Также дополнительно были настроены параметры безопасности ОС: с помощью данной оснастки были исключены команды и вкладки, использованием которых пользователь смог бы нарушить работоспособность АРМ. Например, была удалена возможность получить доступ к «Свойствам папок», через которые можно открыть системные файлы, а также возможность просмотра «Соединения», что не позволит пользователям попытаться сменить прокси-сервер и получить доступ в сеть. Также был настроен порядок работы системы в случае, если сервер будет недоступен, чтобы избежать простоя и финансовых убытков, связанных с ними.

На этом настройка узла «Конфигурация пользователя» закончена.

Вывод по пункту: в данной части лабораторной работе были настроены политики, относящиеся к узлу «Конфигурация пользователя», предназначенному для настроек параметров пользователей. Параметры, которые находятся в этом узле, применяются при входе конкретного пользователя в систему.

Дочерний узел «Конфигурация программ» позволяет указать определенную процедуру установки программного обеспечения.

Дочерний узел «Конфигурация Windows» в основном предназначен для обеспечения безопасности компьютера и учетной записи, для которой применяются данные политики.

Дочерний узел «Административные шаблоны» является крупнейшим из всех возможных расширений групповой политики и включает тысячи параметров для приложений и компонентов операционной системы Windows.

В частности, в процессе выполнения данного задания были настроены:

- Конфигурация Windows, включая сценарии для входа и выхода пользователя из системы, направленные на резервирование данных
- Произведена настройка политики «Настройки Internet Explorer», заключающиеся в основном в запрете пользователю доступа в интернет в целях безопасности данных, хранящихся на АРМ
- Административные шаблоны, включающие в себя компоненты для безопасной работы пользователя на АРМ

Каждый параметр политик и журналов был аргументирован в соответствии с выбранной ролью АРМ, указанной в начале каждого пункта.

Для каждого этапа настройки политик представлен свой промежуточный вывод по этапу, суммирующий проделанную в ходе выполнения каждой задачи работу.

3. **Выводы:**

В данной лабораторной работе были изучены групповые политики безопасности АРМ. В частности, были настроены:

- Политика «Конфигурация компьютера», предназначенная для настройки параметров компьютера, применяемых невзирая на то, под какой учетной записью пользователь вошел в систему
- Политика «Конфигурация пользователя», предназначенная для настроек параметров пользователей. Параметры, которые находятся в этом узле, применяются при входе конкретного пользователя в систему
- Для каждой из политик, упомянутых выше, были настроены дочерние узлы «Конфигурация Windows», включая «Сценарии» и «Параметры безопасности», и «Административные шаблоны»

Каждый параметр политик и настроек их дочерних узлов был аргументирован в соответствии с выбранной ролью АРМ, указанной в начале каждого пункта.