Санкт-Петербург 2020

1. Цель работы

Цель работы — изучить редактор локальной групповой политик и научиться настраивать групповые политик безопасности на АРМ пользователя с установленной на нём ОС Windows для защиты информации от НСД.

Используемое программное обеспечение: ОС версии не ниже WindowsXP. А именно Windows 7 Professional (x64).

Тип ИС закрытого контура: 1Г**.**

2. Теоретическое введение

Групповые политики — это совокупность параметров, используемых для конфигурирования рабочего окружения пользователя или компьютера. Групповые политики — это набор правил, обеспечивающих инфраструктуру, в которой администраторы локальных компьютеров и доменных служб Active Directory могут централизованно развёртывать и управлять настройками пользователей и компьютеров в организации.

Настройки групповой политик насчитывает 3200 параметров и обеспечивает невероятно огромный возможности настройки.

Объекты групповых политик делятся на две категории:

1. *Доменные объекты групповых политик* — используются для централизованного управления конфигурацией компьютеров и пользователей, входящих в состав домена Active Directory.
2. *Локальные объекты групповых политик* — позволяют настраивать конфигурацию локального компьютера, а также всех пользователей, созданных на этом компьютере.

Для управления локальными объектами групповых политик в ОС Windows используется оснастка консоли управления "Редактор локальной групповой политик" .

Узел "Конфигурация компьютера" предназначен для настройки параметров компьютера. В этом узле расположены параметра, которые применяются к компьютеру, невзирая на то, под какой чётной записью пользователь вошёл в систему. Он включает в себя 3 дочерних узла: *Конфигурация программ*, *Конфигурация Windows* и *Административные шаблоны*.

Узел "Конфигурация пользователя" предназначен для настроек параметров пользователей. Параметры, которые находятся в этом узле, применяются при входе конкретного пользователя в систему. Также содержит 3 дочерних узла:

1. *Конфигурация программ* — в нём находится расширение "Установка программ" , с помощью которого можно указать определённую процедуру установки ПО.
2. *Конфигурация Windows* — в основном предназначена для обеспечения безопасности компьютера и учётной записи, для которой применяются данные политики.
3. *Административные шаблоны* — крупнейший из всех возможных расширений групповой политики. Каждому параметру этой политики соответствует определённый параметр системного реестра.

3. Ход выполнения работы

Установка макета варианта лабораторной работы на диске C

Была проведена установка макета на диске G, а именно VirtualBox с ОС Windows 7.

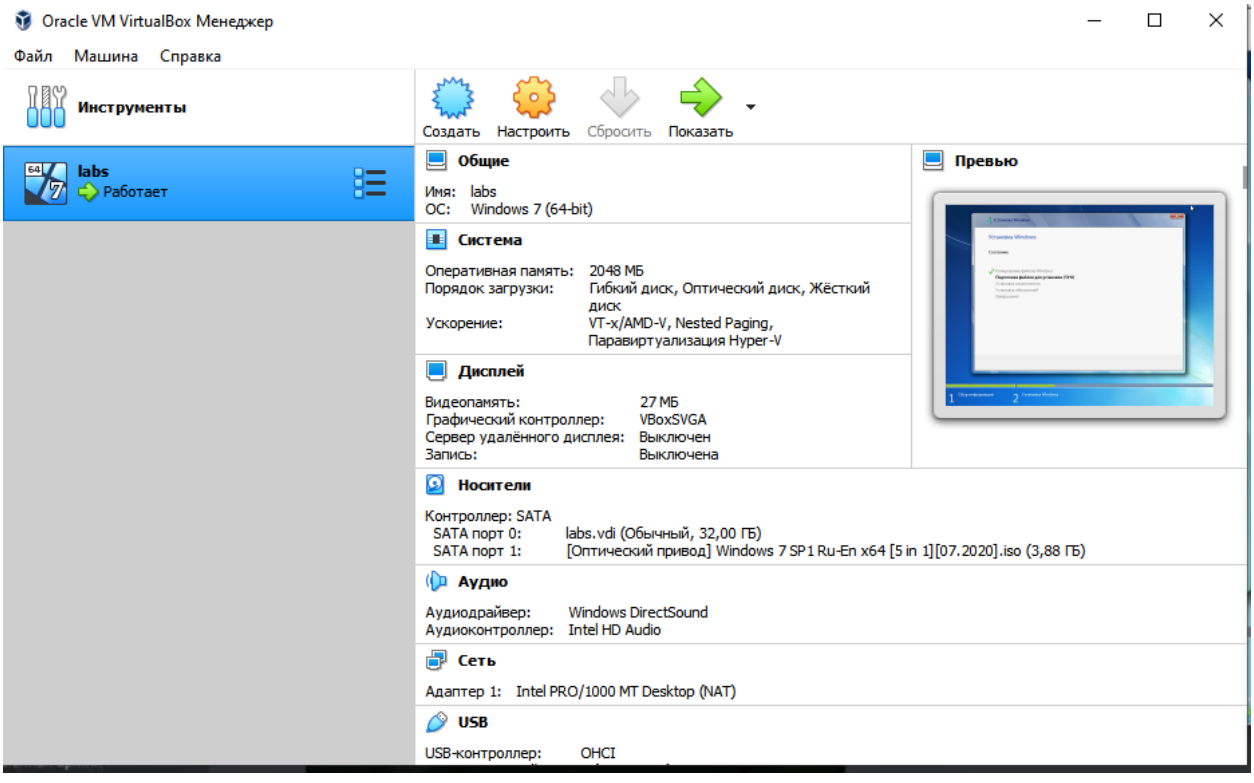


Рисунок 1 - Запуск ОС на ВМ

Оснастка «Редактор локальной групповой политики»

Чтобы открыть данную оснастку воспользуемся комбинацией клавиш "Win+R" для открытия диалога "Выполнить" и введём в его поле gpedit.msc.

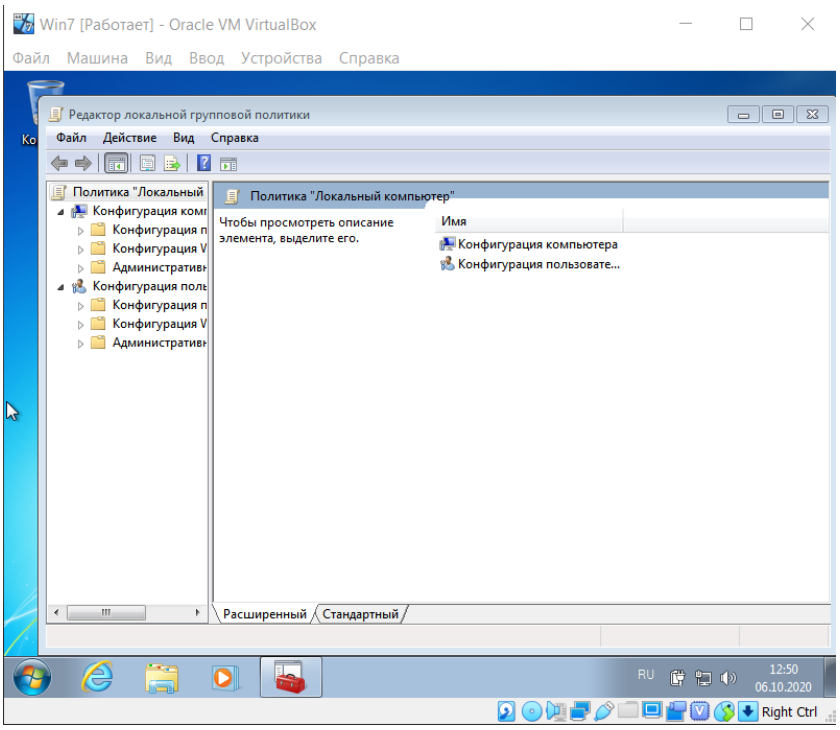


Рисунок 2 - Оснастка "Редактор локальной групповой политики"

Проведение настройки политик безопасности

Для выполнения настроек политик безопасности, учётная запись, под которой выполняются данные действия должна входить в локальную группу Администратор. Для этого при запуске системы зайдём под записью администратора. Проверим является ли текущий пользователь администратором:

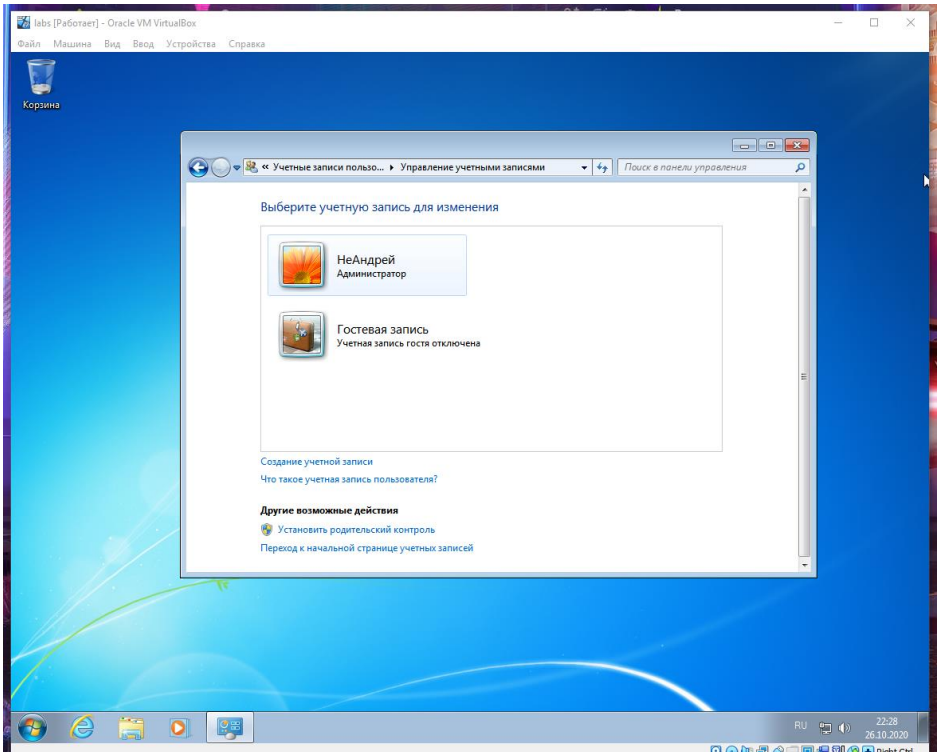


Рисунок 3 - Проверка является ли пользователь администратором

Настройка дочернего узла «Конфигурация Windows»

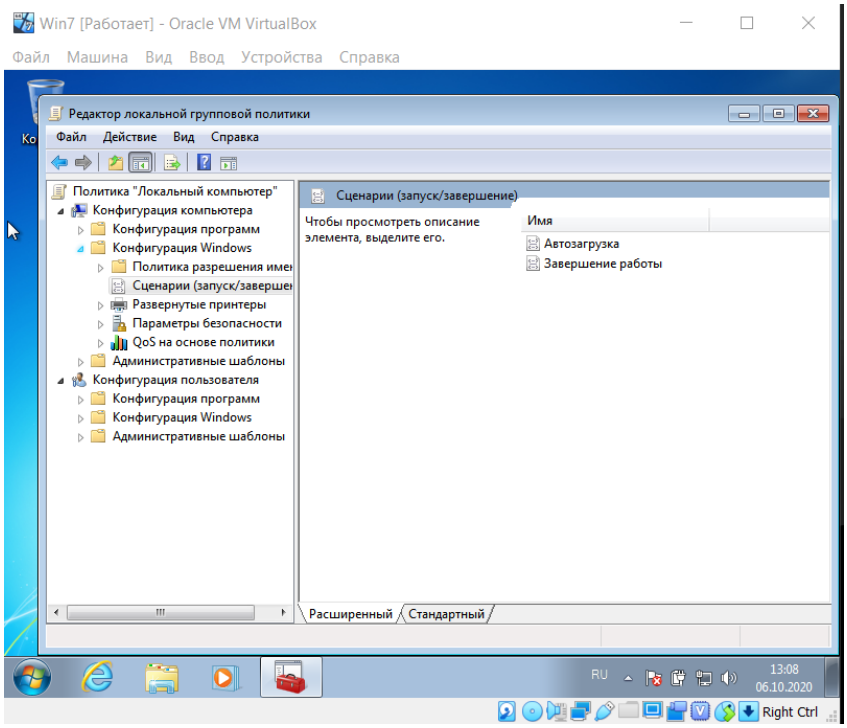


Рисунок 4 - Дочерний узел «Конфигурация Windows»

Так как рассматриваемое АРМ расположено в «закрытом» контуре, целесообразно вести строгий учёт файлов, находящихся на жестком диске, с целью анализа действий пользователя, а также сличение состояния файловой системы в моменты, когда пользователь не пользовался АРМ, т.е. не получил ли некий злоумышленник доступа к АРМ и не внес ли в него изменения, выполнив таким образом, требование 2 «Руководящего документа» по для систем класса 1Г. Для этого 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. Этот скрипт будет запускаться при входе пользователя в систему и при выходе из нее. Приведем программный код этого скрипта:

```
1.  $source="C:"
2.  Get-ChildItem $source -Recurse -Force | where {$_.psIscontainer} | foreach {
3.      $count = Get-ChildItem $_.FullName -Recurse | where {$_.Length} | Measure-Object –Property
    Length -Sum
4.      Write-Host($_.FullName)
5.      $FilesSize = '{0:F}' -f ((($count.Sum)/1024)/1024)
6.      Write-Host("Files: " + $count.Count)
7.      Write-Host("Size: " + $FilesSize + " MB")
```

```
8.          "" + $_.FullName + '","' + $count.Count + '","' + $FilesSize + ""
        | Out-File C:\CountFiles.csv -Append
9.    }
```

Добавим данный скрипт в сценарии «Автозагрузки» и «Завершения работы».

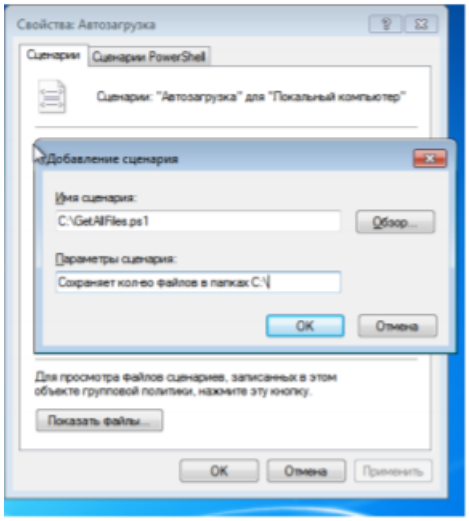


Рисунок 6 - Добавление скрипта в сценарии автозагрузки

До изменений сценарий автозагрузки был пуст. После добавления скрипта сценарий примет вид на Рисунке 7.

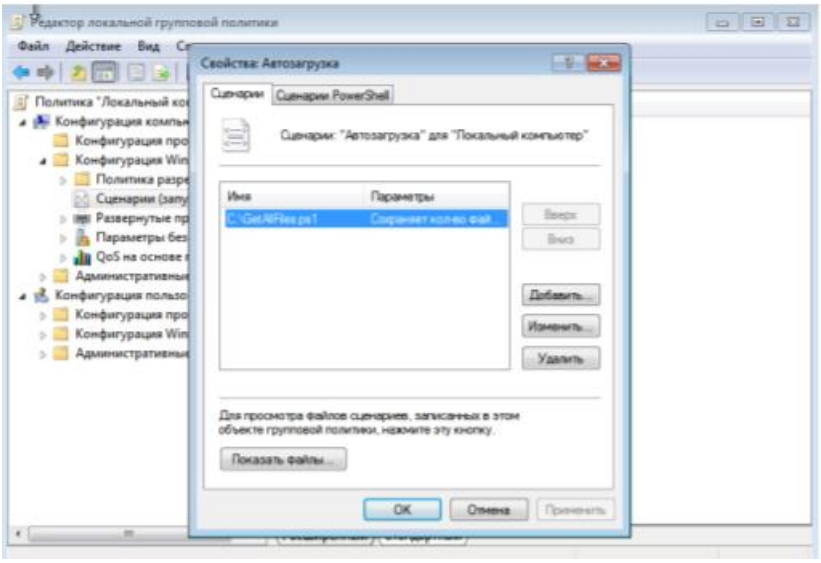


Рисунок 7 - Сценарий автозагрузки после добавления скрипта

Далее добавим данный скрипт в сценарий завершения работы.

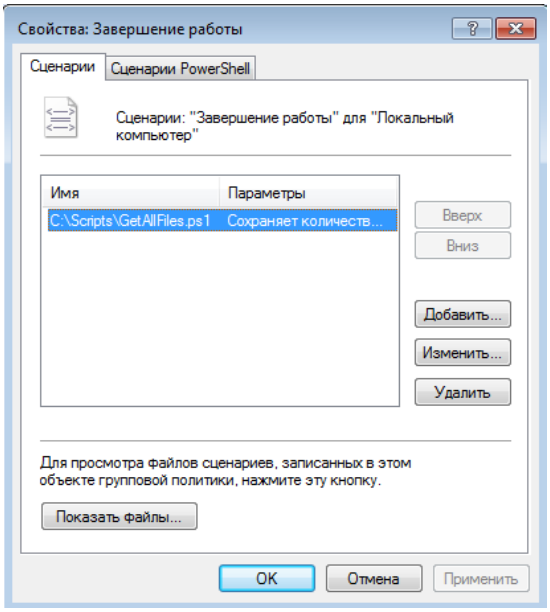


Рисунок 8 - Сценарий завершения работы после добавления скрипта

Настройка узла «Параметры безопасности»

«Параметры безопасности» -- дочерний узел «Конфигурации Windows», позволяющий настраивать политики безопасности средствами «Групповой политики». В этой опции для конфигурации безопасности компьютера доступны следующие настройки политик:

1. *Политики учетных записей*, которые позволяют устанавливать политику паролей и блокировки учетных записей.

2. *Локальные политики*, отвечающие за политику аудита, параметры безопасности и назначения прав пользователя.

3. *Политики открытого ключа*, которые позволяют:

a. настраивать компьютеры на автоматическую отправку запросов в центр сертификации предприятия и установку выдаваемых сертификатов;

b. создавать и распространять список доверия сертификатов (CTL);

c. добавлять агенты восстановления шифрованных данных и изменение параметров политики восстановления шифрованных данных;

d. добавлять агенты восстановления данных шифрования диска BitLocker.

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

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

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

Произведем настройку политик, указанных выше, учитывая соблюдение требований «Руководящего документа» для АРМ класса «1Г».

Настройка «Политики учётных записей»

«Политика паролей»

Следующим инструментом РД при работе на АРМ является установка паролей учётных записей. Надёжность использования паролей, а соответственно подсистемы РД, является правильная настройка «Политики паролей» – совокупности правил,

накладывающих разумные ограничения на пользовательские пароли. К таким правилам относятся:

1. *Максимальные срок действия пароля*, т.е. период времени, в течение которого пользователь обязан изменить пароль для продолжения работы на АРМ. Доступные значения могут быть установлены в промежутке от 0 до 999 дней.

Однако для обеспечения своевременной сменяемости пароля, рекомендуется

выбирать максимальный срок действия от 14 до 30 суток, именно за такой срок, в худшем случае, возможен подбор пароля.

2. *Минимальная длина пароля.* Значение данной политики сравнивается с длиной устанавливаемого пароля и запрещает его использование, в случае если его длина меньше указанной. Рекомендуемое значение от 8 до 16 символов.

3. *Минимальные срок действия пароля,* т.е. период времени, в течение которого изменение пароля невозможно. Следует отметить, что значение данной политики не должно превышать максимального срока действия пароля.

4. *Требование неповторяемости паролей,* т.е. политика, устанавливающая ограничение на установку «старого» пароля в качестве «нового». Значение политики – количество старых паролей, с которыми происходит сравнение при выборе нового. Должна обеспечивать «обновляемость» паролей и согласовываться со сроками смены паролей. Таким образом, при смене паролей каждые 15 суток, хранение квартальной базы (6 прежних паролей) оптимально.

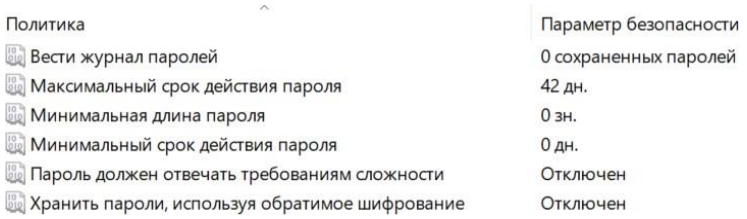
5. *Хранение паролей, используя обратимое шифрование.* Использование данной политики рекомендуется исключительно в тех случаях, когда используются приложения, требующие пароль для аутентификации пользователя.

6. *Пароль должен отвечать требованиям сложности.* Данная политика устанавливает ограничение на характеристики пароля и предотвращает использование «простых» паролей, существенно повышая уровень безопасности, в следствии чего обязательна к использованию. К вносимым ограничениям относятся:

   a. использование букв верхнего и нижнего регистра одновременно;
   b. использование цифр от 0 до 9;
   c. использование специальных символов (например, !, @, #, $, *);
   d. запрет использования имени учетной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков.

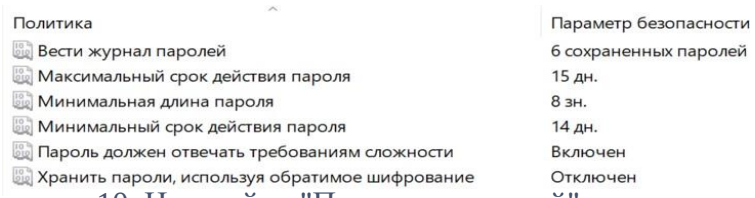
В соответствии с требованиями к классу защищенности 1Г, пароль, используемый при входе в систему, обязан бить длиной не менее шести буквенно-цифровых символов.

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».



Политика	Параметр безопасности
Вести журнал паролей	0 сохраненных паролей
Максимальный срок действия пароля	42 дн.
Минимальная длина пароля	0 зн.
Минимальный срок действия пароля	0 дн.
Пароль должен отвечать требованиям сложности	Отключен
Хранить пароли, используя обратимое шифрование	Отключен

Рисунок 9. "Политики паролей" по умолчанию.



Политика	Параметр безопасности
Вести журнал паролей	6 сохраненных паролей
Максимальный срок действия пароля	15 дн.
Минимальная длина пароля	8 зн.
Минимальный срок действия пароля	14 дн.
Пароль должен отвечать требованиям сложности	Включен
Хранить пароли, используя обратимое шифрование	Отключен

Рисунок 10. Настройки "Политики паролей".

«Политика блокировки учётных записей»

Правильная настройка «Политики паролей» повышает защищенность системы, но не делает «абсолютно защищенной». В ряде случаев, когда злоумышленнику стало известно имя пользователя АРМ, процесс подбора возможно предотвратить, установив дополнительные ограничения на действия пользователя системы. Набор политик узла «Политика блокировки учетной записи», предоставляют администратору соответствующие полномочия.

Для изменения «Политика блокировки учетной записи» необходимо перейти по адресу: WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел «Конфигурация Windows» → узел «Параметры безопасности» → узел «Политики учетных записей» → узел «Политики блокировки учетных записей».

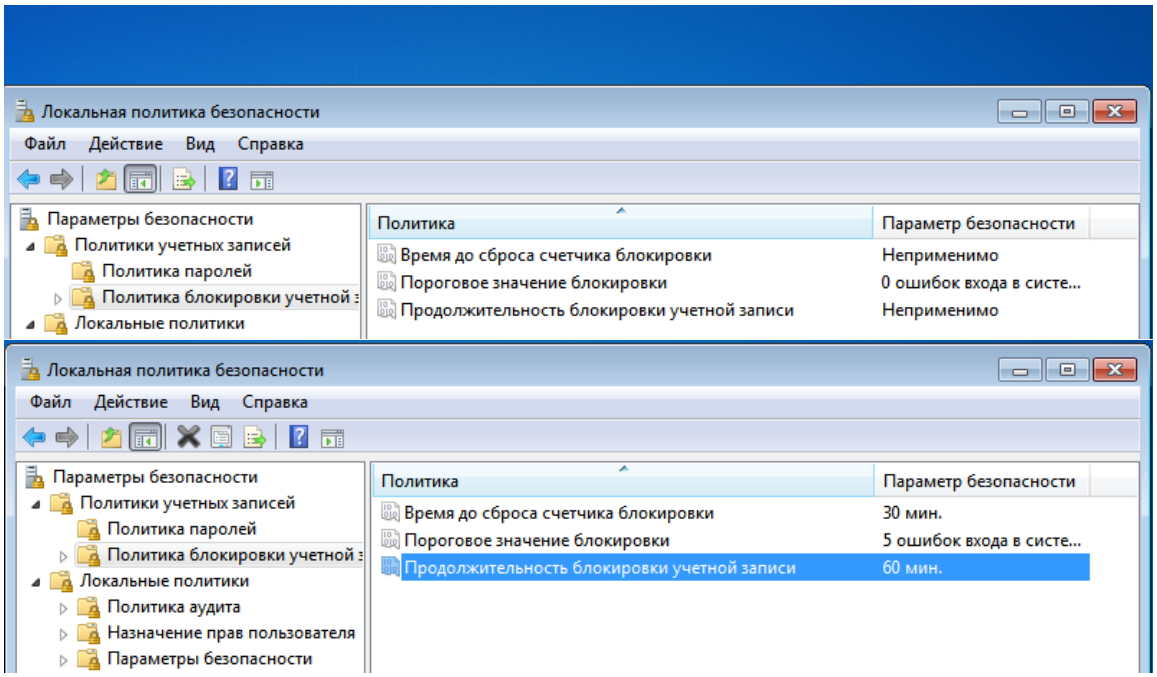


Рисунок 11 - Настройки «Политики блокировки учетных записей»

Настройка «Локальных политик» Политики аудита

Аудит – процесс, проводимый с целью совершенствования используемых мер по обеспечению ИБ на каком-либо объекте информатизации и состоящий в сборе подробной сводки информации обо всех попытках вторжения и случаях неудачной аутентификации пользователей, а также в проведении подробного анализа собранной информации. В свою очередь, *политика аудита* – есть совокупность параметров, определяющих какая информация будет поступать в журнал аудита АРМ.

Важно отметить, что аудит, рассмотренных событий, по умолчанию не проводится, для изменения параметров политики аудита необходимо перейти по адресу: WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел «Конфигурация Windows» → узел «Параметры безопасности» → узел «Локальные политики» → узел «Политика аудита».

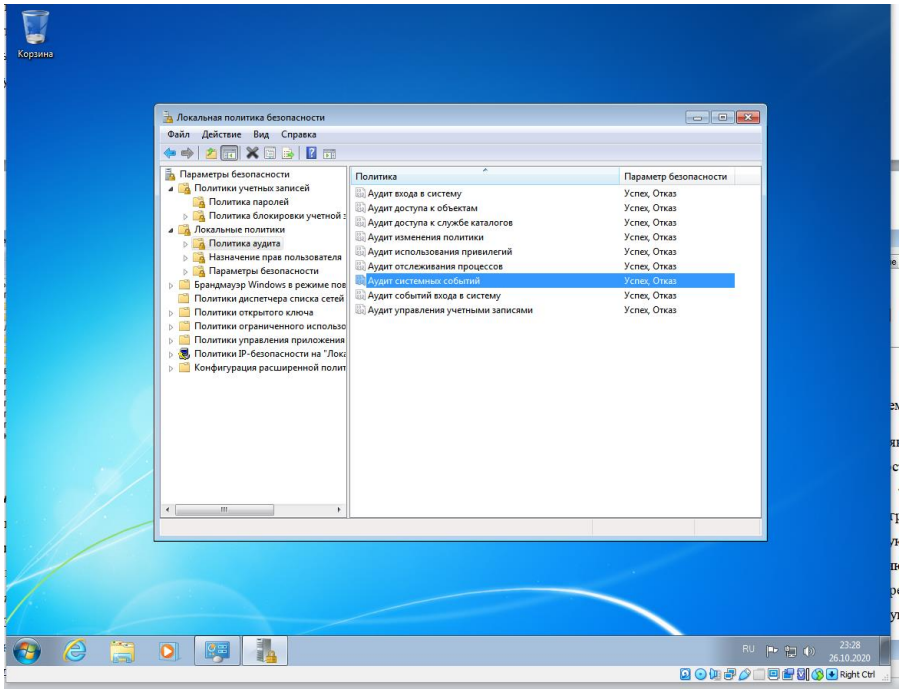


Рисунок 12 - Настройка «Политика аудита»

Политика «Назначение прав пользователей»

Угрозы информационной безопасности могут быть не только внешними, но и внутренними, т.е. ослабление защищенности могут быть вызваны некорректными

действиями легальных пользователей, как в следствии злого умысла, так и недостаточной квалификацией. С целью предупреждения внутренних угроз целесообразно разумно ограничивать права и привилегии пользователей и групп пользователей. Для назначения прав доступны 44 политики безопасности. Рассмотрим некоторые из политик:

1. *Добавление рабочих станций к домену.* Политика, предоставляющая пользователям (или группам пользователей) добавлять компьютеры в домен ActiveDirectory (до 10 компьютеров). Стоит отметить, что по умолчанию все пользователи, прошедшие проверку подлинности, на контроллерах домена могут добавлять до 10 компьютеров, для обеспечения состояния наибольшей защищенности целесообразно назначение данной привилегии исключительно группе администраторов ИС, вне зависимости от обрабатываемой в ИС информации.

2. *Доступ к компьютеру из сети.* Политика, предоставляющая разрешение подключения к компьютеру по сети указанным пользователям (или группам пользователей). На рабочих станциях и серверах данные привилегии предоставляются группам «Администраторы» и «Операторы архивации», «Пользователи» и «Все». В целях предотвращения НСД, для любых ИС, целесообразно ограничивать доступ из сети, т.е. не предоставлять доступ группе «Все».

3. *Завершение работы системы.* Политика, определяющая список пользователей, которые имеют право на использование команды «Завершение работы» после удачного входа в систему. На рабочих станциях и серверах данные привилегии предоставляются группам «Администраторы», «Операторы архивации» и «Пользователи» (только на рабочих станциях). Так как порядок завершение работы ОС напрямую влияет на её правильную работоспособность, целесообразно предоставление соответствующих полномочий исключительно администраторам ИС как «закрытого», так и открытого контура.

4. *Запрет входа в систему через службу удаленных рабочих столов.* Политика, определяющая список пользователей (или групп пользователей), которым запрещён входа в систему в качестве клиента удаленных рабочих столов. По умолчанию, как на рабочих станциях, так и на серверах, всем разрешено входить в систему как клиенту удаленных рабочих столов. Очевидно, что любая учетная запись, которой разрешен вход в систему с помощью служб удаленных рабочих столов, может быть использована для входа в удаленную консоль устройства. Если это право пользователя не ограничивается законными пользователями, которым требуется вход на консоль компьютера, злоумышленник может установить ПО, которое повышает права пользователей, именно поэтому обязателен тщательный отбор пользователей, которым будет предоставлена данная привилегия, вне зависимости от грифа защищаемой информации.

5. *Запрет локального входа.* Политика, запрещающая отдельным пользователям (или группам пользователей) выполнять вход в систему. По умолчанию всем пользователям разрешен вход в систем.

6. *Изменение системного времени.* Политика, предоставляющая право изменения системного времени отдельным пользователям (или группам пользователей). Стоит отметить, что данная политика также предоставляет право изменять соответствующее время отслеживаемых событий в Журнале событий. На рабочих станциях и серверах данные привилегии предоставляются группам «Администраторы» и «Локальная служба».

Для изменения политик по умолчанию необходимо перейти по адресу: WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел «Конфигурация Windows» → узел «Параметры безопасности» → узел «Локальные политики» → узел «Назначение прав пользователей».

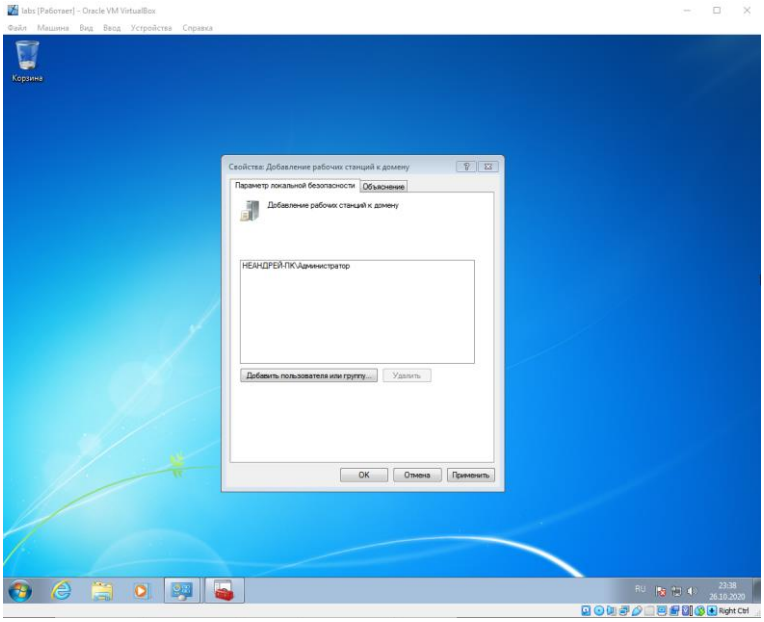


Рисунок 13 - «Добавление рабочих станций к домену»

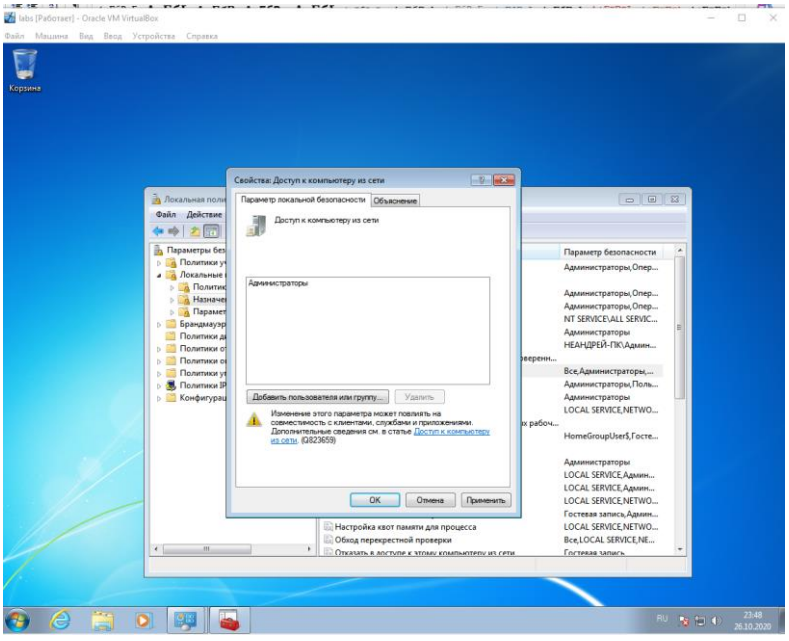


Рисунок 14 - «Доступ к компьютеру из сети»

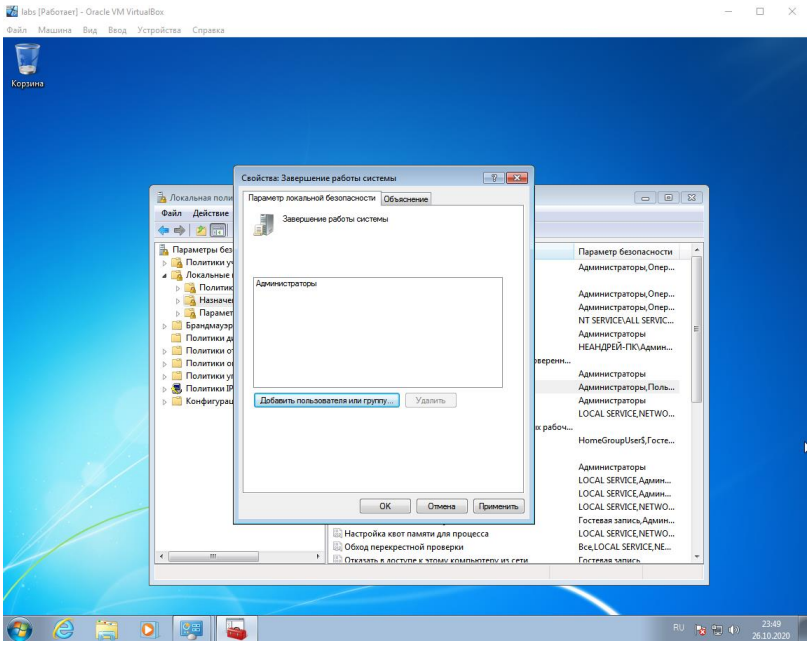


Рисунок 15 - «Завершение работы системы»

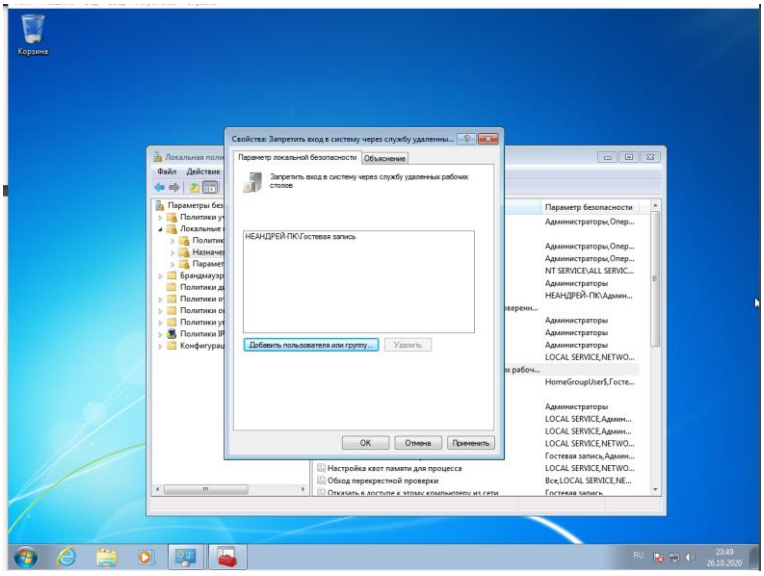


Рисунок 16 - «Запретить вход в систему через службу удаленных рабочих столов»

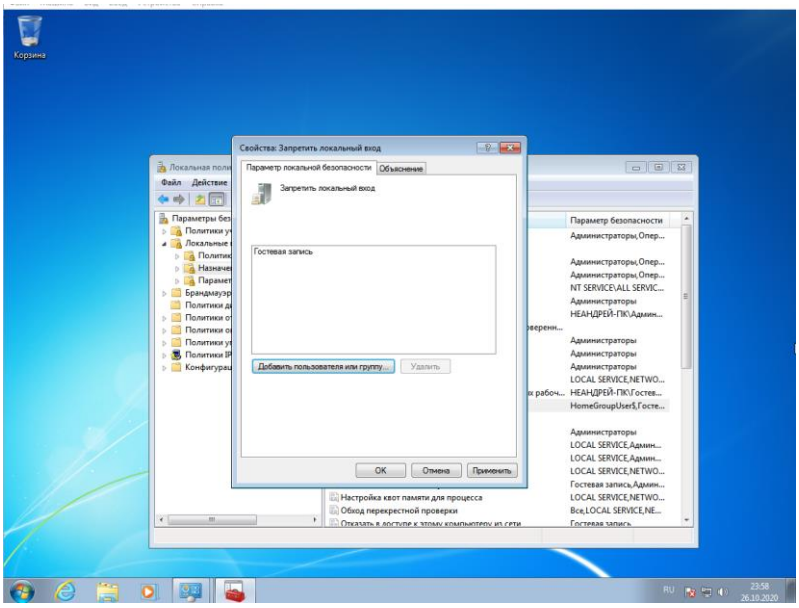


Рисунок 17 - «Запретить локальный вход»

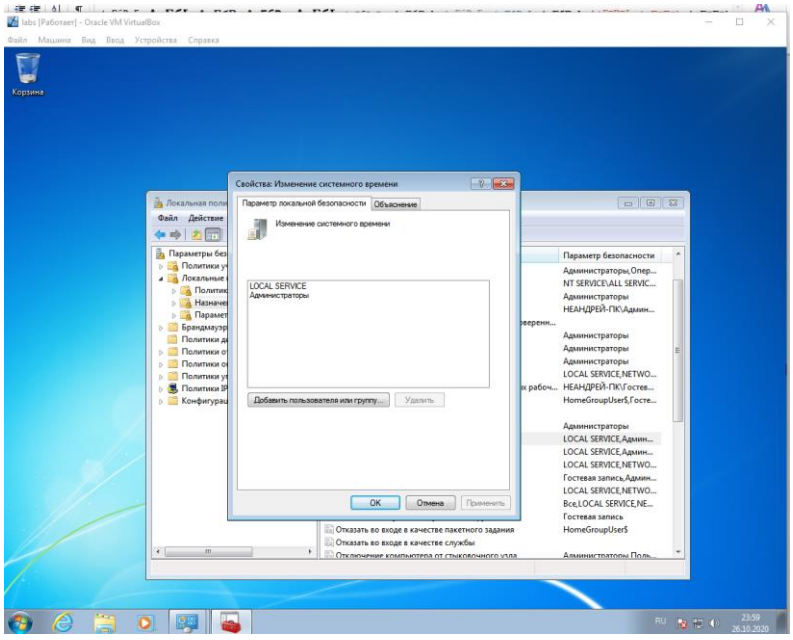


Рисунок 18 - «Изменение системного времени»

Настройка «Политики IP-безопасности на «Локальный компьютер»

Политики IP-безопасности на «Локальный компьютер» определяют порядок создания политик IP-безопасности на АРМ, а также управления списками IP-фильтров.

По умолчанию на АРМ не установлено политик IP-безопасности, для создания и изменения оных необходимо перейти по адресу: WIN+R → gpedit.msc → оснастка

«Групповые политики» → узел «Конфигурация компьютера» → узел «Конфигурация Windows» → узел «Параметры безопасности» → узел «Политики IP-безопасности на

«Локальный компьютер».

Проведем настройку соответствующих политик:

1. Клиент (только ответ). Так как, согласно индивидуальному варианту, настройка политик проводится для АРМ класса «1Г», то в целях соблюдения требования «Руководящего документа», следует ограничить доступ пользователей к сети «Интернет», при этом оставить возможность отвечать на служебные запросы, поступающие от серверов предприятия. Кроме того, с целью выполнения требований по проверке подлинности, необходимо использовать соответствующий протокол «Kerberos».

2. Сервер (запрос безопасности). С целью повышения состояния защищенности IP- безопасности, создадим и настроим политику, обеспечивающую первоочередную передачу запроса безопасности на сервер. А также, с целью соблюдения требований по проверки подлинности, установим требование использования протокола «Kerberos».

3. Сервер безопасности (требуется безопасность). Аналогично пункту 2, выполним настройку сервера безопасности, с целью выполнения требований «Руководящего документа».

Настроим оснастку Политика безопасности IP на "Локальный компьютер" . Поскольку АРМ расположена в "закрытом"контуре, то в целях повышения безопасности пользователям не следует выходить в сеть Internet. И поэтому пользователям запрещается все запросы, разрешено только отправлять ответы. Так же при обращении к серверу вначале передаётся запрос безопасности.

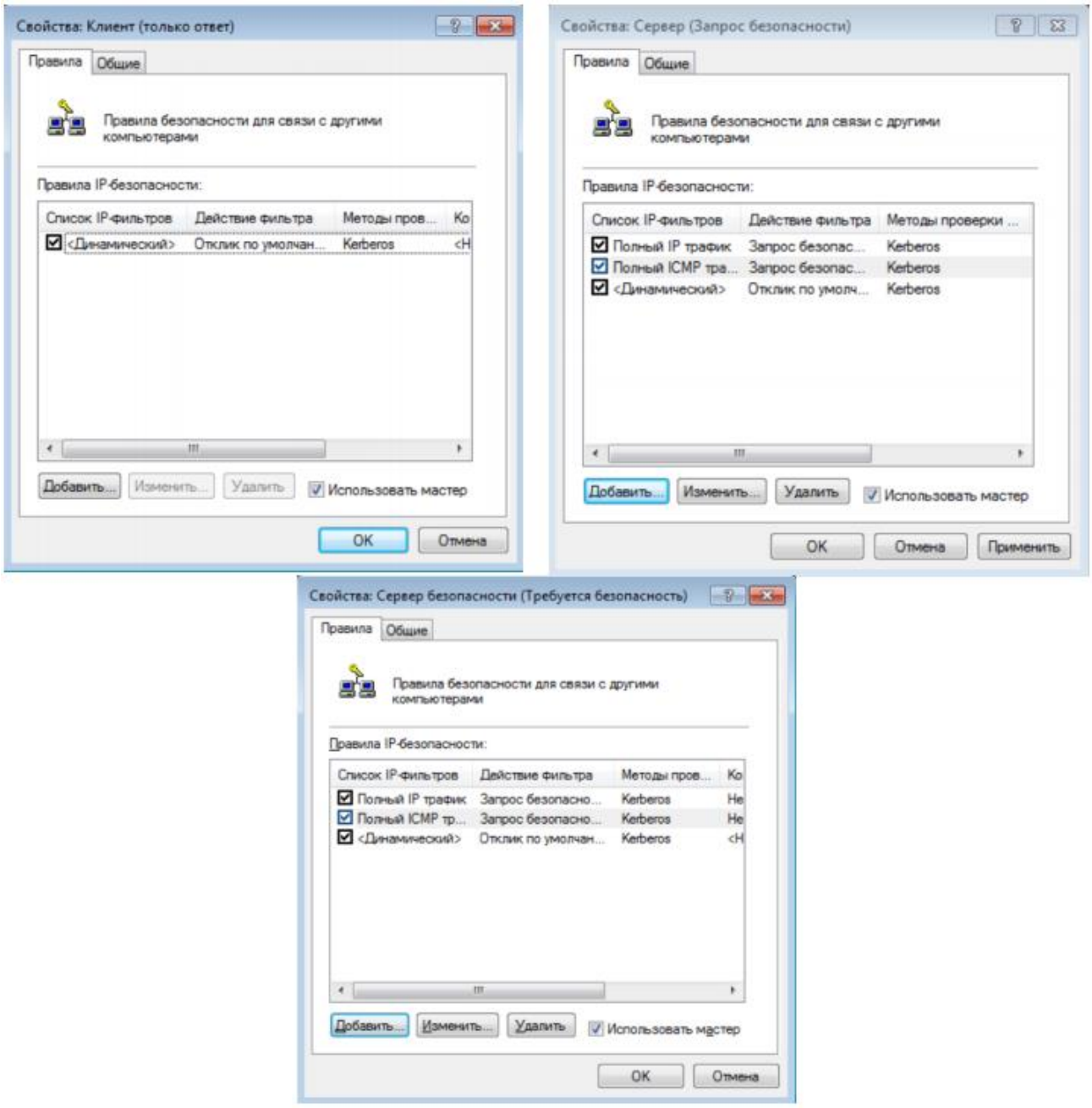


Рисунок 19 - Политика безопасности IP

Настройка дочернего узла «Конфигурация Windows»

Перейдём к настройке узла "Административные шаблоны" в дочерней узле "Конфигурация Windows"приложения "Групповые политики". Дочерний узел "Административные шаблоны" является крупнейшим из всех возможныых расширений групповой политики. Данная политика изменяет значения реестра в HKLM.

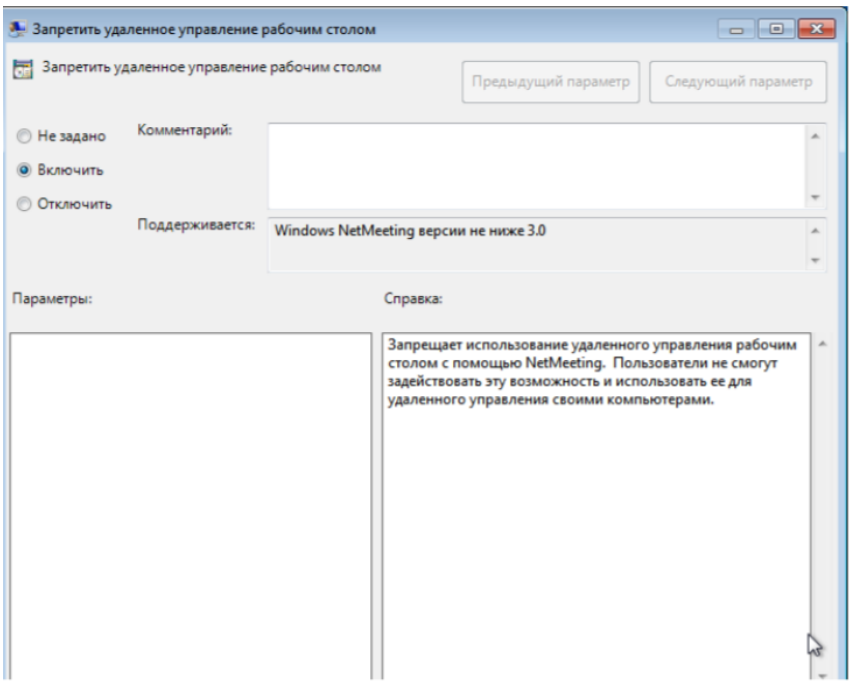


Рисунок 20 - Запретить удалённое управление рабочим столом

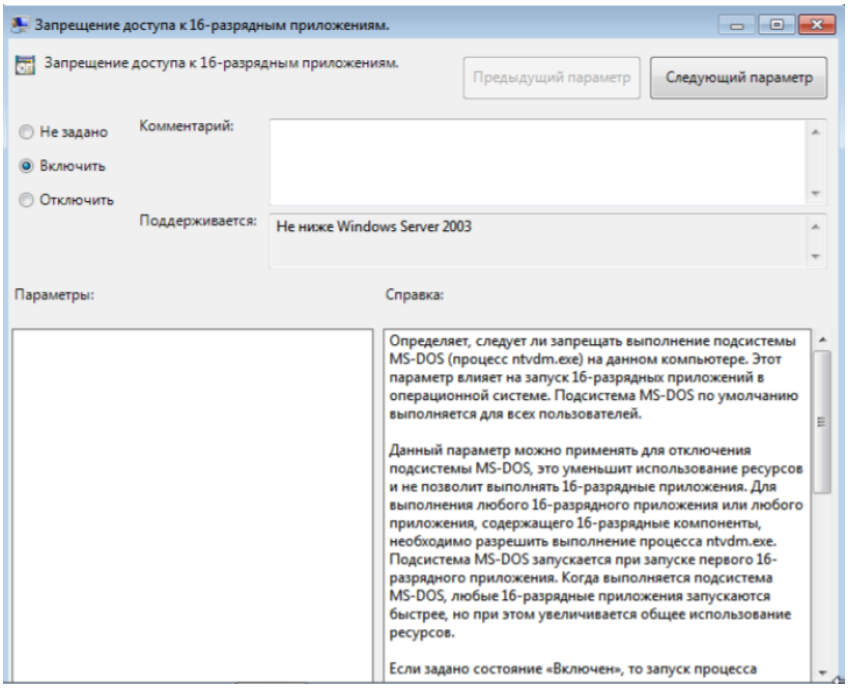


Рисунок 21 - Запрещение доступа 16-разрядным приложениям

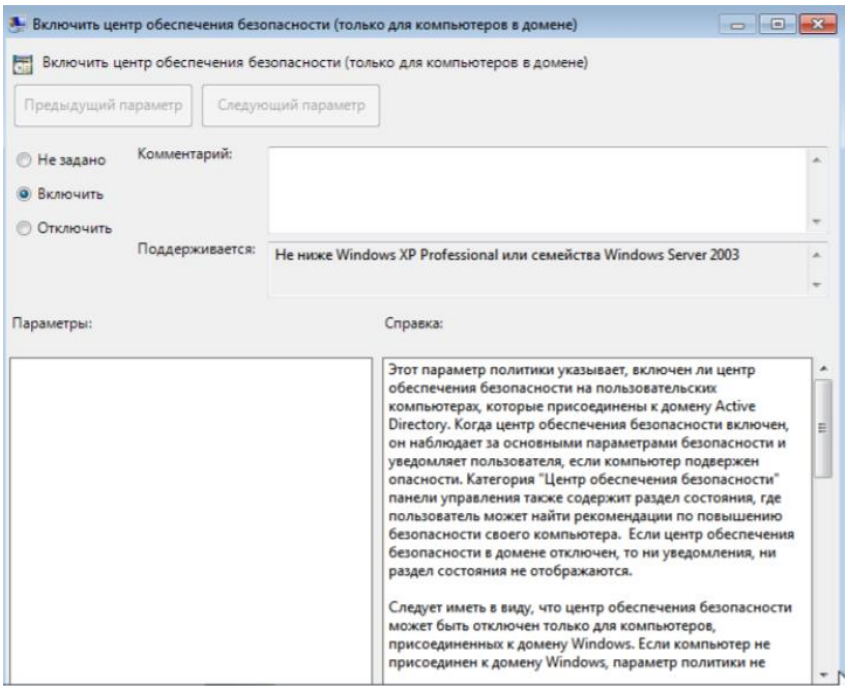


Рисунок 22 - Включить центр обеспечения безопасности

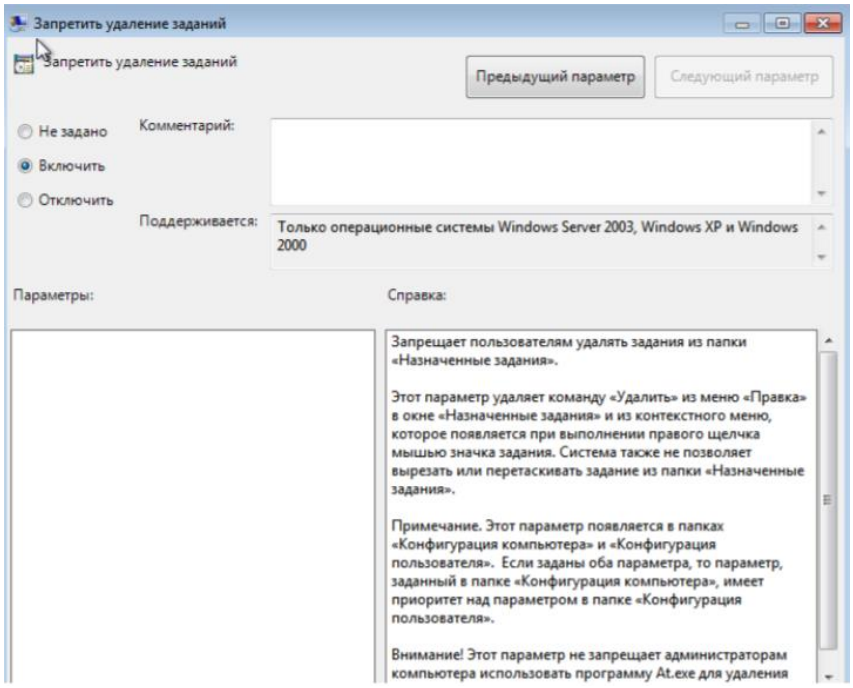


Рисунок 23 - Запретить удаление заданий

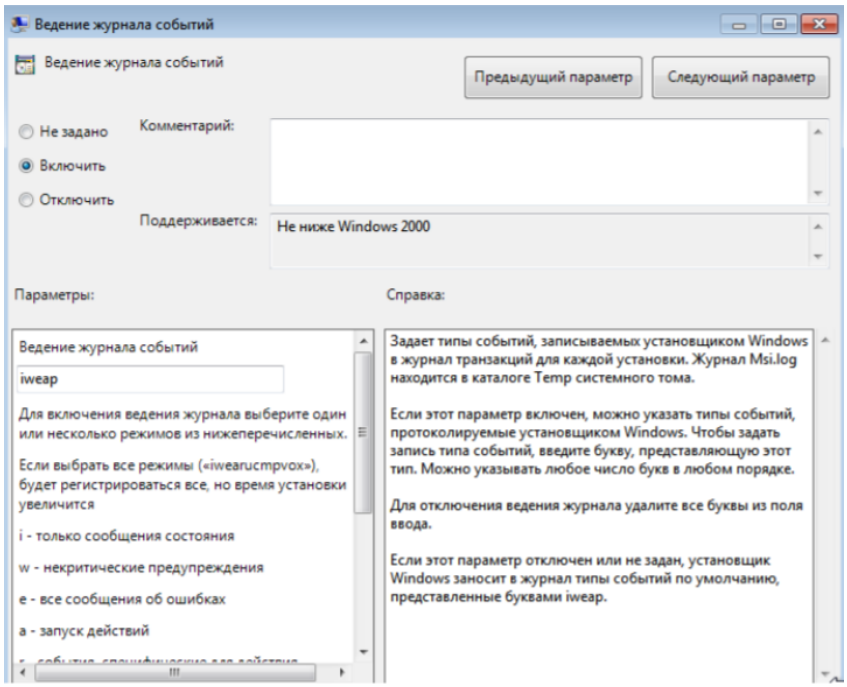


Рисунок 24 - Ведение журнала запуска и установки приложений

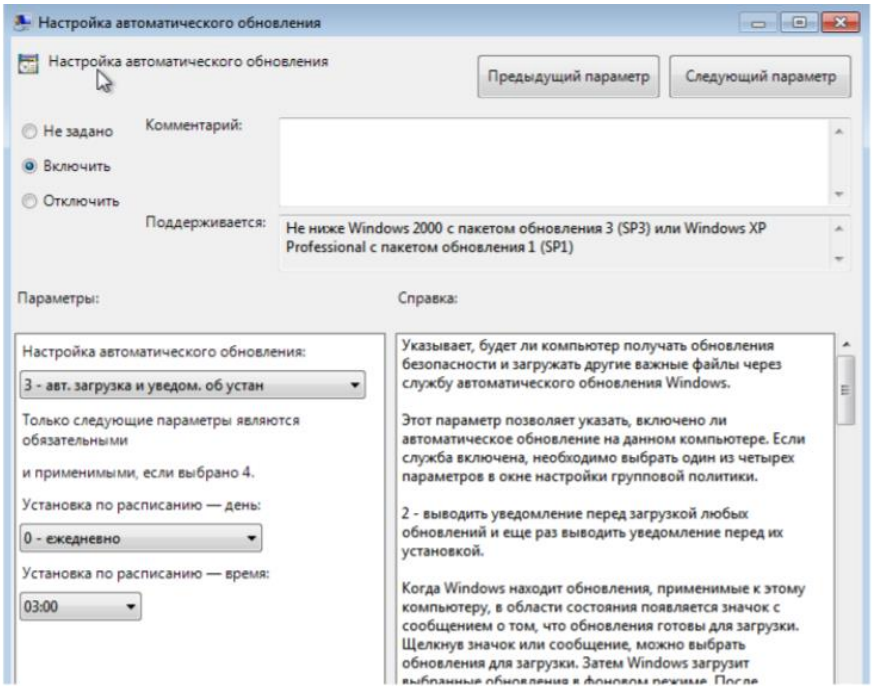


Рисунок 25 - Настройка автоматического обновления

Узел «Конфигурация пользователя»

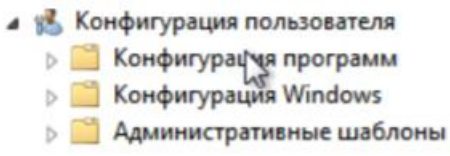


Рисунок 27 - Узел "Конфигурация пользователя"

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 логики 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»

Откроем оснастку "Конфигурация Windows" и перейдём к настройке узла "Сценарии" .

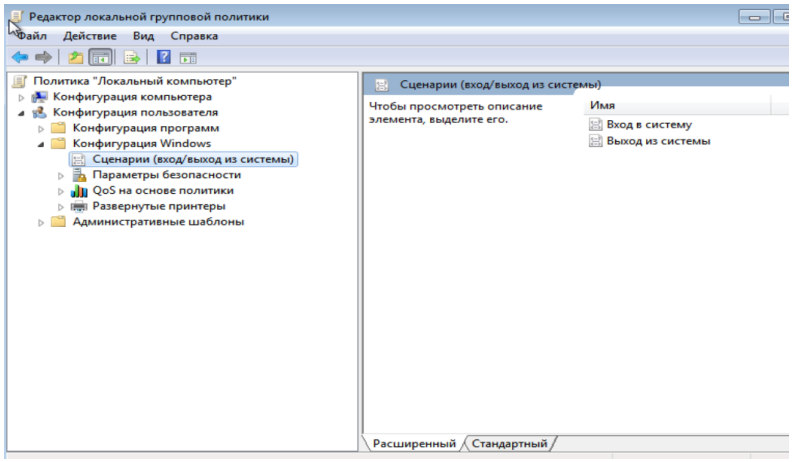


Рисунок 28 - Узел "Сценарии" оснастки "Конфигурация Windows"

Поскольку текущее АРМ представляет ценность для компании воспользуемся скриптом GetBackup.ps1 на языке PowerShell, который будет делать бэкап системы при каждом выходе пользователя из системы.

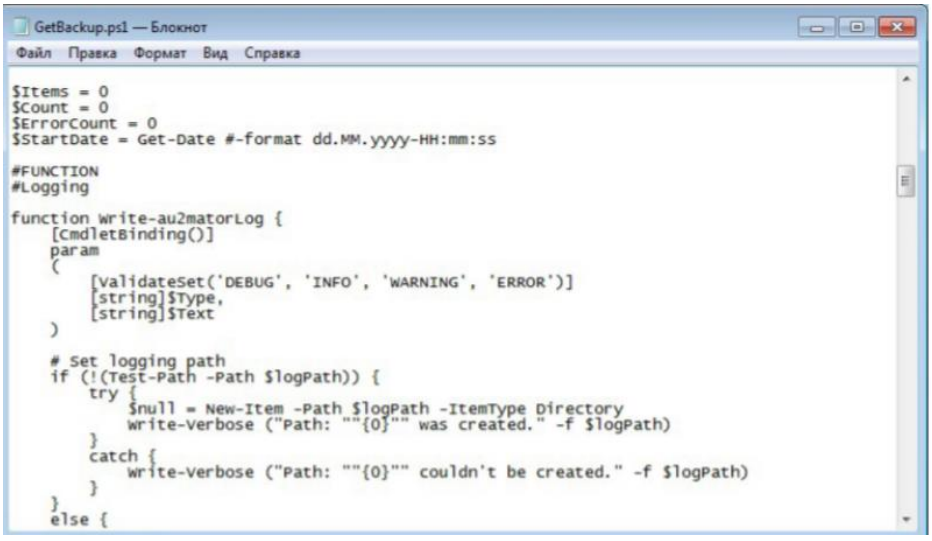


Рисунок 29 - Код скрипта "GetBackup.ps1"

Добавим скрипт *GetBackup.ps1* в сценарии событий входа и выхода из системы:

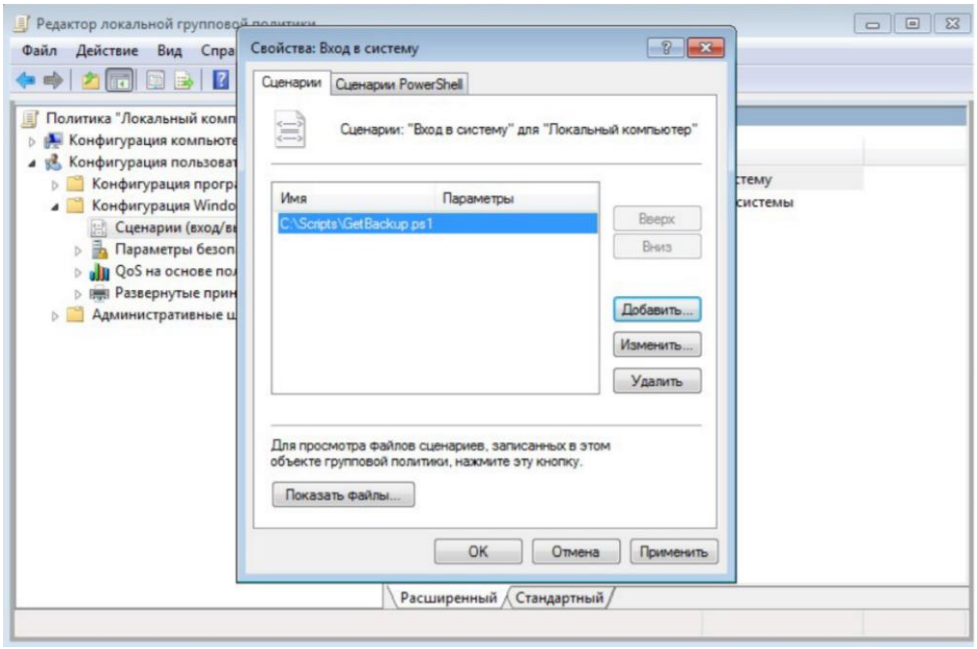


Рисунок 30 - Сценарий событий входа в систему

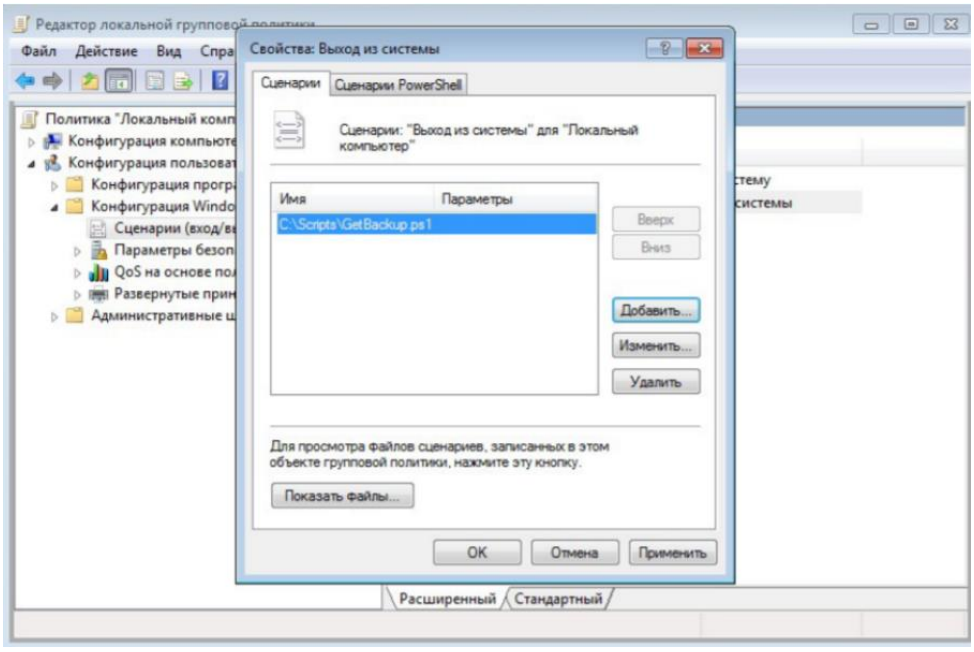


Рисунок 31 - Сценарий событий выхода из системы

3.4.2 Настройка дочернего узла «Административные шаблоны»

Перейдём к настройке узла "Административные шаблоны" .

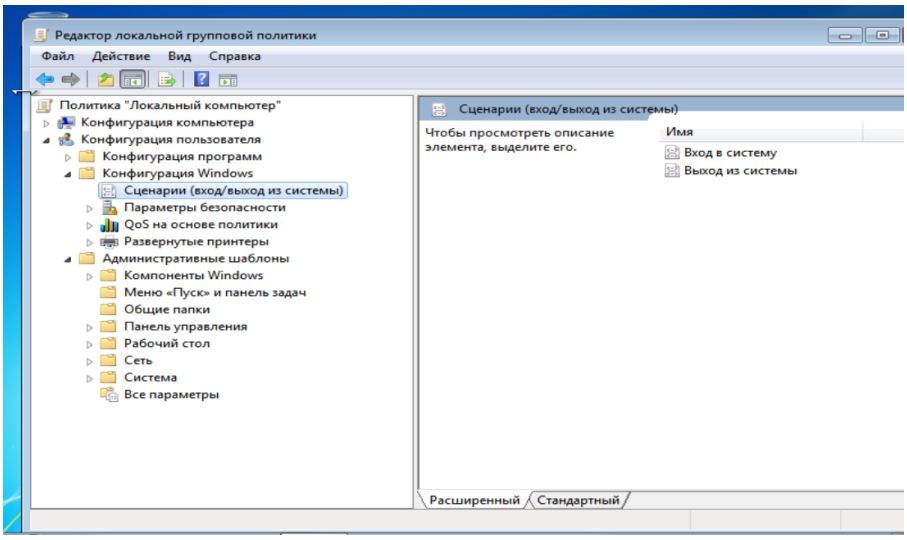


Рисунок 32 - Узел "Административные шаблоны"

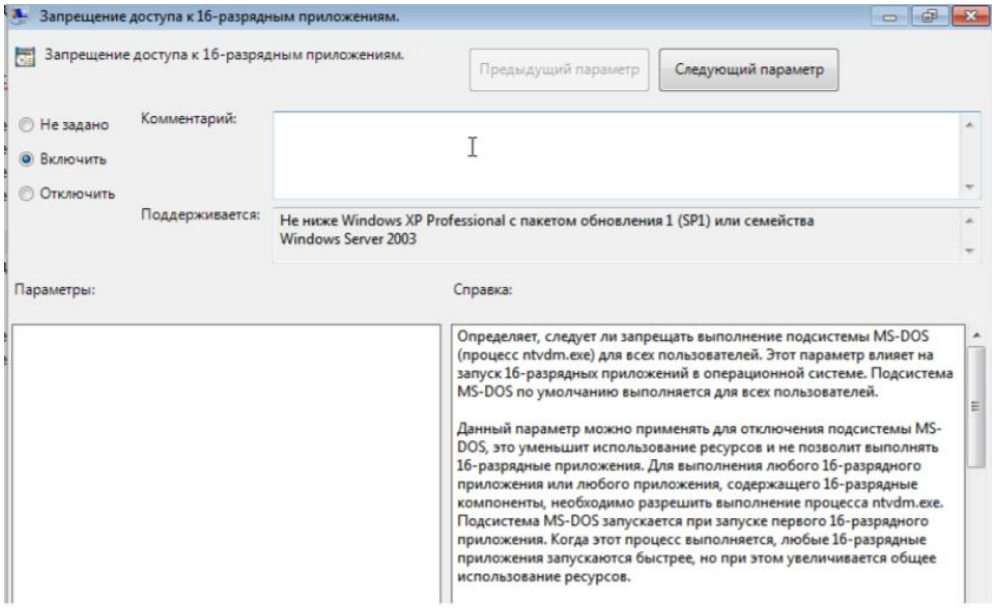


Рисунок 33 - Запрещение доступа к 16-разрядным приложениям

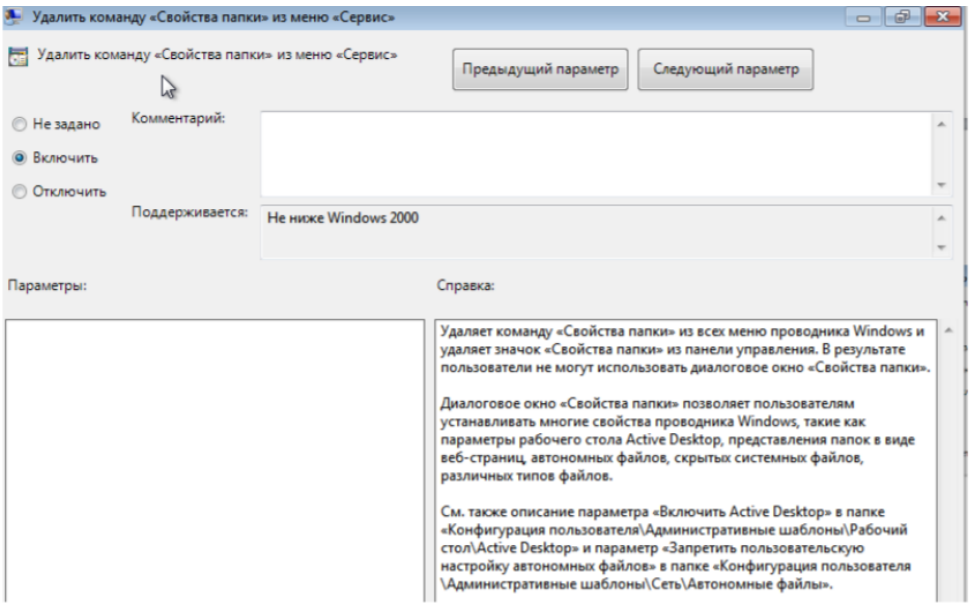


Рисунок 34 - Удалять команду "Свойства папки" из меню "Сервис"

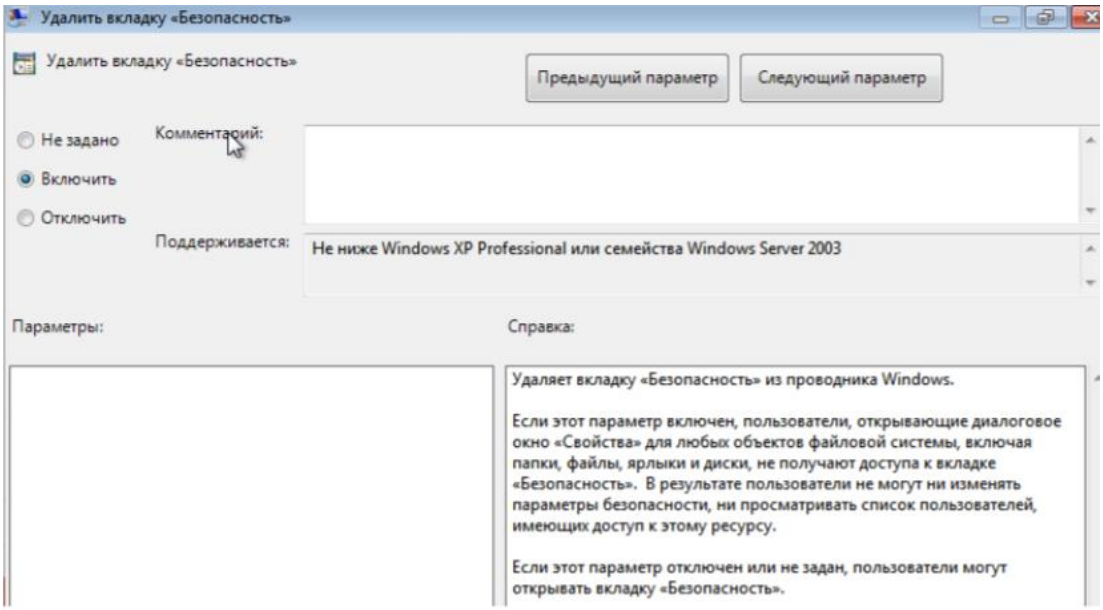


Рисунок 35 - Удалить вкладку "Безопасность"

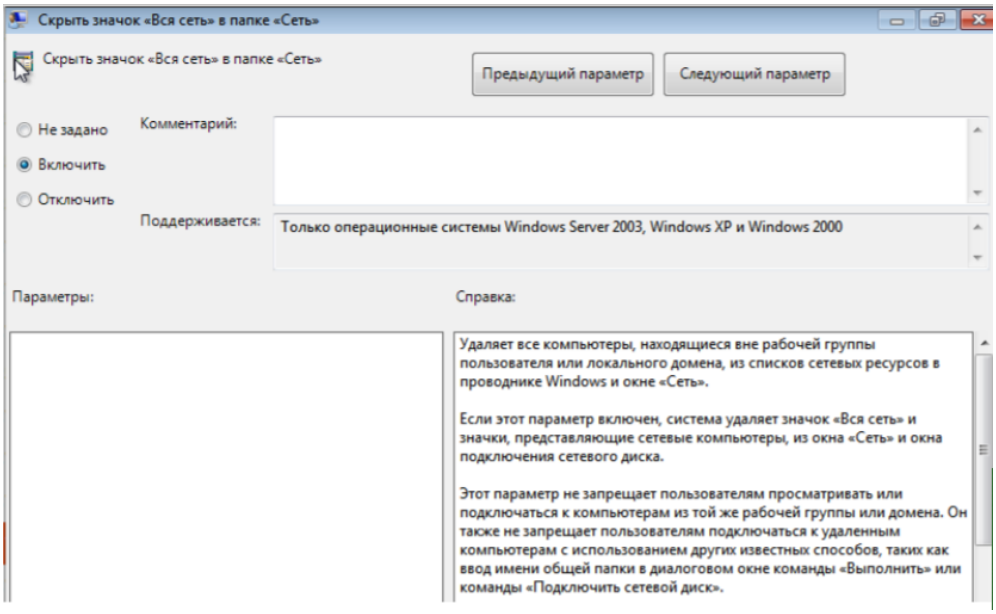


Рисунок 36 - Скрыть значок "Вся сеть" в папке "Сеть"

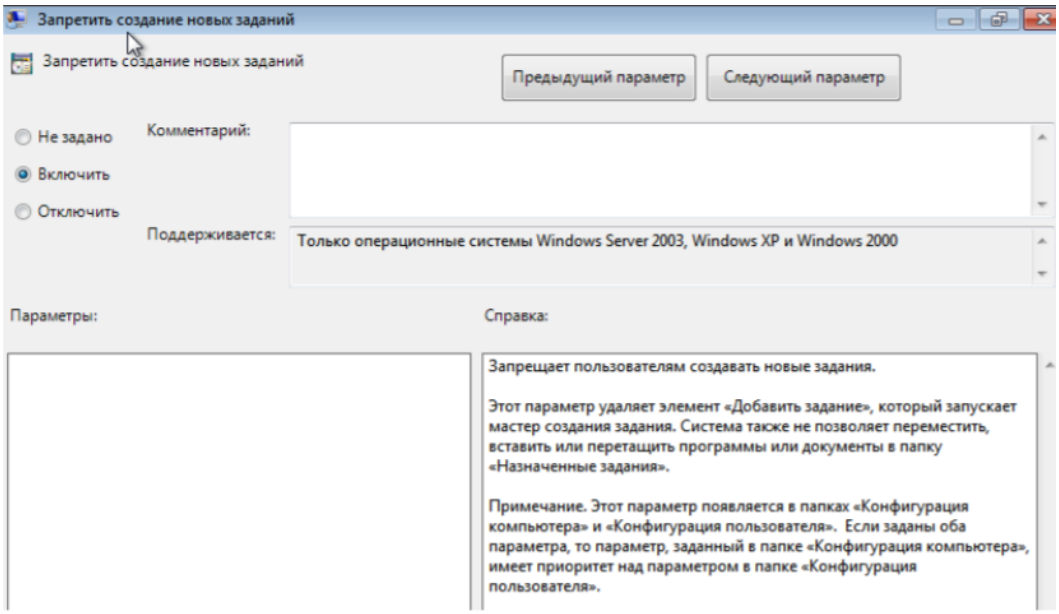


Рисунок 37 - Запретить создание новых заданий

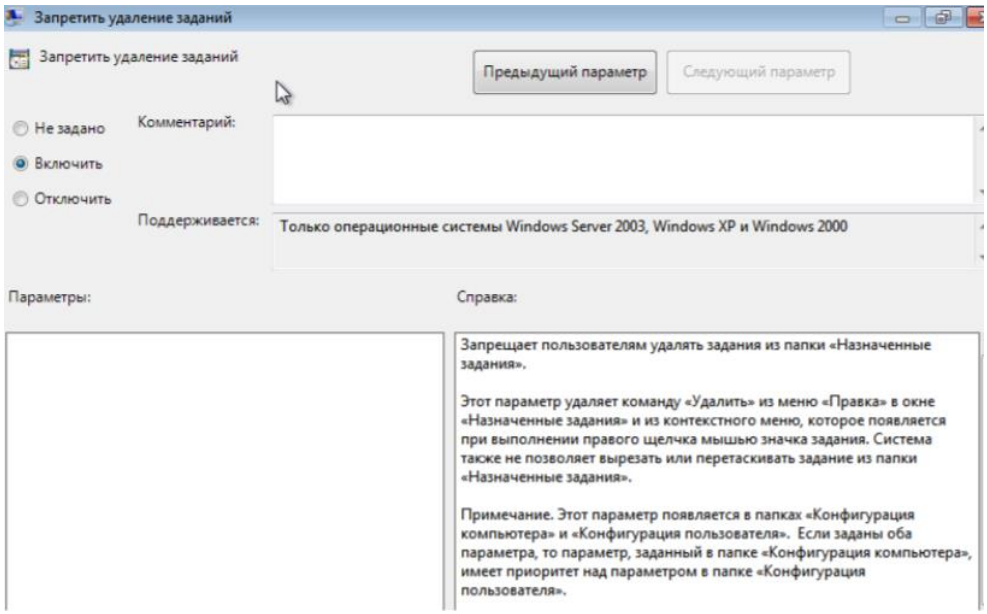


Рисунок 38 - Запретить удаление заданий

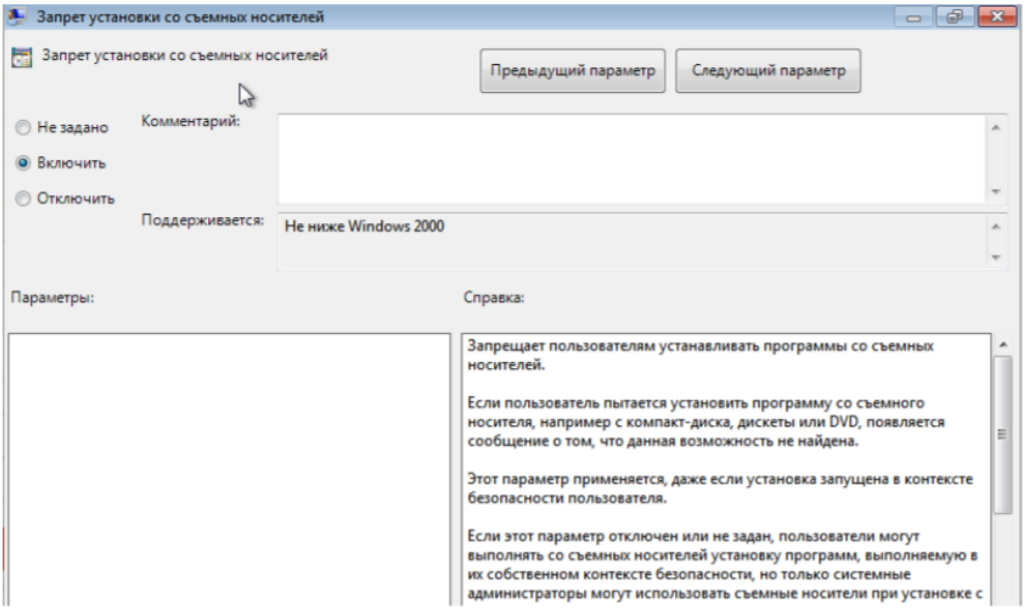


Рисунок 39 - Запрет установки со съёмных носителей

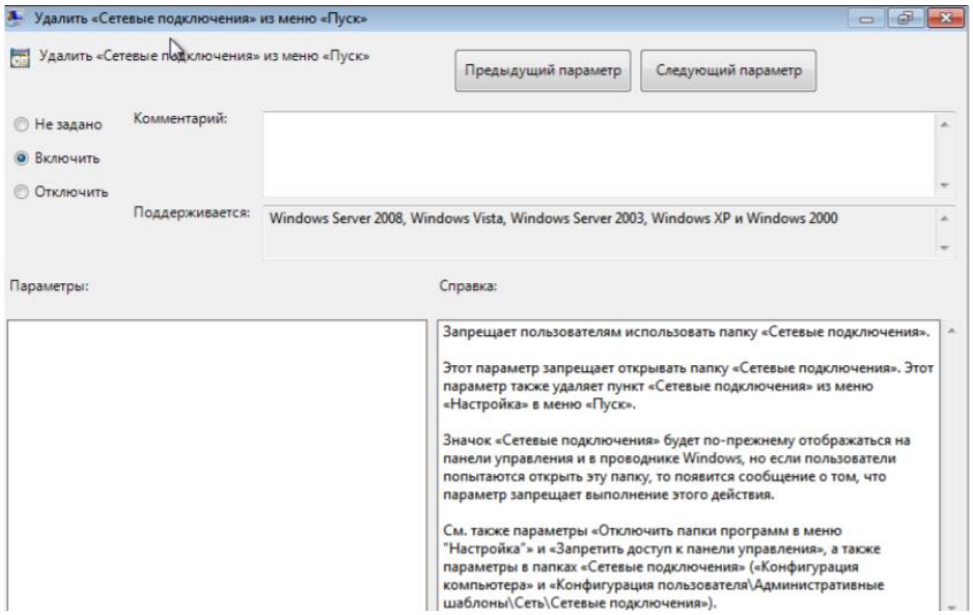


Рисунок 40 - Удалить "Сетевые подключения" из меню "Пуск"

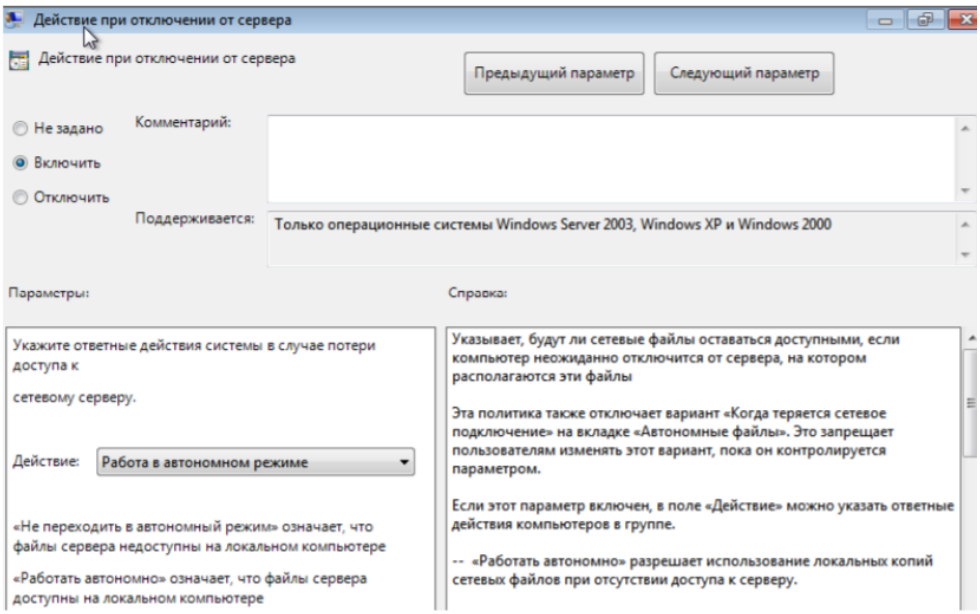


Рисунок 41 - Действия при отключении от сервера

4. Вывод

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 учётной записью пользователь вошёл 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.