Цель работы:

Изучить редактор локальной групповой политики и научиться настраивать групповые политики безопасности на автономном автоматизированном рабочем месте (АРМ) пользователя с установленной на нем операционной системой Windows XP для защиты информации от несанкционированного доступа (НСД).

Основные сведения:

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

Все групповые политики безопасности настраиваются в соответствии с требованиями варианта № 8 (3Б).

Класс защищенности 3Б предназначен для АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Требования к классу защищенности 3Б:

Подсистема управления доступом:

должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов.

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;

- должен проводиться учет всех защищаемых носителей информации с помощью их любой маркировки и с занесением учетных данных в журнал (учетную карточку).

Подсистема обеспечения целостности:

должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды.

При этом:

- целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ;

- целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ;

- должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;

- должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД;

- должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

Выполнение работы:

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

Пуск → Выполнить → gpedit.msc → Групповая политика → Конфигурация компьютера → Конфигурация Windows → Сценарии

С помощью этой оснастки запускаются различные файлы скриптов при загрузке/завершении работы компьютера. Создадим скрипт на языке PowerShell, подсчитывающий количество и размер файлов на диске C и во всех содержащихся в нем папках и подпапках:

```
Get-ChildItem -Path C:\ -Recurse -Force | where ($_.psIscontainer) foreach {
    $count = Get-ChildItem $_.fullname -Recurse | where ($_.length) | Measure-Object -property length -Sum
    Write-Host($_.fullname)
    $size = '{0:F}' -f (($count.Sum)/1024)/1024)
    Write-Host("Files: " + $count.count)
    Write-Host("Size: " + $size)
    '"' + $_.fullname + '","' + $count.count + '","' + $size + '"' | Out-File C:\counter.csv -Apppend
}
```

Рис. 1 – скрипт на языке PowerShell

Укажем в настройках сценариев, что данный скрипт необходимо запускать и при загрузке компьютера и при его выключении. Таким образом, собранные с его помощью данные помогут определить, какие изменения внес пользователь во время своей работы, а какие были внесены во время его отсутствия потенциальным злоумышленником. Это поможет увеличить безопасность информационной системы.

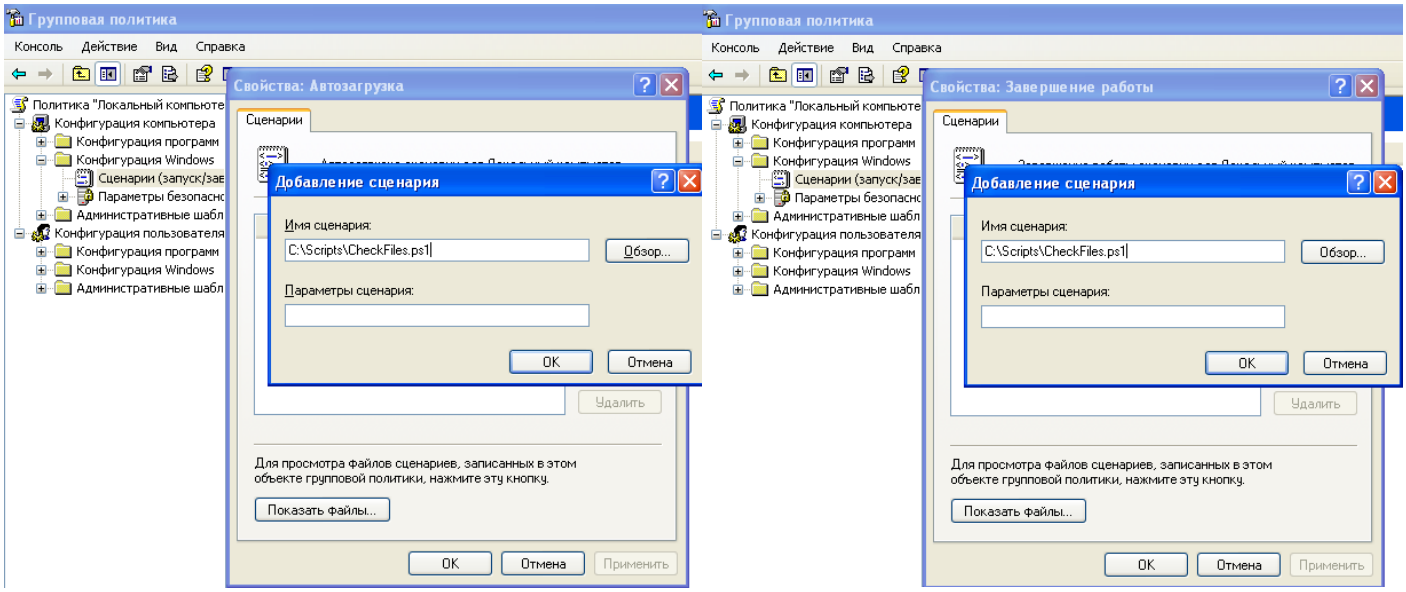

Рис. 2 – настройка сценариев при загрузке и выключении

Пуск → Выполнить → gpedit.msc → Групповая политика → Конфигурация компьютера → Конфигурация Windows → Параметры безопасности → Политики безопасности IP на «Локальный компьютер».

Для пункта «Клиент (Ответ только)» уже используется политика, запрещающая все запросы пользователя и разрешающая только отправлять ответы имеющимся на предприятии серверам. Также там уже указано использование протокола проверки подлинности Kerberos для повышения безопасности. Такие параметры нам подходят, поэтому оставляем их.

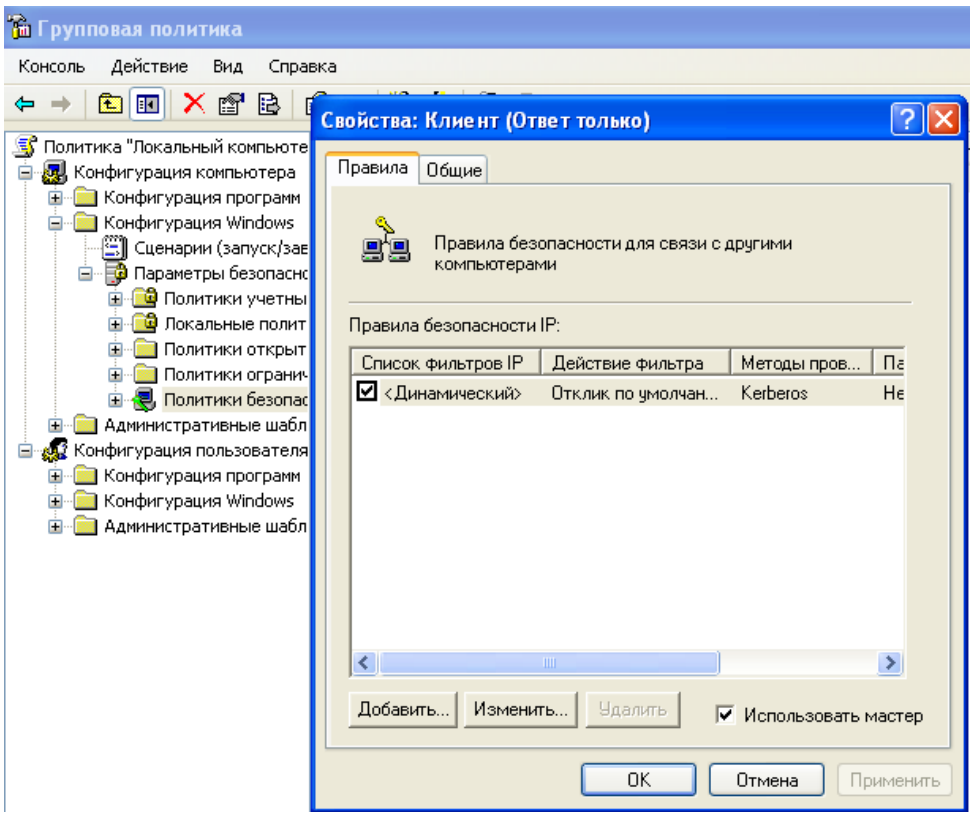

Рис. 3 – настройка пункта «Клиент (Ответ только)»

В разделе «Сервер (Запрос безопасности)» установим для подпункта ICMP-трафика использование запроса безопасности, такая настройка повышает безопасность сети. Методы проверки осуществляются с помощью Kerberos, поэтому эти пункты не требуют дополнительной настройки.

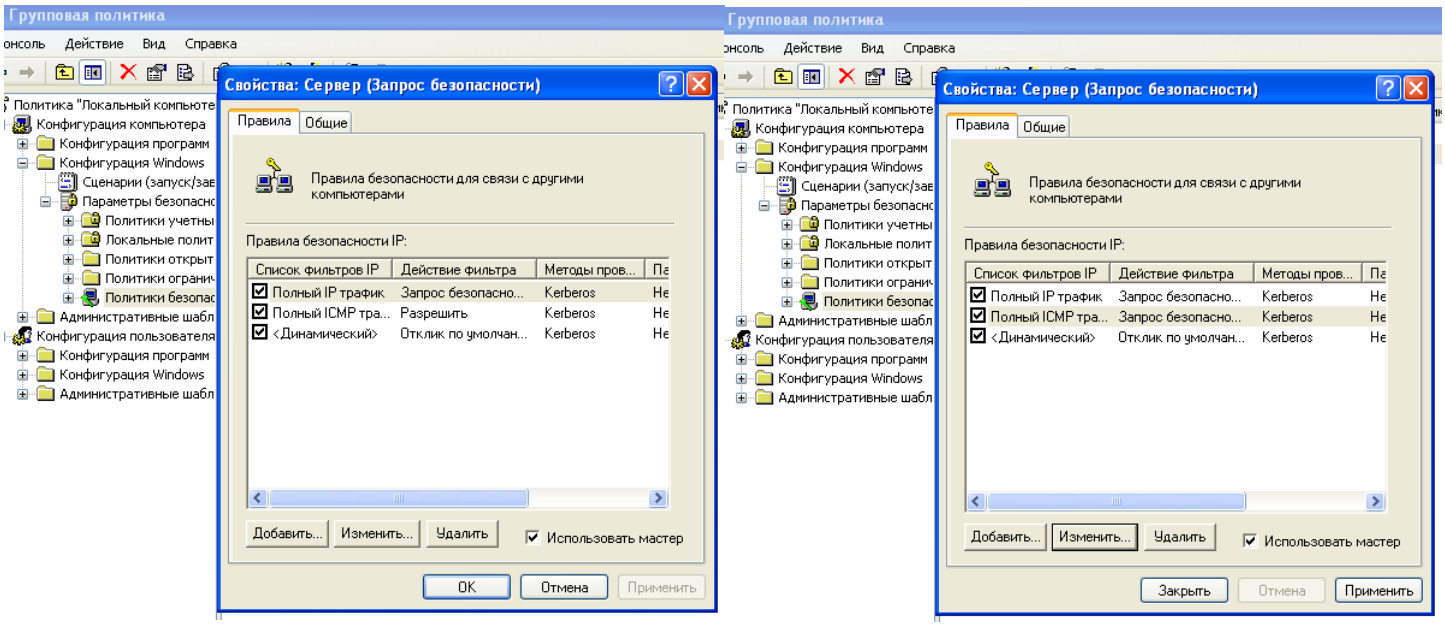

Рис. 4 – настройки «Сервер (Запрос безопасности)» «до» и «после»

В разделе «Сервер безопасности (Требуется безопасность)» установим для подпункта ICMP-трафика фильтр «Требуется безопасность», что также при использовании должно повысить безопасность сети.

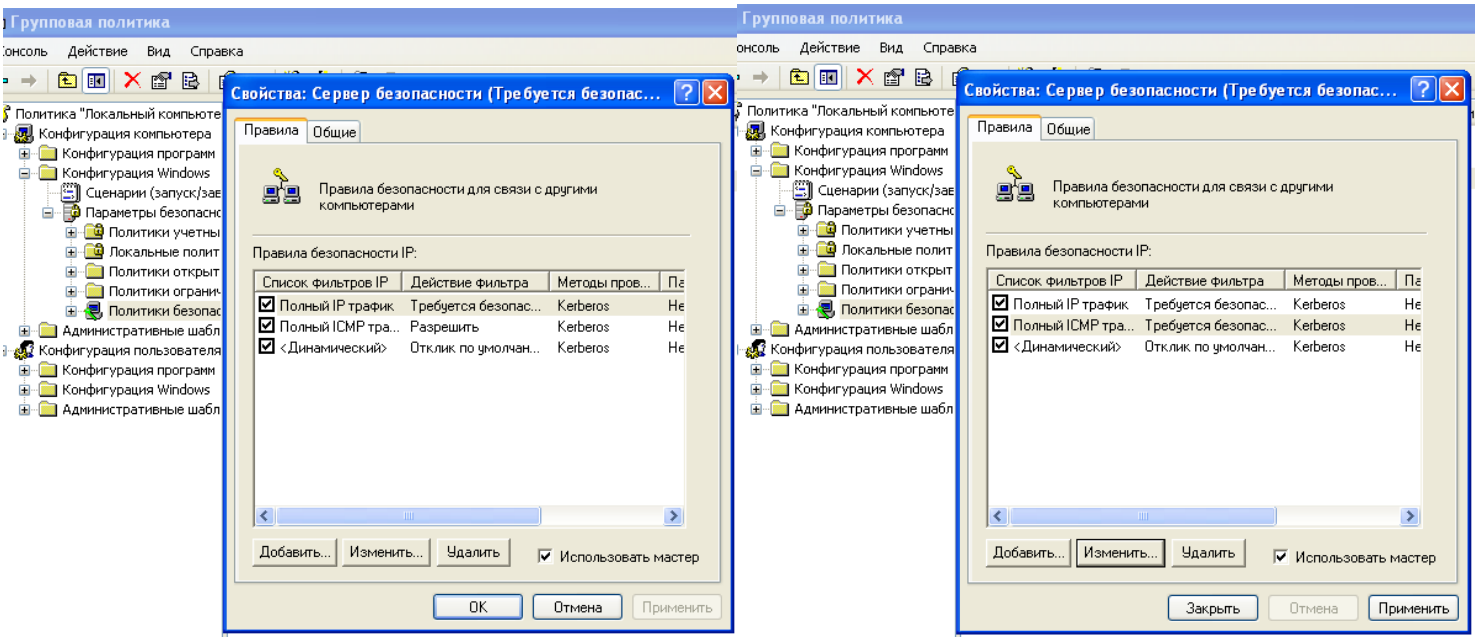

Рис. 5 – настройки «Сервер безопасности (Требуется безопасность)» «до» и «после»

В процессе настройки дочернего узла «Конфигурация Windows» в «Конфигурации компьютера» были настроены сценарии, которые будут выполняться при автозапуске и завершении работы Windows, и позволят собирать информацию о действиях пользователя в течении дня. Была настроена «Политики безопасности IP» на «Локальный компьютер» для повышения защиты информации, обрабатываемой АРМ, и для ограничения пользователю доступа к сети Internet.

Данные настройки обеспечивают требования к системе с классом защищенности 3Б, а именно требования о контроле доступа субъектов в систему, и о регистрации и учете действий пользователей в системе.

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

Пуск → Выполнить → gpedit.msc → Групповая политика → Конфигурация компьютера → Административные шаблоны → Компоненты Windows → NetMeeting → Запретить удаленное управление рабочим столом.

Для рассматриваемого АРМ нет необходимости в удаленном управлении рабочим столом. Такая возможно ставит под угрозу всю сеть. Поэтому для данной оснастки установим значение «Включен».

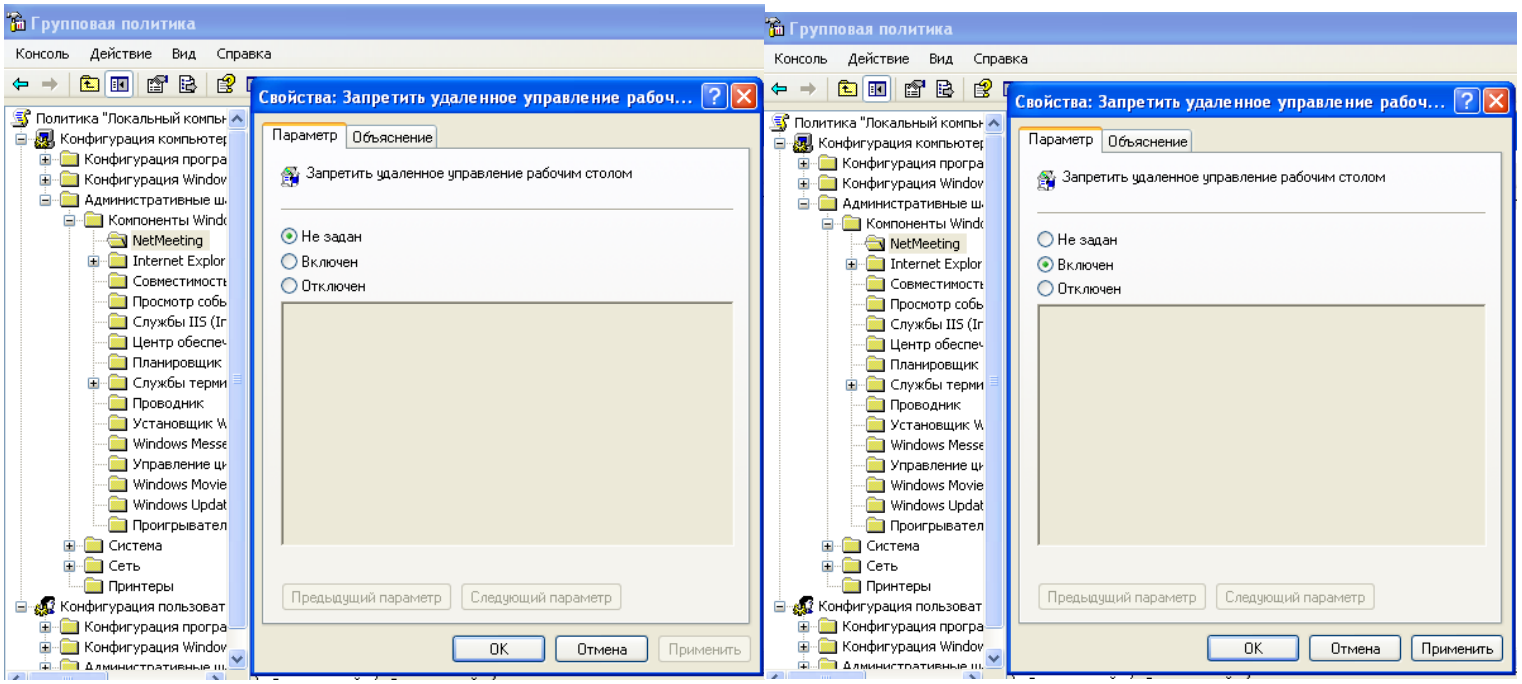

Рис. 6 – настройки «Запретить удаленное управление рабочим столом» «до» и «после»

Пуск → Выполнить → gpedit.msc → Групповая политика → Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Службы терминалов → Разрешать удаленное подключение с использованием служб терминалов.

Для рассматриваемого АРМ нет необходимости в удаленном подключении с использованием служб терминалов. Такая возможно ставит под угрозу всю сеть. Поэтому для данной оснастки установим значение «Отключен».

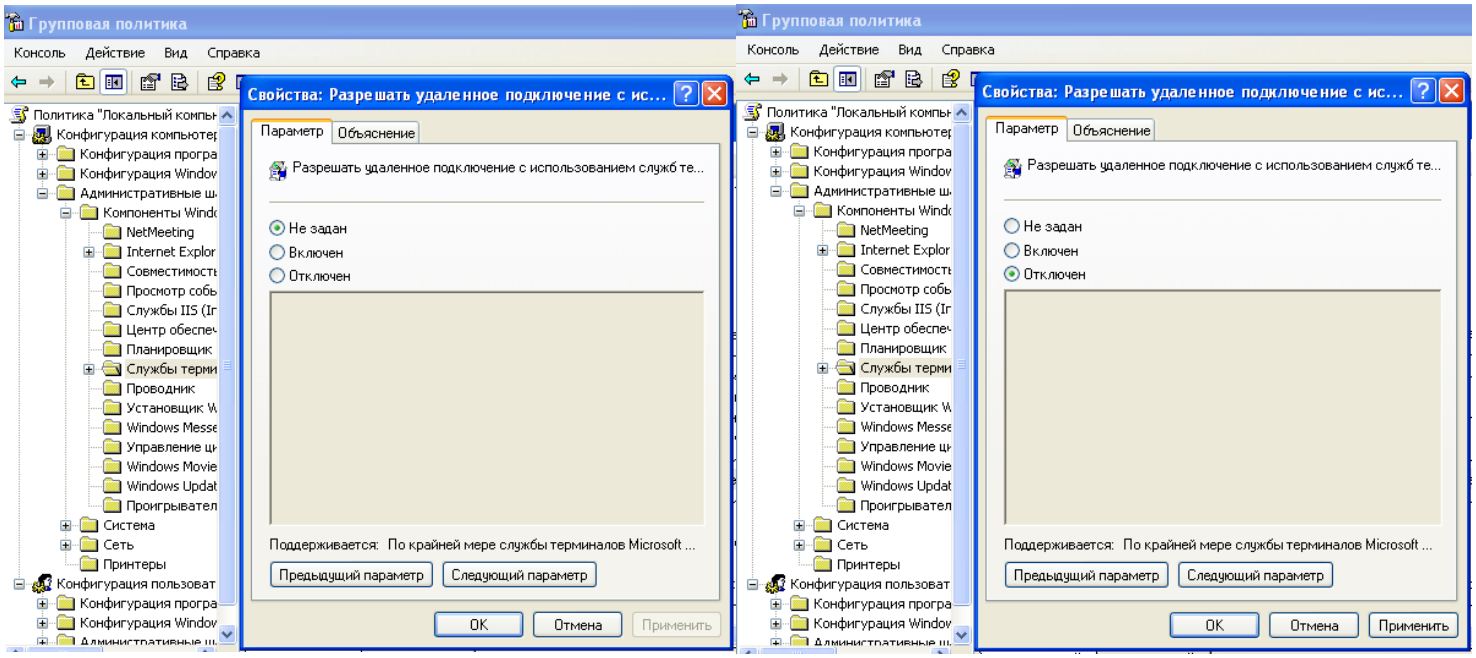

Рис. 7 – настройки «Разрешать удаленное подключение с использованием служб терминалов» «до» и «после»

Пуск → Выполнить → gpedit.msc → Групповая политика → Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Совместимость приложений → Выключить журнал событий справки приложения.

Для оснастки «Выключить журнал событий справки приложения» установим значение «Включен». Это поможет отслеживать запуск приложений – как уже установленных на АРМ, так и загруженных с некоторого носителя. Данная настройка не спасет систему от урона, который может быть нанесен при запуске опасных приложений, но позволит при расследовании понять, что послужило отправной точкой атаки.

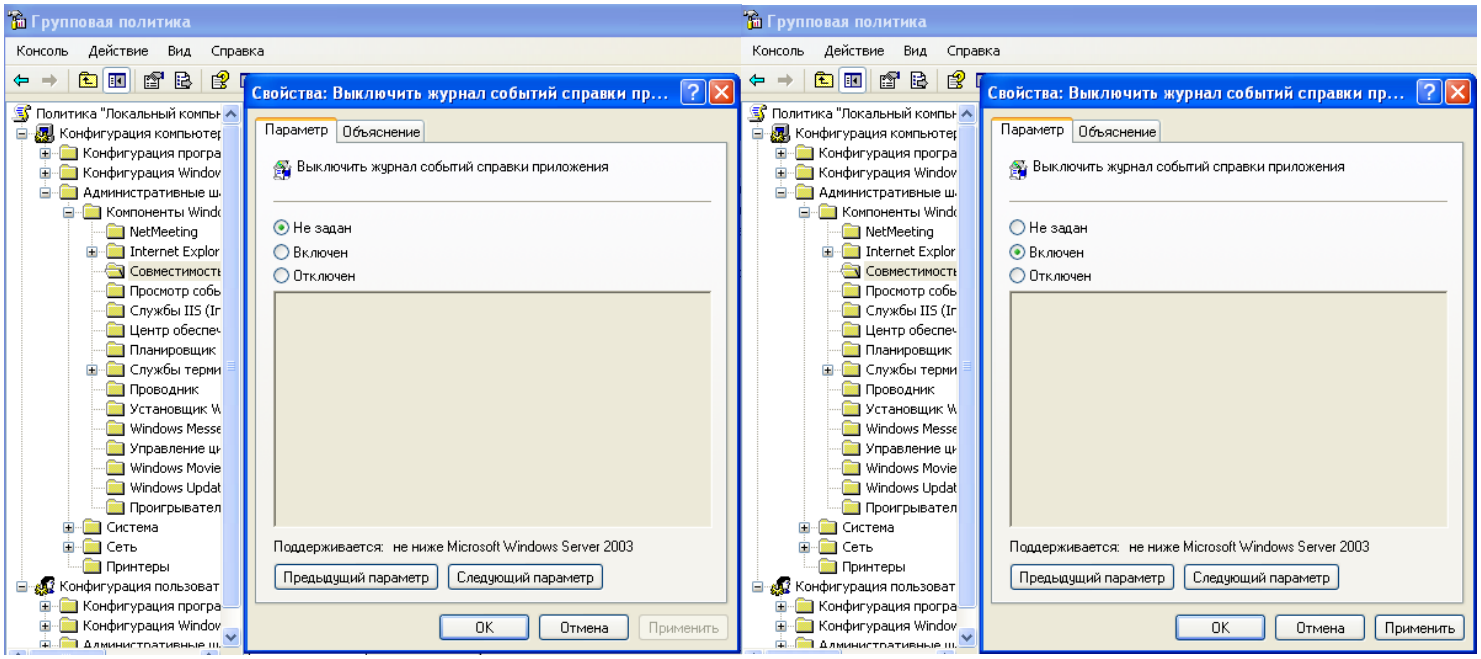

Рис. 8 – настройки «Выключить журнал событий справки приложения» «до» и «после»

Пуск → Выполнить → gpedit.msc → Групповая политика → Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Совместимость приложений → Предотвращение доступа к 16-разрядным приложениям.

16-разрядные приложения могут неправильно функционировать в современных операционных системах с разрядностью 32 и 64 бита, это может привести к сбоям в работе системы. Более того, такие приложения может использовать злоумышленник, ведь их защита на сегодняшний день оставляет желать лучшего. Поэтому для данной оснастки установим значение «Включен».

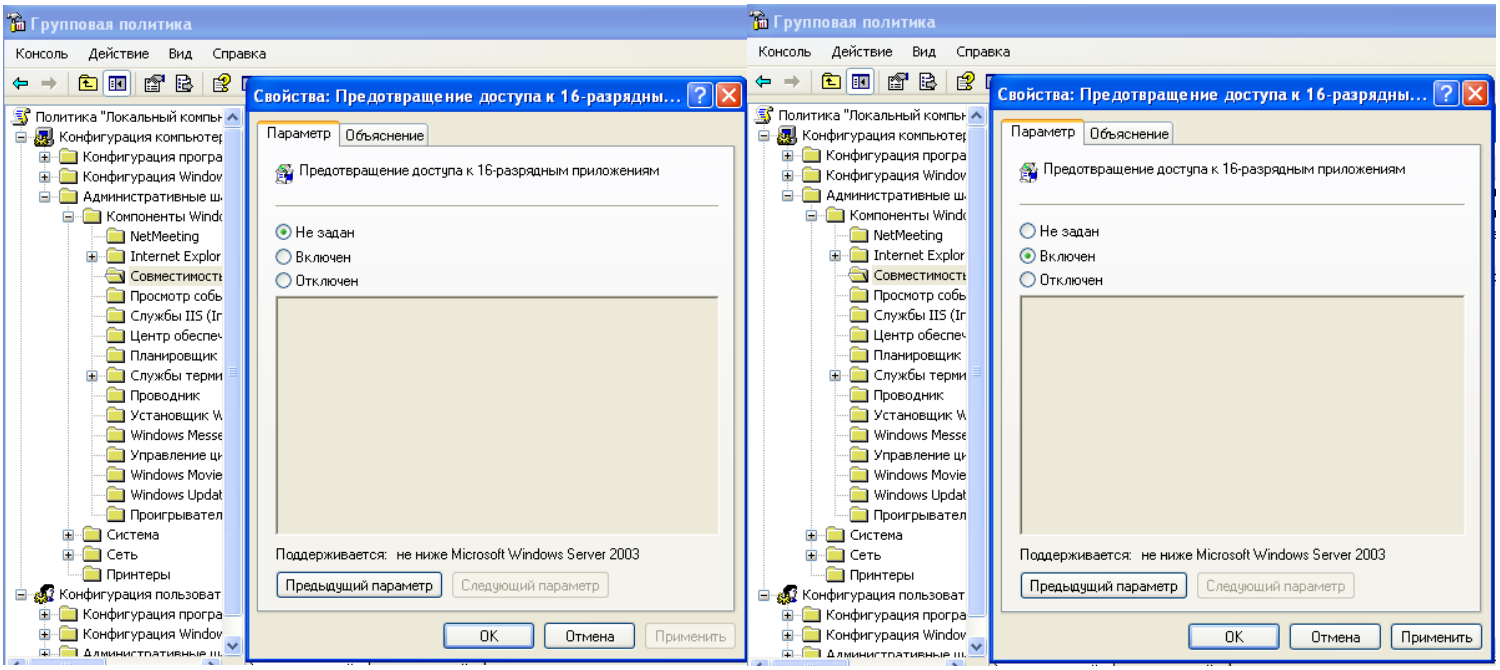

Рис. 9 – настройки «Предотвращение доступа к 16-разрядным приложениям» «до» и «после»

Пуск → Выполнить → gpedit.msc → Групповая политика → Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Центр обеспечения безопасности → Включить «Центр обеспечения безопасности».

Использование центра обеспечения безопасности поможет повысить безопасность средствами операционной системы. Поэтому для данной оснастки установим значение «Включен».

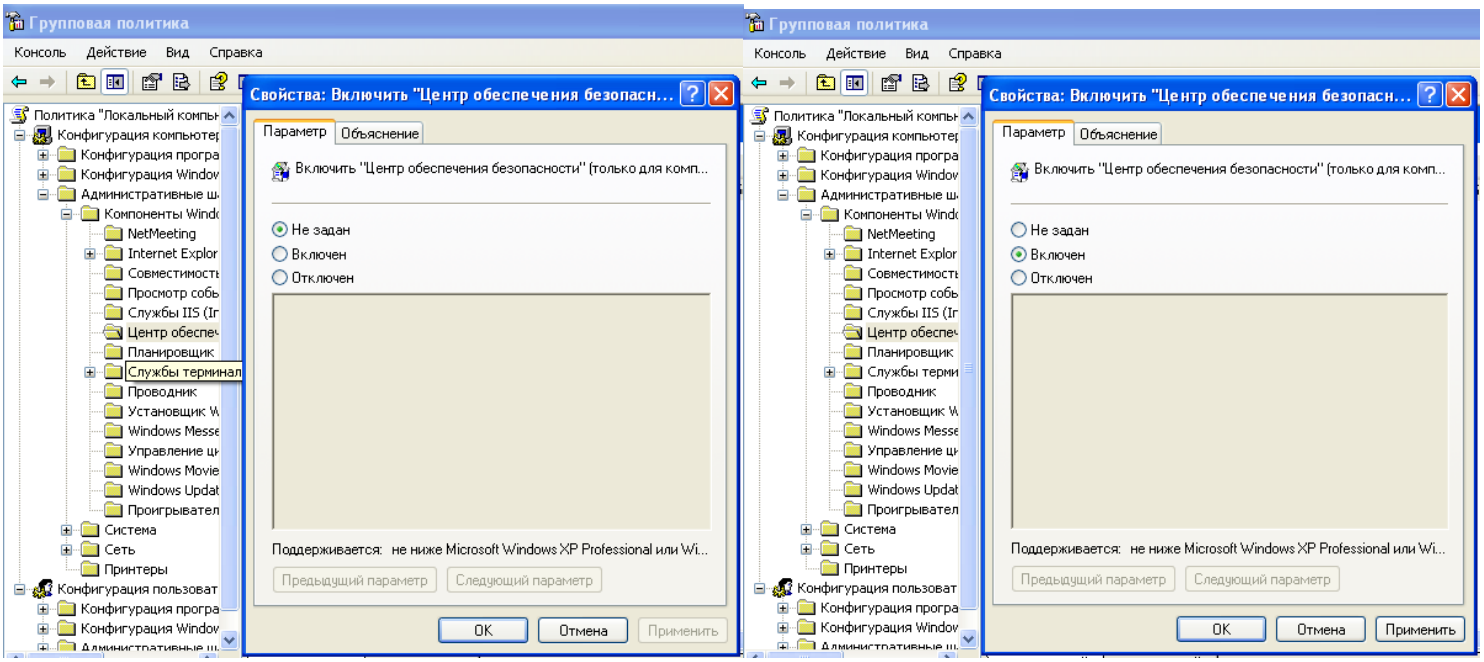

Рис. 10 – настройки «Включить «Центр обеспечения безопасности»» «до» и «после»

Пуск → Выполнить → gpedit.msc → Групповая политика → Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Планировщик заданий → Запретить удаление заданий.

Задания могут использоваться для обеспечения безопасности АРМ, а их удаление может повлечь за собой ослабление безопасности. Поэтому для данной оснастки установим значение «Включен».

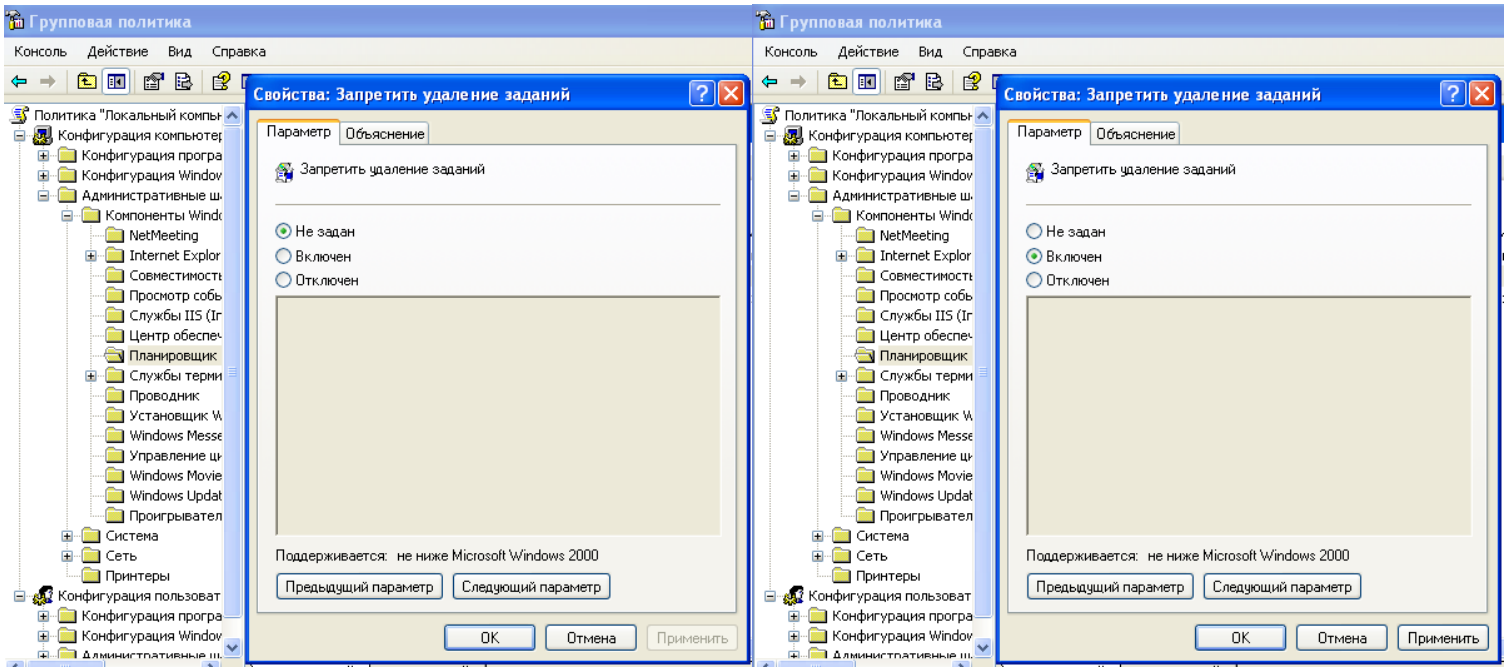

Рис. 11 – настройки «Запретить удаление заданий» «до» и «после»

Пуск → Выполнить → gpedit.msc → Групповая политика → Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Службы терминалов → Удалить элемент «Безопасность Windows» из меню Пуск.

Нарушить систему защиты может как неумелый пользователь, так и злоумышленник. Поэтому целесообразно затруднить действия нарушителя, установив для данной оснастки значение «Включен».

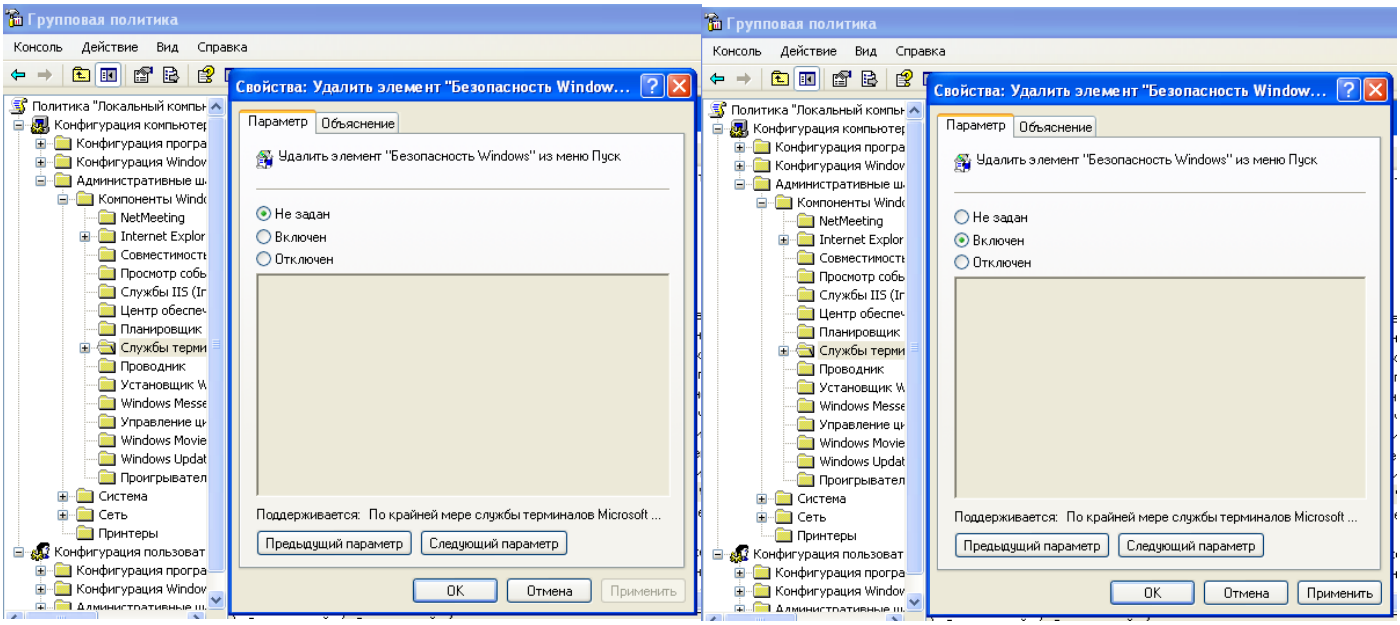

Рис. 12 – настройки «Удалить элемент «Безопасность Windows» из меню Пуск» «до» и «после»

Пуск → Выполнить → gpedit.msc → Групповая политика → Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Проводник → Отключить защищенный режим протокола оболочки.

Защищенный режим протокола оболочки запретит пользователю доступ к некоторым папкам и приложениям, имеющим особую важность для безопасности системы. Поэтому для данной оснастки установим значение «Отключен».

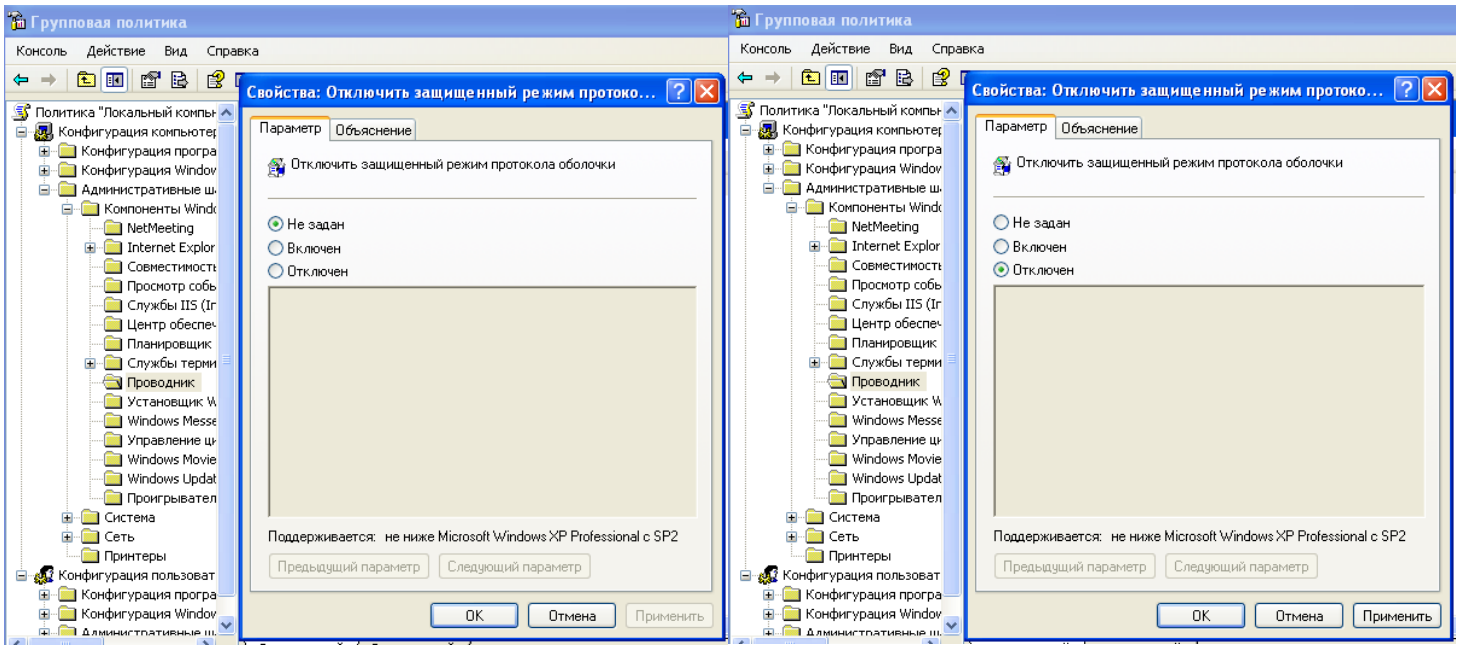

Рис. 13 – настройки «Отключить защищенный режим протокола оболочки» «до» и «после»

Пуск → Выполнить → gpedit.msc → Групповая политика → Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Установщик Windows → Ведение журнала.

Ведение журнала – это очень важная задача, ведь такой журнал позволяет своевременно реагировать на опасные действия пользователей или нарушителей, а также проводить расследования. Поэтому для оснастки «Ведение журнала» установим значение «Включен» и укажем, что в журнал необходимо заносить абсолютно все события.

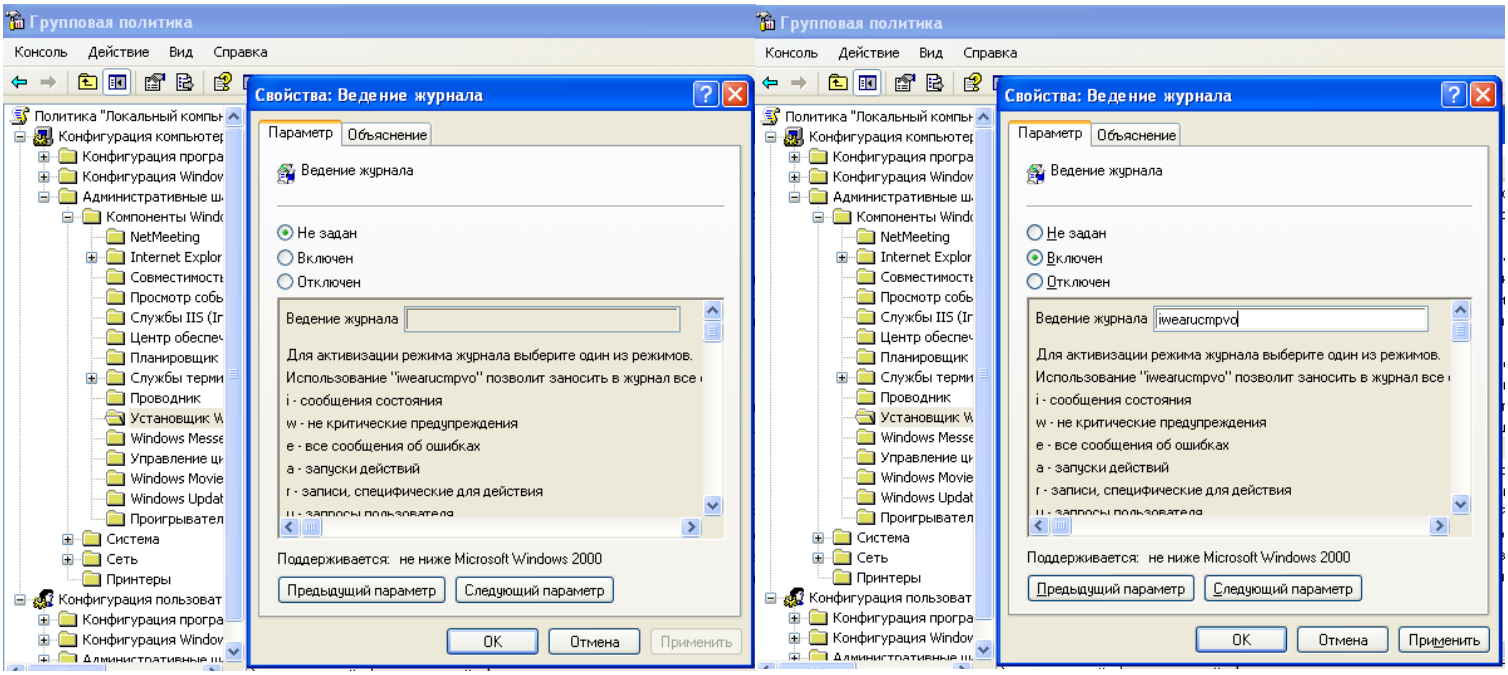

Рис. 14 – настройки «Ведение журнала» «до» и «после»

Пуск → Выполнить → gpedit.msc → Групповая политика → Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Windows Update → Настройка автоматического обновления.

Автоматическое обновление операционной системы позволяет вовремя исправлять ошибки и уязвимости системы, следовательно, лучше активировать данную возможность. Для оснастки «Настройка автоматического обновления» установим значение «Включен» и укажем, что загружать и устанавливать обновления необходимо автоматически, каждый день в 19:00. Так как к 18:00 рабочий день обычно заканчивается, в 19:00 у пользователей точно не будет нужды в использовании компьютеров.

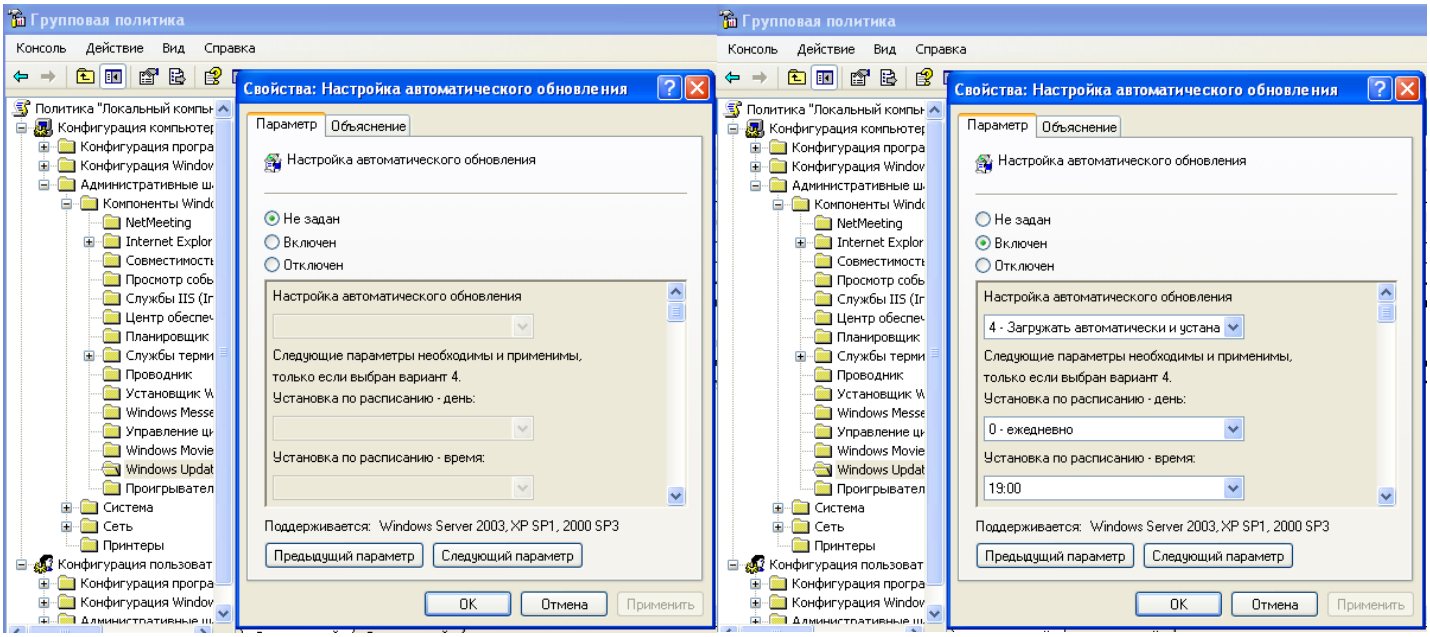

Рис. 15 – настройки «Настройка автоматического обновления» «до» и «после»

В процессе настройки дочернего узла «Административные шаблоны» в «Конфигурации компьютера» были произведены действия, направленные на повышение защищенности АРМ. Запрещены удаленное управление рабочим столом, удаленное подключение с использованием служб терминалов, запуск 16-разрядных приложений и удаление заданий. Включен журнал справки приложения, центр обеспечения безопасности и защищенный режим протокола оболочки. Удален элемент «Безопасность Windows» из меню Пуск. Настроено ведение журнала запуска и установки приложений, настроено автоматическое обновление системы.

Данные настройки обеспечивают требования к системе с классом защищенности 3Б, а именно требования о целостности программных средств и неизменности программной среды. Также повышается общий уровень защищенности системы.

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

Пуск → Выполнить → gpedit.msc → Групповая политика → Конфигурация пользователя → Конфигурация Windows → Сценарии.

С помощью этой оснастки запускаются различные файлы скриптов при входе пользователя в систему или при выходе из нее. Создадим скрипт, удаляющий файлы, которые старше 3 месяцев. Он будет запускаться при выходе из системы. Также создадим скрипт для получения сведений о сеансах входа в систему, и скрипт для получения сведений о

пользователе, который выполнил вход в компьютер. Эти скрипты будут запускаться при входе в систему.

```
$date = (Get-Date).AddMonths(-3)
Get-ChildItem -Path D:\Files\Common | where {!$_.PSIsContainer} |
foreach {
   if ($_.LastWriteTime -lt $date) {
      Remove-Item $_ -whatif
   }
}
```

Рис. 16 – скрипт для удаления старых файлов

```
Get-CimInstance -ClassName Win32_LogonSession
```

Рис. 17 – скрипт для получения сведений о сеансах входа в систему

```
Get-CimInstance -ClassName Win32_ComputerSystem -Property UserName
```

Рис. 18 – скрипт для получения сведений о пользователях, вошедших в систему

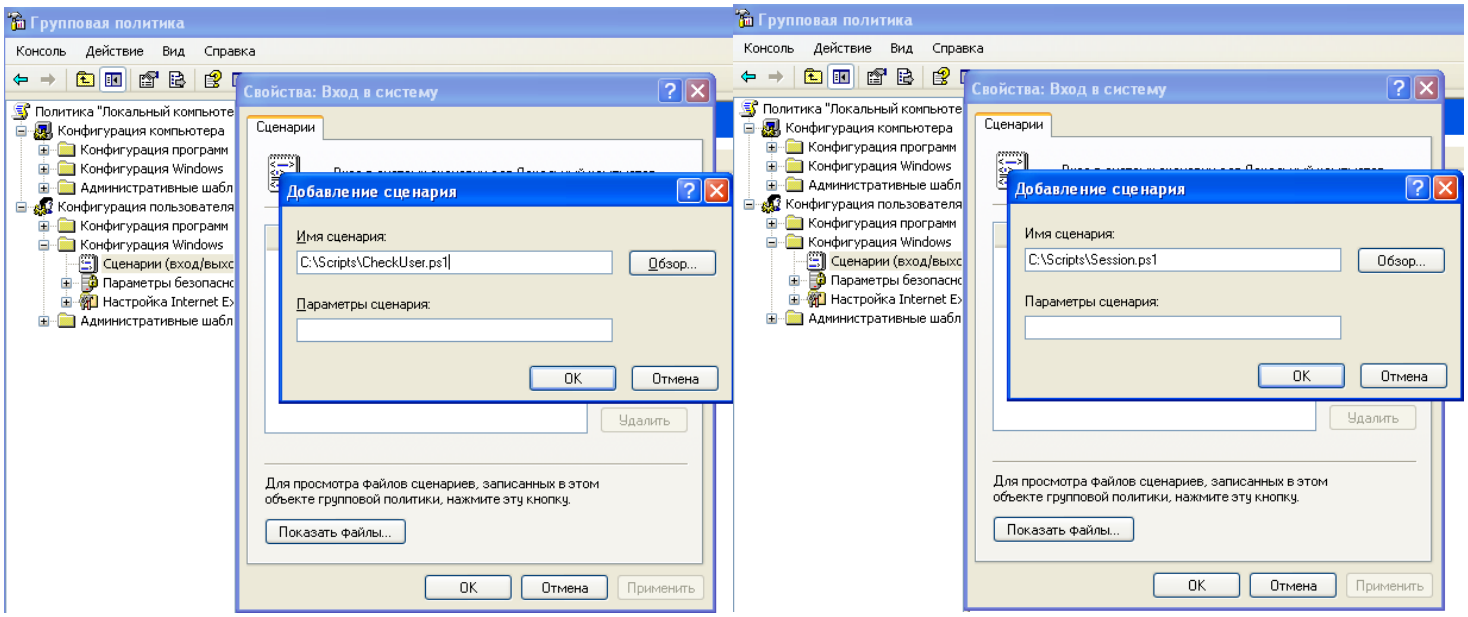

Рис. 19 – настройки выполнения сценария при входе в систему

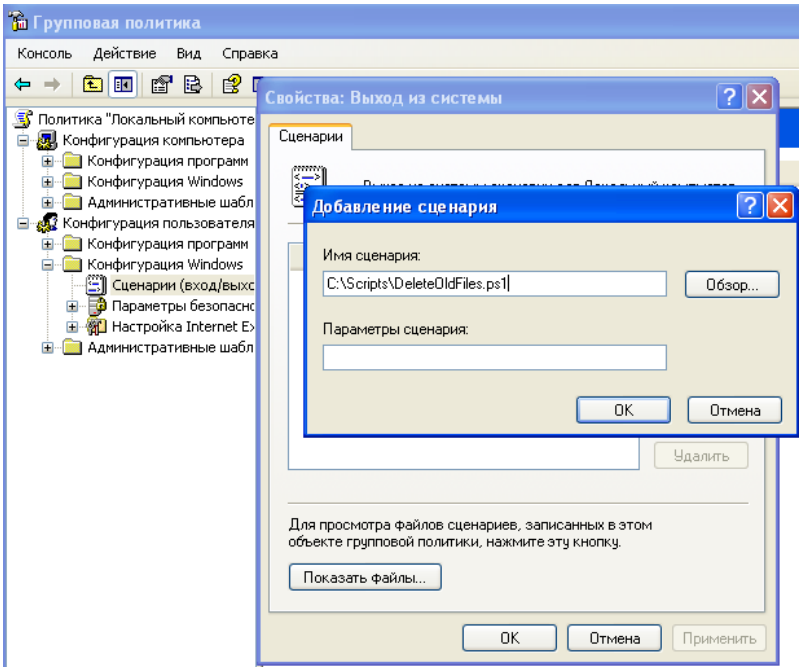

Рис. 20 – настройки выполнения сценария при выходе из системы

В процессе настройки дочернего узла «Конфигурация Windows» в «Конфигурации пользователя» были настроены сценарии, которые будут выполняться при входе в систему и выходе из нее.

Данные настройки обеспечивают требования к системе с классом защищенности 3Б, а именно требования о контроле доступа субъектов в систему. Также был повышен общий уровень защищенности системы.

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

Пуск → Выполнить → gpedit.msc → Групповая политика → Конфигурация пользователя → Административные шаблоны → Компоненты Windows → Совместимость приложений → Предотвращение доступа к 16-разрядным приложениям.

16-разрядные приложения могут неправильно функционировать в современных операционных системах с разрядностью 32 и 64 бита, это может привести к сбоям в работе системы. Более того, такие приложения может использовать злоумышленник, ведь их защита на сегодняшний день оставляет желать лучшего. Поэтому для данной оснастки установим значение «Включен».

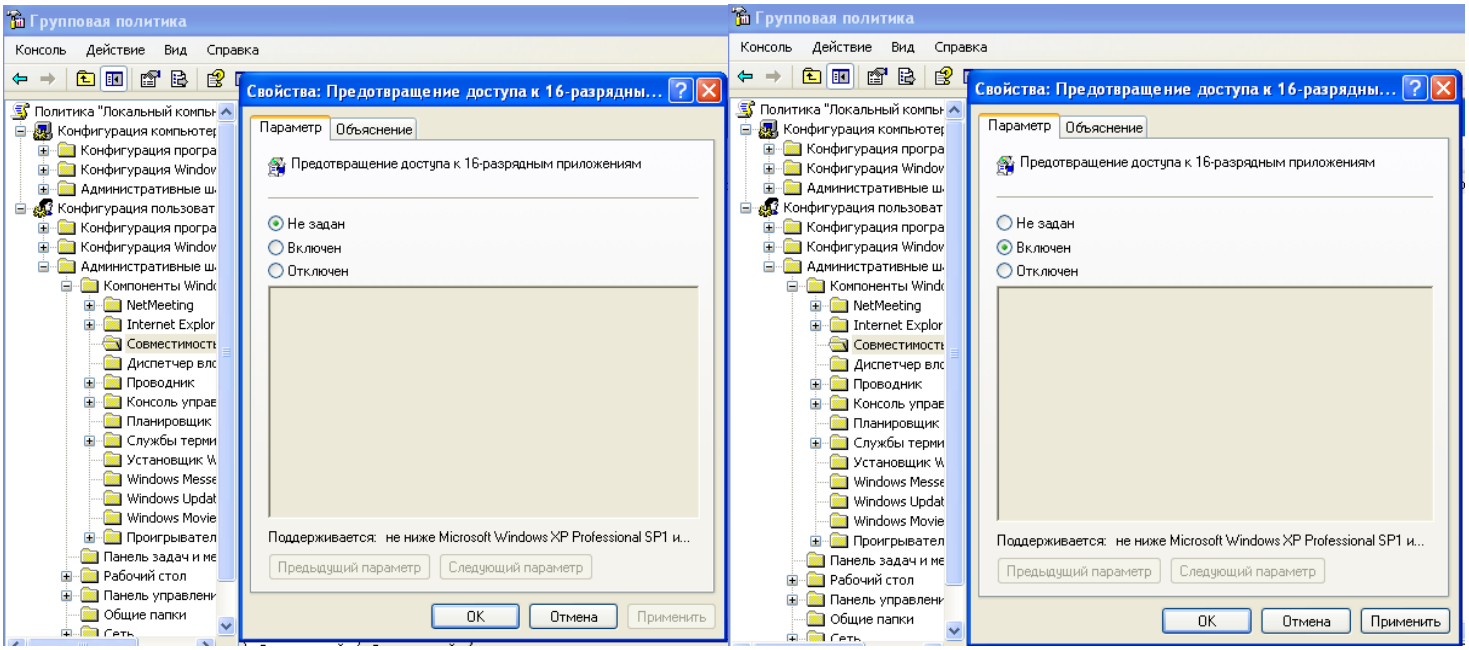

Рис. 22 – настройки «Подтверждение доступа к 16-разрядным приложениям» «до» и «после»

Пуск → Выполнить → gpedit.msc → Групповая политика → Конфигурация пользователя → Административные шаблоны → Компоненты Windows → Проводник → Удалить команду «Свойства папки» из меню «Сервис».

С помощью изменения свойств папки пользователь может настроить отображение скрытых системных файлов, чье изменение может повлечь за собой серьезные проблемы в системе, потому необходимо убрать эту возможность. Для этого у данной оснастки установим значение «Включен».

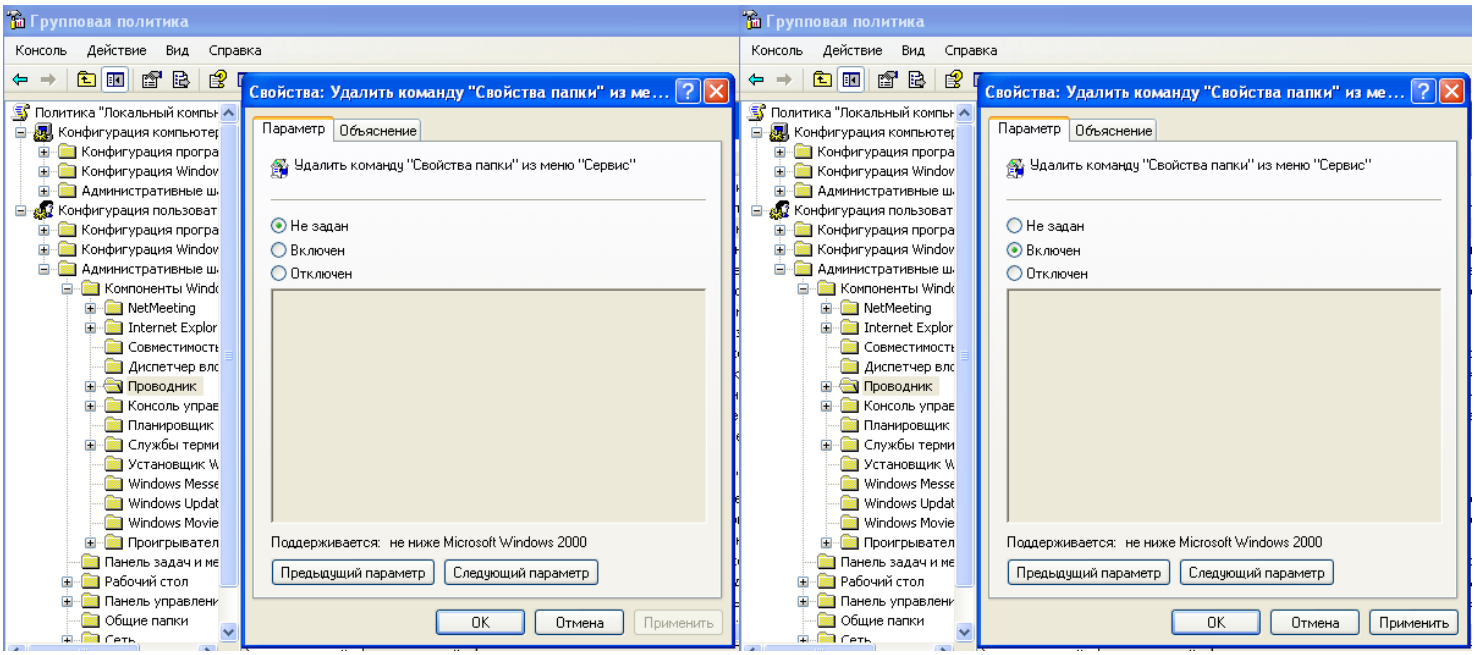

Рис. 23 – настройки «Удалить команду «Свойства папки» из меню «Сервис»» «до» и «после»

Пуск → Выполнить → gpedit.msc → Групповая политика → Конфигурация пользователя → Административные шаблоны → Компоненты Windows → Проводник → Удалить вкладку «Безопасность».

Для оснастки «Удалить вкладку «Безопасность» установим значение «Включен». Если пользователь или нарушитель сможет получить доступ ко вкладке «Безопасность», он сможет изменить настройки так, чтобы ослабить защиту АРМ, что недопустимо.

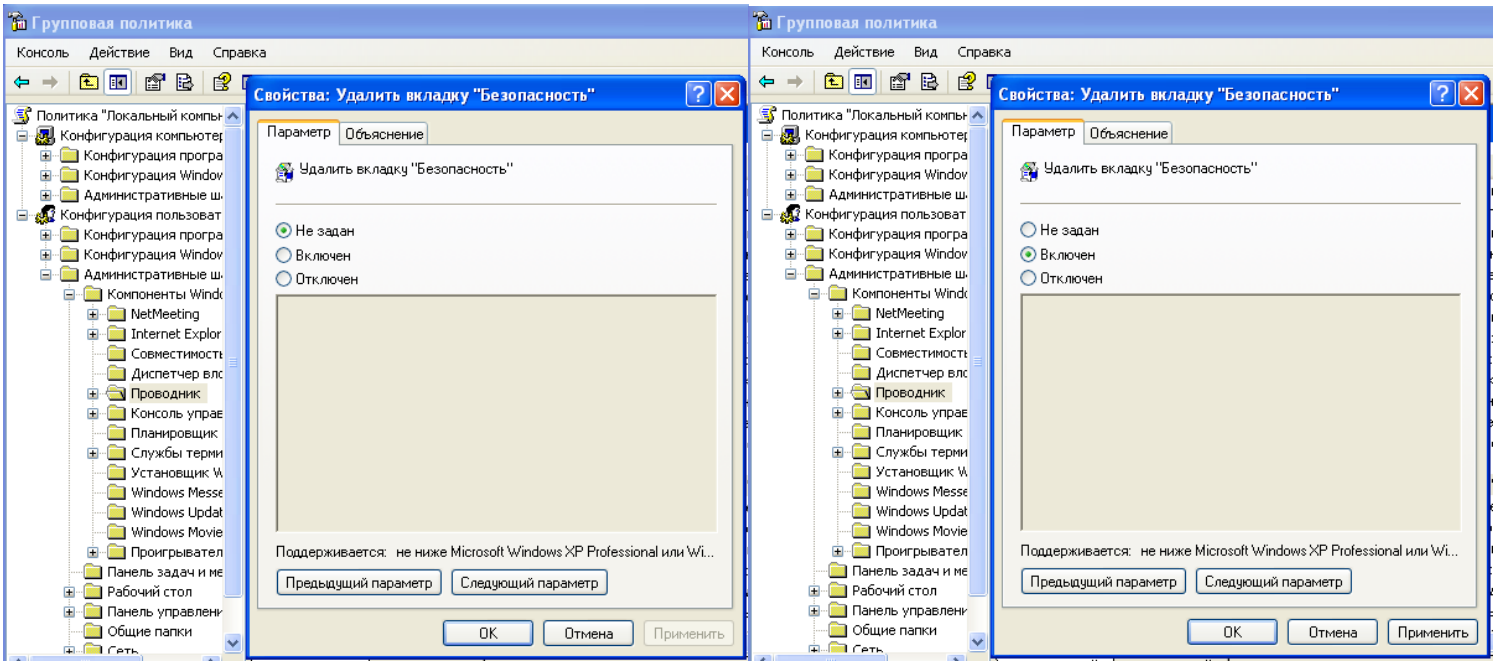

Рис. 24 – настройки «Удалить вкладку «Безопасность»» «до» и «после»

Пуск → Выполнить → gpedit.msc → Групповая политика → Конфигурация пользователя → Административные шаблоны → Компоненты Windows → Проводник → Скрыть значок «Вся сеть» в папке «Сетевое окружение».

Для оснастки «Скрыть значок «Вся сеть» в папке «Сетевое окружение» установим значение «Включен». Просмотр топологии сети может дать преимущества злоумышленнику, если он получит доступ к АРМ, чтобы не допустить этого, скроем соответствующий значок.

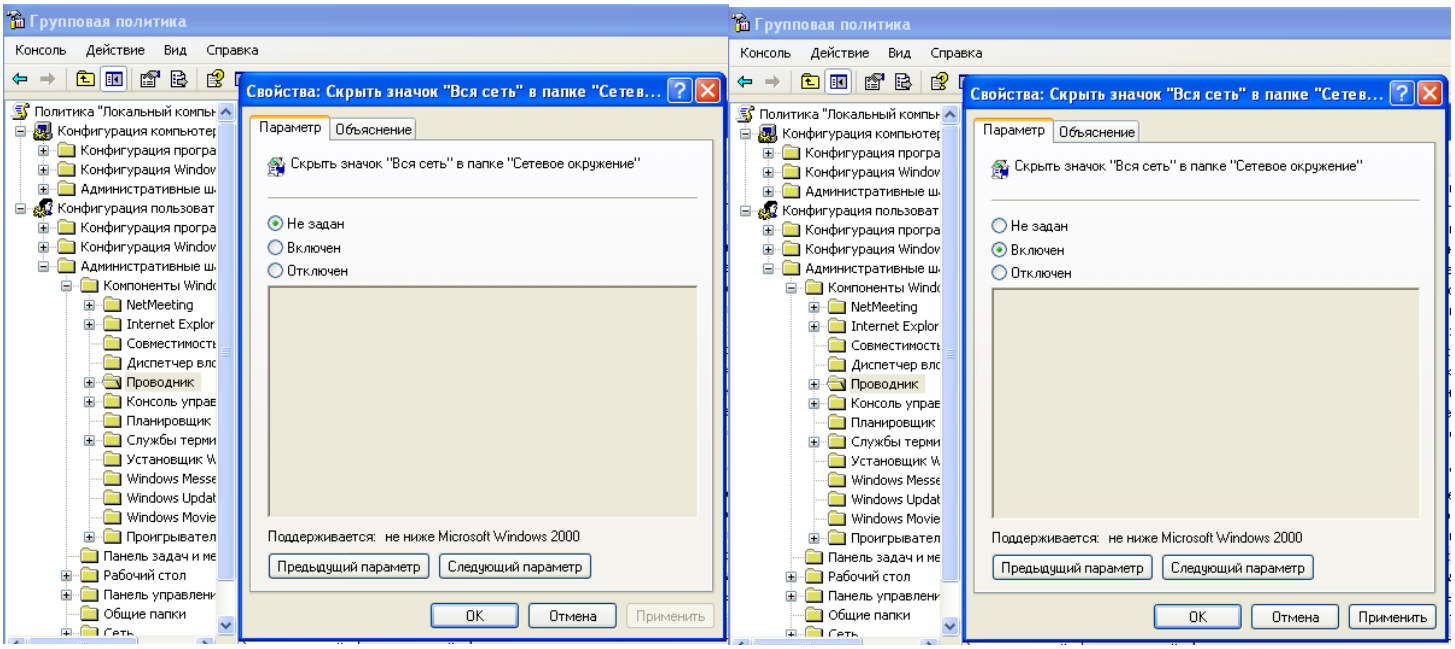

Рис. 25 – настройки «Скрыть значок «Вся сеть» в папке «Сетевое окружение»» «до» и «после»

Пуск → Выполнить → gpedit.msc → Групповая политика → Конфигурация пользователя → Административные шаблоны → Компоненты Windows → Планировщик заданий → Запретить создание новых заданий.

При создании новых заданий пользователей возможно ослабление защиты АРМ, так что отключим эту возможность, установив для данной оснастки значение «Включен».

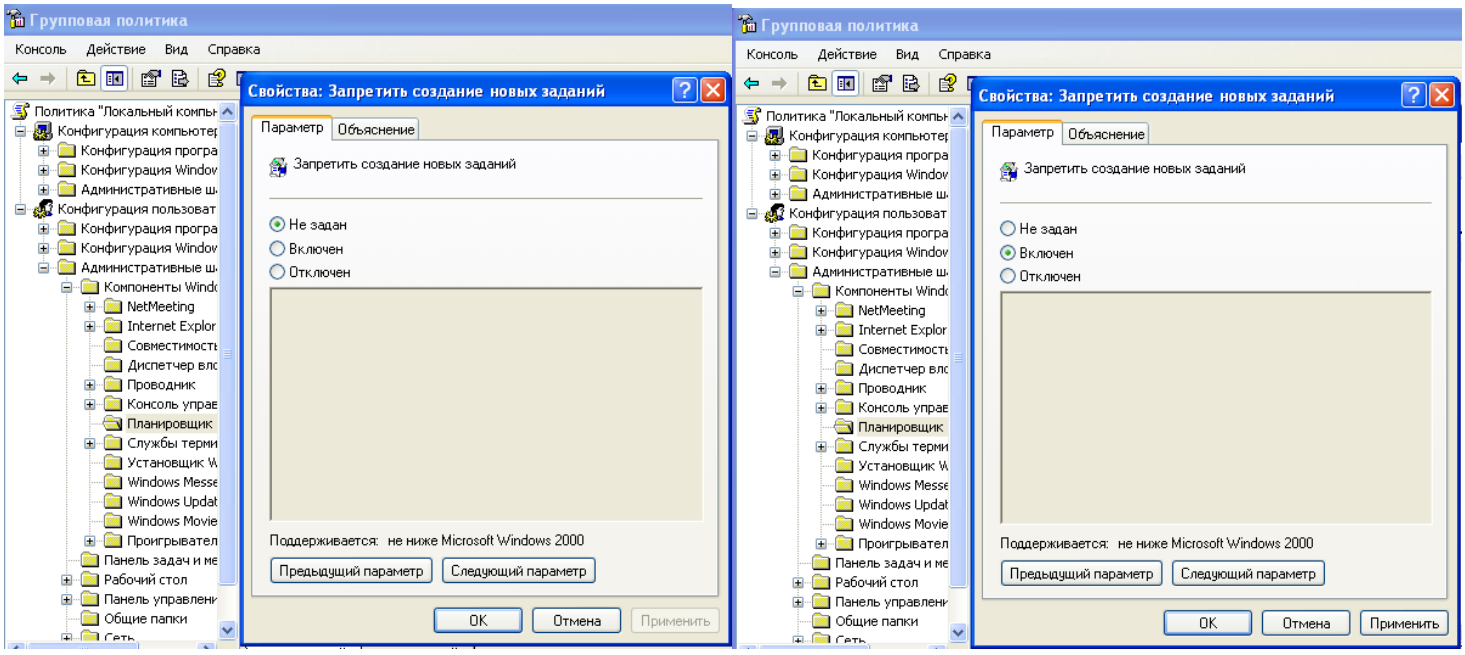

Рис. 26 – настройки «Запретить создание новых заданий» «до» и «после»

Пуск → Выполнить → gpedit.msc → Групповая политика → Конфигурация пользователя → Административные шаблоны → Компоненты Windows → Планировщик заданий → Запретить удаление заданий.

Для оснастки «Запретить удаление заданий» установим значение «Включен». Задания могут использоваться для обеспечения безопасности АРМ, поэтому их удаление может повлечь за собой ослабление безопасности.

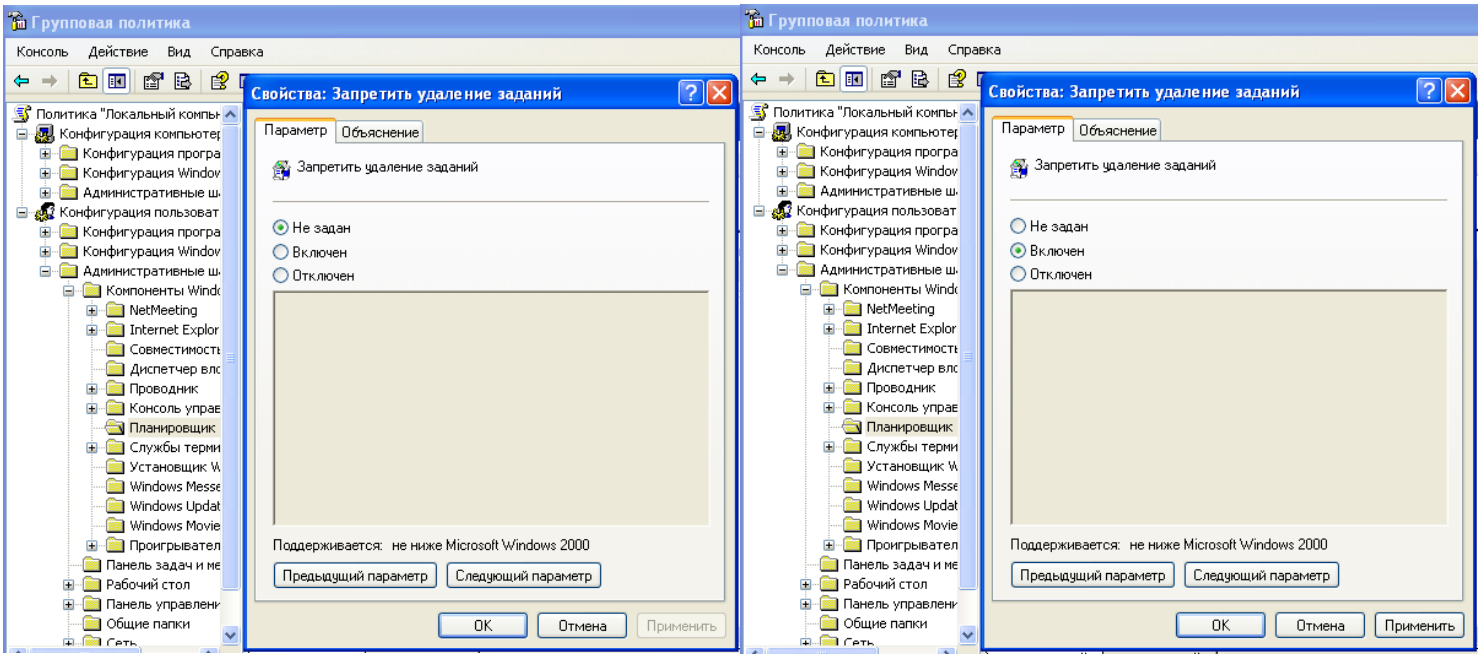

Рис. 27 – настройки «Запретить удаление заданий» «до» и «после»

Пуск → Выполнить → gpedit.msc → Групповая политика → Конфигурация пользователя → Административные шаблоны → Компоненты Windows → Установщик Windows → Запретить использование съемных носителей при установке.

Для оснастки «Запретить использование съемных носителей при установке» установим значение «Включен». Это очень важный пункт, который необходимо учитывать. На носителях могут находиться опасные для системы приложения и даже вирусы. Необходим защититься от этой угрозы.

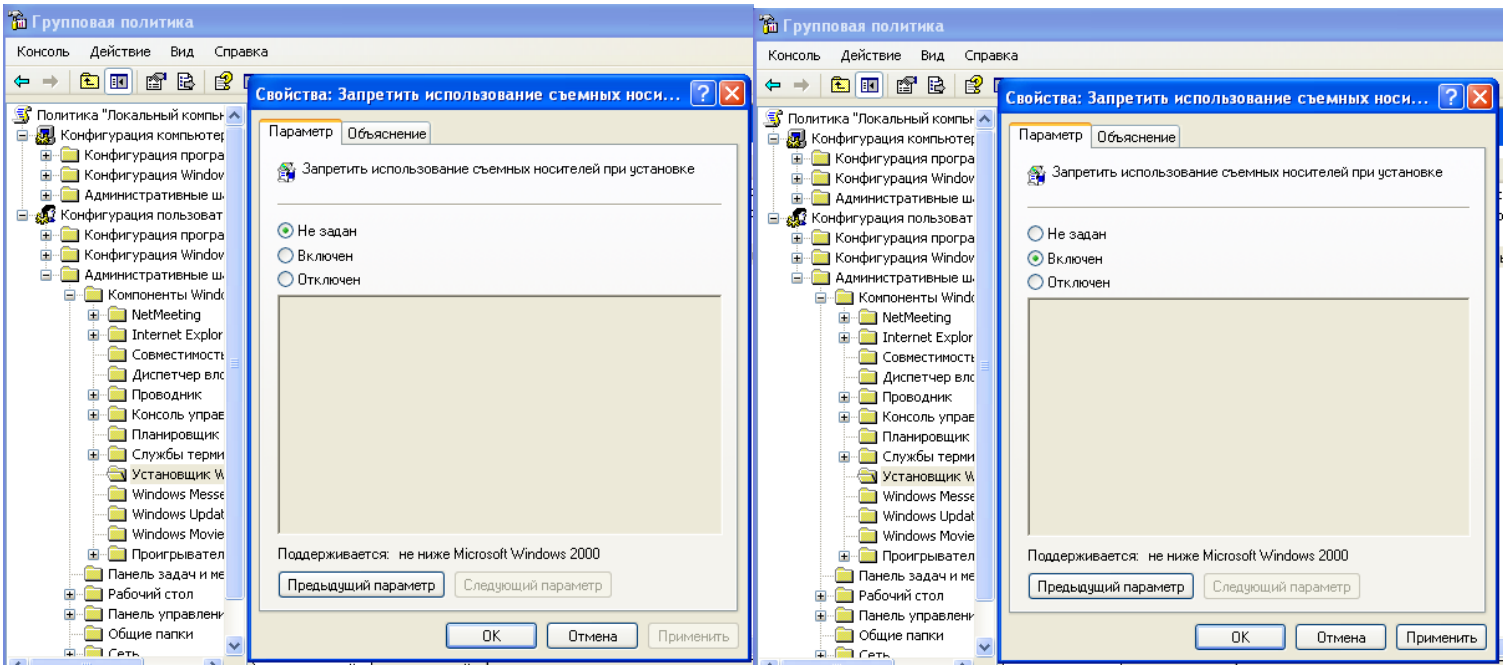

Рис. 28 – настройки «Запретить использование съемных носителей при установке» «до» и «после»

Пуск → Выполнить → gpedit.msc → Групповая политика → Конфигурация пользователя → Административные шаблоны → Панель задач и меню «Пуск» → Удалить «Сетевые подключения» из меню «Пуск».

Для оснастки «Удалить «Сетевые подключения» из меню «Пуск» установим значение «Включен». Пользователь может использовать вкладку «Сетевые подключения» для настройки другого прокси-сервера, что даст ему доступ в интернет. Так как такое развитие событий нежелательно, стоит убрать вкладку.

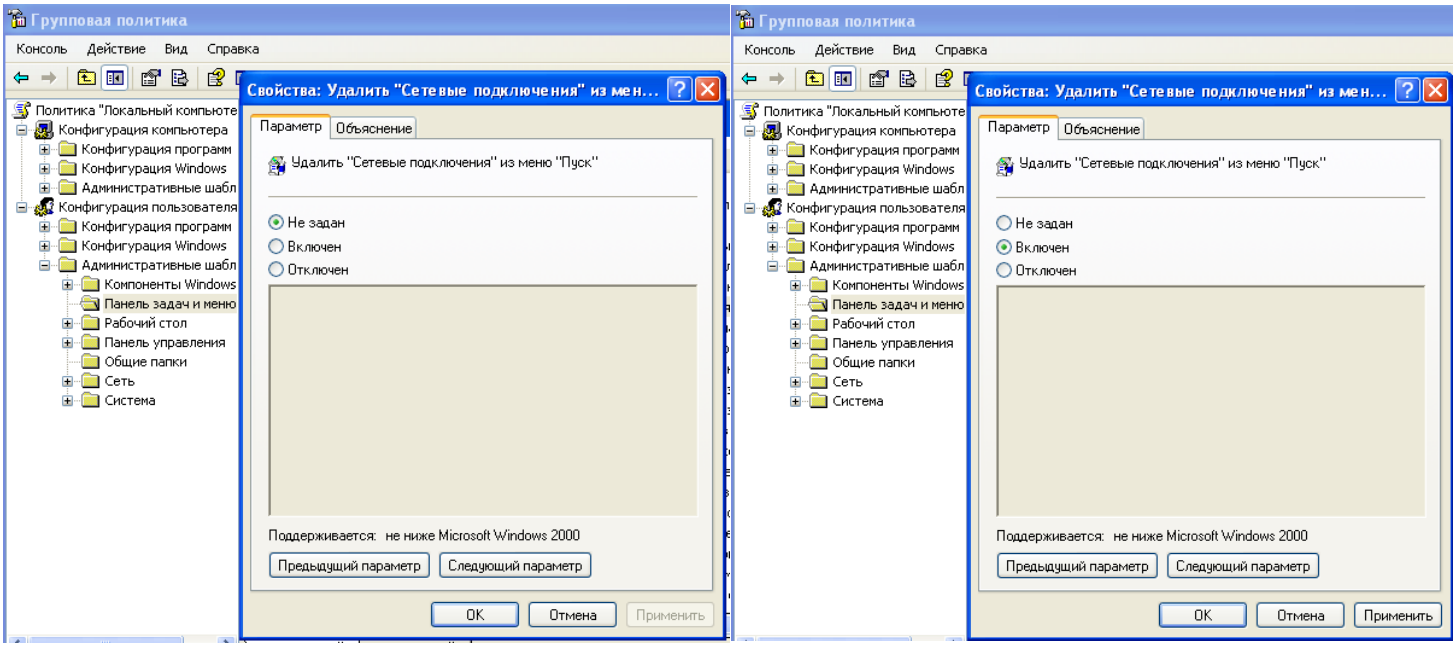

Рис. 29 – настройки «Удалить «Сетевые подключения» из меню Пуск» «до» и «после»

Пуск → Выполнить → gpedit.msc → Групповая политика → Конфигурация пользователя → Административные шаблоны → Сеть → Автономные файлы → Действия при отключении от сервера.

Для оснастки «Действия при отключении от сервера» установим значение «Включен» и реакцию «Работать автономно». Это необходимо, чтобы при потере соединения с сервером, пользователь некоторое время смог бы спокойно продолжать работу, имея доступа к файлам сервера.

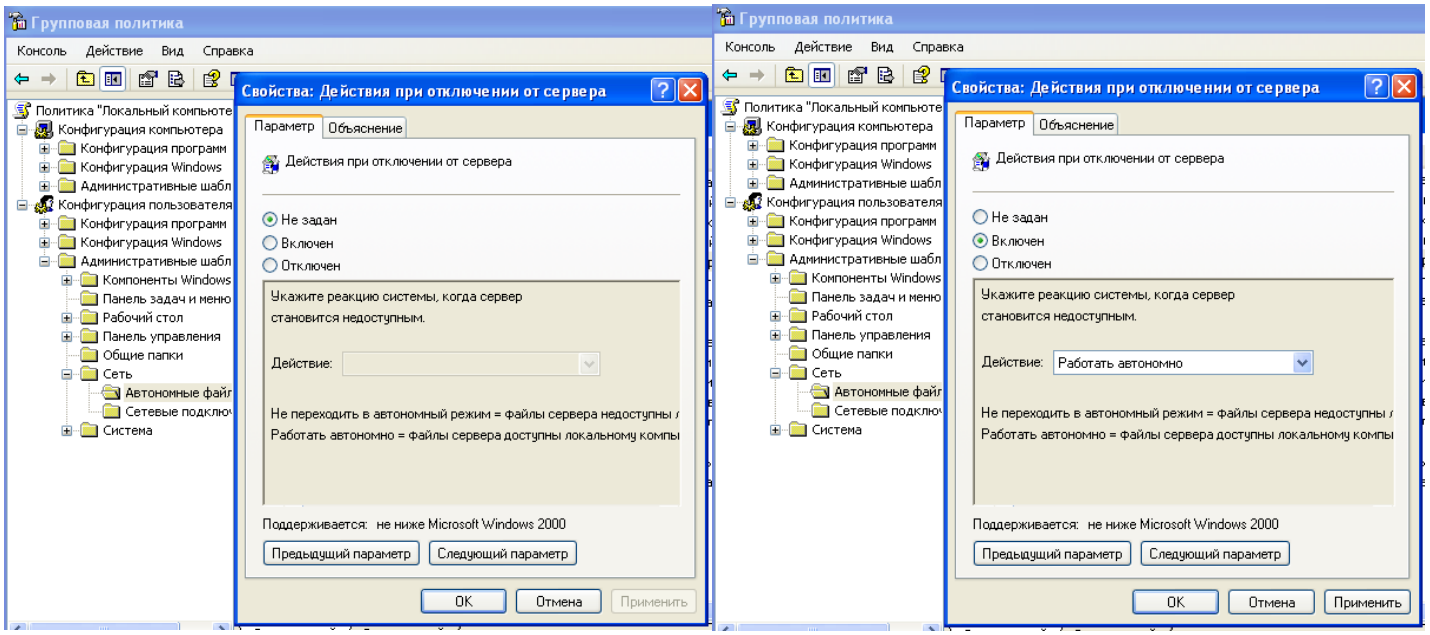

Рис. 30 – настройки «Действия при отключении от сервера» «до» и «после»

В процессе настройки дочернего узла «Административные шаблоны» в «Конфигурации пользователя» были произведены действия, направленные на повышение защищенности АРМ, а именно: запрещен доступ к 16-разрядным приложениям, запрещены создание новых заданий и удаление заданий, запрещено использование съемных носителей при установке. Также были удалены команда «Свойства папки» из меню «Сервис», вкладка «Безопасность», «Сетевые подключения» из меню Пуск. Скрыт значок «Вся сеть» в папке «Сетевое окружение». Настроены действия при отключении от сервера.

Данные настройки обеспечивают требования к системе с классом защищенности 3Б, а именно требования о контроле доступа субъектов в систему, о регистрации и учете действий пользователей в системе, о целостности программных средств и неизменности программной среды. Эти настройки помогли повысить общий уровень защищенности системы.

Вывод:

В результате выполнения лабораторной работы был изучен редактор локальной групповой политики, а также настроены групповые политики безопасности на АРМ пользователя с установленной на нем операционной системой Windows XP для защиты информации от НСД с учетом требований информационной безопасности к системе с классом защищенности 3Б.