Цель работы:

Цель – 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 для защиты информации от несанкционированного доступа (НСД).

Используемое программное обеспечение: операционная система Windows XP.

Основные сведения:

Введение в групповые политики Windows. Как системным администраторам в предприятиях, так и домашним пользователям рано или поздно приходится настраивать компьютеры, а также конфигурацию пользовательских учетных записей. В домашних условиях вы можете просто применить к своему компьютеру и необходимым учетным записям твики 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 компании, 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, а также компьютеров, 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). Групповые политики являются компонентом операционной системы Windows и основываются на тысячах отдельных параметров политик, иначе говоря, политик, определяющих определённую конфигурацию для своего применения.

История 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. Все это объекты хранились в папке %SystemRoot%\System32\Group Policy. 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.

Тип ИС закрытого контура в соответствие с вариантом – **2Б**

Требования к классу защищенности 2Б:

Подсистема управления доступом:

Должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и 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;
- результат попытки входа: успешная или неуспешная (при НСД);
- должен проводиться учет всех защищаемых носителей информации с помощью их 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 во время обработки и (или) хранения защищаемой информации;
- 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, предусматрива ющие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

Подсистемы и требования	Класс 2Б
1. Подсистема управления доступом	
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:	
в систему	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	-
к программам	-
к томам, каталогам, файлам, записям, полям записей	-
1.2. Управление потоками информации	
2. Подсистема регистрации и учета	
2.1. Регистрация и учет:	
входа (выхода) субъектов доступа в (из) систему (узел сети)	+
выдачи печатных (графических) выходных документов	-
запуска (завершения) программ и процессов (заданий, задач)	-
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	-
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	-
изменения полномочий субъектов доступа	-
создаваемых защищаемых объектов доступа	-
2.2. Учет носителей информации	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	-
2.4. Сигнализация попыток нарушения защиты	-
3. Криптографическая подсистема	
3.1. Шифрование конфиденциальной информации	-

3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	-
3.3. Использование аттестованных (сертифицированных) криптографических средств	-
4. Подсистема обеспечения целостности	
4.1. Обеспечение целостности программных средств и обрабатываемой информации	+
4.2. Физическая охрана средств вычислительной техники и носителей информации	+
4.3. Наличие администратора (службы) защиты информации в АС	-
4.4. Периодическое тестирование СЗИ НСД	+
4.5. Наличие средств восстановления СЗИ НСД	+
4.6. Использование сертифицированных средств защиты	-

Ход выполнения работы:

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

Пуск → Выполнить → gpedit.msc → Групповые политики → Конфигурация компьютера → Конфигурация Windows → Сценарии.

Эта оснастка позволяет запускать различные файлы скриптов при загрузке/завершении работы компьютера. Создадим скрипт на языке PowerShell, который будет подсчитывать 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
}
```

Рисунок 1: Содержимое скрипта на языке PowerShell.

В настройках сценариев укажем, что данный скрипт необходимо запускать и при загрузке компьютера и при его выключении: 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. То есть, собранные данные помогут увеличить безопасность информационной системы.

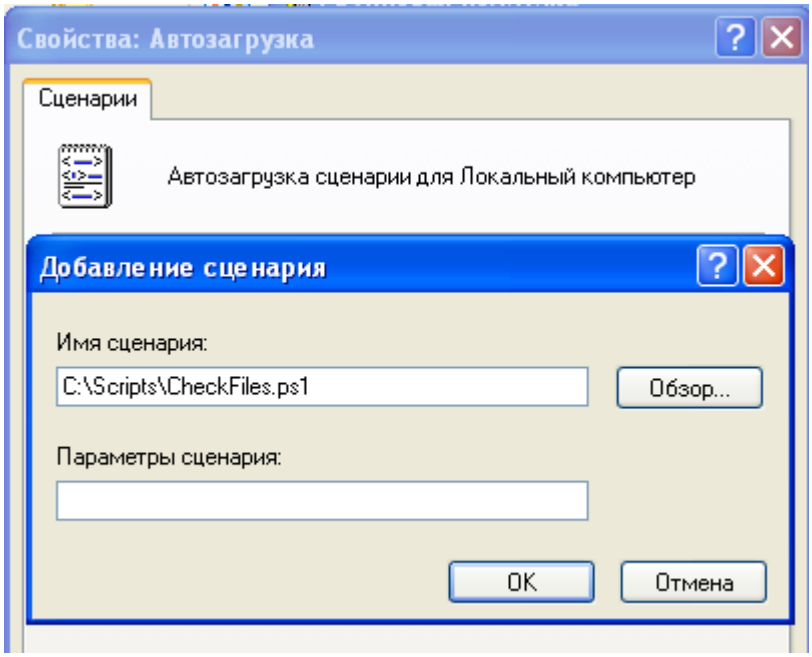

Рисунок 2: Настройка выполнения сценария при загрузке.

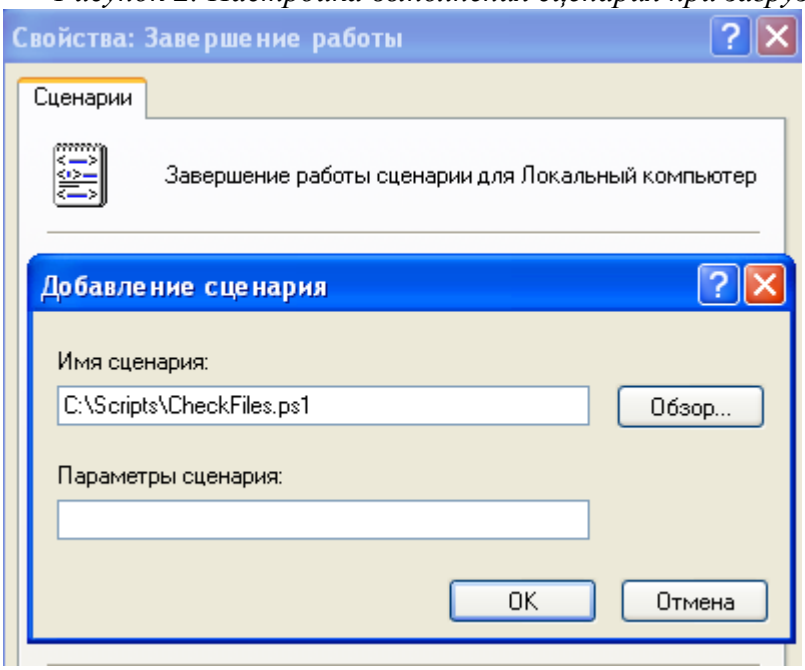

Рисунок 3: Настройка выполнения сценария при выключении.

«Политики учетных записей» и «Локальные политики» в разделе «Параметры безопасности» были настроены в 1 лабораторной работе, поэтому переходим к следующей оснастке.

Откроем другую оснастку, перейдя по адресу: Пуск → Выполнить → gpedit.msc → Групповые политики → Конфигурация компьютера → Конфигурация Windows → Параметры безопасности → Политики открытого ключа → 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. Так как предполагается, что настраиваемое АРМ расположено в «закрытом» контуре, такие параметры нам подходят, поэтому оставляем их.

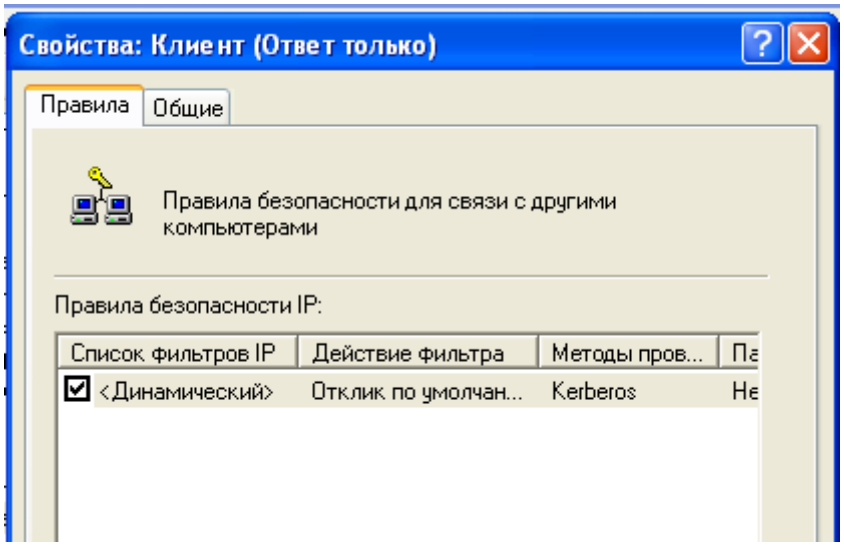

Рисунок 4: Настройка пункта "Клиент (Ответ только)".

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

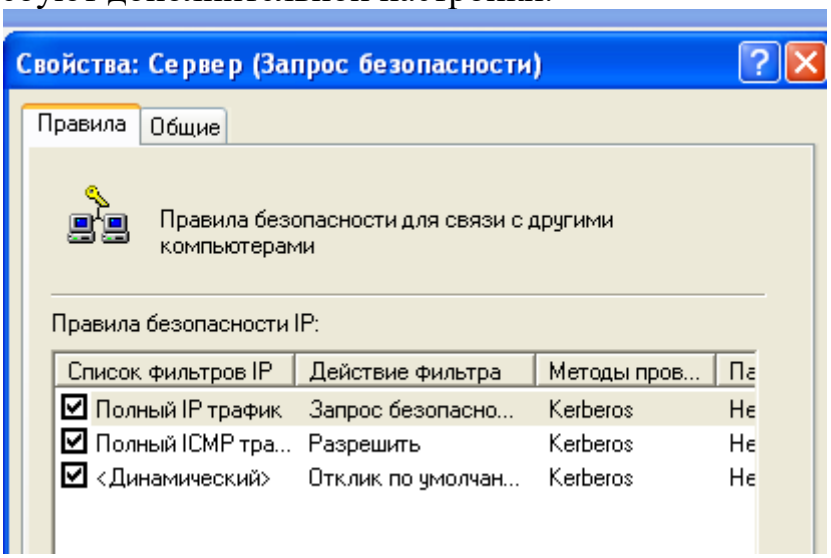

Рисунок 5: Настройки пункта "Сервер (Запрос безопасности)".

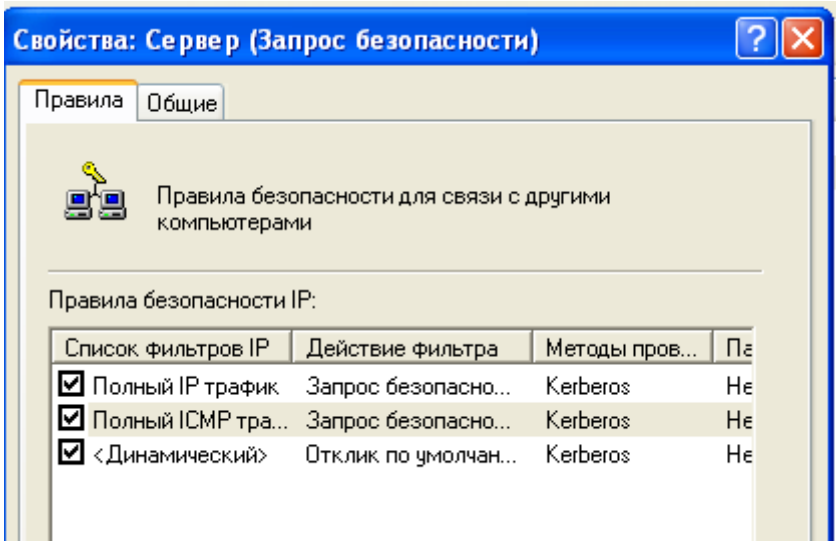

Рисунок 6: Новые настройки пункта "Сервер (Запрос безопасности)".

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

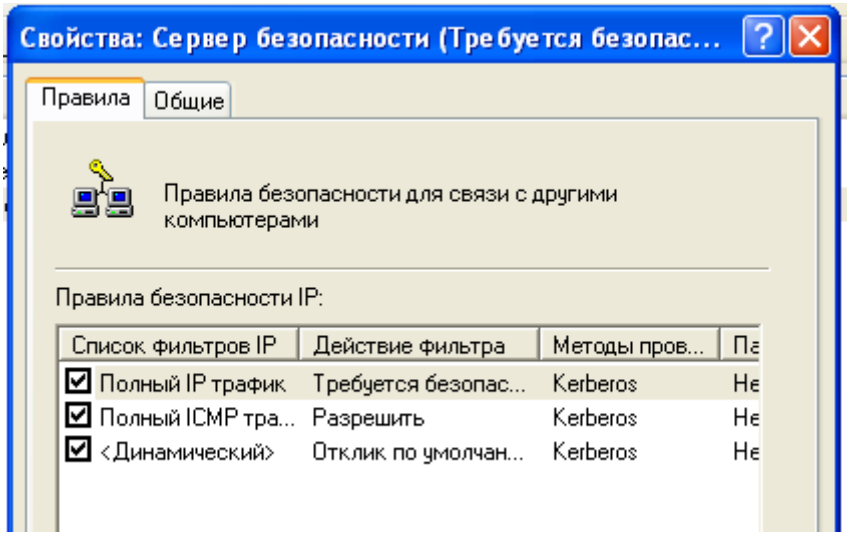

Рисунок 7: Настройки пункта "Сервер безопасности (Требуется безопасность)".

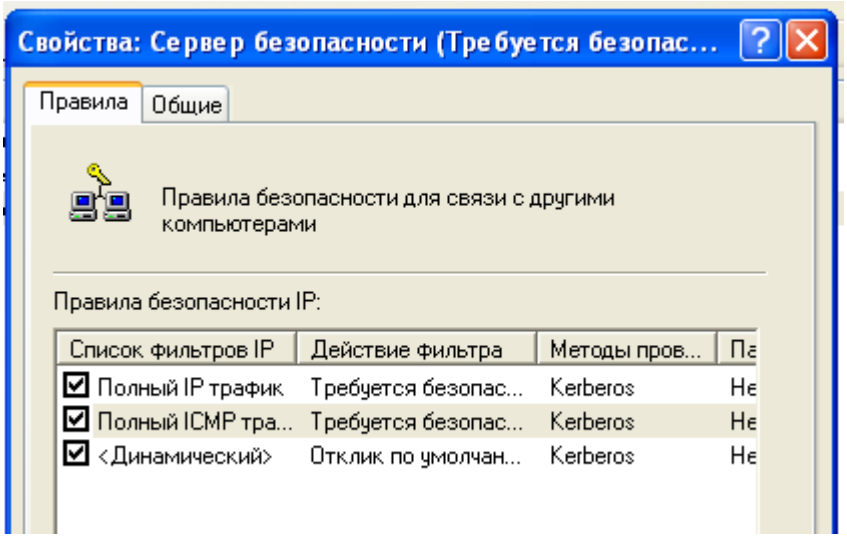

Рисунок 8: Новые настройки пункта "Сервер безопасности (Требуется безопасность)".

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. Были произведены настройки аутентификации и блокировки учетной записи(в соответствии с 1 лабораторной) для предотвращения несанкционированного доступа к АРМ. Была настроена «Политики безопасности IP на «Локальный компьютер» для повышения защиты информации, обрабатываемой АРМ, и ограничения пользователю доступ к сети Internet.

Данные настройки обеспечивают требования к системе с классом защищенности 2Б, 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»

Настроим некоторые оснастки узла «Административные шаблоны».

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

Для оснастки «Запретить удаленное управление рабочим столом» установим значение «Включен». Для рассматриваемого АРМ, находящегося в «закрытом» контуре, нет необходимости в удаленном управлении рабочим столом. Такая возможно ставит под угрозу всю сеть.

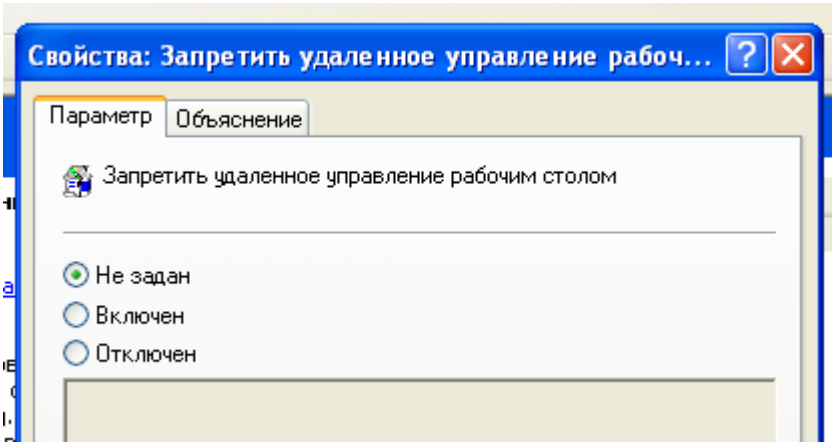

Рисунок 9: Настройки запрета удаленного управления рабочим столом.

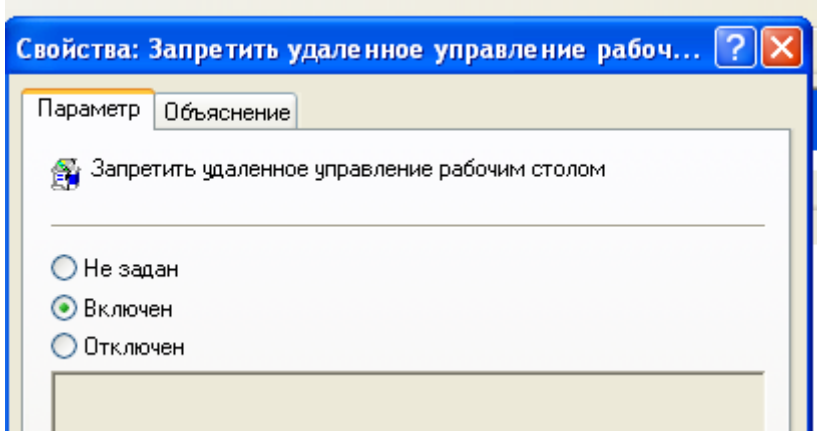

Рисунок 10: Новые настройки запрета удаленного управления рабочим столом.

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

Для оснастки «Разрешать удаленное подключение с использованием служб терминалов» установим значение «Отключен». Для рассматриваемого АРМ, находящегося в «закрытом» контуре, нет необходимости в удаленном подключении с использованием служб терминалов. Такая возможно ставит под угрозу всю сеть.

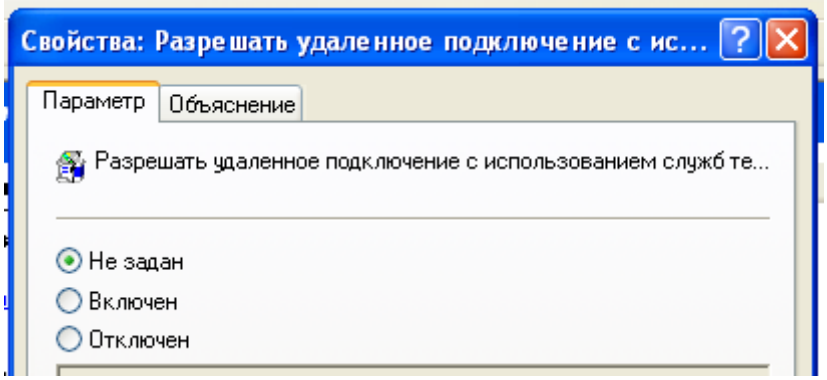

Рисунок 11: Настройки разрешения удаленного подключения с использованием служб терминалов.

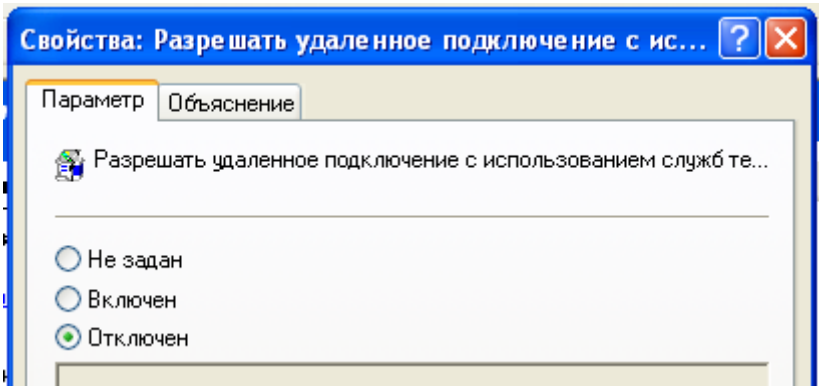

Рисунок 12: Новые настройки разрешения удаленного подключения с использованием служб терминалов.

Пуск → Выполнить → gpedit.msc → Групповые политики → 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. Особый интересе представляет фиксация запуска приложений с носителя. Конечно, данная настройка не спасет систему от гипотетического урона, который может быть нанесен при запуске опасных приложений, но позволит при расследовании найти «корень зла» и понять, что послужило отправной точкой атаки.

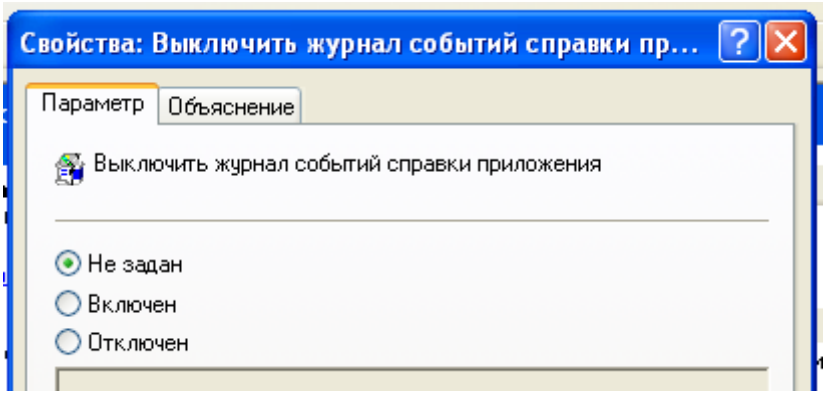

Рисунок 13: Настройки выключения журнала событий справки приложения.

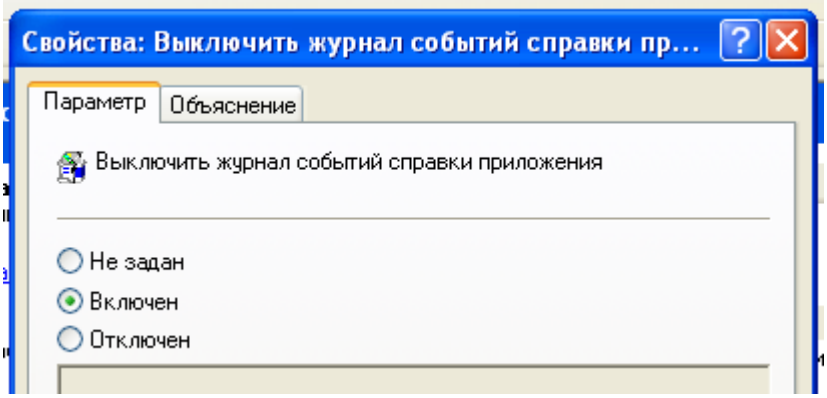

Рисунок 14: Новые настройки выключения журнала событий справки приложения.

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

Для оснастки «Предотвращение доступа к 16-разрядным приложениям» установим значение «Включен». Современные операционные системы имеют разрядность 32 или 64 бита, а потому 16-разрядные приложения могут неправильно функционировать в них, что может привести к сбоям в работе системы. Более того, такие приложения может использовать злоумышленник, ведь защита таких приложений на сегодняшний день оставляет желать лучшего.

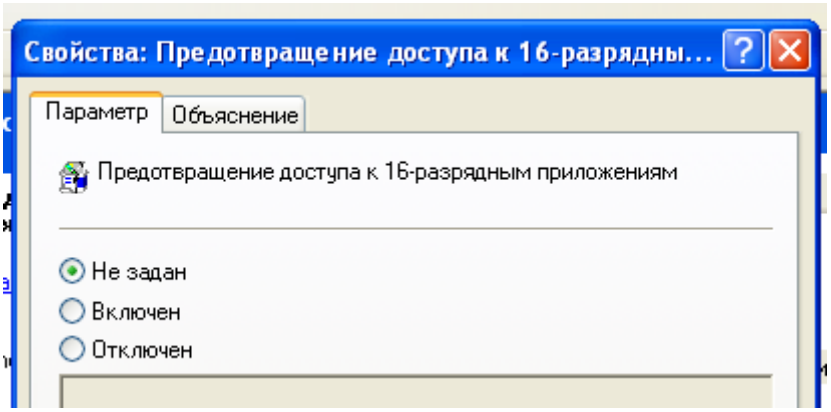

Рисунок 15: Настройки предотвращения доступа к 16-разрядным приложениям.

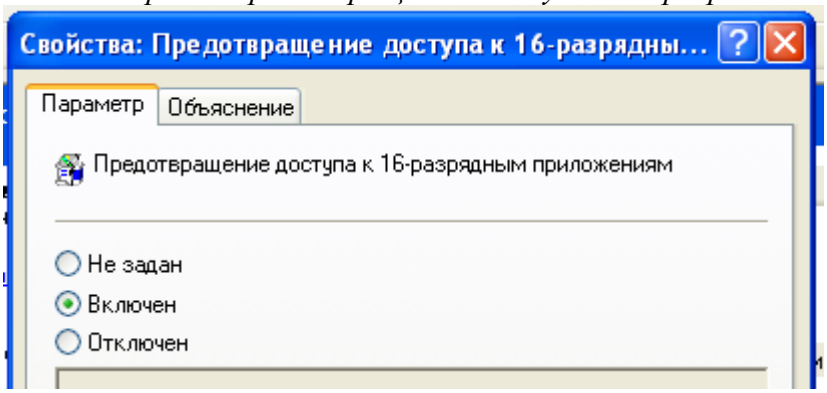

Рисунок 16: Новые настройки предотвращения доступа к 16-разрядным приложениям.

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

Для оснастки «Включить «Центр обеспечения безопасности» установим значение «Включен». Использование центра обеспечения безопасности поможет повысить безопасность средствами операционной системы.

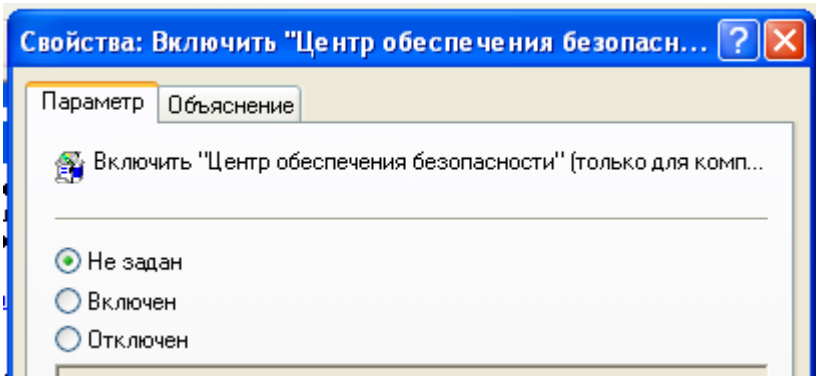

Рисунок 17: Настройки включения "Центра обеспечения безопасности".

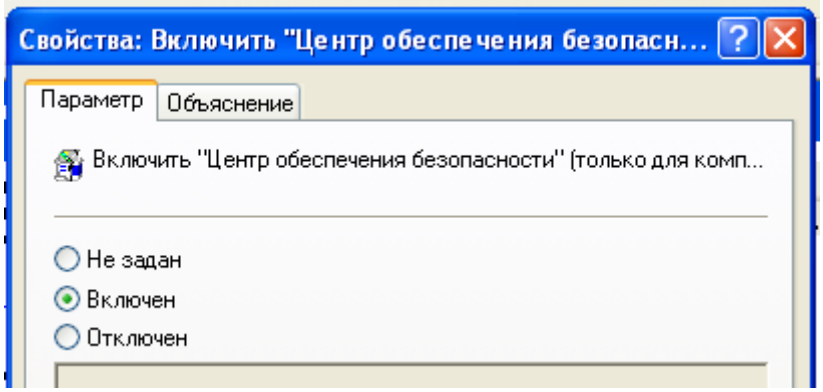

Рисунок 18: Новые настройки включения "Центра обеспечения безопасности".

Пуск → Выполнить → gpedit.msc → Групповые политики → Конфигурация компьютера → 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.

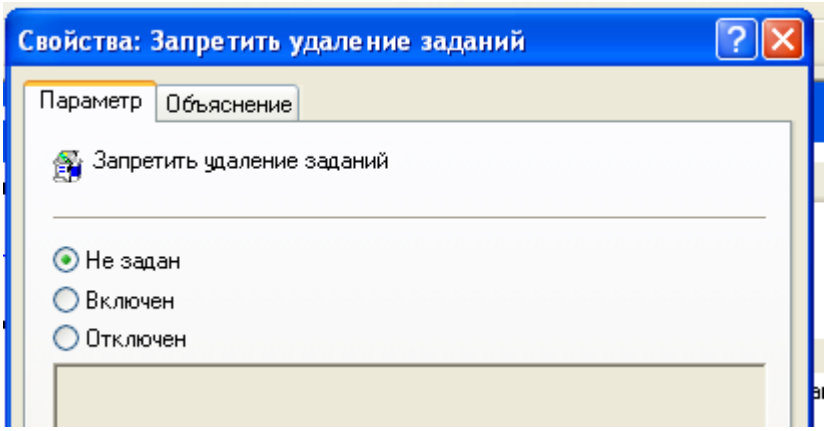

Рисунок 19: Настройки запрета удаления заданий.

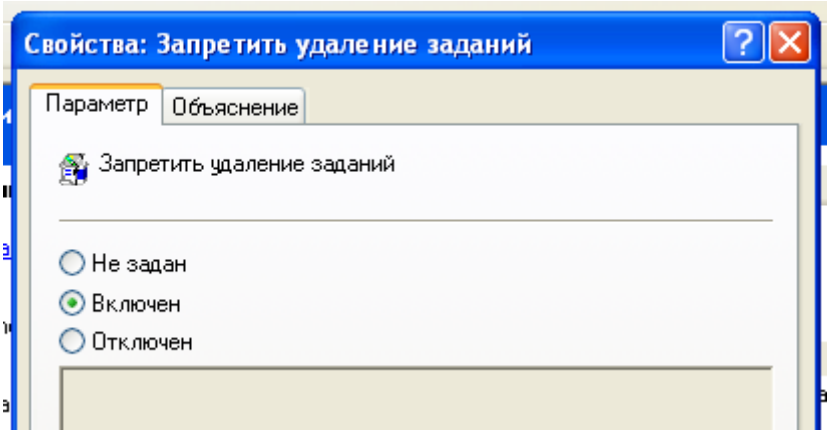

Рисунок 20: Новые настройки запрета удаления заданий.

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

Для оснастки «Удалить элемент «Безопасность Windows» из меню Пуск» установим значение «Включен». Любопытный, но неумелый пользователь может нарушить систему защиты, чего уж говорить про опытного злоумышленника. Поэтому целесообразно усложнить жизнь нарушителям.

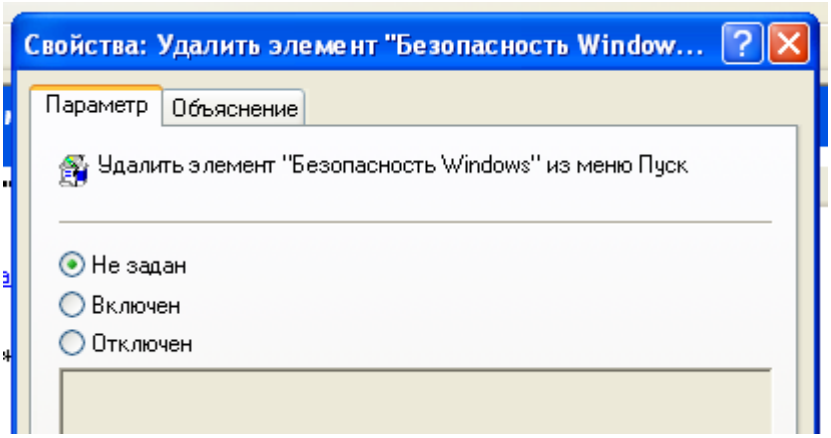

Рисунок 21:Настройки удаления элемента "Безопасность Windows" из меню Пуск.

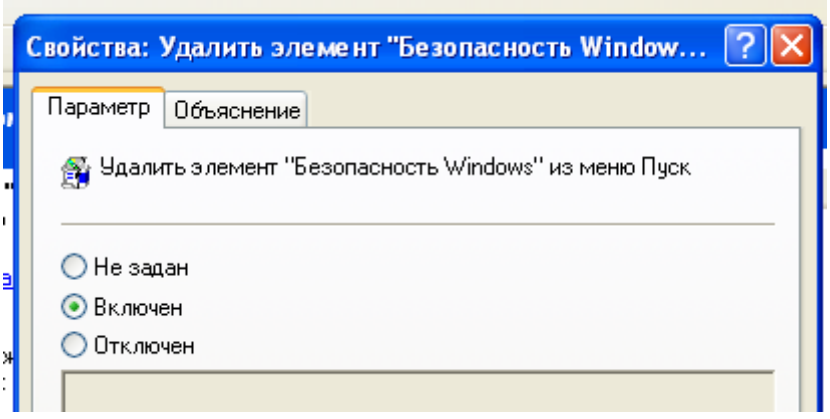

Рисунок 22: Новые настройки удаления элемента "Безопасность Windows" из меню Пуск.

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

Для оснастки «Отключить защищенный режим протокола оболочки» установим значение «Отключен». Защищенный режим протокола оболочки позволит запретить пользователю доступ к некоторым папкам и приложениям, имеющим особую важность для безопасности системы.

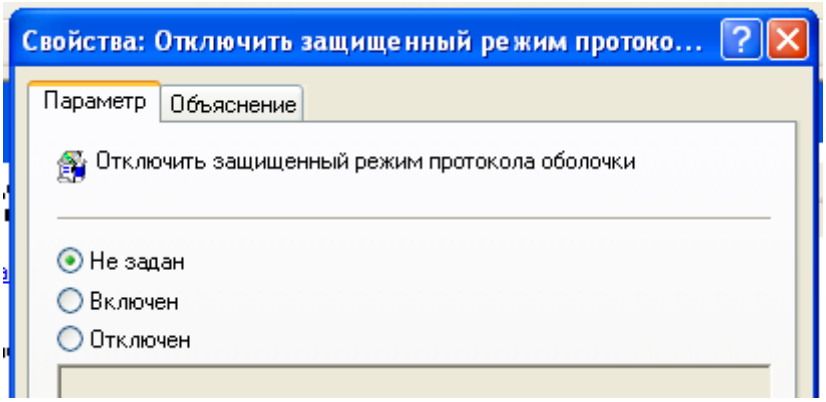

Рисунок 23: Настройки отключения защищенного режима протокола оболочки.

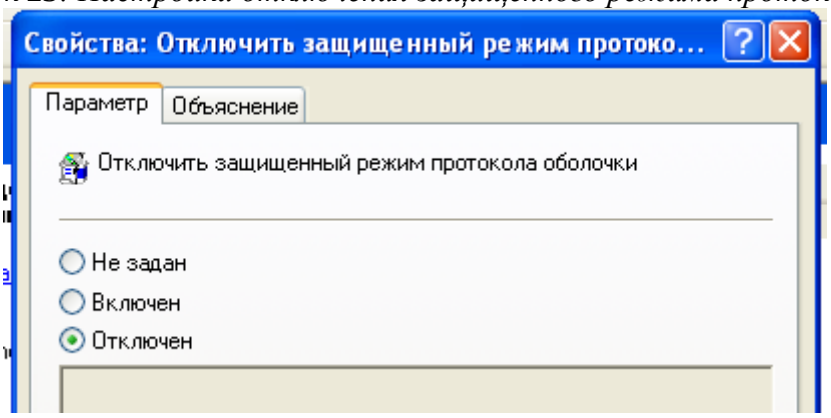

Рисунок 24: Новые настройки отключения защищенного режима протокола оболочки.

Пуск → Выполнить → gpedit.msc → Групповые политики → Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Установщик Windows → Ведение журнала.

Для оснастки «Ведение журнала» установим значение «Включен» и укажем, что заносить в него необходимо абсолютно все события. Ведение журнала – это исключительно важная задача, ведь такой журнал позволяет своевременно реагировать на опасные действия пользователей или нарушителей, а в случае компрометации системы проводить расследование.

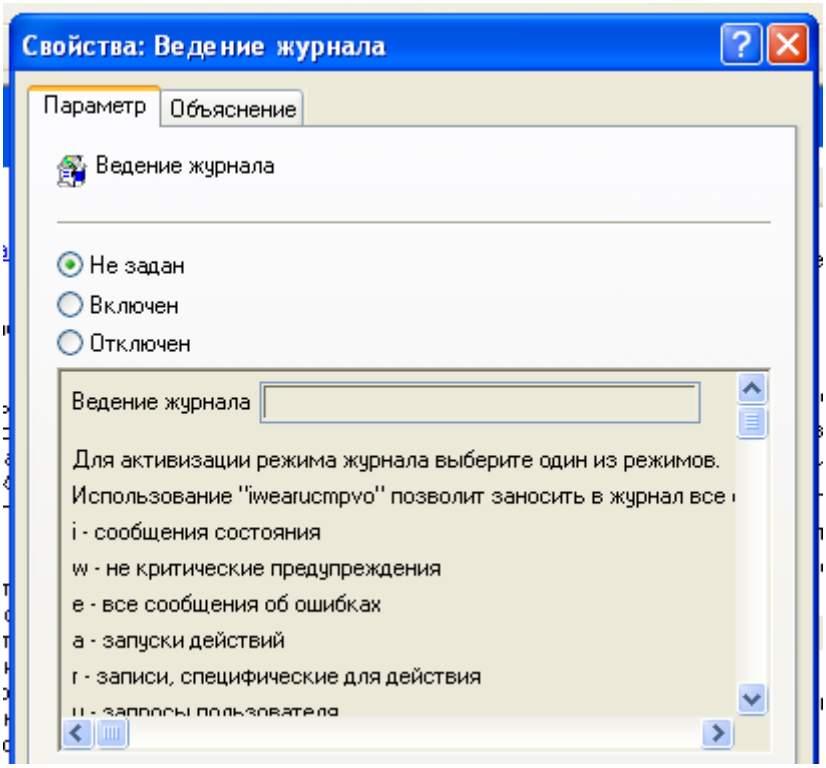

Рисунок 25: Настройки ведения журнала.

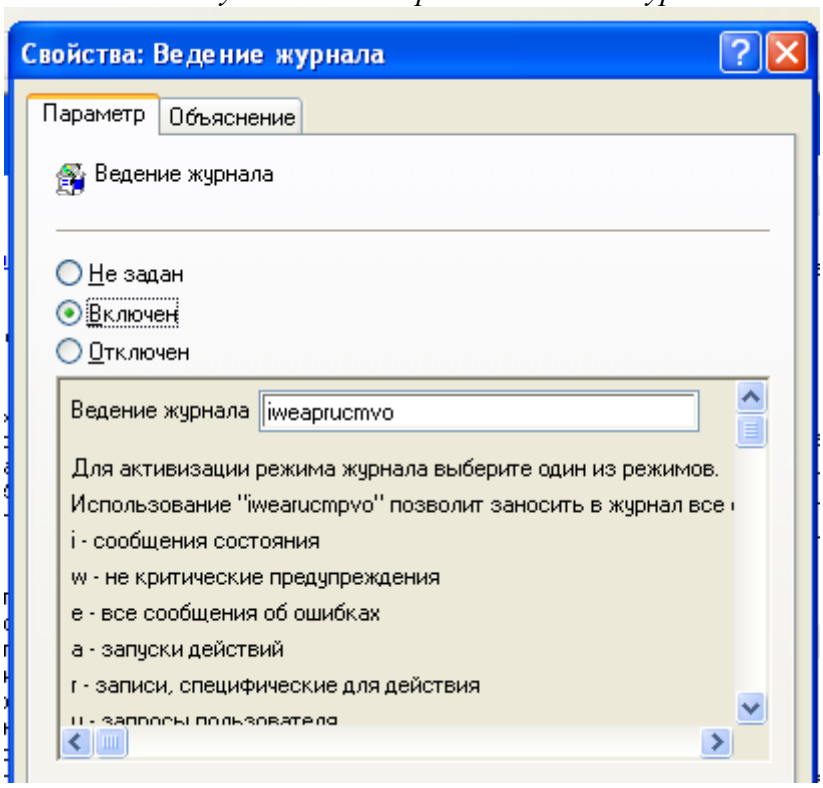

Рисунок 26: Новые настройки ведения журнала.

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

Для оснастки «Настройка автоматического обновления» установим значение «Включен» и укажем, что загружать и устанавливать обновления необходимо автоматически, каждый день в 18:00. Автоматическое обновление

операционной системы позволяют вовремя исправлять ошибки и уязвимости системы, следовательно лучше активировать данную возможность. Время выбрано не случайно, обычно к 18:00 рабочий день заканчивается и у пользователей нет нужды в использовании компьютеров.

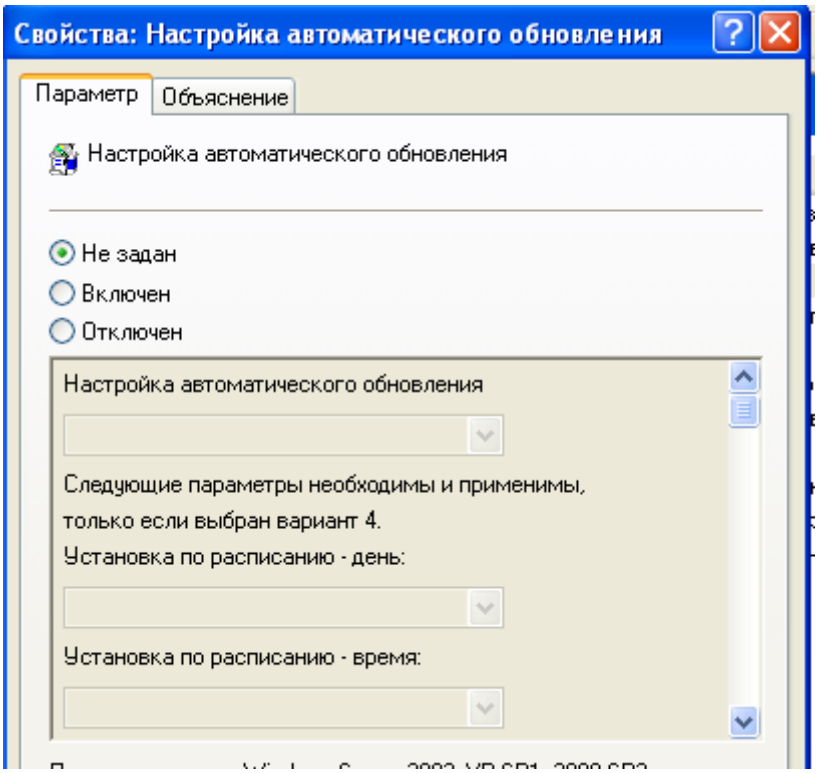

Рисунок 27: Настройки автоматического обновления.

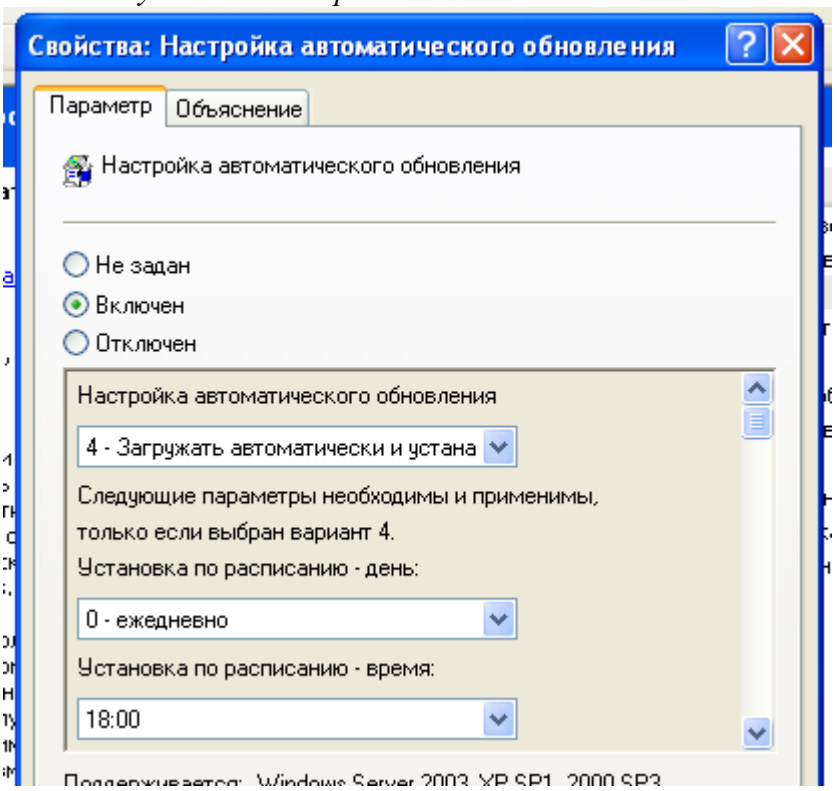

Рисунок 28: Новые настройки автоматического обновления.

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 2Б, а именно требования о целостности приложений.

Также повышен общий уровень защищенности системы.

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

Пуск → Выполнить → gpedit.msc → Групповые политики → Конфигурация пользователя → Конфигурация Windows → Сценарии.

Эта оснастка позволяет запускать различные файлы скриптов при входе пользователя в систему или при выходе из нее. Создадим скрипт, который будет удалять файлы, которые старше 3 месяцев. Его будем запускать 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 будем запускать 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
   }
}
```

Рисунок 29: Скрипт, предназначенный для удаления старых файлов.

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

Рисунок 30: Скрипт, предназначенный для получения сведений о сеансах входа в систему.

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

Рисунок 35: Скрипт, предназначенный для получения сведений о пользователях, которые выполнили вход в компьютер.

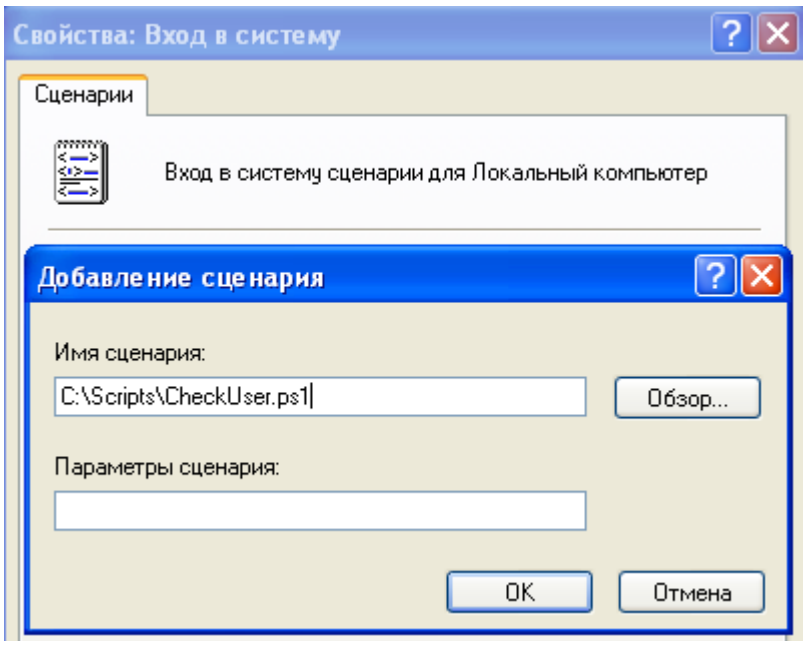

Рисунок 36: Настройки сценария для входа в систему.

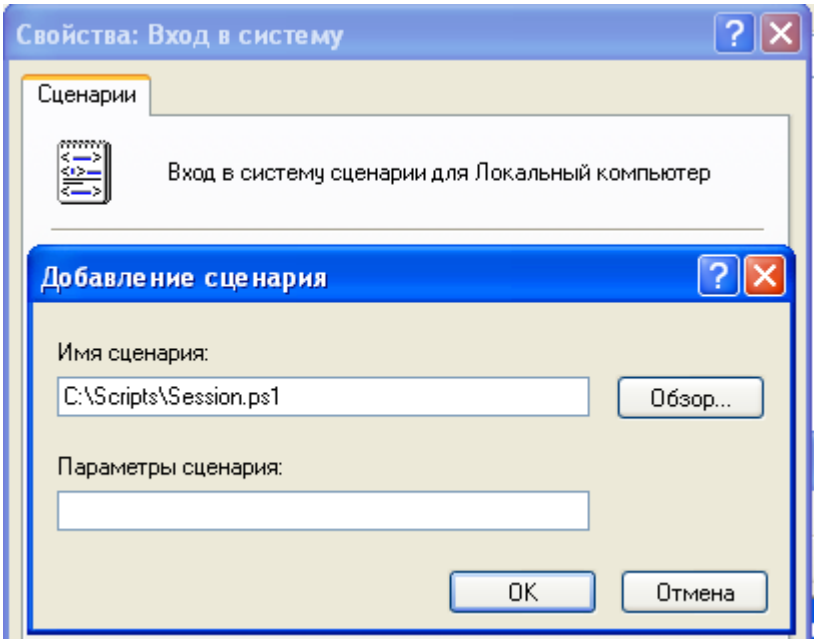

Рисунок 37: Настройки сценария для входа в систему.

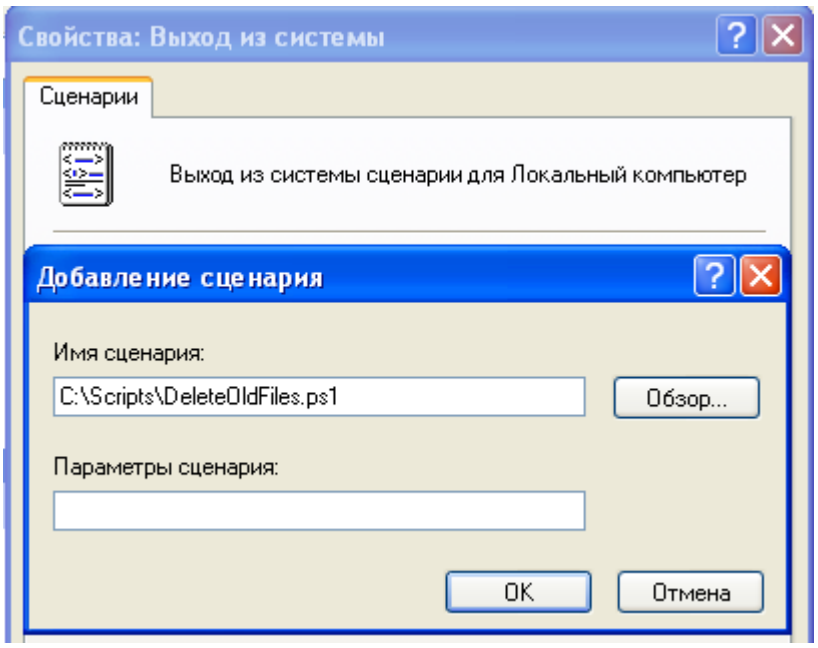

Рисунок 38: Настройки сценария для выхода из системы.

Перейдем к настройке другого узла. Пуск → Выполнить → gpedit.msc → Групповые политики → Конфигурация пользователя → Конфигурация Windows → Настройки Internet Explorer → Подключения → Параметры прокси-сервера.

Будем использовать несуществующий прокси-сервер для того, чтобы запретить пользователям доступ в интернет. Для этого достаточно поставить галочку напротив пункта «разрешить настройку прокси-сервера» и установить адрес прокси-сервера 0.0.0.0. Для того, чтобы разрешить подключение АРМ к серверу информационной сети, укажем адрес этого сервера (пусть данный адрес будет 172.168.13.1) в качестве исключения.

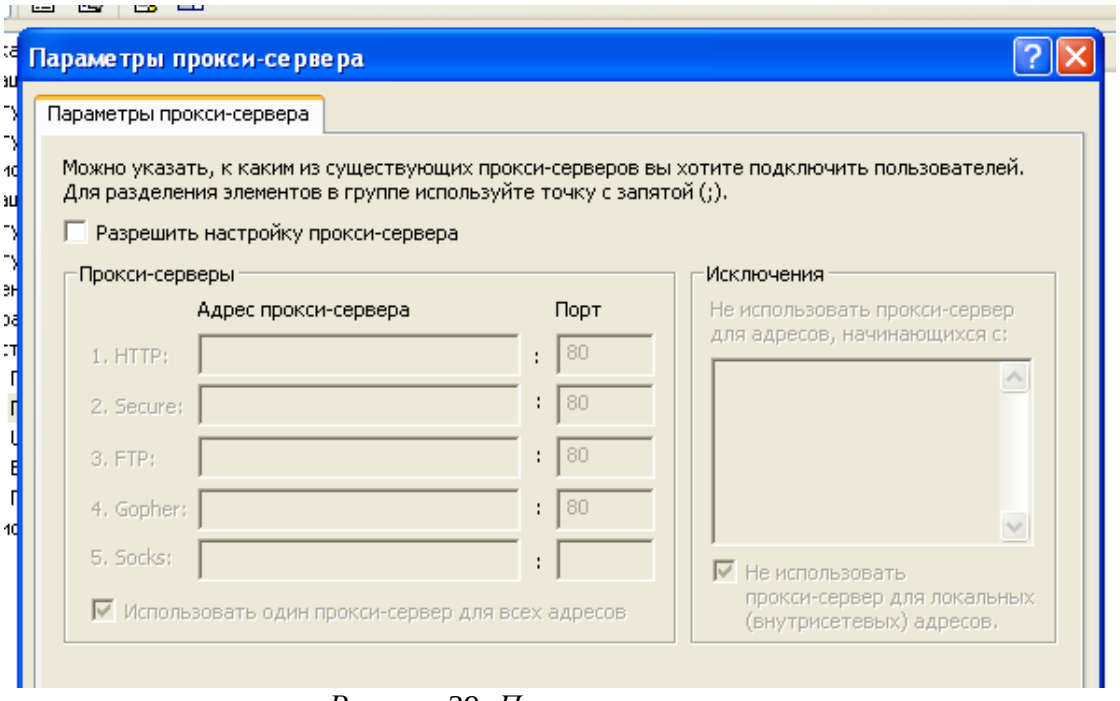

Рисунок 39: Параметры прокси-сервера.

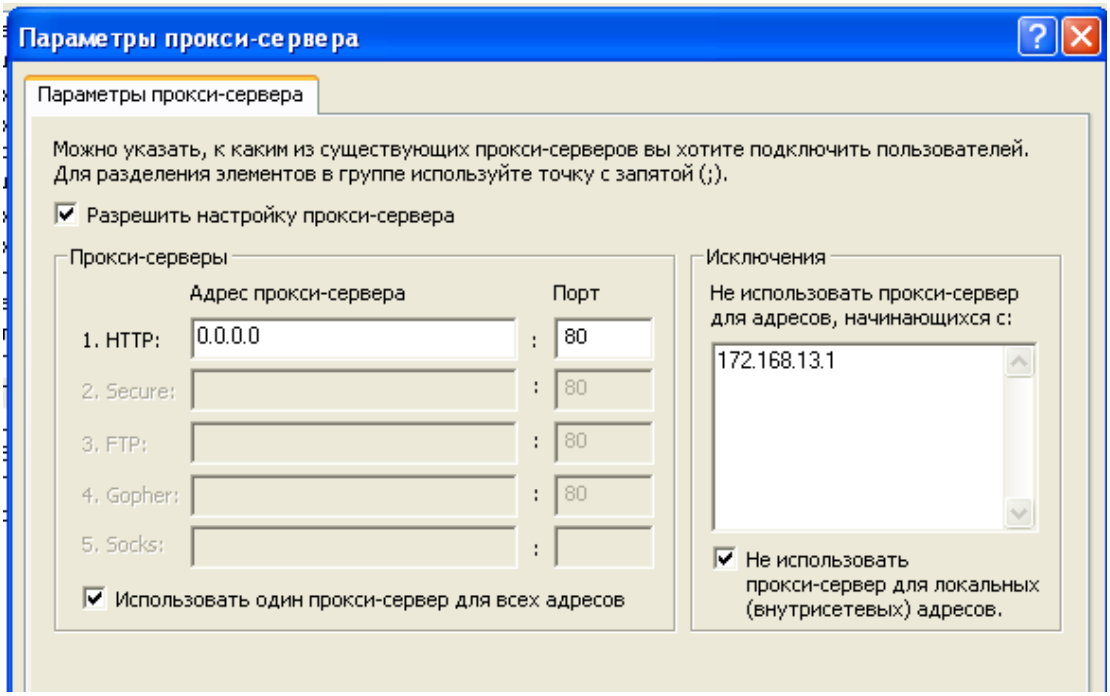

Рисунок 40: Новые параметры прокси-сервера.

В процессе настройки дочернего узла «Конфигурация Windows» в «Конфигурации пользователя» были настроены сценарии, которые будут выполняться при входе в систему и выходе из нее. Был настроен прокси-сервер, запрещающий пользователю выход в интернет и позволяющий связаться только с сервером информационной сети.

Данные настройки обеспечивают требования к системе с классом защищенности 2Б, а именно требования о контроле доступа субъектов в систему.

Также был повышен общий уровень защищенности системы.

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

Настроим некоторые оснастки узла «Административные шаблоны».

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

Для оснастки «Предотвращение доступа к 16-разрядным приложениям» установим значение «Включен». Современные операционные системы имеют разрядность 32 или 64 бита, а потому 16-разрядные приложения могут неправильно функционировать в них, что может привести к сбоям в работе системы. Более того, такие приложения может использовать злоумышленник, ведь защита таких приложений на сегодняшний день оставляет желать лучшего.

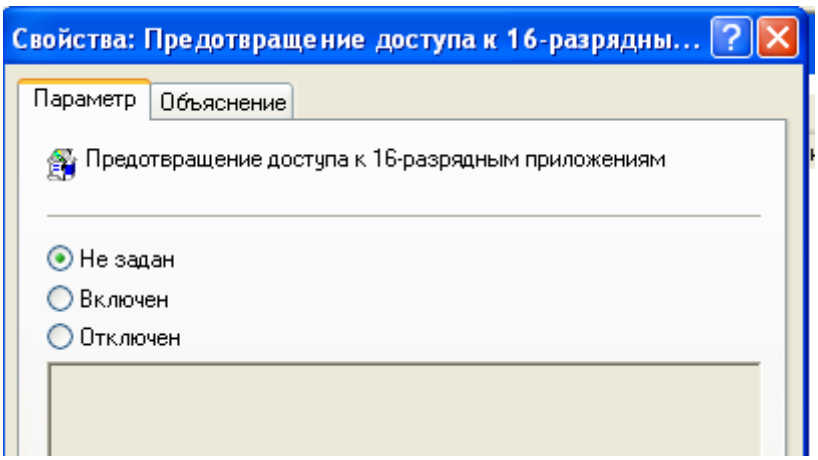

Рисунок 41: Настройки предотвращения доступа к 16-разрядным приложениям.

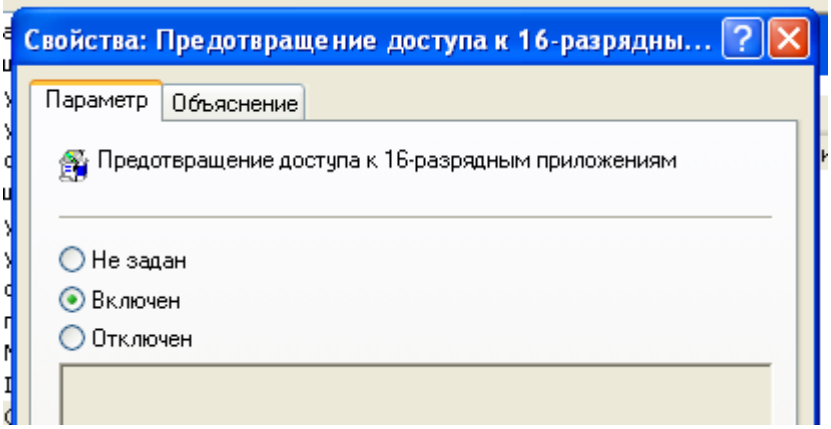

Рисунок 42: Новые настройки предотвращения доступа к 16-разрядным приложениям.

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

Для оснастки «Удалить команду «Свойства папки» из меню «Сервис» установим значение «Включен». 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.

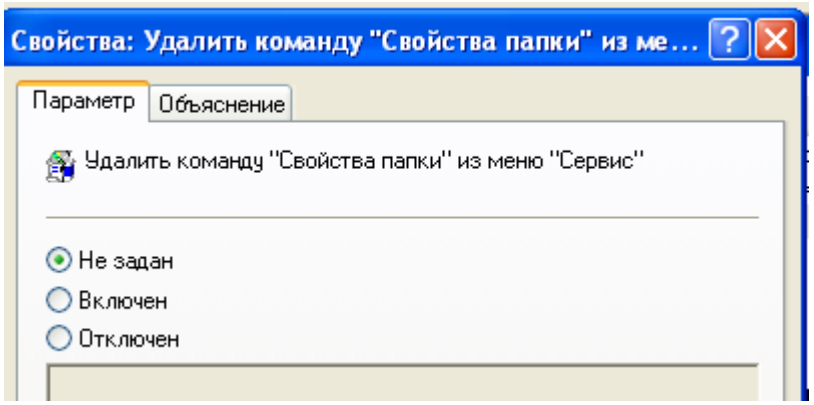

Рисунок 43: Настройки удаления команды "Свойства папки" из меню "Сервис".

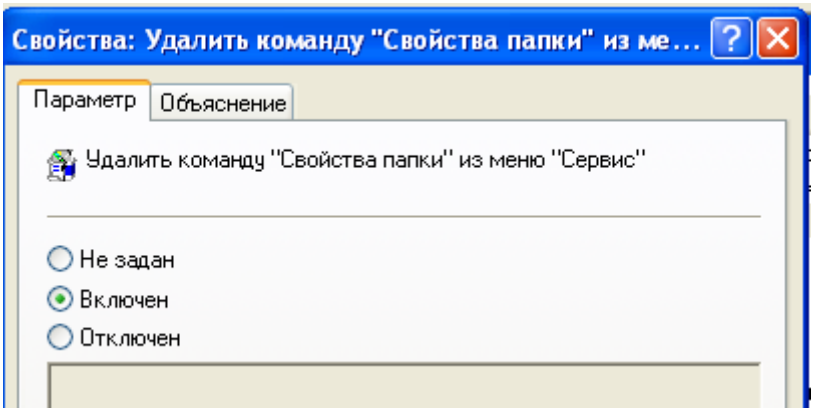

Рисунок 44: Новые настройки удаления команды "Свойства папки" из меню "Сервис".

Пуск → Выполнить → gpedit.msc → Групповые политики → 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.

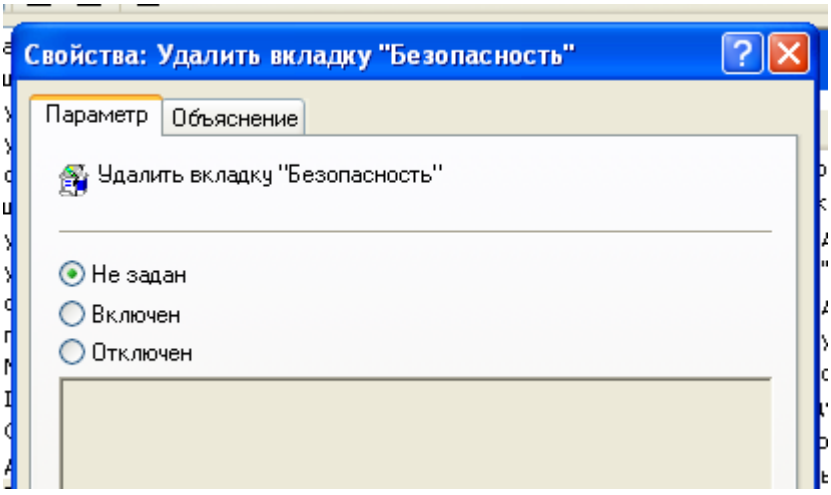

Рисунок 45: Настройки удаления вкладки "Безопасности".

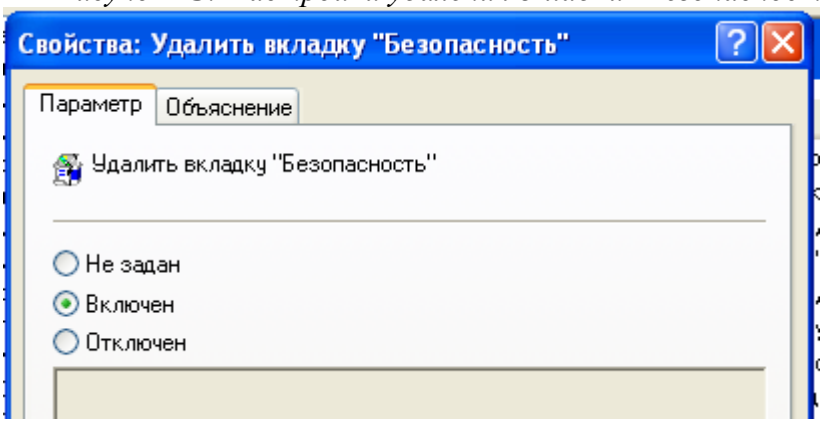

Рисунок 46: Новые настройки удаления вкладки "Безопасности".

Пуск → Выполнить → gpedit.msc → Групповые политики → 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.

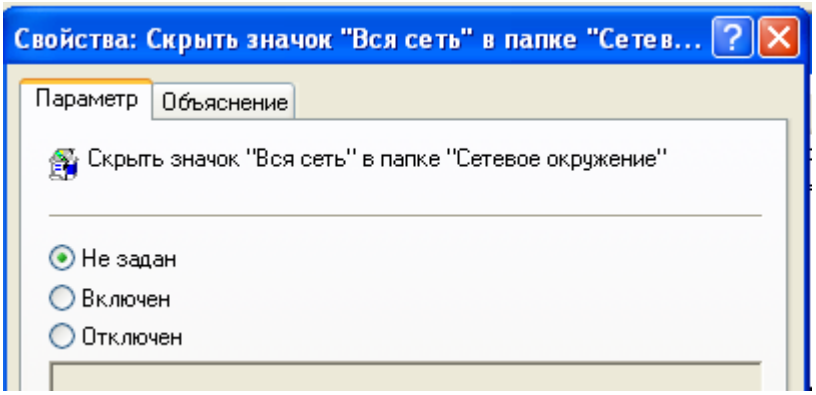

Рисунок 47: Настройки сокрытия значка "Вся сеть" в папке "Сетевое окружение".

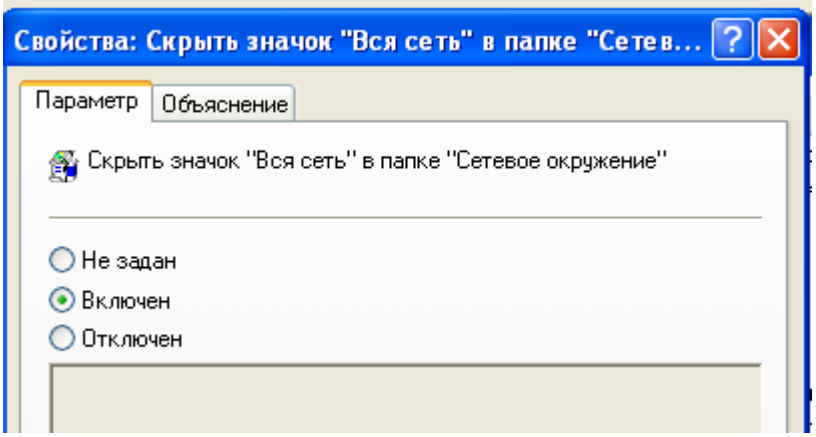

Рисунок 48: Новые настройки сокрытия значка "Вся сеть" в папке "Сетевое окружение".

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

Для оснастки «Запретить создание новых заданий» установим значение «Включен». При создании новых заданий пользователей, возможно ослабление защиты АРМ, так что отключим эту возможность.

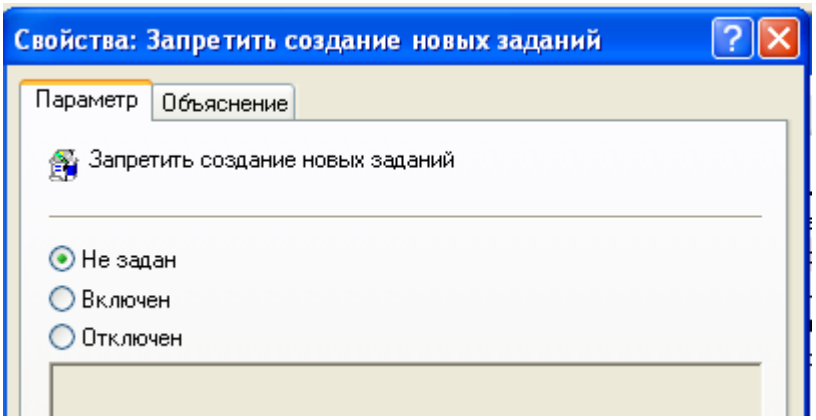

Рисунок 49: Настройки запрета создания новых заданий.

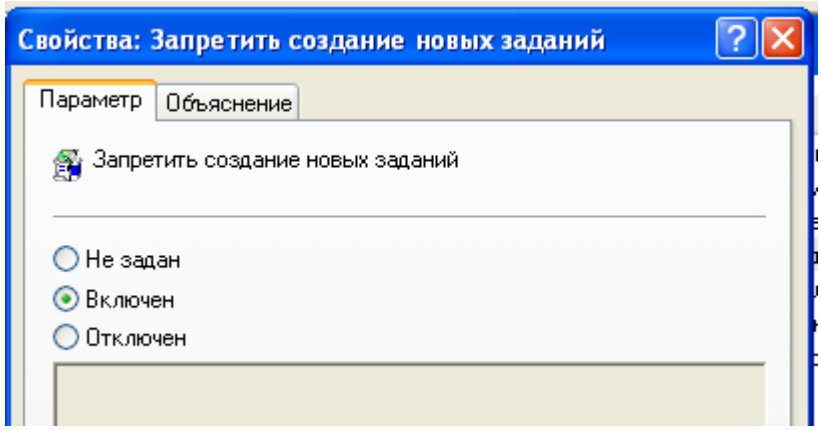

Рисунок 50: Новые настройки запрета создания новых заданий.

Пуск → Выполнить → gpedit.msc → Групповые политики → 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.

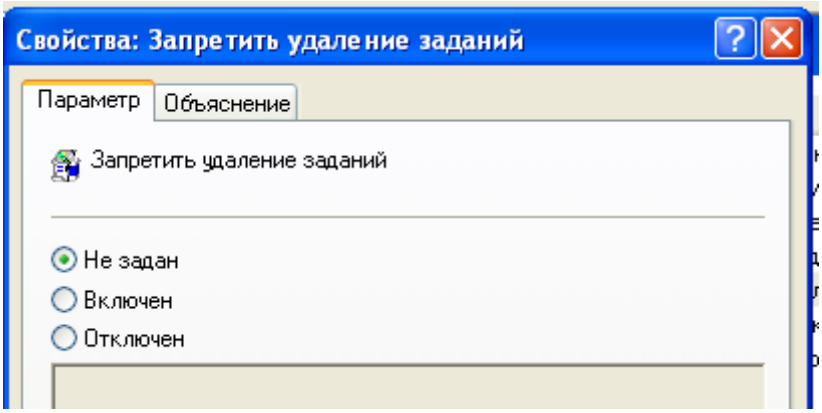

Рисунок 51: Настройки запрета удаления заданий.

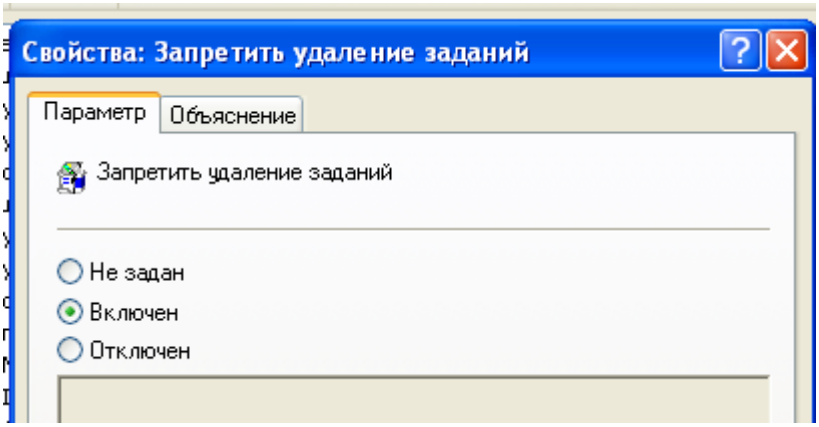

Рисунок 52: Новые настройки запрета удаления заданий.

Пуск → Выполнить → gpedit.msc → Групповые политики → 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.

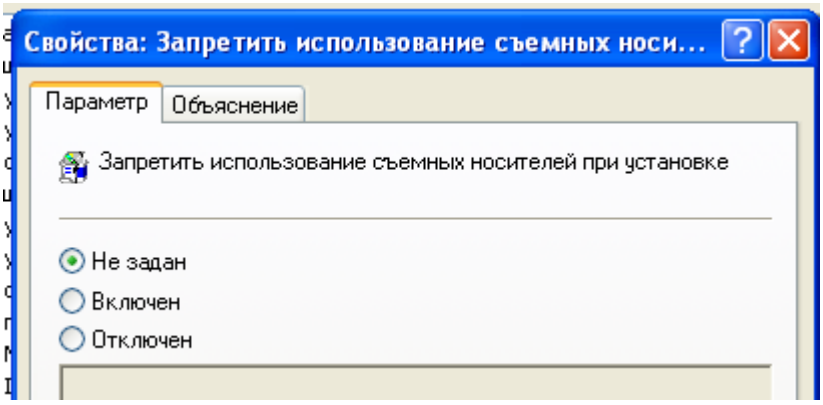

Рисунок 53: Настройки запрета использования съемных носителей при установке.

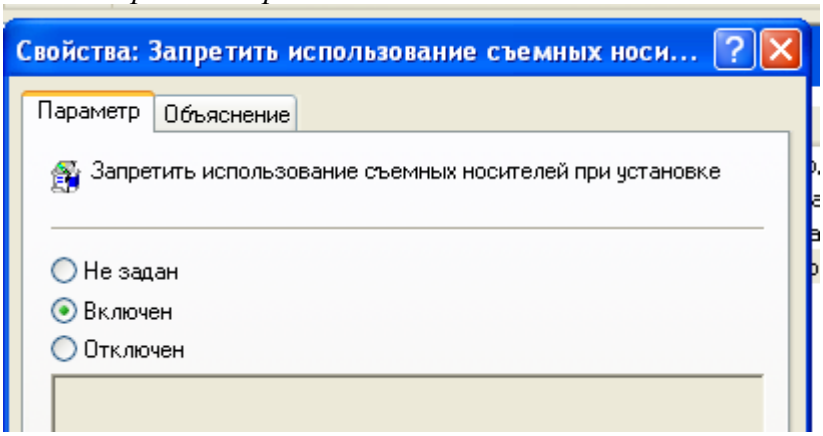

Рисунок 54: Новые настройки запрета использования съемных носителей при установке.

Пуск → Выполнить → gpedit.msc → Групповые политики → 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.

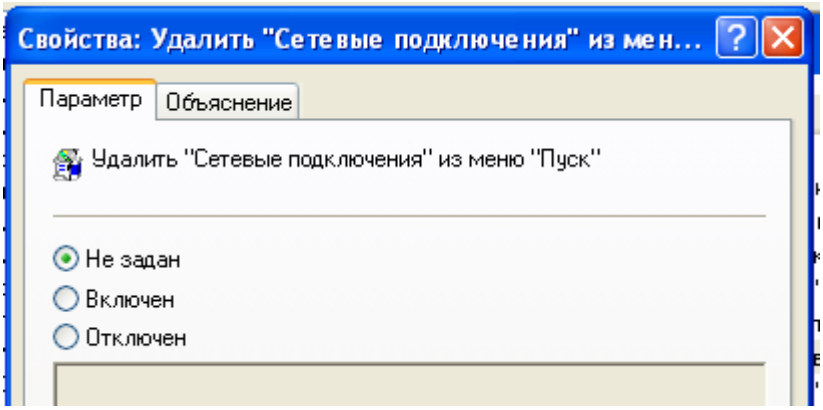

Рисунок 55: Настройки удаления "Сетевых подключений" из меню "Пуск".

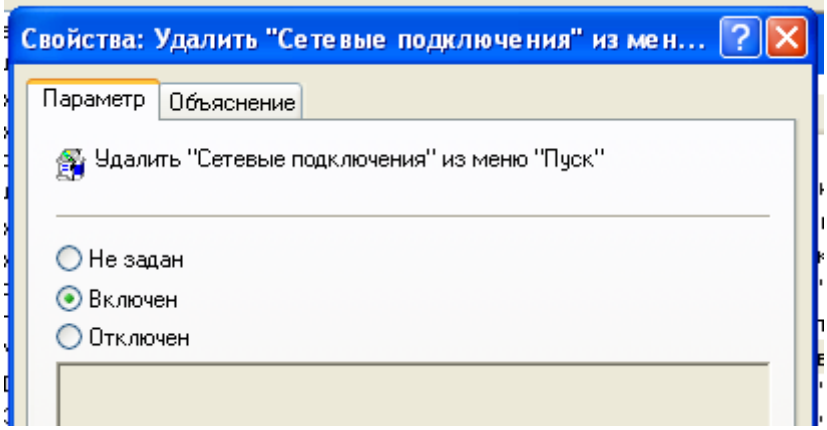

Рисунок 56: Новые настройки удаления "Сетевых подключений" из меню "Пуск".

Пуск → Выполнить → gpedit.msc → Групповые политики → 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.

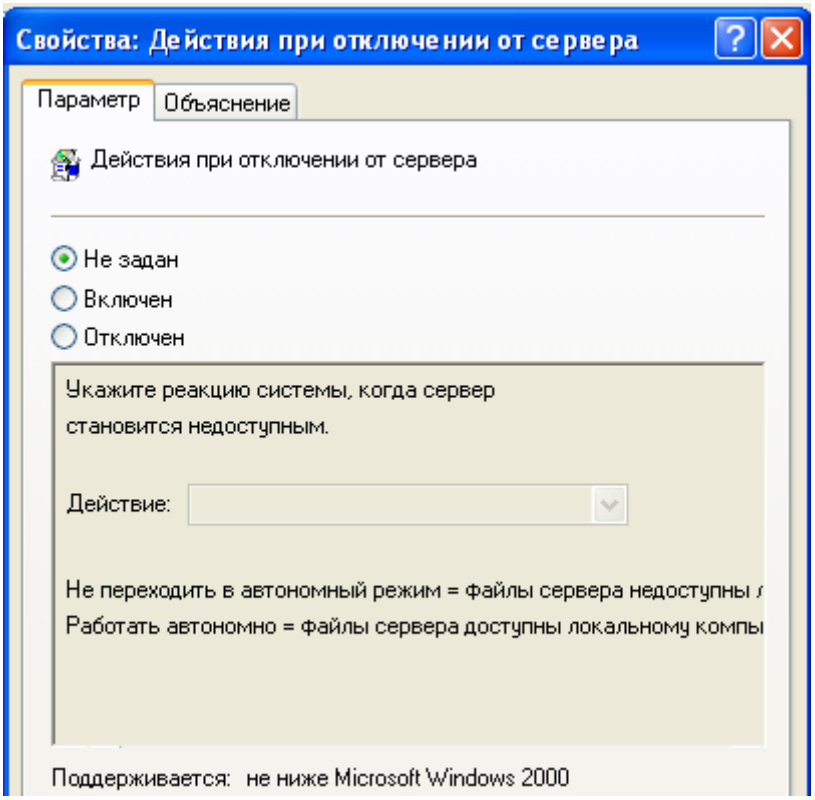

Рисунок 57: Настройки действий при отключении от сервера.

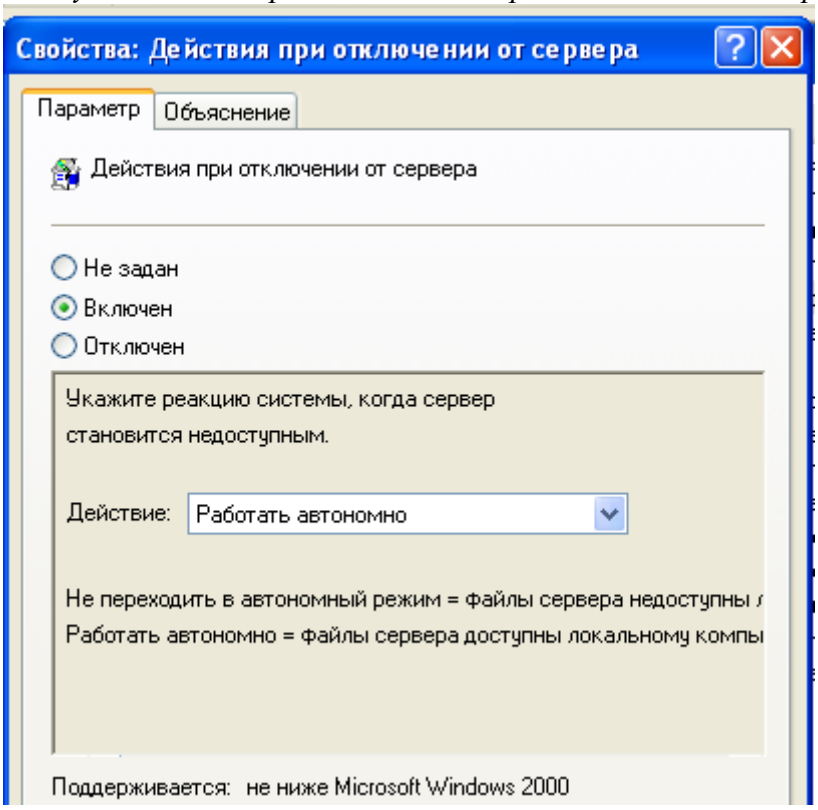

Рисунок 58: Новые настройки действий при отключении от сервера.

В процессе настройки дочернего узла «Административные шаблоны» в «Конфигурации пользователя» были произведены действия, направленные на повышение защищенности АРМ. Запрещены доступ к 16-разрядным приложениям, создание новых заданий, удаление заданий и использование съемных носителей при установке. 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 2Б, а именно требования о контроле доступа субъектов в систему, о регистрации и учете действий пользователей в системе, и о целостности приложений.

Также был повышен общий уровень защищенности системы.

Вывод:

В результате выполнения лабораторной работы изучен редактор локальной групповой политики и настроены групповые политики безопасности на автономном автоматизированном рабочем месте пользователя с установленной на нем операционной системой Windows для защиты информации от несанкционированного доступа с учетом требований информационной безопасности к информационной системе с классом защищенности 2Б. При этом указана последовательность команд для настройки каждой политики безопасности, приведены скриншоты процесса и результата настройки, обоснован выбор каждого из параметров с учетом соответствующих требований к системе с классом защищенности 2Б.