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 для защиты информации от несанкционированного доступа (НСД).

Используемое программное обеспечение: операционная система Windows XP.

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.

Объекты групповых политик делятся на две категории:

- *Доменные объекты групповых политик*, которые используются для централизованного управления конфигурацией компьютеров и пользователей, входящих в состав домена Active Directory. Эти объекты хранятся только на контроллере домена;
- *Локальные объекты групповых политик,* которые позволяют настраивать конфигурацию локального компьютера, а также всех пользователей, созданных на этом компьютере. Эти объекты хранятся только в локальной системе. Локальные объекты групповых политик могут применяться, даже если компьютер входит в состав домена.

Настройка политик

Откроем приложение «Групповая политика». Для этого воспользуемся комбинацией ***Win+R*** и введем команду ***gpedit.msc***.

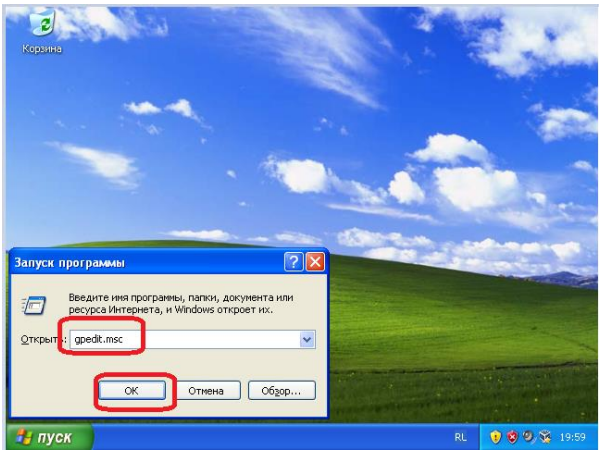


Рисунок 1 - Запуск программы

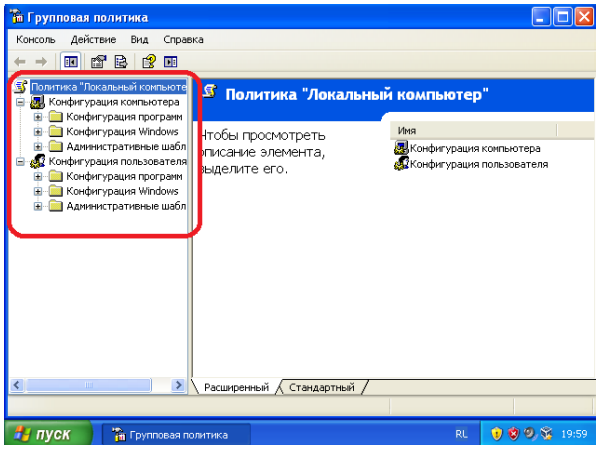


Рисунок 2 - Групповая политика

В оснастке редактора локальных объектов групповой политики присутствуют два основных узла. Рассмотрим и настроим каждый их них.

1.1 Конфигурация компьютера

Узел ***Конфигурация компьютера*** предназначен для настройки параметров компьютера. В этом узле расположены параметры, которые применяются к компьютеру, независимо от учетной записи пользователя, вошедшего в систему. Эти параметры применяются при запуске операционной системы и обновляются в фоновом режиме. Содержит три дочерних узла, при помощи которых настраиваются все параметры локальных объектов групповых политик:

- Конфигурация программ;
- Конфигурация Windows;
- Административные шаблоны.

1.1.1 Конфигурация Windows

Данный узел предназначен для обеспечения безопасности компьютера и учетной записи, для которой применяются данные политики.

1.1.1.1 Сценарий автозагрузки и завершения работы

Настроим сценарии автозагрузки и завершения работы. А именно: создадим и добавим скрипт, который позволит подсчитать количество файлов в папках C:\ и вывести собранную информацию в специально созданный для этого файл C:\CountFiles.csv. Это необходимо для того, что можно было проанализировать действия пользователя и выявить наличие изменений в файловую систему.

В корневой папке создадим файл *GetAllFiles.ps1*, в котором пропишем скрипт, подсчитывающий количество файлов в папке директории *C:/*.

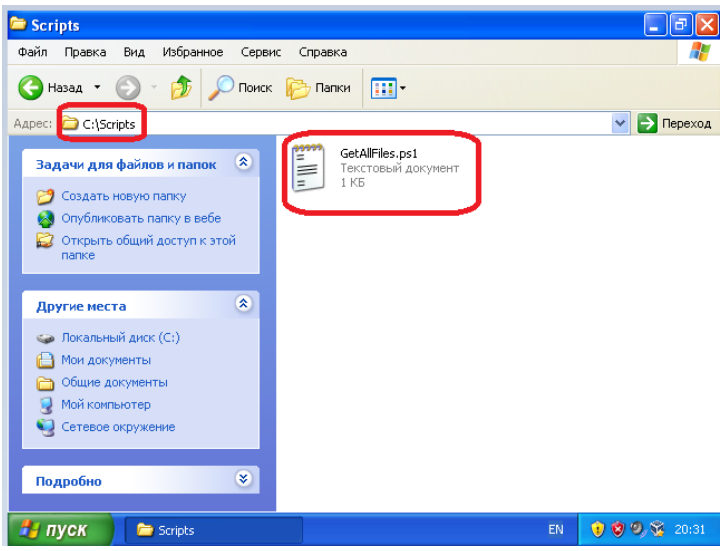


Рисунок 3 - Создание файла

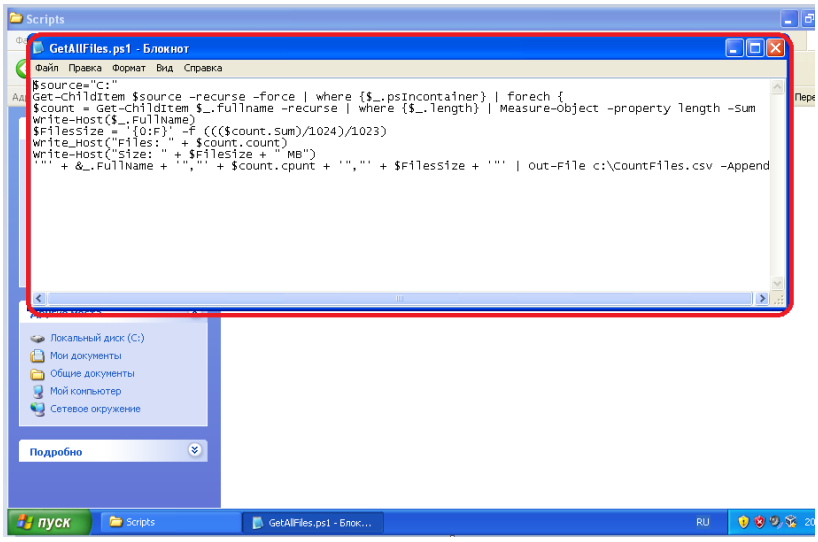


Рисунок 4 - Содержимое скрипта

Данный скрипт необходимо добавить в сценарий автозагрузки. Для этого перейдем в ***конфигурацию компьютера*** и в узел ***конфигурация windows***. Выберем ***сценарий автозагрузки*** и перейдем в свойства. Добавим написанный скрипт.

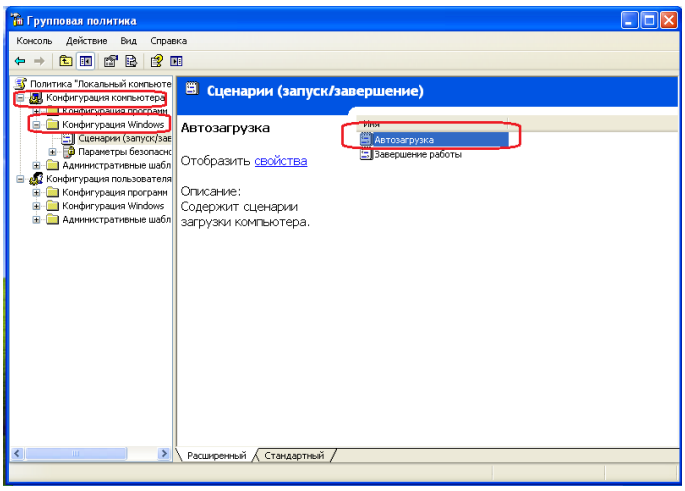


Рисунок 5 - Сценарий автозагрузки

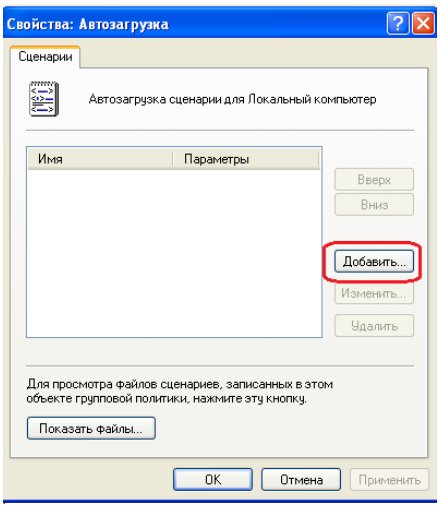


Рисунок 6 - Свойства сценария автозагрузки

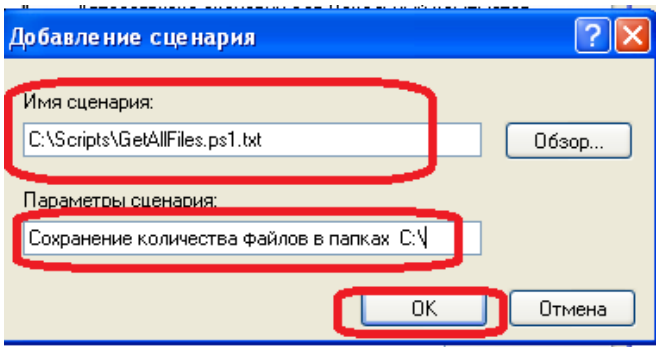


Рисунок 7 - Добавление сценария

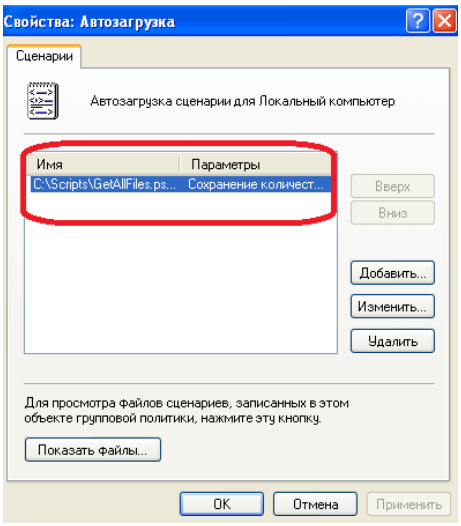


Рисунок 8 - Сценарий добавлен

Этот же скрипт необходимо добавить и в сценарий завершения работы. Выполним аналогичные шаги и убедимся в том, что нужный скрипт добавлен:

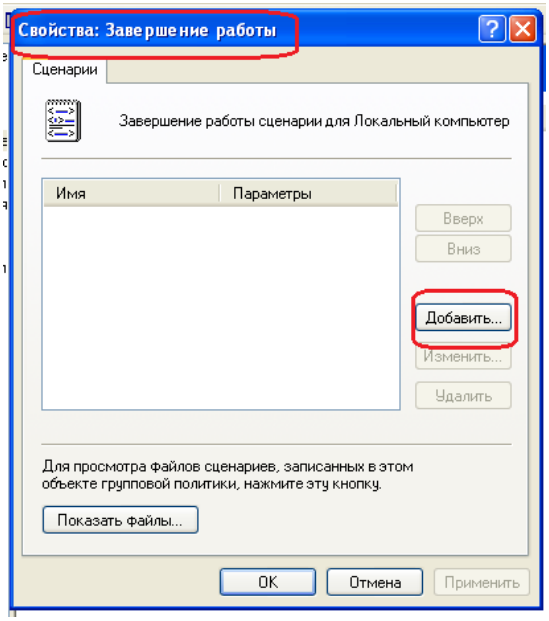


Рисунок 9 - Свойства сценария завершения работы

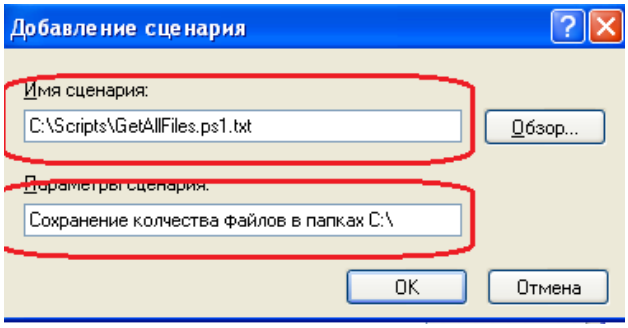


Рисунок 10 - Добавление сценария

1.1.1.2 Политика паролей и блокировки учетных записей

Политика учетных записей аналогична локальным политикам безопасности. Поэтому используем ранее применяемые настройки для настройки ***политики паролей*** и ***политики блокировки учетных записей*** с учетом требований к классу безопасности 1Д.

1.1.1.3 Политика безопасности IP

Настроим ***политику безопасности IP*** с целью ограничения выхода пользователя в интернет и передачи запроса безопасности при обращении к серверу. Убедимся в том, что ***Клиенту*** запрещаются все запросы, а разрешаются только ответы серверам, и что используется протокол проверки подлинности Kerberos. Для этого перейдем в ***Клиента*** и посмотрим свойства:

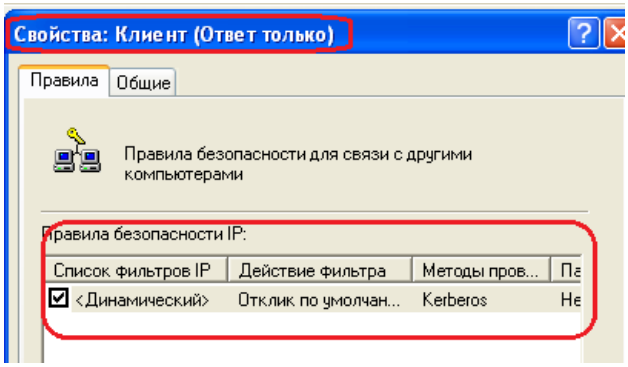


Рисунок 11 - Свойства клиента

Убедимся в том, что при обращении к ***серверу*** вначале передается запрос безопасности, а также, что для всех видов трафика требуется использование проверки подлинности с помощью протокола Kerberos:

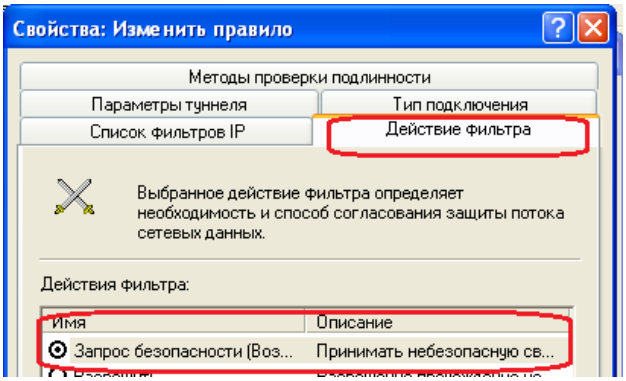


Рисунок 12 – Действие фильтра

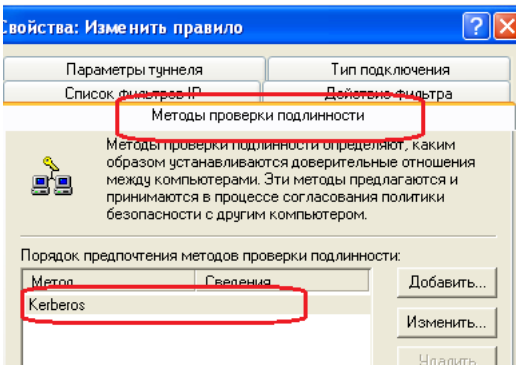


Рисунок 13 - Методы проверки подлинности

1.1.2 Административные шаблоны

Данный узел включает параметры для приложений и компонентов операционной системы Windows.

1.1.2.1 Запрет удаленного управления рабочим столом

Настроим запрет удаленного управления рабочим столом. Данная настройка необходима, так как поможет избежать несанкционированного доступа. Для настройки перейдем в узел ***NetMeeting,*** в узел ***запретить удалённое управление рабочим столом***:

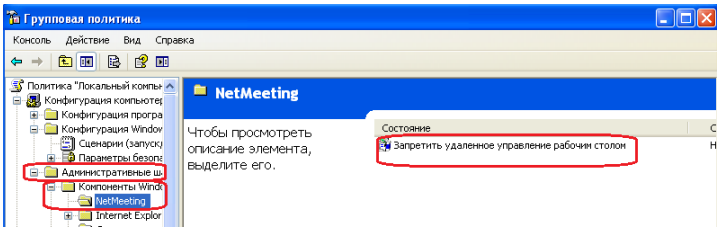


Рисунок 14 - NetMeeting

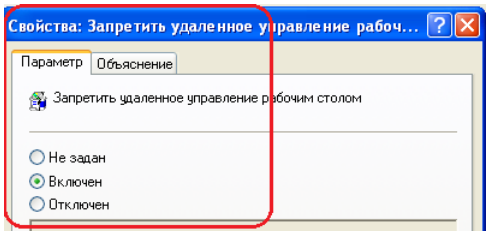


Рисунок 15 - Включение запрета

1.1.2.2 Выключение журнала событий справки приложения

Настроим выключение журнала событий справки приложения. Данная настройка необходима для отслеживания источника запуска приложений и блокировки несовместимых приложений с уведомлением пользователя. Для настройки перейдем в узел

совместимость приложений, в узел ***выключить журнал событий справки приложения***:

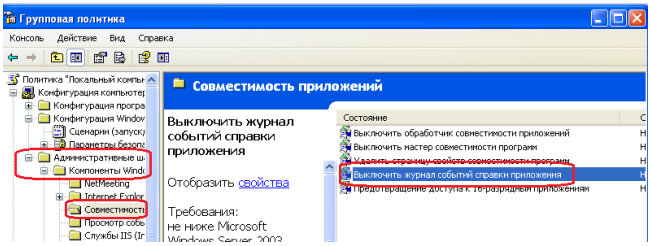


Рисунок 16 - Совместимость приложений

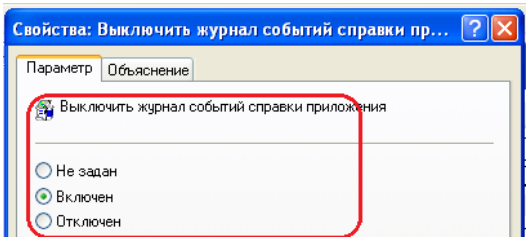


Рисунок 17 - Выключение

1.1.2.3 Предотвращение доступа к 16-разрядным приложениям

Настроим предотвращение доступа к 16-разрядным приложениям. Данная настройка необходима, так как приложения меньшей разрядности могут вызвать проблемы совместимости или же могут открыть доступ злоумышленнику к операционной системе. Для данной настройки перейдем в узел ***совместимость приложений***, в узел ***предотвращение доступа к 16-разрядным приложениям*** и включим данный параметр:

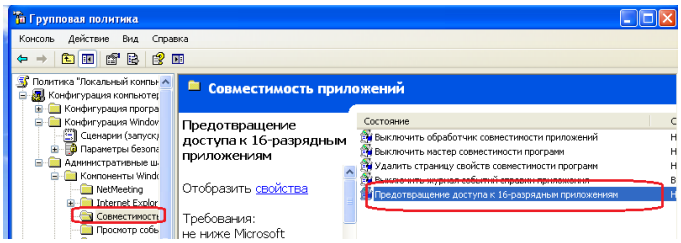


Рисунок 18 - Совместимость приложений

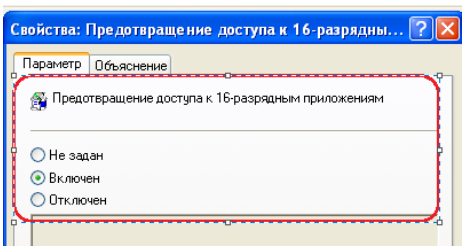


Рисунок 19 - Включение

1.1.2.4 Включение центра обеспечения безопасности

Настройка включения центра обеспечения безопасности. Данная настройка необходима, так как данный центр наблюдает за основными параметрами безопасности (антивирус, брандмауэр, автоматическое обновлении т.п.) и уведомляет пользователей, если их компьютеры подвержены опасности. Для этого перейдем в узел ***центр обеспечения безопасности***, в параметр ***включить центр обеспечения безопасности***:

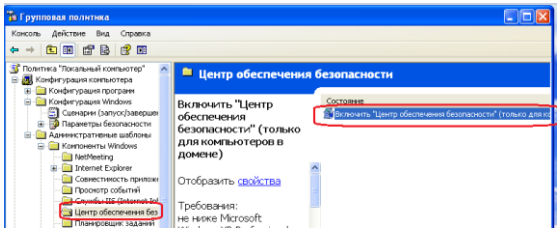


Рисунок 20 - Центр обеспечения безопасности

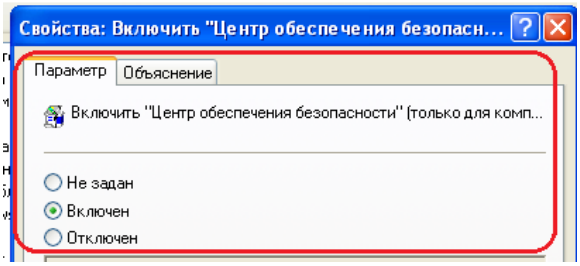


Рисунок 21 - Включение

1.1.2.5 Запрет удаления заданий

Настройка запрета удаления заданий. Данная настройка необходима, так как такие возможности должны быть только у администратора. Для этого перейдем в узел ***планировщик заданий***, в параметр ***запретить удаление заданий***:

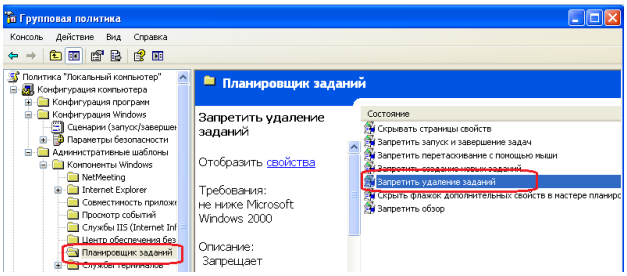


Рисунок 22 - Планировщик заданий

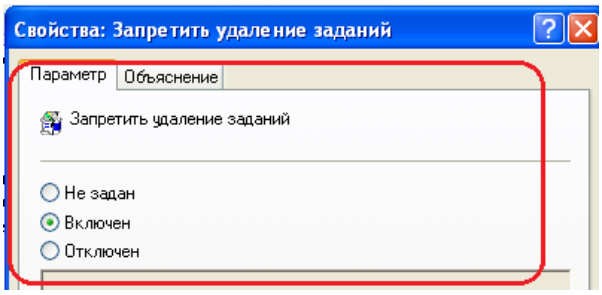


Рисунок 23 - Включение параметра

1.1.2.6 Удаление элемента из меню «Пуск»

Настройка удаления элемента «Безопасность Windows» из меню Пуск. Данная настройка необходима, так как необходимо исключить доступ пользователя к настройкам безопасности. Для этого перейдем в узел ***службы терминалов***, в ***параметр удалить элемент «Безопасность Windows» из меню Пуск***:

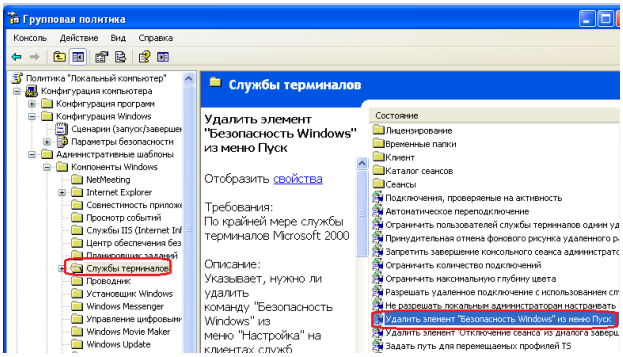


Рисунок 24 - Службы терминалов

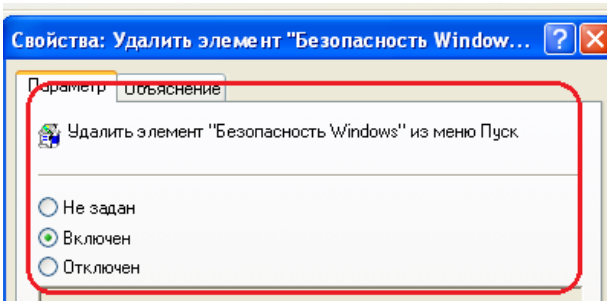


Рисунок 25 - Включение

1.1.2.7 Включение защищенного режима протокола оболочки

Настройка включения защищенного режима протокола оболочки. Данная настройка необходима, так как ограничения запуска некоторых файлов из приложений и исключить возможность изменений, которые могут повредить работоспособности ОС и безопасности АРМ. Для этого перейдем узел ***проводник***, в параметр ***отключить защищенный режим протокола оболочки***:

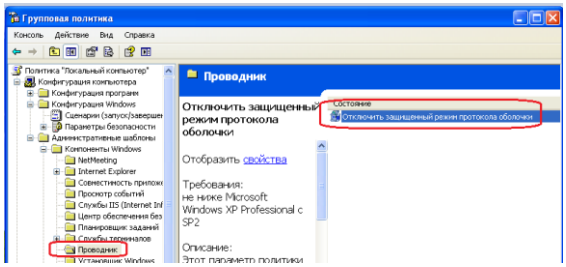


Рисунок 26 - Проводник

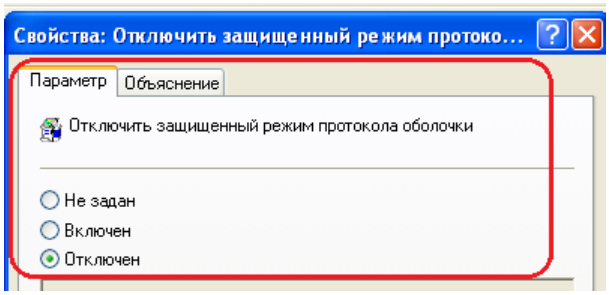


Рисунок 27 - Отключение

1.1.2.8 Ведение журнала запуска и установки приложений

Настройка ведения журнала запуска и установки приложений. Данная настройка необходима, так как необходимо вести журнал событий с целью мониторинга системы и контроля следования политике безопасности предприятия для своевременного обнаружения угроз. Для этого перейдем узел ***установщик Windows***, в параметр ***ведение журнала***:

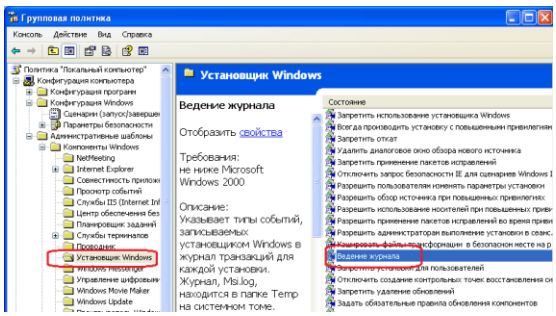


Рисунок 28 - Установщик Windows

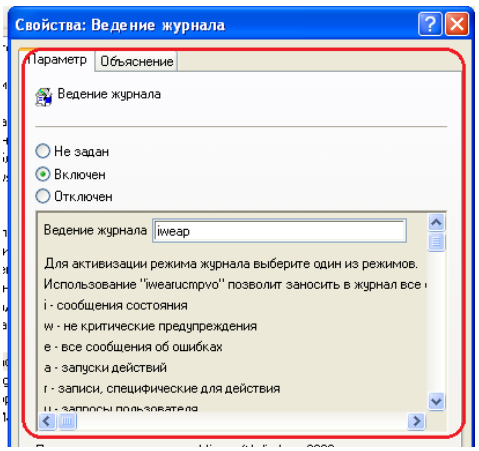


Рисунок 29 - Включение

1.1.2.9 Автоматическое обновление системы

Настройка ***автоматического обновления системы***. Данная настройка необходима, так как злоумышленник может воспользоваться уязвимостями не обновлённой системы. этого перейдем в узел ***Windows Update***, в параметр ***настройка автоматического обновления***:

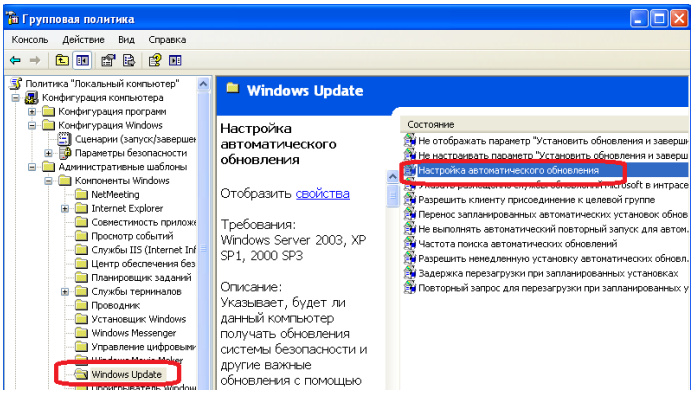


Рисунок 30 - Настройка автоматического обновления

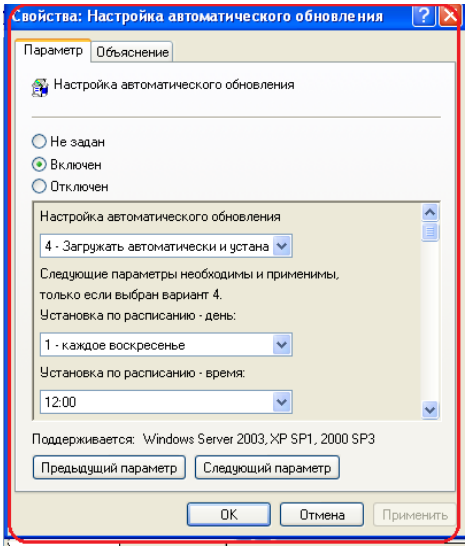


Рисунок 31 - Включение

Обновление ОС занимает время и ресурсы АРМ, во время обновления невозможно пользоваться АРМ, поэтому необходимо настроить автоматическое обновление системы, которое будет осуществляться в нерабочее время пользователя.

1.2 Конфигурация пользователя

Узел *Конфигурация пользователя*, который предназначен для настроек параметров пользователей. Параметры, которые находятся в этом узле, применяются при входе конкретного пользователя в систему. Так же, как и параметры, расположенные в узле конфигурации компьютера, параметры, расположенные в узле конфигурации пользователя обновляются в фоновом режиме. Также содержит три дочерних узла, при помощи которых настраиваются все параметры локальных объектов групповых политик:

- Конфигурация программ;
- Конфигурация Windows;
- Административные шаблоны.

1.2.1 Конфигурация Windows

1.2.1.1 Настройка резервного копирования системы

Напишем скрипт *GetBackup.ps1*, который при каждом выходе пользователя из системы будет делать ее резервную копию. Этот скрипт позволит обезопасить пользователя от потери информации и вызванных этим простоев. Также письмо, генерируемое скриптом и отправляемое системному администратору, позволит последнему быть в курсе происходящего на АРМ.

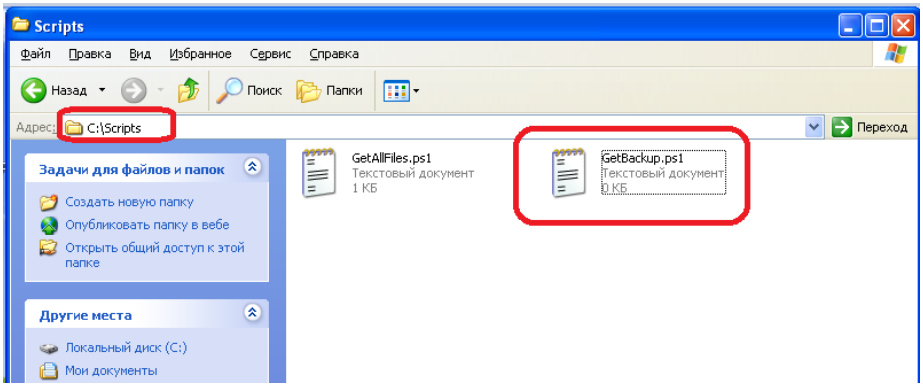


Рисунок 32 - Создание файла

Добавим данный скрипт в сценарий выхода из системы. Для этого перейдем в узел ***конфигурация Windows***, в ***сценарии***, в ***сценарий выхода из системы***:

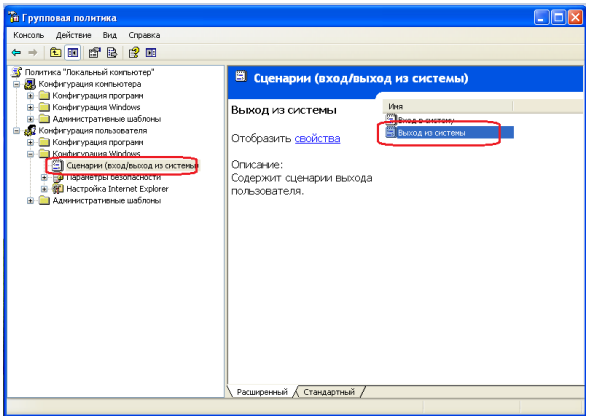


Рисунок 33 - Сценарий выхода из системы

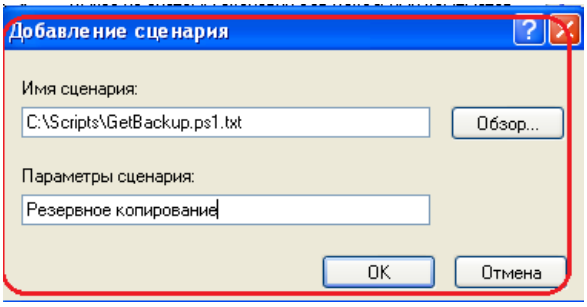


Рисунок 34 - Добавление сценария

Напишем скрипт *KillOldBackups.ps1*, который будет сканировать папку, содержащую резервные копии, и смотреть на дату находящихся там резервных копий, и удалять все резервные копии старше месяца. Это необходимо для того, чтобы сэкономить вычислительные ресурсы и не хранить устаревшую информацию.

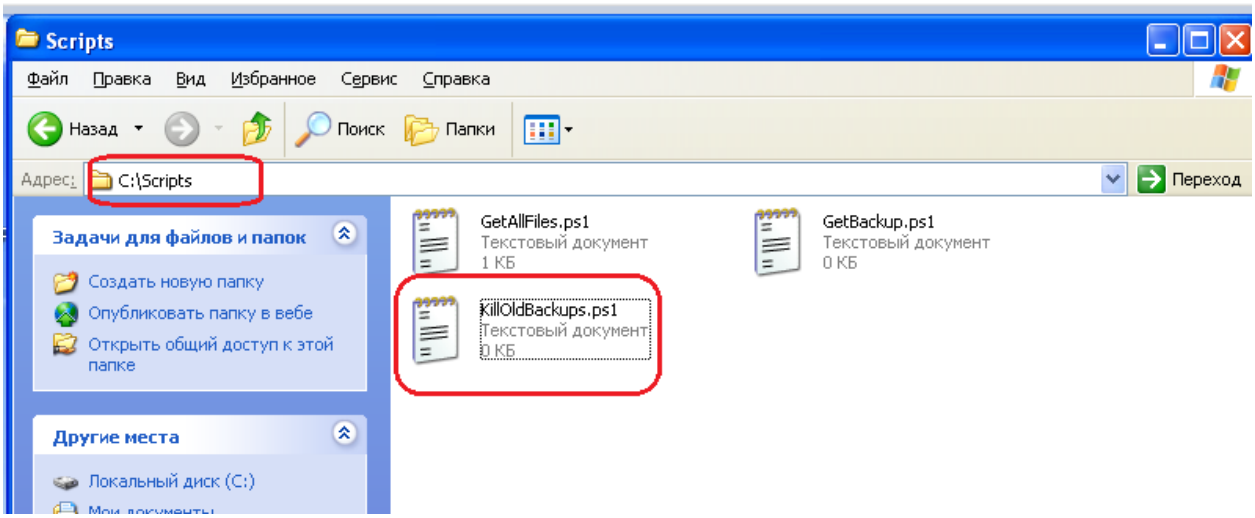


Рисунок 35 - Создание файла

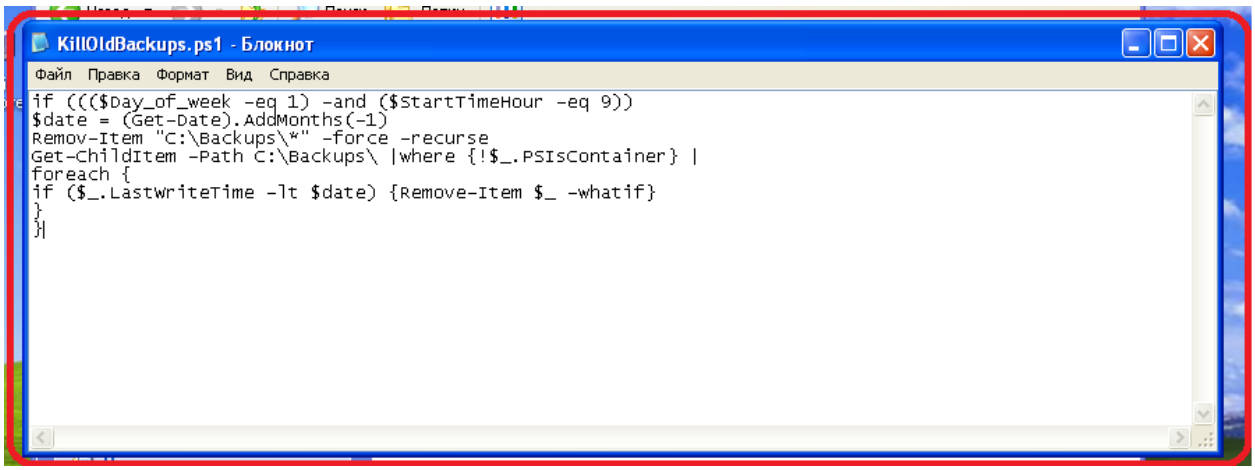


Рисунок 36 - Скрипт для удаления старых копий

Аналогично добавим данный скрипт в сценарий входа в систему. Для этого перейдем в узел ***конфигурация Windows***, в ***сценарии***, в ***сценарий входа в систему***:

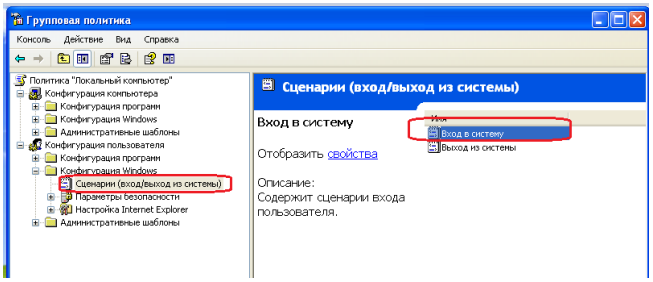


Рисунок 37 - Сценарий входа в систему

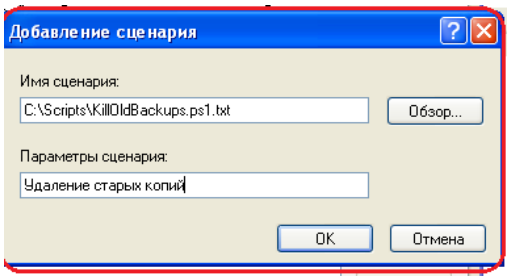


Рисунок 38 - Добавление сценария

1.2.1.2 Настройки Internet Explorer

Данная настройка параметров используемого прокси-сервера необходимо для запрета пользователю выхода в интернет. Для этого перейдем в узел ***настройки Internet Explorer***, в узел ***подключения***, в узел ***параметры прокси-сервера***:

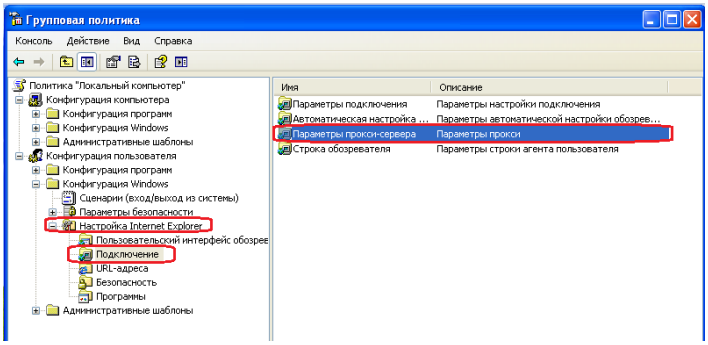


Рисунок 39 - Параметры прокси-сервера

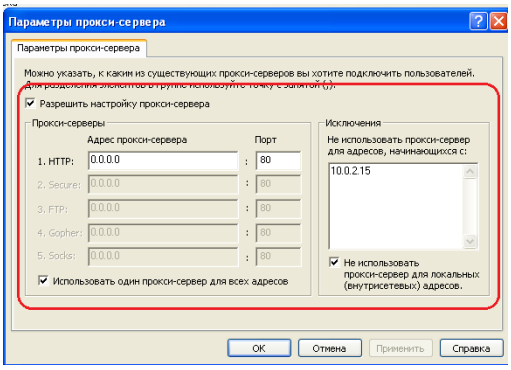


Рисунок 40 - Настройка параметров прокси-сервера

В качестве адреса для всех адресов был использован несуществующий адрес. Однако на АРМ сервера должны быть отправлены резервные копии, поэтому его необходимо указать как внутрисетевой адрес. Проверить IP можно через утилиту командной строки *ipconfig*.

1.2.2 Административные шаблоны

Для пользователя административные шаблоны представляют собой настройки, связанные с интерфейсом АРМ.

1.2.2.1 Запрет доступа к 16-разрядным приложениям

Настроим предотвращение доступа к 16-разрядным приложения. Данная настройка необходима, т.к. запуск приложений меньшей разрядности может вызвать проблемы совместимости. Помимо этого, 16-разрядные приложения небезопасны, что может стать уязвимостью для данного АРМ. Для настройки перейдем в узел ***административные шаблоны***, в узел ***компоненты Windows***, в узел ***совместимость приложений***, в узел ***предотвращение доступа к 16-разрядным приложениям***:

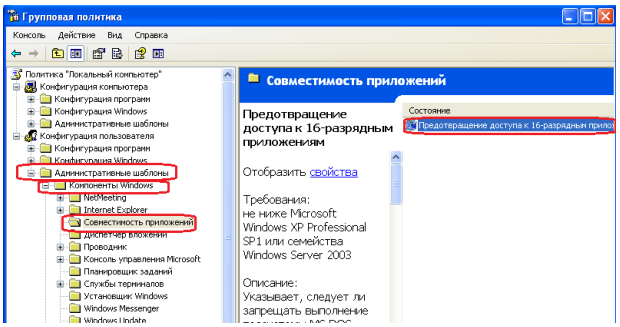


Рисунок 41 - Предотвращение доступа к 16-разрядным приложениям

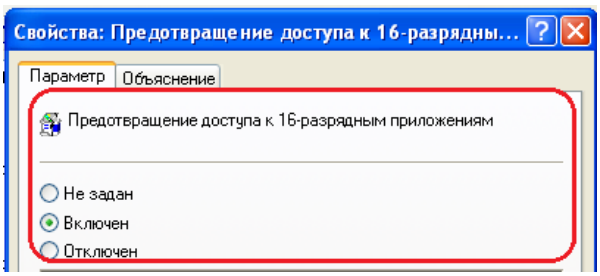


Рисунок 42 - Включение

1.2.2.2 Удаление команды «Свойства папки» из меню «Сервис»

Настроим удаление команды «свойства папки» из меню «сервис». Данная настройка необходима, т.к. в противном случае пользователь сможет видеть скрытые и системные файлы, изменение которых влечет возникновение ошибок в работе системы. Для настройки перейдем в узел ***административные шаблоны***, в узел ***компоненты Windows***, в узел ***проводник***, в узел ***удалить команду «Свойства папки» из меню «Сервис»***:

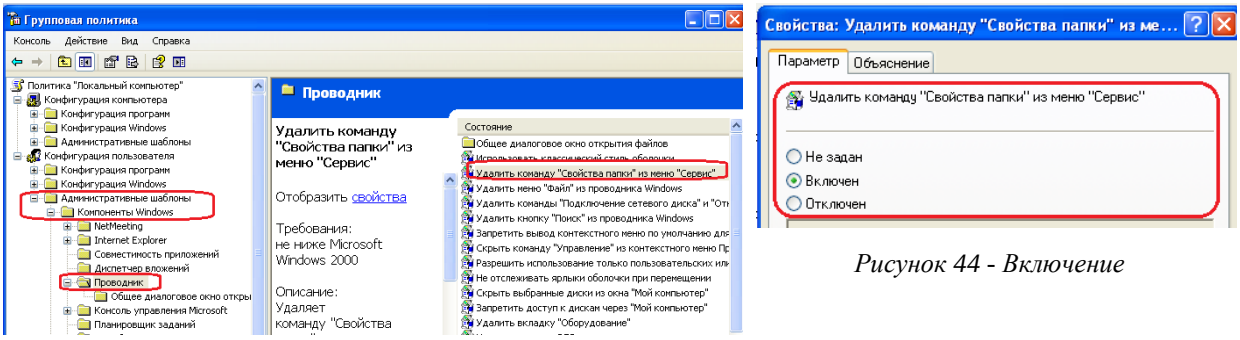


Рисунок 44 - Включение

Рисунок 43 - Удаление команды

1.2.2.3 Удаление вкладки «Безопасность»

Настроим удаление вкладки безопасность. Данная настройка необходима, так как в целях сохранения безопасности нельзя допускать возможность изменения каких-то настроек из системы самим пользователем. Для настройки перейдем в узел ***административные шаблоны***, в узел ***компоненты Windows***, в узел ***проводник***, в узел ***удалить вкладку «Безопасность»:***

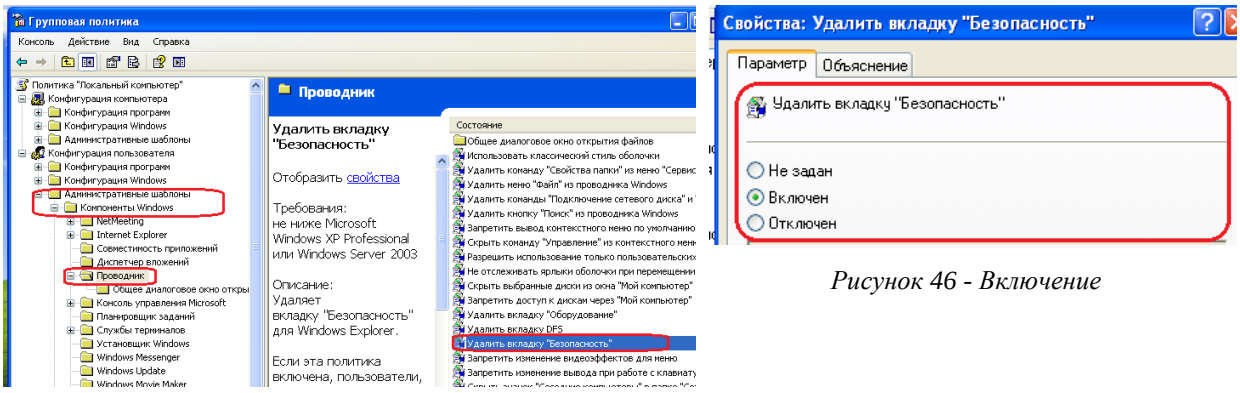


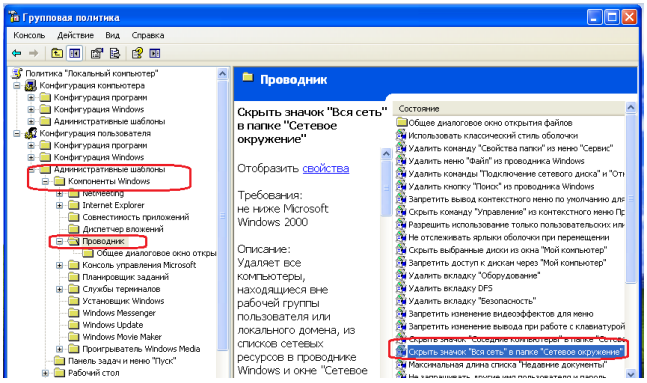
Рисунок 46 - Включение

Рисунок 45 - Удаление вкладки

1.2.2.4 Скрытие значка «Вся сеть» в папке «Сетевое окружение»

Настроим скрытие значка «Вся сеть» в папке «Сетевое окружение». Данная настройка необходима, так как при доступе злоумышленника данный значок даст ему просмотр и понимание всей сети. Для настройки перейдем в узел ***административные***

шаблоны, в узел ***компоненты Windows***, в узел ***проводник***, в узел ***скрыть значок «Вся сеть» в папке «Сетевое окружение»:***



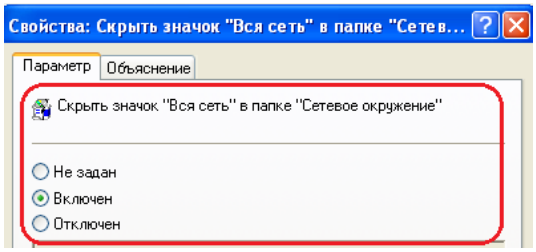
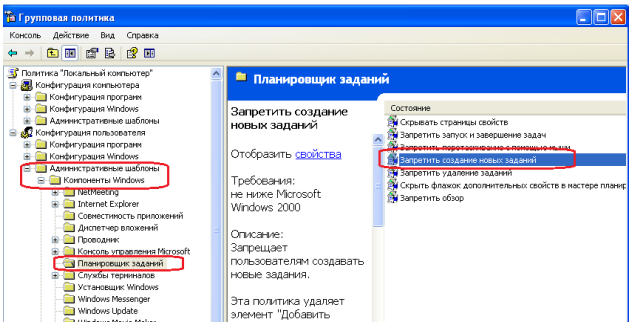


Рисунок 48 - Включение

Рисунок 47 - Скрытие значка

1.2.2.5 Запрет создания новых заданий

Настроим запрет создания новых заданий. Данная настройка необходима, так как доступ к созданию новых заданий должен быть только у администратора. Для настройки перейдем в узел ***административные шаблоны***, в узел ***компоненты Windows***, в узел ***планировщик заданий***, в узел ***запретить создание новых заданий***:



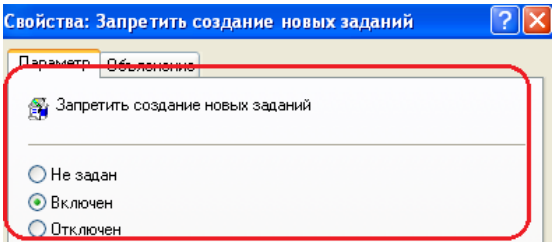


Рисунок 50 - Включение

Рисунок 49 - Запрет создания новых заданий

1.2.2.6 Запрет удаления заданий

Настроим запрет удаления новых заданий. Данная настройка необходима, так как доступ к созданию новых заданий должен быть только у администратора. Для настройки перейдем в узел ***административные шаблоны***, в узел ***компоненты Windows***, в узел ***планировщик заданий***, в узел ***запретить удаление заданий***:

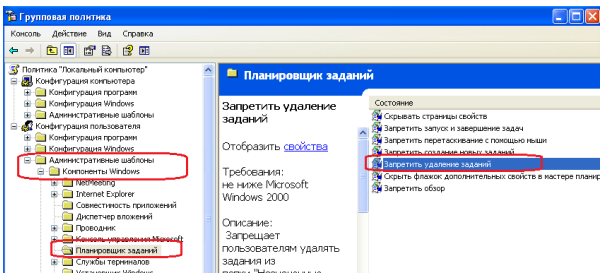


Рисунок 51 - Запрет удаления заданий

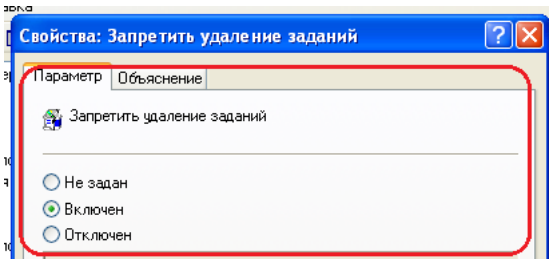


Рисунок 52 - Включение

1.2.2.7 Запрет использования съемных носителей при установке

Настроим запрет использования съемных носителей при установке. Данная настройка необходима, так как использование личных съемных носителей пользователей запрещается в соответствие с требованиями к классу безопасности 1Д. Для настройки перейдем в узел ***административные шаблоны***, в узел ***компоненты Windows***, в узел ***установщик Windows***, в узел ***запретить использование съемных носителей при установке***:

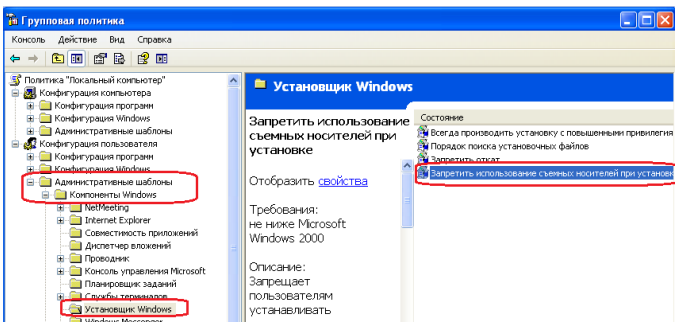


Рисунок 53 - Запрет использования съемных носителей

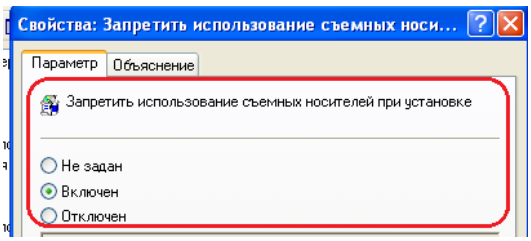


Рисунок 54 - Включение

1.2.2.8 Удаление «Сетевых подключений» из меню «Пуск»

Настроим удаление «сетевых подключений» из меню «пуск». Данная настройка необходима, чтобы пользователь не мог поменять прокси-сервер для выхода в интернет. Для настройки перейдем в узел ***административные шаблоны***, в узел ***панель задач и меню «Пуск»***, в узел ***удалить «Сетевые подключения из меню «Пуск»:***

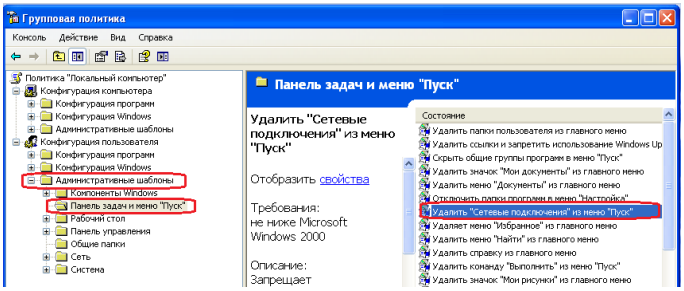


Рисунок 55 - Удаление сетевого подключения

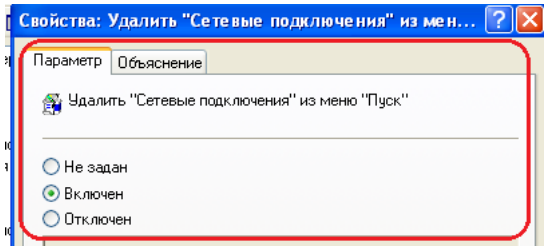


Рисунок 56 - Включение

1.2.2.9 Действия при отключении от сервера

Настроим действия при отключении от сервера. Данная настройка необходима, чтобы при отключении от сервера произошла повторная синхронизация с сервером. Для настройки перейдем в узел ***административные шаблоны***, в узел ***сеть***, в узел ***автономные файлы***, в узел ***действия при отключении от сервера***:

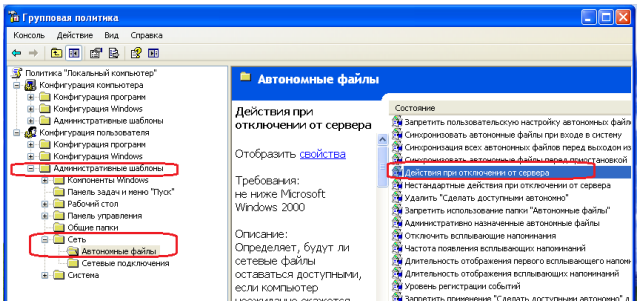


Рисунок 57 - Настройка действия при отключении от сервера

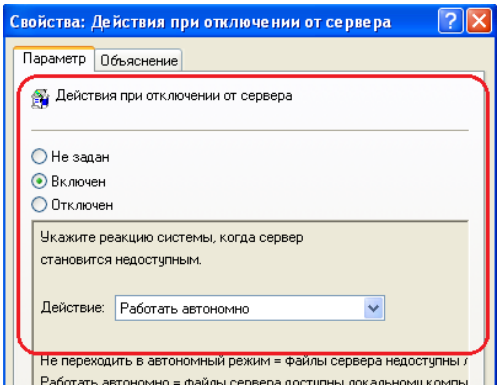


Рисунок 58 - Включение

Выводы: в ходе выполнения лабораторной работы был изучен редактор локальной групповой политики и настроены групповые политики безопасности на автономном автоматизированном рабочем месте (АРМ) пользователя с установленной на нем операционной системой Windows для защиты информации от несанкционированного доступа (НСД) для класса защищенности 1Д.

В узле ***конфигурация компьютера*** были настроены параметры локальных объектов групповых объектов через дочерние узлы ***конфигурация Windows*** и ***административные шаблоны.***

В рамках настройки параметров узла ***конфигурация Windows конфигурации компьютера*** были настроены сценарии автозагрузки и завершения работы с целью

возможности анализа действия пользователя и выявления наличия изменений в файловой системе. Также была настроена политика безопасности IP с целью ограничения выхода пользователя в интернет и передачи запроса безопасности при обращении к серверу.

В рамках настройки параметров узла ***административные шаблоны конфигурации компьютера*** были настроен запрет удаленного управления рабочим столом с целью избежания несанкционированного доступа, настроено выключение журнала событий справки приложения с целью отслеживания источника запуска приложений и блокировки несовместимых приложений с уведомлением пользователя, настроено предотвращение доступа к 16-разрядным приложениям с целью исключения проблемы совместимости или же открытия доступа злоумышленнику к операционной системе. Так же было настроено включение центра обеспечения безопасности с целью наблюдения за основными параметрами безопасности (антивирус, брандмауэр, автоматическое обновлении т.п.) и уведомления пользователей об опасности. Настроен запрет удаления заданий с целью запрета изменения конфигурации заданий. Настроено удаление элемента «Безопасность Windows» из меню Пуск с целью исключения доступа пользователя к настройкам безопасности. Настроено включение защищенного режима протокола оболочки с целью ограничения запуска некоторых файлов из приложений и исключения возможности изменений, которые могут повредить работоспособности ОС и безопасности АРМ. Также было настроено ведение журнала запуска и установки приложений с целью мониторинга системы и контроля следования политике безопасности предприятия для своевременного обнаружения угроз. Настроено автоматическое обновление системы с целью исключения возможности воспользоваться уязвимостями не обновлённой системы.

В узле ***конфигурация пользователя*** были настроены параметры локальных объектов групповых объектов через дочерние узлы ***конфигурация Windows*** и ***административные шаблоны.***

В рамках настройки параметров узла ***конфигурация Windows конфигурации пользователя*** были настроены сценарии входа и выходы из системы с целью избежания потери информации и вызванных этим простоев, а также разгрузки вычислительных ресурсов и удаления неактуальной информации.

В рамках настройки параметров узла ***административные шаблоны конфигурации пользователя*** было настроено предотвращение доступа к 16-разрядным приложения с целью исключения проблемы совместимости или же открытия доступа злоумышленнику к операционной системе, настроено удаление команды «свойства папки» из меню «сервис»,

с целью скрытия скрытых и системных файлов, изменение которых влечет возникновение ошибок в работе системы. Также было настроено удаление вкладки безопасность в целях сохранения безопасности нельзя допускать возможность изменения каких-то настроек из системы самим пользователем, настроено скрытие значка «Вся сеть» в папке «Сетевое окружение» с целью исключения доступа злоумышленника к просмотру и пониманию всей сети. Был настроен запрет удаления и создания новых заданий, так как данные возможности должны быть только у администратора. Также настроен запрет использования съемных носителей при установке в соответствие с требованиями к классу безопасности 1Д, настроено удаление «сетевых подключений» из меню «пуск» с целью предотвращения изменения прокси-сервер для выхода в интернет, настроены действия при отключении от сервера с целью устранения простоя.