МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Институт радиоэлектроники и информационных технологий

ОТЧЕТ

по лабораторной работе №3

«Групповые политики, анализ и настройка безопасности Windows Server»

по дисциплине

«Программное обеспечение вычислительных сетей»

РУКОВОДИТЕЛЬ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_ Кочешков А. А.\_\_

(подпись) (фамилия, и.,о.)

СТУДЕНТ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Игнаков К. М.\_\_\_

(подпись) (фамилия, и.,о.)

\_\_\_\_\_\_19-ВМ\_\_\_\_\_\_\_\_

(шифр группы)

Работа защищена «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_

С оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Нижний Новгород 2022

# Цель работы

Изучить и опробовать системные средства Windows Server, предназначенные для получения информации о системе и настройки безопасности.

Наблюдение за событиями в системе.

Оснастка «Просмотр событий»

"Просмотр событий" (Event Viewer) – это инструмент в Windows, который предназначен для просмотра и анализа событий, записанных в журналы событий системы. Это могут быть события, связанные с программным обеспечением, железом, сетью и т.д. Это позволяет администратору контролировать работу системы и идентифицировать возможные проблемы. Информация, записанная в журналы событий, может быть использована для просмотра трейсов и анализа проблем.

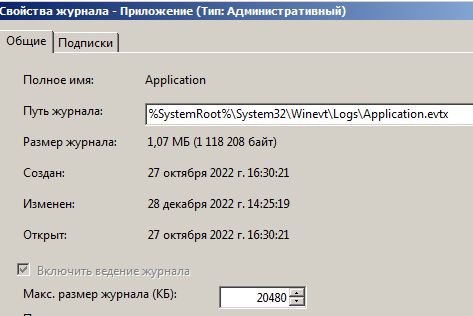
"Просмотр событий" (Event Viewer) содержит следующие поджурналы:

* "Системные" - содержит события, связанные с работой системных компонентов, таких как ядро ОС, устройства ввода/вывода и т.д.
* "Приложения" - содержит события, связанные с работой приложений.
* "Безопасность" - содержит события, связанные с безопасностью, такие как входы/выходы из системы, аудит безопасности и т.д.
* "Учетные данные" - содержит события, связанные с учетными записями пользователей, такие как создание/удаление учетных записей, изменение паролей и т.д.
* "Дополнительно" - содержит события, связанные с дополнительными службами и компонентами ОС.

Каждый поджурнал содержит информацию о конкретных событиях, включая время, тип спробы, уровень серьезности, источник и описание. Это может помочь в анализе проблем и устранении ошибок, а также в оценке безопасности системы. Администраторы сети могут использовать "Просмотр событий" для мониторинга состояния сети, идентификации и устранения проблем, а также для выполнения аудита безопасности.

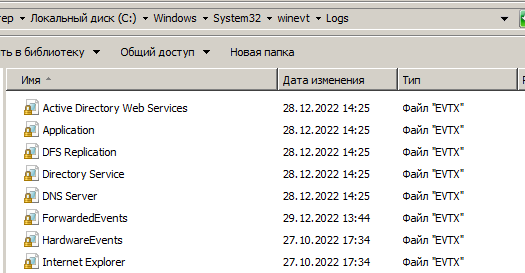
**Практика:**

Выбрав один из журналов в оснастке "Просмотр событий" и выбрав "Свойства", вы узнаете, где находятся файлы журналов и как ими управлять. "Общие" и "Подписки" – это две вкладки, расположенные в "Свойствах".



Вы можете просмотреть информацию о местоположении, размере, датах создания и обновления, времени открытия и закрытия, а также максимальном размере журнала на странице Общие сведения. Кроме того, вы можете решить, что произойдет, когда максимальный размер журнала будет достигнут, с точки зрения действий, которые будут предприняты.

Все журналы событий имеют формат evtx и хранятся в папке C:\Windows\System32\winev\tLogs.



На вкладке "Подписки" можно настроить компьютер на получение событий и их запись с другого компьютера. Администратор сети может использовать эту функцию для удаленного устранения неполадок, чтобы избежать необходимости просматривать журнал компьютера напрямую.

Форма представления данных журнала

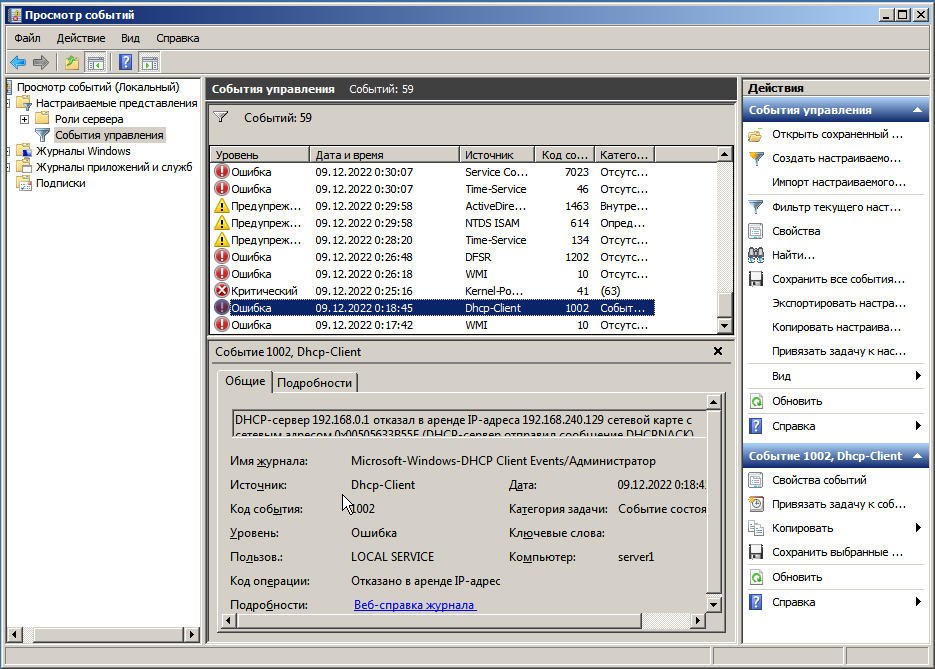
Данные в журнале "Просмотр событий" представлены в табличной форме, где каждая строка представляет собой отдельное событие. Каждая строка содержит следующую информацию:

* Дата и время события
* Уровень серьезности
* Источник события
* Код события
* Описание события

Эта информация позволяет администратору сети быстро идентифицировать и решить проблемы, а также оценить безопасность сети.

Типы событий, которые могут быть записаны в журнале "Просмотр событий" в Windows, включают:

* Системные события: это события, связанные с работой ядра и служб Windows, таких как запуск службы, перезагрузка системы и т.д.
* События безопасности: это события, связанные с безопасностью системы, такие как неудачные попытки входа, блокировка учетных записей и т.д.
* События приложений: это события, связанные с работой приложений, такие как ошибки в приложении, неожиданное завершение приложения и т.д.
* События служб: это события, связанные с работой служб Windows, таких как служба печати, служба удаленных рабочих столов и т.д.
* Информационные события: это события, которые предоставляют дополнительную информации.



Аудит доступа к файловым ресурсам

Политика аудита

Основные события для политики аудита в Windows Server включают:

* События входа/выхода: Аудит входов и выходов для отслеживания того, когда пользователи входят в систему и выходят из нее.
* События доступа к объектам: Аудит доступа к объектам, таким как файлы и папки, для отслеживания того, кто и когда получает доступ.
* События использования привилегий: Аудит использования привилегий, например, права на выключение системы, для отслеживания того, кто использует привилегированные команды.
* Системные события: Аудит событий, связанных с безопасностью системы, например, установка нового программного или аппаратного обеспечения.
* События отслеживания процессов: Аудит создания и завершения процессов для отслеживания выполнения программного обеспечения в системе.
* События изменения политики: Аудит изменений политик безопасности и назначений прав пользователей для отслеживания того, кто и какие изменения вносит.
* События управления учетными записями: События аудита, связанные с управлением учетными записями пользователей, такие как создание, удаление или изменение учетных записей пользователей.
* События доступа к службе каталогов: События аудита, связанные с доступом к объектам службы каталогов, таким как учетные записи пользователей и групп, для отслеживания того, кто получает доступ к каталогу и какие изменения вносятся.

Эти основные события являются хорошей отправной точкой для настройки политики аудита в Windows Server, и администраторы могут настраивать политику аудита в соответствии со своими конкретными требованиями, включая или отключая определенные события аудита.

Ниже приведен пример настройки политики аудита в Windows Server с помощью редактора групповой политики:

1. Откройте редактор групповой политики: Пуск > Выполнить > введите "gpedit.msc" и нажмите Enter.
2. Перейдите в Конфигурация компьютера > Параметры Windows > Параметры безопасности > Локальные политики > Политика аудита.
3. Щелкните правой кнопкой мыши на политике аудита, которую вы хотите настроить, и выберите "Свойства".
4. Установите флажок "Определить этот параметр политики" и выберите "Успех" или "Неудача", чтобы указать тип события, которое вы хотите аудировать.
5. Нажмите OK, чтобы сохранить изменения.
6. Повторите шаги с 3 по 5 для каждой политики аудита, которую вы хотите настроить.
7. Закройте редактор групповой политики.
8. Запустите команду "gpupdate /force" из командной строки, чтобы применить изменения.

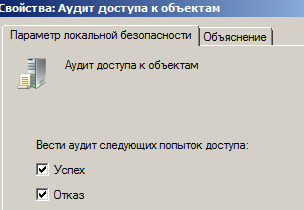
События аудита доступа к файлам

События аудита доступа к файлам относятся к аудиту доступа к файлам и папкам в Windows Server. Эти события регистрируются, когда пользователь пытается получить доступ к файлу или папке, и могут включать такие события, как создание, изменение, удаление и чтение файла.

Вот некоторые из событий аудита доступа к файлам, которые могут быть проверены в Windows Server:

1. События создания файла или папки: События аудита, которые регистрируются при создании нового файла или папки.
2. События модификации файлов или папок: События аудита, которые регистрируются при изменении файла или папки, например, при переименовании файла или изменении его содержимого.
3. События удаления файлов или папок: События аудита, регистрируемые при удалении файла или папки.
4. События чтения файлов или папок: События аудита, которые регистрируются при чтении файла или папки, например, когда пользователь открывает файл для просмотра.
5. События записи файла или папки: События аудита, которые регистрируются при записи в файл или папку, например, когда пользователь сохраняет изменения в файле.
6. События выполнения файла или папки: События аудита, которые регистрируются при выполнении файла или папки, например, когда пользователь запускает программу.

Благодаря аудиту событий доступа к файлам администраторы могут контролировать доступ к файлам и папкам в своей среде и гарантировать, что файлы используются безопасным образом. Конкретные события, которые проверяются для доступа к файлам, могут быть настроены в соответствии с потребностями организации.



**Вывод**:

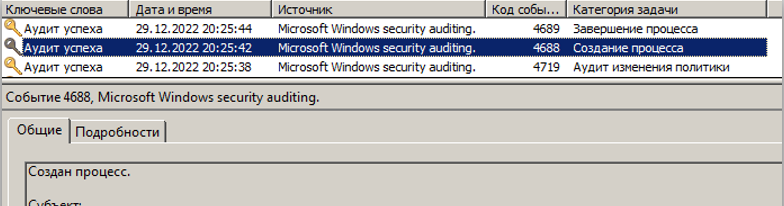
События аудита доступа к файлам – это регистрация попыток доступа к файлам и папкам в Windows Server. Эти события могут включать создание, изменение, удаление, чтение, запись и выполнение файлов. Аудит событий доступа к файлам позволяет администраторам контролировать и обеспечивать безопасное использование файлов в своей среде, а конкретные события, которые подвергаются аудиту, могут быть настроены в соответствии с потребностями организации.

Аудит отслеживания процессов

Аудит отслеживания процессов – это регистрация информации о процессах, запущенных в системе Windows Server. Этот тип аудита может быть полезен для целей мониторинга и устранения неполадок, а также для целей безопасности, поскольку он может помочь выявить вредоносные или несанкционированные процессы, запущенные в системе.

Вот некоторые события аудита отслеживания процессов, которые могут быть проверены в Windows Server:

1. События создания процесса: События аудита, которые регистрируются при создании нового процесса, например, когда пользователь запускает новую программу.
2. События завершения процесса: События аудита, которые регистрируются при завершении процесса, например, когда пользователь закрывает программу.
3. События загрузки изображения процесса: События аудита, которые регистрируются при загрузке образа процесса, например, при запуске программы.
4. События доступа к процессу: События аудита, которые регистрируются при обращении к процессу, например, когда пользователь открывает программу.



Благодаря аудиту событий отслеживания процессов администраторы могут отслеживать активность процессов, запущенных в системе, и выявлять любые подозрительные или несанкционированные процессы. Конкретные события, которые проверяются для отслеживания процессов, могут быть настроены в соответствии с потребностями организации.

**Вывод**:

Аудит отслеживания процессов – это функция в Windows Server, которая регистрирует информацию о процессах, запущенных в системе. Эта информация может включать создание, завершение, загрузку изображений и события доступа. Благодаря аудиту событий отслеживания процессов администраторы могут отслеживать активность процессов и выявлять любые подозрительные или несанкционированные действия. Конкретные события, которые подвергаются аудиту, могут быть настроены в соответствии с потребностями организации.

Анализ и настройка безопасности локального компьютера

Шаблоны безопасности

Шаблоны безопасности – это в предварительно сконфигурированные наборы параметров безопасности, которые можно применять к нескольким компьютерам или серверам. Эти шаблоны предоставляют администраторам удобный способ стандартизации и управления параметрами безопасности нескольких систем.

В Windows Server шаблоны безопасности хранятся в виде файлов .inf и могут быть применены с помощью оснастки Security Configuration and Analysis, которая является частью консоли управления Microsoft Management Console (MMC). Шаблоны безопасности могут быть настроены в соответствии с конкретными потребностями организации и могут использоваться для применения широкого спектра параметров безопасности, включая назначение прав пользователей, параметры безопасности, политики аудита и многое другое.

Использование шаблонов безопасности может помочь администраторам обеспечить согласованную и безопасную конфигурацию систем, а также упростить управление параметрами безопасности. Применяя шаблон безопасности к нескольким системам, администраторы могут сократить время и усилия, необходимые для управления настройками безопасности, и снизить риск неправильной конфигурации безопасности.

Шаблоны безопасности могут влиять на широкий спектр политик и параметров безопасности, включая:

1. Назначение прав пользователей: Шаблоны безопасности можно использовать для определения прав пользователей, назначаемых различным группам и пользователям. Сюда входят такие права, как возможность локального входа в систему, выключения системы и т.д.
2. Параметры безопасности: Шаблоны безопасности можно использовать для настройки параметров безопасности, таких как поведение брандмауэра Windows, UAC (User Account Control) и других параметров, связанных с безопасностью.
3. Политики аудита: Шаблоны безопасности можно использовать для определения политик аудита, применяемых к системе, включая то, какие события проверяются и как они записываются.
4. Политики учетных записей: Шаблоны безопасности можно использовать для настройки политик учетных записей, таких как политики паролей и блокировки, которые помогают обеспечить пользователям надежные и безопасные пароли.
5. Разрешения реестра: Шаблоны безопасности можно использовать для настройки разрешений для различных ключей реестра, которые можно использовать для ограничения доступа к конфиденциальным данным.
6. Разрешения файловой системы: Шаблоны безопасности можно использовать для настройки разрешений для различных файлов и папок, которые можно использовать для ограничения доступа к конфиденциальным данным.

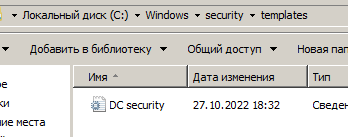
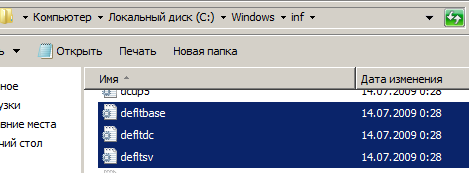
Это лишь несколько примеров политик и параметров, которые могут быть затронуты шаблонами безопасности. Какие именно политики будут затронуты, зависит от конкретного используемого шаблона безопасности и потребностей организации.

Выполнение:

Шаблоны безопасности имеют расширение inf. Стандартные шаблоны безопасности хранятся в каталогах

C:\Windows\security\templates

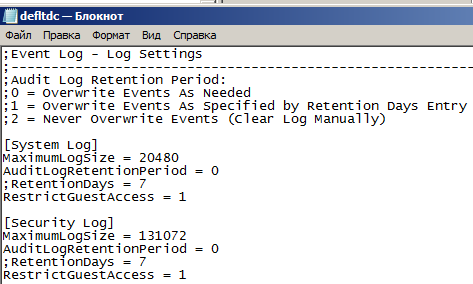
C:\Windows\inf

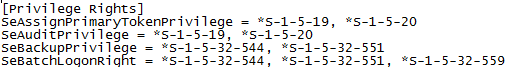
Когда сервер был назначен контроллером домена, для усиления его защиты был создан шаблон "DC security". Этот шаблон был разработан для ограничения входа в систему с помощью учетных записей, не входящих в группу "Администраторы".

C:\Windows\inf хранит три базовых шаблона для рядового сервера - default base, контроллера домена – default dc, и default sv – резервная копия шаблона default base.

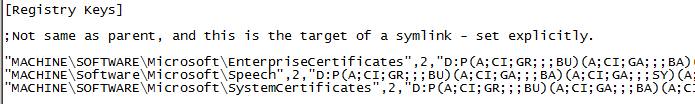
Шаблон безопасности состоит из секций с заданными параметрами для определенных переменных.



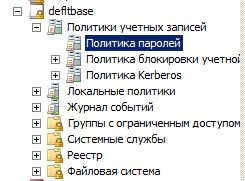
Привилегии выражаются в виде выражений и начинаются с привилегии и соответствующего ей SID. В случаях, когда несколько пользователей имеют привилегию, их SID перечисляются через запятую.



Разрешения доступа к ключам реестра представлены путём и списком разрешений для данного ключа.



С помощью оснастки «Шаблоны безопасности» сопоставим шаблоны для контроллера домена и для рядового сервера. Для этого добавим данную оснастку в консоль Microsoft Management Console.



|  |  |  |
| --- | --- | --- |
| **Свойство** | **default base** | **default dc** |
| **Политика паролей** | | |
| Вести журнал паролей | 0 сохранённых паролей | Не определено |
| Максимальный срок действия пароля | 42 дня | Не определено |
| Минимальная длина пароля | 0 знаков | Не определено |
| Минимальный срок действия пароля | 0 дней | Не определено |
| Пароль должен отвечать требования сложности | Включен | Не определено |
| Хранить пароли, используя обратимое шифрование | Отключен | Не определено |
| **Политика блокировки учетной записи** | | |
| Пороговое значение блокировки | Не определено | 0 ошибок входа в систему |
| **Назначение прав пользователей** | | |
| Завершение работы системы | Все | Оператор архива, Администраторы |
| Загрузка и выгрузка драйверов | Администраторы, Операторы печати | Администраторы |
| Изменение системного времени | Local service, Администраторы | Операторы сервера, Local service, Администраторы |
| Локальный вход в систему | Все | Администраторы, Операторы архива |
| Разрешить вход в системе через службу удаленных рабочих столов | Все | Пользователи удаленного рабочего стола, Администраторы |

**Вывод**:

Большинство шаблонов безопасности имеют схожие параметры безопасности. Однако шаблон default dc по умолчанию накладывает более строгие ограничения безопасности в отношении разрешений пользователей.

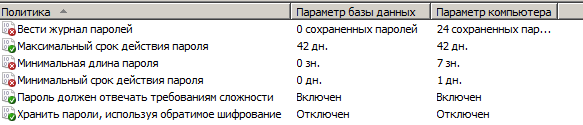
Соответствие текущей конфигурации компьютера шаблону

С помощью оснастки «Анализ и настройка безопасности» проверим соответствие текущей конфигурации рядового сервера Server2 шаблону безопасности deflbase. Для этого необходимо:

* Добавить оснастку в консоль
* Скопировать шаблон безопасности в каталог пользователя, например в C:\Users\Администратор\Documents\Security\Templates
* Создать базу данных безопасности на основе шаблона
* Выбрать в контекстном меню оснастки «Анализ компьютера».

Найдем параметры конфигурации, которые отличаются от шаблона безопасности.

Политики учетных записей - Политика паролей



Настройка "Ведение журнала паролей" определяет количество уникальных паролей, которые должны быть установлены для аккаунта пользователя до повторного использования старого.

Резюме:

В текущей конфигурации, пароль может быть использован повторно только после 24 уникальных паролей. Минимальная длина пароля установлена в 7 символов, а минимальный срок его действия больше, чем в стандартном шаблоне. Текущие настройки для политики паролей более строгие, чем в шаблоне deflbase.

Редактор безопасности secedit.exe

secedit.exe - это исполняемый файл редактора безопасности в операционной системе Windows. Он используется для управления параметрами политики безопасности, включая создание, изменение и применение шаблонов безопасности к локальным или удаленным компьютерам. Назначение secedit.exe - настраивать и применять параметры безопасности в системе, помогая обеспечить конфиденциальность, целостность и доступность данных и ресурсов. secedit.exe можно использовать из командной строки или запускать как пакетный скрипт, и он обычно используется системными администраторами для поддержания безопасности своих сетей и систем.

Основные задачи редактора конфигурации безопасности (secedit.exe) включают:

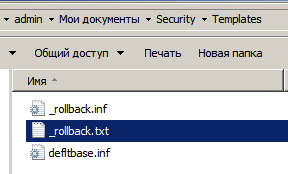
* Создание шаблонов безопасности для определения параметров безопасности для компьютера.
* Применение шаблонов безопасности к компьютеру для настройки параметров безопасности.
* Экспорт шаблонов безопасности с компьютера для резервного копирования или развертывания на других компьютерах.
* Импорт шаблонов безопасности на компьютер для настройки параметров безопасности.
* Анализ конфигурации безопасности компьютера для выявления потенциальных проблем безопасности.
* Сравнение параметров безопасности двух компьютеров для выявления различий.
* Изменение существующего шаблона безопасности для изменения параметров безопасности компьютера.

Создадим шаблон, в котором будет храниться копия текущей конфигурации системы. Он будет использоваться как резервная копия.

Перейдем в каталог C: \Users\admin\Documents\Security\Templates и выполним команду:

secedit.exe /generaterollback /cfg defltbase.inf /rbk \_rollback.inf /log \_rollback.log

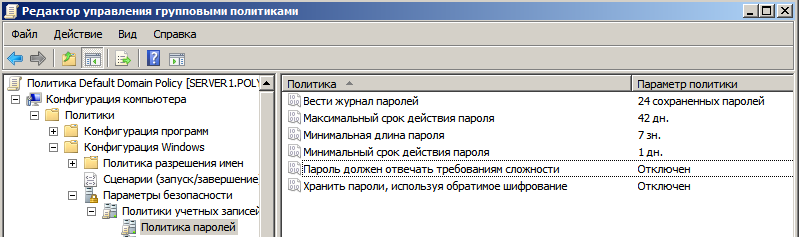
После создаст сценарий отката на основе шаблона безопасности по умолчанию (defltbase.inf) и сохранит его под именем \_rollback.inf. Он также создаст файл журнала процесса с именем \_rollback.log.



Изменение параметров политики учетных записей в базе данных

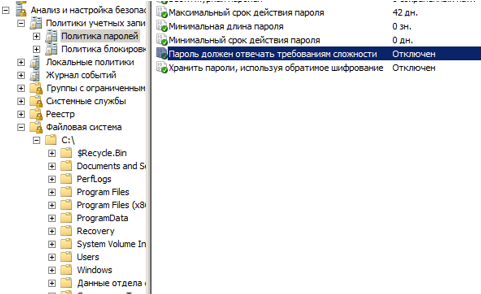
Отключим параметр «Пароль должен соответствовать требованиям сложности» в разделе «Политика паролей».

Включим параметр «Разрешить завершение работы системы без выполнения входа» в разделе «Параметры безопасности».



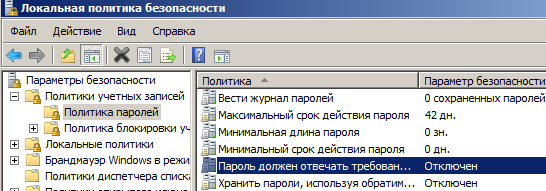
Применим отредактированную базу данных к настройке компьютера. Для этого нажмем ПКМ по «Анализ и настройка безопасности», сначала выберем «Настроить компьютер», после выполнения данного действия, выберем «Анализ компьютера».

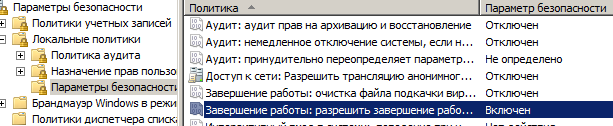
Все изменения были успешно проведены, и применились к параметрам компьютера.



С помощью апплета панели управления «Локальная политика безопасности» убедиться в применении настроек.

Используем оснастку «Локальная политика безопасности», и проверим вступили ли изменения в силу.

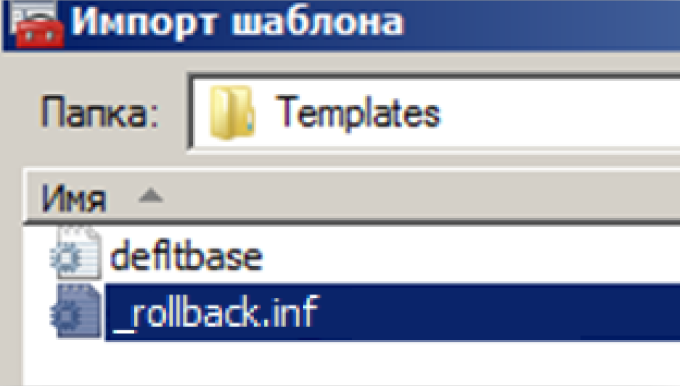




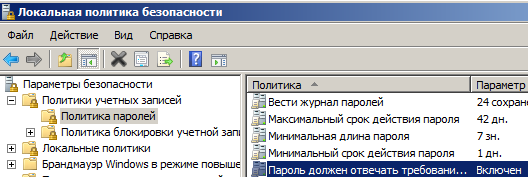
Настроенные политики успешно применились к системе. Разрешения доступа к каталогу проверим с помощью файлового менеджера.

Отменить внесенные изменения

Для отмены внесенных изменений можно откатится с помощью бэкапов созданных ранее:



Проверим, что все вернулось обратно:



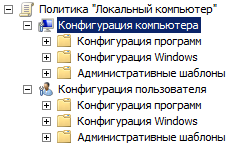
**Вывод**:

Инструмент "Конфигурация и анализ безопасности" анализирует текущие настройки безопасности компьютера на основе заданного шаблона. Шаблоны безопасности – это текстовые файлы, описывающие параметры безопасности системы. С помощью шаблонов безопасности можно быстро настроить все компьютеры в домене. Вам не нужно будет вручную настраивать каждый параметр на каждом компьютере, достаточно загрузить нужный шаблон безопасности. Утилиту secedit можно использовать для создания резервной копии текущей конфигурации системы.

Базовые свойства, структура и применение групповых политик в домене.

Оснастка «Редактора локальной групповой политики»

Оснастка "Редактор локальных групповых политик" – это консоль управления Microsoft, которая предоставляет графический интерфейс для управления локальными групповыми политиками в операционных системах Windows. Она позволяет администраторам настраивать параметры безопасности, политики развертывания программного обеспечения и профили пользователей, а также другие параметры. Оснастку Local Group Policy Editor можно использовать для применения политик к определенным пользователям или компьютерам, что позволяет усилить контроль и настроить среду.



В оснастке Local Group Policy Editor разделы Computer Configuration и User Configuration содержат различные наборы параметров групповой политики, которые управляют поведением и конфигурацией компьютера или пользователя.

Конфигурация компьютера: Этот раздел содержит параметры политики, которые применяются к компьютеру в целом, независимо от того, какой пользователь в данный момент вошел в систему. Эти политики включают параметры установки программного обеспечения, параметры безопасности и сетевые параметры. Например, вы можете использовать раздел Конфигурация компьютера, чтобы указать, какие программы установлены на компьютере, или контролировать доступ к реестру Windows.

Конфигурация пользователя: Этот раздел содержит параметры политики, которые применяются только к текущему вошедшему в систему пользователю. Эти политики включают настройки среды рабочего стола, такие как заставки и обои, а также контроль над меню "Пуск" и оболочкой Windows. Например, вы можете использовать раздел Конфигурация пользователя, чтобы указать, какие программы доступны пользователям, или управлять внешним видом рабочего стола.

В разделах Конфигурация компьютера и Конфигурация пользователя параметры политики организованы в Административные шаблоны, которые представляют собой группы параметров для определенных целей. Эти шаблоны включают настройки для таких компонентов Windows, как Internet Explorer, брандмауэр Windows и удаленный рабочий стол. Вы также можете создавать собственные шаблоны для параметров, которые не входят во встроенные шаблоны.

Разделы «Конфигурация компьютера» и «Конфигурация пользователя» делятся на три контейнера каждый: «Конфигурация программ», «Конфигурация Windows» и «Административные шаблоны».

*«Конфигурация программ»* предоставляет автоматизированный подход к установке программ на компьютеры домена. Существует два механизма:

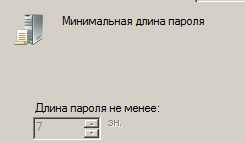
* Администратор сам инициирует автоматическую установку программы;
* Администратор предоставляет данные программы, а пользователь сам устанавливает нужные ему приложения.

*«Конфигурация Windows»*. В данном контейнере содержимое отличается у конфигурации компьютера и пользователя. Более широкие возможности настройки есть для «параметров безопасности» в «конфигурации компьютера», а в «конфигурации пользователя» существует «службы удаленной установки».

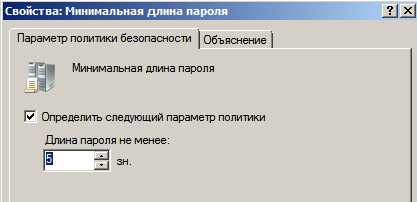
*«Административные шаблоны»*. Здесь сосредоточены параметры, которые влияют на интерфейс системы.

Опробовать изменение параметров "Политика учетных записей" на уровне локального компьютера.

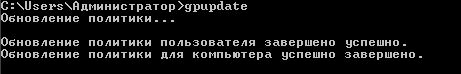
Давайте попробуем изменить минимальную длину пароля на компьютере, который является частью домена. Для этого перейдите в раздел "Конфигурация компьютера" → "Конфигурация Windows" → "Параметры безопасности" → "Политика паролей". Найдите параметр "Минимальная длина пароля". К сожалению, это изменение невозможно, так как существует GPO домена, который отменяет параметры политики учетных записей локального GPO.



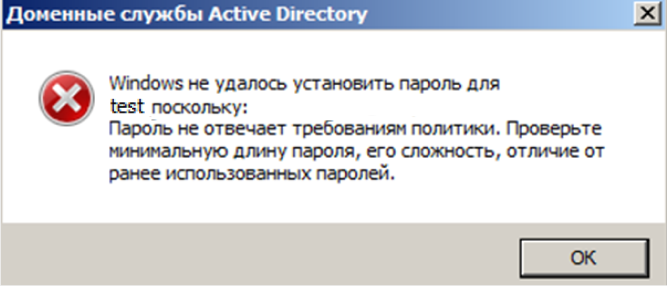
Попробуем изменить минимальную длину пароля на контроллере домена. Перейдем к пункту «Минимальная длина пароля», и установим длину пароля, равную 5 знаков.



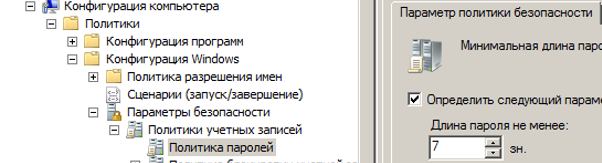
Обновим политику с помощью gpupdate.



Если попробовать создать нового пользователя с паролем меньше 7 символов, то появится ошибка, что пароль не соответствует требованиям.   
Это связано с тем, что над локальными настройками преобладают групповые:



Добавим в консоль оснастку «Политика Default Domain Policy». Перейдем к настройке длины пароля. Минимальное значение длины установлено 7 знаков.



**Вывод**:

Изменение локальных настроек компьютера доступно для тех параметров, для которых нет переопределения на уровне групповых политик домена. На контроллере домена групповые политики домена также преобладают над локальными политиками компьютера.

Административные шаблоны

Административные шаблоны, относящиеся к конфигурации компьютера, включают в себя элементы, определяющие общее функционирование компьютера. Шаблоны, связанные с конфигурацией пользователя, напротив, определяют настройки для окружения конкретного пользователя.

Внутренности контейнеров различаются

*Конфигурация компьютера:*

* Компоненты Windows
* Панель управления
* Принтеры
* Сеть
* Система

Ключ реестра для данных политик: HKEY\_CURRENT\_USER /Software /Microsoft /Windows /CurrentVersion /Policies

*Конфигурация пользователя:*

* Компоненты Windows
* Меню «Пуск» и панель задач
* Общие папки
* Панель управления
* Рабочий стол
* Сеть
* Система

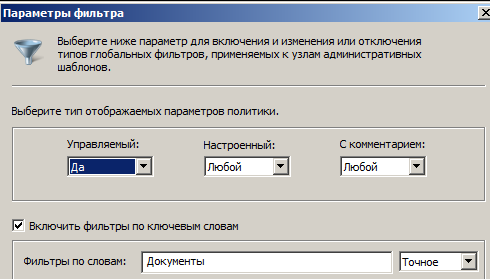
Ключ реестра для данных политик: HKEY\_LOCAL\_MACHINE \SOFTWARE \Policies

*Троичная логика политик*

Состояние политик находится со статусом «Не задан» не вносят изменения в реестр. Если же изменять состояние на «Включен» и «Отключен», то эти изменения заносятся в реестр.

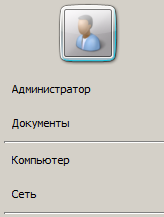
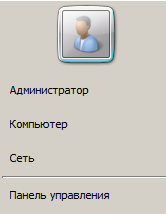
*Применение фильтра*

В разделе «Административные шаблоны» есть раздел «Все параметры». Для лучшей навигации в нём можно воспользоваться фильтром. Применим фильтр с ключевым словом «Документы», и получим все доступные параметры, содержащие это слово.



В результате фильтрации получим список элемента. Изменим значение «Не задана» на «Включить» для параметра «Удалить значок «Документы» из меню «Пуск»».



**Вывод**:

Одной из функций административных шаблонов является изменение интерфейса пользователя. Изменение возможно произвести для компьютера или для конкретного пользователя. Использование фильтра упрощает поиск нужных параметров.

Сравнить возможности защиты сетевых настроек с помощью "Административных шаблонов", заданных для компьютера и для пользователя

Возможность защиты сетевых параметров с помощью набора "Административные шаблоны" одинакова как для компьютера, так и для пользователя. Разница заключается в масштабе настройки. Набор "Административные шаблоны" для компьютера влияет на общую работу компьютера, в то время как набор "Административные шаблоны" для пользователя влияет только на конфигурацию среды для конкретного пользователя. В обоих случаях шаблоны позволяют администраторам контролировать и обеспечивать безопасность и другие параметры, что помогает защитить сеть и поддерживать согласованность сетевых настроек.

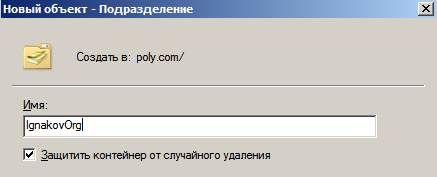
Сетевые настройки для пользователя:

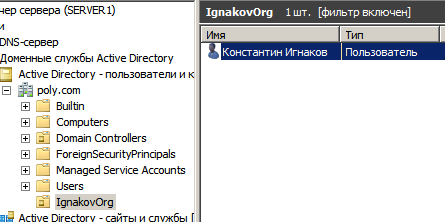
* Запретить дополнительные настройки TCP/IP
* Запрет подключения и разрыва подключения удаленного доступа
* Запрет доступа к свойствам подключений локальной сети
* Запрет доступа к мастеру новых подключений
* Возможность переименовать подключения локальной сети
* Возможность включения/разрыва подключения локальной сети

Сетевые настройки для компьютера, предоставляют возможность конфигурировать параметры Брандмауэра Windows, разрешать или запрещать различные исключения портов или программ. Сетевые настройки для пользователя – в основном все параметры сводятся к запрету/разрешению доступа пользователя к различным частям конфигурации сети.

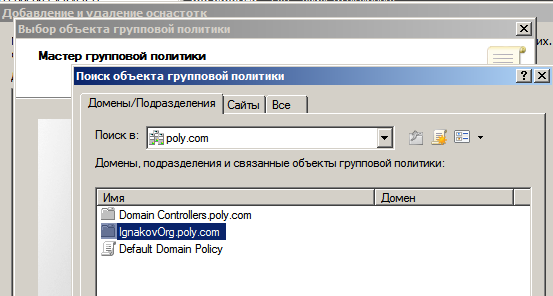
Управление групповой политикой организационного подразделения

В оснастке «Диспетчер сервера» в «Active Directory - пользователи и компьютеры» создадим подразделение и создадим учетную запись пользователя для этого подразделения:



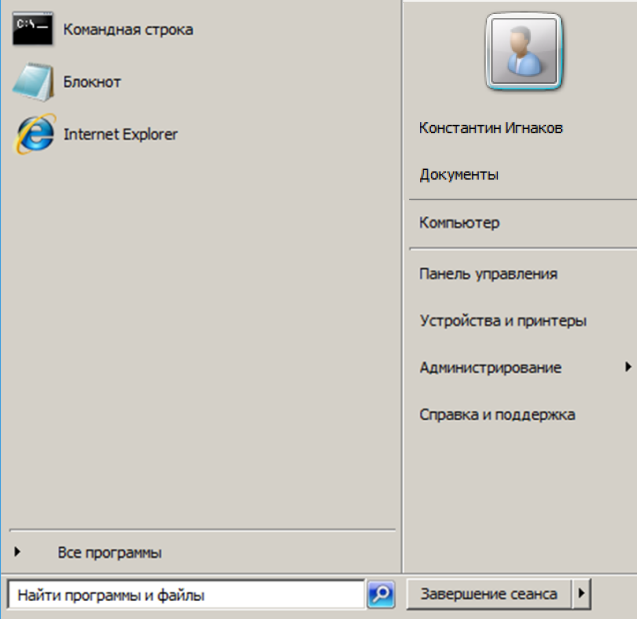
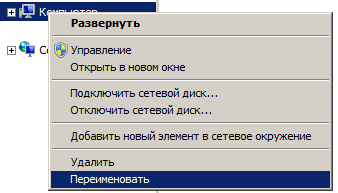


В консоль добавим оснастку «Редактор управления групповыми политиками», в ней выберем созданное подразделение и создадим объект групповой политики.



Настроим окружения пользователя подразделения OU с ограниченными возможностями интерфейса.

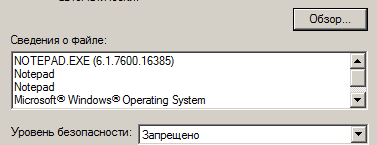
|  |  |  |
| --- | --- | --- |
| **Путь к параметру** | **Название параметра** | **Значение** |
| Меню «Пуск» и панель задач | Закрепить панель задач | Отключена |
| Меню «Пуск» и панель задач | Удалить команду «Выполнить» из меню «Пуск» | Включена |
| Меню «Пуск» и панель задач | Удалить значок сеть «Сеть» из меню «Пуск» | Включена |
| Рабочий стол | Удалить пункт «Свойства» из контекстного меню значка «Компьютер» | Включена |
| Рабочий стол →Active Desktop | Запретить удаление элементов | Включена |



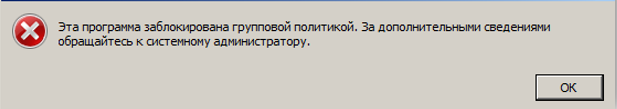
Опробовать применение политики ограниченного использования программ.

С помощью политики ограниченного использования программ можно указать либо программы, которые можно запускать либо те, которые нельзя. Для этого нужно перейти в Конфигурация пользователя → Конфигурация Windows→ Параметры безопасности → Политики ограниченного использования программ. В «Дополнительные правила» создадим «правило для хэша», тогда запуск программы будет недоступен независимо от её расположения.

Установим запрет на запуск программы блокнот.



Выполним вход от имени учётной записи «Игнаков Константин» и попытаемся открыть текстовый файл. Возникла ошибка, следовательно, политика настроена правильно.



С помощью оснастки редактора управления групповыми политиками найти свойства безопасности объектов политик GPO домена и организационного подразделения.

Чтобы оценить разрешения безопасности объекта групповой политики, выполните следующие действия:

1. Откройте редактор управления политиками
2. Выберите нужный объект
3. Зайдите в его свойства
4. Перейдите в раздел "Безопасность".

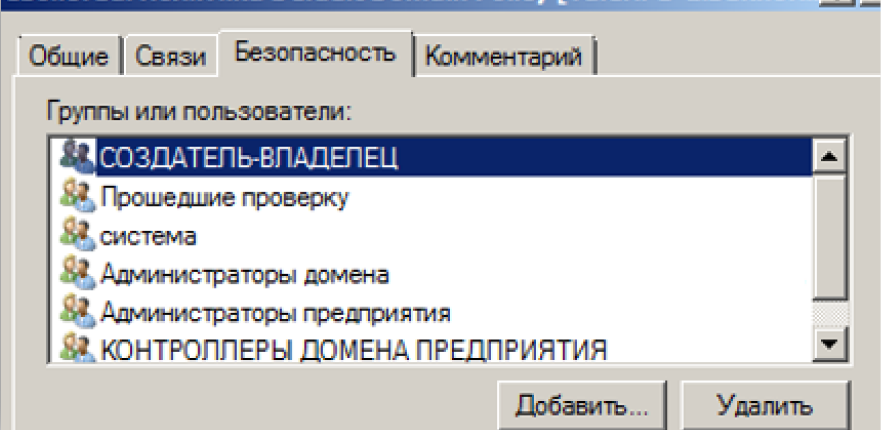


Таблица разрешений безопасности:

|  |  |
| --- | --- |
| **Администраторы домена** | Список содержимого, прочитать/записать все свойства, чтение разрешений, смена владельца и разрешений, создание объектов |
| **Администраторы предприятия** | Список содержимого, прочитать/записать все свойства, чтение разрешений, смена владельца и разрешений, создание объектов |
| **Администраторы домена** | Все разрешения, кроме применения групповой политики (на все дочерние объекты) |
| **Администраторы предприятия** | Все разрешения, кроме применения групповой политики (на все дочерние объекты) |
| **Создатель-владелец** | Все разрешения, кроме применения групповой политики (на дочерние объекты) |
| **система** | Все разрешения, кроме применения групповой политики (на этот объект и все дочерние объекты) |
| **Контроллеры домена предприятия** | Список содержимого, прочитать свойства, чтение разрешений (на этот объект и все дочерние объекты) |

Созданное подразделение:

|  |  |
| --- | --- |
| **Администраторы домена** | Все разрешения, кроме применения групповой политики (на этот объект и все дочерние объекты) |
| **Администраторы предприятия** | Все разрешения, кроме применения групповой политики (на этот объект и все дочерние объекты) |
| **Создатель-владелец** | Все разрешения, кроме применения групповой политики (на дочерние объекты) |
| **система** | Все разрешения, кроме применения групповой политики (на этот объект и все дочерние объекты) |
| **Контроллеры домена предприятия** | Список содержимого, прочитать свойства, чтение разрешений (на этот объект и все дочерние объекты) |

**Вывод**:

Различие между ними заключается в том, что параметры безопасности объекта политики домена разделяют авторизацию для групп "Администраторы домена" и "Администраторы предприятия" на разрешения для объекта домена и разрешения для его подобъектов, в то время как параметры безопасности объекта политики группы организационной единицы не имеют такого различия.

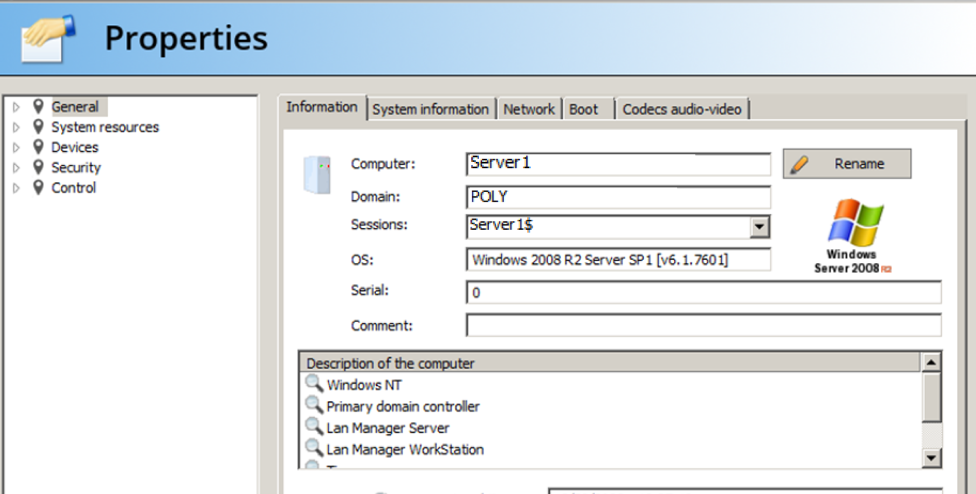
После всех действий, показанных выше система была восстановлена в исходное состояние.

Использовать систему дистанционного администрирования Ideal Administration

Получение информации о контроллере домена

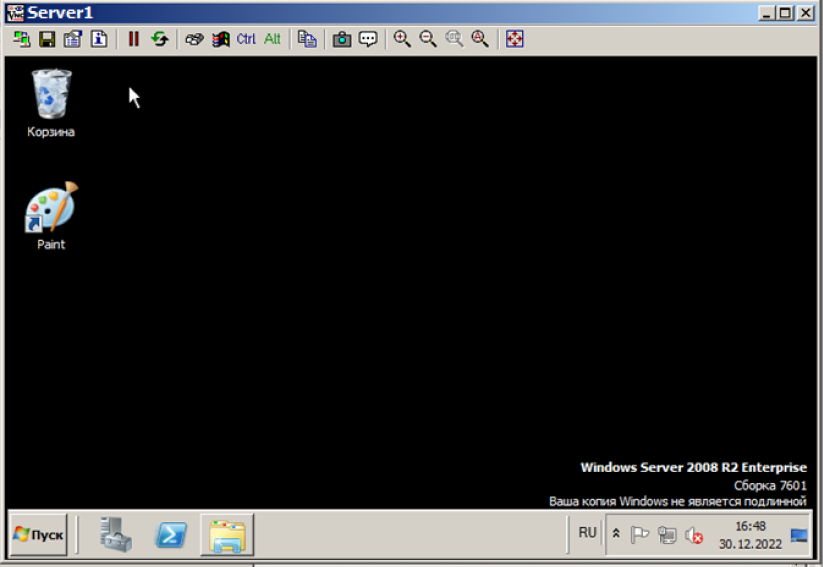
IDEAL Administration – это программное средство, которое помогает администраторам управлять ИТ-инфраструктурой своей организации. Он предоставляет централизованный интерфейс для управления серверами, пользователями, компьютерами и другими ресурсами в сетевой среде. Инструмент позволяет администраторам выполнять такие задачи, как создание и управление учетными записями пользователей, установка и настройка серверов, мониторинг сетевой активности, резервное копирование и восстановление данных. Он также предлагает функции отчетности и аудита, помогающие администраторам отслеживать изменения и обеспечивать безопасность сети.

В интерфейсе IA перейдем в Microsoft Windows Network, выберем компьютер – контроллер домена и нажмем Properties. Откроется окно, в котором мы можем просмотреть различные свойства выбранного компьютера, такую как имя компьютера, к какому домену он принадлежит, активные сессии, информацию о комплектующих, информацию о сети компьютера и другие характеристики.



Реализовать сеанс терминального доступа

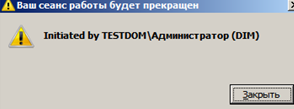
Для терминального доступа в списке компьютеров выберем тот, к которому хотим подключиться, в меню программы перейдем в «Remote Desktop», и выберем пункт «TightVNC Remote Desktop». Откроется подобное окно:



Попробуем удалить папку на рабочем столе. Удаление прошло успешно.

Когда мы подключаемся к рабочему столу другого компьютера, у него запускается процесс tnvserver.exe, благодаря которому мы и можем управлять этим компьютером удаленно. Найдем процесс tvnserver в диспетчере задач и попробуем его завершить через AI с другого компьютера. После нажатия завершения процесса, получаем ошибку «Failed to receive data from socket» и удаленный рабочий стой закрывается.

Попробуем выполнить удаленную перезагрузку. Для этого в интерфейсе AI выберем контроллер домена и нажмем shutdown / Restart. Откроется окно, в котором мы можем установить обратный отсчет до начала перезагрузки, установим 10 секунд и нажмем Reboot. На удаленном компьютере появляется сообщение о том, что сеанс работы пользователя будет прекращен.



VNC расшифровывается как Virtual Network Computing. Это технология, позволяющая удаленно управлять компьютером через Интернет или локальную сеть. С помощью VNC можно получить удаленный доступ к рабочему столу компьютера и управлять им, что позволяет видеть, что происходит на компьютере, и выполнять задачи так, как будто вы сидите перед ним. VNC часто используется для удаленного доступа и поддержки других компьютеров или для обеспечения удаленного доступа к компьютеру с мобильного устройства или планшета.

**Вывод**:

В ходе выполнения данного пункта лабораторной работы я ознакомился с программой IDEAL Administration, её функционалом, а также возможностью администрирования через удаленный рабочий. Эта программа очень полезна для арсенала системного администратора.

Вывод

В ходе лабораторной работы основное внимание уделялось изучению и использованию системных инструментов, предлагаемых Windows Server для сбора информации о системе и управления параметрами безопасности. Это включало просмотр событий из Event Viewer, анализ и управление доступом к файловым ресурсам с помощью аудита, использование консоли Security Analysis and Configuration для оценки безопасности компьютера, создание шаблонов отката и просмотр шаблонов безопасности. Кроме того, особое внимание уделялось пониманию структуры и свойств групповых политик и практическим экспериментам с этими GPO с помощью различных оснасток. В лабораторной работе также был представлен IDEAL Administration в качестве инструмента для администрирования и включено администрирование удаленного рабочего стола.