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:

_____ Сухоруков В.А.

(подпись) (фамилия, и.,о.)

19-ВМ

(шифр группы)

Работа защищена «___»_____

С оценкой _____

Нижний Новгород 2022

Оглавление

Цель работы

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

Ход работы

1. Наблюдение за событиями в системе.

1.1. Оснастка «Просмотр событий»

Теория:

Программа «Просмотр событий» используется для просмотра событий, записанных в журнале событий. Обычно на компьютере ведутся журналы приложений, безопасности, системы. На компьютере также могут содержаться другие журналы, в зависимости от роли компьютера и установленных приложений.

На компьютере-сервере доступны такие разделы журнала как:

- ❖ Настраиваемые события- используются для перенаправления отдельных записей журнала событий. Присутствует возможность настроить фильтр. Данный раздел содержит такие фильтры как:
  - *Роли сервера* – содержит перенаправленные записи журнала, связанные со службами, выполняемыми на данном сервере. На контроллере домена в данном разделе хранятся записи о DNS- сервере, Доменных службах Active Directory.
  - *События управления* – содержит ошибки и предупреждения служб управления.
- ❖ Журнал Windows – содержит 3 поджурнала:
  - *Приложения (Application log) — содержит данные, относящиеся к работе приложений и программ.*
  - *Безопасность (Security log) — содержит записи об успешных и безуспешных попытках доступа в систему, о событиях, относящихся к использованию ресурсов.*
  - *Система (System log) — содержит записи о событиях, внесенные компонентами системы. Например, в системный журнал записываются такие события, как сбой в процессе загрузки драйвера или другого системного компонента при запуске системы.*
- ❖ Журнал приложений и служб - содержит перенаправленные записи журнала, относящихся к определенным службам и приложениям.

Выполнение:

Чтобы определить расположение файлов журналов и возможности управления ими нужно в оснастке «Просмотр событий» выбрать один из журналов, и перейти к его свойствам «Свойства». Свойства содержат 2 вкладки: «Общие» и «Подписки».

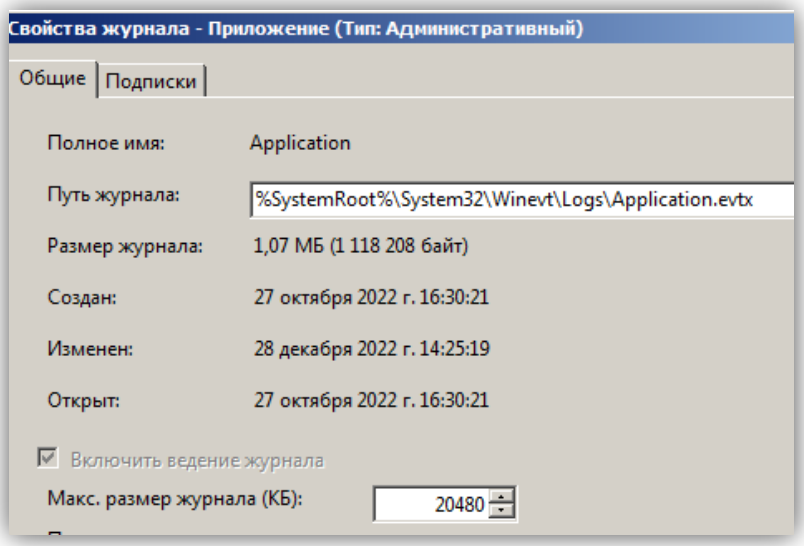


Рис 1.

На вкладке «Общие» можно просмотреть расположение файлов журнала, размер, даты создания, изменения, открытия, максимальный размер журнала. Так же возможно выбрать действия, которые будут выполняться по достижении максимального размера журнала.

Все журналы событий хранятся в каталоге C:\Windows\System32\winevt\Logs, и имеют формат evtx.

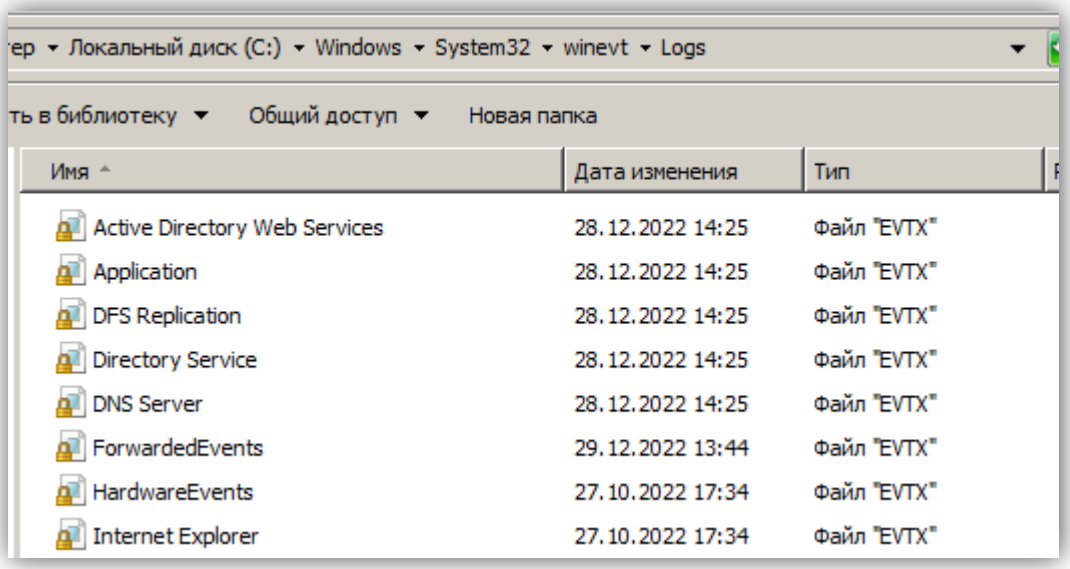


Рис 2.

На вкладке «Подписки» можно выбрать настроить компьютер на получение событий и их запись с другого компьютера. Данная функция полезна для удаленного поиска ошибок, чтобы администратору сети не приходилось просматривать журнал непосредственно на компьютере.

1.2. Форма представления данных журнала

Существует 5 типов событий:

- ❖ «Сведения» - показывает изменения в приложениях и компонентах. Это может быть выполнение операции, создание ресурса, запуск службы.
- ❖ «Ошибка» - показывает проблемы, которые могут влиять на функции.

- «Предупреждения» - показывает событие, которые указывают на возможные неполадки в будущем.
- «Аудит успеха» - показывает, что операции были выполнены.
- «Аудит отказа» - показывает, что операции были не выполнены.

Каждая запись журналов содержит следующую информацию о событии:

- Источник;
- Код события;
- Уровень события;
- Пользователь;
- Код операции;
- Дата и время наступления события;
- Категория задачи;
- Ключевые слова;
- Компьютер;

Рассмотрим событие аудита успеха из раздела «Безопасность» на компьютере-члене домена (Рис 3). Данное событие было создано при входе в систему. Субъект, создавший событие - доменная учетная запись «Sukhorukov\Тимур_Игоревич».

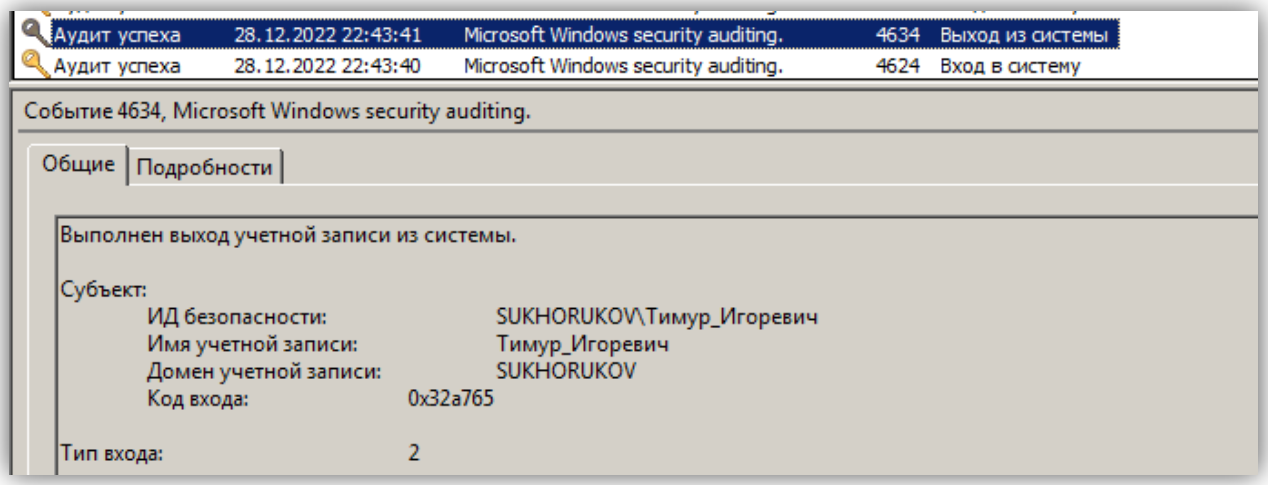


Рис 3.

На контроллере домена, на 1 секунду раньше, в журнал «Безопасность» было записано события запроса билета Ticket Granted Ticket.

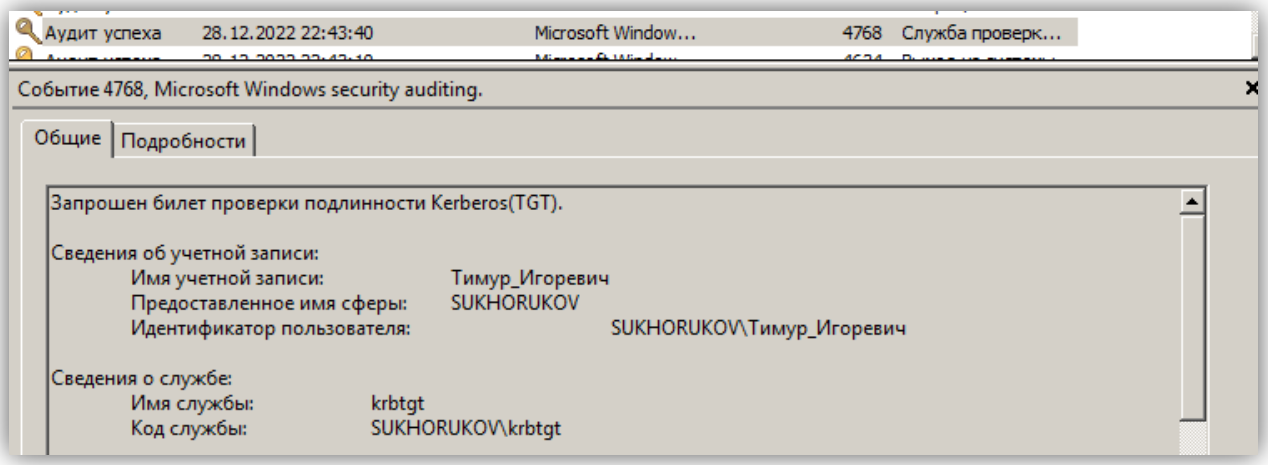


Рис 4.

Рассмотрим событие ошибки из раздела «Система» (Рис 5). Запись в журнале была сформирована службой групповых политик из-за того, что контроллер домена в данный момент был отключен. Для предотвращения таких ошибок, контроллер домена всегда должен быть включен при работе на других компьютерах домена.

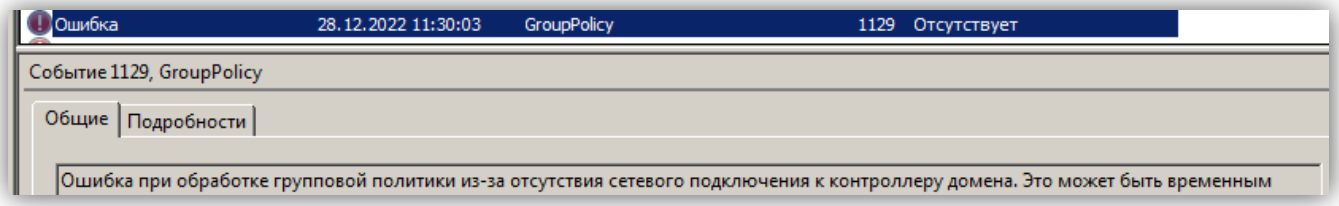


Рис 5.

2. Аудит доступа к файловым ресурсам

2.1. Политика аудита

С помощью оснастки «Локальная политика безопасности» можно настроить политику аудита. Есть возможность вести аудит успеха и отказа тех или иных событий. К «базовой» политике аудита относятся следующие события:

- *Вход в систему* - попытки пользователя войти в систему с компьютера или выйти из неё
- *Доступ к объектам* - события доступа пользователя к объекту: например к файлу, папке, разделу реестра, принтеру
- *Доступ к службе каталогов* - события доступа пользователя к объекту каталога Active Directory, для которого задана собственная системная таблица управления доступом (SACL)
- *Изменение политик* - факт изменения политик назначения прав пользователей, политик аудита или политик доверительных отношений.

- *Использование привилегий* - каждая попытка пользователя воспользоваться предоставленным ему правом.
- *Отслеживание процессов* - такие события, как активизация программы, завершение процесса, повторение дескрипторов и косвенный доступ к объекту.
- *Системные события* - события перезагрузки или отключения компьютера, а также события, влияющие на системную безопасность или на журнал безопасности.
- *Управление учетными записями* - события, связанные с управлением учетными записями на компьютере. К таким событиям относятся, в частности, следующие:
  - Создание, изменение или удаление учетной записи пользователя или группы
  - Переименование, отключение или включение учетной записи пользователя
  - Задание или изменение пароля.

При включении аудита успеха или отказа соответствующие событие будет фиксироваться в оснастке «Просмотр событий».

Расширенная политика аудита (Рис 6) позволяет более тонко настроить журнал событий. Например, на вкладке «Вход учетной записи» (Рис 7) есть возможность включить ведение не всех событий, а только службы проверки подлинности с помощью Kerberos, или другие события входа учетных записей.

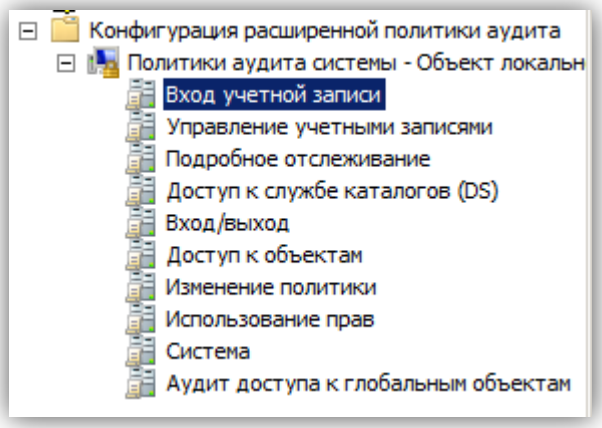


Рис 6.

Подкатегория	События аудита
Аудит проверки учетных данных	Не настроено
Аудит службы проверки подлинности Kerberos	Не настроено
Аудит операций с билетами службы Kerberos	Не настроено
Аудит других событий входа учетных записей	Не настроено

Рис 7.

2.2. События аудита доступа к файлам

На компьютере-члене домена создадим каталог «Сухоруков_Тест_Аудита». Для группы пользователей «Оператор call-цента» разрешим полный доступ (Рис 8). Далее на вкладке «Аудит» в свойствах созданного каталога добавим аудит для доменной глобальной группы «Пользователи домена», где укажем аудит и на успех и на отказ (Рис 9). Также включим аудит в свойствах локальной политики безопасности (Рис 10).

Имя объекта: C:\Сухоруков_Тест_Аудита

Элементы разрешений:

Тип	Имя	Разрешение	Унаследовано от	Применять к
Разреш...	Оператор call-центра (...	Полный доступ	<не унаследовано>	Для этой папки, ее под...

Рис 8.

Имя объекта: C:\Сухоруков_Тест_Аудита

Элементы аудита:

Тип	Имя	Доступ	Унаслед...	Применять к
Все	Пользователи домена (SUKHORUKOV\Польз...	Полный доступ	<не уна...	Для этой папки, е...

Рис 9.

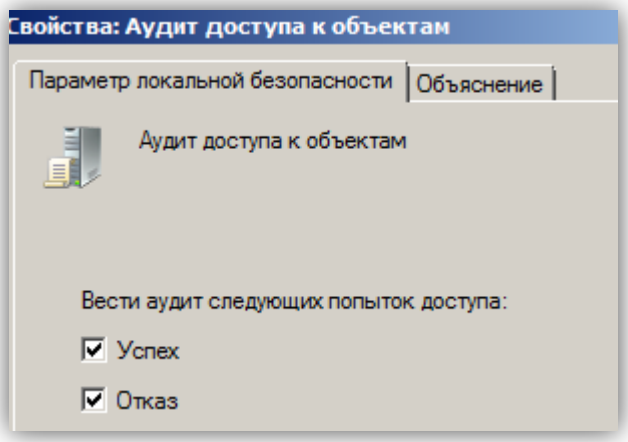


Рис 10.

Попробуем получить доступ к каталогу от учетной записью «Тимур_Игоревич», которая не входит в группу «операторы call-центра», и от учетной записью «Саша», входящей в указанную группу. В журнале событий сформировались события аудита успеха (Рис 12), и аудита отказа (Рис 11).

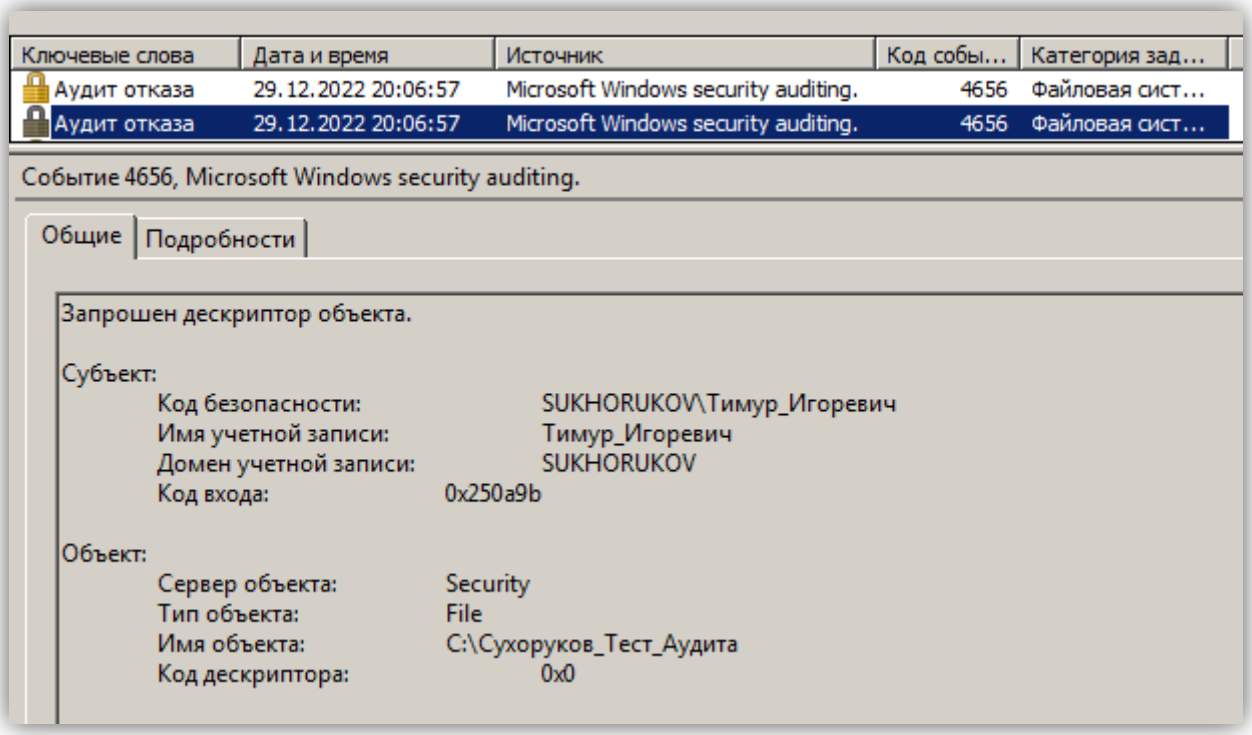


Рис 11.

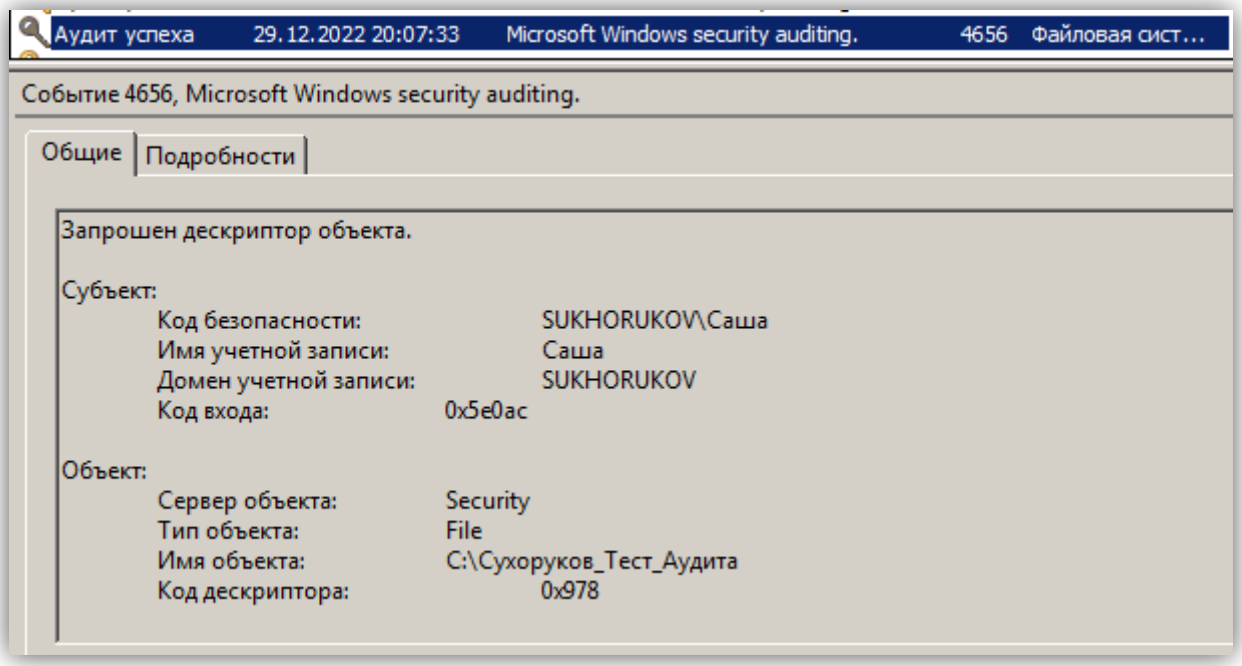


Рис 12.

Вывод:

Среди политик подключения аудита присутствует политика доступа к объектам. Данная политика позволяет осуществлять аудит объектов ФС, как было приведено в примере выше. События, для которых выполняется аудит могут быть настроены индивидуально для каждого из объектов ФС.

2.3. Аудит отслеживания процессов

Включим аудит отслеживания процессов на успех. Откроем и закроем «Блокнот». В журнале «Безопасность» появилось две записи: создание процесса, и завершение процесса.

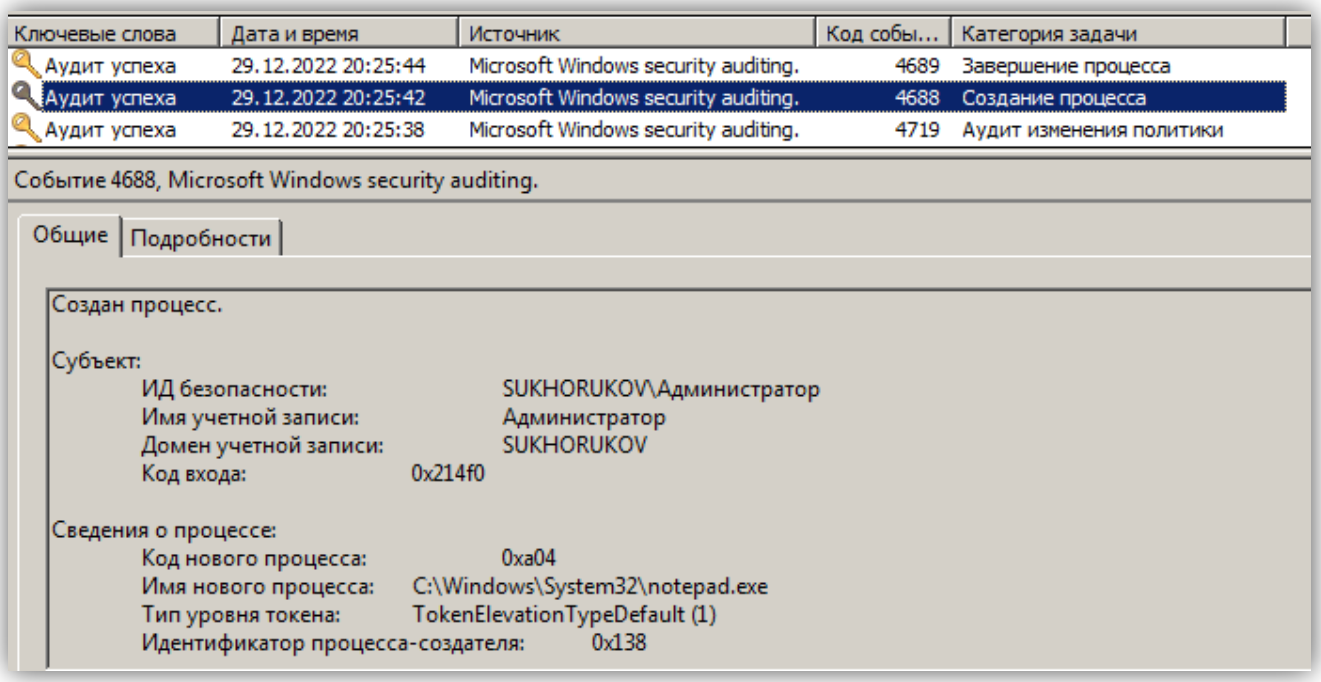


Рис 13.

После завершения «экспериментов» необходимо вернуть политики аудита в исходное состояние. Отключим аудит отслеживания процессов, и доступа к объектам.

Вывод:

Аудит отслеживания процессов позволяет отслеживать запуск разными пользователями программ. Аудит включать нужно осторожно, так как при большом потоке информации в журнал аудита возрастает нагрузка на систему.

3. Анализ и настройка безопасности локального компьютера

3.1. Шаблоны безопасности

Теория:

Шаблоны безопасности позволяют централизованно управлять параметрами безопасности на рабочих станциях и серверах. Они используются для применения к отдельным компьютерам заданных наборов параметров групповой политики, связанных с безопасностью. Эти наборы затрагивают следующие политики:

- *Политики учетных записей* - безопасность паролей, блокировка учетных записей и Kerberos.
- *Локальные политики* - аудит, назначение прав пользователей и другие параметры безопасности.
- *Политики журнала событий* - безопасность журнала событий.
- *Политики групп с ограниченным доступом* -администрирование членства в локальных группах.
- *Политики системных служб* - безопасность и режим запуска локальных служб.
- *Политики файловой системы* - безопасность путей к файлам и папкам локальной файловой системы.
- *Политики реестра* - значения параметров реестра, связанных с безопасностью.

Выполнение:

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

- C:\Windows\security\templates (Рис 14)
- C:\Windows\inf (Рис 15)

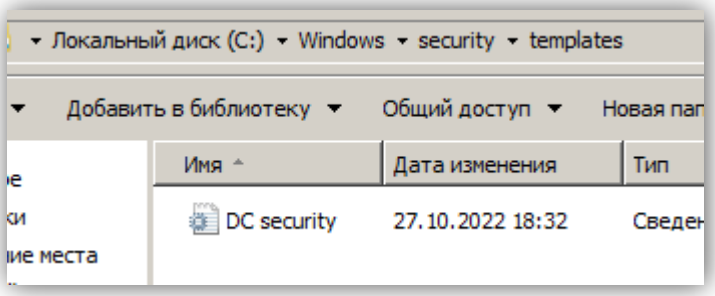


Рис 14.

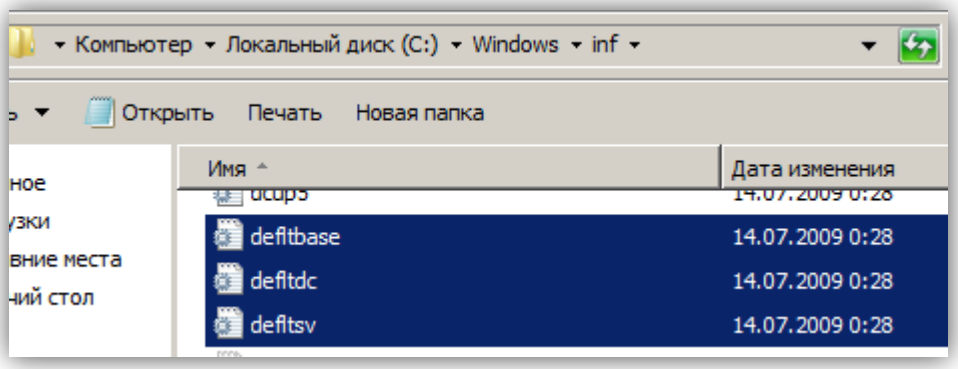


Рис 15.

На контроллере домена при присвоении ему такого статуса был создан шаблон «DC security», предназначенный для повышенной защиты сервера - в частности запрет входа с использованием 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.

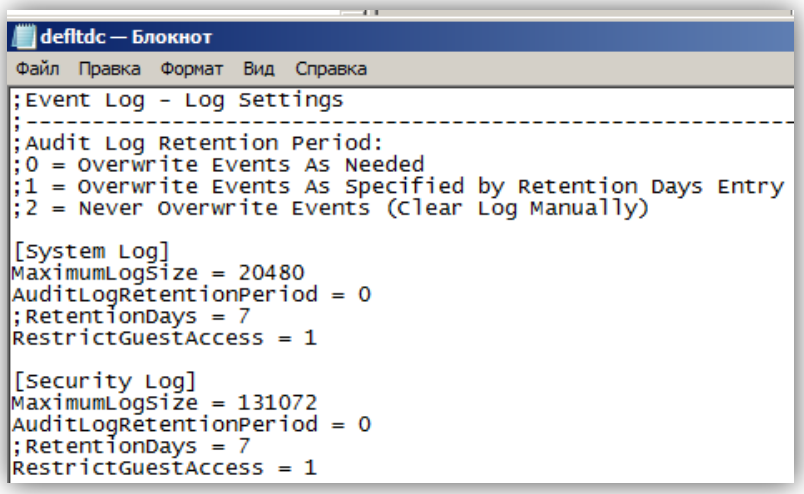


Рис 16.

Привилегии представлены, как выражения. В начале записана привилегия и ей сопоставленные SID пользователя. Если пользователей для, какой-то привилегии несколько, то SID`ы перечисляются через «,».

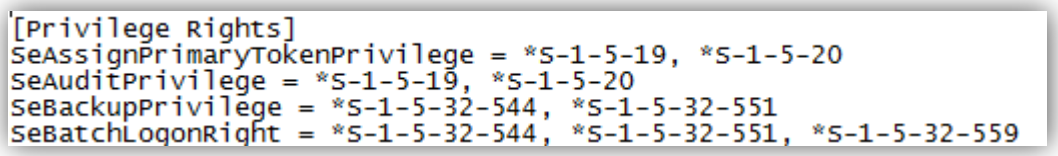


Рис 17.

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

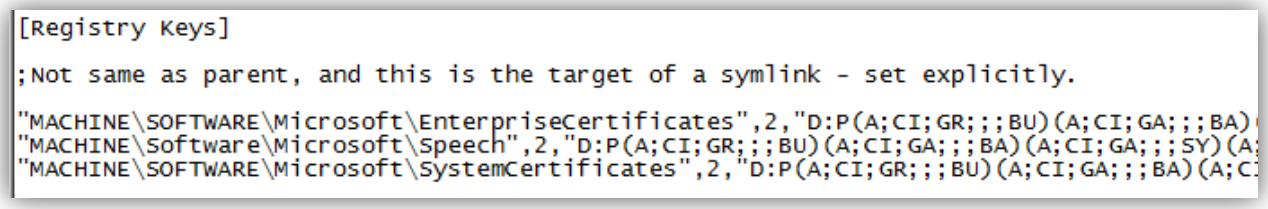


Рис 18.

С помощью оснастки «Шаблоны безопасности» сравним шаблоны для контроллера домена и для рядового сервера. Для этого добавим данную оснастку в консоль Microsoft Management Console (Рис 17).

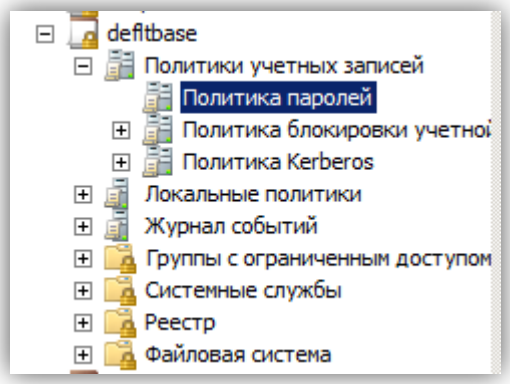


Рис 19.

Сведем параметры, которые отличаются у двух шаблонов в таблицу

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, Admini-

		страторы
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

Таблица 1.

Вывод:

Встроенные шаблоны безопасности идентичны по большей части параметров. Но шаблон default dc задает более строгие ограничения безопасности по части прав пользователей.

3.2. Соответствие текущей конфигурации компьютера шаблону

С помощью оснастки «Анализ и настройка безопасности» проверим соответствие текущей конфигурации рядового сервера Valerii-S-2 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**

Политика	Параметр базы данных	Параметр компьютера
Вести журнал паролей	0 сохраненных паролей	24 сохраненных пар…
Максимальный срок действия пароля	42 дн.	42 дн.
Минимальная длина пароля	0 зн.	7 зн.
Минимальный срок действия пароля	0 дн.	1 дн.
Пароль должен отвечать требованиям сложности	Включен	Включен
Хранить пароли, используя обратимое шифрование	Отключен	Отключен

Рис 20.

- Параметр «Вести журнал паролей» определяет число новых уникальных паролей, которые должны быть назначены учетной записи пользователя до повторного использования старого пароля.

Анализ полученных данных:

При текущей конфигурации пароль можно использовать повторно только после 24 других, отличных от него паролей. Минимальная длина пароля составляет 7 символов, вместо 0 в шаблоне. Минимальный срок действия пароля больше чем в шаблоне – пароль не получится повторно изменить сразу после его изменения. Параметры данного раздела являются более строгими, чем в шаблоне безопасности → при начальной конфигурации сервера для раздела политики паролей не используется стандартный шаблон deflbase.

❖ **Локальные политики → Назначение прав пользователей**

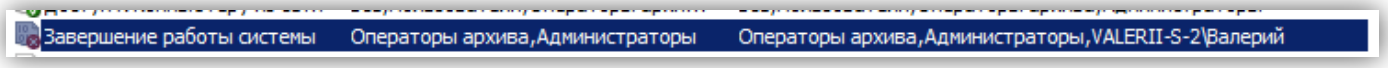


Рис 21.

Анализ полученных данных:

В первой лабораторной работе исследовались типы учетных записей. В ходе работы была создана локальная учетная запись Valerii-S-2\Валерий. Ей было предоставлено разрешение завершение работы системы. Значение текущей конфигурации данного разрешения не совпадает с шаблоном. В шаблоне установлено разрешение только для групп «Администраторы» и «Операторы архива».

3.3. Редактор безопасности secedit.exe

Утилита secedit запускается из командной строки и служит для управления политикой безопасности, применяющейся к компьютеру. Ее основными задачами являются:

- ❖ Анализ настроек безопасности системы
- ❖ Применение шаблонов безопасности
- ❖ Перезагрузка политики безопасности
- ❖ Экспорт политики безопасности в файл шаблона

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

Перейдем в каталог C: \ Users \ Администратор. SUKHORUKOV \ Documents\ Security \ Templates и выполним команду:

secedit.exe /generaterollback /cfg defltbase.inf /rbk sukhorukov_rollback.inf /log sukhorukov_rollback.log

После выполнения данной команды был создан шаблон на основе текущей конфигурации.

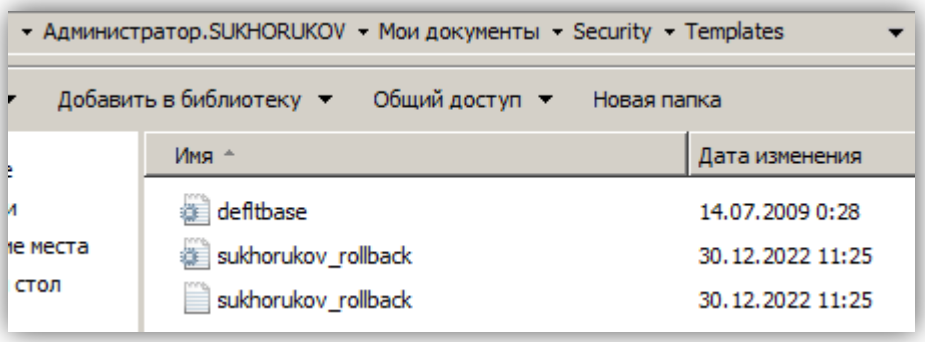


Рис 22.

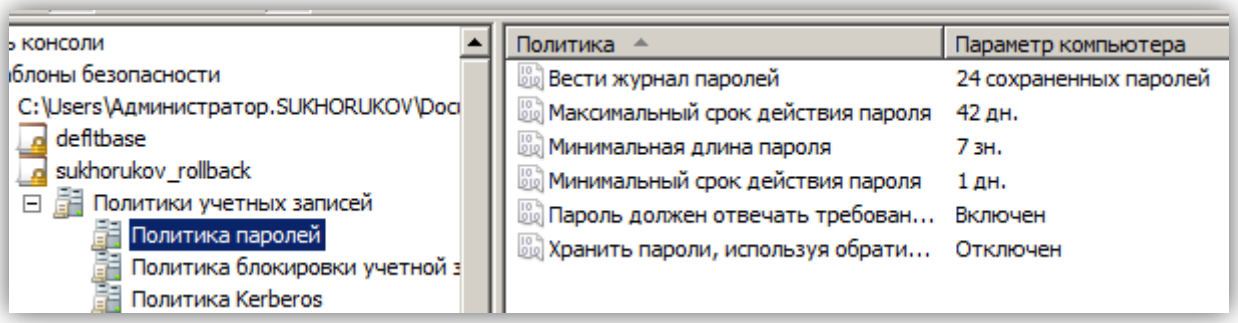


Рис 23.

3.4. 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».

❖ Добавим настройку разрешений доступа к каталогу C:\Сухоруков_Тест_Политик в политиках файловой системы:

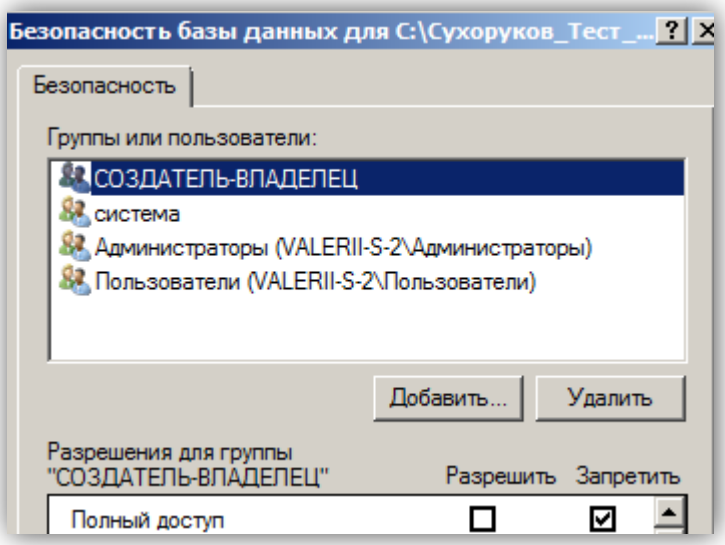


Рис 24.

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».

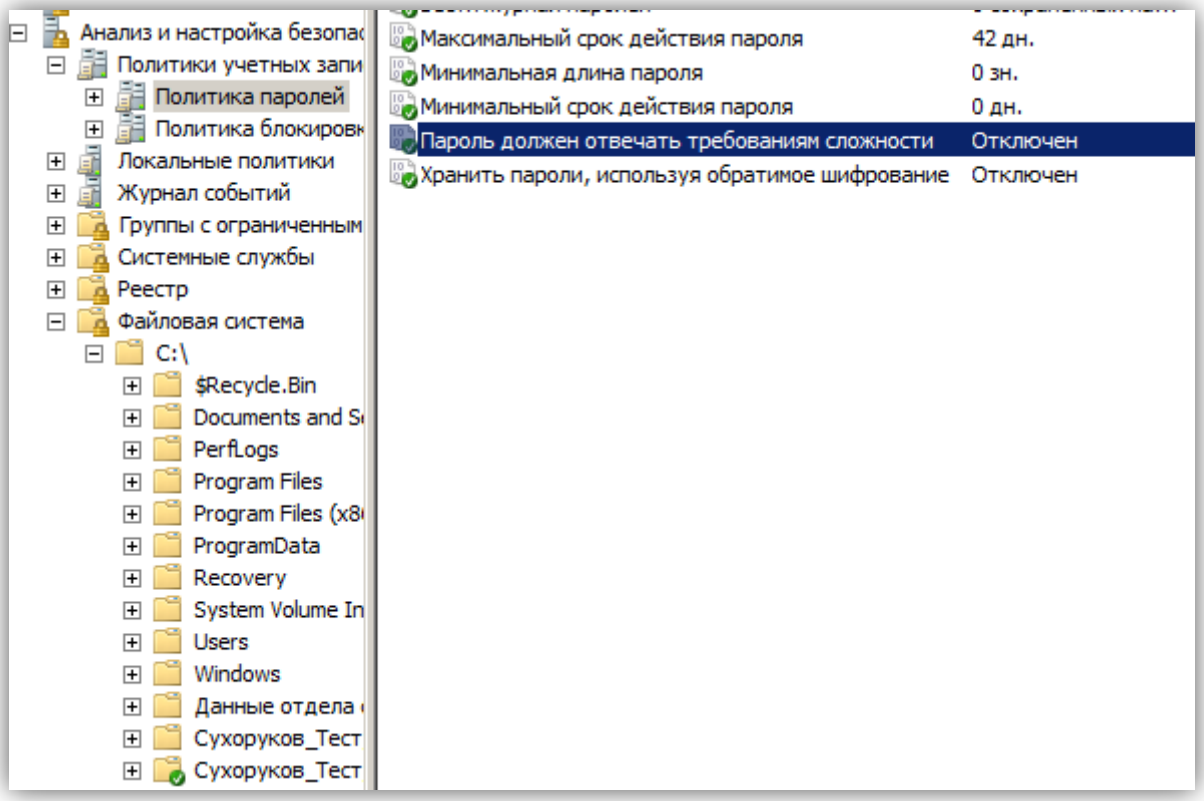


Рис 25.

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

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

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

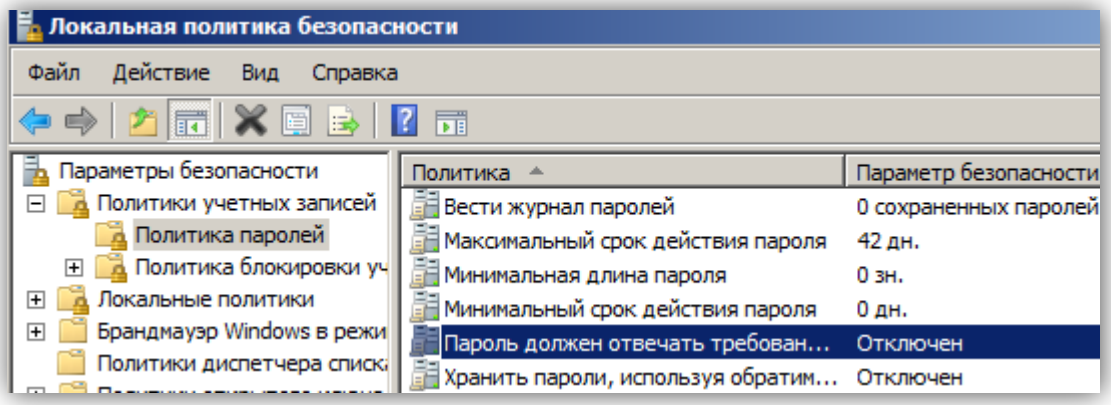


Рис 26.

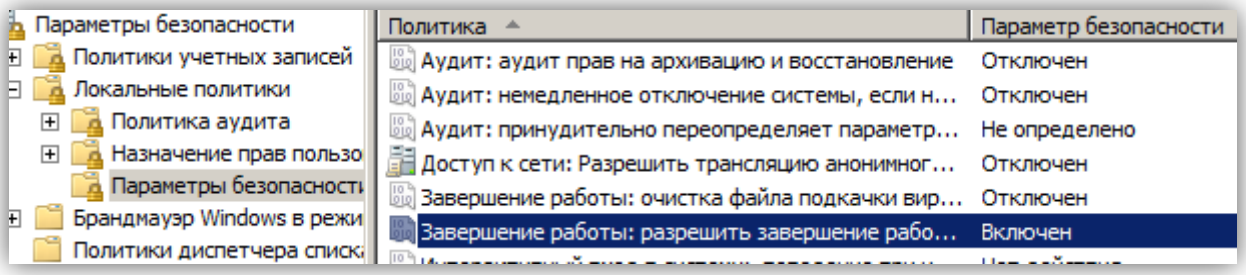


Рис 27.

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

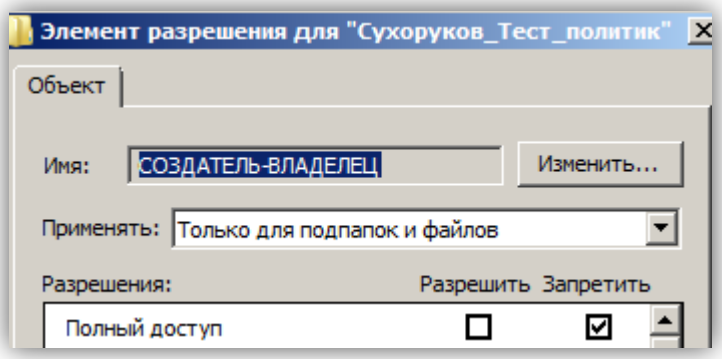


Рис 28.

Разрешения доступа применились успешно.

3.6. Отменить внесенные изменения.

Создадим базу данных на основе созданного шаблона резервной копии.

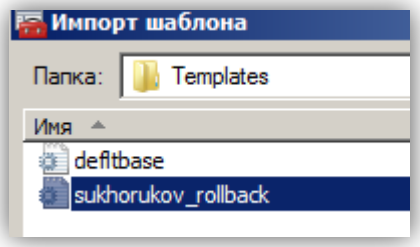


Рис 29.

Настроим компьютер в соответствии с этой базой данных.

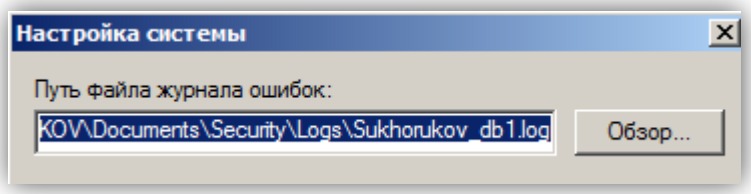


Рис 30.

Проверим применение изменений с помощью «Локальной политики безопасности».

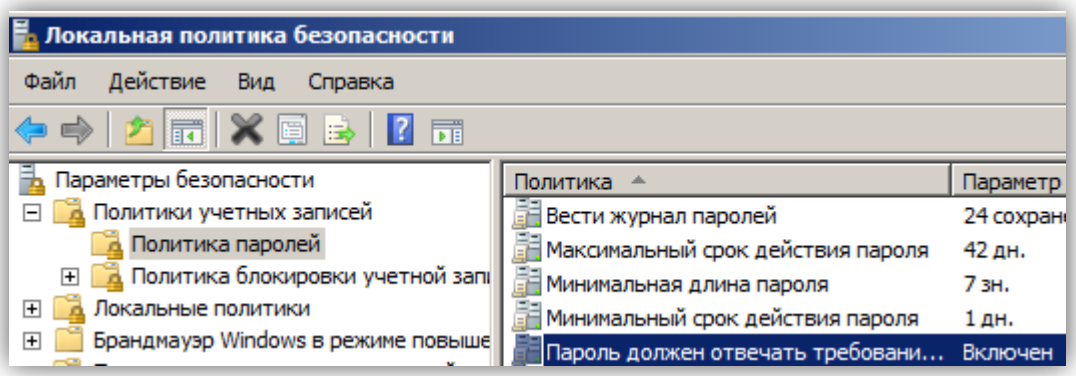


Рис 31.

Вывод:

- Оснастка "Анализ и настройка безопасности" позволяет проанализировать текущие настройки параметров безопасности компьютера в соответствии с заданным шаблоном.
- Шаблоны безопасности представляют собой текстовые файлы, в которых описаны настройки параметров безопасности системы.
- При помощи шаблонов безопасности можно настроить все компьютере в домене за очень короткое время. Не нужно будет настраивать каждый параметр на каждом компьютере вручную, необходимо будет только загрузить нужный шаблон безопасности.
- С помощью утилиты secedit возможно создавать резервную копию текущей конфигурации системы.

4. Базовые свойства, структура и применение групповых политик в домене.

4.1. Оснастка «Редактора локальной групповой политики»

Групповая политика — это совокупность параметров, используемых для конфигурирования рабочего окружения пользователя.

Создадим консоль и добавим в нее оснастку локальной групповой политики.

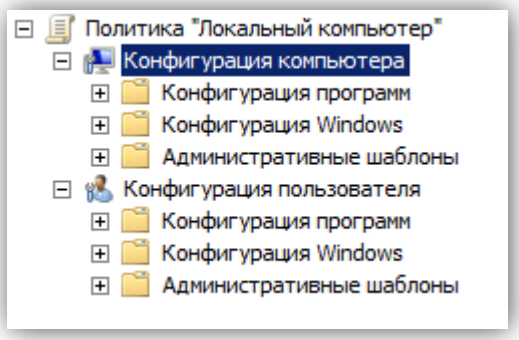


Рис 32.

Групповые политики применяются к двум категориям объектов: компьютеры и пользователи. «Конфигурация компьютера» влияет на окружение пользователя для конкретного компьютера независимо от зарегистрированных пользователей. Поэтому такие параметры применяются один раз в момент загрузки ОС. Политики «конфигурация пользователя» влияют на окружение конкретной учетной записи независимо от компьютера. Параметры политик пользователей применяются в момент регистрации пользователя.

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.

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

Попробуем изменить минимальную длину пароля на компьютере-члене домена. Для этого перейдем в «Конфигурация компьютера» → «Конфигурация Windows» → «Параметры безопасности» → «Политика паролей». Перейдем к пункту «Минимальная длина пароля». Изменение данного пункта недоступно т.к. в домене поверх локального GPO действует GPO домена, в котором параметры политики учетных записей переопределяются.

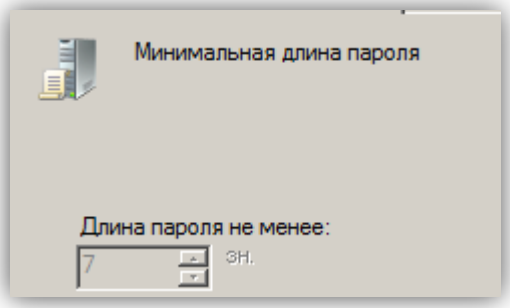


Рис 33.

Попробуем изменить минимальную длину пароля на контроллере домена. Перейдем к пункту «Минимальная длина пароля», и установим длину пароля, равную 4 знаком.

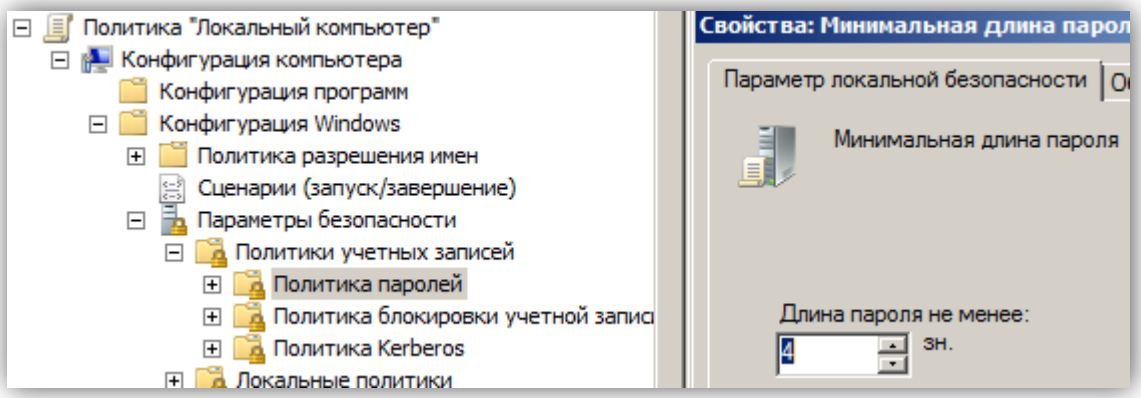


Рис 34.

Обновим политику с помощью gpupdate.

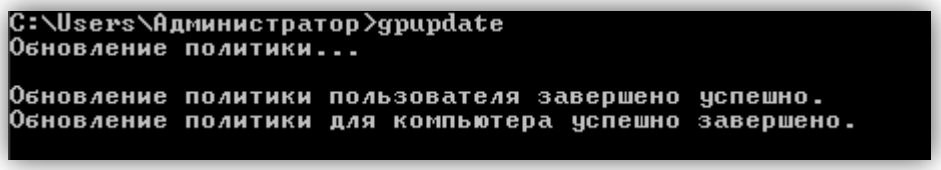
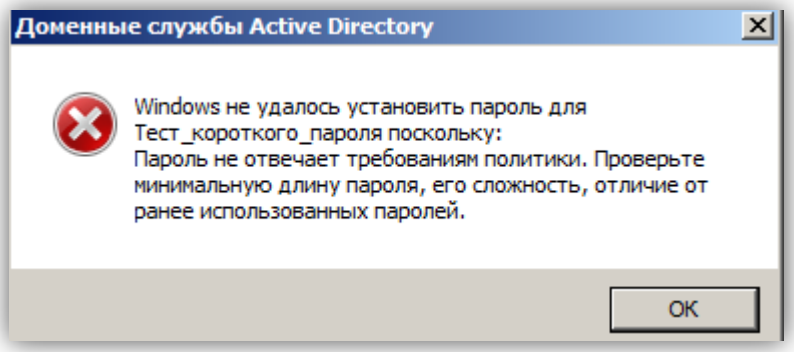


Рис 35.

Теперь попробуем создать пользователя с количеством символов в пароле менее 7, выведется ошибка:



Это связано с тем, что над локальными настройками компьютера преобладают настройки групповой политики домена.

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

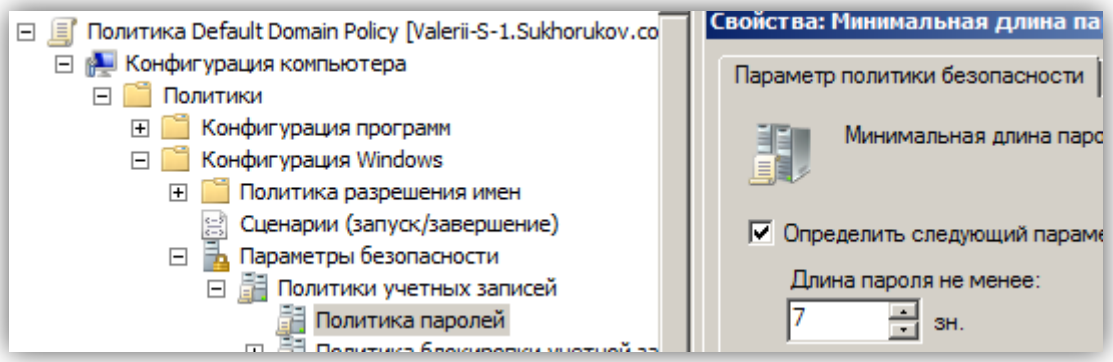


Рис 36.

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.

4.3. Административные шаблоны

Административные шаблоны, относящиеся к конфигурации компьютера, включают в себя компоненты, определяющие работу компьютера в целом. Шаблоны, которые относятся к конфигурации пользователя, определяют конфигурацию 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.

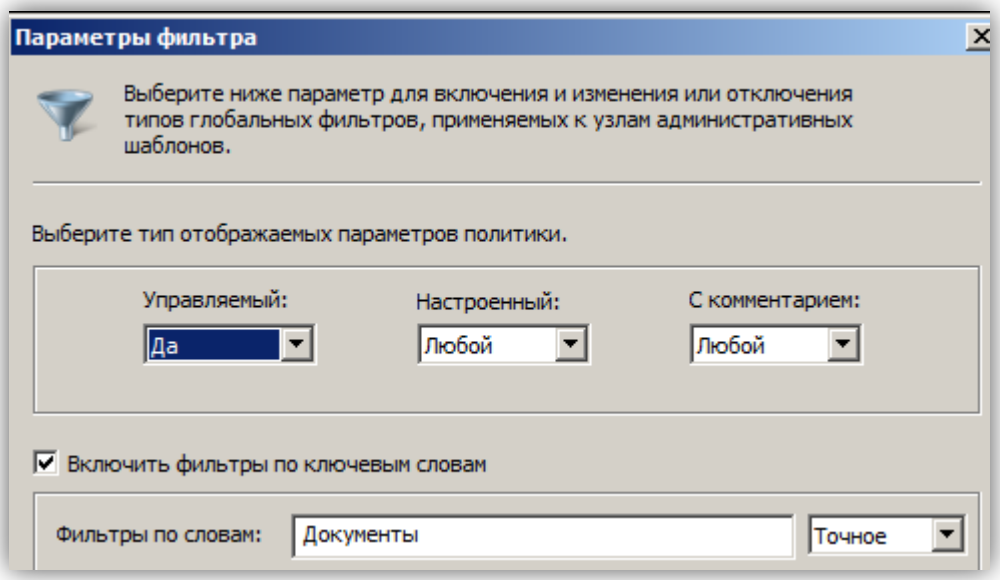


Рис 37.

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

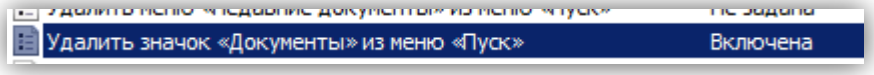


Рис 38.

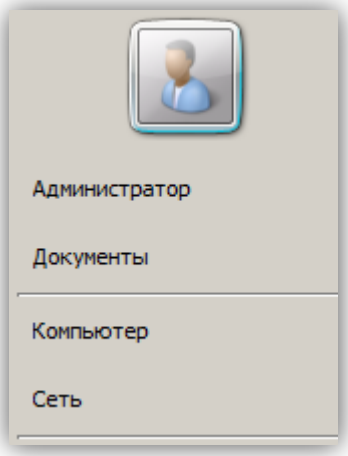


Рис 39.

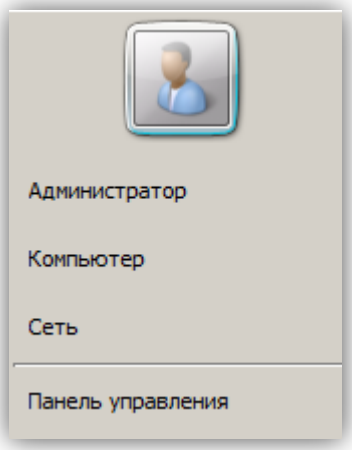


Рис 40.

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.

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

Для сравнения открываем настройки сети в конфигурации компьютера и пользователя, количестве настроек различается.

- **Сетевые настройки для компьютера:**

…/сеть/сетевые подключения/Брандмауэр Windows/Профиль домена

…/сеть/сетевые подключения/Брандмауэр Windows /Стандартный профиль

Параметры обоих профилей одинаковые, рассмотрю некоторые из них (как следует из родительского каталога, все параметры связаны с Брандмауэром Windows:

- Разрешить локальные исключения портов
- Разрешить локальные исключения программ
- Разрешить исключения для входящих сообщений удаленного администрирования
- Разрешить ведение журнала
- Защита всех сетевых подключений
- Не разрешать исключения

- **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.

4.5. Управление групповой политикой организационного подразделения

С помощью «Active Directory - пользователи и компьютеры» создадим организационное подразделение SukhorukovOU.

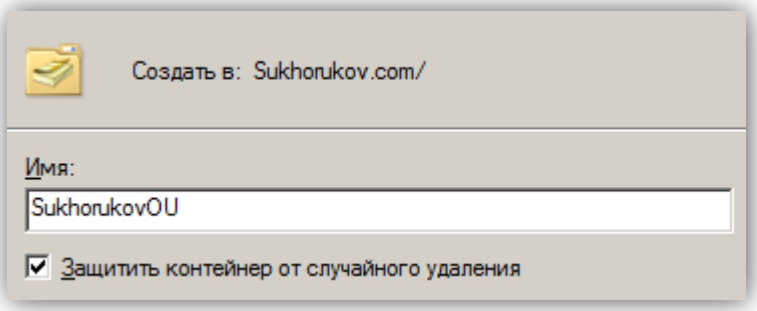


Рис 41.

Создадим учетную запись пользователя в данном подразделении.

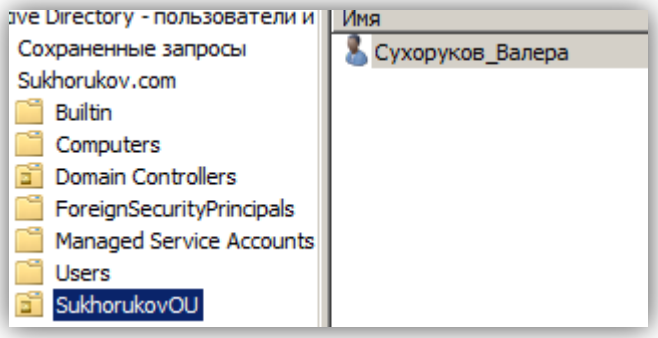


Рис 42.

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

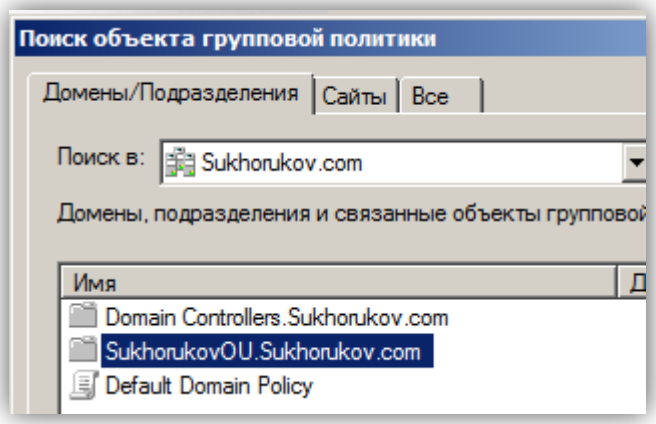


Рис 43.

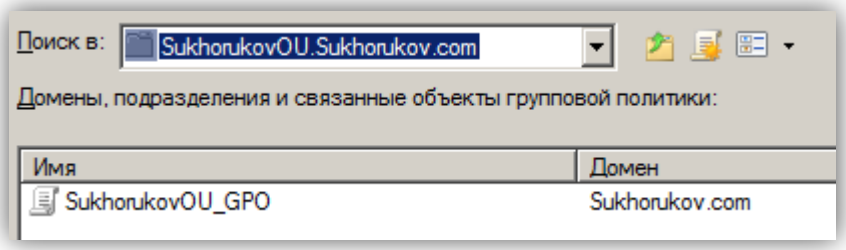


Рис 44.

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

Таблица 2.

Обновим групповую политику с помощью gpupdate. Проверим применение изменений.

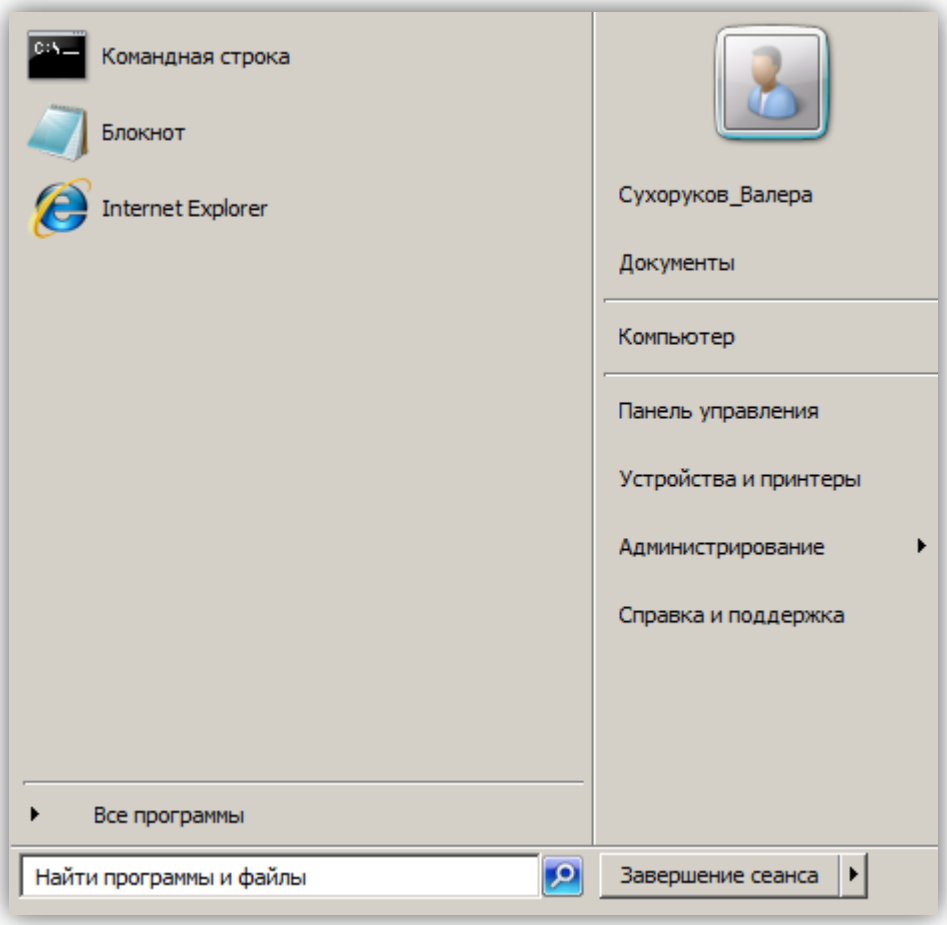


Рис 45.

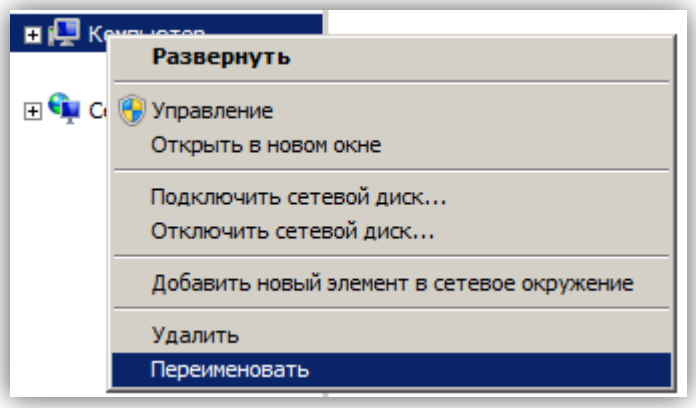


Рис 46.

4.6. 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.

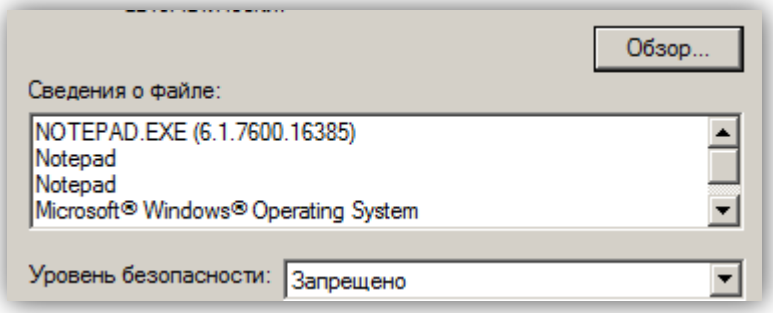


Рис 47.

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

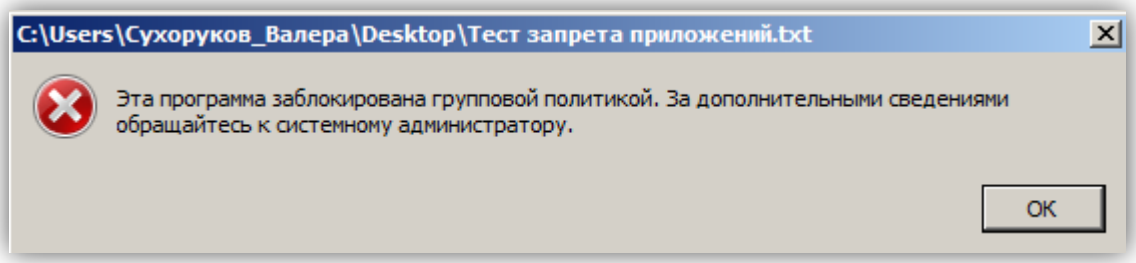


Рис 48.

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

Рассмотрим разрешения безопасности объекта групповой политики. Для этого необходимо в редакторе управления политиками выбрать нужный объект, перейти к его свойствам, и выбрать раздел «Безопасность».

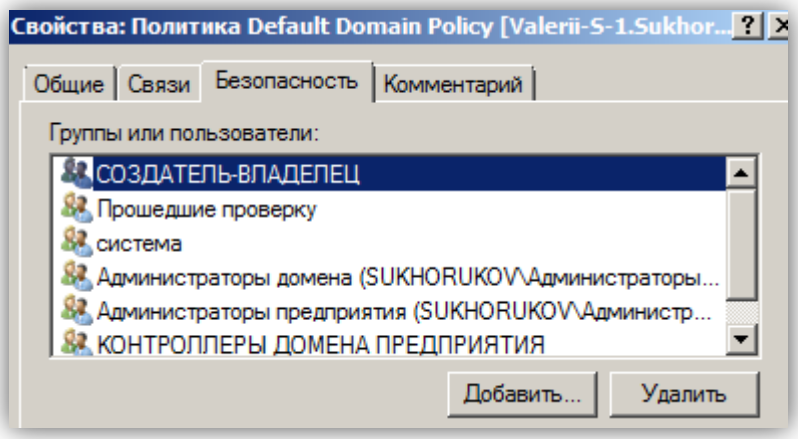


Рис 49.

Составим таблицу разрешений безопасности.

Домен:

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)

Таблица 3.

Подразделение SukhorukovOU:

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)

Таблица 4.

Вывод:

Различие между этими свойствами заключается в том, что в свойствах безопасности объекта политик домена происходит разделение разрешений для групп «Администраторы домена» и «Администраторы предприятия» на разрешения для объекта домена и разрешения для его дочерних объектов, в то время, как в свойствах безопасности объекта групповой политики организационного подразделения таких разделений нет.

4.8. Восстановить все свойства системы в исходное состояние

После завершения работ по групповым политикам в домене все настройки, проходя заново все действия из предыдущих пунктов, были возвращены по умолчанию.

Вывод:

Благодаря GPO можно задать конфигурацию компьютеров, также они указывают для пользователей программное обеспечение, перенаправленные папки, файлы и папки для автономного использования, профили пользователей (когда они перемещаются) - в общей сложности несколько сотен опций.

5. Использовать систему дистанционного администрирования Ideal Administration

5.1. Получение информации о контроллере домена

IDEAL Administration – программа для централизованного администрирования сетей, объединяющая в функциональные возможности, необходимые для управления пользователями, серверами и доменами.

IDEAL Administration упрощает:

- Управление группами пользователей,
- Установку учетных записей,
- Системный реестр,
- Сетевые свойства,
- Сессии,
- Процессы,
- Работу внешних устройств

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.

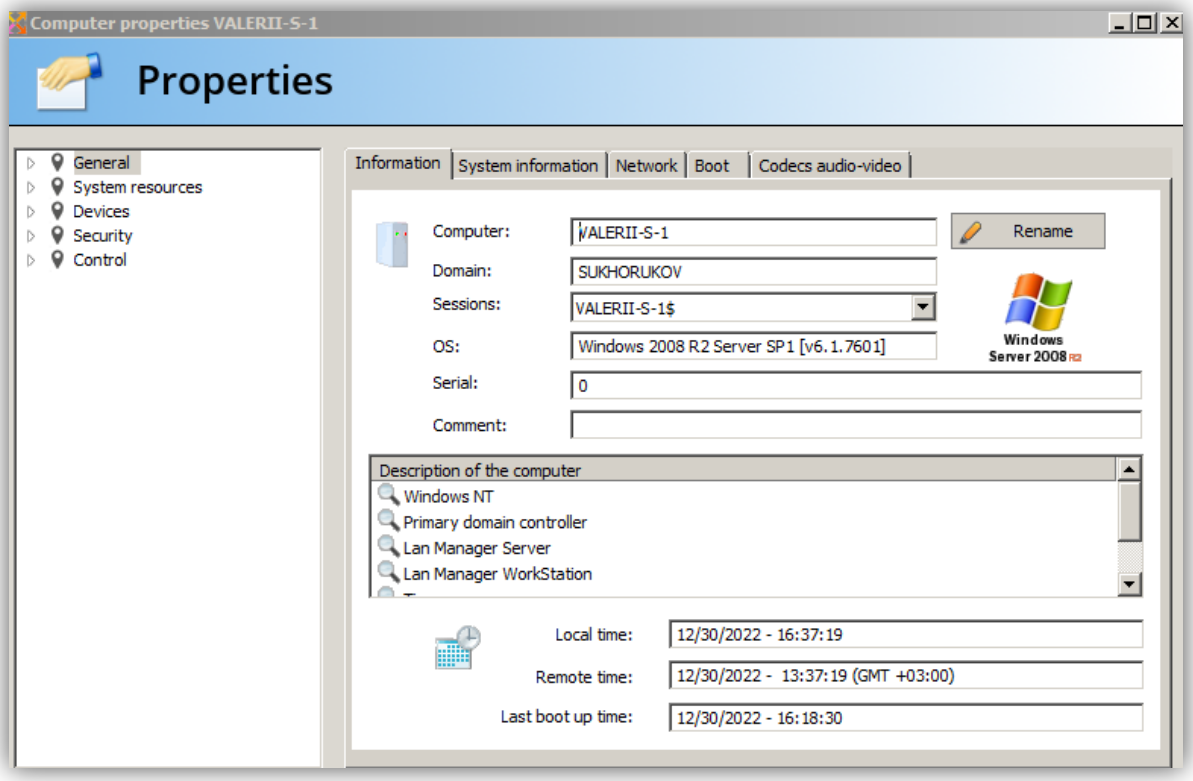


Рис 50.

5.2. 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».

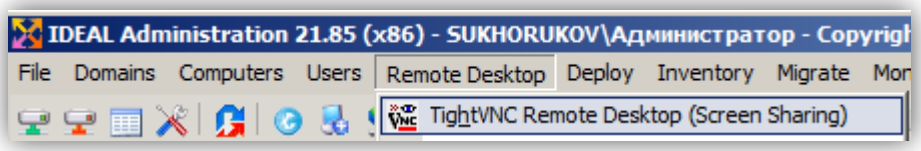


Рис 51.

Откроется рабочий стол выбранного компьютера.

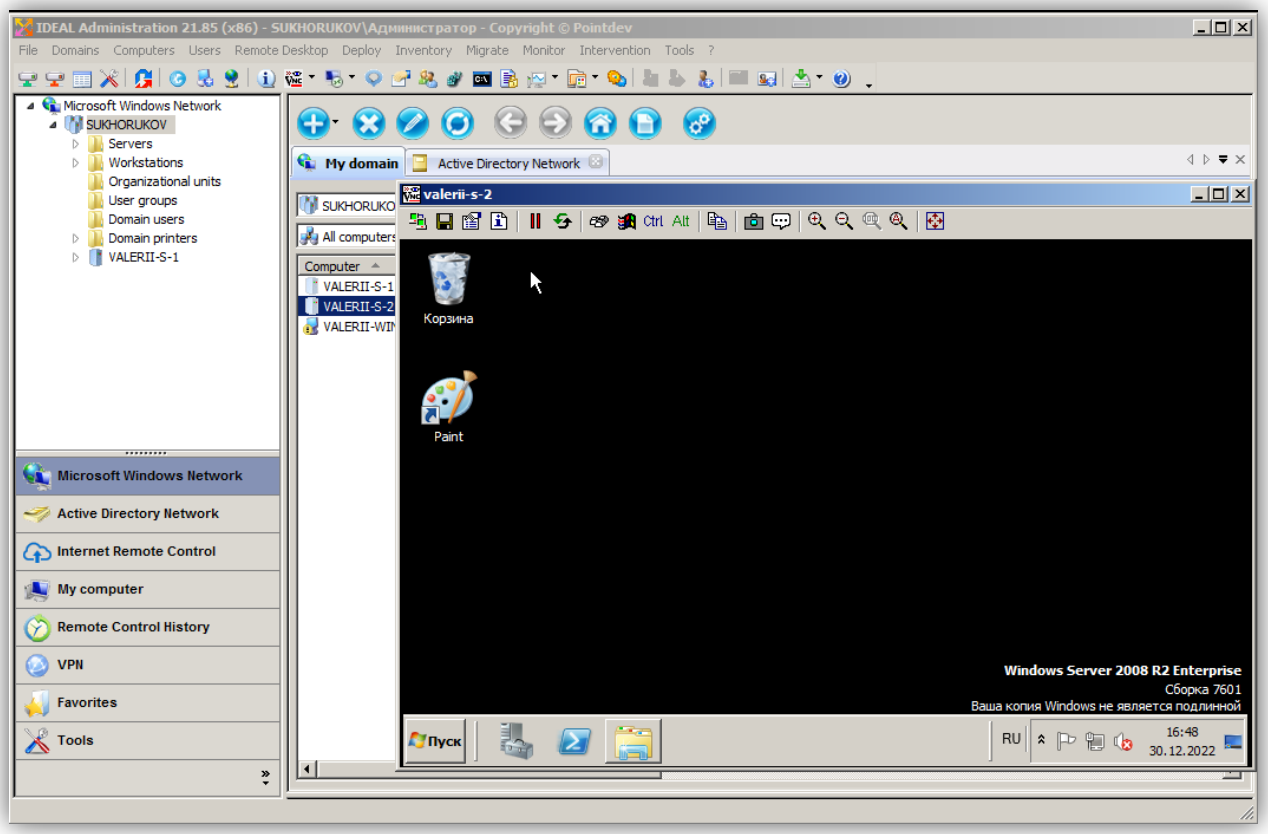


Рис 52.

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.

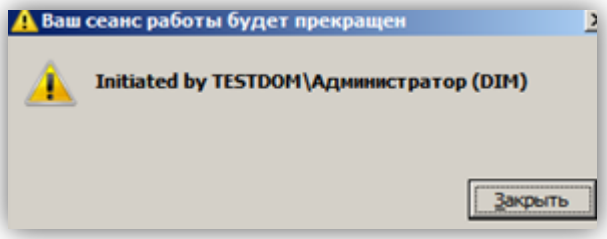


Рис 53.

Вывод:

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

Вывод

- В ходе выполнения данной лабораторной работы были изучены и опробованы на практике системные средства, предоставленные Windows Server, для получения информации о системе и настройки безопасности.
- Рассмотрены различные события из оснастки "Просмотр событий".
- Произведён анализ и работа с аудитом доступа к файловым ресурсам.
- С помощью консоли "Анализ и настройка безопасности" проанализирована конфигурация безопасности компьютера, созданы шаблоны отката и рассмотрены шаблоны безопасности.
- Также было произведено ознакомление со свойствами и структурой групповых политик, изучена их структура.
- С помощью многих оснасток производил эксперименты над этими GPO. Так же ознакомился с программой IDEAL Administration, и произвел администрирование через удаленный рабочий стол.