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 №1

«Администрирование пользователей 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

Ознакомиться с основными задачами администрирования, процедурами создания и формирования свойств пользователей и групп. Изучить свойства встроенных локальных и доменных учетных записей и групп. Ознакомиться с применением инструментальных средств управления учетными записями, группами домена и настроек привилегий пользователей.

Ход работы

1. Локальные учетные записи компьютера

1.1. Ознакомиться с составом встроенных локальных учетных записей и групп компьютера

Встроенные учетные записи – это учетные записи, которые создаются системой по умолчанию и не могут быть удалены. Список локальных учетных записей и групп можно получить через консоль «Диспетчер сервера», оснастку «Локальные пользователи и группы».

Встроенные локальные учетные записи пользователей в операционной системе Windows Server 2008 R2:

«Администратор»- Встроенная учетная запись администратора компьютера/домена,

«Гость»- Встроенная учетная запись для доступа гостей к компьютеру или домену.

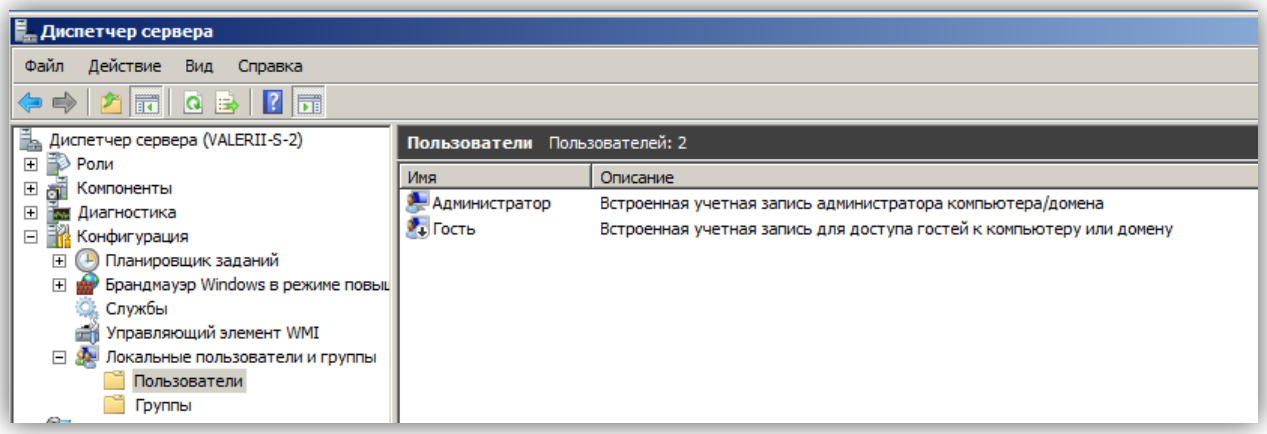

Рис 1. Оснастка «Локальные пользователи и группы»

1.2. Изучить назначение и возможности локальных групп компьютера - члена домена.

Встроенные локальные группы в операционной системе Windows Server 2008 R2 –

- «IIS_IUSRS»

Описание - группа для служб, которые используют IIS.

Члены группы по умолчанию – «NT_AUTHORITY\IUST (S-1-5-17)».

- «Администраторы»

Описание - группа для пользователей, которые имеют полные права доступа к компьютеру или домену.

Члены группы по умолчанию – встроенная локальная учетная запись «Администратор», члены группы «Администраторы домена» («SUKHORUKOV\Администраторы домена»).

- «Гости»

Описание - Гости по умолчанию имеют те же права, что и пользователи, за исключением учётной записи "Гость", ещё более ограниченной в правах.

Члены группы по умолчанию - встроенная локальная учетная запись «Гость».

- «Операторы архива»

Описание - Члены этой группы могут архивировать и восстанавливать любые файлы на контроллере домена в зависимости от наличия личных разрешений на эти файлы.

Члены группы по умолчанию – Отсутствуют.

- «Операторы настройки сети»

Описание - Пользователи, входящие в эту группу, могут изменять параметры TCP/IP, а также обновлять и освобождать адреса TCP/IP на контроллерах домена в домене.

Члены группы по умолчанию – Отсутствуют.

- «Операторы печати»

Описание - Члены группы имеют права на администрирование принтеров домена.

Члены группы по умолчанию – Отсутствуют.

- «Опытные пользователи»

Описание – в Windows Server 2008 R2 Категория опытных пользователей оставлена для обратной совместимости и обладает ограниченными административными правами.

Члены группы по умолчанию – Отсутствуют.

- «Пользователи»

Описание – Пользователи не имеют прав на изменение параметров системы и могут запускать большинство приложений.

Члены группы по умолчанию – «NT_AUTHORITY \ ИНТЕРАКТИВНЫЕ (S-1-5-4)», «NT_AUTHORITY \ Прошедшие проверку (S-1-5-11)» , «NT_AUTHORITY \ Пользователи домена».

- «Пользователи DCOM»

Описание – Члены этой группы могут запускать, активизировать и использовать объекты DCOM на этом компьютере.

Члены группы по умолчанию – Отсутствуют.

- «Пользователи журналов производительности»

Описание – Члены этой группы могут управлять счетчиками производительности, журналами и оповещениями на контроллерах домена в домене, на локальном или удаленном компьютере, не являясь при этом участниками группы «Администраторы».

Члены группы по умолчанию – Отсутствуют.

- «Пользователи системного монитора»

Описание – Члены данной группы имеют как местный, так и удаленный доступ к счетчику производительности.

Члены группы по умолчанию – Отсутствуют.

- «Пользователи удаленного рабочего стола»

Описание – Члены этой группы имеют право на выполнение удаленного входа.

Члены группы по умолчанию – Отсутствуют.

- «Репликатор»

Описание – Члены этой группы имеют право на поддержку репликации файлов в домене.

Члены группы по умолчанию – Отсутствуют.

❖ «Читатели журнала репликации»

Описание – Члены этой группы могут читать журналы событий с локального компьютера.

Члены группы по умолчанию – Отсутствуют.

1.3. Изучить свойства локальных учетных записей Администратор, Гость.

В окне свойств учетной записи есть следующие вкладки:

❖ **Общие.** На этой вкладке настраиваются общие параметры, такие как: Полное имя, описание учетной записи, отключение, блокировка и тд.

❖ **Членство в группах.** На это вкладке можно добавлять учетную запись к группам.

❖ **Профиль.** Можно настроить профиль учетной записи, ввести такие параметры как: путь к профилю, сценарий входа, домашняя папка.

❖ **Среда** – используется для настройки среды служб терминалов. Здесь можно назначить программу, запускаемую при входе в систему, а также подключаемые устройства (диски, принтер и выбор основного принтера)

❖ **Сеансы** – установка параметров таймаута и повторного подключения.

❖ **Удаленное управление** – настройка параметров удаленного управления служб терминалов.

❖ **Профиль служб терминалов** – настройка параметров профиля пользователя служб терминалов.

❖ **Входящие звонки** – разрешения на удаленный доступ VPN или модем, настройка ответного вызова сервера, явное указание статического IP адрес пользователя, использование статической адресации.

1) *Учетная запись Администратор*

Эта предопределенная учетная запись обладает полным доступом к файлам, папкам, службам и другим ресурсам; ее нельзя отключить или удалить. В Active Directory она обладает доступом и привилегиями во всем домене. В остальных случаях Администратор обычно имеет доступ только к локальной системе. Файлы и папки можно временно закрыть от администратора, но он имеет право в любой момент вернуть себе контроль над любыми ресурсами, сменив разрешения доступа.

Обычно менять основные параметры учетной записи Администратор не требуется, однако иногда следует сменить такие дополнительные параметры, как ее членство в некоторых группах.

По умолчанию учетная запись включена в группу: «Администраторы» .

2) *Учетная запись Гость*

Эта учетная запись предназначена для пользователей, которым нужен разовый или редкий доступ к ресурсам компьютера или сети. Гостевая учетная запись обладает весьма ограниченными системными привилегиями.

По умолчанию учетная запись включена в группу: «Гости». Все гостевые учетные записи являются членами неявной группы «Все» (Everyone), которая обычно по умолчанию имеет доступ к файлам и папкам и располагает стандартным набором прав пользователя.

2. Новая локальная учетная запись

2.1. Создание локальной учетной записи

Создадим новую локальную учётную запись. Сделать это можно с помощью оснастки «Локальные пользователи и группы» (Рис 2). В контекстном меню нового пользователя выберем пункт «Свойства». На вкладке «Членство в группах» новый пользователь принадлежит к группе «Пользователи» (Рис 3).

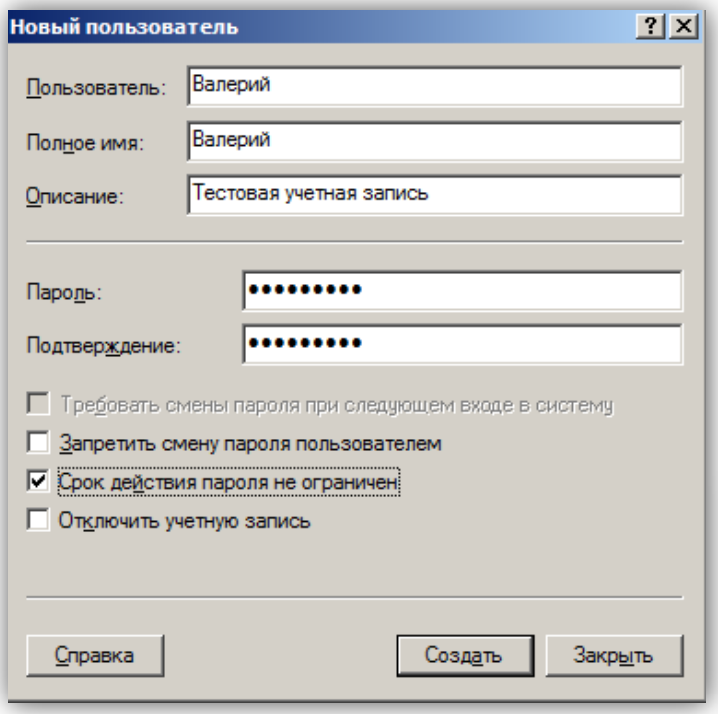

Рис 2. Создание локальной учетной записи

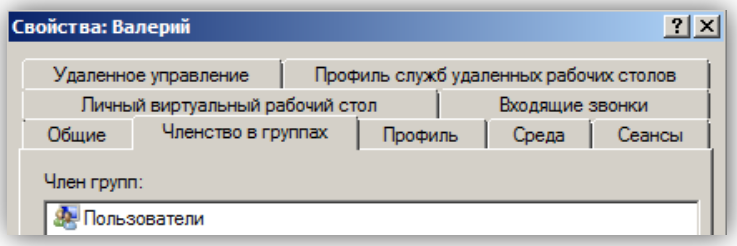

Рис 3. Членство в группах новой учетной записи

2.2. Свойства профиля локальной учетной записи

Зайдем в систему под учетной записью нового пользователя. При первом входе в систему создается локальный профиль пользователя, который состоит из домашнего каталога пользователя и настроек реестра ntuser.dat. Для этого в каталог пользователя «C:\Users\Валерий» копируется содержимое каталога «Default», который представляет собой профиль по умолчанию. На созданный каталог устанавливаются права доступа таким образом, что полный доступ имеет только сам пользователь, администраторы и система (Рис 5).

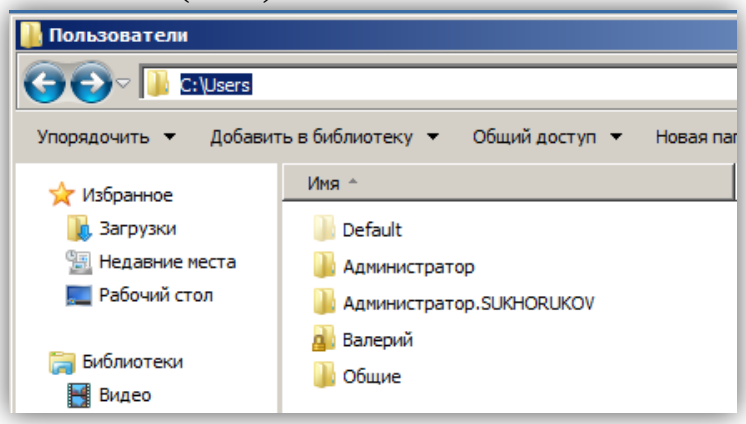

Рис 4. Структура каталога «C:\Users»

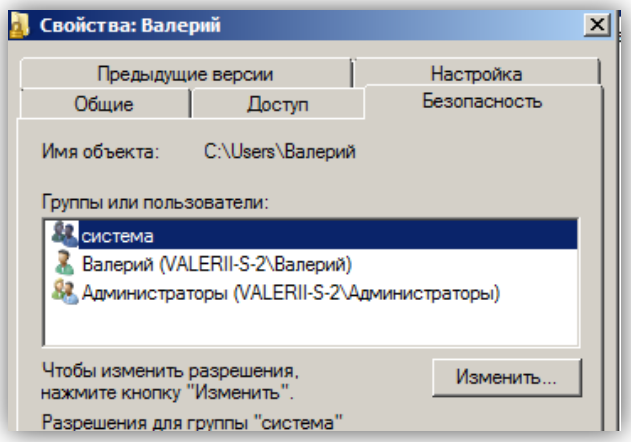

Рис 5. Права доступа к каталогу «C:\Users\Валерий»

Каталог пользователя содержит директории, файлы реестра (ntuser.dat, ntuser.dat.log) и Junction Points для совместимости с более старшими версиями Windows. Для того чтобы «увидеть» Junction Points можно настроить отображение скрытых файлов в каталоге, или использовать команду dir /al (Рис 6).

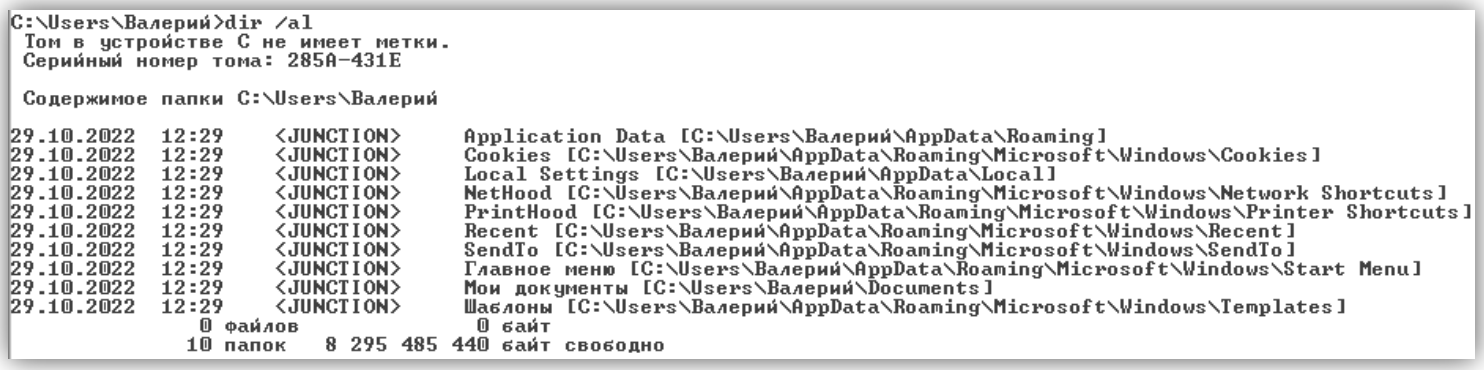

Рис 6. Junction Points каталога пользователя

2.3. SID новой локальной учетной записи

С помощью команды whoami можно получить сведения о текущем пользователе. Применим эту команду для пользователя «Валерий» с ключом /user для получения информации о SID.

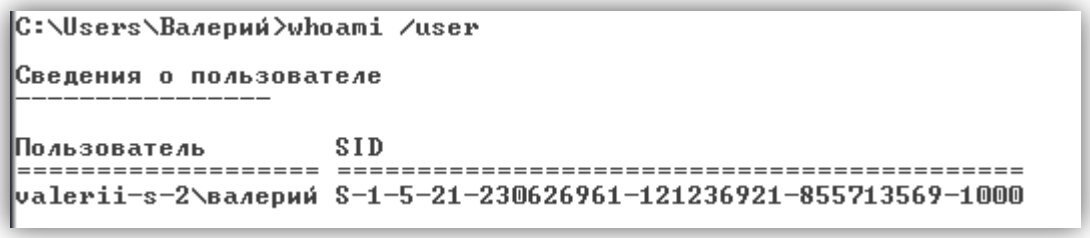

Рис 7. SID новой локальной учетной записи

- S-1-5-21 - означает, что это локальная учётная запись.
- 2306…569 – это уникальный идентификатор компьютера, выдавшего SID.
- 1000 - относительный идентификатор безопасности объекта (RID). Начинается с 1000 и увеличивается на 1 для каждого нового объекта.

3. Управление локальными параметрами безопасности

При помощи оснастки «Локальная политика безопасности» можно определять:

- Кто имеет доступ к компьютеру
- Какие ресурсы пользователи могут использовать на вашем компьютере;
- Включение и отключение записи действий пользователя или группы в журнале событий.

Применение политики на компьютере, входящем в домен:

Если локальный компьютер входит в домен, политика безопасности определяется политикой домена или политикой подразделения, членом которого является компьютер.

Если политика локального компьютера определяется более чем одним источником, приоритет при разрешении конфликтов политик имеют представленные далее источники в следующем порядке:

- Политика подразделения
- Политика домена
- Политика узла
- Политика локального компьютера

При изменении параметров безопасности на локальном компьютере с помощью локальной политики безопасности изменения вносятся непосредственно на локальном компьютере. Поэтому новые параметры сразу вступают в силу, но могут иметь временный характер.

3.1. Структура компонентов локальной политики безопасности

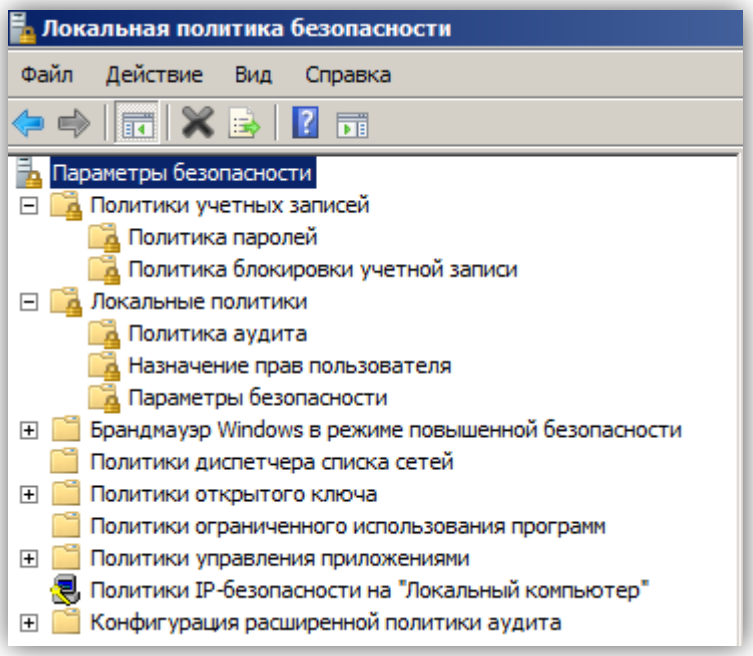

Рис 8. Структура компонентов локальной политики безопасности

❖ **Политика паролей** - используются для учетных записей доменов или локальных компьютеров. Определяют параметры паролей, такие как:

- Ведение журнала паролей – по умолчанию «24 Сохранённых паролей».
- Максимальный срок действия пароля – по умолчанию «42 Дня».
- Минимальная длина пароля – по умолчанию «7 Знаков».
- Минимальный срок действия пароля – по умолчанию «1 День».
- Пароль должен отвечать требованиям сложности – по умолчанию «Включен»
- Хранить пароли, используя обратимое шифрование – по умолчанию «Отключен».

❖ **Политика блокировки учетной записи** - используются для учетных записей доменов или локальных компьютеров. Определяет параметры блокировки учетной записи, такие как:

- Время до сброса счетчика блокировки – по умолчанию «Неприменимо».
- Пороговое значение блокировки – по умолчанию «0 ошибок входа в систему».
- Продолжительность блокировки учетной записи – по умолчанию «Неприменимо».

❖ **Назначение прав пользователя** – содержит множество прав пользователей по отношению к системе и доступу к ресурсам. Все права разделены между группами пользователей.

❖ **Параметры безопасности** – содержит настройки для завершения работы, входа в систему, настройки контроллера домена, члена домена, контроля учетных записей, сетевой безопасности и сетевого доступа.

3.2. Права (User rights) и разрешения (permissions)

Подсистема контроля доступа Windows, которая определяет пользователей, имеющих доступ к тем или иным ресурсам, основана на концепциях разрешений (permission) и пользовательских прав (user right). Разрешения связаны с объектами - например, разрешения для распечатывания файла, создания папки и добавления объекта user в Active Directory (AD). Пользовательские права (привилегии) связаны с системой Windows в целом - например, право пользователя регистрироваться в системе Windows или изменять системные часы.

Права пользователя Windows подразделяются на две категории: привилегии пользователя (user privilege) и права регистрации (logon right). Привилегии пользователя, такие как «Change the System Time» и «Shut down the System», обеспечивают контроль над си-

стемными ресурсами и операциями, связанными с системой. Права регистрации задают учетные записи пользователей, которые могут регистрироваться в системе Windows, и способ регистрации учетной записи пользователя в системе.

Привилегии пользователей преобладают над разрешениями.

3.3.Соотнесение прав пользователей (User rights) с группами пользователей.

Права Пользователя	Администраторы	Local Service	Network Service	Операторы архива	Пользователи	Прошедшие проверку	Все
Архивация файлов и каталогов	+			+			
Восстановление файлов и каталогов	+			+			
Вход в качестве службы			+				
Выполнение задач по обслуживанию томов	+						
Доступ к компьютеру из сети	+			+	+		+
Завершение работы системы	+			+			
Загрузка и выгрузка драйверов устройств	+						
Замена маркера уровня процесса		+	+				
Изменение системного времени	+	+					
Изменение часового пояса	+	+					
Имитация клиента после проверки подлинности	+	+	+				
Локальный вход в систему	+			+	+		
Настройка квот памяти для процесса	+	+	+				
Обход перекрёстной проверки	+	+	+	+	+		+
Отладка программ	+						
Профилирование производительности системы	+		+				
Смена владельцев файлов и других объектов	+						
Создание аудитов безопасности		+	+				
Создание глобальных объектов	+	+	+				
Увеличение рабочего набора процессов					+		

Таблица 1. Права групп пользователей

Анализ таблицы: Группа пользователей «Администраторы», согласно описанию, обладает практически неограниченными правами и может выполнять любые действия над системой.

Группа «Local Service» имеет возможность управлять процессами компьютера. Local Service предоставляет минимальный уровень разрешений службам, которым достаточно доступа только к локальным ресурсам. Службы Smart Card, Remote Registry и Telnet

используют учетную запись Local Service. Служба, работающая от имени Local Service, обращается к сетевым ресурсам с учетными данными «Anonymous».

Группа «Network Service» обеспечивает минимальный уровень разрешений для служб, которым необходим доступ к другим компьютерам в сети. Служба Network Service обращается к сетевым ресурсам с данными учетной записи компьютера. Службам Domain Name System (DNS) и Remote Procedure Call (RPC) по умолчанию присваиваются разрешения Network Service.

Группа «Операторы архива» предназначенная для выполнения резервного копирования и восстановления. Участники группы могут завершать работу системы на серверах и переопределять права доступа в целях резервного копирования. Пользователи этой группы могут администрировать локальные учетные записи и группы (кроме администраторов), создавать сетевые ресурсы, управлять доступом на них, и менять NTFS ACL (кроме смены владельца папки).

Группе «Пользователи» разрешены базовые операции с системой – вход в систему, удалённый доступ, просмотр и редактирование несистемных файлов.

Группа «Прошедшие проверку» включает в себя всех пользователей, чья подлинность была подтверждена при входе в систему, в них входят как локальные учетные записи, так и учетные записи доверенных доменов (кроме учетных записей гостя, LOCAL_SERVICE, NETWORK_SERVICE и некоторых других встроенных учетных записей). *Специальных прав группе не предоставлено.*

Группа «Все» (Everyone) включает всех членов группы Authenticated Users, а также гостевую учетную запись Guest и некоторые другие встроенные учетные записи, такие как LOCAL_SERVICE, NETWORK_SERVICE и др. *Группе предоставлены права «доступа к компьютеру из сети», и «Обхода перекрёстной проверки».*

3.4. Изменение прав по отношению к созданному пользователю

Теперь попробуем изменить локальную политику по отношению к пользователю Валерий. Разрешим пользователю «Завершение работы системы» (Рис 9), и запретим «Вход в систему через службу удалённых рабочих столов» (Рис 10) .

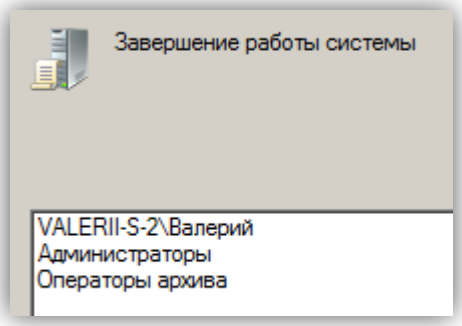

Рис 9.

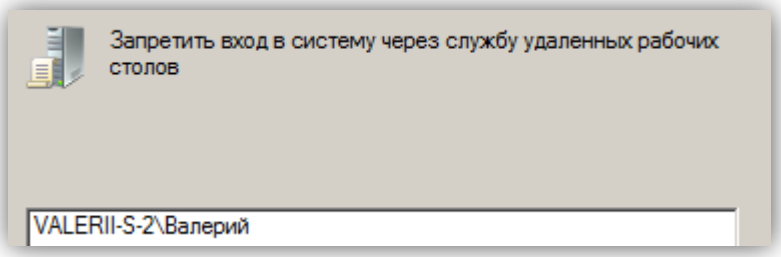

Рис 10.

Без перезагрузки компьютера войдём под учетной записью Валерий и убедимся, что завершение работы не доступно (Рис 11). Вернёмся в учетную запись администратора и перезагрузим компьютер для применения политик безопасности. Теперь завершение работы доступно новой учетной записи (Рис 12).

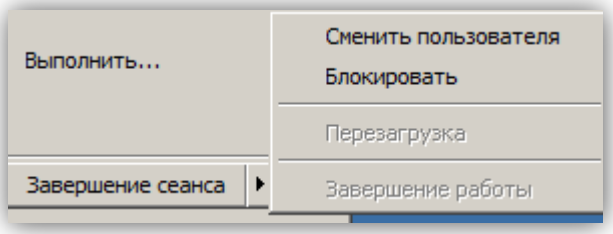

Рис 11.

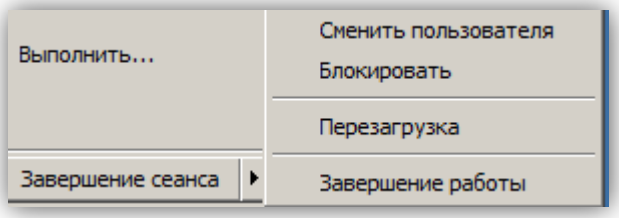

Рис 12.

3.5. Использование утилиты whoami

Получим с помощью команды whoami /all необходимые данные об учетных записях: SID, вхождение в группы и права.

- **SID**
- Valerii-S-2\Валерий

```
Пользователь          SID
===================== ============================================
valerii-s-2\валерий S-1-5-21-230626961-121236921-855713569-1000
```

- Valerii-S-2\Администратор

```
Пользователь                SID
=========================== ============================================
valerii-s-2\администратор S-1-5-21-230626961-121236921-855713569-500
```

- SUKHORUKOV\Администратор

```
Пользователь                SID
=========================== ============================================
sukhorukov\администратор S-1-5-21-467547321-4288138238-276818024-500
```

- Первая часть S-1-5-21 - означает, что это локальная учётная запись. У трех учетных записей совпадает.
- Вторая часть - это уникальный идентификатор компьютера или домена, выдавшего SID. У учетных записей компьютера Valerii-S-2 совпадает, у доменной учетной записи «Администратор» отличается.
- Третья часть - относительный идентификатор безопасности объекта (RID). Начинается с 1000 для создаваемых учетных записей, у «Администратора» - 500.

- **Сведения о группах**

Название группы	**SID**	**Valerii-S-2 \Валерий**	**Valerii-S-2 \Администратор**	**SUKHORUKOV \Администратор**
Все	S-1-1-0	+	+	+
BULTIN \ Пользователи	S-1-5-32-545	+	+	+
NT AUTHORITY \ Интерактивные	S-1-5-4	+	+	+
Консольный вход	S-1-2-1	+	+	+
NT AUTHORITY \ Прошедшие проверку	S-1-5-11	+	+	+
NT AUTHORITY \ Данная организация	S-1-5-15	+	+	+
Локальные	S-1-2-0	+	+	+
NT AUTHORITY \ Проверка подлинности NTLM	S-1-5-64-10	+	+	
Обязательная метка \ Средний обязательный уровень	S-1-16-8192	+		
BULTIN \ Администраторы	S-1-5-32-544		+	+
Обязательная метка \ Высокий обязательный уровень	S-1-16-12288		+	+
SUKHORUKOV\Владельцы-создатели групповой политики	S-1-5-21-46…024-520			+

SUKHORUKOV\Администраторы домена	S-1-5-21-46…024-512			+
SUKHORUKOV\Администраторы Схемы	S-1-5-21-46…024-518			+
SUKHORUKOV\Администраторы предприятия	S-1-5-21-46…024-519			+
SUKHORUKOV\Группа с запрещением репликации паролей RODC	S-1-5-21-46…024-572			+

Таблица 2. Сведения о группах разных типов учетных записей

Состав групп для «Valerii-S-2\Администратор» и «Valerii-S-2\Валерий» отличается тем, что Администратор имеет более высокий уровень «Высокий обязательный уровень» и входит в группу «BULTIN \ Администраторы». Остальные группы совпадают.

Учетная запись «SUKHORUKOV\Администратор» является администратором домена и входит в соответствующие доменные группы. Эта учетная запись не входит в группу «NT AUTHORITY\Проверка подлинности NTLM».

NTLM (NT LAN Manager) — протокол сетевой аутентификации, разработанный фирмой Microsoft для Windows NT. Основные проблема NTLMv1 :

- ❖ слабое шифрование
- ❖ хранение хэша пароля в оперативной памяти в службе LSA, который может извлечь различными утилитами и использовать хэш для дальнейших атак,
- ❖ отсутствие взаимной проверки подлинности клиента и сервера, что делает вполне реальными атаки перехвата данных и неавторизованного доступа к ресурсам сети
- ❖ ряд других уязвимостей.

Для доменной учетной записи администратора используется аутентификация с помощью Kerberos.

- ❖ **Сведения о привилегиях**

Описание привилегии	**Valerii-S-2 \Валерий**	**Valerii-S-2 \Администратор**	**SUKHORUKOV \Администратор**
Завершение работы системы	+	+	+
Обход перекрёстной проверки	+	+	+
Увеличение рабочего набора процессов	+	+	+
Настройка квот памяти для процесса		+	+
Управление аудитом и журналом безопасности		+	+
Смена владельцев файлов и других объектов		+	+
Загрузка и выгрузка драйверов устройств		+	+
Профилирование производительности системы		+	+
Изменение системного времени		+	+

Профилирование одного процесса		+	+
Увеличение приоритета выполнения		+	+
Создание файла подкачки		+	+
Архивация файлов и каталогов		+	+
Восстановление файлов и каталогов		+	+
Отладка программ		+	+
Выполнение задач по обслуживанию томов		+	+
Создание символических ссылок		+	+
Создание глобальных объектов		+	+

Таблица 3. Сведения о привилегиях разных типов учетных записей

Администраторы домена и администраторы компьютера имеют одинаково полный набор привилегии по отношению к системе. «Обычный» пользователь имеет очень ограниченный набор привилегий и не имеет доступа к управлению системой.

4. Elcomsoft System Recover

Elcomsoft System Recover – программа для восстановления доступа к учетным записям Windows, как к локальным, так и к сетевым.

Данная программа работает с локальными учётными записями (SAM), а также с учётными записями Active Directory.

В ней доступны следующие режимы работы:

- Изменение паролей и свойств учётных записей
- Дамп хэшей паролей для дальнейшей расшифровки
- Восстановление реестра или AD из сохранённой копии
- Редактор базы SAM
- Сохранение реестра или AD в архиве

Для загрузки данной программы необходимо изменить приоритет устройств загрузки виртуальной машины (Рис 13).

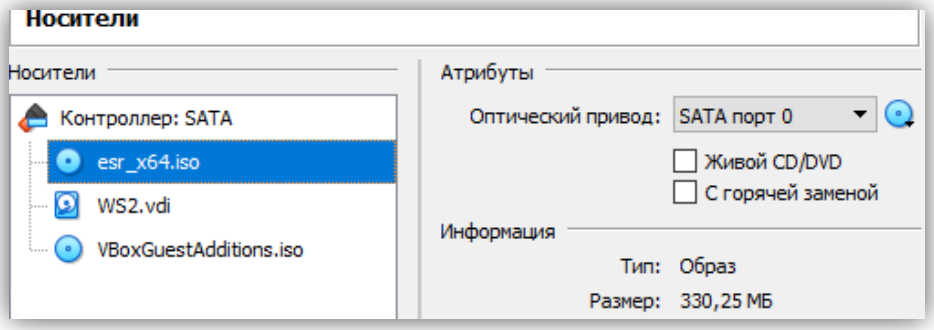

Рис 13.

При запуске программы появляется окно лицензионного соглашения программы. После принятия согласия, программа отображает структуру дисков с указанием их типа, файловой системы и размера (Рис 14). Выбираем тот диск, на котором установлена Операционная система.

На следующем этапе можно выбрать источник данных. Выбираем работу с базой данных SAM. Далее выбираем режим работы «Редактор SAM» .

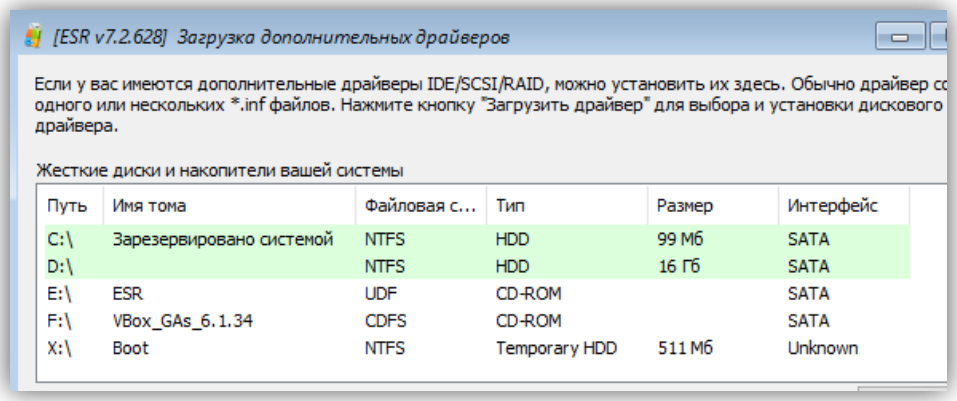

Рис 14. Выбор диска

По прошествии некоторого времени программа собрала данные об учетных записях (Рис 15).

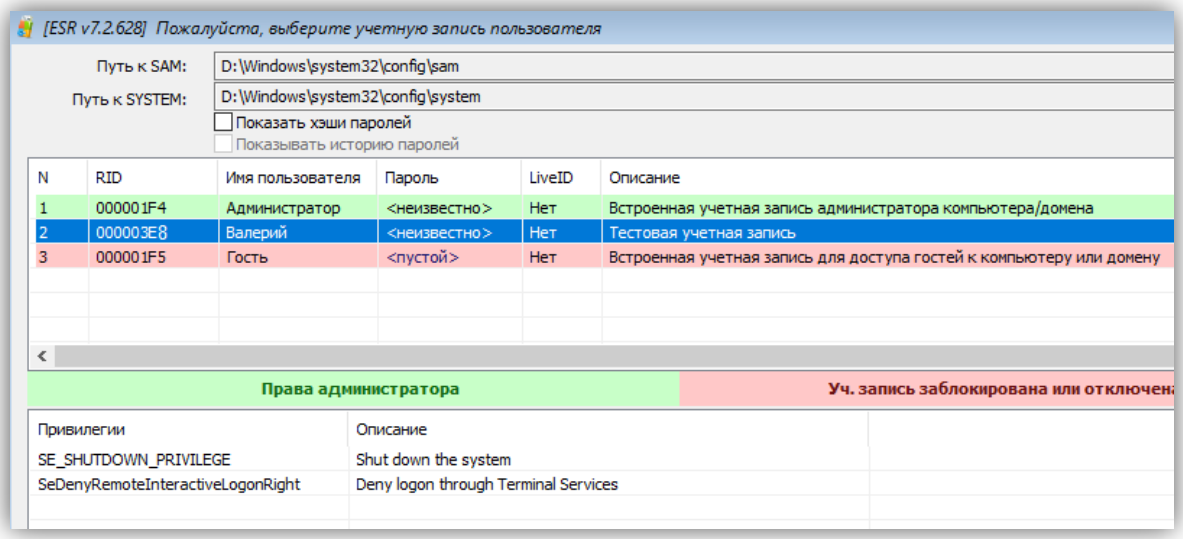

Рис 15. БД SAM

К полученным данным относятся:

- RID учётной записи в 16-ричной системе
- Имя пользователя
- Пароль – для гостя пароль пуст, для администратора и созданной учетной записи программа не смогла выявить пароль.
- Описание учетной записи.
- Предоставленные привилегии.

Выберем учетную запись «Валерий» и получим о ней больше сведений.

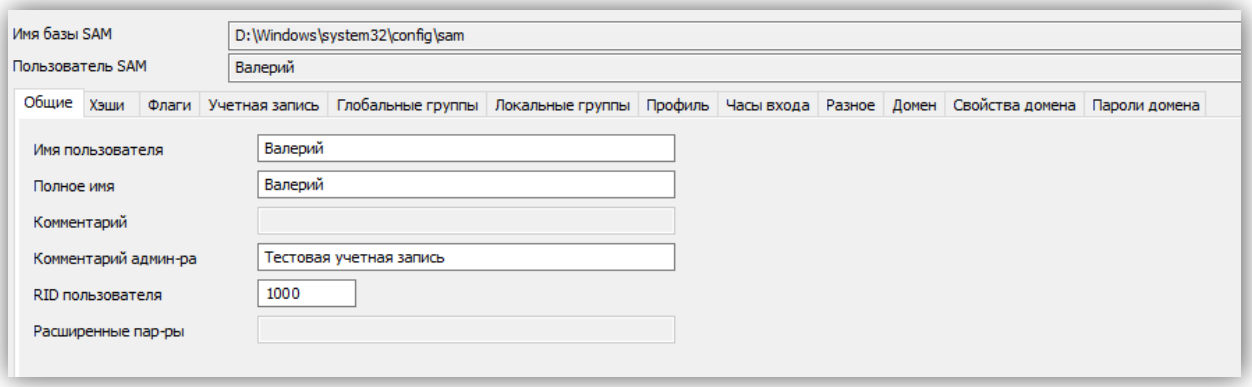

Рис 16.

На вкладке «Общее» можно изменить имя пользователя, полное имя, комментарий администратора, RID пользователя.

На вкладке «Хэши» можно изменить LM- и NT-хэши.

❖ При применении LM-хэширования длина пароля ограничена 14 символами. Самым большим недостатком алгоритма получения LM-хэша является разделение пароля на две части, каждая из которых состоит из семи символов. Если вводимый пользователем пароль менее 14 символов, то при преобразовании к нему добавляются нулевые символы, то есть символы с кодом 0, чтобы получить строку, состоящую из 14 символов. Если же пароль пользователя превышает 14 символов, то LM-хэш соответствует пустому паролю.

❖ NT-хэш лишен недостатков, присущих LM-хэшу. Во-первых, при NT-хэшировании используется алгоритм шифрования MD4, при котором пароль не разбивается на две 7-символьные части. Во-вторых, при NT-хэшировании нет ограничения по длине пароля в 14 символов. В-третьих, NT-хэш является регистрозависимым.

На вкладке «Флаги» можно изменить различные свойства учетной записи: отключить, отменить обязательный пароль и другие (Рис 17).

«Учетная запись» отображает данные последнего входа и выхода, а также время изменения пароля.

«Глобальные группы» и «Локальные группы» предоставляют возможность внесения или удаления учетной записи из той или иной группы.

На вкладке «Домен» можно увидеть или изменить SID домена (Рис 18).

«Пароли домена» предоставляет информацию о сроках действия пароля, его длине и ключ шифрования БД SAM (Рис 19).

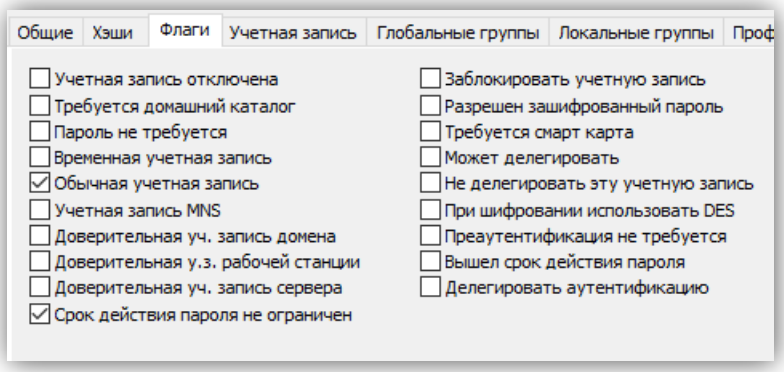

Рис 17.

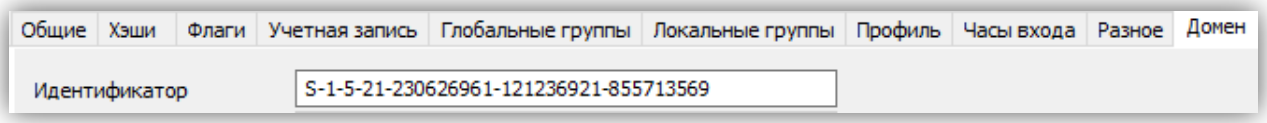

Рис 18.

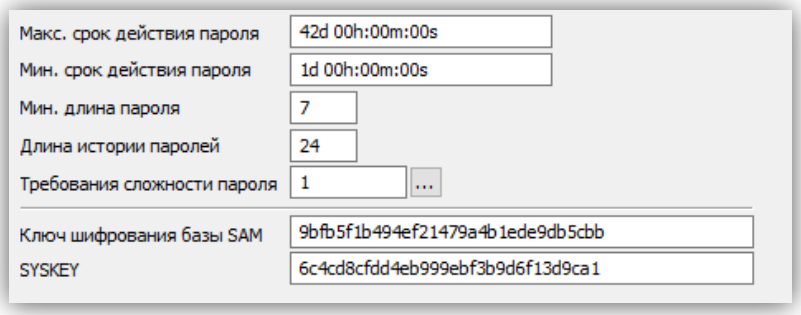

Рис 19.

5. Доменные учетные записи и группы

5.1. Состав встроенных доменных учетных записей и групп

На контроллере домена откроем консоль «Active Directory – пользователи и компьютеры», чтобы изучить состав учётных записей, локальных и глобальных групп домена.

Домен содержит следующие контейнеры:

- Builtin – содержит встроенные локальные группы домена.
- Computers – содержит учётные записи всех компьютеров, подключаемых к домену.
- Domain Controllers – содержит информацию обо всех контроллерах домена.
- ForeignSecurityPrincipals – контейнер для SID учетных записей пользователей из внешних доверенных доменов.
- Users – содержит информацию обо всех пользователях домена и о локальных, глобальных, универсальных группах домена.

Локальная в домене — используется для управления разрешениями доступа к ресурсам только того домена, где она была создана. Локальную группу нельзя использовать в других доменах (однако в локальную группу могут входить пользователи другого домена). Локальная группа может входить в другую локальную группу, но не может входить в глобальную.

Глобальная группа – данная группа может использоваться для предоставления доступа к ресурсам другого домена. В эту группу можно добавить только учетные записи из того же домена, в котором создана группа. Глобальная группа может входить в другие глобальные и локальные группы.

Универсальная группа — рекомендуется использовать в лесах из множества доменов. С помощью нее можно определять роли и управлять ресурсами, которые распределены на нескольких доменах. В том случае, если в вашей сети имеется много филиалов, связанных медленными WAN каналами, желательно использовать универсальные группы только для редко изменяющихся групп. Т.к. изменение универсальной группы вызывает необходимость репликации глобального каталога во всем предприятии.

Локальные группы контейнера Builtin имеют короткие «Хорошо известные» SID-ы. Под хорошо известными идентификаторами SID понимаются группы SID, идентифицирующие общих пользователей или общие группы. Их значения остаются постоянными во всех операционных системах.

5.2. Структура учетных записей и групп

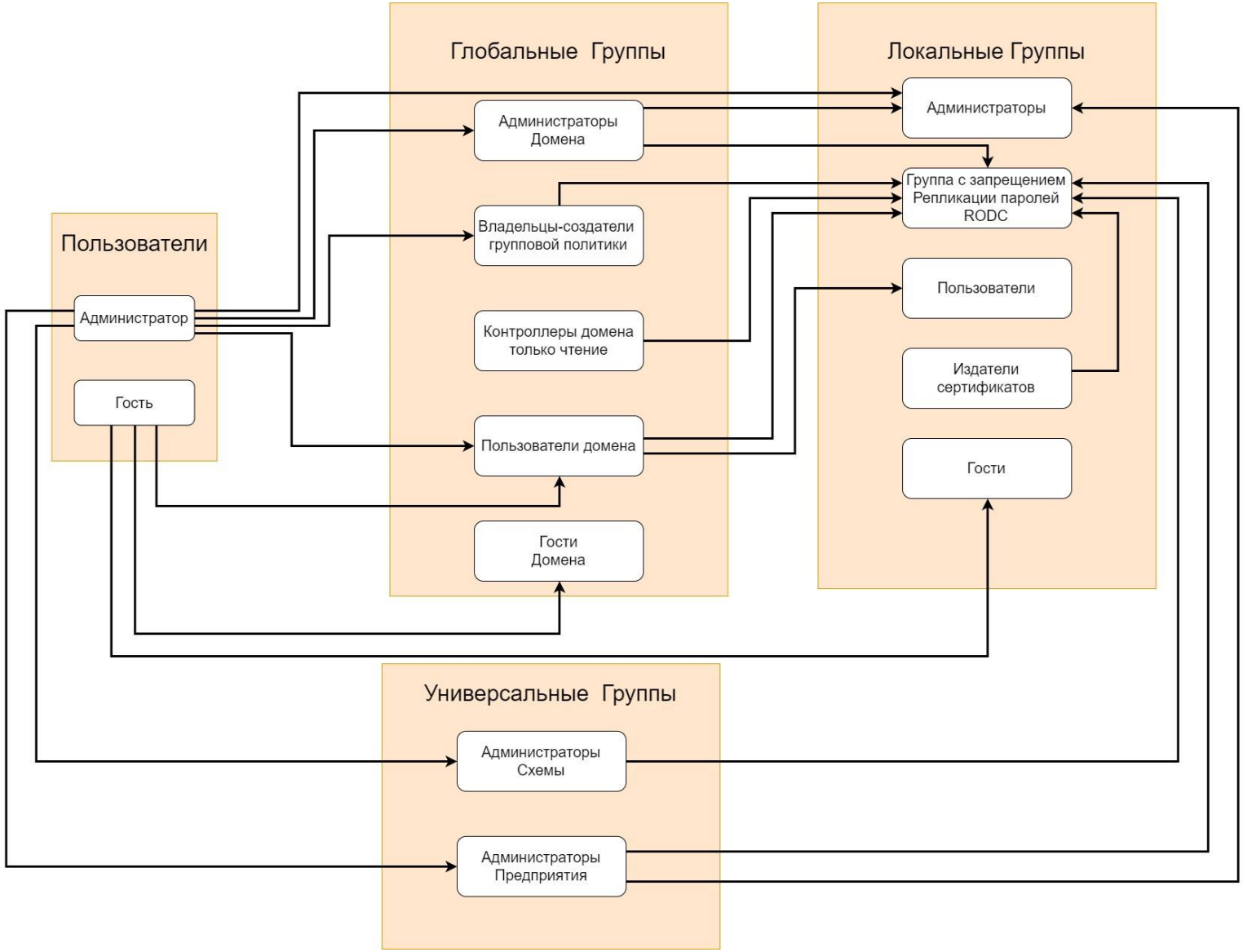

Рис 20.

На рисунок не были помещены группы, не имеющие привязок.

6. Планирование модели доменной сети небольшой организации

6.1. Определение категорий пользователей

Спроектируем модель отдела call-центра, занимающегося обработкой обратной связи от клиентов и приёмом заказом. В этой организации можно выделить такие категории пользователей, как:

- Руководитель отдела
- Оператор call-центра
- Администратор сети
- Администратор по управлению пользователями
- Сотрудник службы охраны

Необходимо сформулировать требования и условия работы пользователей.

Категория	Административные возможности	Доступ к данным	Возможность применения программ
Руководитель отдела	Руководитель отдела не должен иметь административные возможности. Поскольку он не является опытным пользователем и может что-нибудь «сломать».	Должен иметь доступ ко всем данным отдела. Во избежание возможных ошибок, доступ к некоторым файлам может быть предоставлен только по чтению.	Может иметь доступ к любым программам.
Оператор call - центра	Оператор не входит в группу сотрудников, которая имеет возможность изменять «важные свойства системы», административных возможностей у него быть не должно.	Должен иметь полный доступ к тем данным, с которыми он работает. Доступ к данным других операторов может быть только по чтению.	Сотрудники отдела не должны отвлекаться от работы. В качестве примера запретим доступ к приложению «Paint».
Администратор сети	Администратор сети должен иметь доступ к изменению сети, настройке стека TCP/IP.	Не имеет доступа к коммерческим данным отдела.	Может иметь доступ к любым программам.
Администратор по управлению пользователями	Администратор по управлению пользователями должен иметь доступ к настройке групп и учетных записей пользователей.	Не имеет доступа к коммерческим данным отдела.	Может иметь доступ к любым программам.
Сотрудник службы охраны	Сотрудник службы охраны является «почти посторонним человеком», которому ни в коем случае нельзя предоставлять доступ к административным возможностям.	Не имеет доступа к данным отдела. Имеет доступ к «Журналу посещения» - должен записывать всех входящих и выходящих.	Необходимо запретить доступ к специфическому ПО, используемому сотрудниками отдела. Для примера запретим доступ к приложению «Командная строка».

Таблица 4. Требования к категориям пользователей

6.2. Структура учетных записей и групп пользователей

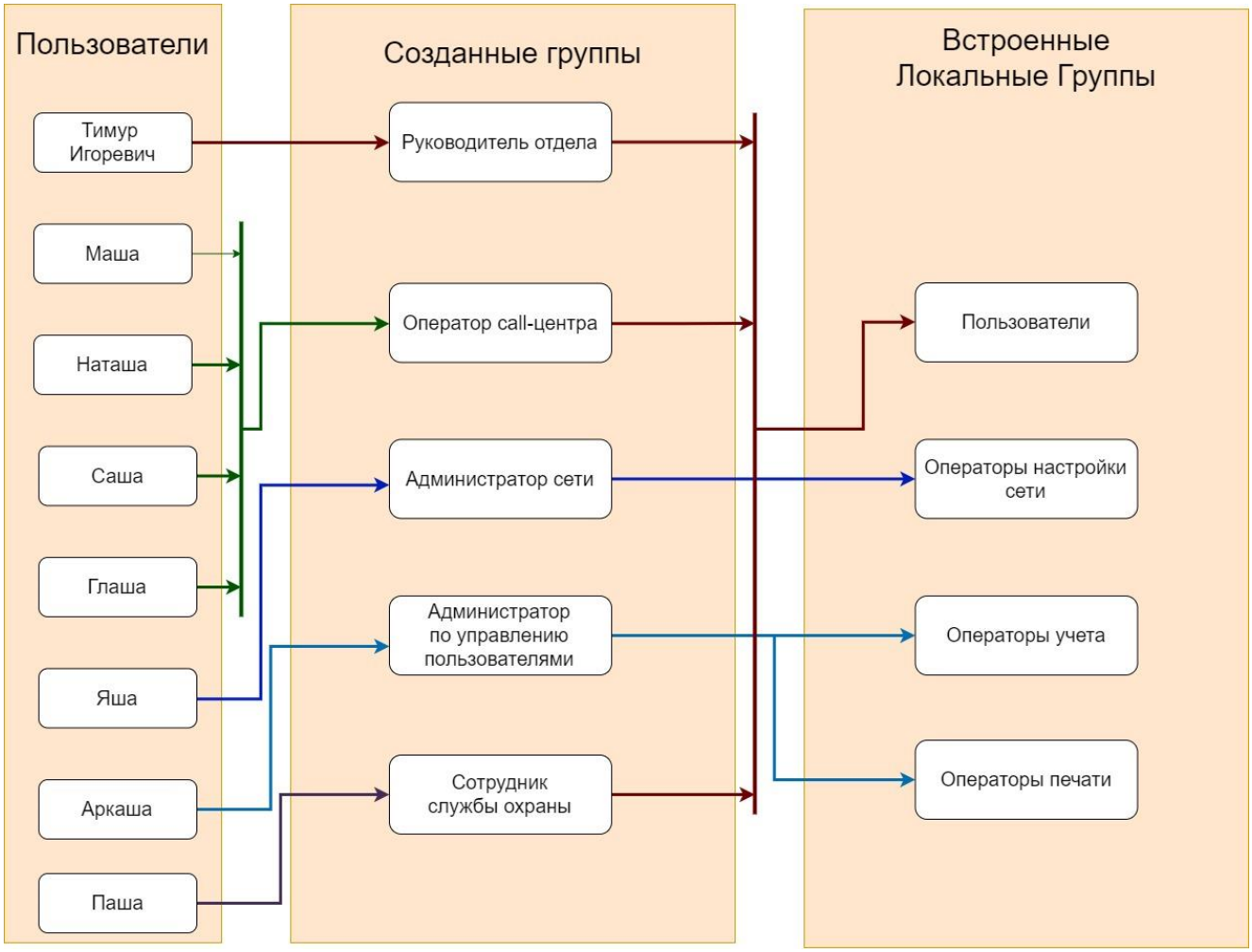

Рис 21.

- *Пользователи* - пользователи не имеют прав на изменение параметров системы и могут запускать большинство приложений.
- *Операторы настройки сети* - члены этой группы могут иметь некоторые административные права для управления настройкой сетевых параметров.
- *Операторы учета* - члены группы имеют права на администрирование учетных записей пользователей и групп.
- *Операторы печати* - члены группы имеют права на администрирование принтеров домена.

6.3. Создание учетных записей и групп

Чтобы создать нового пользователя, выбираем контейнер (Users) и в меню «Действия» в пункте «Создать» выбираем «Пользователь» (Рис 22).

Возникает окно создания нового пользователя, где предлагается указать следующие параметры:

- Имя
- Фамилия
- Инициалы
- Полное имя входа пользователя – доменное имя, состоящее из имени пользователя и dns-имени домена
- Имя входа пользователя (пред-Windows 2000) – NetBIOS-имя пользователя

Указав необходимую информацию нажимаем «Далее». Следующее окно – свойства пароля (Рис 23). Нужно указать пароль с дополнительными параметрами:

- Требование смены пароля при следующем входе в систему
- Запрет смены пароля пользователем
- Неограниченный срок действия пароля
- Отключение учётной записи

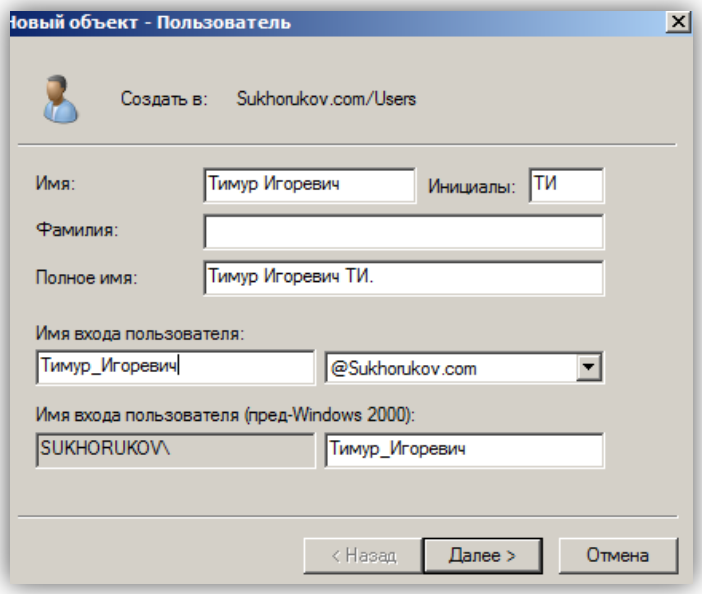

Рис 22.

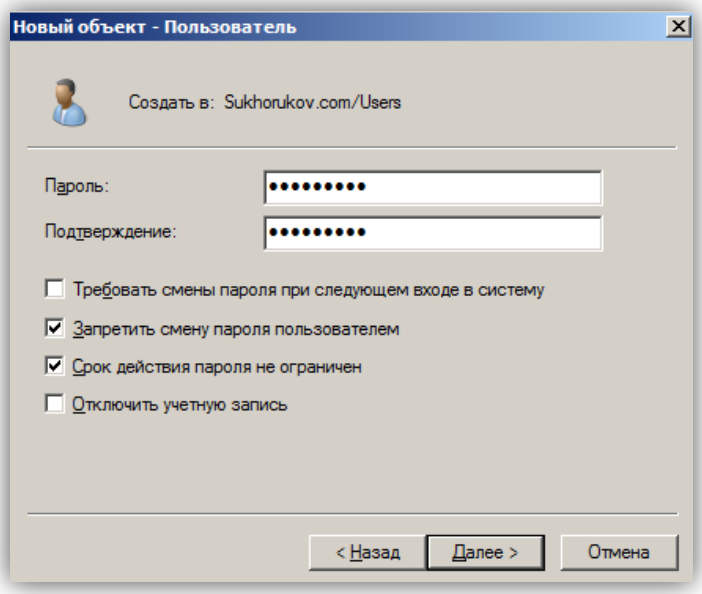

Рис 23.

Создадим оставшиеся учётные записи пользователей (Рис 24).

Для создания новой группы выделим контейнер «Users», в котором будем создавать группу и в меню «Действия» в пункте «Создать» выбираем «Группа» Открывается окно создания группы (Рис 25). Указываем следующие параметры:

- Имя группы: Руководитель отдела
- Область действия группы: Глобальная
- Тип группы: Группа безопасности

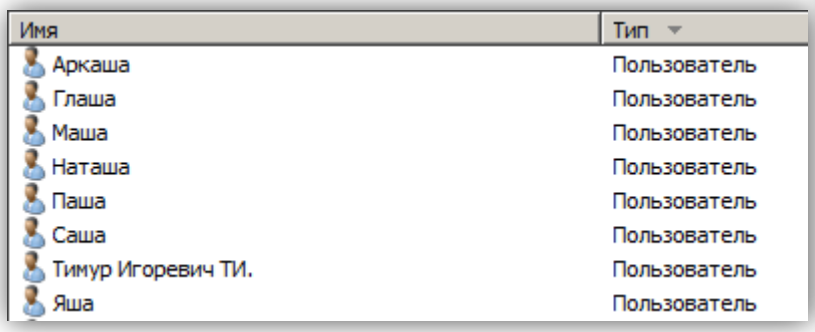

Рис 24.

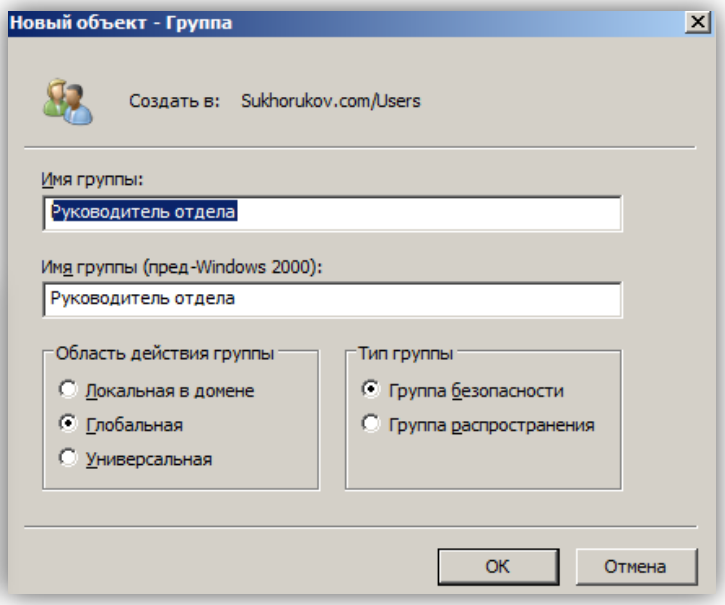

Рис 25.

Аналогично создадим остальные глобальные группы (Рис 26).

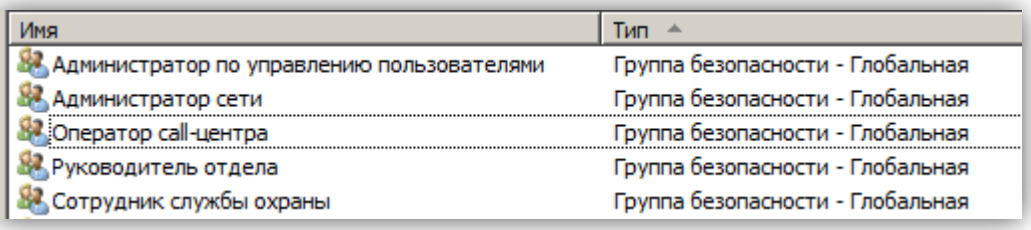

Рис 26.

Теперь включим пользователей в созданные глобальные группы, глобальные группы во встроенные локальные группы согласно плану. Для этого в свойствах группы выберем пункт «Члены группы» → «Добавить» (Рис 27 -28).

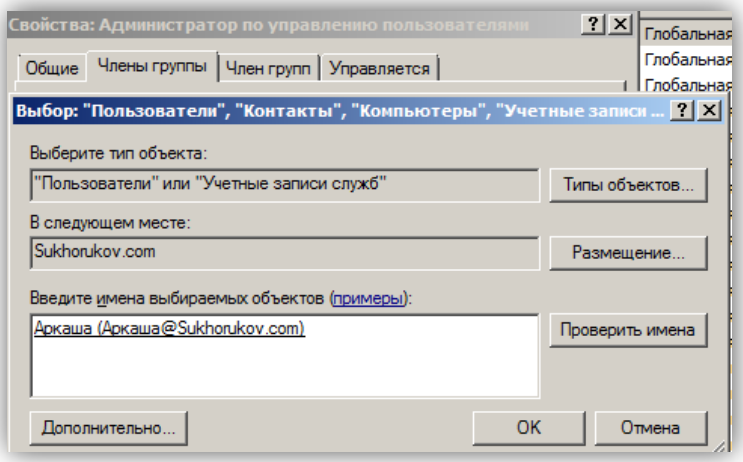

Рис 27.

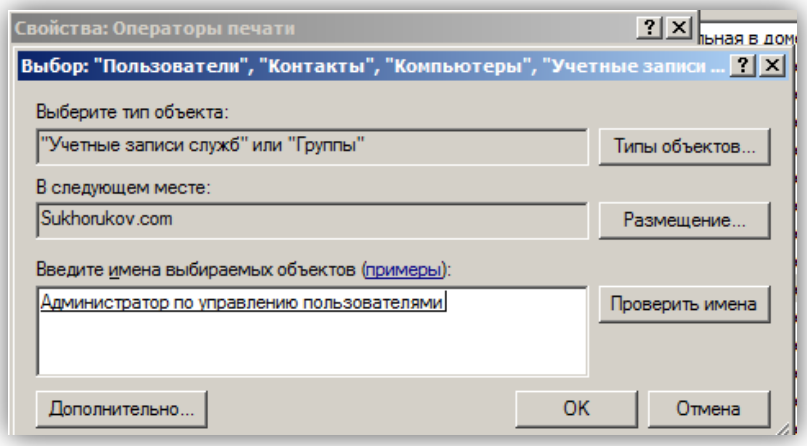

Рис 28.

6.4. Ограничение запуска программ

6.4.1. Использование прав пользователей

В качестве примера рассмотрим запрет участникам группы «Операторы call—центра» запуск приложения «Paint» с помощью Прав пользователей. Для этого в окне оснастки «Локальной политики безопасности» создадим политику «Создать политики ограниченного использования программ».

В результате создаются две вкладки: «Уровень безопасности» и «Дополнительные правила». В уровне безопасности создались три правила:

- Запрещено
- Обычный пользователь
- Неограниченный

причем по умолчанию установлен уровень «Неограниченный», эти три уровня определяют, что делать с программой в правиле – разрешать или запрещать ее выполнение, данную вкладку мы оставим без изменения.

Запрещать запуск программ, не относящихся к служебной деятельности сотрудников, будем во вкладке «Дополнительные правила». Первый и самый простой способ запретить запуск ПО – это запрет накладываемый на запуск по пути исполняемого файла. Однако пользователь может изменить имя файла, и он будет запускаться. Второй способ – создать правило для файла не по его имени и пути, а по хешу.

Создадим правило на основе хэш-функции файла, в окне обзор выбираем файл, в сведениях о файле отображается имя файла, название программы, издатель программы (Рис 29).

Теперь зададим необходимый уровень безопасности, и описание правила (Рис 30).

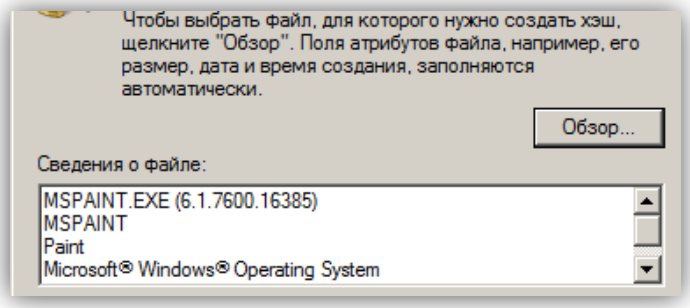

Рис 29.

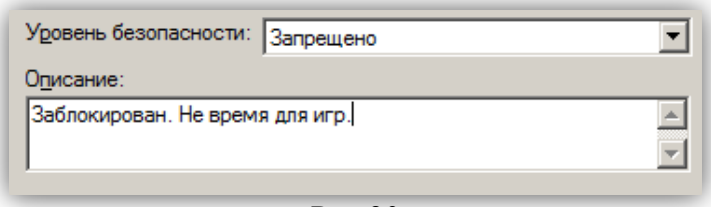

Рис 30.

Перезапустим компьютер для применения изменений, и войдем под учетной записью «Саша» и проверим ограничение (Рис 31).

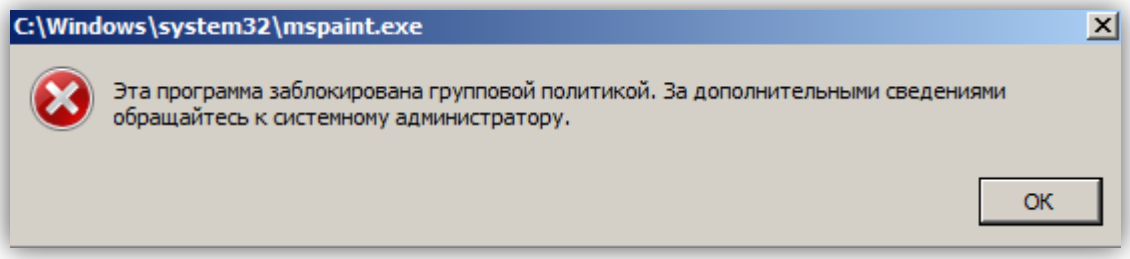

Рис 31.

Однако ограничения, накладываемые данным способом, действуют на всех пользователей компьютера. Поэтому удалим данные правило политики безопасности и используем разрешения для запрета запуска программы.

6.4.2. Использование разрешений

Поскольку программа «MS paint» находится в системном каталоге, то изменить разрешения доступа к ней не удастся (Рис 32). Поэтому войдём под учетной записью администратора, создадим ярлык на программу, изменим разрешения доступа к нему (Рис 33) и поместим ярлык на рабочий стол пользователя «Саша» (Рис 34). Далее войдем под учетной записью «Саша» и удостоверимся, что программа не запускается с помощью ярлыка.

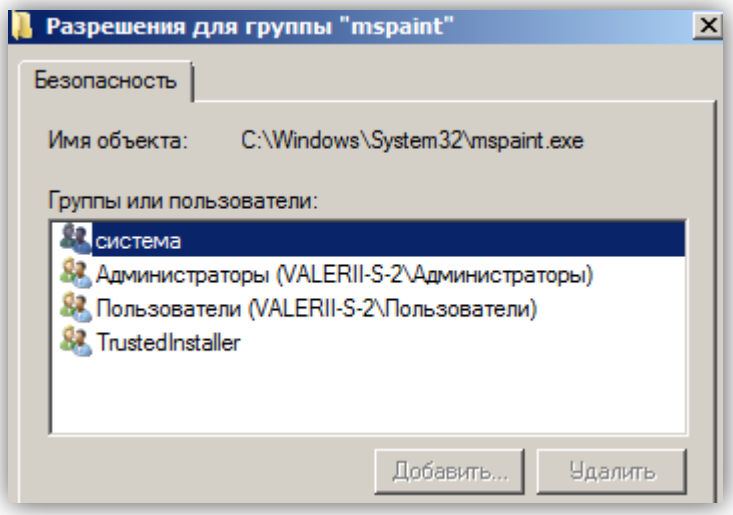

Рис 32.

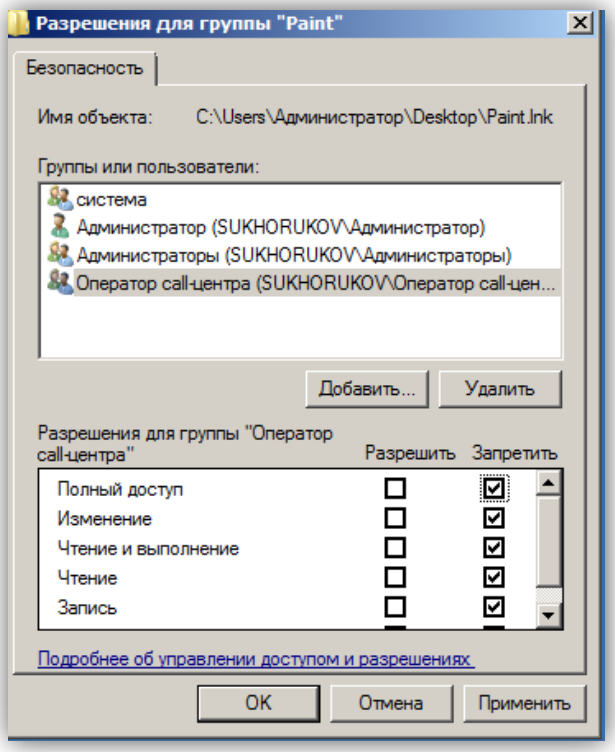

Рис 33.

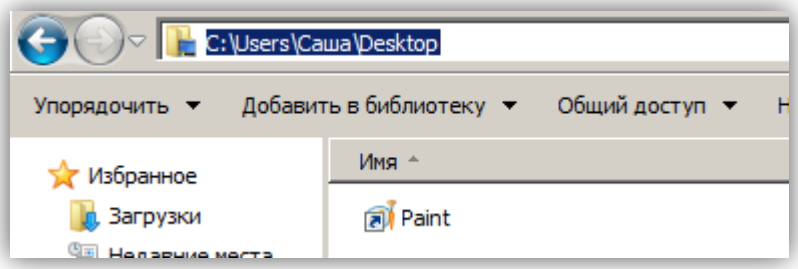

Рис 34.

6.5. Ограничение доступа к файлам и каталогам

В корне диска С создадим папку «Данные отдела». Разрешим доступ к ней группам «Оператор call-центра» и «Руководитель отдела».

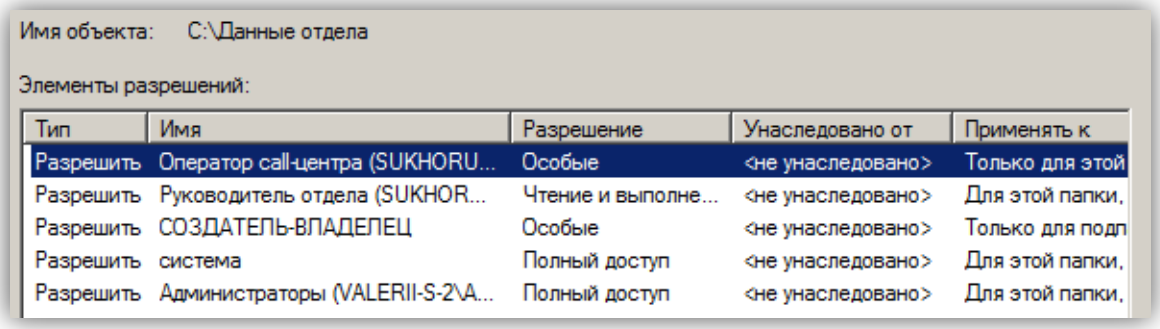

Рис 35.

Внутри создадим каталоги для каждого члена отдела с соответствующими правами (Рис 36), и общий каталог (Рис 37).

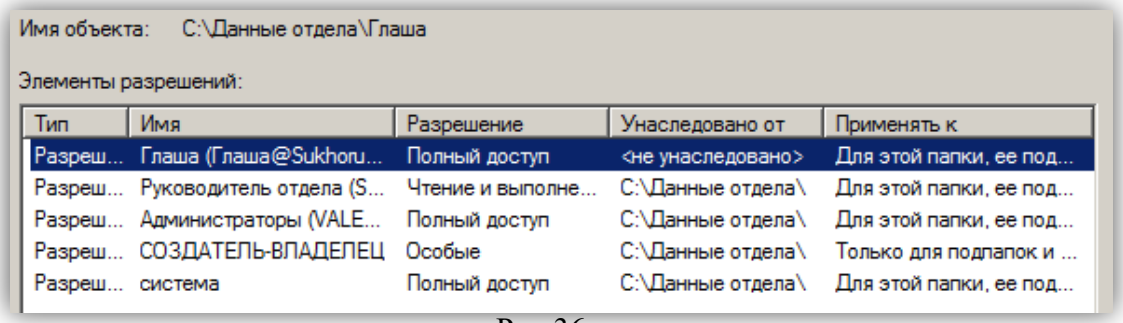

Рис 36.

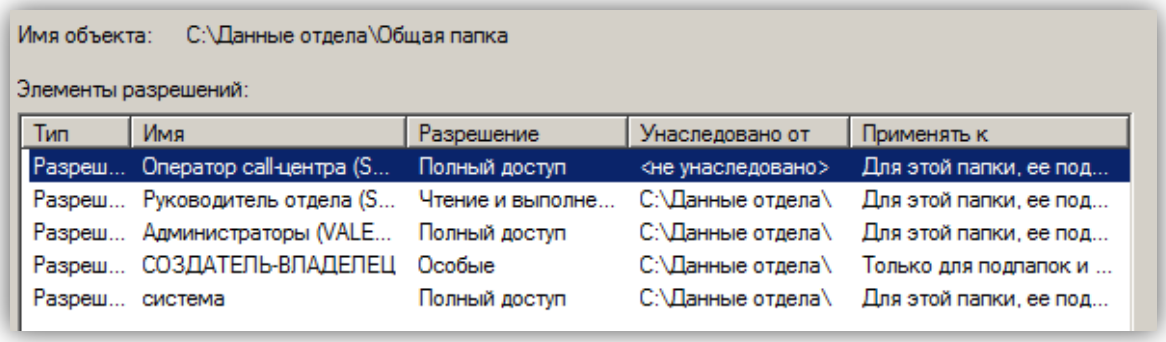

Рис 37.

Проверим выполнение разрешений с учетной записи Саша.

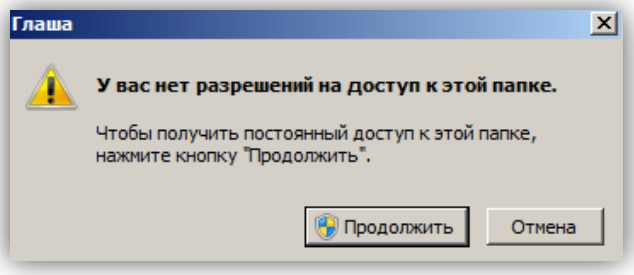

Рис 38.

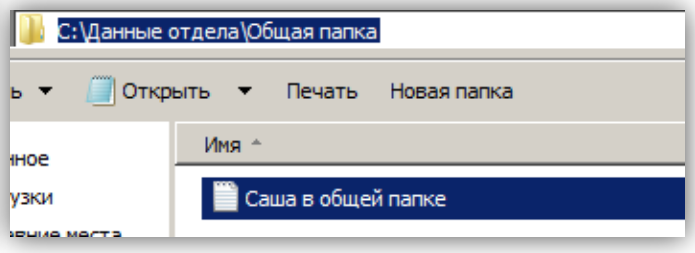

Рис 39.

Создадим текстовый файл «Журнал службы охраны» и предоставим разрешение на чтение – группе «Руководитель отдела» и специальные разрешения– группе «Сотрудник службы охраны» (Рис 40).

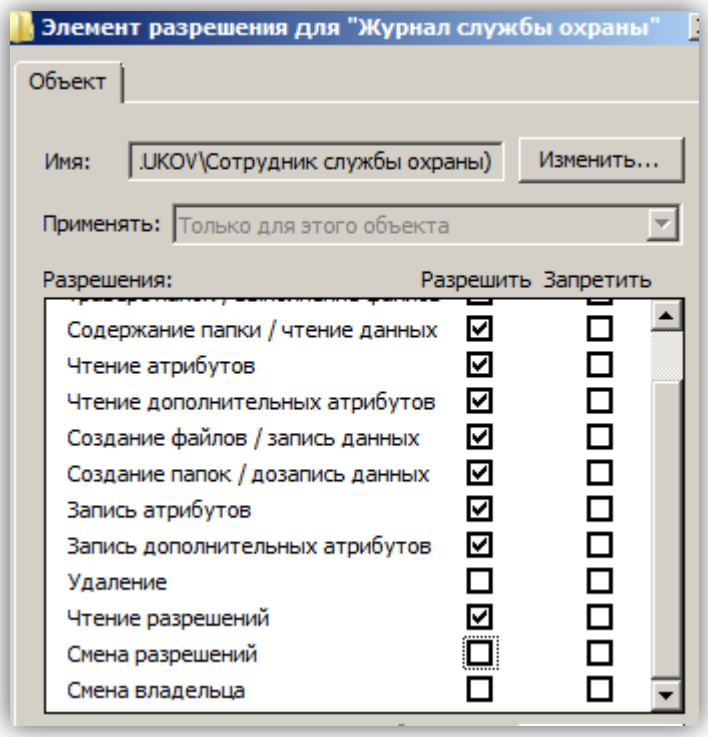

Рис 40.

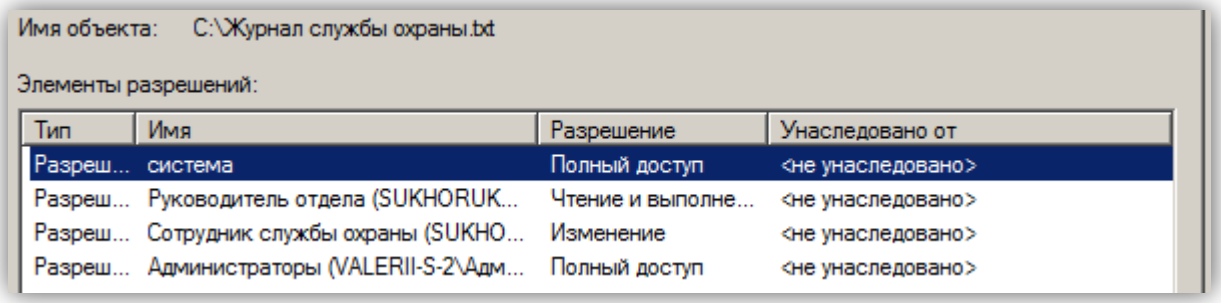

Рис 41.

7. Протокол Kerberos

Kerberos — сетевой протокол аутентификации, который предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними, причём в протоколе учтён тот факт, что начальный обмен информацией между клиентом и сервером происходит в незащищенной среде, а передаваемые пакеты могут быть перехвачены и модифицированы.

7.1. Процесс аутентификации пользователя с помощью доменной учетной записи

❖ Пользователь вводит пароль доменной учетной записи. Клиентская часть Kerberos (C) вычисляет хэш от введенного пароля и использует его как ключ для шифрования секретной части аутентификатора. Клиент посылает серверу аутентификации запрос AS_REQ с аутентификатором, в котором содержатся идентификатор клиента ID(C), идентификатор сервера выдачи разрешений ID(TGS), а также информация INFO(C), предназначенная для идентификации конкретного запроса клиента: время, сетевой адрес и т.п.

❖ Служба KDC ищет пользователя по его UPN в AD, выявляет мастер ключ пользователя, который основан на пароле пользователя и пытается расшифровывать аутентификатор хэшем хранимого пароля. Если не получается – пароль не верен и дается отказ в аутентификации.

Результат успешной расшифровки является подтверждением правильности пароля и успешной аутентификации. Извлекаются сведения об учетной записи и временные метки и выполняется обработка по протоколу. Разница во времени отправки запроса и текущего времени на контроллере домена не должно превышать определенного значения, установленного политикой протокола Kerberos.

❖ KDC создает два объекта:

- сеансовый ключ Клиент/TGS, посредством которого будет обеспечиваться шифрование данных при обмене между клиентом и службой TGS,
- билет на получение TGT: идентификатор и сетевой адрес клиента, метку времени KDC, период действия билета и сеансовый ключ Клиент/TGS. TGT шифруется с использованием секретного ключа службы TGS. Служба KDC зашифровывает аутентификатор пользователя и ключ сессии с помощью ключа клиента. После этого ответ AS_REP отправляется клиенту.

❖ Клиент получает AS_REP, расшифровывает его тем же правильным хэшем и сохраняет в своем локальном кэше билет TGT и сеансовый ключ Клиент/TGS.

❖ Клиент обращается к службе TGS с запросом TGS_REQ, в котором есть имя сервиса в формате SPN, зарегистрированное в AD, билет TGT и аутентификатор, зашифрованный ключом Клиент/TGS.

❖ TGS расшифровывает TGT своим ключом, извлекает сеансовый ключ Клиент/TGS, расшифровывает им аутентификатор. TGS формирует билет сервиса, включающий ID клиента, сетевой адрес, метку времени, время жизни, сеансовый ключ Клиент/Сервис. Посылает клиенту (TGS_REP) сеансовый ключ Клиент/Сервис, ID сервиса и время жизни билета.

❖ Клиент сохраняет сеансовый билет сервиса в своем кэше для последующей работы с сервисом.

❖ Клиент обращается за услугой к сервису ресурса, посылая сообщение, содержащее:

- зашифрованный билет сервиса, полученный ранее
- новый аутентификатор, зашифрованный сеансовым ключом Клиент/Сервис, и включающий ID клиента и метку времени.

Сервер, расшифровав своим ключом сеансовый билет, сравнивает сеансовый ключ в билете и в аутентификаторе. Факт совпадения говорит о подлинности клиента.

❖ Kerberos позволяет сделать аутентификацию взаимной и выполнить подтверждение подлинности сервера на клиенте. Для этого сервер модифицирует метку времени, полученную от клиента (+1). Клиент расшифровывает подтверждение, используя сессионный ключ клиент/сервис и проверяет, действительно ли метка времени корректно обновлена. Если это так, то клиент может доверять серверу и может начать посылать запросы на сервер.

❖ Сервер предоставляет клиенту требуемый сервис в соответствии с авторизацией прав доступа к ресурсу.

7.2. Использование команды klist

Команда возвращает следующие данные:

Клиент – имя области (домена), где сгенерирован билет. Служба KDC может создавать билеты только для серверов собственной области, поэтому здесь, по существу, указывается имя области, где расположен сервер.

Сервер – основное имя службы, зарегистрированное в AD, с которой клиент хочет установить соединение.

Тип шифрования билетов (KerbTicket) – тип шифрования, используемый для шифрования билета Kerberos.

Флаг билета – флаги свойств билета. Набор флагов Flags являются поименованными битовыми признаками свойств и возможностей билета.

Время начала и окончания – интервал действия билета.

Время продления– наибольшее значение поля время окончания (с возможностью обновления ключа), которое может быть задано с помощью флага RENEWABLE (поле необязательное).

Тип ключа сеанса – сеансовый ключ, используемый клиентом в сеансе со службой сервера.

Используем команду на команду на компьютере Valerii-S-2 и проанализируем полученные данные.

- Билет №0 – получен от сервера krbtgt/SUKHORUKOV.COM. Флаги билета:

FORWARDABLE - указывает, что на основании данного билета TGT служба выдачи билетов может генерировать новый билет TGT с другим сетевым адресом.

FORWARDED - указывает на то, что данный билет TGT был переадресован или генерирован на основе другого билета TGT, прошедшего переадресацию.

RENEWABLE - задает время жизни билета, разрешая периодическое обновление службой KDC билетов с повышенным сроком действия.

Время получения билета 11/5/2022 13:19:40.

Назначение билета -

- Билет №1 – получен от сервера krbtgt/SUKHORUKOV.COM. Флаги билета:

FORWARDABLE.

RENEWABLE.

INITIAL – указывает, что данный билет является билетом выдачи билетов.

Время получения билета 11/5/2022 13:17:20.

Назначение билета - Этот билет выдается KDC после успешной аутентификации клиента. TGT зашифрован и содержит разрешения на то, к каким службам может получить доступ клиент, как долго предоставляется доступ, а также ключ сеанса, используемый для связи с клиентом.

- Билет №2 – получен от сервера cifs/Valerii-S-1.SUKHORUKOV.COM. Флаги билета:

FORWARDABLE.

RENEWABLE.

OK_AS_DELEFATE – означает, что учетной записи службы доверяется делегирование.

Время получения билета 11/5/2022 13:19:40.

Назначение билета – связан с работой файловой системы по сети. Клиент получает этот билет и будет предъявлять его, если обращается к другим узлам.

- Билет №3 – получен от сервера ldap/Valerii-S-1.SUKHORUKOV.COM. Флаги билета:

FORWARDABLE.

RENEWABLE.

OK_AS_DELEFATE.

Время получения билета 11/5/2022 13:19:40.

Назначение билета –обращение к БД Active Directory.

7.3. Очистка кэша билетов и оценка динамики получения билетов

Выполним очистку кэша через команду klist purge и убедимся, что кэш пустой.

```
C:\Users\Администратор.SUKHORUKOV>klist purge

Текущим идентификатором входа является 0:0x14b18
        Удаление всех билетов:
        Билеты очищены.

C:\Users\Администратор.SUKHORUKOV>klist

Текущим идентификатором входа является 0:0x14b18

Кэшированные билеты: (0)
```

Рис 42.

Теперь при взаимодействии по сети клиент сначала должен пройти аутентификацию, взаимодействовать с контроллером, получить новый билет и уже потом его использовать для обращения к серверу.

Выполним повторную регистрацию в системе и проанализируем полученные билеты (Рис 43).

```
C:\Users\Администратор.SUKHORUKOV>klist

Текущим идентификатором входа является 0:0x14b18

Кэшированные билеты: (2)

#0>     Клиент: Администратор @ SUKHORUKOV.COM
        Сервер: krbtgt/SUKHORUKOV.COM @ SUKHORUKOV.COM
        Тип шифрования KerbTicket: AES-256-CTS-HMAC-SHA1-96
        флаги билета 0x40e00000 -> forwardable renewable initial pre_authent
        Время начала: 11/6/2022 19:26:07 (локально)
        Время окончания:   11/7/2022 5:26:07 (локально)
        Время продления: 11/13/2022 19:26:07 (локально)
        Тип ключа сеанса: AES-256-CTS-HMAC-SHA1-96


#1>     Клиент: Администратор @ SUKHORUKOV.COM
        Сервер: LDAP/Valerii-S-1.Sukhorukov.com/Sukhorukov.com @ SUKHORUKOV.COM
        Тип шифрования KerbTicket: AES-256-CTS-HMAC-SHA1-96
        флаги билета 0x40a40000 -> forwardable renewable pre_authent ok_as_delegate
        Время начала: 11/6/2022 19:26:08 (локально)
        Время окончания:   11/7/2022 5:26:07 (локально)
        Время продления: 11/13/2022 19:26:07 (локально)
        Тип ключа сеанса: AES-256-CTS-HMAC-SHA1-96


C:\Users\Администратор.SUKHORUKOV>_
```

Рис 43.

Был получен билет аутентификации от сервера krbtgt/SUKHORUKOV.COM, после него был получен билет для доступа к базе данных Active Directory. Через некоторое время был получен билет для доступе к службу cifs на контроллере домена (Рис 44).

```
Клиент: Администратор @ SUKHORUKOV.COM
Сервер: cifs/valerii-s-1.sukhorukov.com @ SUKHORUKOV.COM
Тип шифрования KerbTicket: AES-256-CTS-HMAC-SHA1-96
флаги билета 0x40a40000 -> forwardable renewable pre_authent ok_as_delegate
Время начала: 11/6/2022 20:29:59 (локально)
Время окончания:   11/7/2022 6:29:58 (локально)
Время продления: 11/13/2022 20:29:58 (локально)
Тип ключа сеанса: AES-256-CTS-HMAC-SHA1-96
```

Рис 44.

7.4. Временные метки

Билет Kerberos содержит временные метки для того, чтобы билеты не могли быть перехвачены и использованы позже. Если часы клиента, сервера или KDC не синхронизированы, протокол не будет функционировать корректно. Поэтому синхронизация времени на компьютерах, взаимодействующих между собой с использованием протокола Kerberos, является необходимой и важной задачей.

В оснастке «Локальная политика безопасности» можно установить максимальную погрешность синхронизации часов компьютера. По умолчанию этот параметр равен 5 минутам.

Если изменить время на контроллере домена на более 5 минут, аутентификацию по Kerberos не будет проходить, а значит невозможен вход в систему.

Но здесь срабатывает политика безопасности, связанная с локальным кэшированием предыдущих входов (в случае отсутствия доступа к контроллеру домена). Если данная политика отключена и нет доступа к контроллеру домена, то войти не получится.

Вывод: Клиент-серверное взаимодействие в домене может обеспечиваться безопасным образом, если клиент и сервер прошли взаимную аутентификацию по Kerberos. При этом подтверждается не только вход самого пользователя, но и то, что клиент, сервер, и служба – легитимные. Тогда клиент получает билеты, потом, при обращении к службе на другом хосте, эти билеты предъявляет и хранит в своем кэше.