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.

Студент:

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

группа 19-ВМ

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

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

Нижний Новгород 2022

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

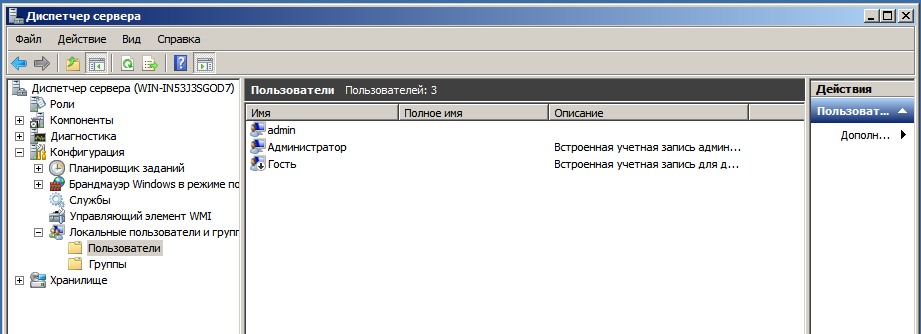
1. Локальные учетные записи компьютера
   1. Ознакомиться с составом встроенных локальных учетных записей и групп компьютера

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.



### 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» («POLY\_SLADKIY\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.

### 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 т.д.
* 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.

**«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*».

**«Гость»**

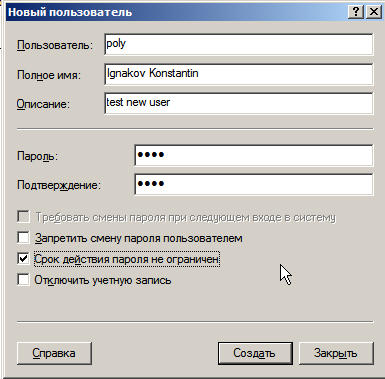
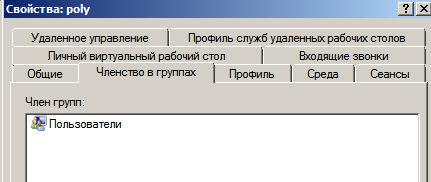
Гостевая учетная запись — это локальная учетная запись по умолчанию, которая имеет ограниченный доступ к компьютеру и по умолчанию отключена. По умолчанию пароль гостевой учетной записи остается пустым. Пустой пароль позволяет получить доступ к гостевой учетной записи, не требуя ввода пароля пользователем.

Гостевая учетная запись позволяет случайным или однократным пользователям, у которых нет отдельной учетной записи на компьютере, входить на локальный сервер или домен с ограниченными правами и разрешениями. Гостевая учетная запись может быть включена, а пароль можно настроить при необходимости, но только участник группы администраторов в домене.

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.

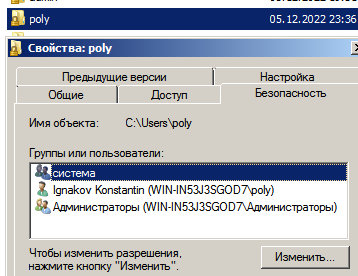
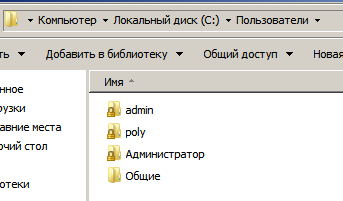
1. Новая локальная учетная запись
   1. Создание локальной учетной записи

С помощью утилиты «Локальные пользователи и группы» создадим новую учетную запить. Новый пользователь принадлежит к «*Пользователи*», это можно посмотреть в «Свойства» - «Членство в группах».

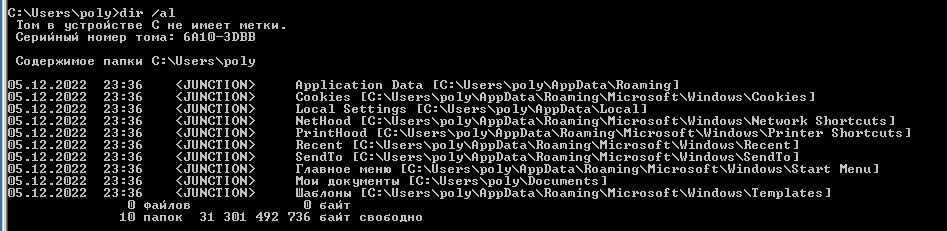
 

### Свойства профиля локальной учетной записи

При первом входе под новым пользователем в систему создается локальный профиль пользователя, который состоит из домашнего каталога пользователя и настроек реестра ntuser.dat. Из содержимого каталога «Default» копируются в каталог нового пользователя «C:\Users\<new\_user>». «Default» - каталог, который представляет профиль по умолчанию. Так же на новый каталог устанавливаются ограничения, доступ к нему имеют сам пользователь, администратор и система.

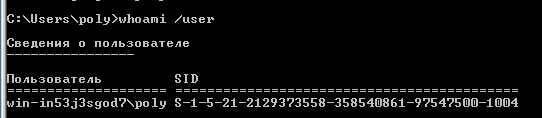


Каталог пользователя содержит директории, файлы реестра (ntuser.dat, ntuser.dat.log) и Junction Points для совместимости с более старшими версиями Windows. Для того чтобы «увидеть» Junction Points можно настроить отображение скрытых файлов в каталоге, или использовать команду dir /al.

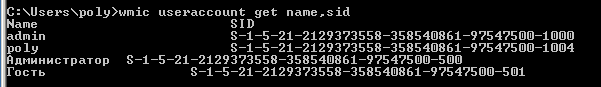


### SID новой локальной учетной записи

У нового пользователя так же существует его уникальный SID номер, чтобы получить SID текущего пользователя, необходимо в терминале ввести команду «whoami /user».



Чтобы получить SID всех пользователей выполняется команда «wmic useraccount get user,sid»



**Обозначения:**

* 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.

1. 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.

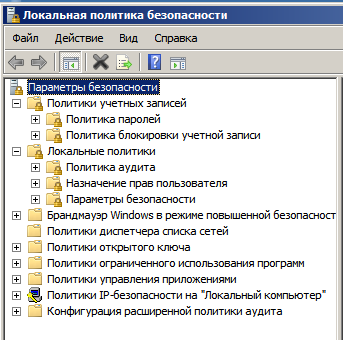
Если политика локального компьютера определяется более чем одним источником, приоритет при разрешении конфликтов политик имеют представленные далее источники в следующем порядке:

* 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.

### Структура компонентов локальной политики безопасности

Рассмотрим структуру компонентов 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.

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

Подсистема контроля доступа Windows, которая определяет пользователей, имеющих доступ к тем или иным ресурсам, основана на концепциях разрешений (*permissions*) 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.

Привилегии пользователей преобладают над разрешениями.

### 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 |  |  |  |  | + |  |  |

**Анализ таблицы:**

*Администраторы* – согласно описанию, обладает практически неограниченными правами и может выполнять любые действия над системой.

*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».

*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.

*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).

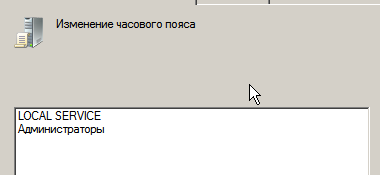
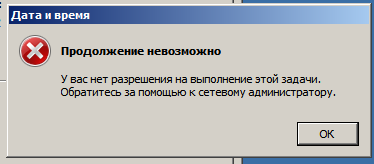
*Пользователи* – разрешены базовые операции с системой – вход в систему, удалённый доступ, просмотр и редактирование несистемных файлов.

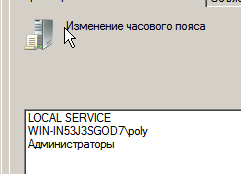
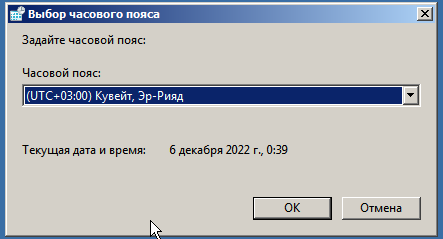
*Прошедшие проверку* – включает в себя всех пользователей, чья подлинность была подтверждена при входе в систему, в них входят как локальные учетные записи, так и учетные записи доверенных доменов (кроме учетных записей гостя, LOCAL\_SERVICE, NETWORK\_SERVICE и некоторых других встроенных учетных записей).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

*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 се-ти», и «Обхода перекрёстной проверки».

### Изменение прав по отношению к созданному пользователю.

Чтобы продемонстрировать работу службы управления правами пользователь изменим права в отношении нового пользователя, например, пользователь не мог изменять часовой пояс, для начала проверим это, далее изменим права от имени Администратора и снова зайдем под новым пользователем, чтобы удостоверится, что права появились.

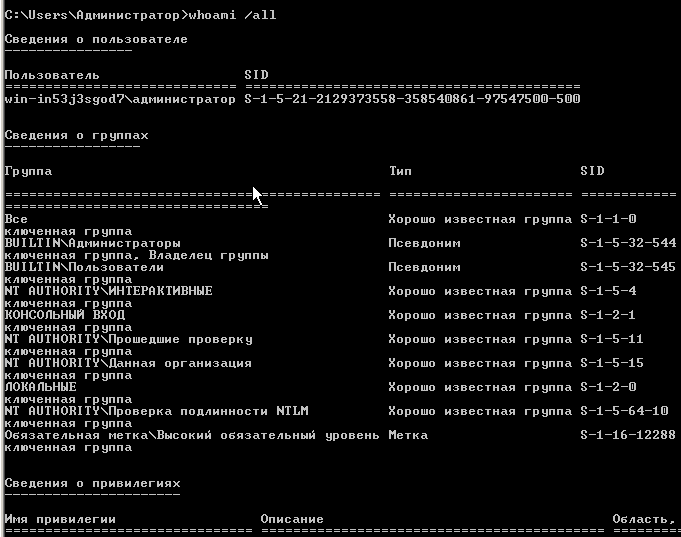
 

Стоит обратить внимание на то, что новые права пользователя заработают только после завершения сеанса и повторном входе в систему.

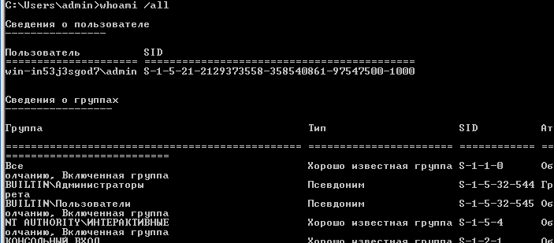
### Использование утилиты whoami

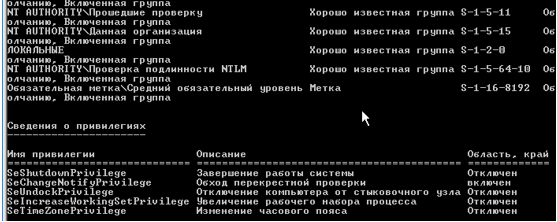
Получим с помощью команды whoami /all необходимые данные об учетных записях: SID, вхождение в группы и права.

**Администратор:**

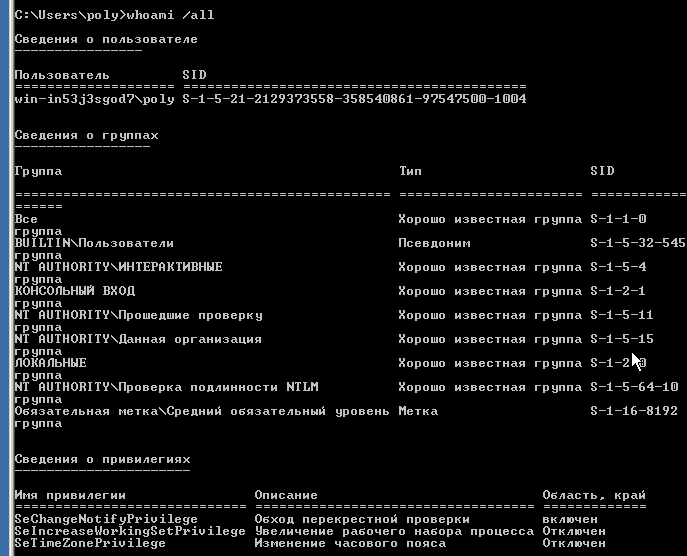


**admin** – пользователь создан во время установки образа Windows Server 2008 R2 на виртуальных машинах с помощью VMware Player:





**poly** – новый пользователь в системе:



* 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 совпадает, у доменной учетной записи отличается.
* Третья часть - относительный идентификатор безопасности объекта (RID). Начинается с 1000 для создаваемых учетных записей, у «Администратора» - 500.

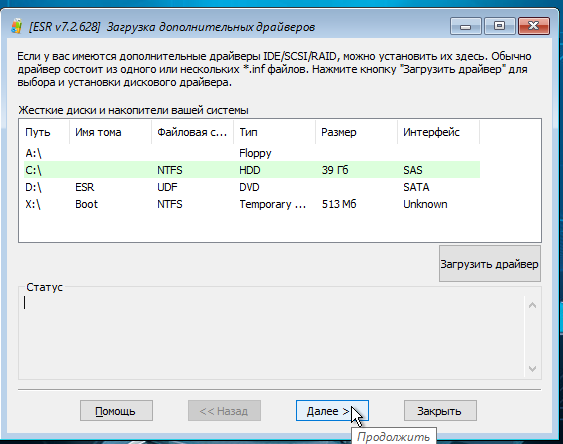
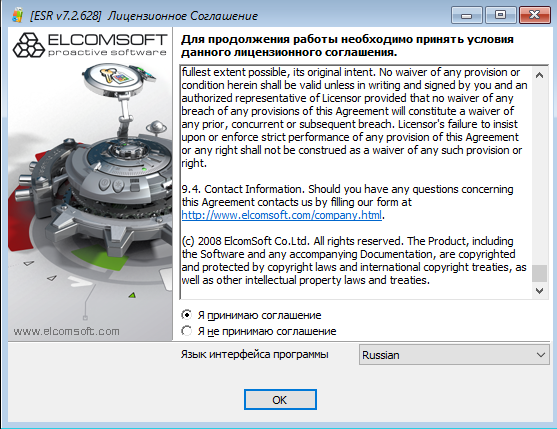
1. Elcomsoft System Recover

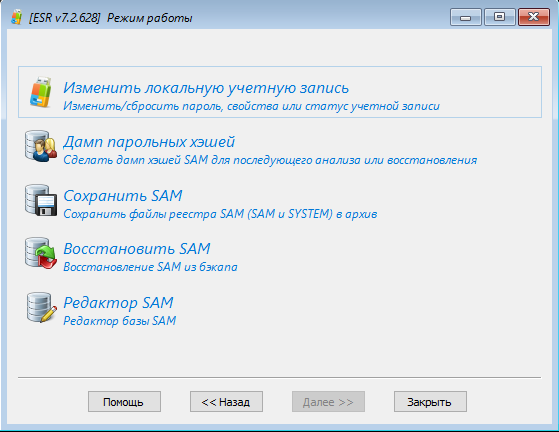
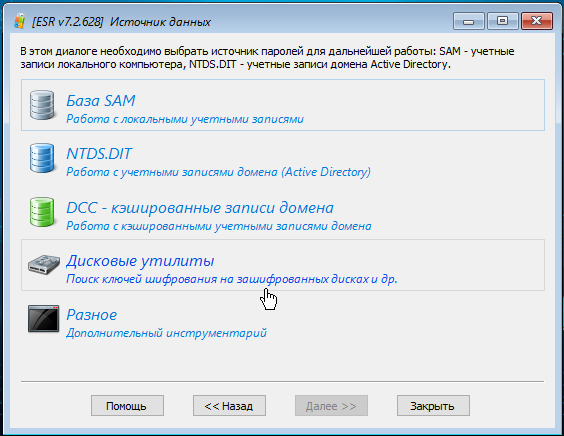
*Elcomsoft System Recover* – программа для восстановления доступа к учетным записям Windows, как к локальным, так и к сетевым.

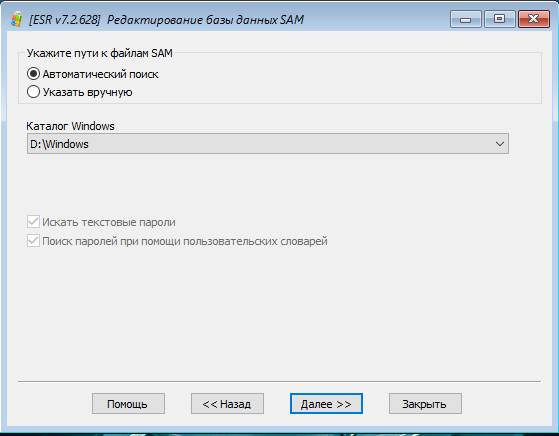
Данная программа работает с локальными учётными записями (SAM), а также с учётными записями Active Directory.

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

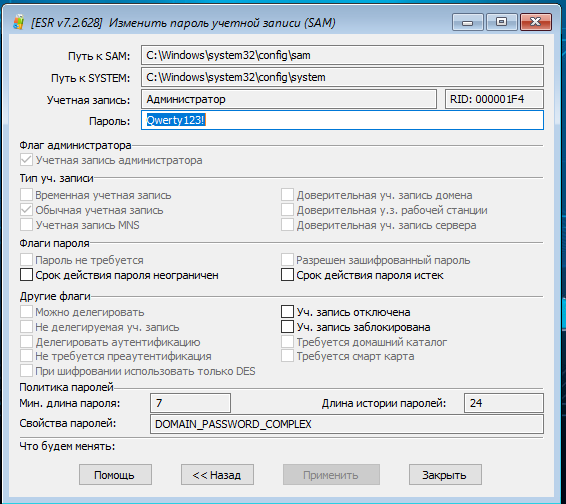
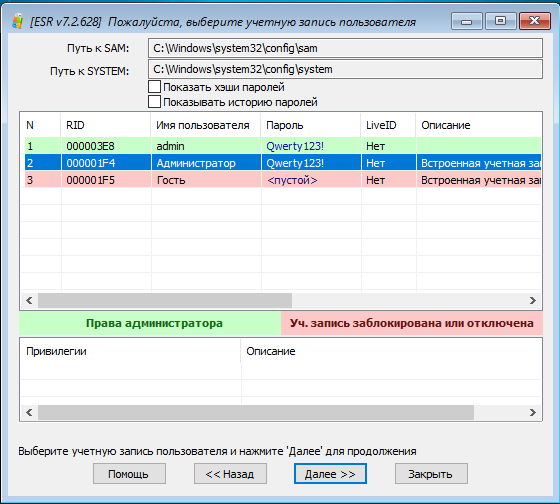






Данные об учётных записях, собранные программой:

* 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.

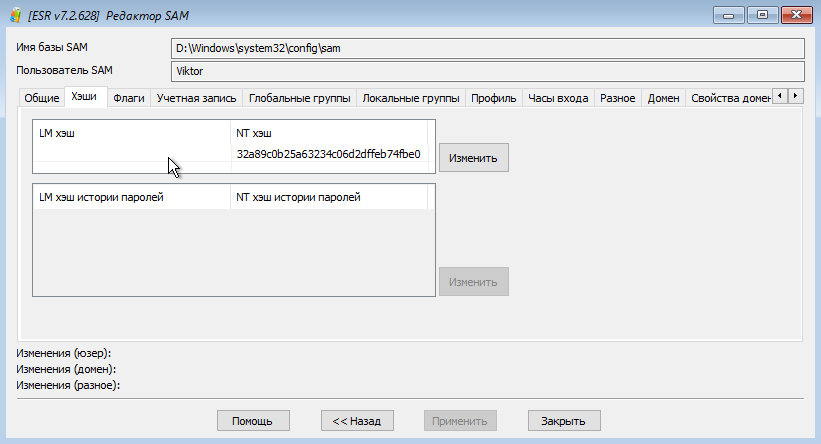


Выберем пользователя, чтобы получить больше сведений

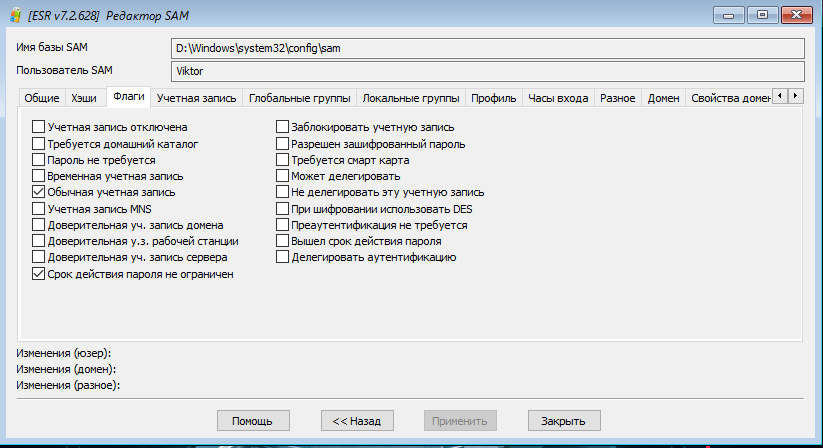
На вкладке «Общее» можно изменить имя пользователя, полное имя, комментарий администратора, RID пользователя.

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

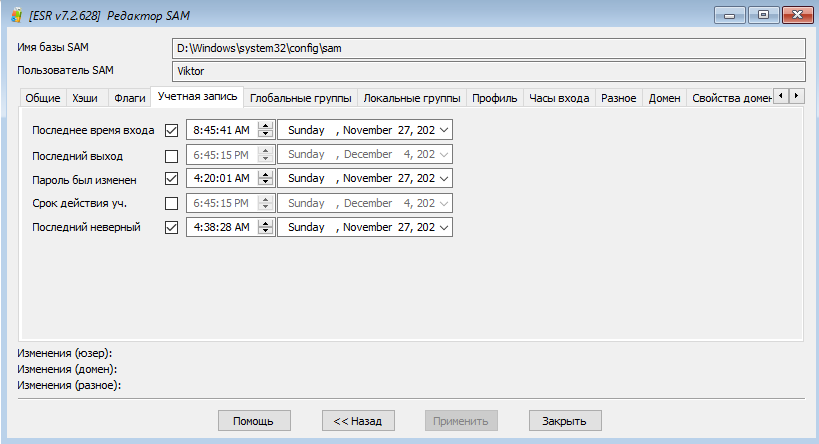
* При применении LM-хэширования длина пароля ограничена 14 символами. Самым большим недостатком алгоритма получения LM-хэша является разделение пароля на две части, каждая из которых состоит из семи символов. Если вводимый пользователем пароль менее 14 символов, то при преобразовании к нему добавляются 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.



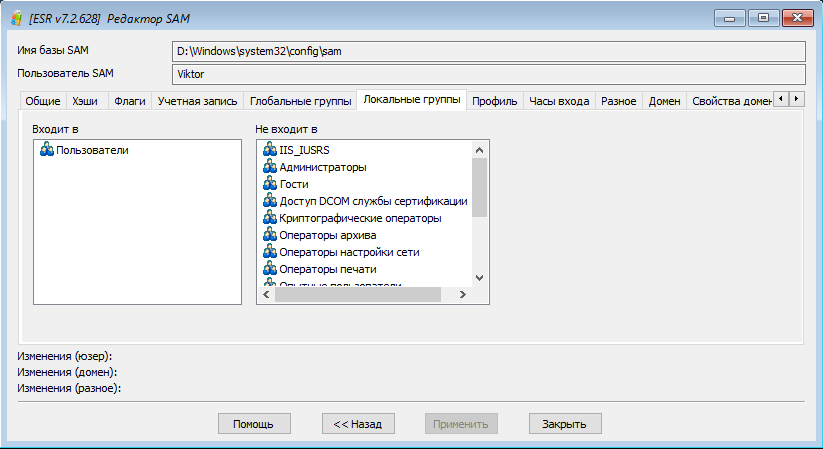
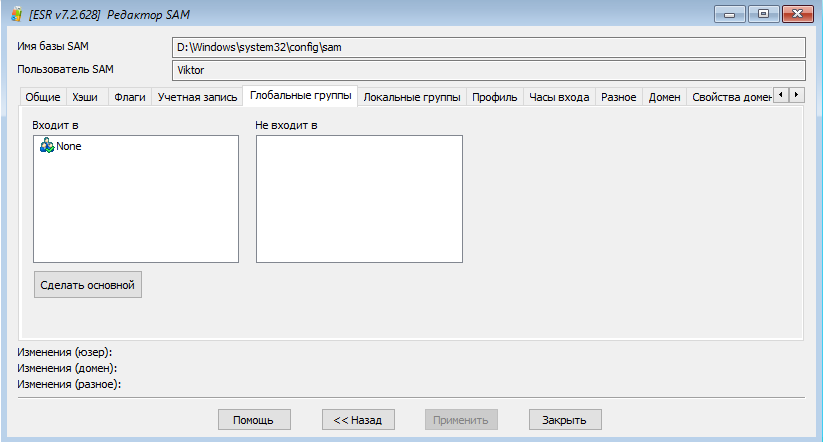
На вкладке «Флаги» можно изменить различные свойства учетной записи: отключить, отменить обязательный пароль и другие.



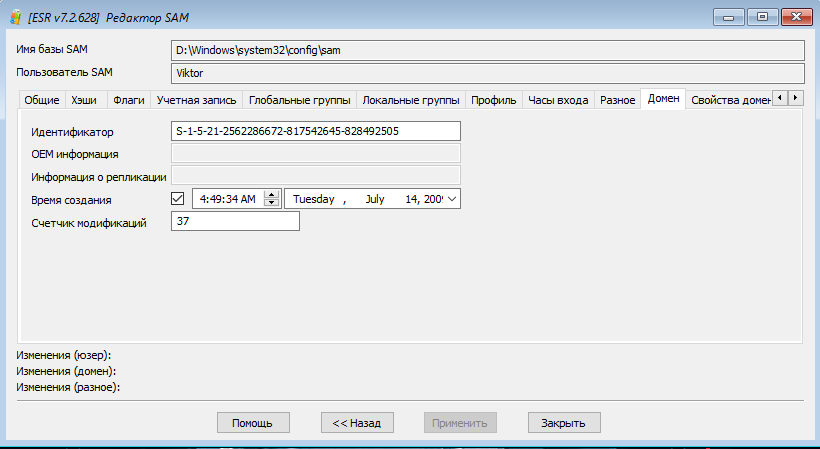
«Учетная запись» отображает данные последнего входа и выхода, а также время изменения пароля.



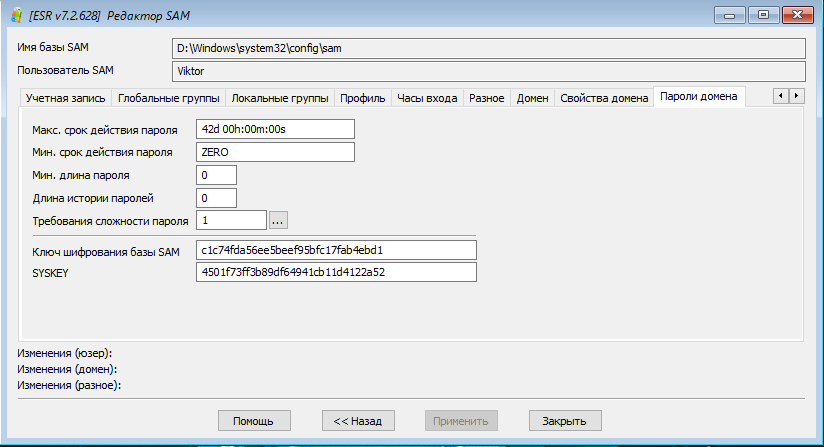
«Глобальные группы» и «Локальные группы» предоставляют возможность внесения или удаления учетной записи из той или иной группы.



На вкладке «Домен» можно увидеть или изменить SID домена.

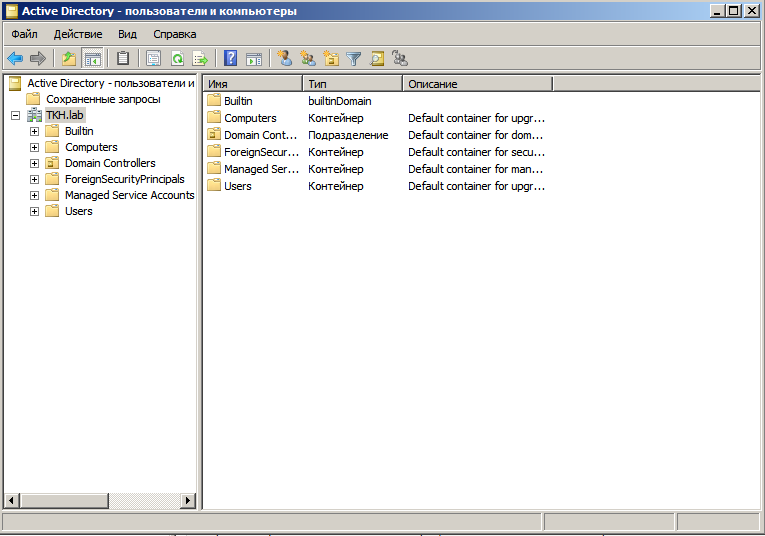


«Пароли домена» предоставляет информацию о сроках действия пароля, его длине и ключ шифрования БД SAM



1. Доменные учетные записи и группы

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.

Структура учетных записей и групп (без групп, не имеющих привязок):

