



# Operating Systems & Security

Часть 2

2024

Антонов ДМ





# ПОЛЕЗНЫЕ ССЫЛКИ

25 октября 2022 года был выпущен новый стандарт системы управления информационной безопасностью ISO 27001. ISO/IEC 27001 является одним из самых известных в мире стандартов управления информационной безопасностью, поскольку он перешёл из сферы кибербезопасности в мир бизнеса.

<https://www.isms.online/iso-27001/>

Пример реализации

<https://www.kaspersky.ru/blog/iso-27001-certification/26358/>

Решения Positive Technologies защиты бизнеса в различных отраслях

<https://www.ptsecurity.com/ru-ru/products/>

Карта компетенций специалиста по ИБ

<https://static.ptsecurity.com/events/matrica-kompetenciy.pdf>

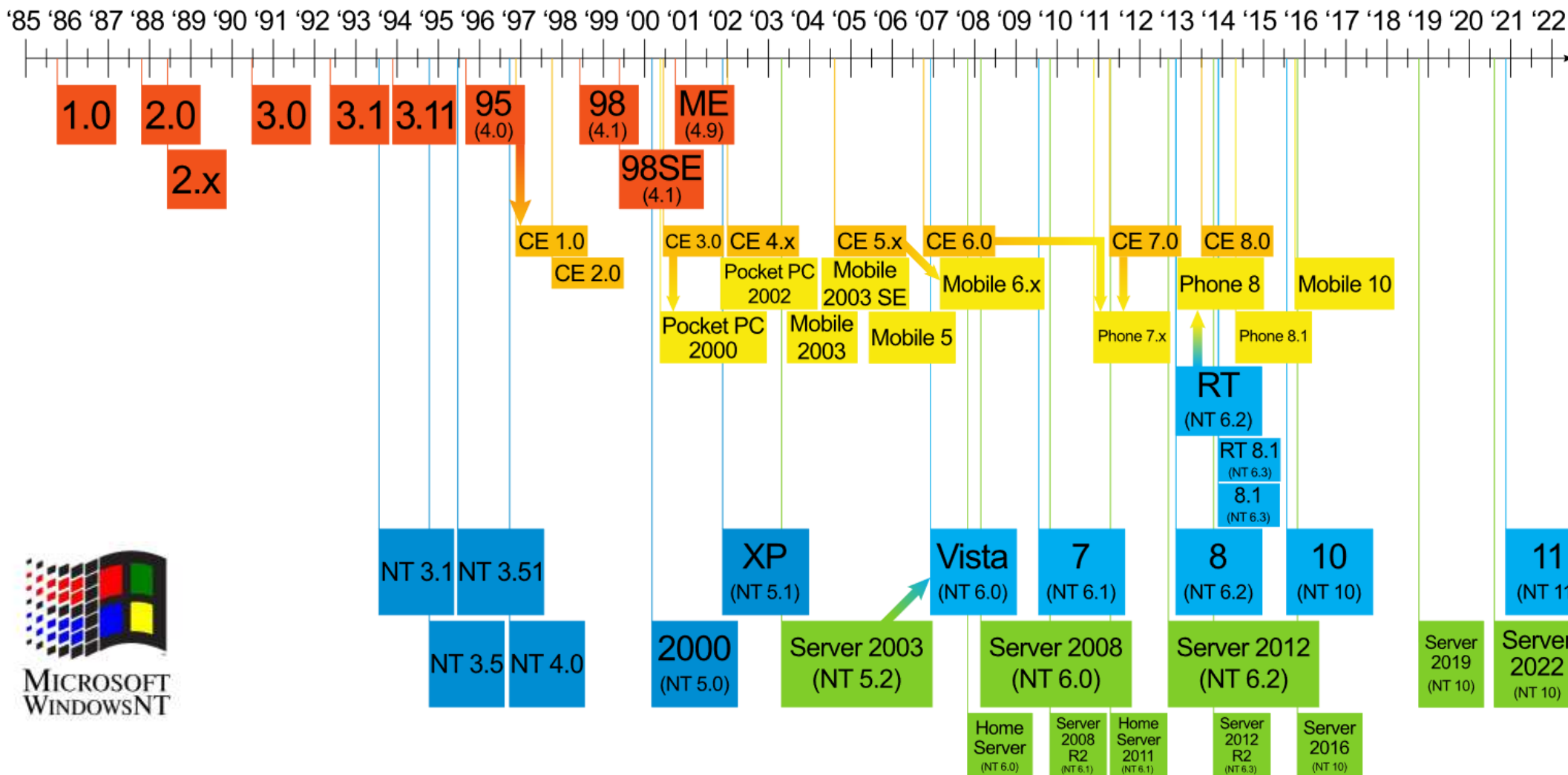


## Часть 2.

1. Основы Windows
2. Модель доступа Windows
3. Инструменты Windows
4. Протоколы аутентификации
5. Локальная политика безопасности



# ИСТОРИЯ ОПЕРАЦИОННЫХ СИСТЕМ WINDOWS





# СУБЪЕКТЫ И ОБЪЕКТЫ

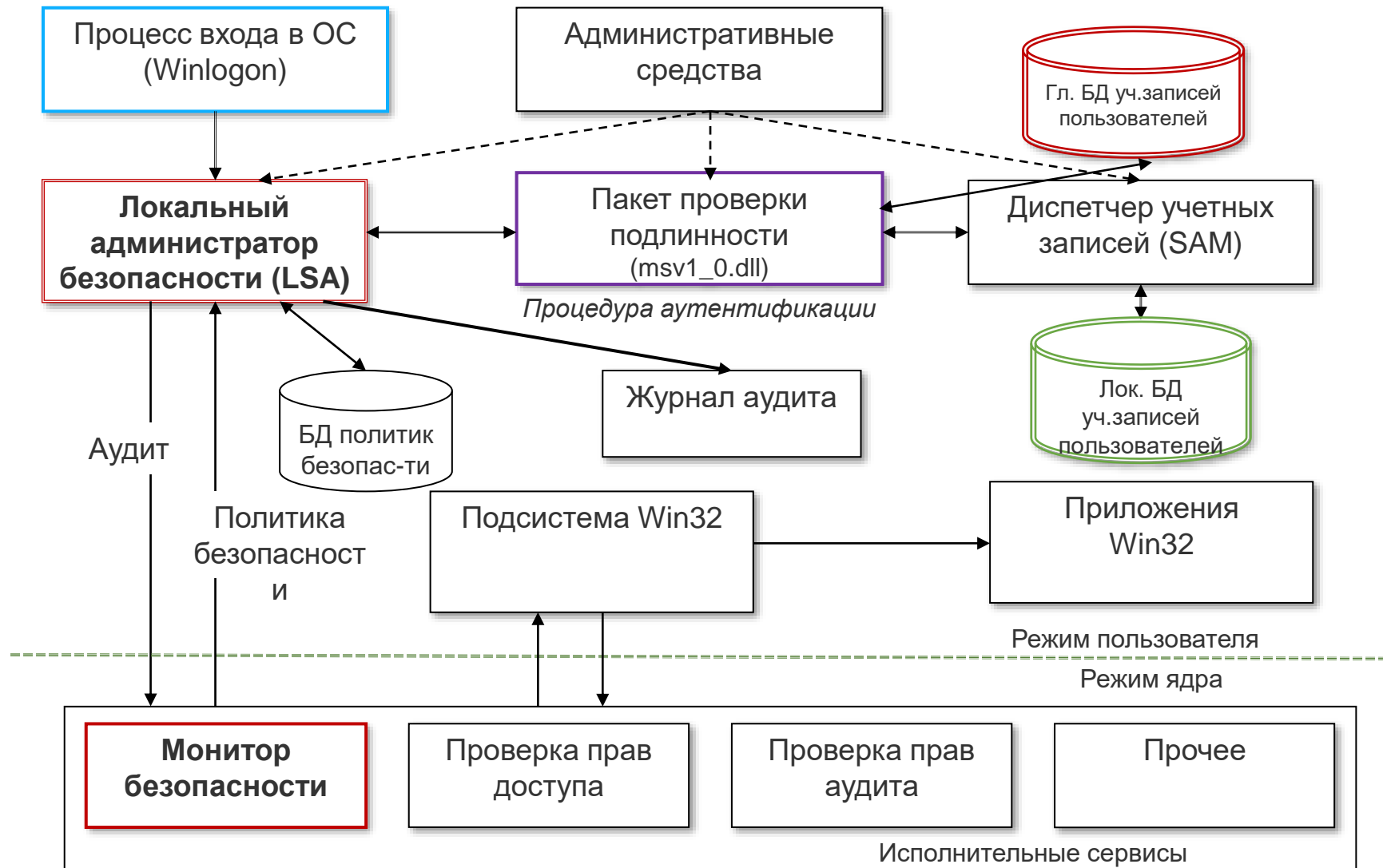


Для построения моделей безопасности принято представлять ОС в виде совокупности взаимодействующих сущностей – **субъектов** (s) и **объектов** (o).

Защищаемые объекты *Windows* включают: *файлы, устройства, каналы, события, семафоры, разделы общей памяти, разделы реестра* ряд других. Сущность, от которой нужно защищать объекты, называется "субъектом". Субъектами в *Windows* являются процессы и потоки, запускаемые конкретными пользователями.

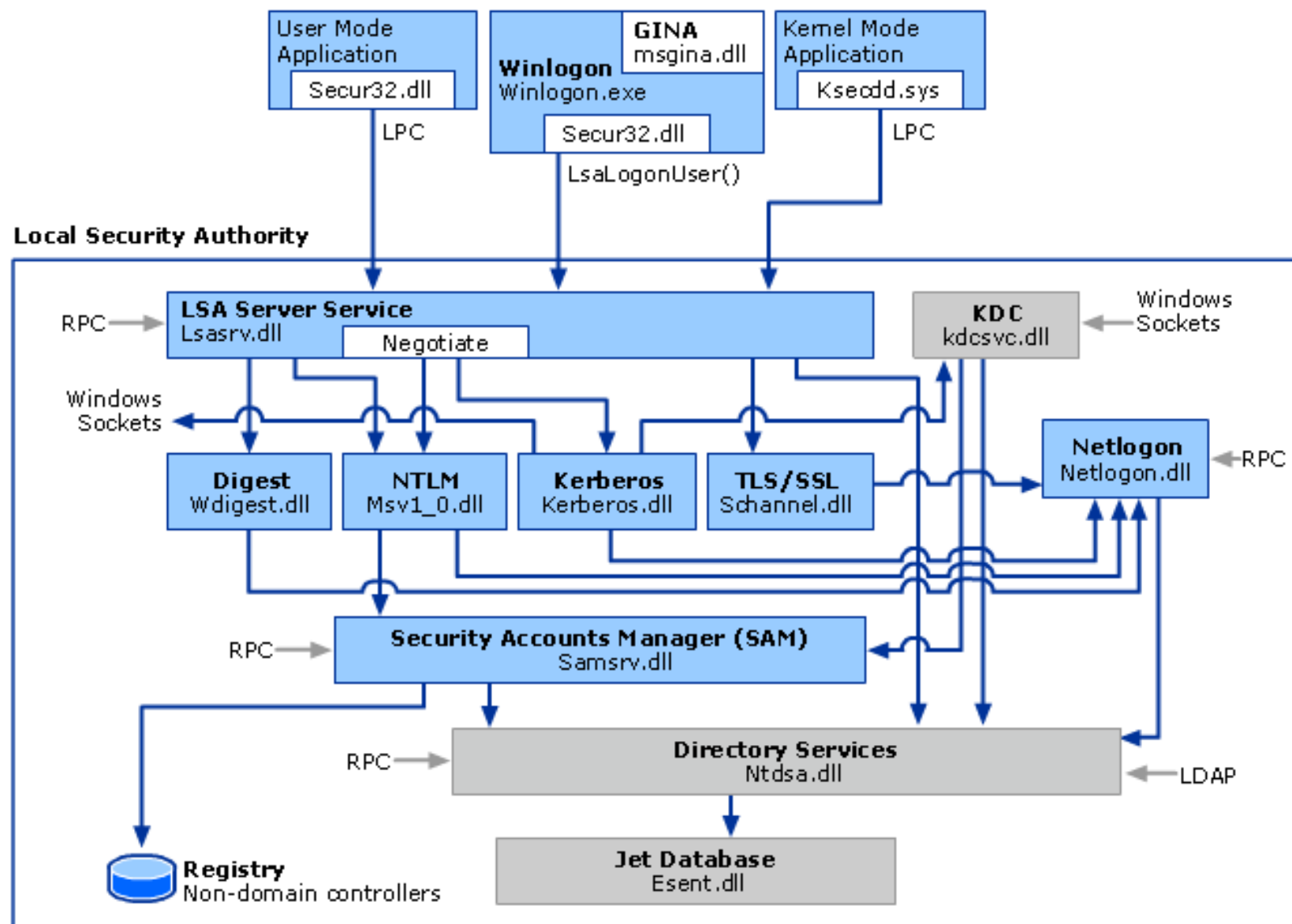
Помимо **дискреционного доступа** *Windows* поддерживает управление **привилегированным** доступом. Это означает, что в системе имеется *пользователь-администратор* с расширенными (неограниченными) правами. Кроме того, для упрощения администрирования (а также для соответствия стандарту *POSIX*) пользователи *Windows* объединены в группы. Принадлежность к группе связана с определенными привилегиями, например, *привилегия выключать компьютер*. Пользователь, как член группы, облекается, таким образом, набором полномочий, необходимых для его деятельности, и играет определенную роль. Подобная стратегия называется управление **ролевым** доступом.

# СТРУКТУРА WINDOWS





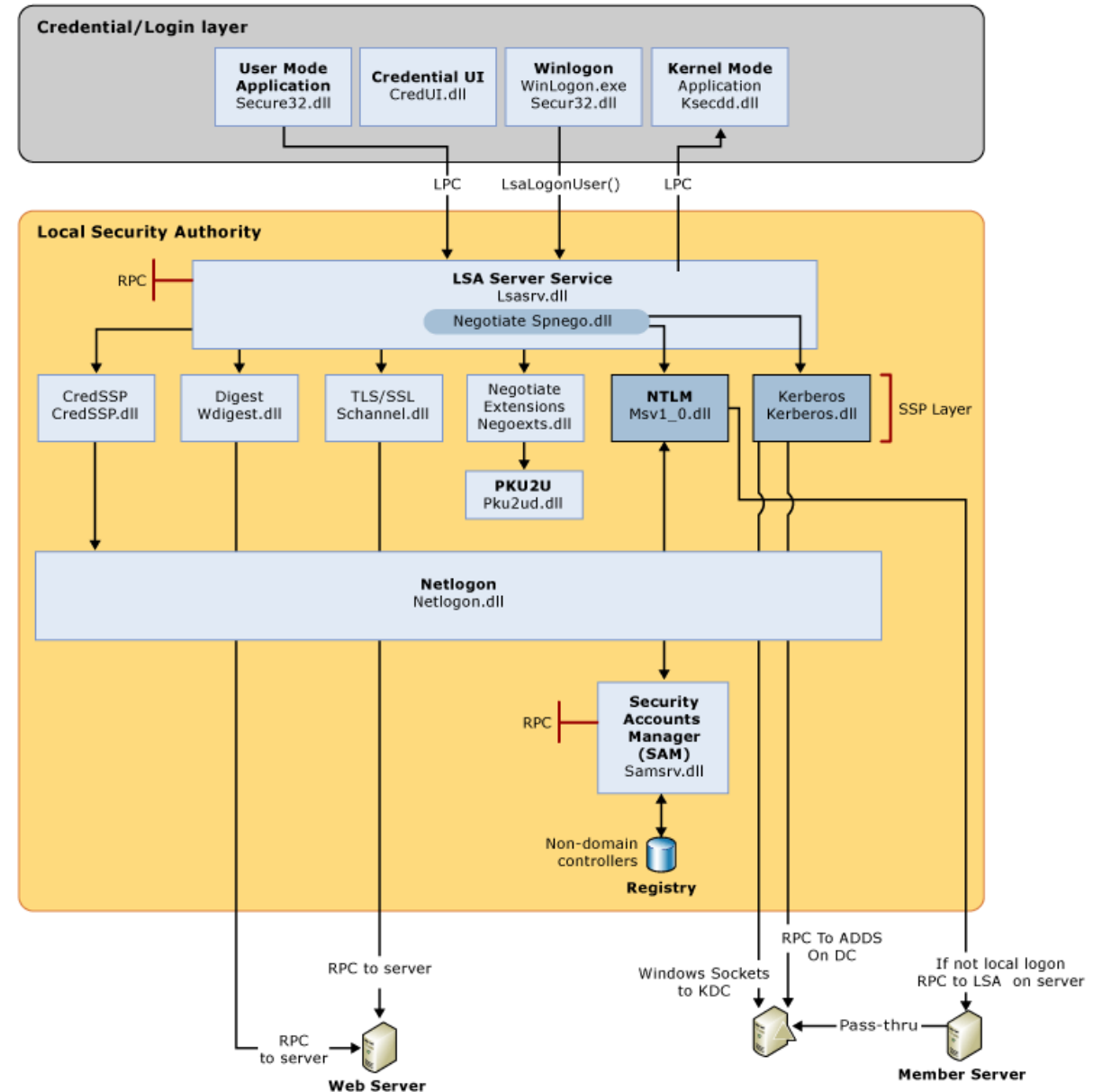
# СТРУКТУРА WINDOWS



<https://docs.microsoft.com/ru-ru/windows-server/security/windows-authentication/credentials-processes-in-windows-authentication>

# СТРУКТУРА WINDOWS

<https://docs.microsoft.com/ru-ru/windows-server/security/windows-authentication/credentials-processes-in-windows-authentication>





# СУБЪЕКТЫ И ОБЪЕКТЫ



# СУБЪЕКТЫ И ОБЪЕКТЫ



## Ключевые термины:

SID – Security Identifier, идентификатор безопасности;

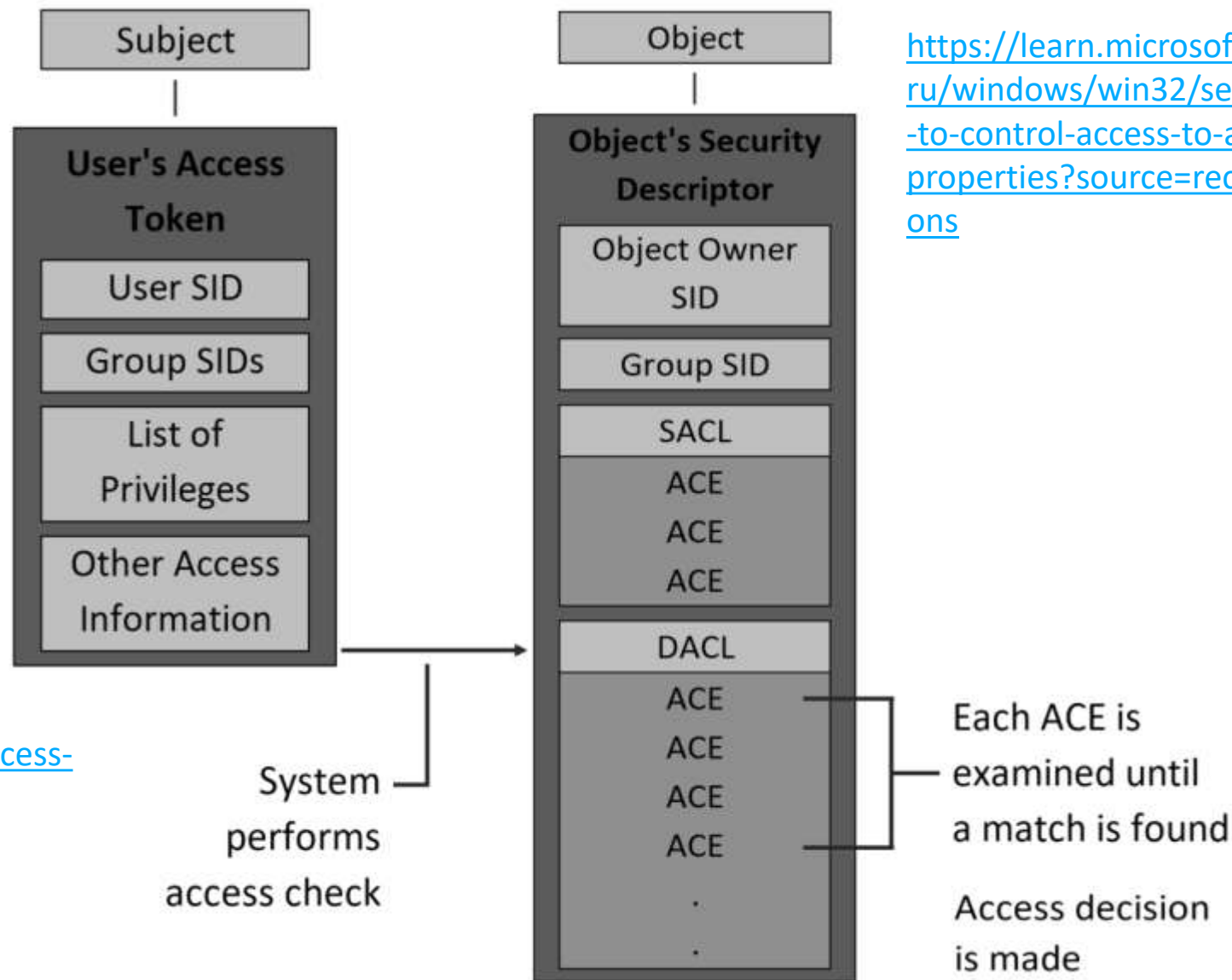
SACL – System Access Control List, системный список контроля доступа;

DACL – Discretionary Access Control List, дискреционный список контроля доступа;

ACE – Access Control Entries, запись контроля доступа.

<https://docs.microsoft.com/ru-ru/windows/security/identity-protection/access-control/security-identifier>

<https://learn.microsoft.com/ru-ru/windows/win32/secauthz/aces-to-control-access-to-an-object-properties?source=recommendations>



# СУБЪЕКТЫ + SID

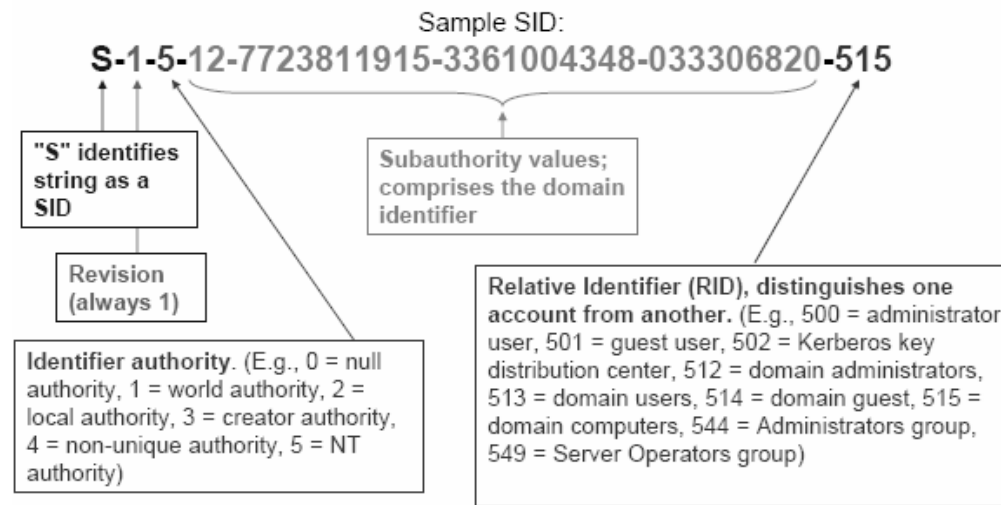


## Структура SID

Subauthority Count	Reserved	Revision
Identifier Authority		
Subauthority [1]		
.		
.		
Subauthority [n]		

Domain Identifier

Relative Identifier



## Как узнать идентификаторы безопасности (SID) пользователей?

- whoami /user
- wmic useraccount where name="%username%" get name,sid
- wmic useraccount where name="TestUser1" get sid
- Get-WmiObject -Class Win32\_UserAccount -Filter "name='TestUser1'"
- (gwmi win32\_useraccount -Filter "sid = \'SID\'").name
- (gwmi win32\_useraccount -Filter "sid = \'S-1-5-21-3210479907-464018182-414762983-1002\'").name

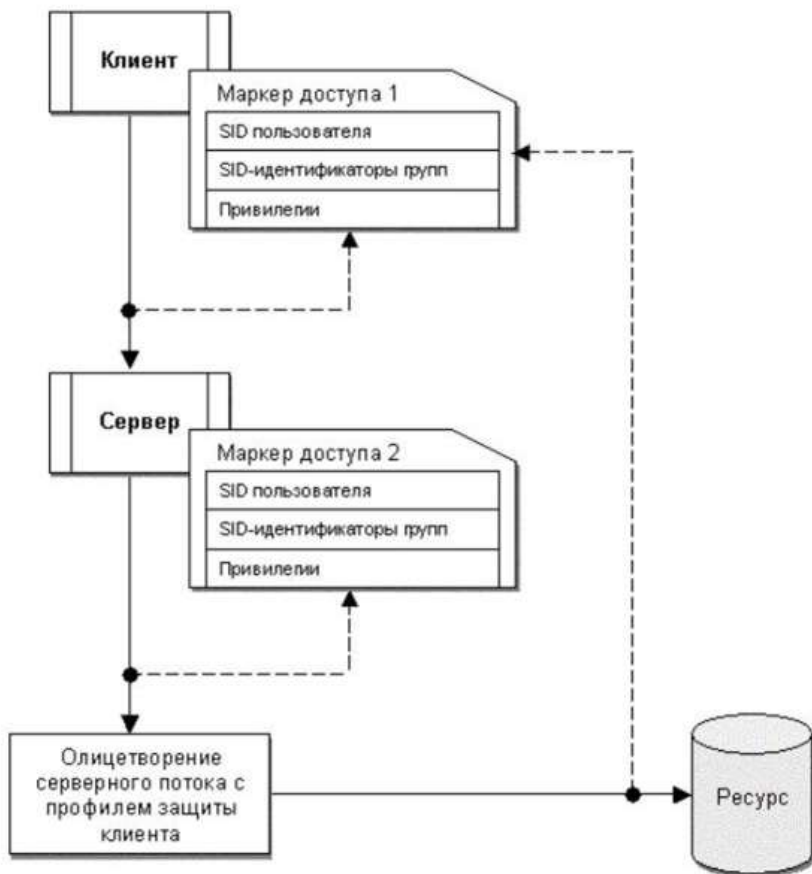
HKEY\_LOCAL\_MACHINE\\SOFTWARE\\  
\\Microsoft\\Windows  
NT\\CurrentVersion\\ProfileList

<https://docs.microsoft.com/ru-ru/windows/security/identity-protection/access-control/security-identifier>

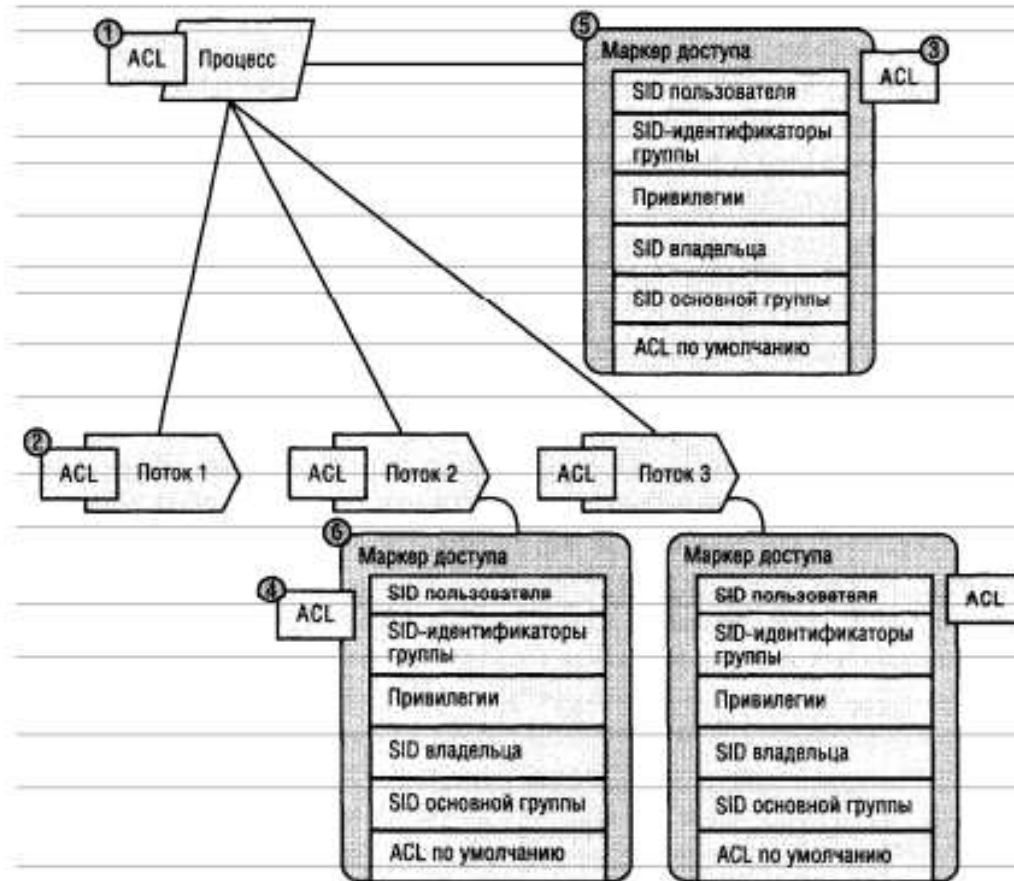
<https://docs.microsoft.com/ru-ru/windows/win32/secauthz/well-known-sids>



# ОЛИЦЕТВОРЕНИЕ И ИМПРЕСОНАЛИЗАЦИЯ



4 уровня олицетворения, определяющие операции, которые сервер может выполнять в контексте клиента



По умолчанию у потоков в ОС нет собственного маркера доступа и для целей безопасности используется маркер доступа процесса-родителя (поток 1). При необходимости каждый поток может получить собственный маркер доступа (потоки 2 и 3).

# ПРАВА И ПРИВИЛЕГИИ



conhost.exe:3488 Properties

User: [redacted]  
SID: S-1-5-21-1241004363-267861926-1289139162-1607  
Session: 2 Logon Session: d01788  
Virtualized: No Protected: No

	Flags
IN\Администраторы	Deny
IN\Пользователи	Mandatory
IN\Пользователи журналов производительности	Mandatory
R\Denied RODC Password Replication Group	Mandatory
R\Development department	Mandatory
R\Domain Admins	Deny
R\Domain Users	Mandatory
R\IT department	Mandatory
R\NextCloud Access	Mandatory
R\test	Mandatory
IT\HORITY\LogonSessionId_0_13637330	Mandatory
IT\HORITY\Данная организация	Mandatory

Group SID: S-1-5-32-544

Privilege	Flags
SeChangeNotifyPrivilege	Default Enabled
SeIncreaseWorkingSetPrivilege	Disabled
SeShutdownPrivilege	Disabled
SeTimeZonePrivilege	Disabled
SeUndockPrivilege	Disabled

Permissions

OK Cancel

cmd.exe:10424 Properties

User: [redacted]  
SID: S-1-5-21-1241004363-267861926-1289139162-1607  
Session: 2 Logon Session: d01728  
Virtualized: No Protected: No

	Flags
IN\Администраторы	Owner
IN\Пользователи	Mandatory
IN\Пользователи журналов производительности	Mandatory
R\Denied RODC Password Replication Group	Mandatory
R\Development department	Mandatory
R\Domain Admins	Mandatory
R\Domain Users	Mandatory
R\IT department	Mandatory
R\NextCloud Access	Mandatory
R\test	Mandatory
IT\HORITY\LogonSessionId_0_13637330	Mandatory
IT\HORITY\Данная организация	Mandatory

Group SID: S-1-5-32-544

Privilege	Flags
SeBackupPrivilege	Disabled
SeChangeNotifyPrivilege	Default Enabled
SeCreateGlobalPrivilege	Default Enabled
SeCreatePagefilePrivilege	Disabled
SeCreateSymbolicLinkPrivilege	Disabled
SeDebugPrivilege	Disabled
SeDelegateSessionUserImpersonatePrivilege	Disabled
SeImpersonatePrivilege	Default Enabled

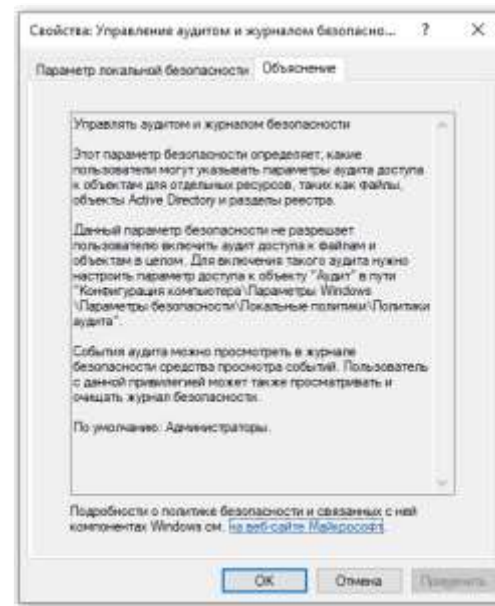
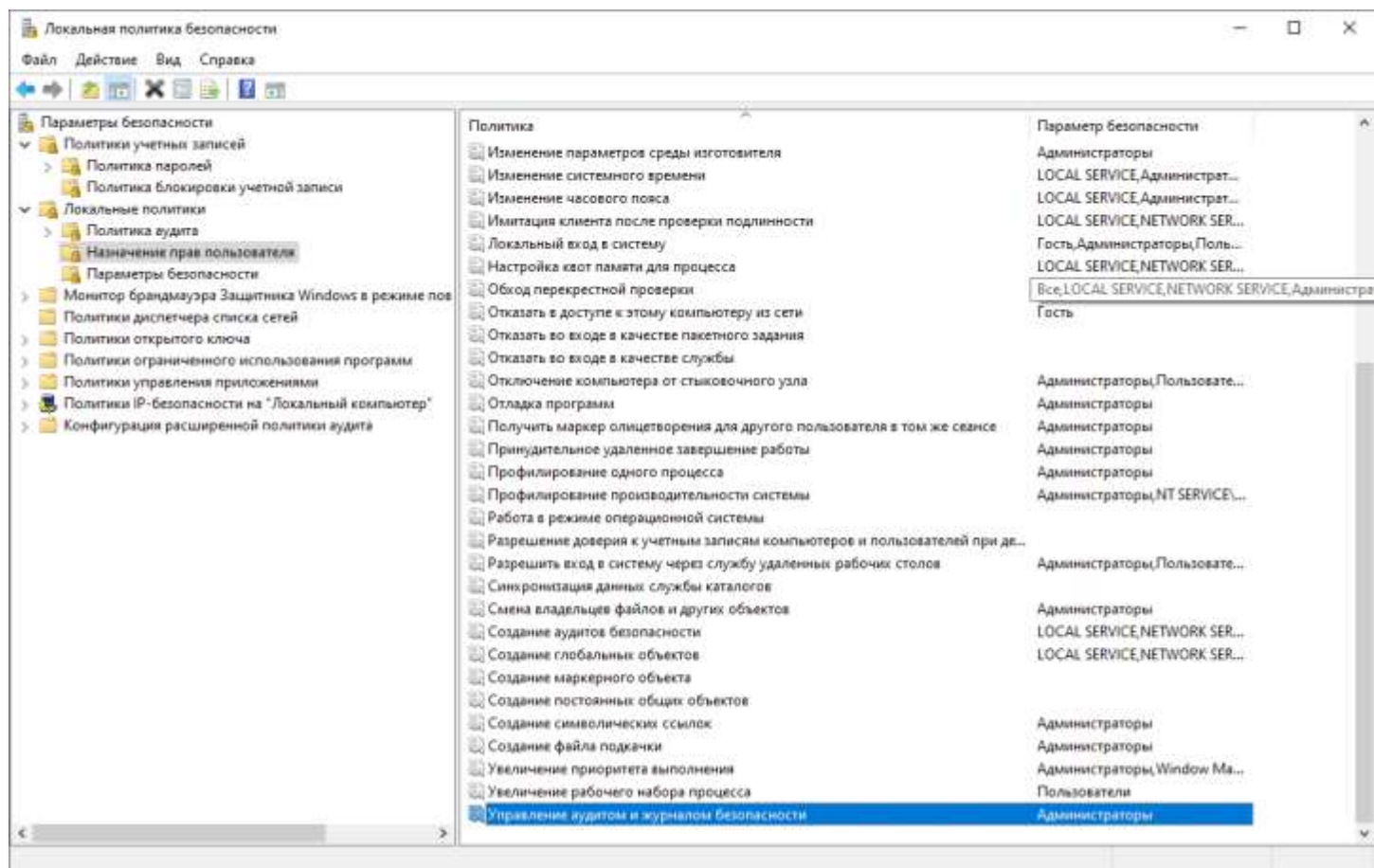
Permissions

OK Cancel





# ПРАВА И ПРИВИЛЕГИИ



# СТРУКТУРА МАРКЕРОВ ДОСТУПА

Структура DACL и SACL:



**Ключевые термины:**

Универсальные права

Стандартные права

Специфичные права

Запрещающее право

Разрешающее право

Наследуемое право

Ненаследуемое право



# ОБЪЕКТ ДОСТУПА: DACL И DAC

## Динамическое управление доступом (DAC)

Механизм избирательного управления доступом, описанный выше был еще с первой версии **Windows NT**. Но начиная с **Windows 8** и **Server 2012** появилось динамическое управление доступом (**DAC**). Оно рассчитано на домен.

Суть в том что в **маркер доступа** стало возможно добавлять различные атрибуты учетных записей домена. Например город в котором работает сотрудник:

Благодаря расширению маркера доступа и тега, **DAC** позволяет настраивать гибкие правила. **DAC** не заменяет **DACL**, а лишь дополняет его. Так что если **DACL** запрещало доступ к файлу, то с помощью **DAC** открыть доступ мы не сможем. Получится лишь ограничить доступ ещё сильнее, оставив доступ только у тех, кому он действительно нужен.

Свойства: [файл]

Член групп Входящие звонки Среда Сеансы Удаленное управление

Профиль служб удаленных рабочих столов COM+

Общие Адрес Учетная запись Профиль Телефоны Организация

Улица: [текстовое поле]

Почтовый ящик: [текстовое поле]

Город: [текстовое поле]

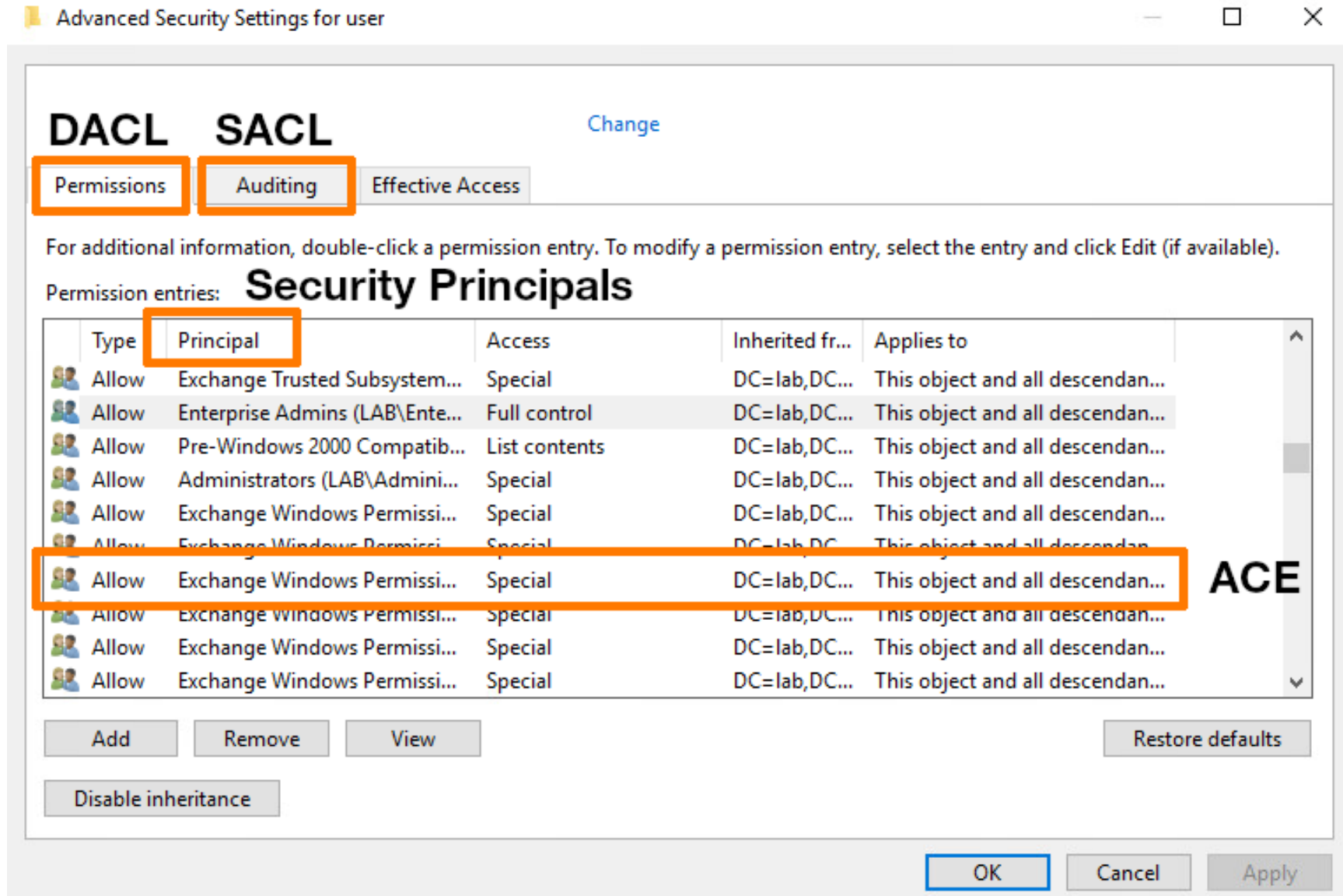
Область, край: [текстовое поле]

Почтовый индекс: [текстовое поле]

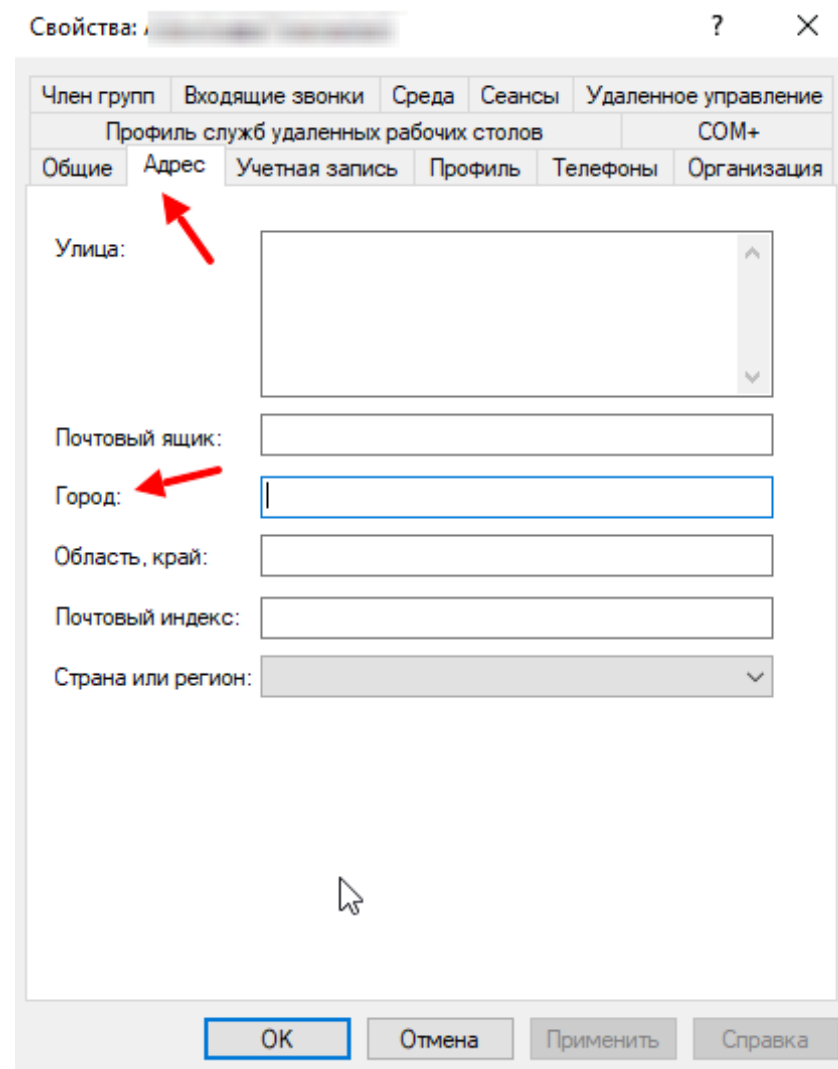
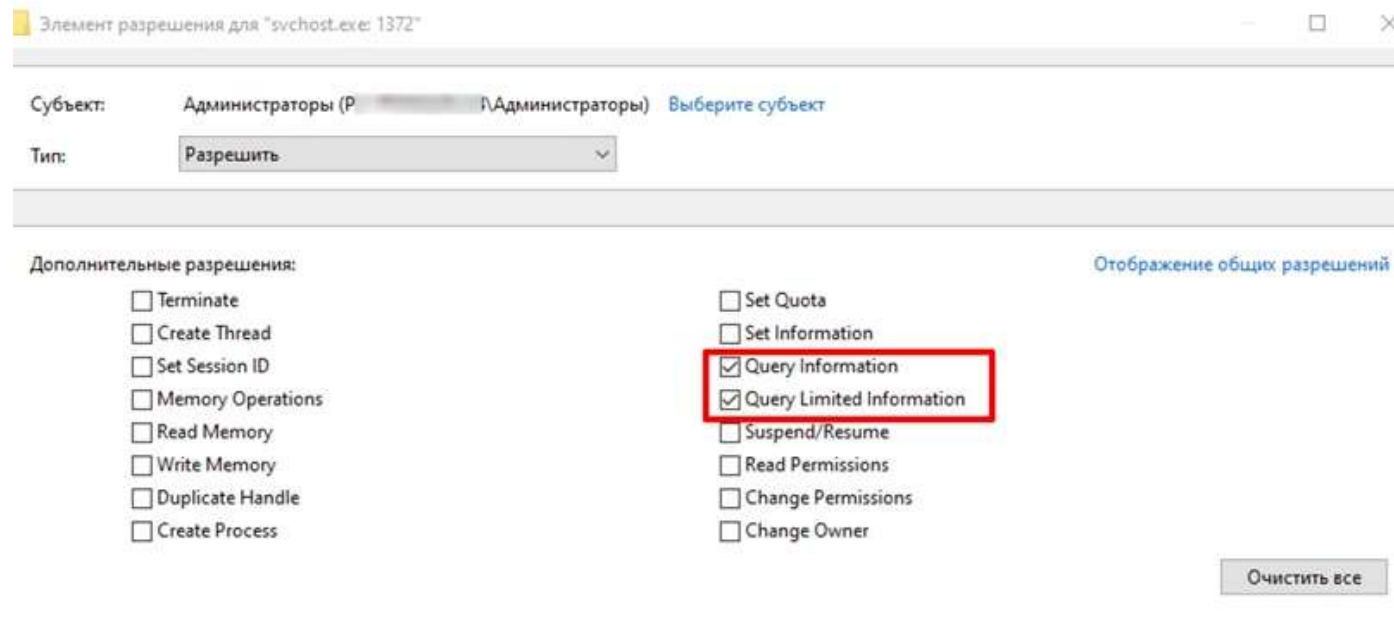
Страна или регион: [выпадающий список]

OK Отмена Применить Справка

# Объект доступа в Windows: DACL и SACL

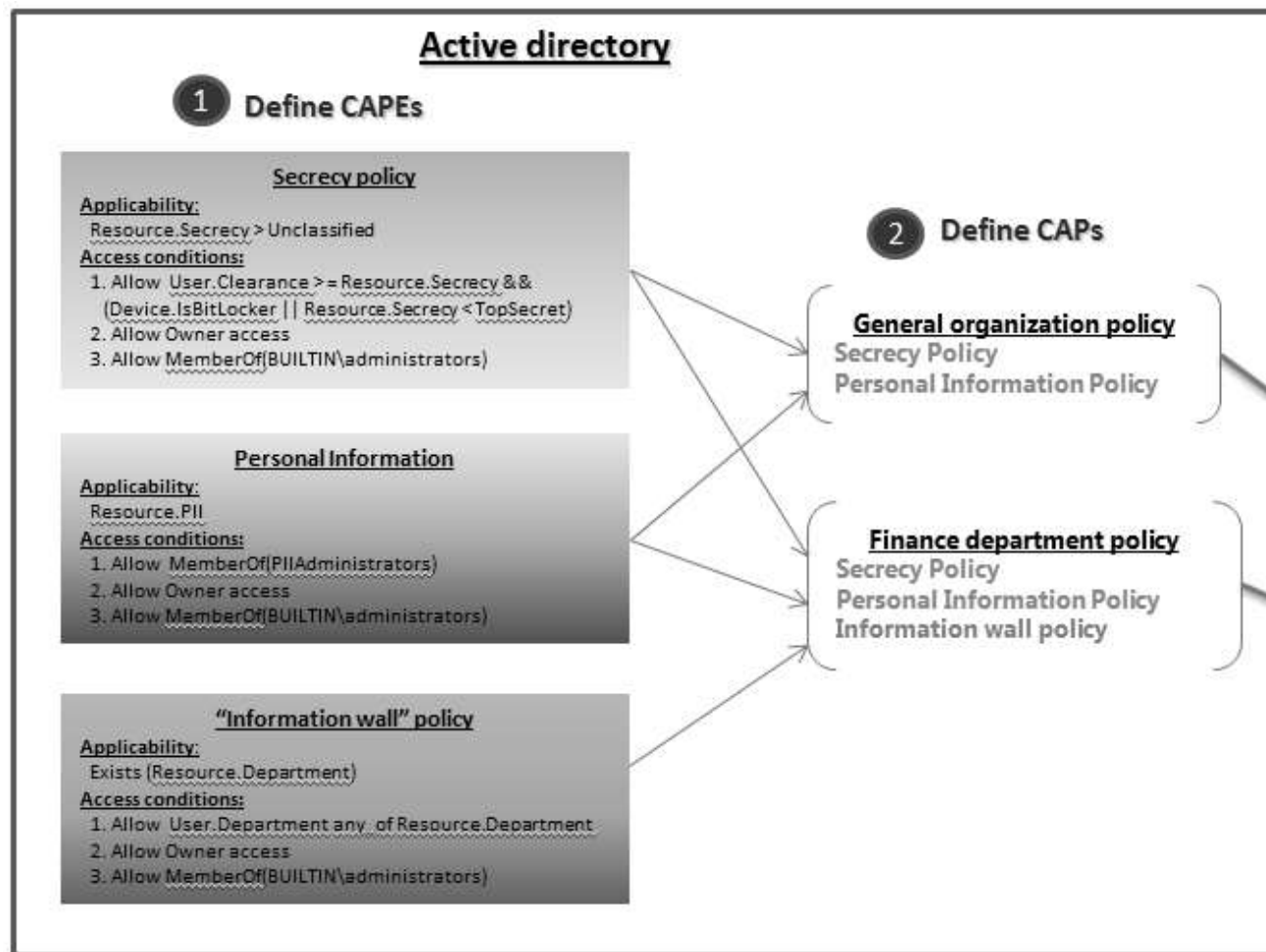


# Объект доступа в Windows: DACL и DAC





# Объект доступа в Windows: DACL и DAC



Предоставляется несколько новых абстракций политик авторизации, позволяющих администратору централизованно определять эти политики и упростить процесс определения, разрешая каждому из этих требований доступа определяться и поддерживаться отдельно, но применяться как одна политика.

# ПРАВА ДОСТУПА



Для управления NTFS разрешениями в Windows можно использовать встроенную утилиту **icaccls**. Утилита командной строки `icacls.exe` позволяет получить или изменить списки управления доступом (ACL — **A**ccess **C**ontrol **L**ists) на файлы и папки на файловой системе NTFS.

Команда вернет список пользователей и групп, которым назначены права доступа. Права указываются с помощью сокращений:

- F** — полный доступ
- M** — изменение
- RX** — чтение и выполнение
- R** — только чтение
- W** — запись
- D** — удаление

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> icacls 'C:\Share\Veteran\'
C:\Share\Veteran\ CREATOR OWNER:(OI)(CI)(IO)(F)
                  RESOURCE\fs01_Veteran_R:(OI)(CI)(RX)
                  RESOURCE\fs01_Veteran_RW:(OI)(CI)(M)
                  NT AUTHORITY\SYSTEM:(OI)(CI)(F)
                  RESOURCE\k_ _ov:(F)
                  BUILTIN\Administrators:(OI)(CI)(F)
                  BUILTIN\Users:(CI)(S,WD,AD)
                  BUILTIN\Users:(OI)(CI)(RX)

Successfully processed 1 files; Failed processing 0 files
```

А также бэкап (экспорт) текущих NTFS разрешений каталога

# ПРАВА ДОСТУПА



**SAM (*Security Account Manager*)** Диспетчер учётных записей безопасности — RPC-сервер Windows, оперирующий базой данных учетных записей.

SAM выполняет следующие задачи:

- Идентификация субъектов (трансляции имен в идентификаторы (SID'ы) и обратно);
- Проверка пароля, авторизация (участвует в процессе входа пользователей в систему);
- Хранит статистику (время последнего входа, количества входов, количества некорректных вводов пароля);
- Хранит настройки политики учетных записей и приводит их в действие (политика паролей и политика блокировки учетной записи);
- Хранит логическую структуру группировки учетных записей (по группам, доменам, алиасам);
- Контролирует доступ к базе учетных записей;
- Предоставляет программный интерфейс для управления базой учетных записей.

База данных SAM хранится в реестре (в ключе HKEY\_LOCAL\_MACHINE\SAM\SAM), доступ к которому запрещен по умолчанию даже администраторам. SAM-сервер реализован в виде DLL-библиотеки samsrv.dll, загружаемой lsass.exe. Программный интерфейс для доступа клиентов к серверу реализован в виде функций, содержащихся в DLL-библиотеке samlib.dll.

**SYSKEY** — утилита, которая шифрует информацию хешированного пароля в базе данных SAM в системе Windows, используя 128-битный ключ шифрования.



Home > [Recovering SAM](#)

**Редактор базы данных пользовательской SAM**


---

**11.10.2022**  
**Office password recovery tools**  
 Support for Nvidia RTX 40xx devices

**11.10.2022**  
**Windows Password Recovery v15.1**  
 Support for Nvidia RTX 40xx devices

**10.10.2022**  
**Windows Password Recovery v15.2**  
 Support for Nvidia GeForce RTX 40xx devices

**28.08.2022**  
**Chinese and Hindi articles**  
 Chinese and Hindi articles

 Email (new)

---


**Articles and video**


You may find it helpful to read our articles on Windows security and password recovery examples. Video lessons contain a number of movies about our programs in action.

## Windows Password Recovery - редактор SAM

Редактор **SAM** предназначен для просмотра, анализа и редактирования записей в статистике учетных записей: записей пользователей Windows, SAM, сохраненных в Security Account Manager, для RPC-сервера, управляющей базой данных учетных записей Windows и аутентифицирующей функции хранения паролей и приватных данных пользователей, поддерживаемых локальной Windows: записей, настройки политики безопасности (мажорны, приватия паролей или (полуприоритетный записи), сбора статистики данных последнего входа, количества входов, количества неизвестных входов паролей и т.д.) и контраста доступа к базе. База данных SAM хранится в файле реестра **HKEY\_LOCAL\_MACHINE\SAM\SAM**, доступ к которому запрещен всем, кроме системы (для администраторов). На функциональном уровне, база SAM предоставляет собой двоичный файл реестра с двоичным названием, который расположен в каталоге **%WINDIR%\System32\Config**, где **%WINDIR%** - установленный каталог Windows.

В начале работы Мастер предлагает выбрать тип базы данных SAM: локальную или удаленную.

 Укажите, если выбрать публичную базу, то в целях безопасности режим редактирования будет недоступен, база будет открыта только для чтения.



The screenshot shows the SAM Explorer application window. It has a title bar 'SAM Explorer' and a standard Windows interface. The main area is titled 'Selecting SAM registry source' and shows a tree view with 'SAM' selected. A progress bar at the bottom indicates 'Step 1/4'. Below the main area, there is a text box explaining the tool's purpose: 'SAM Explorer can help you investigating both public and private properties of any regular user account, as well as some attributes and internal structure of your Security Account Manager database.'

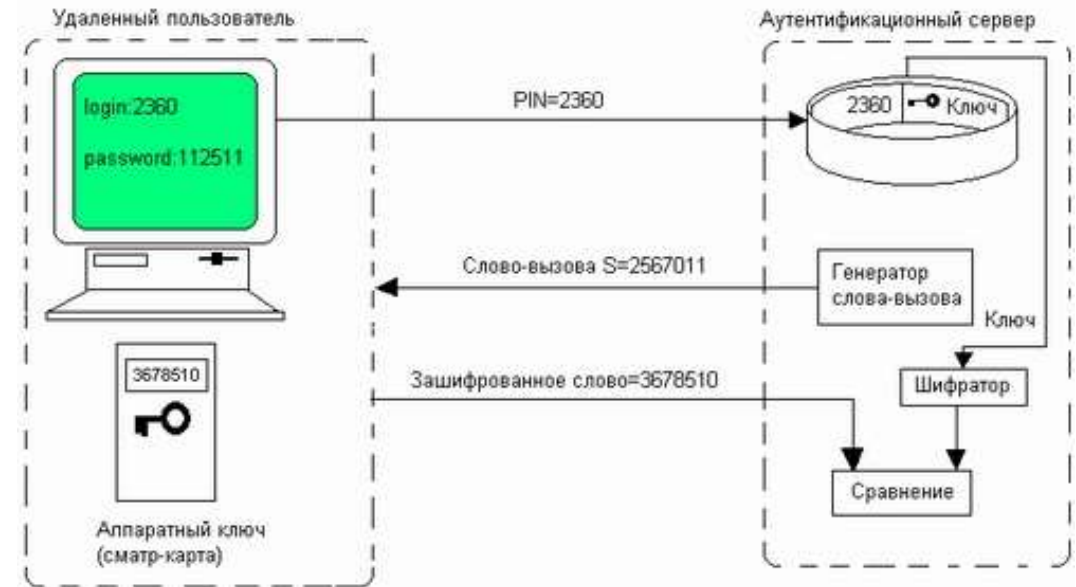
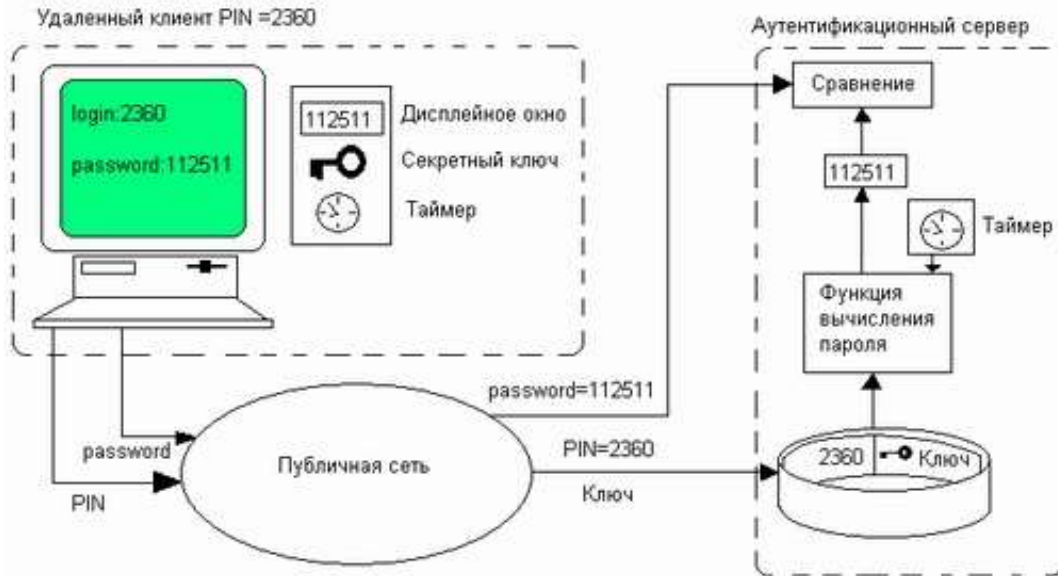
```
root@kali:~/media/CC742C62742C518E/Windows/System32/config# cd /root/Desktop/
root@kali:~/Desktop# cat hashes.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0
c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
:
vijay:1001:aad3b435b51404eeaad3b435b51404ee:c7e86705ea4642f5b8a6e34d86333955:
::
root@kali:~/Desktop# john --format=nt2 --users=vijay hashes.txt
Created directory: /root/.john
Loaded 1 password hash (NTLMv2 [MSB178128 SSE2 intrinsics 12x])
aad123 (vijay)
john 4.7.0 11:00:00:00 DONE (Mon Apr 27 01:18:58 2015) c/s: 574782 tr
ing: 4/1
password
Use the --show option to display all of the cracked passwords reliably
```

ОПРЕДЕЛЕНИЕ  
31.10.2018





# ПРОТОКОЛЫ АУТЕНТИФИКАЦИИ





# ПРОТОКОЛЫ АУТЕНТИФИКАЦИИ



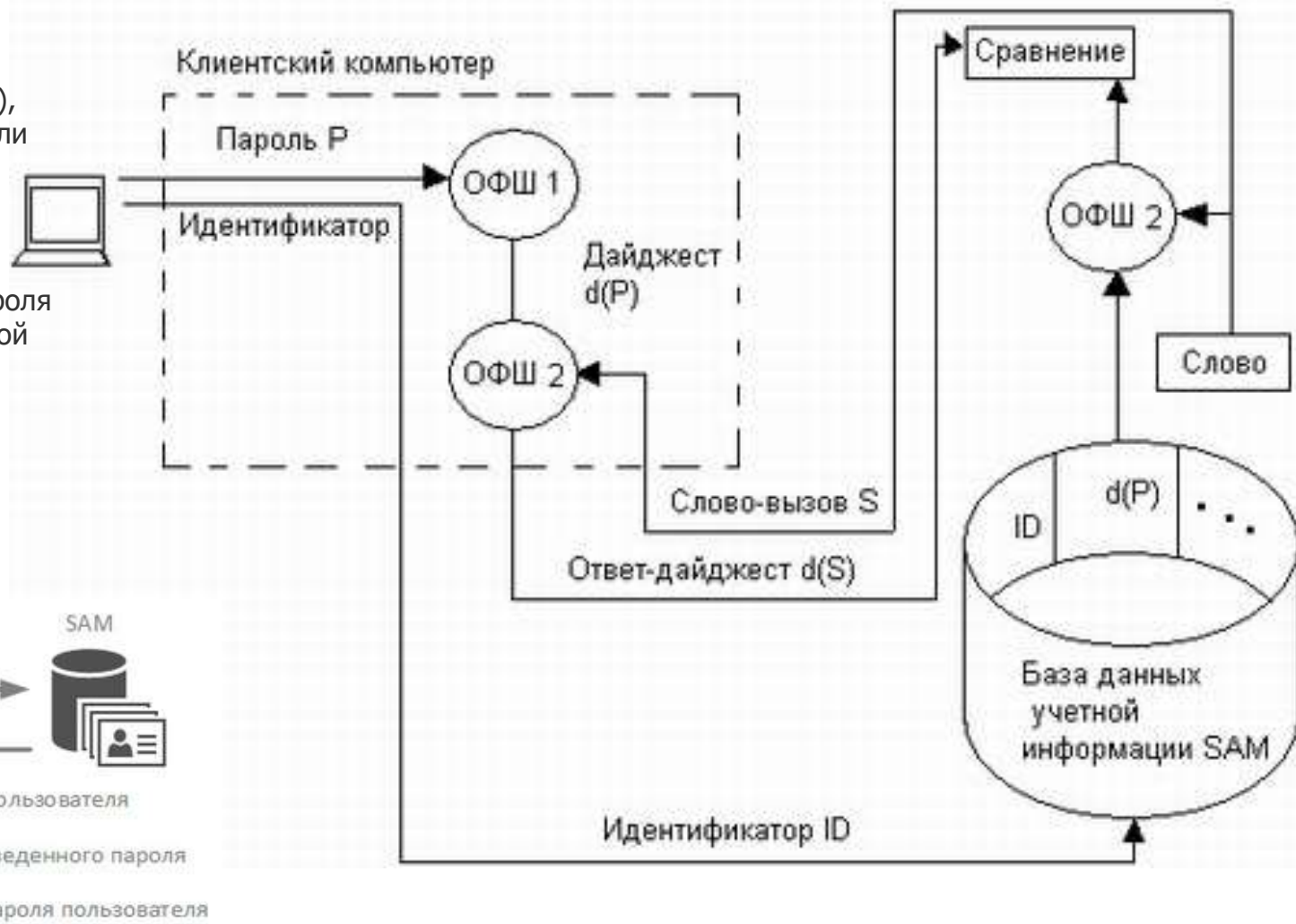
1. Пользователь вводит логин и пароль

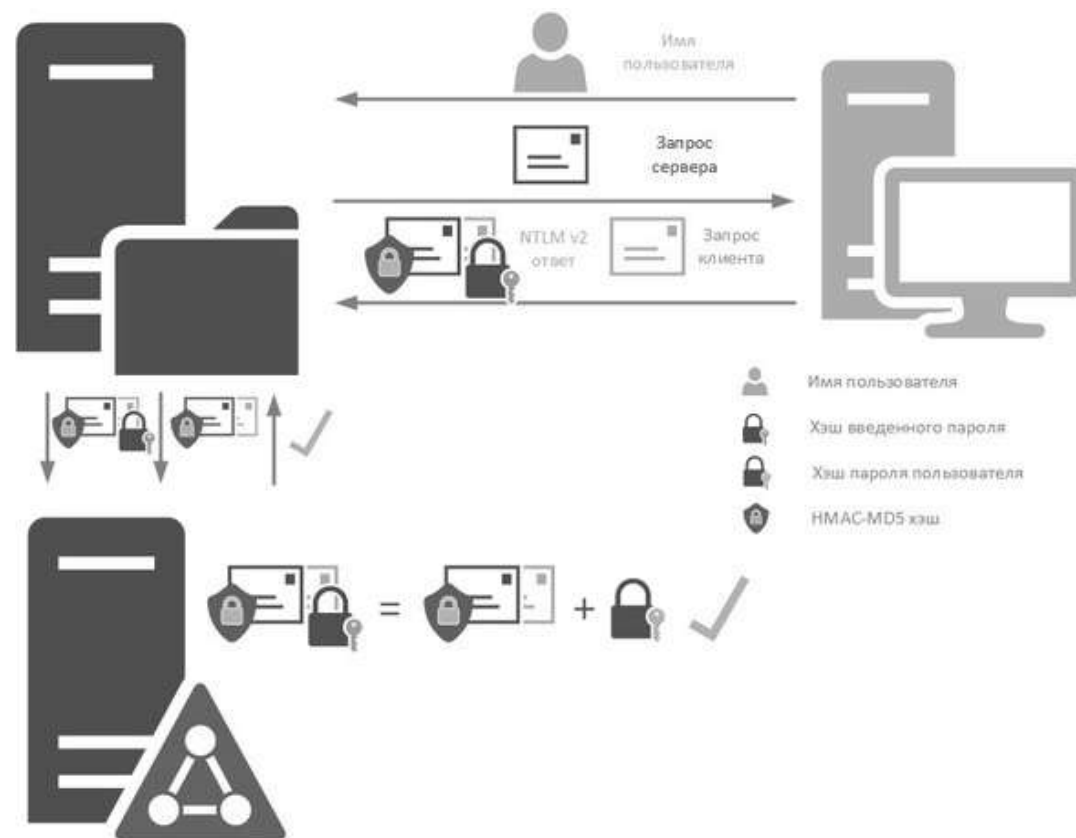
2. Данные передаются подсистеме локальной безопасности (LSA), которая сразу преобразует пароль в хэш. В открытом виде пароли нигде не хранятся.

3. Служба LSA обращается к диспетчеру учетных записей безопасности (SAM) и сообщает ему имя пользователя

4. Диспетчер обращается в базу SAM и извлекает оттуда хэш пароля указанного пользователя, сгенерированный при создании учетной записи (или в процессе смены пароля)

5. Затем LSA сравнивает хэши, в случае их совпадения аутентификация считается успешной, а хэш введенного пароля помещается в хранилище службы LSA и до окончания сеанса пользователя







# ПРОТОКОЛЫ АУТЕНТИФИКАЦИИ

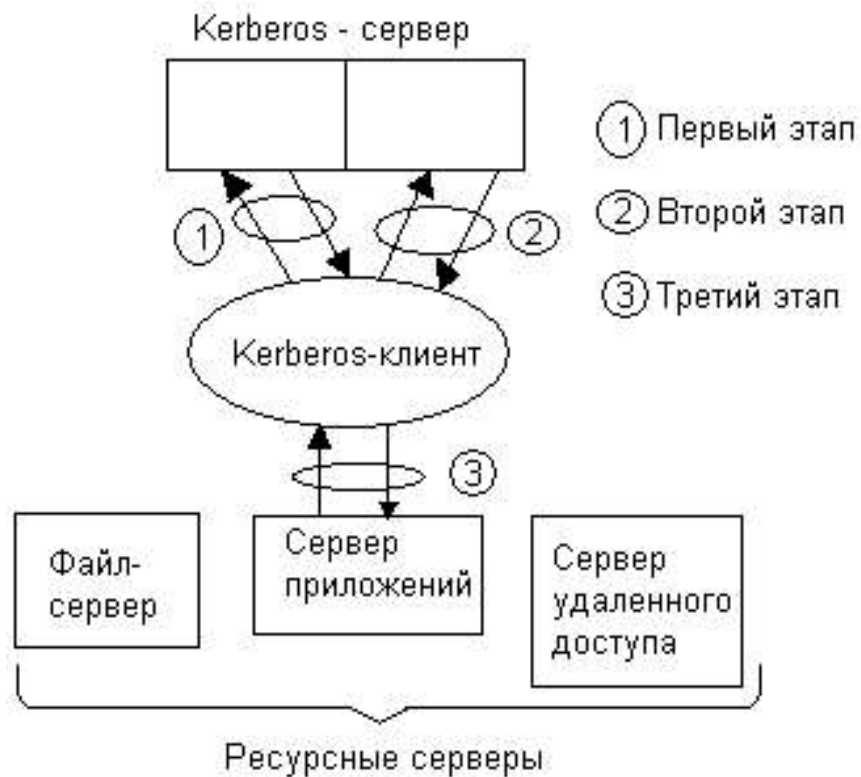
- LAN Manager (LM),
- NT LAN Manager (NTLM),
- NT LAN Manager версии 2 (NTLM v2)
- Kerberos

## **Схема работы протокола NTLMv2 с контроллером домена**

1. Клиент при обращении к серверу сообщает ему имя пользователя и имя домена
2. Сервер передает ему случайное число - запрос сервера
3. Клиент генерирует также случайное число, куда, кроме прочего, добавляется метка времени, которое называется запрос клиента
4. Запрос сервера объединяется с запросом клиента и от этой последовательности вычисляется HMAC-MD5 хэш
5. От данного хэша берется еще один HMAC-MD5 хэш, ключом в котором выступает NT-хэш пароля пользователя. Получившийся результат называется NTLMv2-ответом и вместе с запросом клиента пересылается серверу
6. Сервер, получив NTLMv2-ответ и запрос клиента, объединяет последний с запросом сервера и также вычисляет HMAC-MD5 хэш, затем передает его вместе с ответом контроллеру домена (КД)
7. КД извлекает из хранилища сохраненный хэш пароля пользователя и производит вычисления над HMAC-MD5 хешем запросов сервера и клиента, сравнивая получившийся результат с переданным ему NTLMv2-ответом
8. В случае совпадения серверу возвращается ответ об успешной аутентификации.



# KERBEROS

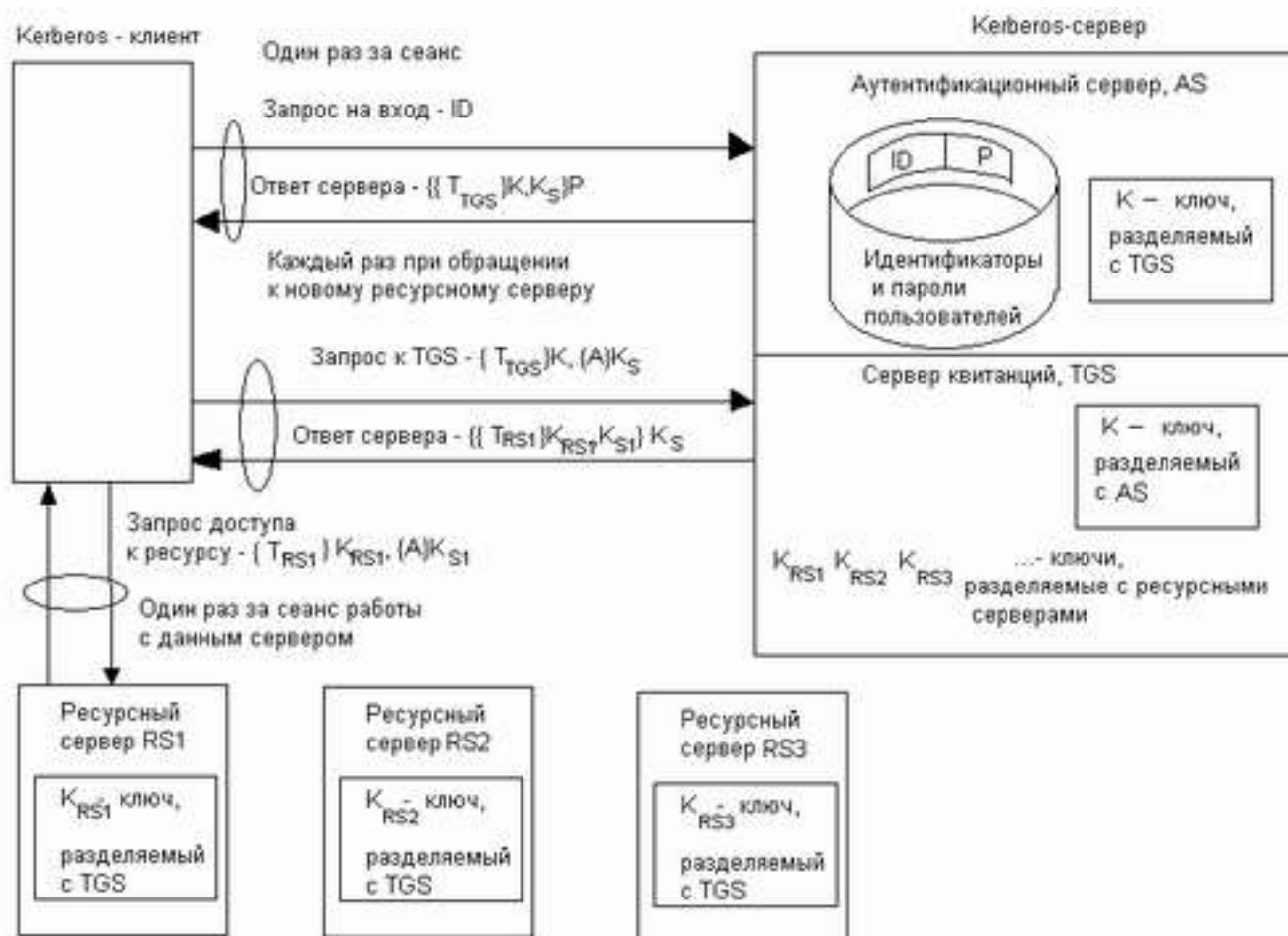


Протокол Kerberos был специально разработан для того, чтобы обеспечить надежную аутентификацию пользователей. Предусматривается, что начальный обмен информацией между клиентом и сервером происходит в незащищённой среде, а передаваемые пакеты могут быть перехвачены и модифицированы.

Протокол Kerberos может использовать централизованное хранение аутентификационных данных и является основой для построения механизмов Single Sign-On (возможность использования единой учетной записи пользователя для доступа к любым ресурсам области).

Протокол основан на понятии Ticket (билет). Ticket (билет) является зашифрованным пакетом данных, который выдается доверенным центром аутентификации, в терминах протокола Kerberos — Key Distribution Center (KDC, центр распределения ключей).

# KERBEROS



Протокол использует понятие **Ticket** (билет, удостоверение).

**Ticket** является зашифрованным пакетом данных, выданным выделенным доверенным центром аутентификации, в терминах протокола Kerberos - **KDC (Key Distribution Center, центр распределения ключей)**.

**KDC** состоит из двух компонент:

- сервер аутентификации (англ. Authentication Server, сокр. **AS**);
- сервер выдачи разрешений (англ. Ticket Granting Server, сокр. **TGS**).





# ПОЛИТИКА KERBEROS

Параметры политики расположены в **\Computer Configuration\Windows Параметры\Security Параметры\Account Policies\Kerberos Policy**.

	Описание
<a href="#">Принудительные ограничения входа пользователей</a>	Описывает лучшие практики, расположение, значения, управление политикой и соображения безопасности для параметра Политики безопасности принудить пользователей к ограничениям в области безопасности.
<a href="#">Максимальный срок жизни билета службы</a>	Описывает лучшие практики, расположение, значения, управление политикой и соображения безопасности для параметра Максимальное время службы для политики безопасности билета на обслуживание.
<a href="#">Максимальный срок жизни билета пользователя</a>	Описывает лучшие практики, расположение, значения, управление политикой и соображения безопасности для максимального срока службы для параметра <b>политики пользовательских</b> билетов.
<a href="#">Максимальный срок жизни для возобновления билета пользователя</a>	Описывает лучшие практики, расположение, значения, управление политиками и соображения безопасности для параметра политики безопасности максимального срока службы для политики обновления билетов пользователей.
<a href="#">Максимальная погрешность синхронизации часов компьютера</a>	Описывает лучшие практики, расположение, значения, управление политикой и соображения безопасности для обеспечения максимальной допустимости для безопасности <b>синхронизации часов</b> компьютера

# ВЗЛОМ KERBEROS



**Kerberos 5** является развитием четвертой версии, включает всю предыдущую функциональность и содержит множество расширений.

Основной причиной появления пятой версии являлась невозможность расширения. Со временем, **атака полным перебором** на DES используемом в Kerberos 4 стала актуальна, но используемые поля в сообщениях имели фиксированный размер и использовать более стойкий алгоритм шифрования не представлялось возможным.

Оригинальный протокол Kerberos 4 подвержен перебору по словарю.

Данная уязвимость связана с тем, что KDC выдает по требованию зашифрованный TGT любому клиенту. Важность данной проблемы также подчеркивает то, что пользователи обычно выбирают простые пароли.

Чтобы усложнить проведение данной атаки, в Kerberos 5 было введено предварительное установление подлинности. На данном этапе KDC требует, чтобы пользователь удостоверил свою личность прежде, чем ему будет выдан мандат.

За предварительную аутентификацию отвечает политика KDC, если она требуется, то пользователь при первом запросе к серверу аутентификации получит сообщение KRB\_ERROR. Это сообщение скажет клиенту, что необходимо отправлять AS\_REQ запрос со своими данными для установления подлинности. Если KDC не опознает их, то пользователь получит другое сообщение KRB\_ERROR, сообщающее об ошибке, и TGT не будет выдан.



# ВЗЛОМ KERBEROS

Хакеры нашли 5 основных способов обойти систему Kerberos, основанных на нацеливании на уязвимые системные настройки, слабые пароли или распространение вредоносного вредоносного ПО.

- **Pass-the-ticket:** этот метод создает ложный сеансовый ключ путем подделки ложного TGT. Затем хакер может представить TGT службе как действительные учетные данные. Наличие сеансового ключа позволяет этой подделке обходить все этапы проверки Kerberos, которые предшествуют этапу предоставления сеансового ключа.
- **Золотой билет:** этот метод подделывает билет со статусом администратора. Хакер имеет неограниченный доступ ко всему домену при использовании этого билета; доступны отдельные устройства, серверы, данные и настройки.
- **Серебряный билет:** Подобно атаке Золотого билета, серебряные билеты — это поддельный билет проверки подлинности службы, который предоставляет доступ к службе. Этот метод дает меньший доступ, чем атака по золотому билету, но его также труднее обнаружить.
- **Грубая сила:** самый очевидный метод, грубая форсировка, включает использование автоматического подбора паролей для ввода тысяч паролей до тех пор, пока не будет найден правильный. Для брутфорса не требуются украденные учетные данные, но его легко обнаружить из-за нечеловеческого поведения при входе.
- **Вредоносное ПО с скрытым ключом бэкдора :** в этом методе хакеры устанавливают скрытый ключ-ключ доступа к бэкдору в систему, чтобы позволить им войти в систему как любой пользователь в любое время в будущем. Этот метод требует ранее успешной атаки Golden Ticket Attack, поскольку эти скелетные ключи могут быть установлены только с административным доступом.



# ВЗЛОМ KERBEROS

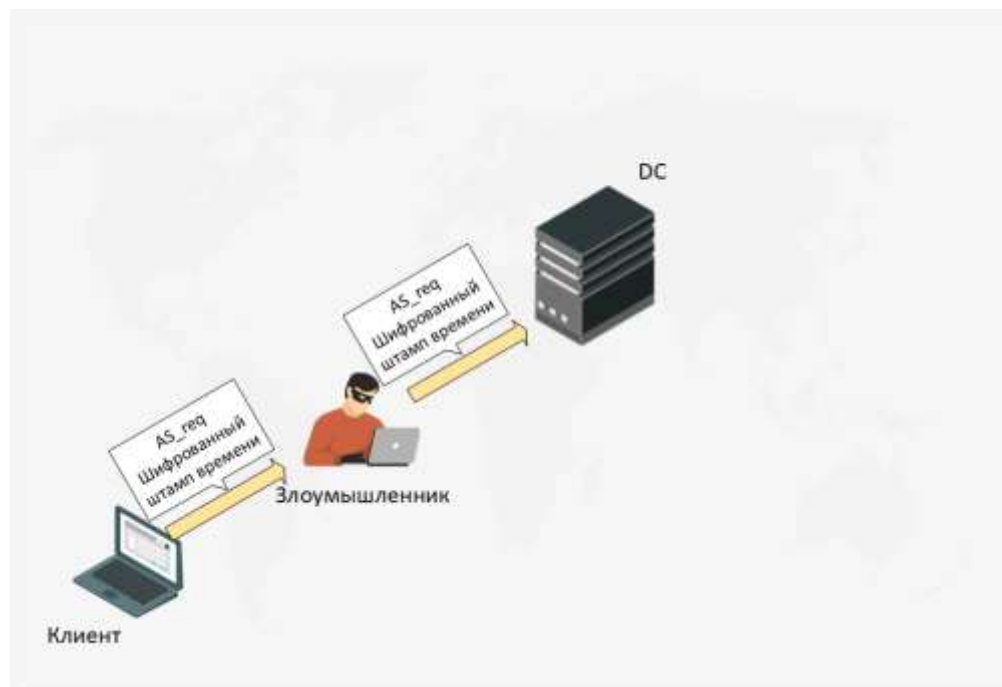
Kerberoasting является возможным т.к. DC не занимается авторизацией Клиента, то есть имеет ли право Клиент посещать те или иные сервисы — это не вопрос DC. И поэтому атакующий, имея одну лишь доменную учетную запись, может создать легитимный запрос билета TGS ко всем SPN в домене

T1208 - Kerberoasting				
Tool	PowerShell Invoke-Kerberoast	Rubeus kerberoast	Mimikatz kerberos::ask	Rubeus asktgs
Managed Code	.NET KerberosRequestorSecurityToken			
Windows API Function	InitializeSecurityContext		LsaCallAuthenticationPackage	
RPC	4f32adc8-6052-4a04-8701-293ccf2096f0 C:\WINDOWS\SYSTEM32\SspiSrv.dll			
Network Protocol	Kerberos TGS-REQ/REP			

Атаку можно разделить на несколько этапов:

1. Атакующий приступает к аутентификации в домене (AS\_req и AS\_rep).
2. Атакующий использует билет TGT для запроса получения билета TGS для конкретного SPN (TGS\_req и TGS\_rep).
3. Атакующий извлекает хеш зашифрованного билета TGS из TGS\_rep.

# ВЗЛОМ KERBEROS



Свойства: testuser1

? X

Организация	Член групп	Входящие звонки	Среда	Сеансы	
Удаленное управление					
Профиль служб удаленных рабочих столов			COM+		
Общие	Адрес	Учетная запись	Профиль	Телефоны	Делегирование
Имя входа пользователя:					
<input type="text" value="testuser1"/>		<input type="text" value="@testdomain.local"/>			
Имя входа пользователя (пред-Windows 2000):					
<input type="text" value="TESTDOMAIN\"/>		<input type="text" value="testuser1"/>			
<input data-bbox="1378 639 1582 682" type="button" value="Время входа..."/>		<input data-bbox="1607 639 1811 682" type="button" value="Вход на..."/>			
<input type="checkbox"/> Разблокировать учетную запись					
Параметры учетной записи:					
<input type="checkbox"/> Использовать только типы шифрования Kerberos DES для					
<input type="checkbox"/> Данная учетная запись поддерживает 128-разрядное					
<input type="checkbox"/> Данная учетная запись поддерживает 256-разрядное					
<input type="checkbox"/> Без предварительной проверки подлинности Kerberos					
Срок действия учетной записи					
<input checked="" type="radio"/> Никогда					
<input type="radio"/> Истекает: <input data-bbox="1592 1125 2109 1168" type="text" value="6 октября 2021 г."/>					
<input data-bbox="1536 1289 1689 1332" type="button" value="OK"/>		<input data-bbox="1709 1289 1862 1332" type="button" value="Отмена"/>		<input data-bbox="1882 1289 2035 1332" type="button" value="Применить"/>	
<input data-bbox="2056 1289 2209 1332" type="button" value="Справка"/>					

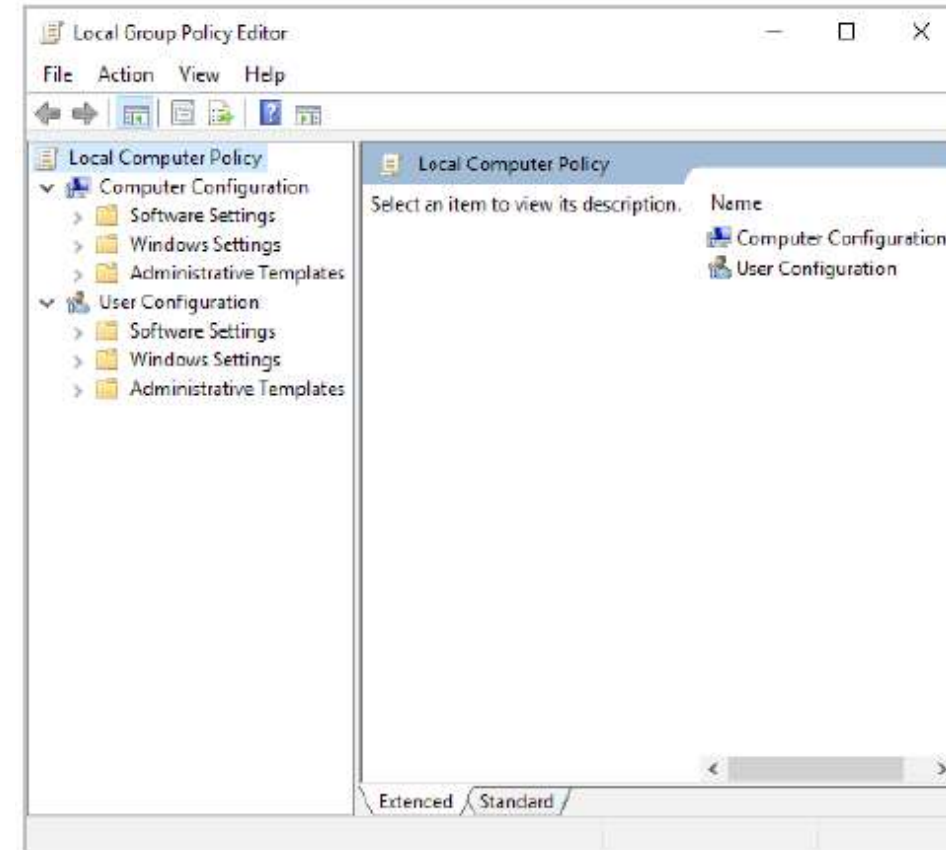


# ПОЛИТИКИ БЕЗОПАСНОСТИ



## Конфигурирование политик безопасности

**Политика безопасности** — это набор параметров, которые регулируют безопасность компьютера и управляются с помощью локального объекта **GPO**.  
Настраивать данные политики можно при помощи оснастки «**Редактор локальной групповой политики**» или оснастки «**Локальная политика безопасности**».  
Оснастка «**Локальная политика безопасности**» используется для изменения политики учетных записей и локальной политики на локальном компьютере, а политики учетных записей, привязанных к домену Active Directory можно настраивать при помощи оснастки «**Редактор управления групповыми политиками**».



Политики локального компьютера — включают настройки компьютера и пользователя; другие политики содержат только пользовательские настройки



# ПОЛИТИКИ БЕЗОПАСНОСТИ

## **Настройка локальных политик безопасности**

С помощью политики локального компьютера вы можете установить широкий диапазон параметров безопасности в разделе «Конфигурация компьютера\Параметры Windows\Параметры безопасности» (Computer Configuration\Windows Settings\Security Settings). Эта часть политики локального компьютера также известна как **Локальная политика безопасности** (*Local Security Policy*). Отдельно запустить оснастку локальной политики безопасности можно при помощи команды **Secpol.msc**, либо по пути **Панель управления-Администрирование-Локальные политики безопасности**.

**Политики учетной записи** (*Account Policies*). Правила для учетных записей используются для настройки функций блокировки пароля и учетной записи.

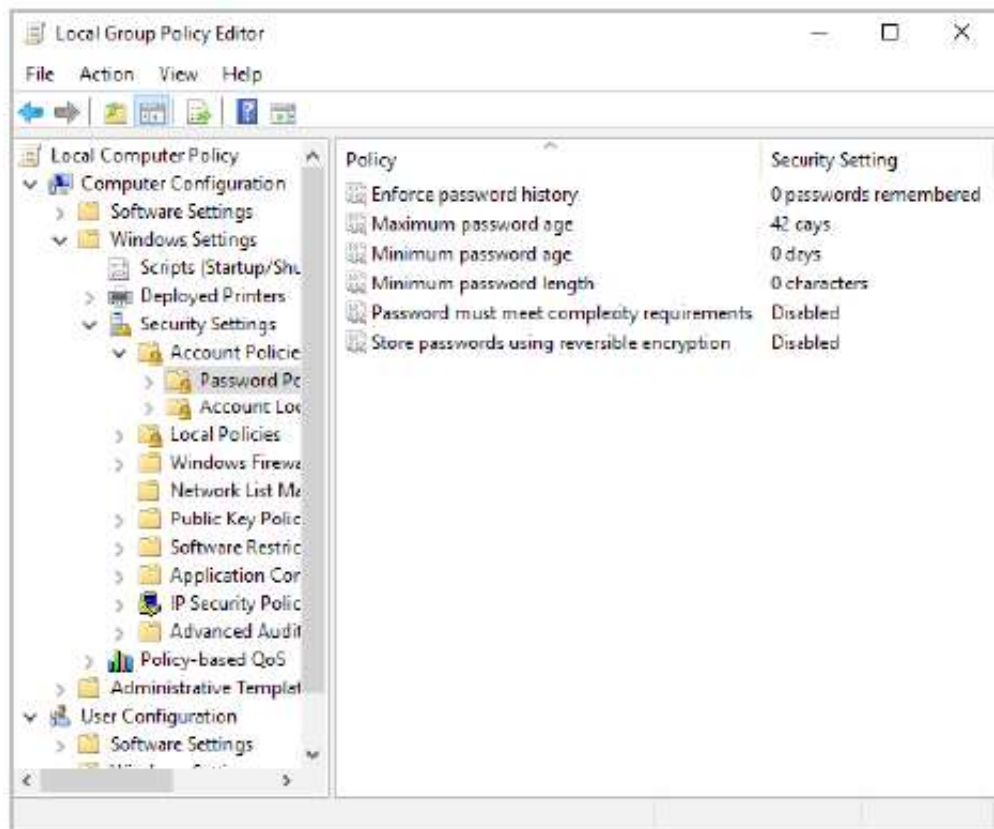
**Локальные политики** (*Local Policies*). Локальные политики используются для настройки аудита, прав пользователей и параметров безопасности.

**Брандмауэр Windows с повышенной безопасностью** (*Windows Firewall with Advanced Security*).

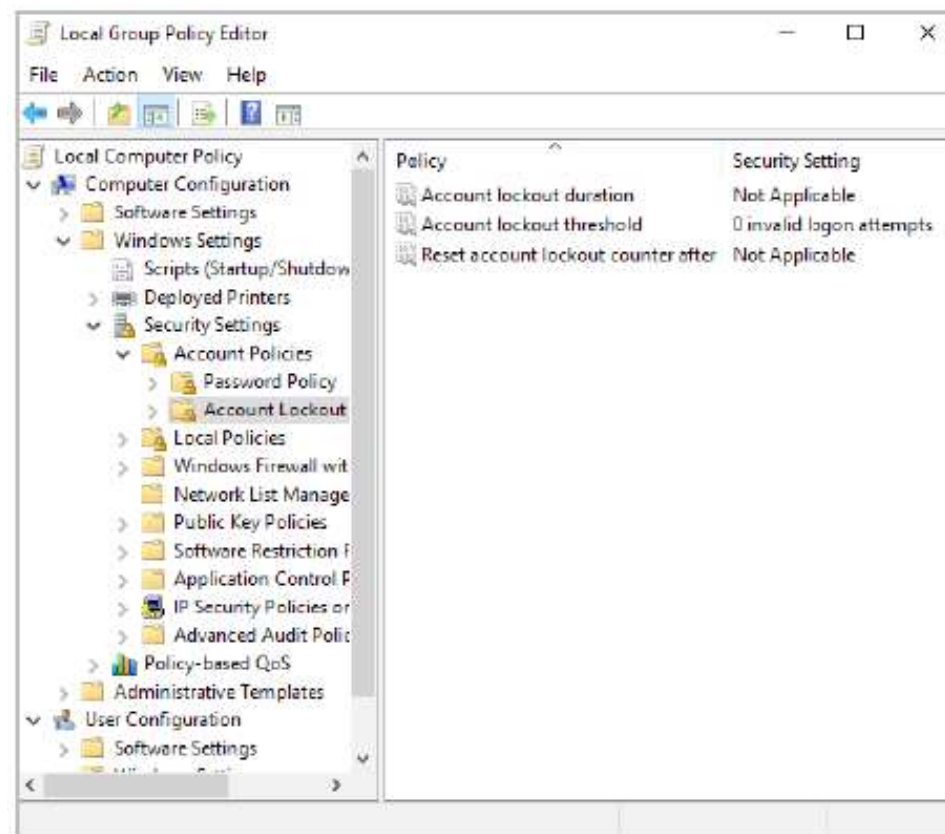
# ПОЛИТИКИ БЕЗОПАСНОСТИ



## Настройка паролей



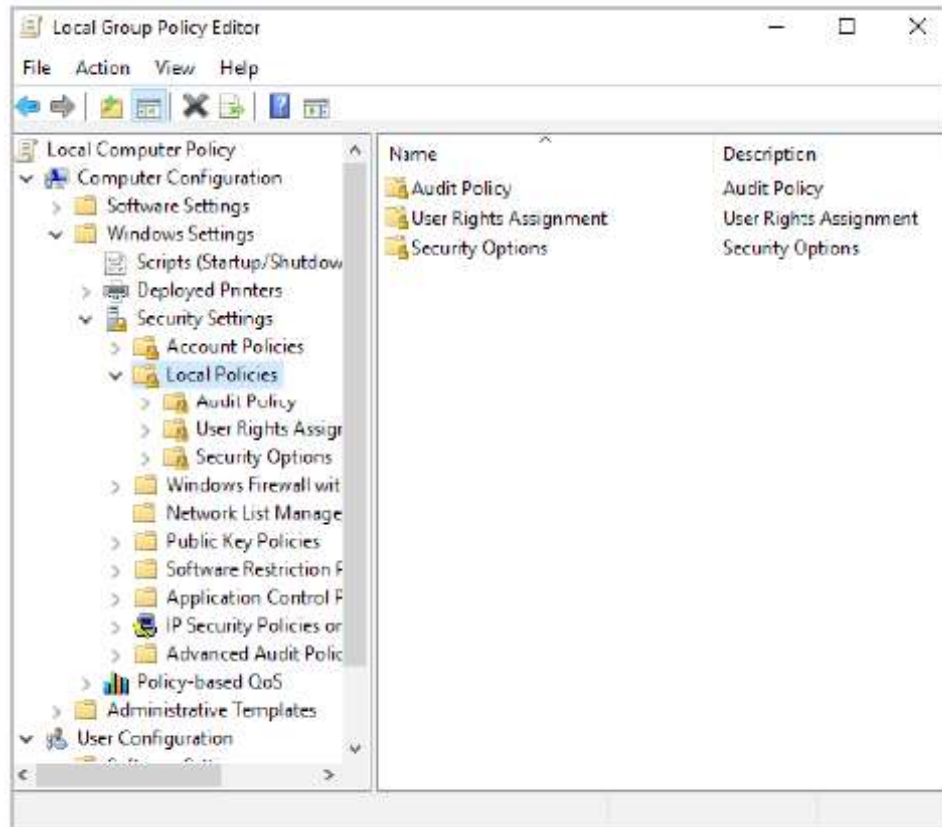
## Настройка политик блокировки учетной записи



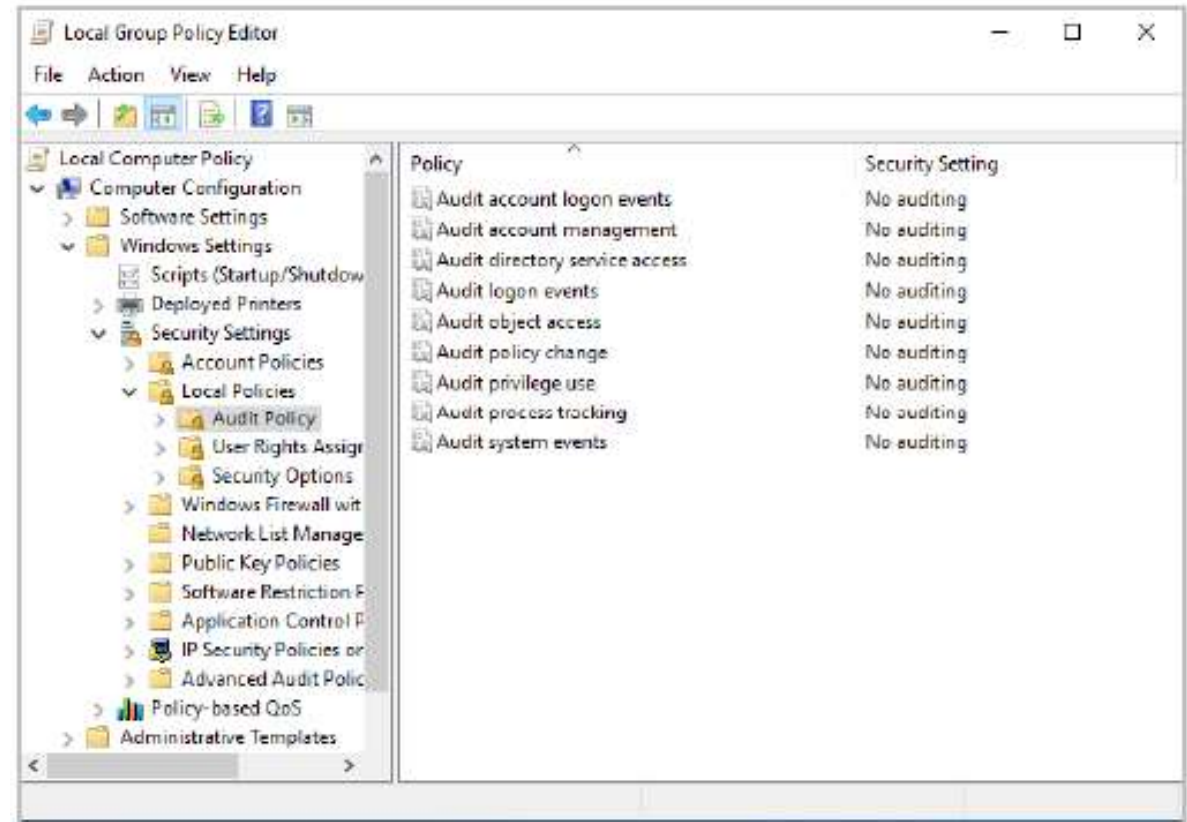


# ПОЛИТИКИ БЕЗОПАСНОСТИ

## Использование локальных политик



## Настройка политики аудита



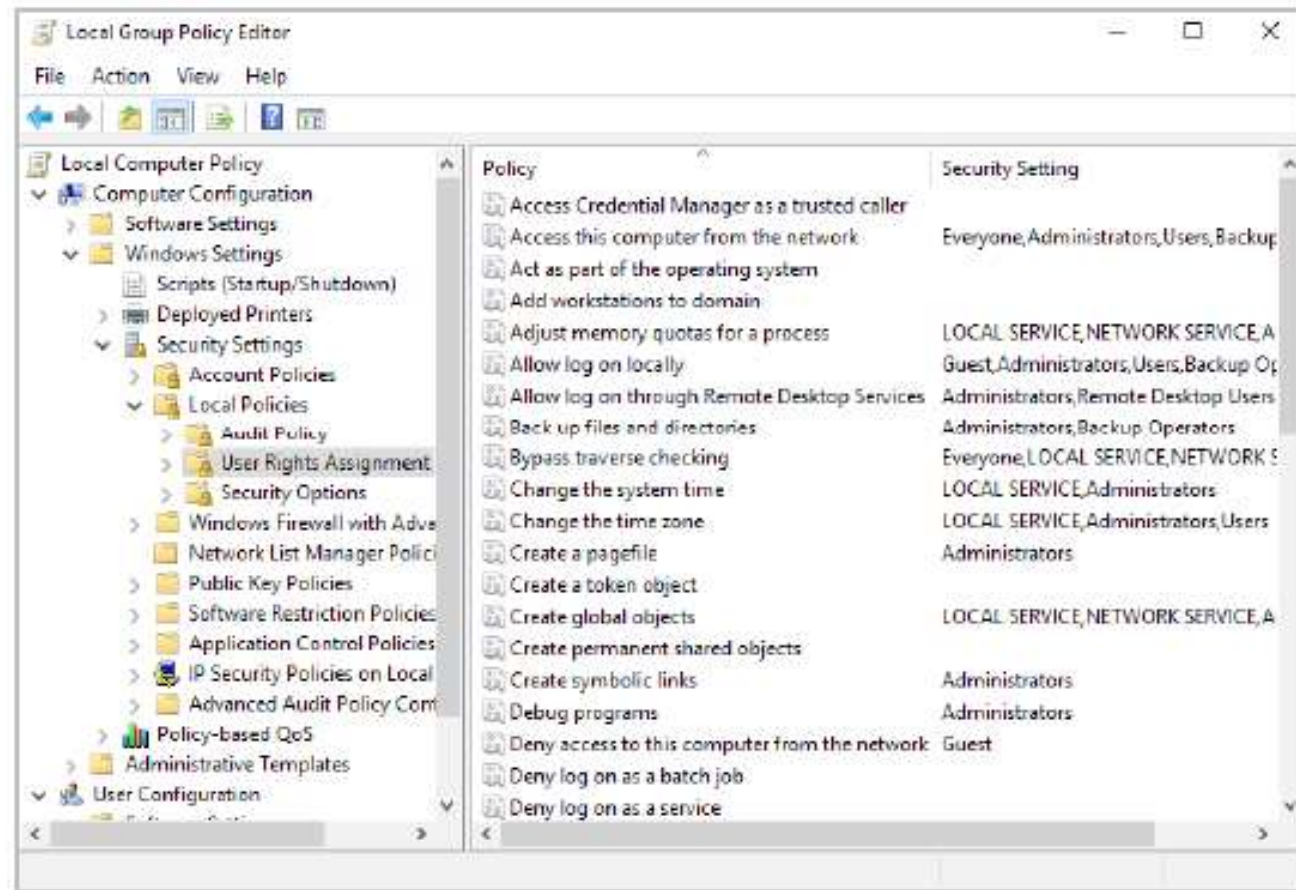




# ПОЛИТИКИ БЕЗОПАСНОСТИ

## Назначение прав пользователей

Политики прав пользователя определяют, какие права пользователь или группа имеют на компьютере. Права пользователя, также называемые привилегиями, применяются к системе. Они не совпадают с разрешениями, которые применяются к определенному объекту. Примером права пользователя является резервное копирование файлов и каталогов. Это право позволяет пользователю создавать резервные копии файлов и папок, даже если у пользователя нет разрешений, определенных с помощью разрешений файловой системы NTFS.





# ПОЛИТИКИ БЕЗОПАСНОСТИ



## *Настройка контроля учетных записей пользователей*

Большинство администраторов вынуждены были выбирать между безопасностью и возможностью корректного запуска приложений. Раньше некоторые приложения просто не запускались корректно под Windows, если только пользователь, запускающий приложение, не был локальным администратором.

Проблема в том, что многие приложения требуют, чтобы пользователи имели права на запись в защищенные папки и в реестр. Решение, применяемое в Windows 10 — это Контроль учетных записей (UAC). UAC позволяет пользователям, не являющимся администраторами, выполнять стандартные задачи, такие как установка принтера, настройка VPN или беспроводного соединения и установка обновлений, а также предотвращение ими выполнения административных задач, таких как установка приложений.



UAC защищает компьютеры, требуя повышения привилегий для всех пользователей, даже для пользователей, входящих в группу локальных администраторов. Это предотвращает запуск вредоносных программ без вашего ведома.



## **Повышение привилегий для пользователей**

Все пользователи работают с правами стандартного пользователя. Когда пользователь пытается выполнить действие, требующее административных полномочий, например, создает новую учетную запись, его полномочия должны быть повышены до прав локального администратора. Это действие и называется повышением полномочий. Основная функция UAC — контролировать процесс повышения полномочий. Он гарантирует, что доступ к административным правам не будет предоставлен без ведома пользователя.

## **Повышенные привилегии для исполняемых файлов**

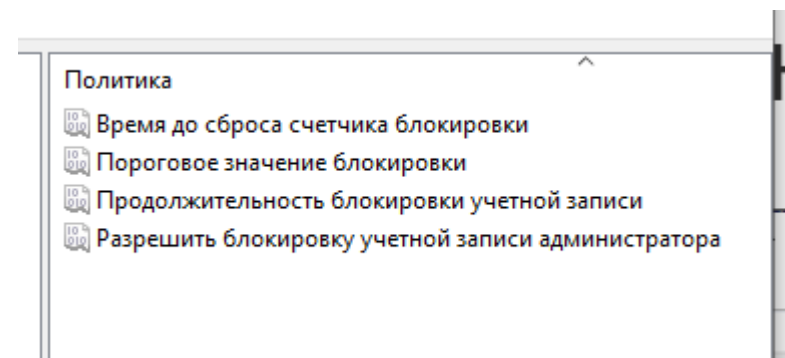
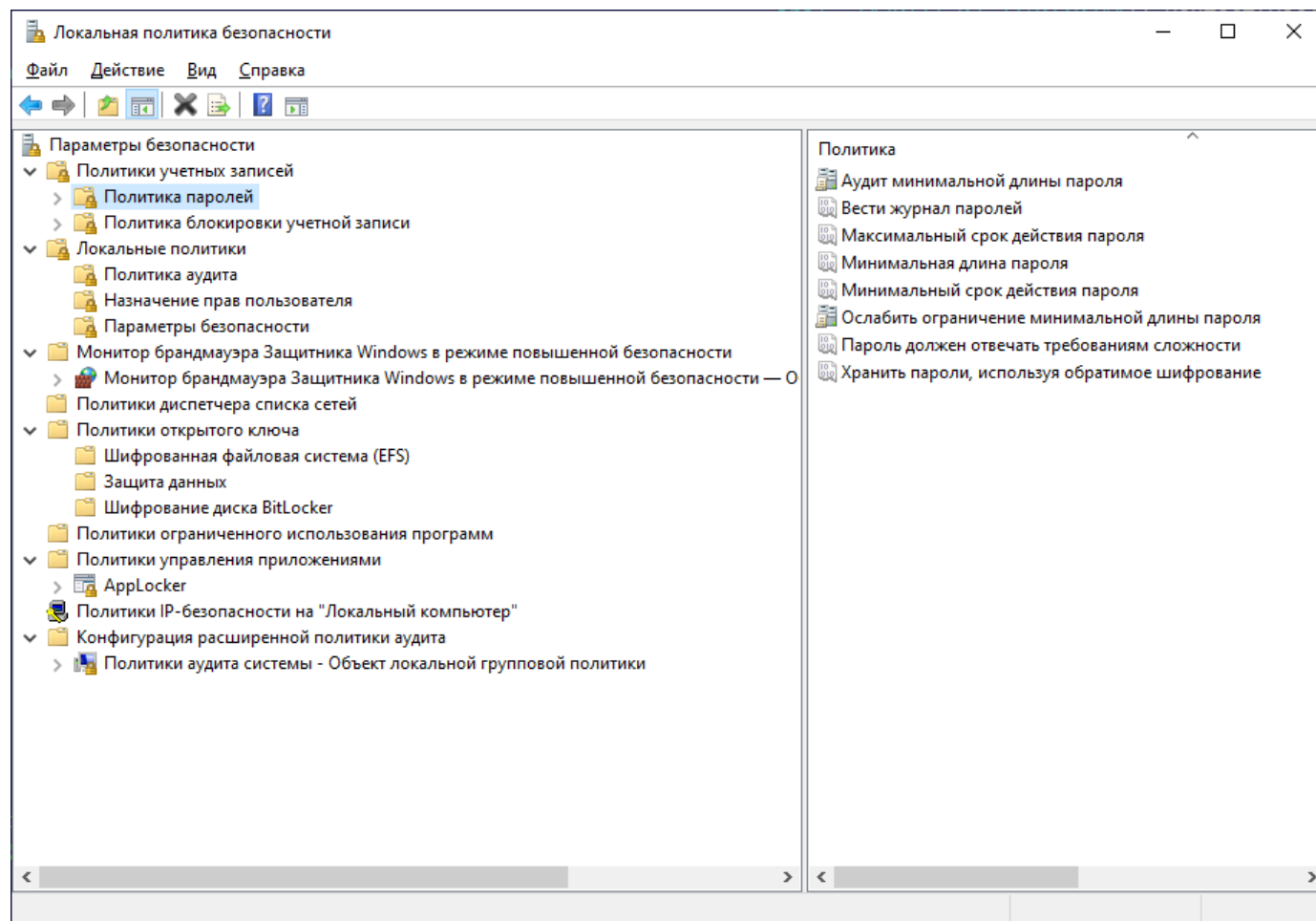
Вы также можете запустить на выполнение исполняемый файл с повышенными привилегиями. Для этого в контекстном меню ярлыка или самого исполняемого файла необходимо выбрать **«Запуск от имени администратора»**.

Что делать, если вам нужно на постоянной основе настроить приложение для работы с повышенными привилегиями, но запускаемое от имени стандартного пользователя?

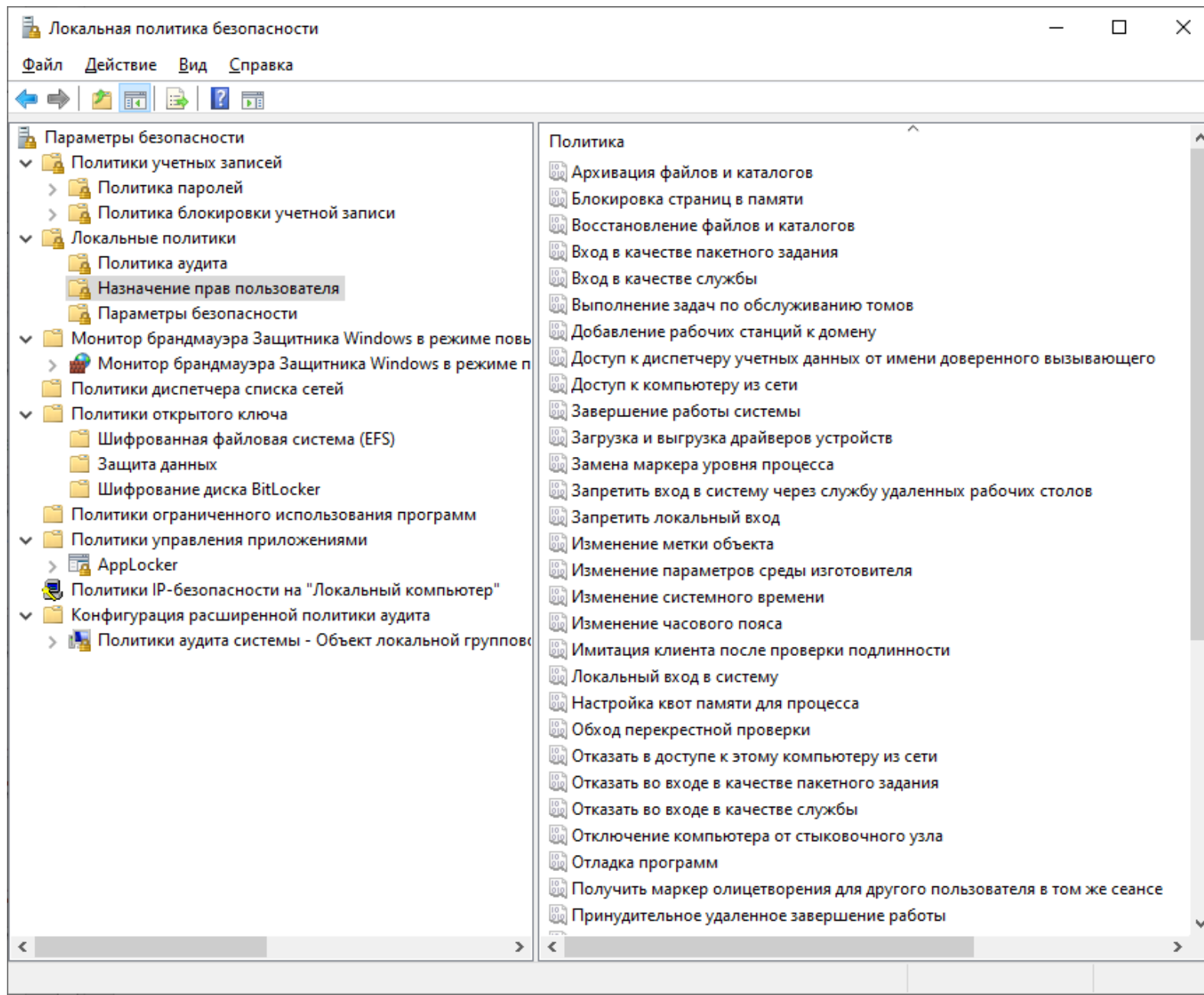
Для этого войдите в систему как администратор, откройте контекстное меню ярлыка или исполняемого файла и выберите **«Свойства»**. На вкладке **«Совместимость»** установите флажок **«Запускать эту программу от имени администратора»**.

Если флажок недоступен, программа заблокирована от постоянной работы от имени администратора, либо потому что программе не нужны административные привилегии или вы не вошли в систему как администратор.

# ПОЛИТИКИ БЕЗОПАСНОСТИ



# ПОЛИТИКИ БЕЗОПАСНОСТИ



# ПОЛИТИКИ БЕЗОПАСНОСТИ



Локальная политика безопасности

Файл Действие Вид Справка

Параметры безопасности

- Политики учетных записей
  - Политика паролей
  - Политика блокировки учетной записи
- Локальные политики
  - Политика аудита
  - Назначение прав пользователя
  - Параметры безопасности
- Монитор брандмауэра Защитника Windows в режиме пов...
- Политики диспетчера списка сетей
- Политики открытого ключа
  - Шифрованная файловая система (EFS)
  - Защита данных
  - Шифрование диска BitLocker
- Политики ограниченного использования программ
- Политики управления приложениями
  - AppLocker
- Политики IP-безопасности на "Локальный компьютер"
- Конфигурация расширенной политики аудита
  - Политики аудита системы - Объект локальной группов...

Политика	Параметр безопасн
Сетевая безопасность: не хранить хэш-значения LAN Manager при следующей смене пароля	Включен
Сетевая безопасность: ограничения NTLM: аудит входящего трафика NTLM	Не определено
Сетевая безопасность: ограничения NTLM: аудит проверки подлинности NTLM в этом домене	Не определено
Сетевая безопасность: ограничения NTLM: входящий трафик NTLM	Не определено
Сетевая безопасность: ограничения NTLM: добавить исключения для серверов в этом домене	Не определено
Сетевая безопасность: ограничения NTLM: добавить удаленные серверы в исключения проверки п...	Не определено
Сетевая безопасность: ограничения NTLM: исходящий трафик NTLM к удаленным серверам	Не определено
Сетевая безопасность: ограничения NTLM: проверка подлинности NTLM в этом домене	Не определено
Сетевая безопасность: Принудительный вывод из сеанса по истечении допустимых часов работы	Отключен
Сетевая безопасность: разрешить LocalSystem использовать нулевые сеансы	Не определено
Сетевая безопасность: разрешить использование сетевых удостоверений в запросах проверки под...	Не определено
Сетевая безопасность: разрешить учетной записи локальной системы использовать удостоверени...	Не определено
Сетевая безопасность: требование цифровой подписи для LDAP-клиента	Согласование цифр
Сетевая безопасность: уровень проверки подлинности LAN Manager	Не определено
Сетевой доступ: запретить анонимный доступ к именованным каналам и общим ресурсам	Включен
Сетевой доступ: модель общего доступа и безопасности для локальных учетных записей	Обычная - локальн
Сетевой доступ: не разрешать перечисление учетных записей SAM анонимными пользователями	Включен
Сетевой доступ: не разрешать перечисление учетных записей SAM и общих ресурсов анонимным...	Отключен
Сетевой доступ: не разрешать хранение паролей или учетных данных для сетевой проверки подли...	Отключен
Сетевой доступ: ограничить количество клиентов, которым разрешены удаленные вызовы SAM	Не определено
Сетевой доступ: разрешать анонимный доступ к именованным каналам	Не определено
Сетевой доступ: разрешать анонимный доступ к общим ресурсам	Не определено
Сетевой доступ: разрешать применение разрешений "Для всех" к анонимным пользователям	Отключен
Сетевой доступ: удаленно доступные пути и вложенные пути реестра	System\CurrentCont
Сетевой доступ: удаленно доступные пути реестра	System\CurrentCont
Сетевой сервер (Майкрософт): попытка S4U2Self получить информацию об утверждении	Не определено
Сетевой сервер (Майкрософт): уровень проверки сервером имени участника-службы конечного о...	Не определено
Системная криптография: использовать FIPS-совместимые алгоритмы для шифрования, хэширов...	Отключен
Системная криптография: обязательное применение сильной защиты ключей пользователей, хра...	Не определено



Локальная политика безопасности

Файл Действие Вид Справка

Параметры безопасности

Политики учетных записей

Политика паролей

Политика блокировки учетной записи

Локальные политики

Политика аудита

Назначение прав пользователя

Параметры безопасности

Монитор брандмауэра Защитника Windows в режиме пов...

Монитор брандмауэра Защитника Windows в режиме п...

Политики диспетчера списка сетей

Политики открытого ключа

Шифрованная файловая система (EFS)

Защита данных

Шифрование диска BitLocker

Политики ограниченного использования программ

Политики управления приложениями

AppLocker

Политики IP-безопасности на "Локальный компьютер"

Конфигурация расширенной политики аудита

Политики аудита системы - Объект локальной группово...

Политика

Сетевая безопасность: не хранить хэш-значения LAN Manager при следующей смене пароля

Сетевая безопасность: ограничения NTLM: аудит входящего трафика NTLM

Сетевая безопасность: ограничения NTLM: аудит проверки подлинности NTLM в этом домене

Сетевая безопасность: ограничения NTLM: входящий трафик NTLM

Сетевая безопасность: ограничения NTLM: добавить исключения для серверов в этом домене

Сетевая безопасность: ограничения NTLM: добавить удаленные серверы в исключения проверки п...

Сетевая безопасность: ограничения NTLM: исходящий трафик NTLM к удаленным серверам

Сетевая безопасность: ограничения NTLM: проверка подлинности NTLM в этом домене

Сетевая безопасность: Принудительный вывод из сеанса по истечении допустимых часов работы

Сетевая безопасность: разрешить LocalSystem использовать нулевые сеансы

Сетевая безопасность: разрешить использование сетевых удостоверений в запросах проверки под...

Сетевая безопасность: разрешить учетной записи локальной системы использовать удостоверени...

Сетевая безопасность: требование цифровой подписи для LDAP-клиента

Сетевая безопасность: уровень проверки подлинности LAN Manager

Сетевой доступ: запретить анонимный доступ к именованным каналам и общим ресурсам

Сетевой доступ: модель общего доступа и безопасности для локальных учетных записей

Сетевой доступ: не разрешать перечисление учетных записей SAM анонимными пользователями

Сетевой доступ: не разрешать перечисление учетных записей SAM и общих ресурсов анонимным...

Сетевой доступ: не разрешать хранение паролей или учетных данных для сетевой проверки подли...

Сетевой доступ: ограничить количество клиентов, которым разрешены удаленные вызовы SAM

Сетевой доступ: разрешать анонимный доступ к именованным каналам

Сетевой доступ: разрешать анонимный доступ к общим ресурсам

Сетевой доступ: разрешать применение разрешений "Для всех" к анонимным пользователям

Сетевой доступ: удаленно доступные пути и вложенные пути реестра

Сетевой доступ: удаленно доступные пути реестра

Сетевой сервер (Майкрософт): попытка S4U2Self получить информацию об утверждении

Сетевой сервер (Майкрософт): уровень проверки сервером имени участника-службы конечного о...

Системная криптография: использовать FIPS-совместимые алгоритмы для шифрования, хэширов...

Системная криптография: обязательное применение сильной защиты ключей пользователей, хра...

Параметр безопасн

Включен

Не определено

Не определено

Не определено

Не определено

Не определено

Не определено

Отключен

Не определено

Не определено

Согласование цифр

Не определено

Включен

Обычная - локальн

Включен

Отключен

Отключен

Не определено

Отключен

System\CurrentCont

System\CurrentCont

Не определено

Не определено

Отключен

Не определено