



RUDN
university

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук
Кафедра прикладной информатики и теории вероятностей

Презентация №2

Управление Пользователями в Windows

Студент: Эйвази Мани

Группа: НПИбд-03-24

Студенческий билет №: 1032245107

Управление Пользователями в Windows

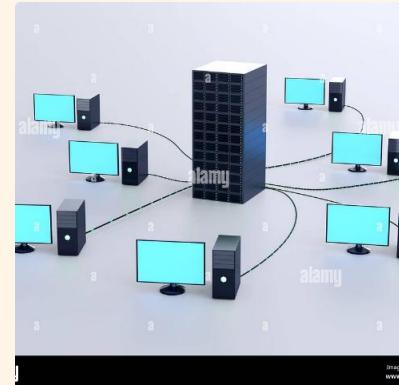
Основы администрирования
локальных учетных записей и групп



Локальные vs. Доменные Учетные Записи

Локальные учетные записи

Создаются и хранятся непосредственно на конкретном компьютере. Используются для доступа к ресурсам этого компьютера. Не требуют подключения к домену Active Directory. Идеальны для автономных машин или небольших рабочих групп без централизованного управления.



Доменные учетные записи

Создаются и управляются централизованно в Active Directory. Предоставляют доступ к ресурсам во всей доменной сети. Позволяют применять групповые политики и централизованно администрировать тысячи пользователей. Основной выбор для корпоративных сред.

Встроенные Учетные Записи Windows

Windows поставляется с несколькими предопределенными учетными записями, которые имеют особые функции и разрешения. Понимание их назначения критически важно для безопасности и эффективного управления системой.

Учетная запись "Администратор"

Обладает полными правами на управление локальным компьютером. Рекомендуется переименовывать эту учетную запись и использовать ее только для выполнения административных задач, а не для повседневной работы, чтобы минимизировать риски безопасности.

Учетная запись "Гость"

Предназначена для временного доступа пользователей, которым не требуется постоянная учетная запись. Имеет ограниченные права, запрещающие изменение системных настроек и установку программ. По умолчанию отключена в современных версиях Windows из соображений безопасности.

Создание и Удаление Локальных Пользователей

Основной инструмент для управления локальными пользователями и группами — оснастка "Локальные пользователи и группы" (`lusrmgr.msc`).

Через `lusrmgr.msc`

- Откройте "Выполнить" (`Win+R`) и введите `lusrmgr.msc`.
- В разделе "Пользователи" выберите "Действие" -> "Новый пользователь...".
- Заполните имя пользователя, полное имя, описание и задайте пароль. Определите опции пароля (например, "Сменить пароль при следующем входе").
- Для удаления пользователя выберите его и нажмите "Удалить".



❑ Использование оснастки является наиболее наглядным и удобным способом для ручного управления небольшим количеством учетных записей.

Управление Учетными Записями через Командную Строку

Для автоматизации или управления пользователями без графического интерфейса можно использовать команду `net user` в командной строке или PowerShell.



Создание
пользователя

```
net user username  
password /add
```

Например: net user testuser
P@ssw0rd! /add



Удаление
пользователя

```
net user username /delete
```

Например: net user testuser
/delete



Просмотр
информации

```
net user username
```

Например: net user Administrator



Изменение пароля

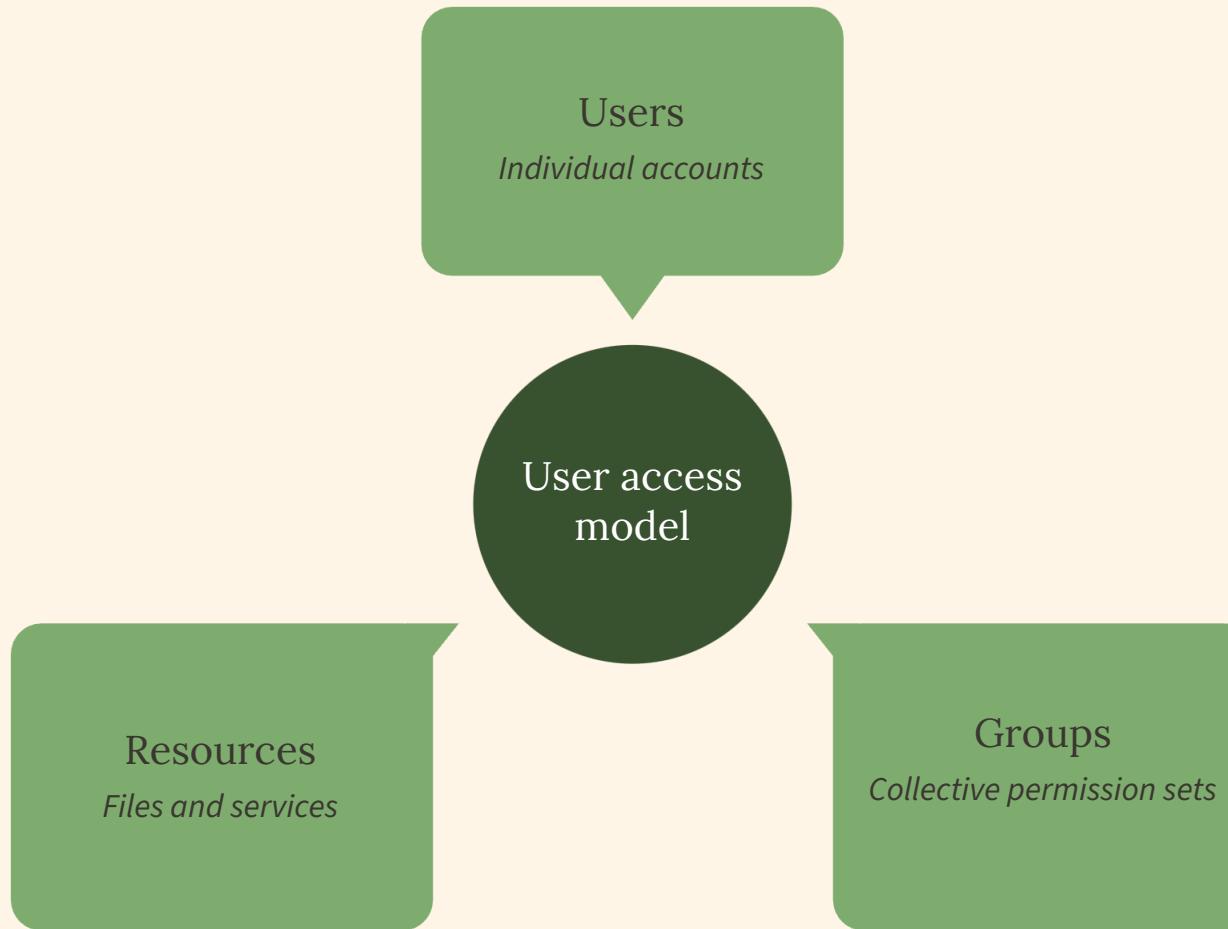
```
net user username  
password
```

Например: net user testuser
NewP@ssw0rd!

Команды `net user` предоставляют гибкий способ управления пользователями, особенно полезный для написания скриптов автоматизации.

Группы Пользователей: Назначение и Встроенные Группы

Группы пользователей упрощают управление разрешениями. Вместо того чтобы назначать права каждому пользователю, достаточно добавить пользователя в соответствующую группу.



Пользователи являются членами групп, а группам назначаются разрешения на доступ к различным системным ресурсам. Это значительно упрощает процесс администрирования.

Ключевые встроенные группы:

- **Администраторы (Administrators)**: Полный контроль над системой.
- **Пользователи (Users)**: Ограничены права для повседневной работы.
- **Гости (Guests)**: Очень ограниченные права, по умолчанию отключена.
- **Пользователи удаленного рабочего стола (Remote Desktop Users)**: Разрешен удаленный вход в систему.
- **Операторы настройки сети (Network Configuration Operators)**: Могут управлять сетевыми настройками.



Права и Разрешения: Разграничение Доступа

Разграничение доступа – фундаментальный аспект безопасности. Это процесс определения, кто и к каким ресурсам (файлам, папкам, принтерам, службам) имеет право доступа и какие действия он может выполнять.

1 NTFS-разрешения

Применяются к файлам и папкам на дисках с файловой системой NTFS. Позволяют точно контролировать доступ: чтение, запись, выполнение, изменение, полный доступ.

2 Разрешения общего доступа (Share Permissions)

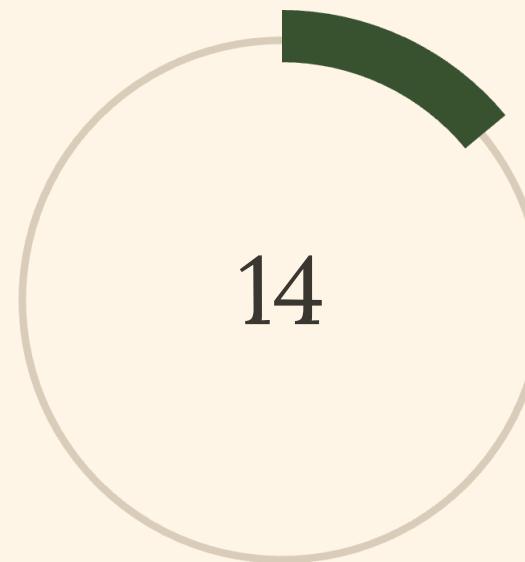
Применяются к сетевым папкам, доступ к которым осуществляется по сети. Обычно менее детализированы, чем NTFS-разрешения. Эффективные разрешения – это пересечение NTFS и Share Permissions.

3 Принцип наименьших привилегий

Пользователям и группам должны быть предоставлены только те права и разрешения, которые абсолютно необходимы для выполнения их задач. Это значительно снижает риски безопасности.

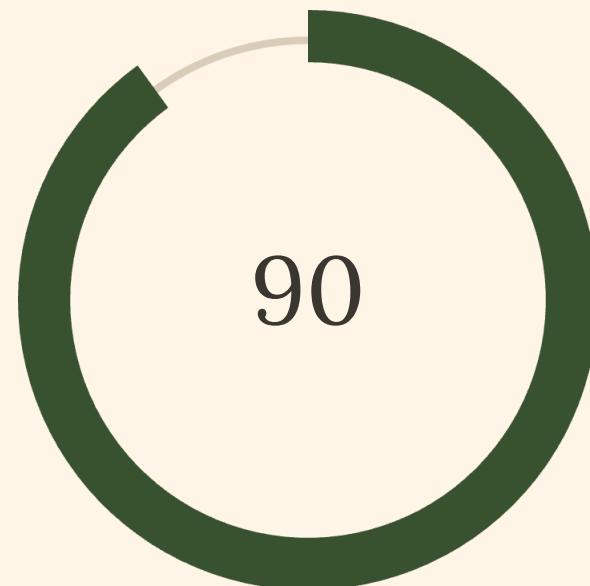
Политика Паролей и Блокировки Учетных Записей

Надежная политика паролей и меры по блокировке учетных записей являются первой линией защиты от несанкционированного доступа.



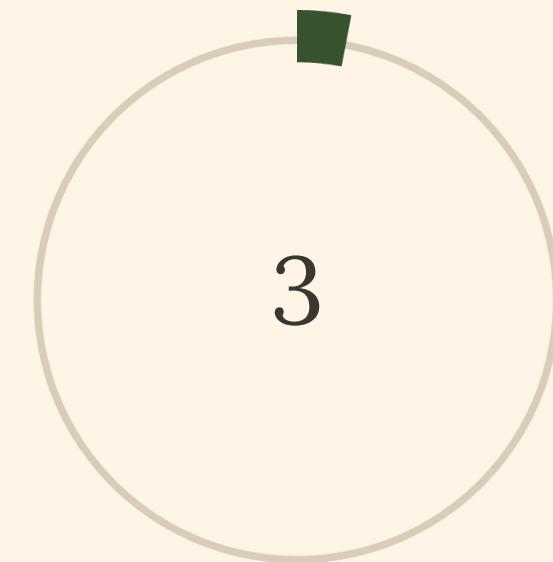
Минимальная длина пароля

*Рекомендованная длина для обеспечения
устойчивости к брутфорсу.*



Срок действия пароля (дней)

*Частота смены паролей для снижения риска
компрометации.*



Попытки входа до блокировки

*Количество неудачных попыток ввода пароля, после
которых аккаунт блокируется.*

- **Сложность пароля:** Пароли должны включать заглавные и строчные буквы, цифры и специальные символы.
- **История паролей:** Запрет использования ранее применявшихся паролей.
- **Продолжительность блокировки:** Время, на которое учетная запись блокируется после превышения лимита неудачных попыток входа.

Профили Пользователей

Профиль пользователя хранит все настройки рабочей среды: внешний вид рабочего стола, параметры проводника, сетевые подключения и т.д.



Локальный профиль

Создается при первом входе пользователя на конкретном компьютере и хранится на этом компьютере. Изменения сохраняются только на данной машине.



Перемещаемый профиль

Хранится на сетевом ресурсе и загружается на любой компьютер в домене, на который входит пользователь. Обеспечивает единую рабочую среду независимо от используемого ПК.



Обязательный профиль

Сетевой профиль, изменения в котором не сохраняются.

Применяется для создания стандартизованных рабочих мест, например, для общедоступных терминалов.

Спасибо за внимание