

# МДК.02.02 Организация администрирования компьютерных сетей 3-курс

Занятие 15, 16

**Создание групп и подразделений.  
Удаление пользователей, групп и  
подразделений.**

# Для чего нужны группы в домене

К одному из ключевых моментов концепции доменных служб Active Directory можно отнести обеспечение авторизации **принципов безопасности** для получения доступа к имеющимся сетевым ресурсам.

Несмотря на то, что весь доступ к сетевым ресурсам основан на **учетных записях** отдельных пользователей, компьютеров или служб, со временем **они могут меняться**.

В средних и крупных компаниях **управление** существующими пользователями требует **большой административной нагрузки**.

# Для чего нужны группы в домене

Стоит учесть, что **пользователи**, выполняющие в компании конкретную роль, **могут меняться**, но сама роль должна оставаться **без** каких-либо **изменений**.

Если назначать доступ к сетевым ресурсами индивидуально для каждого отдельного пользователя, то списки контроля доступа ACL вскоре станут **неуправляемыми**.

Если пользователь **сменит** один отдел на другой вам нужно будет **учесть** все возможные **разрешения доступа**.

Так как этот процесс может легко выйти из-под контроля, задачи, связанные с управлением должны быть **привязаны к объектам групп**.

# Для чего нужны группы в домене

Чаще всего группы используются для:

- идентификации ролей пользователей и компьютеров,
- фильтрации групповой политики,
- назначения уникальных политик паролей, прав, разрешений доступа, приложений электронной почты и многое другое.

Сами по себе, группы представляют собой принципы безопасности с уникальными **Идентификаторами безопасности** (Security Identifier или **SID**), которые могут содержать в атрибуте **member** такие принципы безопасности, как пользователи, компьютеры, группы и **контакты**.

# Для чего нужны группы в домене

Перед тем как создавать группы следует знать, какие существуют **разновидности** групп.

Так как структура доменных служб предназначена для поддержки сложных и крупных распределительных сред, Active Directory включает в себя:

- **два типа групп** домена с **тремя** областями действия в каждой из них,
- а также локальную группу **безопасности**.

Типы групп, а также их область действия подробно рассмотрены в следующих подразделах.

# Типы групп

В доменных службах Active Directory Windows Server можно отметить **два** типа групп:

- **безопасности и**
- **распространения.**

При создании новой группы в диалоговом окне  
«**Новый объект – группа**»

оснастки «**Active Directory – пользователи и компьютеры**» можно выбрать одну из этих двух групп.

Группы безопасности относятся к принципам безопасности с SID-идентификаторами (**Идентификаторами безопасности**).

# Типы групп

В связи с этим данный тип группы считается самым **распространенным** и группы такого типа можно использовать:

- для управления **безопасностью** и
- назначения **разрешений доступа** к сетевым ресурсам в списках ACL.

В общем, **группу безопасности** стоит использовать в том случае, если они будут использоваться для **управления безопасностью**.

Access Control List или ACL — список управления доступом, который определяет, кто или что может получать доступ к объекту (программе, процессу или файлу), и какие именно операции разрешено или запрещено выполнять субъекту (пользователю, группе пользователей).



# Типы групп

В свою очередь, **группа распространения** изначально используется приложениями электронной почты.

Она **не может** служить принципам **безопасности**.

Другими словами, этот тип группы не является субъектом безопасности.

Так как эту группу нельзя использовать для назначения доступа к ресурсам, она чаще всего используется при установке Microsoft Exchange Server в том случае, когда **пользователей** необходимо **объединить в группу** с целью отправки электронной почты **сразу всей группе**.

# Типы групп

Ввиду того, что именно группы **безопасности** вы можете использовать:

- как с целью назначения доступа к ресурсам,
- так и с целью распространения электронной почты,

многие организации используют только этот тип группы.

В домене с функциональным уровнем не ниже Windows 2000 можно **преобразовывать** группы безопасности в группы распространения и наоборот.

# Область действия групп

**Область действия** группы определяет диапазон, в котором применяется группа внутри домена.

Группы могут:

- содержать пользователей и компьютеры,
- быть членами других групп,
- ссылаться на списки ACL, фильтры объектов и групповых политик и прочее.

ACL (**Access Control List**) – это список управления доступом, который определяет, кто или что может получать доступ к объекту (программе, процессу или файлу), и какие именно операции разрешено или запрещено выполнять субъекту (пользователю, группе пользователей).

# Область действия групп

**Граница** диапазона области действия группы может определяться **заданием режима** работы домена.

К основным характеристикам области действия групп можно отнести такие как:

- членство (определение принципов безопасности, которые может содержать группа),
- репликация — это процесс, под которым понимается **копирование** данных из одного источника на другой (определение области репликации группы),
- доступность (определение местонахождения группы, возможности включения этой группы в членство другой, добавление группы в список ACL).

# Область действия групп

Существует четыре **области действия** групп:

- локальная,
- локальная в домене,
- глобальная и
- универсальная.

Рассмотрим подробнее каждую из них.

# Область действия групп

## Локальная группа.

Локальная группа считается самой **примитивной**, так как она так доступна только на одном компьютере.

Такая группа создается в базе данных диспетчера безопасности учетных записей рядового компьютера и поэтому в домене управление локальными группами не нужно.

В списках ACL можно использовать такие группы только на **локальном компьютере**.

В другие системы такие группы не реплицируются, но эта группа содержит пользователей, компьютеры, глобальные и локальные группы в домене в своем домене, пользователей, компьютеры и глобальные и универсальные группы в любом домене леса.

# Область действия групп

**Локальная группа в домене.**

**Группы с областью локальные группы** в домене предназначены для управления разрешениями доступа к ресурсам и функционируют в том случае, если домен работает на функциональном уровне не ниже Windows 2000.

В том случае, если домен работает на уровне Windows NT или в смешанном уровне, то эти группы будут использоваться лишь как локальные группы.

Такая группа определяется в контексте именования домена.

**Локальную группу** в домене можно добавлять в списки ACL любого ресурса **на любом рядовом компьютере** домена.

# Область действия групп

В локальную группу в домене могут входить пользователи, компьютеры, глобальные и локальные группы в текущем домене, любом другом домене леса, а также универсальные группы в любом домене леса.

Другими словами, репликация и доступность такой группы **позволяет её использовать в пределах всего домена.**

В связи с этим, локальные группы в домене обычно используют для предоставления **правил доступа** во всем домене, а также для членов доверительных доменов.

Чаще всего, с локальными группами в домене связаны сценарии, подобные следующему: нужно предоставить **доступ** к папке с секретной документацией **восьми** пользователям из разных отделов.



# Область действия групп

Нужно учесть, что кто-либо из этих пользователей может **перейти** в другой отдел или **уволиться** и позже вам придется изменять разрешения доступа на принтере.

А если доступ нужно предоставить **не восьми**, а восьмидесяти пользователям из разных подразделений и доменов?

Поэтому, **чтобы упростить** такую рутинную работу вы можете создать **группу** с локальной областью безопасности в домене и **разрешить доступ** к папке именно этой **группе**.

После этого вы можете **добавлять**, любых пользователей из этой группы и все пользователи, входящие в состав этой группы автоматически получают доступ к папке;

# Область действия групп

## Глобальная группа.

Основной целью глобальных групп безопасности является определение коллекции объектов доменов на основании бизнес-правил и управление объектами, которые требуют ежедневного использования.

Чаще всего, членами таких групп выступают пользователи и компьютеры.

Группы безопасности удобно использовать для фильтрации области действия групповых политик, так как область действия таких групп не реплицируется за пределы своего домена, при этом не вызывая дополнительного трафика к глобальному каталогу.

# Область действия групп

Глобальная группа может содержать пользователей, компьютеры и другие глобальные группы **только из одного домена**.

Несмотря на это, глобальные группы могут быть членами любых универсальных и локальных групп как в своем домене, так и доверяющем домене.

Помимо этого, глобальные группы можно добавлять в списки ACL в домене, лесу и в доверяющем домене, что делает управление группами более простым и рациональным;

# Область действия групп

## Универсальная группа.

Универсальные группы целесообразно задействовать только в лесах, состоящих из множества доменов для их объединения.

Эти группы позволяют управлять ресурсами, распределенными **на нескольких доменах**, поэтому универсальные группы считаются самыми **гибкими**.

Универсальные группы определяются в одном домене, но реплицируются в глобальный каталог.

# Область действия групп

Например, для того чтобы **получить** пользователям из домена В **доступ** к ресурсам, расположенным в домене А, нужно **добавить** учетные записи пользователей домена В в глобальные группы безопасности.

Затем эти группы нужно **вложить** в универсальную группу.

Универсальная группа может быть членом другой универсальной или локальной группы домена в лесу.

Также Универсальная группа может использоваться для управления ресурсами;

# Область действия групп

В некоторых случаях перед вами может встать необходимость **преобразования** одной области действия в другую.

Например, в связи с тем, что по умолчанию при создании группы **фокус установлен** на глобальной группе безопасности.

По **невнимательности** можно оставить все без изменений и создать группу.

После создания группы, ее область действия можно изменить на вкладке «**Общие**» диалогового окна свойств группы, одним из следующих доступных способов:

# Область действия групп

- **Глобальную** группу в **универсальную** в том случае, если изменяемая группа не является членом другой глобальной группы;
- **Локальную** группу в домене в **универсальную** в том случае, если эта группа не содержит другую локальную группу в домене в качестве члена;
- **Универсальную** группу в **глобальную** в том случае, если эта группа не содержит в качестве члена другую универсальную группу;
- **Универсальную** группу в **локальную** группу в домене.

# Область действия групп

Как можно было заметить, **глобальную** группу просто так невозможно модифицировать в **локальную** группу в домене.

Несмотря на это, можно сначала **глобальную** группу преобразовать в **универсальную**, а затем уже получившуюся **универсальную** группу – в **локальную** группу в домене.

На первый взгляд все эти области групп могут показаться **одинаковыми**, но для наилучшего понимания их использования можно рассмотреть простой пример.

Допустим, есть два домена.

На первом домене (домен **A**) есть папка, для которой должен быть предоставлен доступ сотрудникам отдела продаж обоих доменов.



# Область действия групп

В домене **A**, доступ к этой папке могут получить любые пользователи, но для более рационального использования пользователей, которым должен предоставляться доступ можно поместить их в **глобальную** группу безопасности.

Но **глобальная** группа «Продажи» домена **B** не может получать доступ к папке в домене **A**.

Поэтому **глобальную** группу «Продажи» из домена **B** нужно включить в **универсальную** группу, скажем «Доступ к ресурсам домена **A**».

# Область действия групп

Затем, в домене **A** нужно создать **локальную** группу в домене (например, «Доступ к секретным материалам»), так как **универсальная** группа не может быть членом **глобальной** группы.

Теперь нужно включить в **локальную** группу «Доступ к секретным материалам» **глобальную** группу «Продажи» из домена **A** и **универсальную** группу «Доступ к ресурсам домена **A**» домена **B**.

Только после этого, члены групп «Продажи» из обоих доменов **будут иметь разрешения** на использование секретных документов, расположенных в домене **A**.

# Область действия групп

Для того, чтобы **запомнить** все эти связи – вы можете просто запомнить интересный термин: AGUDLP, что расшифровывается как:

«Account - Global - Universal - Domain Local – Permissions» (Учетная запись – Глобальная – Универсальная – Локальная в домене - Доступ),

то есть запомнив эту аббревиатуру вы не ошибетесь при назначении доступа к любым ресурсам.

Стратегию AGUDLP рекомендует, например, Компания Microsoft.

С помощью этой **стратегии** можно легко управлять разрешениями и правами в большой компании.

# Область действия групп

Другими словами, **учетные записи** пользователей добавляются в **глобальные** группы, а **глобальные** группы добавляются в **локальные** группы, а **локальным** группам предоставляется доступ к ресурсам.

Организация такой стратегии на предприятие позволит системному администратору намного **упростить** управление правами и разрешениями.

Преимущества:

- удобство,
- сокращение времени на изменение прав и разрешений.

Не зря **глобальные** группы называют **учетными**, а **локальные** **ресурсными**.

# Область действия групп

Но если это для Вас сложно или Вы думаете что это просто не нужно, то можно использовать стратегию AGP, т.е.

**глобальной** группе **предоставлять доступ** к ресурсам, а в свою очередь в **глобальную** группу **добавлять** пользователей.

На эту тему можно говорить и спорить долгое время.

В качестве небольшого подведения итогов стоит сказать, что создание групп в Active Directory всегда оказывается очень **полезным!**

Группы нужно **использовать**, с помощью вышеперечисленных стратегий, или какой-то другой, например, своей собственной стратегии.

# Создание группы в домене

Чаще всего при создании:

- учетные записи пользователей,
- создании группы

используется функционал оснастки «**Active Directory – пользователи и компьютеры**».

Этот способ обладает графическим интерфейсом, который позволяет корректно создать группу любого типа и с любой областью действия.

С ним может легко **справиться** даже начинающий системный администратор, который открыл данную оснастку впервые.

# Создание группы в домене

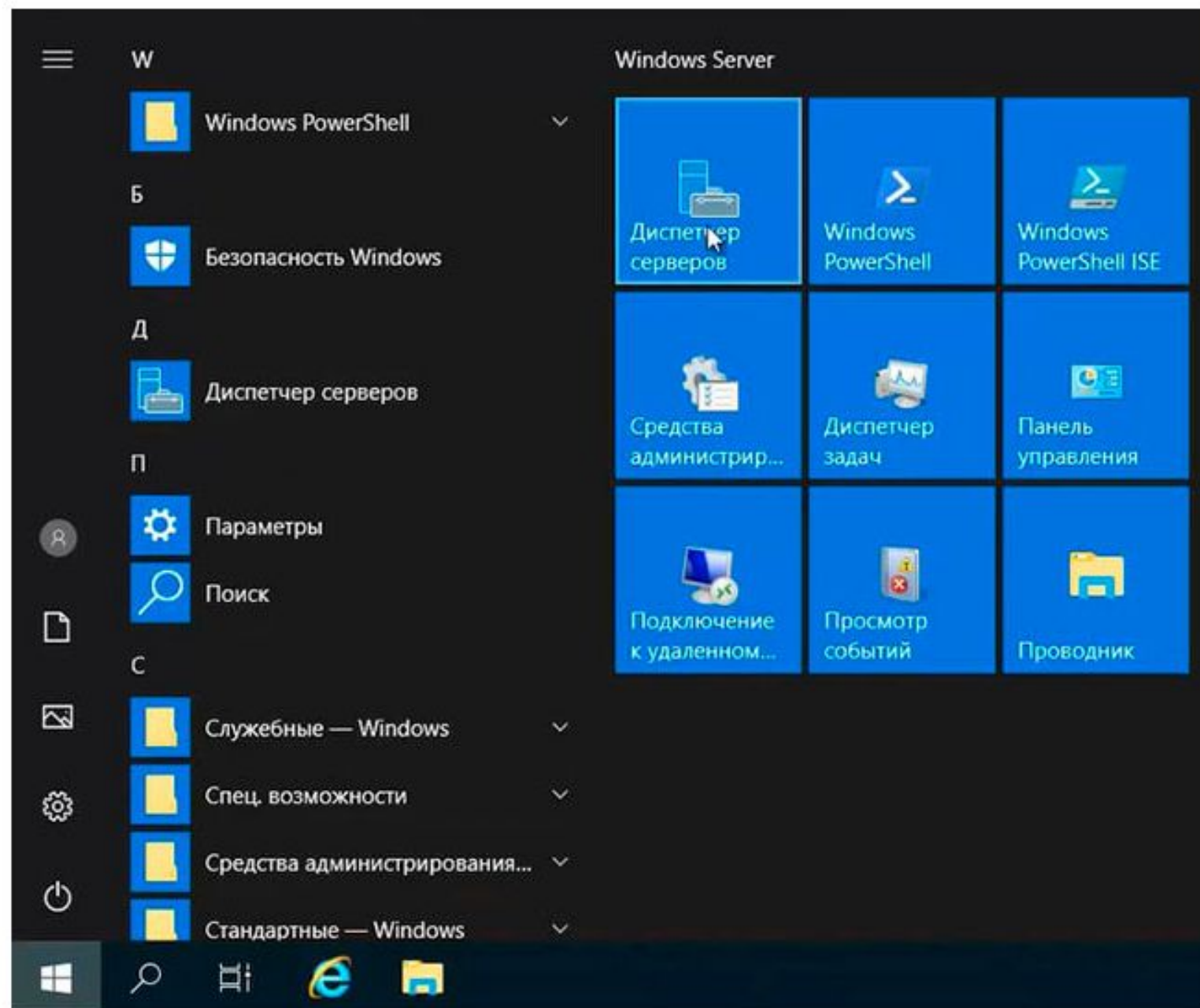
После того, как установлена роль **Active Directory** в домене **Windows Server**, появляется возможность **управления доменом**.

Далее можно создать:

- пользователей, которые будут входить под учетными записями,
- группы и
- подразделения.

Как создавать новых пользователей, мы уже рассматривали.

Теперь разберём, как создавать **группы и подразделения**





# Создание группы в домене

Для создания или удаления **группы** пользователей воспользуемся средством централизованного управления сервером – «**Диспетчер серверов**».

Для этого на сервере нажимаем:

- кнопку «**Пуск**»,
- далее выбираем «**Диспетчер серверов**».

При этом в новом окне откроется «**Диспетчер серверов**».

Диспетчер серверов

« Панель мониторинга

Управление Средства Вид Справка

Панель мониторинга

- Локальный сервер
- Все серверы
- AD DS
- DHCP
- DNS
- Файловые службы и сл...

Вас приветствует диспетчер серверов

Быстрый запуск

Что нового

Подробнее

РОЛИ И ГРУППЫ СЕРВЕРОВ

Роли: 4 | Группы серверов: 1 | Всего серверов: 5

AD DS	1
Управляемость	
События	

1 Наст...

2 До...

3 До...

4 Со...

5 По...

- Active Directory - домены и доверие
- Active Directory — сайты и службы
- DHCP
- DNS
- ODBC Data Sources (32-bit)
- Windows PowerShell
- Windows PowerShell (x86)
- Windows PowerShell ISE
- Windows PowerShell ISE (x86)
- Диск восстановления
- Инициатор iSCSI
- Источники данных ODBC (64-разрядная версия)
- Конфигурация системы
- Локальная политика безопасности
- Модуль Active Directory для Windows PowerShell
- Монитор брандмауэра Защитника Windows в режиме повышенной безопасности
- Монитор ресурсов
- Оптимизация дисков
- Очистка диска
- Планировщик заданий
- Пользователи и компьютеры Active Directory**
- Просмотр событий
- Редактирование ADSI

11:17 23.04.2019 ENG

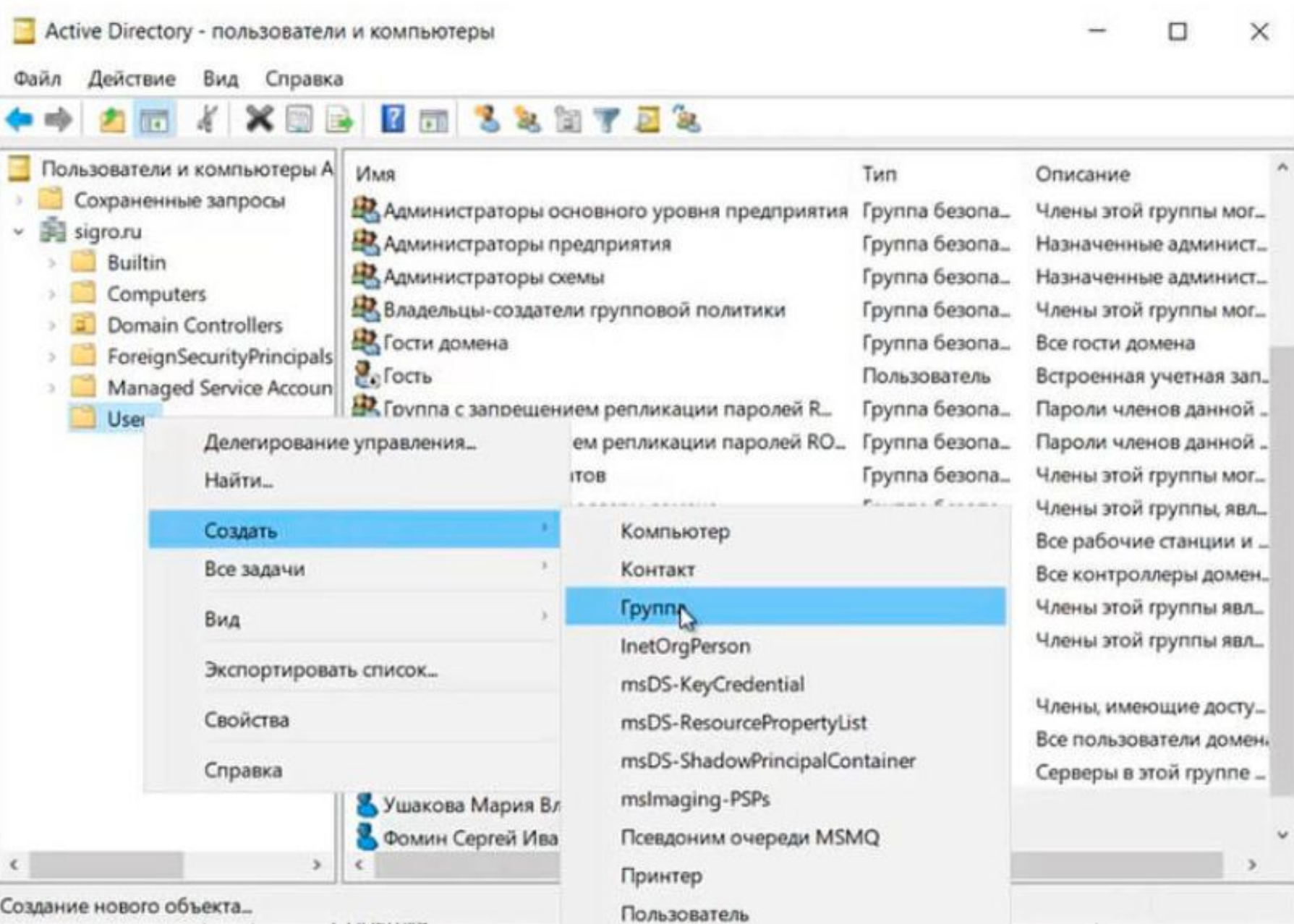
# Создание группы в домене

В открывшемся новом окне вверху слева находим и нажимаем «**Средства**».

Далее в открывшемся списке выбираем «**Пользователи и компьютеры Active Directory**».

При этом откроется новое окно:

«**Active Directory – пользователи и компьютеры**».



# Создание группы в домене

В открывшемся новом окне

«**Active Directory – пользователи и компьютеры**»

находим папку «**Users**», нажимаем правой клавишей мыши, в выпадающем меню выбираем

«**Создать**», далее

«**Группа**».

Новый объект - Группа



Создать в: sigro.ru/Users

Имя группы:

Department1

Имя группы (пред-Windows 2000):

Department1

Область действия группы

- ☐ Локальная в домене
- ☒ Глобальная
- ☐ Универсальная

Тип группы

- ☒ Группа безопасности
- ☐ Группа распространения

OK

Отмена

# Создание группы в домене

Откроется новое окно:

«**Новый объект - Группа**».

В этом окне задаём «**Имя группы**»,

Далее выбираем в разделе «**Область действия группы**» один из вариантов:

- Локальная в домене;
- Глобальная,
- Универсальная.

Например, можно выбрать «**Глобальная**».

# Создание группы в домене

В разделе «**Тип группы**» всего два варианта:

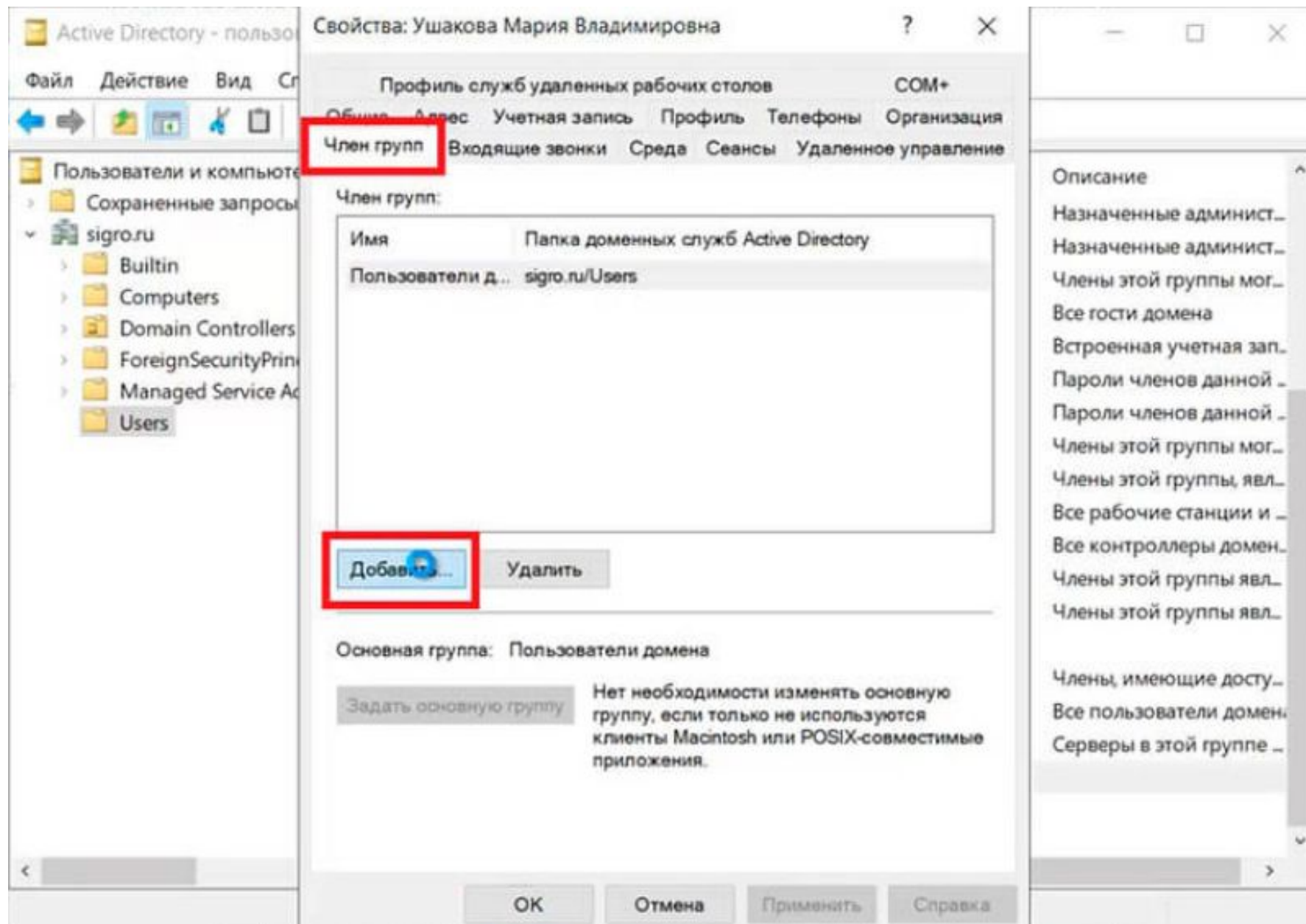
- Группа безопасности;
- Группа распространения.

В качестве примера выбираем «**Группа безопасности**».

Далее нажимаем «**ОК**».

После чего будет создана группа с тем именем, которое мы указали.





# Создание группы в домене

Теперь необходимо **добавить пользователя** в группу.

Для этого в окне:

**«Active Directory – пользователи и компьютеры»**

находим папку **«Users»**, заходим в неё, открываем пользователя, выбираем вкладку:

**«Член групп»**, нажимаем кнопку:

**«Добавить»**.

Выбор: "Группы"



Выберите тип объекта:

"Группы" или "Встроенные субъекты безопасности"

Типы объектов...

В следующем месте:

sigro.ru

Размещение...

Введите имена выбираемых объектов ([примеры](#)):

Department1

Проверить имена

Дополнительно...

ОК

Отмена

# Создание группы в домене

Откроется окно «**Выбор “Группы”**».

В этом окне вводим **имя группы**, в которую будет добавлен пользователь.

Проверяем нажав кнопку «**Проверить имена**», далее нажимаем «**ОК**».

После этого пользователь добавлен в группу!

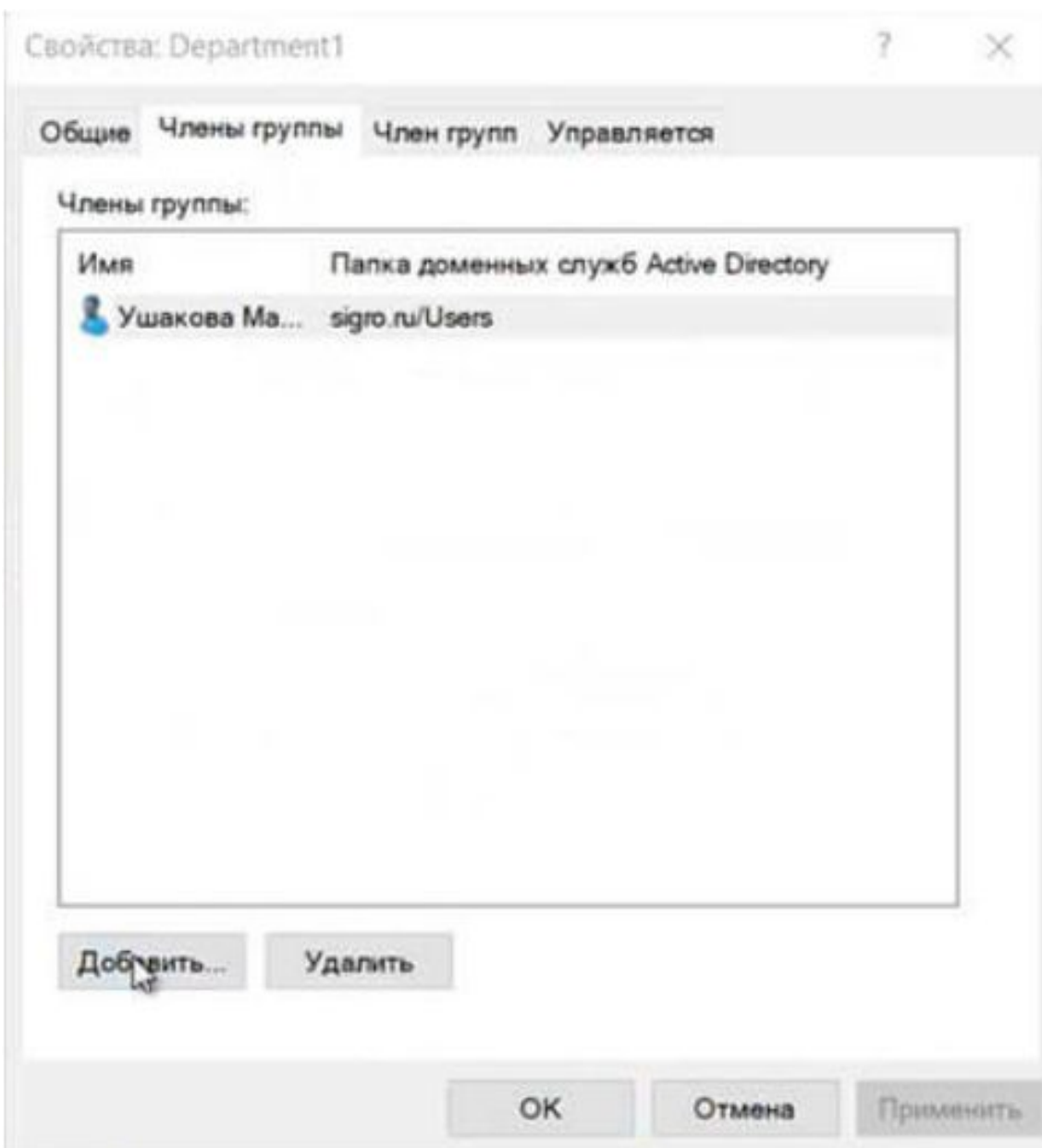
# Создание группы в домене

Можно **добавить пользователя** в группу другим способом.

Для этого в окне:

**«Active Directory – пользователи и компьютеры»**

находим нужную группу.



# Создание группы в домене

Откроется окно «**Свойства “Группы”**».

Далее выбираем вкладку «**Члены группы**».

Нажимаем «**Добавить**».

Выбор: "Пользователи", "Контакты", "Компьютеры", "Учетные записи служ..." X

Выберите тип объекта:

"Пользователи", "Учетные записи служб", "Группы" или "Другие"

Типы объектов...

В следующем месте:

sigro.ru

Размещение...

Введите имена выбираемых объектов ([примеры](#)):

Фомин Сергей Иванович (FominSI@sigro.ru)

Проверить имена

Дополнительно...

OK

Отмена



# Создание группы в домене

В новом окне вводим имена пользователей, которые будут добавлены в группу.

Проверяем нажав клавишу «**Проверить имена**», далее «**ОК**».

# Создание подразделения в домене

**Организационное подразделение** (Organizational Unit — OU) представляет собой контейнер в домене Active Directory.

Организационное подразделение может содержать различные объекты из того же самого домена AD:

- другие контейнеры,
- группы,
- аккаунты пользователей и компьютеров.

Организационное подразделение представляет собой единицу административного управления внутри домена, на который администратор может назначить объекты групповых политик и назначить разрешения другим пользователям.

# Создание подразделения в домене

Выделим две основные задачи использования **Организационного подразделения** кроме хранения объектов Active Directory:

- Делегирование управления и административных задач внутри домена другим администраторам и обычным пользователям без предоставления им прав администратора домена;
- Назначение групповых политик на все объекты (пользователей и компьютеры), которые находятся в данном подразделении (OU).



# Создание подразделения в домене

Чтобы создать подразделение в домене нужно зайти в «**Active Directory – пользователи и компьютеры**».

Находим **домен**, нажимаем на него правой клавишей мыши.

В появившемся меню выбираем:

«**Создать**», далее выбираем

«**Подразделение**».

Новый объект - Подразделение



Создать sigro.ru/

Имя:

Department1

☒ Защитить контейнер от случайного удаления

OK

Отмена

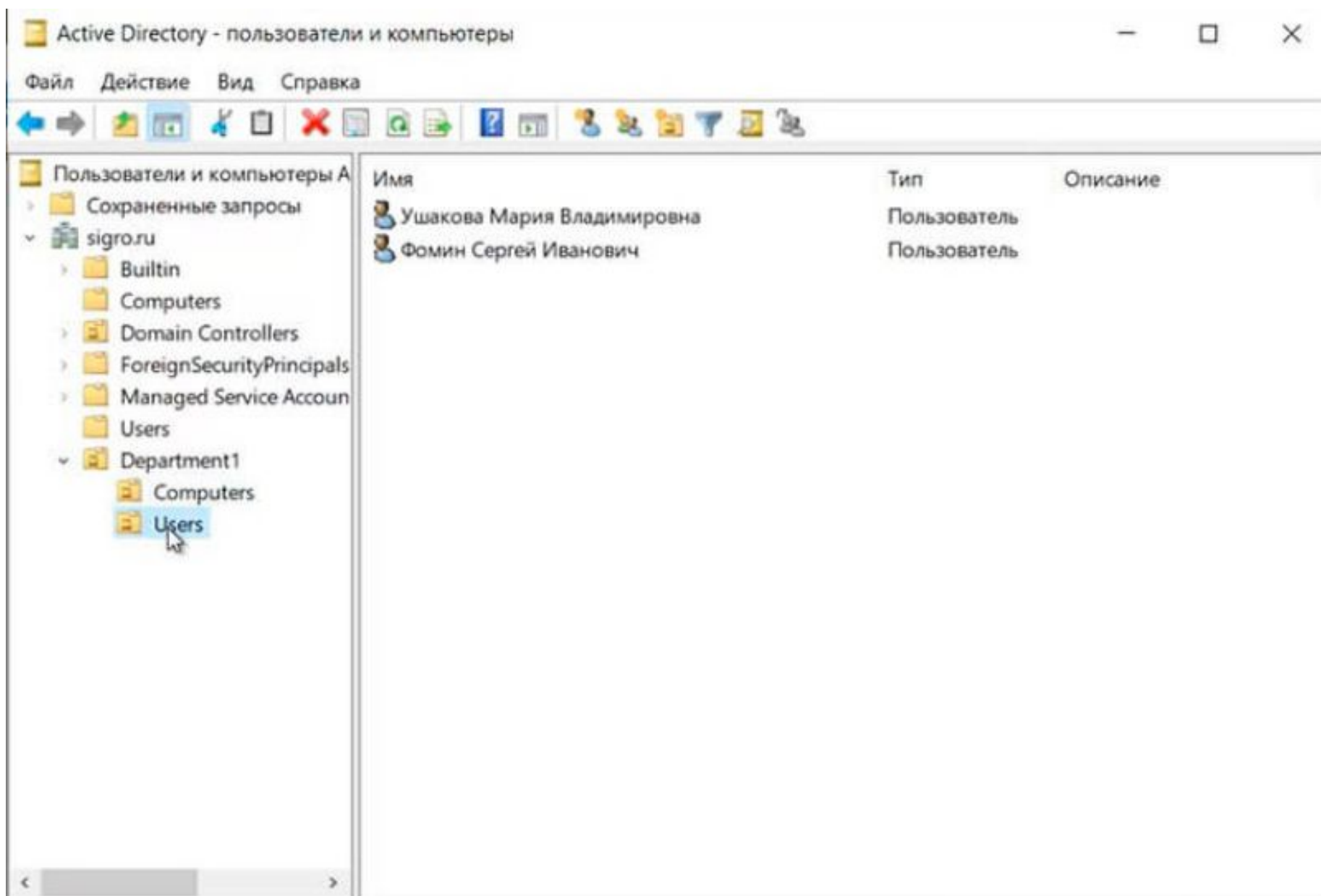
Справка

# Создание подразделения в домене

Появится новое окно:

**«Новый объект - Подразделение».**

Здесь необходимо задать имя подразделения и нажать **«ОК»**.





# Создание подразделения в домене

Если это необходимо, то в созданном подразделении можно аналогичным образом создать **вложенные подразделения**.

Далее в созданные **вложенные подразделения** можно перенести или создать различные объекты:

- пользователи,
- компьютеры,
- группы.

# Список литературы:

1. Беленькая М. Н., Малиновский С. Т., Яковенко Н. В. Администрирование в информационных системах. Учебное пособие. - Москва, Горячая линия - Телеком, 2011.
2. Компьютерные сети. Принципы, технологии, протоколы, В. Олифер, Н. Олифер (5-е издание), «Питер», Москва, Санк-Петербург, 2016.
3. Компьютерные сети. Э. Таненбаум, 4-е издание, «Питер», Москва, Санк-Петербург, 2003.
4. <https://bigro.ru/system/170-win2019-create-user-group-object.html>
5. <http://www.oszone.net/13435/>

# Список ссылок:

<https://>

# Благодарю за внимание!

Преподаватель: Солодухин Андрей Геннадьевич

Электронная почта: [asoloduhin@kait20.ru](mailto:asoloduhin@kait20.ru)