БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

Ханты-Мансийского автономного округа – Югры

«Сургутский государственный университет»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Политехнический институт

Кафедра автоматизированных систем обработки информации и управления

Принят комиссией кафедры

«\_\_\_» «\_\_\_\_\_\_\_\_\_\_» 2025\_\_\_г.

Зав. кафедрой АСОИУ

\_\_\_\_\_\_\_\_\_\_\_Бушмелева К.И.

(подпись) (инициалы и фамилия)

**ОТЧЁТ**

**По Производственной практике, технологической (проектно-технологической) практике**

В Сургутском государственном университете, кафедре АСОИУ

студентки 4 курса 606-11з группы

Хорина Вера Юрьевна \_\_\_\_\_\_\_\_\_\_

(подпись)

По теме «Изучение информационной системы управления учетными записями пользователей и устройствами печати»

|  |  |
| --- | --- |
| Руководитель практики от  предприятия  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (должность)  \_\_\_\_\_\_\_\_\_\_\_\_ Калачикова Е.П.  (подпись) (инициалы и фамилия) | Руководитель практики от  университета  ассистент  (должность)  \_\_\_\_\_\_\_\_\_\_\_\_ Калачикова Е.П.  (подпись) (инициалы и фамилия) |

Сургут, 2025

Содержание

[ВВЕДЕНИЕ 3](#_Toc198641466)

[1. ACTIVE DIRECTORY: СИСТЕМА УПРАВЛЕНИЯ УЧЕТНЫМИ ЗАПИСЯМИ 5](#_Toc198641467)

[1.1 Архитектура и принципы работы Active Directory 5](#_Toc198641468)

[1.2 Управление учетными записями и группами пользователей 8](#_Toc198641469)

[1.3 Механизмы авторизации и разграничения доступа 11](#_Toc198641469)

[2. СЛУЖБА ПЕЧАТИ WINDOWS SERVER 14](#_Toc198641470)

[2.1 Архитектура службы печати в среде Windows Server 14](#_Toc198641471)

[2.2 Классификация политик доступа к принтерам 16](#_Toc198641472)

[3. ПРИМЕНЕНИЕ СИСТЕМ ACTIVE DIRECTORY И WINDOWS SERVER 20](#_Toc198641470)

[3.1 Создание учетных записей пользователей в Active Directory 20](#_Toc198641471)

[3.2 Настройка групп и прав доступа в домене 21](#_Toc198641472)

[3.3 Добавление и настройка сетевых принтеров 23](#_Toc198641472)

[3.4 Мониторинг и управление печатью 26](#_Toc198641472)

[ЗАКЛЮЧЕНИЕ 29](#_Toc198641473)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 30](#_Toc198641474)

# ВВЕДЕНИЕ

Современные организации используют централизованные системы управления пользователями и ресурсами, чтобы повысить эффективность и безопасность ИТ- инфраструктуры. Одной из ключевых технологий является служба каталогов Microsoft Active Directory (AD), которая обеспечивает хранение и организацию данных об учетных записях пользователей, компьютеров и других объектов сети, а также предоставляет средства для аутентификации и авторизации доступа к ресурсам. Active Directory позволяет администраторам централизованно управлять учетными записями и политиками, применять единые настройки безопасности и конфигурации на всех компьютерах домена. Одновременно с управлением пользователями важным аспектом инфраструктуры является организация печати в сети. Служба печати Windows Server (Print and Document Services) дает возможность централизованно развертывать и настраивать сетевые принтеры, контролировать очереди печати и разграничивать доступ пользователей к устройствам печати. Внедрение серверов печати позволяет оптимизировать использование печатных ресурсов и облегчает поддержку, по сравнению с локальной установкой принтеров на каждом ПК. Таким образом, тема управления учетными записями пользователей и устройствами печати с помощью Active Directory и Windows Server является актуальной для обеспечения эффективной и безопасной работы корпоративных информационных систем.

Цель практики – изучить информационную систему управления учетными записями пользователей и устройствами печати на примере Microsoft Active Directory и службы печати Windows Server в условиях корпоративной сети.

Исходя из поставленной цели, были определены следующие задачи практики:

1. Рассмотреть архитектуру и принцип работы Active Directory как основной системы управления учетными записями в доменной среде;
2. Изучить способы управления учетными записями пользователей и группами в Active Directory;
3. Исследовать механизмы авторизации пользователей в домене и методы разграничения доступа к ресурсам с помощью AD;
4. Изучить архитектуру службы печати Windows Server и ее интеграцию с Active Directory;
5. Дать классификацию и описание политик доступа к сетевым принтерам в Windows-среде;
6. На практике выполнить настройку доменной инфраструктуры.

Объект исследования: информационная система управления учетными записями и сетевыми ресурсами на базе Microsoft Active Directory и Windows Server (на примере инфраструктуры Сургутского государственного университета).

Предмет исследования: методы управления учетными записями пользователей и устройствами печати в доменной сети Windows.

Методы исследования: анализ специализированной литературы и технической документации Microsoft, изучение практических руководств, а также выполнение практических действий по настройке Active Directory и службы печати в учебном стенде.

Структура отчёта: введение, две главы теоретической части, содержащие пять подразделов, практическая часть с последовательным описанием выполнения задач, заключение и список использованных источников.

## 1. ACTIVE DIRECTORY: СИСТЕМА УПРАВЛЕНИЯ УЧЕТНЫМИ ЗАПИСЯМИ

## Архитектура и принципы работы Active Directory.

Active Directory (AD) – это служба каталогов корпорации Microsoft для операционных систем Windows Server, предназначенная для хранения информации об объектах в сети и организации этой информации в иерархическом виде. В архитектуре Active Directory реализована многоуровневая модель, которая включает логическую и физическую структуру.

Логическая структура AD состоит из лесов, деревьев, доменов и подразделений (OU). Лес (forest) – это совокупность всех объектов и правил каталога AD, представляющая предельную границу безопасности. В пределах леса может быть один или несколько деревьев доменов, связанных транзитивными отношениями доверия. Каждое дерево включает один или несколько доменов. Домен – основная административная единица AD, представляющая группу объектов (пользователи, компьютеры, группы и пр.), объединённых общей базой данных каталога и политиками безопасности. Домен также является границей репликации и единицей, в пределах которой действуют определённые настройки безопасности и учетные данные. Объекты домена организуются в иерархии путем использования организационных подразделений (OU) – логических контейнеров, предназначенных для объединения объектов по организационному или функциональному признаку. Подразделения позволяют делегировать административные полномочия на нижнем уровне и часто служат для целенаправленного применения групповых политик. На рис. 1 показана упрощённая логическая структура каталога Active Directory.

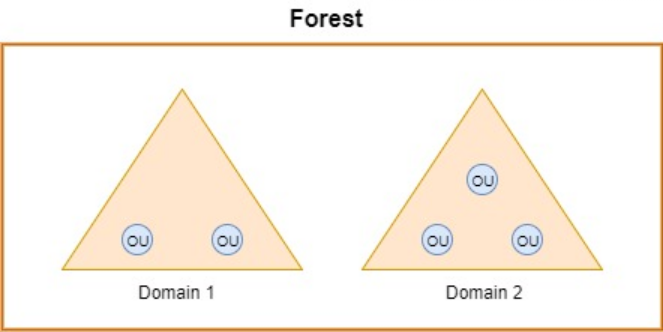


Рисунок 1 - Логическая структура Active Directory.

Каталог Active Directory хранит информацию об объектах сети в виде записей в специализированной базе данных (NTDS.dit) на контроллерах домена. Объекты AD представляют различные сущности: учётные записи пользователей и компьютеров, а также сетевые ресурсы (например, принтеры) и сервисы (например, электронная почта). Каждый объект имеет уникальное имя и набор атрибутов (свойств), определённых схемой каталога. Схема AD – это набор определений, описывающих типы объектов и допустимые атрибуты. Схема едина для всего леса AD и обеспечивает консистентность данных: она определяет, какие объекты (пользователь, группа, компьютер и т.д.) могут существовать и какие свойства они имеют. Схема может расширяться по необходимости (например, при установке новых приложений, интегрирующихся с AD), но изменения схемы выполняются с осторожностью, так как влияют на весь лес.

Физическая структура Active Directory базируется на контроллерах домена (domain controllers, DC). Контроллер домена – это сервер под управлением Windows Server, на котором установлена роль Active Directory Domain Services и хранится реплика каталога домена. Все контроллеры домена равноправны (модель multi-master): каждый из них содержит копию базы данных каталога, доступную для чтения и записи. При изменении данных (например, создание нового пользователя) на одном контроллере, эти изменения реплицируются на другие контроллеры данного домена. Репликация осуществляется протоколом RPC внутри сайтов (локальных сетей) и может использовать SMTP между сайтами, в зависимости от настроек и качества связи. Для оптимизации репликации крупные сети делятся на сайты – группы контроллеров, соединённых хорошими каналами связи; репликация между сайтами происходит реже и по расписанию, чтобы не перегружать медленные каналы.

В каждом домене существует глобальный каталог (Global Catalog, GC) – особая роль, которую обычно выполняет один из контроллеров. Глобальный каталог хранит обзорную информацию обо всех объектах леса (урезанный набор атрибутов), что позволяет быстро осуществлять поиск объектов по всему лесу, не обращаясь к каждому домену отдельно. Глобальный каталог отвечает на запросы о любых объектах леса (например, поиск пользователя по имени, если неизвестно, в каком домене он находится).

Для имени объектов и доменов Active Directory использует интеграцию с DNS. Каждый домен AD сопоставлен пространству имен DNS, а контроллеры домена регистрируют в DNS специальные записи (SRV-записи) для того, чтобы клиенты могли обнаруживать услуги каталога. Таким образом, DNS обеспечивает разрешение имен и играет критическую роль в функционировании AD.

Основные принципы работы Active Directory заключаются в централизованном хранении данных и предоставлении этих данных по запросу пользователей и приложений, в обеспечении единого механизма аутентификации (единого входа – Single Sign-On) и в поддержке групповых политик для управления конфигурацией рабочих станций и учетных записей. AD поддерживает стандартные протоколы (например, LDAP для доступа к каталогу, Kerberos для аутентификации), что обеспечивает совместимость с различными клиентскими приложениями. При внедрении Active Directory организация получает единый инструментарий для управления учетными записями, компьютерами и сетевыми ресурсами, а пользователи – возможность использовать одну учетную запись для доступа ко всем разрешенным ресурсам сети.

* 1. Управление учетными записями и группами пользователей.

Управление учетными записями в Active Directory включает создание, изменение и удаление учетных записей пользователей и учетных записей компьютеров, а также организацию их в группы для упрощения администрирования доступа. Учетные записи являются объектами каталога и содержат атрибуты, необходимые для идентификации и аутентификации субъекта (например, логин, хеш пароля, имя, контактные данные пользователя и пр.). Администраторы управляют учетными записями с помощью консоли Active Directory Users and Computers (ADUC) или других инструментов, таких как Центр администрирования Active Directory (ADAC) и командлеты PowerShell. Для создания новой учетной записи пользователя администратор должен обладать соответствующими правами (по умолчанию это члены групп Domain Admins, Account Operators или пользователи с делегированными правами на соответствующий OU). В ADUC создание пользователя происходит через контекстное меню нужного контейнера или OU: New → User. После ввода имени пользователя, логина (User Login Name) и задания первоначального пароля аккаунт сохраняется в каталоге. Администратор может сразу указать параметры, требующие смены пароля при первом входе, либо отключить учетную запись до определенного времени. Впоследствии для учетной записи можно заполнить дополнительные свойства – например, отдел, должность, телефон – и добавить пользователя в группы, определяющие его права (рис. 2).

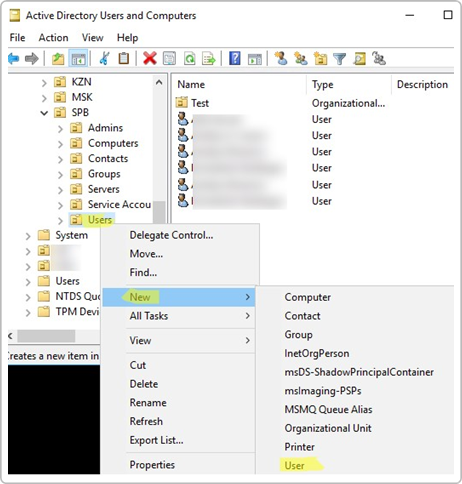


Рисунок 2 - Интерфейс консоли ADUC для создания нового пользователя в домене Active Directory.

После создания учетной записи важно правильно настроить ее членство в группах безопасности. Группы в Active Directory используются для объединения учетных записей с целью однократного назначения разрешений на ресурсы сразу для всех членов группы. AD поддерживает два типа групп: группы безопасности (Security Groups) – используются для назначения прав доступа к ресурсам, и группы рассылки (Distribution Groups) – используются для рассылки электронной почты и не применяются для доступа к ресурсам. Кроме того, группы имеют область действия (scope), определяющую, в каких частях леса можно применять данную группу: локальная группа домена (Domain Local) – действует только в пределах своего домена (может включать пользователей из любых доменов леса) и обычно применяется для назначения доступа к ресурсам этого домена; глобальная группа (Global) – может включать только объекты из своего домена, но сама может использоваться для предоставления доступа к ресурсам во всех доменах леса; универсальная группа (Universal) – может включать объекты из любых доменов леса и использоваться во всех доменах . Правильное использование типов и областей групп облегчает администрирование: распространенная стратегия – добавлять учетные записи пользователей в глобальные группы по ролям или отделам, глобальные группы вкладывать в локальные группы, созданные для конкретных ресурсов, и уже на ресурсе давать права только локальной группе (модель AGDLP – Accounts → Global Groups → Domain Local → Permissions).

Создание новой группы в ADUC происходит аналогично созданию пользователя: New → Group, после чего задаются имя группы, ее тип и область действия (см. рис. 3) . Добавление пользователей в группу можно выполнить на вкладке «Members» (Члены группы) в свойствах группы либо через контекстное меню пользователя («Add to a group…» – Добавить в группу). При добавлении пользователя в группу безопасности система автоматически обновляет маркеры доступа (Access Token) пользователя при следующем входе, и тот получает права, присущие группе. Удаление пользователя из группы, соответственно, лишает его групповых привилегий после обновления сеанса.

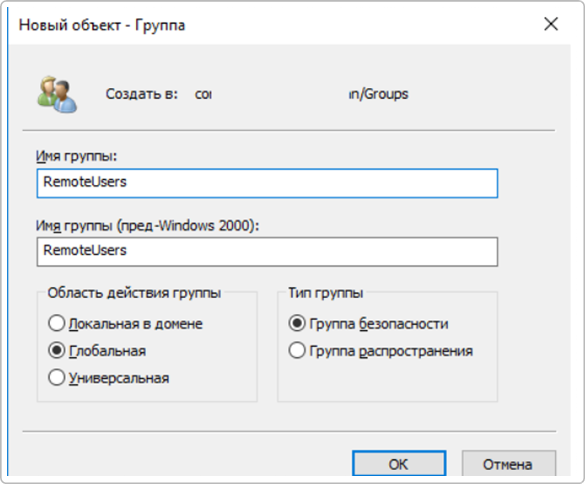


Рисунок 3 - Создание новой группы безопасности в Active Directory.

Кроме стандартных учетных записей и групп, Active Directory предусматривает учетные записи служб (service accounts) для приложений и сервисов, специальные предопределенные группы (например, Domain Admins, Backup Operators, которые имеют заранее сконфигурированные права), а также механизмы делегирования полномочий. Делегирование позволяет предоставить определенным пользователям или группам право выполнять административные операции над объектами в конкретном OU (например, создавать новых пользователей в подразделении, сбрасывать пароли и т.д.) без предоставления им полномочий администратора домена. Такой подход повышает гибкость управления и разгружает администраторов домена, позволяя распределить задачи администрирования между доверенными сотрудниками на местах.

1.3 Механизмы авторизации и разграничения доступа в AD.

Active Directory обеспечивает централизованную аутентификацию и авторизацию пользователей при доступе к ресурсам домена. Аутентификация – это проверка подлинности пользователя (его логина и пароля), а авторизация – определение прав пользователя на доступ к тому или иному ресурсу. В домене AD по умолчанию используется протокол Kerberos для аутентификации: при входе в систему учетная запись запрашивает билет Kerberos у контроллера домена (службы KDC) и затем с этим билетом может получать доступ к ресурсам без повторного ввода пароля. Если по каким-либо причинам Kerberos недоступен или клиент его не поддерживает, система автоматически использует запасной протокол NTLM для аутентификации. Оба протокола интегрированы в Windows и работают «за кадром» для пользователя, предоставляя единый вход (Single Sign-On) в доменной среде.

После успешной аутентификации и получения маркера доступа (Access Token), который содержит SID пользователя и SID всех групп, в которые он входит, происходит авторизация на конкретных ресурсах. Разграничение доступа в среде Windows осуществляется с помощью списков контроля доступа (ACL) на каждом защищаемом объекте – файле, папке, принтере, ключе реестра и т.д. В ACL объекта записаны ACE (Access Control Entries) – записи, в каждой из которых указан SID пользователя или группы и набор разрешений (allow/deny) на определённые действия. Когда пользователь пытается получить доступ к ресурсу, система сверяет его SID и SID его групп из маркера доступа с записями ACL, чтобы решить, разрешить или отказать в запрошенных действиях.

Active Directory играет ключевую роль в этой схеме, поскольку именно AD хранит учетные записи пользователей и групп, а также атрибуты, влияющие на авторизацию. Например, у каждой учетной записи есть атрибут Account Control, в котором могут быть флаги: «аккаунт отключен», «требовать смену пароля», «не позволять смену пароля пользователю» и др. Эти свойства влияют на то, сможет ли пользователь войти и какие ограничения будут действовать. AD также обеспечивает групповые политики (Group Policy) – механизм, позволяющий администраторам задавать конфигурации и правила безопасности, применяемые к компьютерам и пользователям. С помощью групповых политик можно, например, настроить политики паролей (минимальная длина, срок действия и сложность пароля), политики блокировки учетной записи (сколько неудачных попыток до блокировки) и другие настройки безопасности домена. Политики паролей и блокировок по умолчанию применяются на уровне домена и влияют на всех пользователей домена. В Windows Server 2008 и выше появилась возможность Fine-Grained Password Policies – задавать разные политики паролей для разных групп пользователей, но это выходит за рамки нашего обзора.

Еще один механизм разграничения доступа – делегирование прав в AD. Как упоминалось, администратор домена может делегировать определенные административные задачи (например, создание пользователей, сброс паролей, перемещение объектов) группе или пользователю на уровне OU. Для этого в консоли ADUC есть мастер Delegation of Control, который прописывает в ACL нужного контейнера разрешения на выполнение выбранных операций доверенному лицу. Таким образом, часть управления может осуществляться локальными ИТ- специалистами без предоставления им полномочий доменных администраторов.

Наконец, стоит отметить, что безопасность Active Directory – критически важный аспект. С компрометацией учетной записи администратора домена злоумышленник получает контроль над всей инфраструктурой. Поэтому в крупных организациях применяют концепцию административных уровней (tiers) и выделяют привилегированные учетные записи для разных задач, используют многофакторную аутентификацию, привязывают критичные операции (как изменение схемы AD) к привилегированным контроллерам, изолированным от повседневной работы. Эти меры направлены на то, чтобы ограничить потенциальный ущерб от компрометации отдельных узлов и учётных записей.

# 2. СЛУЖБА ПЕЧАТИ WINDOWS SERVER.

## 2.1 Архитектура службы печати в среде Windows Server.

Служба печати Windows Server (Print and Document Services) – это роль сервера, которая предоставляет централизованные функции управления печатными устройствами и очередями печати в корпоративной сети. Архитектура службы печати состоит из следующих основных компонентов: сервер печати, клиенты печати, драйверы принтеров, очередь печати (spooler) и физические принтеры.

Сервер печати – это сервер под управлением Windows Server, на котором установлена роль Print Server. На сервере печати регистрируются сетевые принтеры, устанавливаются соответствующие драйверы устройств, и запускается служба Print Spooler (диспетчер очереди печати) для обработки заданий. Клиенты печати – рабочие станции или другие устройства, которые отправляют задания печати на сервер. Клиенты могут автоматически получать драйверы принтеров с сервера при подключении к общему принтеру, что облегчает администрирование (администратору достаточно установить и обновлять драйвер только на сервере).

При отправке документа на печать клиентское устройство формирует печатное задание (обычно в формате EMF либо RAW) и передает его на сервер печати по сети. На сервере служба Spooler принимает задание, помещает его в очередь печати и при необходимости выполняет спулинг – преобразование данных задания в формат, понятный конкретному принтеру, с помощью установленного драйвера принтера. Драйверы являются важной частью архитектуры: они обеспечивают интерпретацию универсальных команд печати в команды, специфичные для модели принтера, и присутствуют как на сервере, так и на клиентах (при модели с централизованным сервером печати клиент обычно использует копию драйвера с сервера).

После подготовки задания spooler передает его на устройство принтера по соответствующему порту/протоколу: это может быть локальный порт (например, USB/LPT) на сервере или сетевой порт (например, стандартный порт TCP/IP, IPP и т.д.). Физический принтер, получив задание, выполняет печать, а сервер отслеживает состояние задания (печатается, выполнено, произошла ошибка и т.д.). Если принтер недоступен или офлайн, задания остаются в очереди на сервере до восстановления связи либо могут быть перенаправлены.

На рисунке 4 представлена схема, отражающая типовую архитектуру сетевой печати: несколько клиентских ПК отправляют задания на единый сервер печати, который обрабатывает их и перенаправляет на соответствующий принтер.

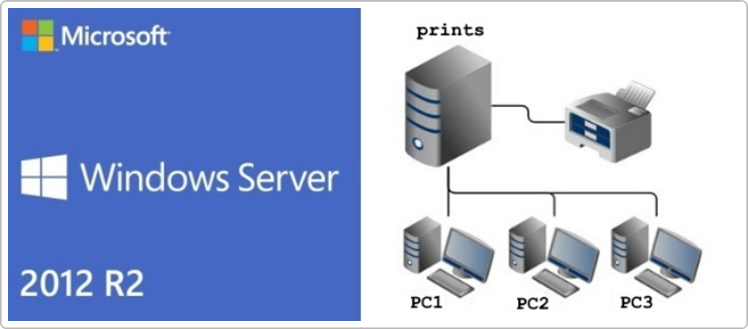


Рисунок 4 - Централизованный сервер печати в Windows Server.

Преимущества использования выделенного сервера печати в том, что администраторы получают централизованный контроль над всеми принтерами организации. Это включает единое место для установки и обновления драйверов, настройку параметров устройств, мониторинг очередей печати и устранение неполадок. Все принтеры могут быть опубликованы в Active Directory, что позволяет пользователям легко их находить (в Windows для поиска принтера можно открыть каталог и увидеть принтеры, опубликованные администратором в AD). Кроме того, через групповую политику можно автоматически подключать принтеры на пользовательских компьютерах – например, при входе пользователя в домен ему сразу назначается ближайший принтер, соответствующий его отделу или местоположению.

Windows Server поддерживает не только традиционную печать по протоколу SMB (клиенты Windows), но и печать по протоколу IPP (Internet Printing Protocol), позволяющему печатать через HTTP. Для этого в составе роли Print and Document Services можно включить компонент Internet Printing, который предоставляет веб-интерфейс для отправки заданий печати и общения с принтером через интернет/интранет. Также доступна служба LPR/LPD для печати из систем UNIX/Linux.

Архитектура службы печати включает возможность создания пулов печати (printer pool) – когда несколько физических принтеров, одинаковых по модели, объединяются в один логический принтер на сервере. Пользователь отправляет задание на такой пул, а сервер сам решает, на какое из реальных устройств его направить (обычно на первое свободное). Это повышает отказоустойчивость и производительность при больших объемах печати.

С точки зрения надежности, сервер печати может быть кластеризован (в среде Windows Server Enterprise/Datacenter) для устранения единой точки отказа: два узла могут обеспечивать отказоустойчивость роли Print Server. Также важно регулярно делать резервные копии конфигурации принтеров (списка принтеров, портов, драйверов), чтобы в случае сбоя быстро восстановить сервис печати. Для миграции принтеров между серверами существует встроенный Print Management консоль (printmanagement.msc) с функцией экспорта/импорта принтеров.

2.2 Классификация политик доступа к принтерам

В среде Windows Server разграничение доступа к принтерам осуществляется через систему разрешений (permissions) и групповую политику. Политики доступа к принтерам можно условно разделить на две категории: разрешения на уровне сервера печати и разрешения на уровне конкретного принтера.

Права на уровне сервера печати. Они определяют, какие действия пользователь может выполнять глобально на данном сервере печати. Существует два ключевых разрешения: «View Server» (Просмотр сервера) и «Manage Server» (Управление сервером).

Просмотр сервера (View Server) – позволяет пользователю просматривать принтеры, установленные на сервере, и их очереди. Пользователь без этого права вообще не увидит принтеры данного сервера в списке. По умолчанию право на просмотр сервера предоставлено группе Everyone, то есть любой аутентифицированный пользователь видит опубликованные принтеры.

Управление сервером (Manage Server) – дает более широкие полномочия: создание и удаление очередей печати на сервере, добавление/удаление портов и форм. Пользователь с этим правом, не будучи администратором системы, фактически является делегированным администратором печати (Print Administrator) на данном сервере. По умолчанию это право обычно ограничено администраторами, так как включает возможность установки драйверов принтера и изменение конфигурации сервера печати.

Права на уровне принтера. Эти разрешения определяют, что пользователь может делать с отдельной очередью печати (с конкретным принтером). Для каждого принтера в Windows задаются три основных уровня доступа:

1. Печать (Print) – базовое право, позволяющее подключиться к принтеру и отправлять задания на печать. Обладатель этого разрешения может также управлять своими заданиями – приостанавливать, возобновлять или отменять собственные документы в очереди. По умолчанию право «Print» назначается группе Everyone при создании новой очереди, что означает: любой пользователь сети может отправить задание на данный принтер, если администратор не сузил права.
2. Управление документами (Manage Documents) – расширенное разрешение, позволяющее управлять всеми заданиями в очереди данного принтера. Пользователь с таким правом может просматривать, приостанавливать, возобновлять и отменять печать любых документов других пользователей. Это полезно, например, для оператора печати или секретаря, который ведает общей очередью: он сможет устранить «застрявшие» задания, менять приоритеты и т.д.
3. Управление принтером (Manage Printer) – самое полное право на принтер: позволяет изменять настройки принтера, шарить или прекращать общий доступ к принтеру, изменять его разрешения (ACL), приостанавливать сам принтер (не только отдельные задания), а также удалять очередь принтера.
4. Обладатель этого разрешения имеет практически полный контроль над очередью, включая возможность изменить, кто еще может печатать. Обычно это право имеют администраторы печати. По умолчанию при создании принтера право «Manage Printer» предоставляется группе Administrators и группе.
5. Print Operators (если такая группа есть в домене/системе, она предназначена специально для делегирования управления принтерами).

Комбинация этих разрешений формирует эффективную политику доступа для каждого пользователя или группы относительно конкретного принтера. Как правило, рядовым пользователям дают только право «Print», некоторым ответственным лицам – «Manage Documents» (например, для отделов, где необходимо отслеживать очередь), а администраторам и операторам – «Manage Printer».

Помимо разрешений, политики доступа к принтерам могут включать и групповые политики, влияющие на поведение системы при работе с принтерами. Например, политика Point and Print Restrictions в Windows позволяет администратору контролировать, могут ли пользователи без повышения привилегий устанавливать драйверы принтера, когда они подключаются к общему принтеру. По соображениям безопасности можно запретить автоматически принимать новые драйверы с сервера печати или разрешить только доверенные подписанные драйверы – всё это настраивается через групповую политику для компьютеров. Другой пример – политика, запрещающая пользователям удалять свои задания из очереди или, наоборот, разрешающая им видеть только свои задания.

В организациях с чувствительной информацией могут применяться и административные меры политики доступа: например, определенные принтеры доступны только членам конкретных групп (через ACL принтера), на некоторых принтерах включен аудит печати – когда в журнал безопасности Windows пишутся события начала и окончания печати каждого документа, что позволяет отслеживать, кто и что печатал. Специализированное программное обеспечение может вводить дополнительные политики – квоты на печать (ограничение количества страниц, которые пользователь может распечатать за месяц), удержание заданий до подтверждения (secure print, когда задание печати выполняется только после того, как пользователь подойдёт к принтеру и идентифицирует себя) и т.п. Эти механизмы выходят за рамки стандартного функционала Windows Server, но могут быть интегрированы в общую систему управления печатью.

3. ПРИМЕНЕНИЕ СИСТЕМ ACTIVE DIRECTORY И WINDOWS SERVER

3.1 Создание учетных записей пользователей в Active Directory.

Создание пользователя в домене. На контроллере домена (Windows Server с установленной ролью AD DS) откройте консоль Active Directory Users and Computers. Перейдите в контейнер или OU, в котором следует создать нового пользователя (например, в OU «Users» или специально созданное подразделение для отдела). Щелкните правой кнопкой по выбранному OU и в контекстном меню нажмите New → User. Откроется мастер создания учетной записи пользователя. В поле First name введите имя, Last name – фамилию пользователя. Также укажите User login name – имя для входа (логин) в домен. Нажмите «Далее (Next)». На следующем шаге задайте начальный пароль для учетной записи и установите флажки политик пароля: по требованию безопасности обычно включается «User must change password at next logon» (пользователь должен сменить пароль при первом входе). После ввода и подтверждения пароля нажмите Finish, чтобы завершить создание пользователя. В консоли ADUC появится новый объект пользователя в указанном OU.

Проверка и редактирование свойств учетной записи. Найдите созданного пользователя в списке и дважды щелкните, чтобы открыть свойства учетной записи. Убедитесь, что основные данные (имя, фамилия, отображаемое имя) заполнены корректно. При необходимости заполните дополнительные вкладки: Address (адрес и контактная информация), Organization (должность, отдел, компания) и т.д. На вкладке Member Of можно увидеть, в какие группы входит пользователь, и при необходимости добавить его в существующие группы домена (кнопкой Add...). Например, если для отдела продаж существует группа “Sales”, включите нового сотрудника в эту группу, чтобы унаследовать соответствующие права доступа. После изменения свойств нажмите OK.

Создание нескольких учетных записей (при необходимости). Аналогично, создайте учетные записи для остальных пользователей согласно заданию. При большом количестве пользователей имеет смысл освоить методы автоматизации – например, создание учетных записей через PowerShell командлет New-ADUser или с помощью импорта списка из CSV-файла – однако в рамках данной практики мы ограничились графическим интерфейсом для наглядности. Убедитесь, что каждый созданный пользователь имеет уникальное имя входа и находится в правильном OU, соответствующем его подразделению (это облегчит дальнейшее управление через групповые политики).

3.2 Настройка групп и прав доступа в домене.

1. Создание групп безопасности для разделения прав. Для управления доступом к ресурсам создадим несколько групп безопасности в Active Directory. В консоли ADUC перейдите в нужный контейнер (например, можно завести отдельный OU «Groups» для всех групп безопасности организации). Щелкните правой кнопкой по контейнеру и выберите New → Group. В поле Group name задайте понятное имя группы, отражающее ее назначение, например «IT\_Department» или «Print\_Operators». Выберите тип группы: Security (группа безопасности) и область действия (scope) – в большинстве случаев достаточно Global (глобальная), если группа будет содержать пользователей одного домена и потенциально давать им доступ к ресурсам в других доменах, либо Domain Local, если группа предназначена строго для ресурсов внутри текущего домена. Нажмите OK, группа появится в списке объектов. Таким образом, создайте необходимые группы согласно политике предприятия – например, группы по отделам («Sales», «HR», «IT»), группы по ролям («Managers», «Interns») или специальные группы для доступа к отдельным ресурсам.

2. Добавление пользователей в группы. После создания групп заполните их членство. Дважды щелкните по созданной группе (или правой кнопкой – Properties) и перейдите на вкладку Members («Членство»). Нажмите Add… и в открывшемся диалоговом окне добавления объектов введите имена пользователей, которых нужно включить. Можно нажать Advanced -> Find для поиска пользователей по списку. Добавьте соответствующих пользователей в группы: например, всех сотрудников отдела продаж – в группу «Sales», ИТ- персонал – в «IT\_Department», и т.д. Нажмите OK, список членов группы обновится (в нашем стенде в группу «Print\_Operators» были добавлены учетные записи, которым планируется поручить управление принтерами). Закройте свойства группы нажатием OK.

3. Назначение прав доступа через группы. Группы безопасности в AD сами по себе лишь контейнеры – их роль проявляется, когда группы используются при назначении разрешений на ресурсы. В рамках данной практики, предположим, что существует общая сетевого папка или ресурс, доступ к которому должен быть ограничен. Демонстрация: была создана тестовая папка на сервере, в ее свойствах безопасности (Security) старая группа “Domain Users” заменена на более конкретные группы – например, доступ разрешен только группе «IT\_Department» (Full Control) и «Managers» (Read). Таким образом, участники этих групп получают доступ, а остальные пользователи домена – нет. Аналогично поступают и с принтерами – о чем далее – права «Print» и другие можно назначать не отдельным пользователям, а группам AD. В результате администратор управляет доступом, меняя членство пользователей в группах, без редактирования ACL ресурсов для каждого изменения. Это демонстрирует принцип RBAC (Role-Based Access Control) на базе групп AD: права привязываются к ролям (группам), а пользователи включаются или исключаются из групп в соответствии со своими текущими задачами и должностями.

4. Делегирование прав в AD (при необходимости). В завершение настройки прав внутри домена можно делегировать часть полномочий. В нашем случае была использована группа «IT\_Department» для делегирования: через мастер Delegation of Control в ADUC на уровне всего OU “Users” группе ИТ-отдела даны права сбрасывать пароли пользователей и создавать/удалять учетные записи в этом OU. Это значит, что члены группы «IT\_Department» (например, специалисты техподдержки) смогут выполнять базовое администрирование пользователей, не имея статуса администраторов домена. Делегирование отразится в списках ACL соответствующего OU и можно проверить, что для группы появились разрешения (например, свойство «Reset Password» на класс User). Данная настройка облегчает распределение обязанностей в ИТ-отделе и повышает безопасность (минимизируется использование учётной записи Domain Admin для рутинных операций).

3.3 Добавление и настройка сетевых принтеров.

1. Установка роли сервера печати. Перед добавлением принтера убедитесь, что на сервере (может быть тот же контроллер домена или отдельный сервер) установлена роль Print and Document Services. В Windows Server 2012R2/2016 это делается через Server Manager: Add Roles and Features → Print and Document Services → Print Server. В ходе практики роль была установлена на сервере SRV-PRINT, после чего стала доступна консоль Print Management для управления печатью.

2. Добавление нового принтера в сервер печати. Откройте консоль Print Management (Диспетчер печати) на сервере печати: через Server Manager → Tools → Print Management. В дереве консоли раскройте Print Servers → \<имя сервера> → Printers. В списке сейчас могут быть только встроенные «Microsoft XPS Document Writer» и др. Щелкните правой кнопкой по узлу Printers и выберите Add Printer… – запуск мастера добавления принтера. Запустится Network Printer Installation Wizard с выбором метода установки принтера (рис. 5).

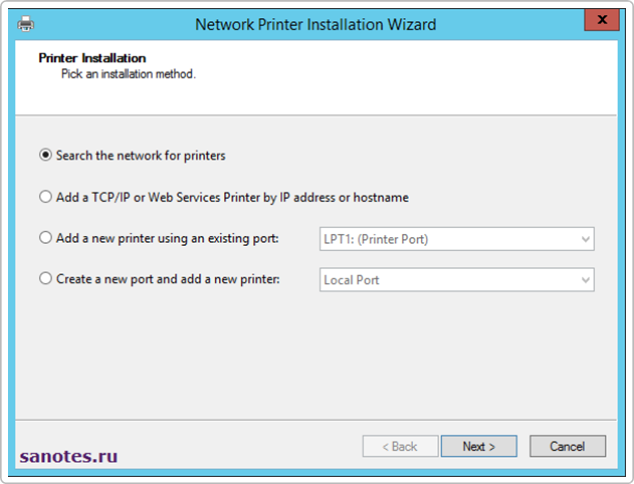


Рисунок 5 - Мастер установки принтера на сервере Windows (Network Printer Installation Wizard).

2. Выбор метода подключения принтера. Если принтер, который нужно добавить, уже подключен к сети и имеет свой IP-адрес, целесообразно использовать вариант Add a TCP/ IP or Web Services Printer by IP address or hostname. Выберите этот пункт и нажмите Next. Мастер попросит указать адрес: введите, например, (если принтер – с сетевым интерфейсом) или имя хоста. Оставьте тип устройства Auto Detect (автоопределение порта). Нажмите Next – система попытается связаться с устройством. Если принтер доступен, на следующем шаге появится окно выбора драйвера.

3. Установка драйвера принтера. Если данный принтер уже имеет подходящий драйвер в системе, его можно выбрать из списка установленных. Иначе нажмите Windows Update, чтобы система загрузила список драйверов с Windows Update, или Have Disk… для ручного выбора файла драйвера. В нашем случае для практики был заранее скачан универсальный драйвер PCL6 для принтеров HP. Мы нажали Have Disk…, указали путь к файлу драйвера и установили его. После установки драйвера мастер отобразит его в списке. Выберите соответствующую модель и нажмите Next.

4. Завершение добавления принтера. Задайте имя принтера в системе (например, «HP LaserJet M402dne») и при необходимости имя общего ресурса (Share name), под которым принтер будет виден пользователям. Можно указать местоположение (Location), например «Офис 3 этаж, комната 301», и комментарий (Comment) – это поможет пользователям идентифицировать правильный принтер. Отметьте галочку List in the directory («публиковать в каталоге AD»), чтобы принтер был виден при поиске в AD. Нажмите Next и затем Finish. Новый принтер появится в списке Printers на сервере. Теперь этот принтер расшарен в сети, и пользователи домена (при наличии прав) могут его подключать.

5. Настройка прав доступа к принтеру. По умолчанию новый принтер будет доступен всем (группа Everyone с правом Print). Если требуется ограничить, кто может печатать, или назначить операторов, откройте свойства принтера -> вкладка Security. Здесь можно убрать Everyone и добавить конкретные группы или учетные записи. В нашей практике, например, мы создали группу «Office\_Print» и включили туда сотрудников конкретного офиса, затем предоставили этой группе разрешение Print, а группе «IT\_Department» – разрешения Manage Documents и Manage Printer (то есть ИТ-специалисты смогут управлять очередью и настройками). Примените изменения ACL, тем самым настроив политику доступа: теперь только члены «Office\_Print» могут отправлять задания на принтер. Аналогично можно назначить ответственным лицам (например, начальнику отдела) право Manage Documents, чтобы он мог удалять из очереди застрявшие задания своего отдела.

6. Автоматическое подключение принтера пользователям (опционально). Для удобства пользователей можно настроить GPO, которая при входе в систему будет подключать им этот сетевой принтер. В консоли Print Management найдите добавленный принтер, щелкните по нему правой кнопкой и выберите Deploy with Group Policy…. В открывшемся окне нажмите Browse… и выберите нужную групповую политику или создайте новую, затем отметьте, применять к пользователям или компьютерам. Например, можно создать новую GPO «Deploy\_OfficePrinter» и применить ее к OU с пользователями данного офиса, указав развёртывание принтера в качестве пользовательской политики. После обновления политики у соответствующих пользователей принтер появится автоматически в списке устройств. (В рамках практики этот шаг был изучен теоретически без непосредственного применения, так как в лабораторном стенде одна учетная запись.)

3.4 Мониторинг и управление печатью.

1. Просмотр очереди печати. Для мониторинга работы принтера администратор или пользователь с правами может открывать очередь печати. Сделать это можно на сервере через консоль Print Management (раздел Printers → Двойной клик по принтеру откроет окно очереди) либо на клиентском ПК – после подключения принтера двойным щелчком по значку принтера. В окне очереди отображаются все задания, ожидающие печати, с указанием пользователя, имени документа, размера, статуса (Printing, Spooling, Paused). В рамках практики нами было отправлено несколько тестовых заданий на принтер, и на рис. 6 (ниже) была бы показана очередь с тремя заданиями – их можно было видеть и на сервере, и на клиенте. Приоритет печати по умолчанию одинаковый, но администратор может через меню Document → Properties изменить приоритет конкретного задания (значение 1–99) или время, в которое задание разрешено печатать. Это позволяет, например, срочным заданиям давать более высокий приоритет.

2. Управление заданиями печати. Пользователи с базовым правом Print могут управлять только своими заданиями: например, отменить свой документ, если передумали печатать, – через меню Document → Cancel в окне очереди (либо командой в контекстном меню задания). Пользователь с правом Manage Documents может делать то же самое для любых заданий: например, секретарь отдела видит все документы в очереди и может приостанавливать их или удалять, если документ застрял. Мы проверили эту функцию, включив пользователя в группу «IT\_Department» с правом Manage Documents – под его учетной записью была возможность останавливать чужие задания. Администратор печати (право Manage Printer) имеет дополнительные опции: он может приостановить весь принтер (Printer → Pause Printing – при этом все новые задания будут ждать, а принтер не будет печатать до возобновления), очистить очередь (Cancel All Documents), изменить настройки порта, драйвера, общие свойства принтера. В лабораторном стенде, имитируя проблему, мы приостанавливали печать на сервере – пользователи видели статус принтера как “Paused” и не могли печатать, пока мы не возобновили работу (Resume Printing).

3. Устранение неполадок печати. При работе принтера возникают типичные проблемы: отсутствие бумаги, замятие, закончился тонер, сбой драйвера и т.п. В окне очереди в колонке Status может появляться соответствующая информация (Offline, Paper Jam, Toner Low и т.д., если принтер передает статус). Администратор должен реагировать: либо технически решить проблему (заменить картридж, устранить замятие), либо перенаправить задания на другой принтер. В Windows Server администратор может настроить отправку уведомлений или запуск скриптов при определенных событиях печати – для этого используется аудит событий и можно создать задачу в планировщике, реагирующую на событие в логах (например, Event ID 13 – принтер офлайн). В рамках практики мы ограничились просмотром журнала событий Windows: в разделе Applications and Services Logs → Microsoft → Windows → PrintService включили лог Operational. При печати документов там регистрируются события ID 307 (задача напечатана) с информацией о пользователе, документе, количестве страниц и байт. Это пригодно для последующего анализа использования принтера. Мы зафиксировали в журнале несколько событий печати наших тестовых документов. Такой аудит позволяет вести учет нагрузки на принтеры и обнаруживать, кто печатал документ, если, скажем, на принтере остались конфиденциальные бумаги.

4. Средства управления печатью для пользователей. В пользовательской среде (Windows 10/11) есть упрощенный интерфейс в параметрах для управления принтерами, однако при проблемах пользователи часто обращаются к ИТ. Чтобы помочь им, администратор может удаленно просмотреть очередь: консоль Print Management позволяет подключиться к любому серверу печати (или даже рабочей станции, если знать ее имя) и видеть очереди.

Кроме того, утилита командной строки rpcclient (в составе Samba) или PowerShell cmdlet Get-PrintJob и Remove-PrintJob могут использоваться для скриптового мониторинга и очистки зависших задач. В практических заданиях мы опробовали команду Get-PrintJob – ComputerName SRV-PRINT - PrinterName "HP LaserJet M402dne" - она возвращала список заданий на указанном принтере с их статусом. Это подтвердило, что можно мониторить очередь без GUI, что важно при удаленном администрировании серверов Core без графического интерфейса.

# ЗАКЛЮЧЕНИЕ

В ходе производственной практики была изучена и реализована система централизованного управления учетными записями пользователей и устройствами печати на платформе Microsoft. Были рассмотрены архитектура и основные компоненты Active Directory, включая логическую структуру (лес, домены, OU) и физическую организацию (контроллеры домена, репликация, глобальный каталог), а также принципы работы службы каталогов. Изучены методы управления учетными записями и группами: создание пользователей, применение групп безопасности для упрощения администрирования доступа, делегирование полномочий на уровне подразделений. Также разобраны механизмы обеспечения безопасности – аутентификация Kerberos в домене, авторизация через ACL и группы, групповые политики, – которые позволяют гибко разграничивать доступ к информационным ресурсам.

Отдельная часть работы была посвящена службе печати Windows Server. Были изучены возможности серверов печати: централизованная установка принтеров и драйверов, публикация принтеров в AD и развёртывание через групповые политики, создание пулов принтеров. Сформирована классификация политик доступа к принтерам – от системных разрешений (Print, Manage Documents, Manage Printer) до административных мер (использование групп для контроля доступа, аудита и квотирования печати).

Все поставленные задачи практики были выполнены. На примере реальной инфраструктуры были показаны, как Active Directory применяется для управления учетными записями и правами пользователей, а служба печати Windows Server – для централизации управления принтерами и заданиями печати. Полученные знания и навыки имеют непосредственную практическую значимость: они позволяют администрировать корпоративные сети, обеспечивать информационную безопасность (через правильное распределение прав и своевременный аудит) и поддерживать бесперебойную работу столь важных сервисов, как учет пользователей и печать документов.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Active Directory. Официальная документация Microsoft. URL: https://learn.microsoft.com/ru-ru/windows-server/identity/ad-ds/active-directory-domain-services-overview. – 2025.

2. Active Directory — Википедия. URL: https://ru.wikipedia.org/wiki/Active\_Directory. – 2025.

3. Создание пользователя в домене Active Directory (PowerShell и ADUC) / WinITPro.ru. URL: https://winitpro.ru/index.php/2022/10/13/create-ad-user/. – 2022.

5. Типы групп Active Directory. Как создать новую группу в AD? / VMBlog.ru. URL: https://vmblog.ru/tipy-grupp-active-directory/. – 2018.

6. Служба печати Windows Server: настройка и обслуживание / Sanotes.ru. URL: https://sanotes.ru/print-services-windows-server-setup/. – 2017.

7. View a printer’s print queue in Windows / Microsoft Support. URL: https://support.microsoft.com/en-us/windows/view-a-printer-s-print-queue-in-windows. – 2023.

8. Windows 10 Print Management Tips / TechTarget. URL: https://www.techtarget.com/searchwindowsserver/tip/Windows-10-print-management-tips. – 2021.

**Индивидуальное задание на**

**Производственную практику, технологическую (проектно-технологическую практику**

Студенту направления **09.03.01 «Информатика и вычислительная техника», профиль «Автоматизированные системы обработки информации и управления»**, курс 4 гр. 606-11з  
Хориной Веры Юрьевны.

**На предприятии** Сургутский государственный университет.

**Тема:** *Изучение информационной системы управления учетными записями пользователей и устройствами печати.*

**Целевая установка:**

1. Рассмотреть архитектуру системы управления учетными записями;
2. Изучить способы управления учетными записями;
3. Дать классификацию и описание политик доступа к сетевым принтерам.

**Исходные данные:** методические, нормативно-справочные материалы, указания

**Начало практики:** 10.03.2025

**Конец практики:** 01.04.2025

**Содержание работы**

Система управления учетными записями Active Directory, служба печати Windows Server.

**Отчетный материал**

Письменный отчет в формате WinWord в соответствии с методическими указаниями по оформлению отчетов.

**Литература, используемая на практике:**

1. Типы групп Active Directory. Как создать новую группу в AD? / VMBlog.ru. URL: https://vmblog.ru/tipy-grupp-active-directory/. – 2018.
2. Служба печати Windows Server: настройка и обслуживание / Sanotes.ru. URL: https://sanotes.ru/print-services-windows-server-setup/. – 2017.

Дата выдачи задания:10.03.2025г.

Подписи:

Руководитель от предприятия:\_­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_КалачиковаЕ.П. Руководитель от университета:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Калачикова Е.П.

Задание принял к исполнению:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Хорина В.Ю.

Зав. кафедрой АСОИУ :\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Бушмелева К.И.