# Имена и идентификаторы объектов Active Directory

Тверской государственный технический университет
Прохныч А.Н.

# Поддержка имен стандартных форматов

- UPN (RFC822)
  - ✔ формат основного имени пользователя (User Principal Name)
  - ✔ имя@домен – адрес электронной почты
  - ✔ AD обеспечивает «дружественные» имена
  - ✔ может использоваться наравне с учетной записью SAM при входе в систему

# Поддержка имен стандартных форматов

- HTTP URL
  - ✔ используем протокол HTTP
- UNC (Universal Naming Convention)
  - ✔ путь в иерархической структуре к объекту
  - ✔ \\MyServer.MyCorp,Ru\Division.Finance.Russian
- LDAP URL и имена X.500
  - ✔ используем протокол LDAP
  - ✔ атрибутированное именование
  - ✔ LDAP://CN=PIvanov, OU=WorkSpace, DC=MyCompany, DC=RU

# Модель именования LDAP

- Distinguished Name (DN)
  - ✔ отличительные имена, составные имена
  - ✔ определяет положение объекта в дереве каталога
- спецификаторы DN
  - ✔ DC (Domain Component) – составная часть доменного имени
  - ✔ OU (Organizational Unit) – организационная единица
  - ✔ CN (Common Name) – общее имя

# Модель именования LDAP

- Relative Distinguished Name (RDN)
  - ✔ относительное отличительное имя
  - ✔ часть DN
  - ✔ уникальность в пределах одного уровня иерархии

# Канонические имена

- Canonical Name
- принцип построения аналогичен DN
- не используются спецификаторы
- запись в «противоположенную» сторону – от корня к объекту

# Идентификаторы в AD: GUID

- GUID (Globally Unique Identifier) – глобальный идентификатор
  - ✔ есть у каждого объекта
  - ✔ основа для репликации
  - ✔ 128 бит, уникальность «во всем мире»
  - ✔ частная реализация MS стандарта UUID
  - ✔ хранится в атрибуте objectGUID

# Идентификаторы в AD: SID

- SID (Security Identifier) – идентификатор безопасности
  - ✔ есть только у инициаторов системы безопасности (Security Principal)
    - пользователь
    - группа, но не контейнер!!!
    - компьютер…
  - ✔ используется при разграничении доступа
  - ✔ хранится в атрибуте objectSID

# Состав SID

- S-1-5-Y1-Y2-Y3-Y4
  - ✔ S-1 – SID ревизия (сейчас только 1)
  - ✔ 5 – кем был выдан SID
    5 – NT Authority
    1 – без привязки к схеме безопасности
  - ✔ Y1-Y2-Y3 – идентификатор домена
  - ✔ Y4 – относительный идентификатор (Relative ID, RID)
  - ✔ 1- 500 – системные
  - ✔ 500 -1000 – стандартные учетные записи (встроенные)

# Особенности SID

- идентификаторы удаленных объектов никогда не используются
  - ✔ объект безопасности лучше не удалять, а перемещать в специальный контейнер
- SID встроенной учетной записи везде одинаковый