

Презентация

Автоматизация массового создания
учетных записей для работы с
терминальной фермой предприятия с
использованием сценариев PowerShell

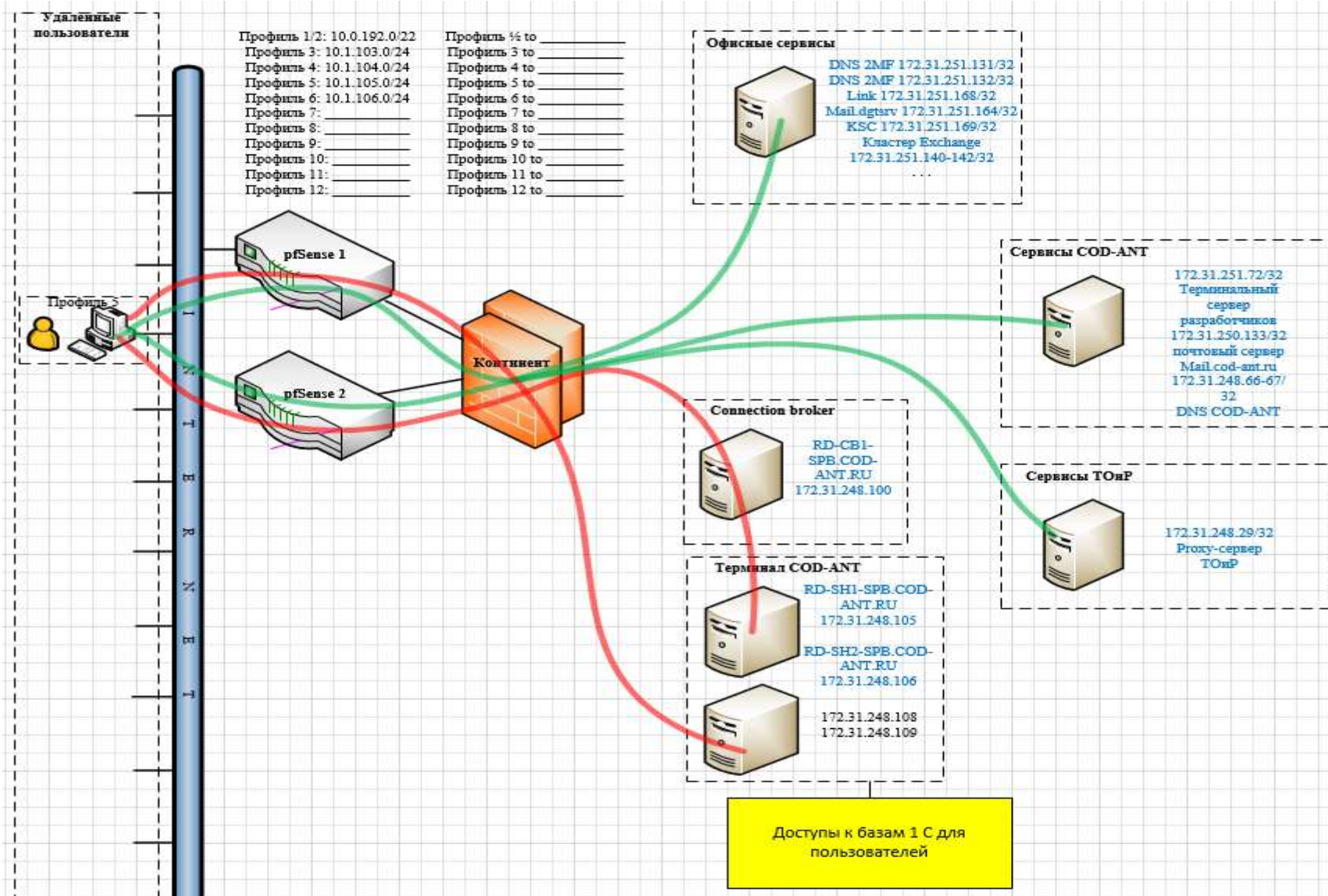
Выполнил: Фролов Д.М.

Руководитель дипломного проектирования: Норка Е.О.

Санкт-Петербург 2022

Описание целевой IT инфраструктуры

Пользователи могут работать с нужными системами, получая доступ к терминальной ферме COD-ANT



Цель и задачи ВКР

ЦЕЛЬ РАБОТЫ:

разработка системы, позволяющей осуществлять генерацию и анализ корректности созданных учётных записей AD

ЗАДАЧИ РАБОТЫ:

1. Анализ теоретических положений применения технологии AD;
2. Обоснование необходимости защиты устройств и методов обеспечения их информационной безопасности;
3. Разработка и описание использования разработанного сценария массового создания учётных записей

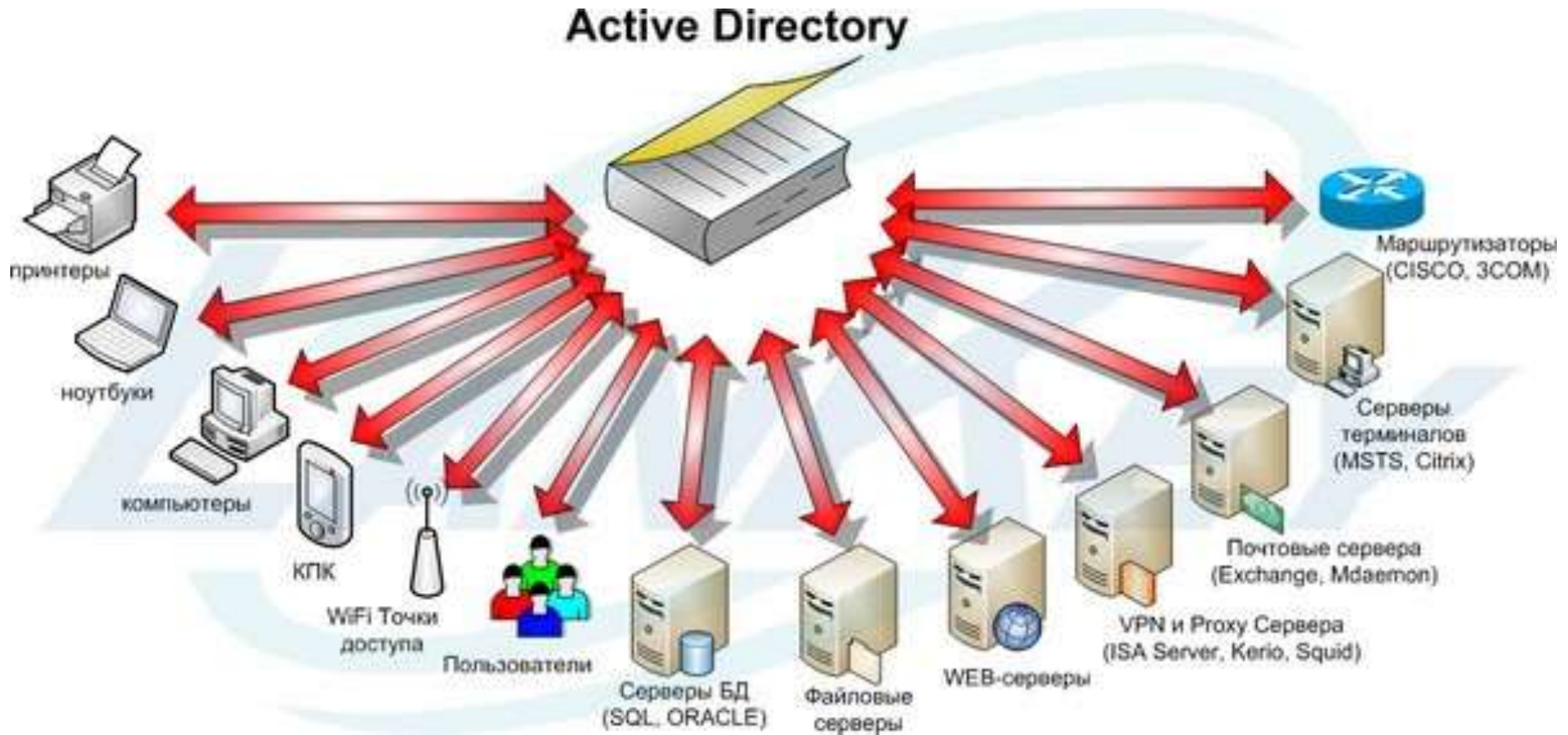
Способы защиты информации



Процесс управления доступом

- идентификация пользователей при использовании системы, а также ее ресурсов;
- использование идентификатора пользователя для его опознания и доступа в систему;
- осуществление проверки полномочий пользователя на доступ в систему (в целях проверки соответствия всех атрибутов установленным регламентам);
- обеспечение условий для работы в пределах выделенного регламента;
- протоколирование всех обращений к обеспечиваемым защитой ресурсам;
- обеспечение реакции на несанкционированные действия (сигнализация или отключение доступа).

Служба AD



Команды для создания

Import-Module activedirectory

Get-Command New-ADUser -Syntax

```
New-ADUser -Name «Albert Schmidt» -GivenName «Albert» -Surname  
«Schmidt» -SamAccountName «a.schmidt» -UserPrincipalName «[email protected]» -  
Path «OU=Users,OU=Accounts,OU=Berlin,OU=DE,DC=heyadvice,DC=com» -  
AccountPassword(Read-Host -AsSecureString «Input Password») -Enabled $true
```

```
PS C:\WINDOWS\system32> New-ADUser -Name "Albert Schmidt" -GivenName "Albert" -Surname "Schm  
dt" -UserPrincipalName "a.schmidt@woshub.com" -Path "OU=Users,OU=Accounts,OU=Berlin,OU=DE,DC=  
ord(Read-Host -AsSecureString "Input Password") -Enabled $true  
Input Password: *****
```

Создание с помощью файла

Киров - Блокнот

Файл Правка Формат Вид Справка

```
№;Организация;Подразделение (Полностью);Должность (Полностью);Имя;Отчество;Фамилия;Инициал отчества;ФИО (Краткое лат.);Email;Телефон;Пароль ТФ;Информационная система;
1;"АО ""Газпром газораспределение Киров"" ";Сунский газовый участок ;Специалист 3 категории;Владислав;Владимирович;Гущинн;В.;;v.gushchin@gpgrkirov.ru;(83369) 3-14-01;
2;"АО ""Газпром газораспределение Киров"" ";Немский газовый участок ;Специалист 2 категории;Антон;Владимирович;Уссков;В.;;a.uskov@gpgrkirov.ru;(83350) 2-14-01;
3;"АО ""Газпром газораспределение Киров"" ";Уржумский газовый участок;Специалист 1 категории;Игорь;Алексеевич;Роддыгин;А.;;i.rodygin@gpgrkirov.ru;(83363) 2-32-88;
4;"АО ""Газпром газораспределение Киров"" ";Нолинский газовый участок ;Специалист 3 категории;Дмитрий;Александрович;Кривохижин;А.;;d.krivozhizhin@gpgrkirov.ru;(83363) 2-15-47;
5;"АО ""Газпром газораспределение Киров"" ";;Александр;Сергеевич;Романов;С.;Специалист 2 категории;a.romanov@gpgrkirov.ru;(83368) 2-15-47;;ИУС ТОиР;
6;"АО ""Газпром газораспределение Киров"" ";Зуевский ГУ-Н;;Павел;Петрович;Малльцев;П.;Специалист 1 категории;p.malcev@gpgrkirov.ru;(83363) 2-15-47;;ИУС ТОиР;
```

Скрипт



Скрипт

*sozdaniye_users – Блокнот

Файл Правка Формат Вид Справка

```
# Import active directory module for running AD cmdlets
```

```
Import-Module activedirectory
```

```
$city = "kirov"
```

```
$OUname = "GRO_$city"
```

```
#$OUname = "$city"
```

```
$result = @()
```

```
$groups = @('1C_users', 'development', 'ODP-ASCUG-Sever', 'ODP-ASCUG-Nalchik', 'ODP-ASCUG-Smolensk', 'RDFarm-Spb-1c')
```

```
$group = $groups[1]
```

```
#Store the data from ADUsers.csv in the $ADUsers variable
```

```
$ADUsers = Import-csv C:\ps\$city.csv -Delimiter ';' -Encoding Default
```

```
#Loop through each row containing user details in the CSV file
```

```
foreach ($User in $ADUsers)
```

```
{
```

```
    #Read user data from each field in each row and assign the data to a variable as below
```

```
    $email = $User.email
```

```
    $Firstname = ($User.Имя).Trim()
```

```
    $MiddleName = ($User.Отчество).Trim()
```

```
    if ($User.Фамилия) {
```

```
        $Lastname = ($User.Фамилия).Trim()
```

```
    }
```

```
    else {
```

```
        continue
```

```
    }
```

```
    $telephone = $User.Телефон
```

```
    $company = if (($User.Организация).Length -lt 64) {$User.Организация} else {($User.Организация).Substring(0, 63)}
```

```
    $department = if (($User.'Подразделение (Полностью)').Length -lt 64) {$User.'Подразделение (Полностью)'} else {($User.'Подразделение (Полностью)').Substring(0, 63)}
```

```
    $title = if (($User.'Должность (Полностью)').Length -lt 64) {$User.'Должность (Полностью)'} else {($User.'Должность (Полностью)').Substring(0, 63)}
```

```
    if ($User."ФИО (Краткое лат.)") {
```

```
        $Username = $User.'ФИО (Краткое лат.)'
```

```
    }
```

```
    else {
```

```
        $Username = (ConvertTo-Translit $Lastname) + (ConvertTo-Translit $Firstname).Substring(0, 1) + (ConvertTo-Translit $MiddleName).Substring(0, 1)
```

```
    }
```

```
    if ($User."Пароль ТФ") {
```

```
        $Password = $User.'Пароль ТФ'
```

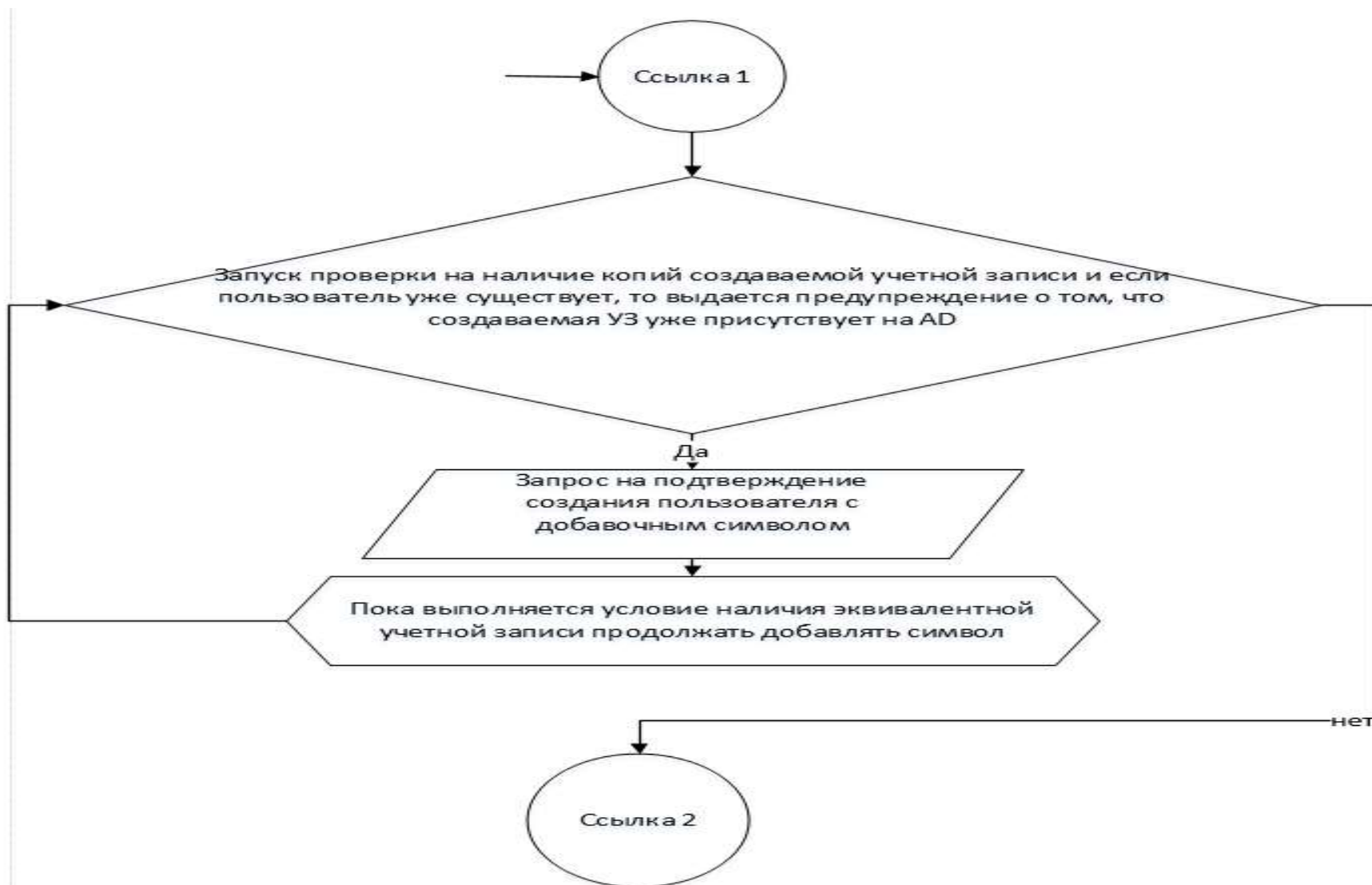
```
    }
```

```
    else {
```

```
        $Password = [System.Web.Security.Membership]::GeneratePassword(10,1)
```

```
    }
```

Скрипт



Скрипт проверка на дубликаты

```
#Check to see if the user already exists in AD
if ($usr = Get-ADUser -F {SamAccountName -eq $Username}) {

    #If user does exist, get approve
    $OU = ($usr.DistinguishedName -split ",",3)[1]
    Write-Warning "A user account with username $Username already exist in Active Directory, $OU."
    $answer = Read-Host "Are you sure?"
    if (!(($answer -eq "y" -or $answer -eq "yes") ) {
        continue
    }

    $i = 0
    $Username_tmp = $Username
    Do {
        $i += 1
        $Username = $Username_tmp + $i
    } while ( Get-ADUser -F {SamAccountName -eq $Username} )

}
```

Скрипт заведение на AD, добавление в группу и выгрузка паролей



Скрипт заведение на AD, добавление в группу и выгрузка паролей

```
#Account will be created in the OU provided by the $OU variable read from the CSV file
New-ADUser `
  -SamAccountName $Username `
  -UserPrincipalName "$Username@cod-ant.ru" `
  -Name ("$Lastname $Firstname $MiddleName " + " " *$i) `
  -DisplayName "$Lastname $Firstname $MiddleName " `
  -GivenName $Firstname `
  -Surname $Lastname `
  -Enabled $True `
  -Path "OU=$OUname, OU=Access_Ferma, OU=OVPN, DC=cod-ant, DC=ru" `
  -Company $company `
  -OfficePhone $telephone `
  -EmailAddress $email `
  -Department $department `
  -Title $title `
  -AccountPassword (ConvertTo-SecureString $Password -AsPlainText -Force) -ChangePasswordAtLogon $false -CannotChangePassword $true -PasswordNeverExpires $true

if ($group) {
  Add-ADGroupMember -Identity $group -Members $Username
}

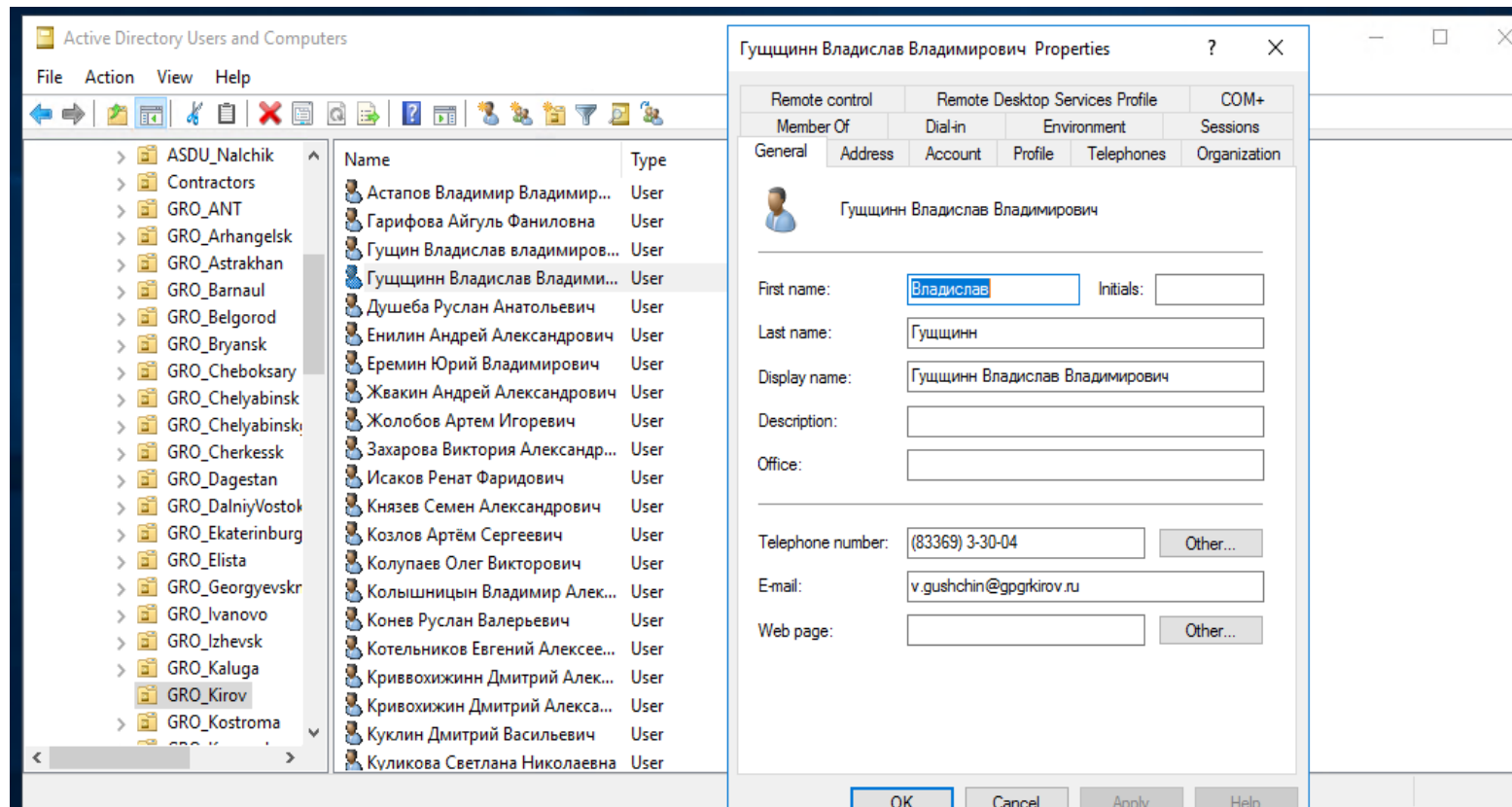
$details = @{
  Фамилия = $Lastname
  Пользователь = $Username
  Пароль = $Password
  #Имя = $Firstname
  #Отчество = $MiddleName
  #email = $email
  #Телефон = $telephone
  #Организация = $company
  #Подразделение = $department
}

$result += New-Object PSObject -Property $details

}

$result | export-csv -Path C:\ps\Result_$city.csv -NoTypeInformation -Encoding Default -Delimiter ";"
```

Созданные пользователи



Спасибо за внимание!