МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«Санкт-Петербургский национальный исследовательский университет

информационных технологий, механики и оптики»

Факультет информационных технологий и программирования

Кафедра компьютерных технологий

Лабораторная работа №4

**Основы работы с Active Directory в Windows Server**

Выполнил студент группы

№М32342:

Ларионов Андрей Николаевич

Проверил:

Береснев Артем Дмитриевич

САНКТ -ПЕТЕРБУРГ  
2020

**Вопросы:**

**1) Раскройте смысл терминов дерево доменов, лес и схема Active Directory?**

*Домен* - минимальная структурная единица организации Active Directory (может состоять из пользователей, компьютеров, принтеров, прочих общих ресурсов).

*Дерево доменов* - иерархическая система доменов, имеющая единый корень (корневой домен).

*Лес доменов* - множество деревьев доменов, находящихся в различных формах доверительных отношений.

*Схема Active Directory* - набор определений всех типов объектов каталога и связанных с ними атрибутов. Схема определяет способ хранения и конфигурирования в AD всех пользователей, компьютеров и других данных объектов, стандартизируя всю структуру Active Directory.

Лес и домен составляют основу логической структуры. Высший уровень логической иерархии AD — это лес. Лесом называют полностью самостоятельную организацию Active Directory, которая имеет определенный набор атрибутов и является периметром безопасности организации. В состав леса могут входить как один, так и несколько доменов. Все объекты, создаваемые внутри леса, имеют общий набор атрибутов. Меняя этот набор, мы меняем его для всех объектов леса. Такой набор называется схемой AD. Она описывает все объекты, которые мы можем создать, и их структуру. Под доменом понимается логическая группа пользователей и компьютеров, которые поддерживают централизованное администрирование и настройки безопасности. Дерево — не что иное, как набор доменов, которые используют связанные пространства имен. Резюмируя, можно условно нарисовать такую схему: «Лес — дерево — домен».

**2) Где на контроллере домена хранится данные об объектах Active Directory в виде файлов? Какие файлы за что отвечают?**

База данных Active Directory хранится на контроллере домена в файле NTFS.DIT, который находится в папке %SYSTEMROOT%\NTDS.

В каталоге находятся файлы:

*NTDS.DIT* – база данных Active Directory  
*EDD.CHK* – проверочный файл (checkpoint)  
*EDB.LOG* – журнал событий (≤10 Мб)  
*EDBxxxx.LOG* – вспомогательные журналы событий (создаются, когда EDB.Log > 10Мб)

*RES1.LOG* – резервный файл журнала событий

*RES2.LOG* – резервный файл журнала событий

*TEMP.EDB* – временный журнал, содержит информацию о событиях, происходящих в настоящий момент

*SHEMA.INI* – необязательный файл, используется для инициализации NTDS.DIT во время загрузки контроллера домена

**3) Где на контроллере домена хранятся файлы, содержащие групповые политики домена?**

Forest -> Domains -> <Ваш домен> -> Group Policy Objects

**4) Какие компоненты устанавливаются мастером при добавлении ролей Active Directory?**



**5) Для чего нужен пароль DSRM?**

Пароль режима восстановления служб каталога (DSRM) требуется для входа на контроллер домена, если служба Active Directory Domain Services не запущена, либо потому что она была остановлена, либо потому что контроллер домена был запущен в режиме DSRM. Пароль DSRM не совпадает с паролем учетной записи администратора домена.

**6) Как восстановить пароль DSRM, если он был утерян после установки?**

Воспользоваться ntdsutil.exe с правами администратора  
set dsrm password  
reset password on server NULL  
новый пароль  
подтверждение пароля  
quit  
quit

**7) Зачем нужно имя домена NetBIOS?**

*NetBIOS* обеспечивает такие возможности как:   
- регистрация и проверка сетевых имен;  
- установление и разрыв соединений;  
- связь с гарантированной доставкой информации;  
- связь с негарантированной доставкой информации;  
- поддержка управления и мониторинга драйвера и сетевой карты.

**8) Какие записи в DNS создаются специально для AD? Перечислите их, укажете их назначение.**

Для AD DS создается:

* Зона \_msdcs. Для поиска определённых ролей в лесу и в домене.
* SRV-записи служб (адрес, протокол, порт)
* DNS должен поддерживать динамические обновления, так как служба NetLogon регистрирует специальные SRV записи.

SRV записи регистрируемые службой Net Logon:  
  
\_ldap.\_tcp.DnsDomainName  
\_ldap.\_tcp.SiteName.\_sites.DnsDomainName  
\_ldap.\_tcp.dc.\_msdcs.DnsDomainName  
\_ldap.\_tcp.SiteName.\_sites.dc.\_msdcs.DnsDomainName  
\_ldap.\_tcp.pdc.\_msdcs.DnsDomainName  
\_ldap.\_tcp.gc.\_msdcs.DnsForestName  
\_ldap.\_tcp.SiteName.\_sites.gc.\_msdcs. DnsForestName  
\_gc.\_tcp.DnsForestName  
\_gc.\_tcp.SiteName.\_sites.DnsForestName  
\_ldap.\_tcp.DomainGuid.domains.\_msdcs.DnsForestName  
\_kerberos.\_tcp.DnsDomainName.  
\_kerberos.\_udp.DnsDomainName  
\_kerberos.\_tcp.SiteName.\_sites.DnsDomainName  
\_kerberos.\_tcp.dc.\_msdcs.DnsDomainName  
\_kerberos.tcp.SiteName.\_sites.dc.\_msdcs.DnsDomainName  
\_kpasswd.\_tcp.DnsDomainName  
\_kpasswd.\_udp.DnsDomainName

\_ldap — запись идентифицирует LDAP серверы, имеющиеся в сети.

\_kerberos — SRV-записи \_kerberos идентифицируют все ключевые центры распределения (KDC — Key Distribution Centers) в сети.

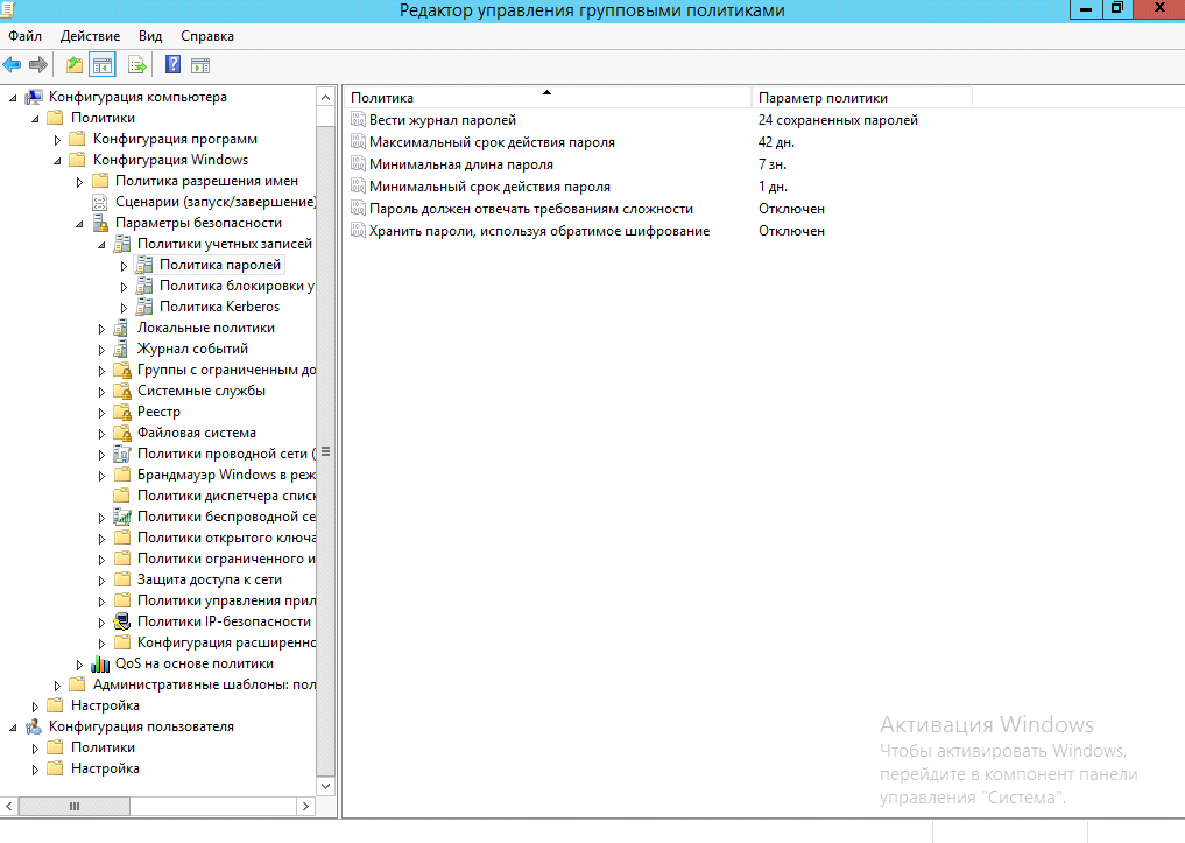
\_kpassword — идентифицирует серверы изменения паролей kerberos в сети;

\_gc — запись, относящаяся к функции глобального каталога в Active Directory.

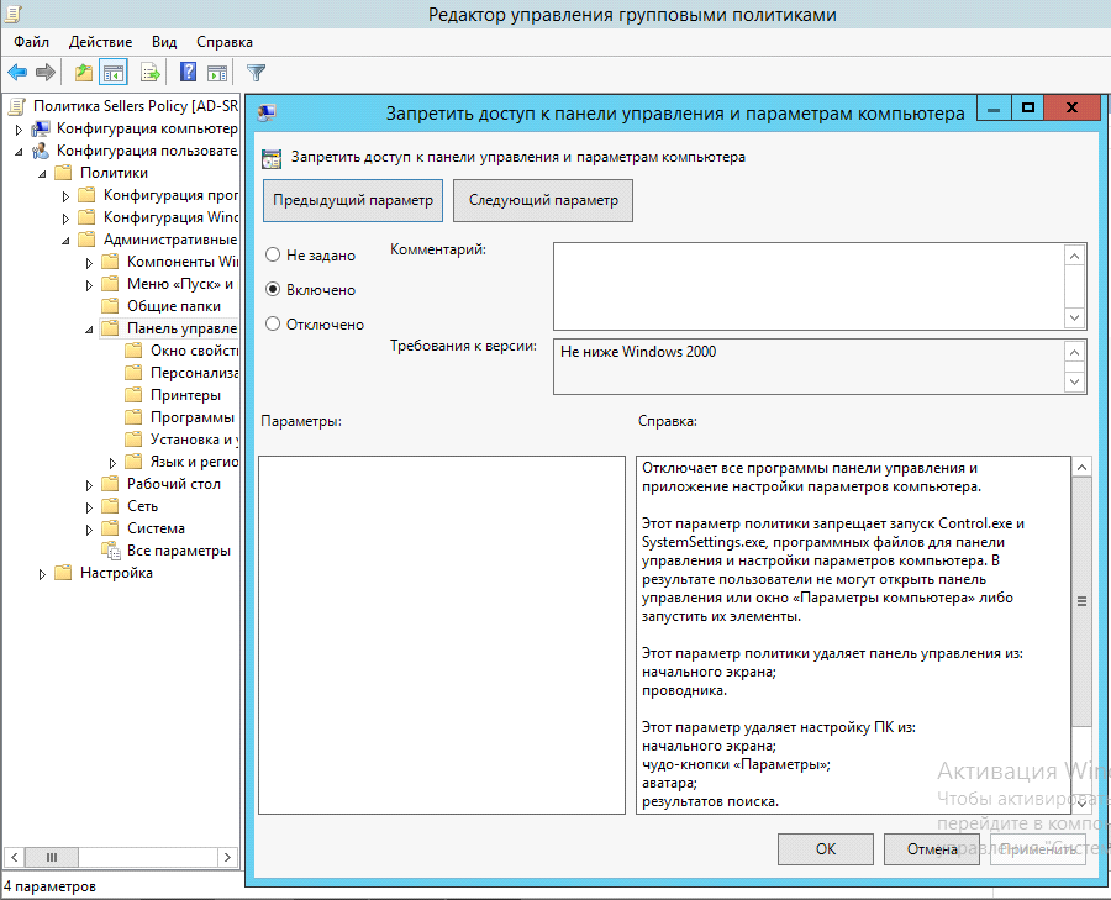
**Артефакты:**

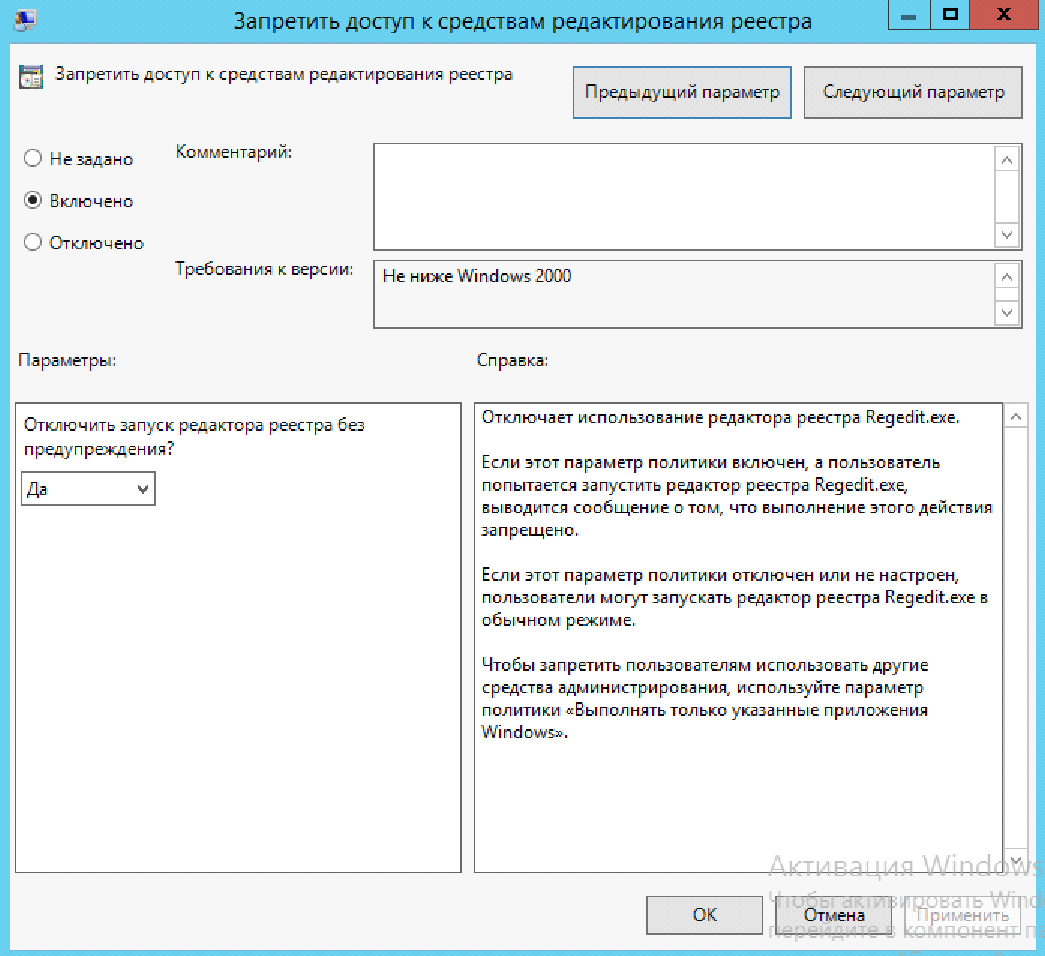
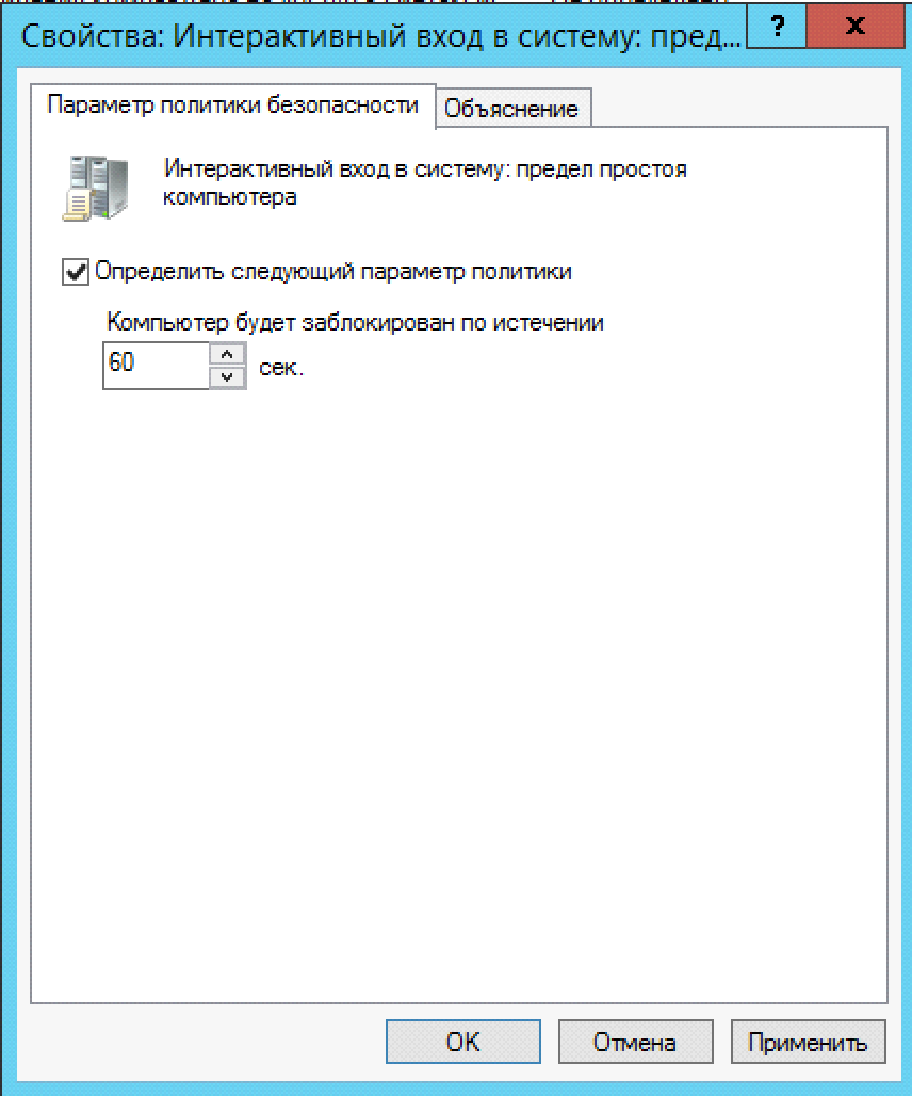
**1) Приведите скриншоты групповых политик AD из части 4.**

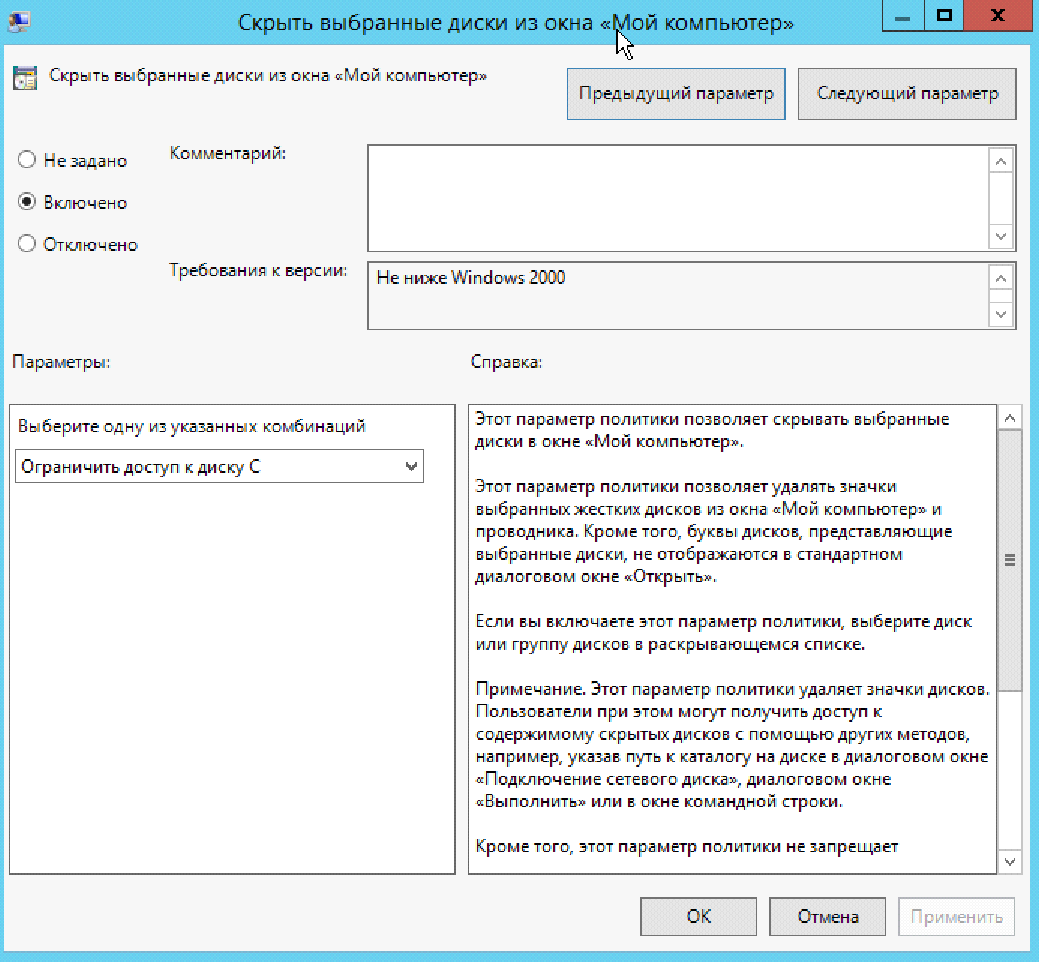
1.1)



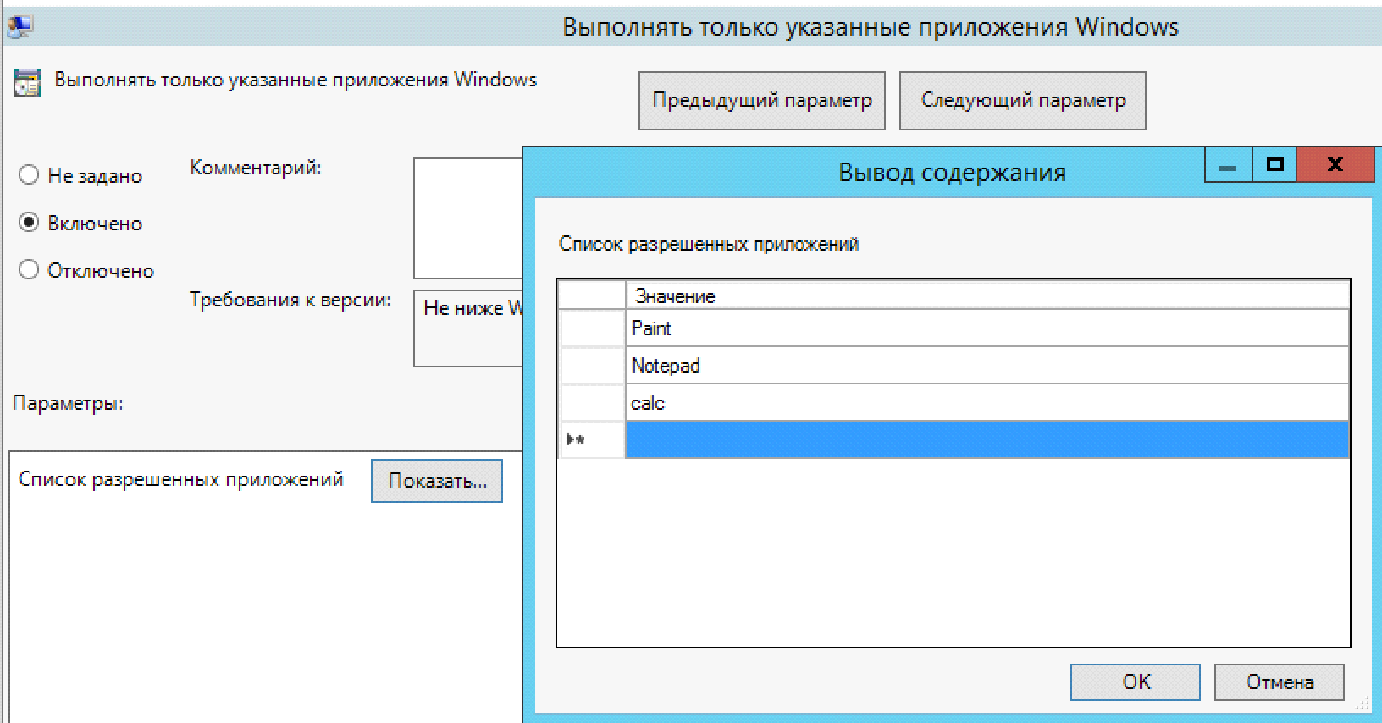
1.2)



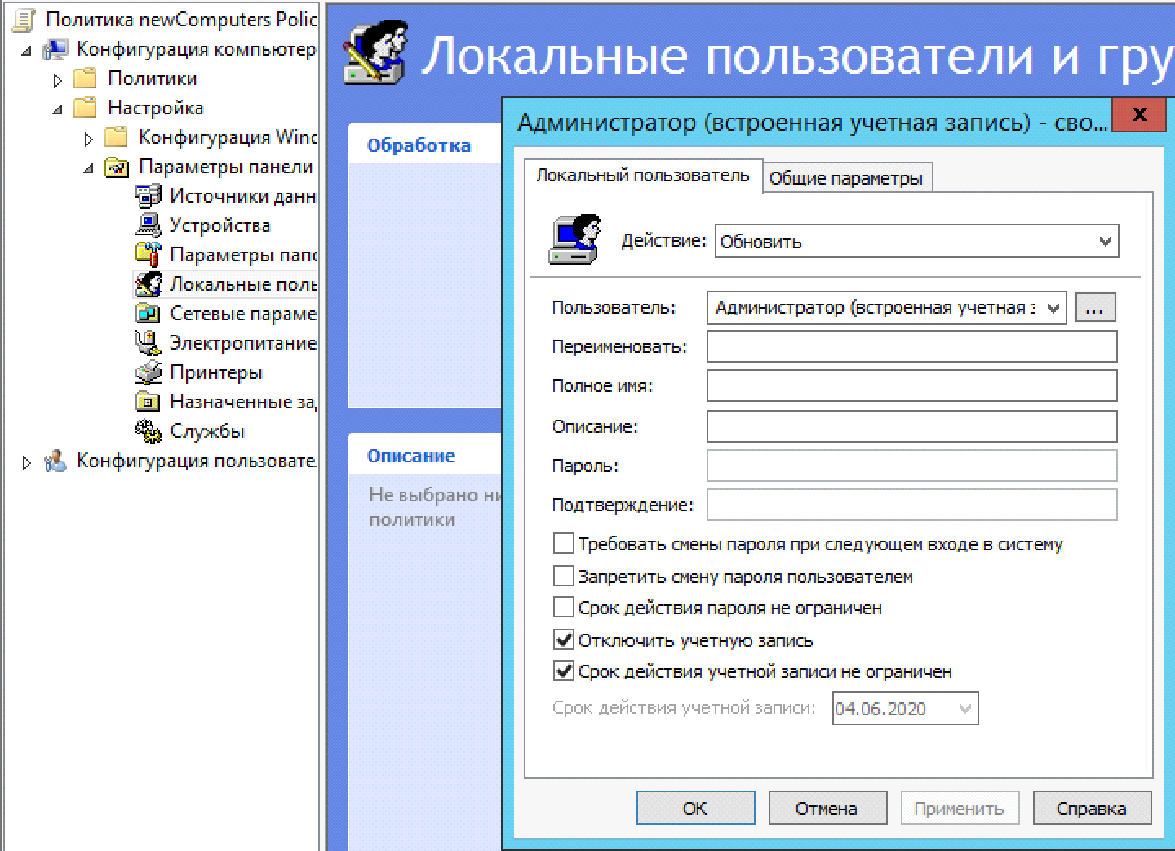
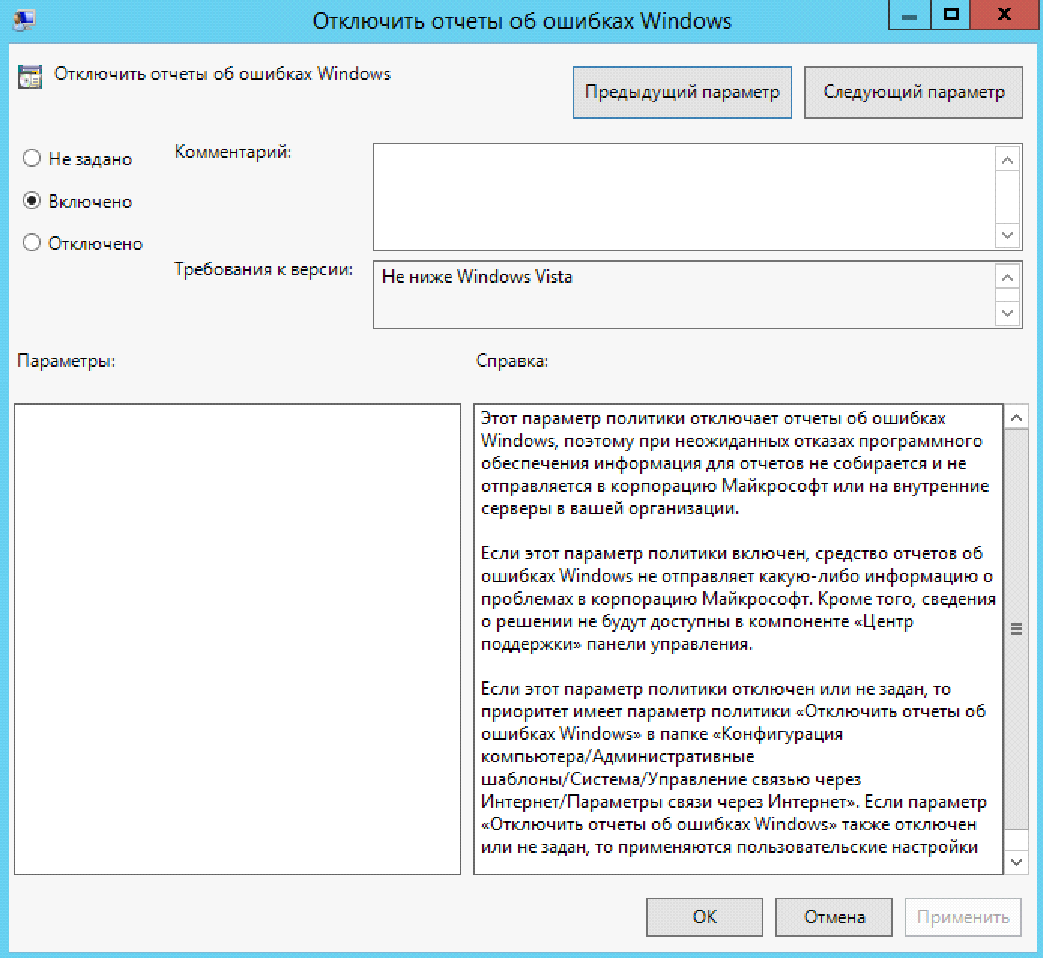


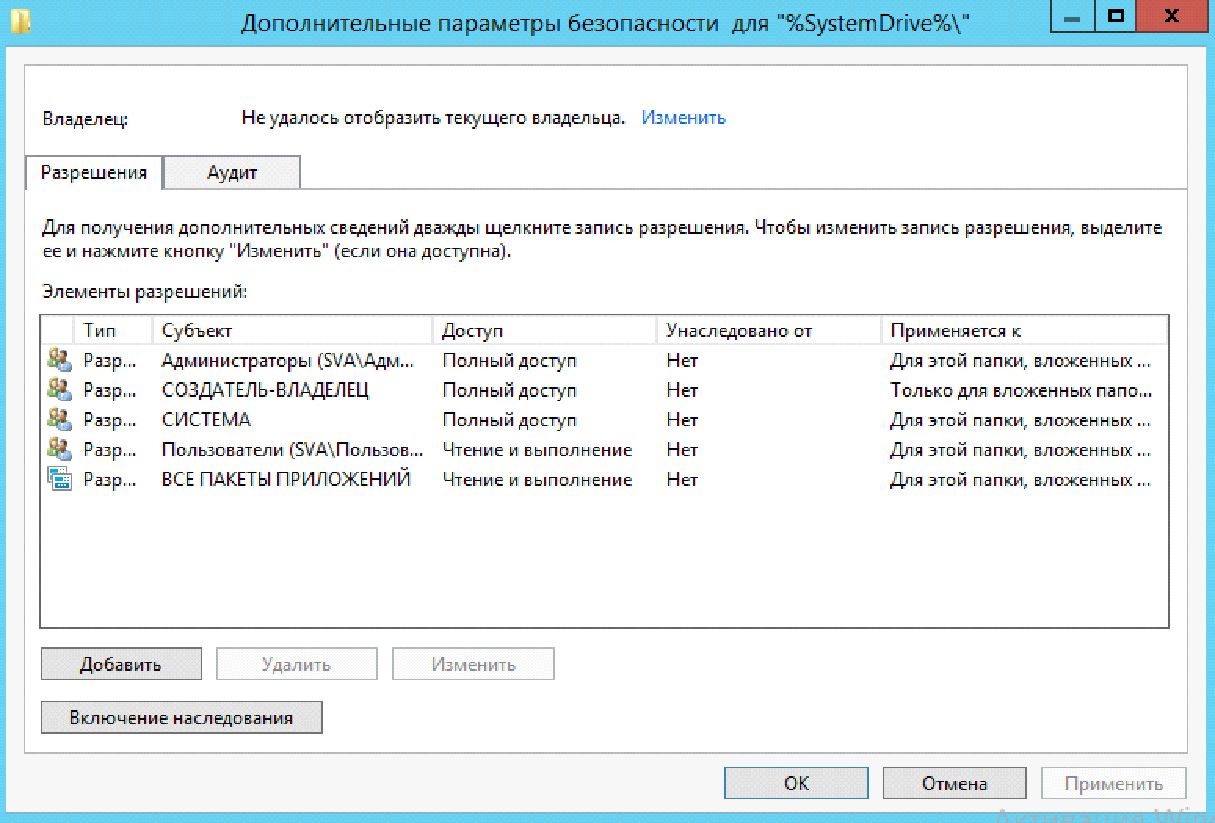
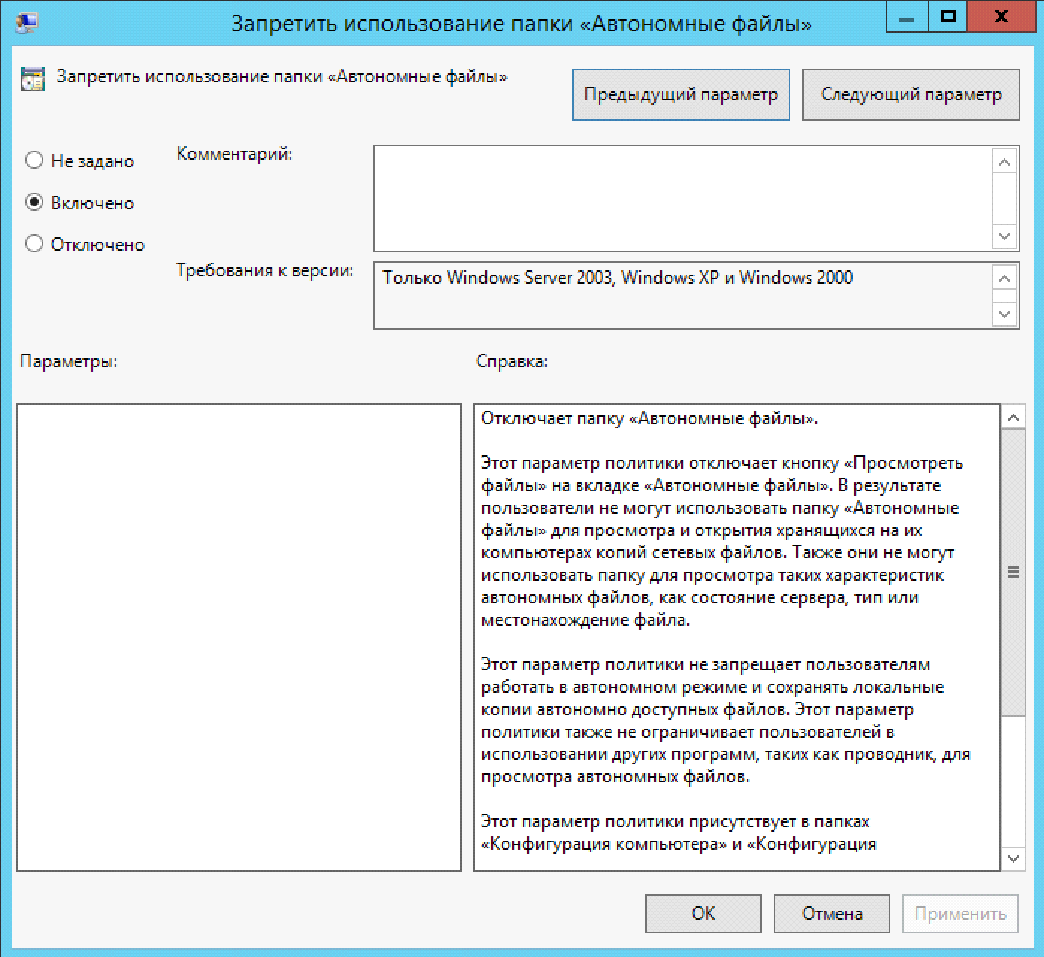


1.3)



1.4)





1.5)

**2) Приведите скрипт из части 5.**

$filePath=$args[0] #.\data.json

$jsonData = (gc $filePath | out-string)

$jsonData = ConvertFrom-Json –InputObject $jsonData

$html = ''

$table = @{

    "Object" = ""

    "Name" = ""

    "Location" = ""

}

ForEach ($user in $jsonData.users){

$password = ConvertTo-SecureString $user.password -AsPlainText -Force

$path = 'OU=' + $user.containerName + ',DC=LAN,DC=local'

$homeDirectory = '[\\AD-SRV\UsersHome$\](about:blank)' + $user.login

$OU = "LDAP://OU="+ $user.containerName + ",DC=LAN,DC=local"

if(![adsi]::Exists($OU)){ New-ADOrganizationalUnit -Name $user.containerName -Path "DC=LAN,DC=local" -ProtectedFromAccidentalDeletion $False

     $table['Object'] = 'Organization unit'

        $table['Name'] = $user.containerName

        $table['Location'] = 'LAN.local'

        $html += [PSCustomobject]$table| ConvertTo-Html -Fragment -As Table

    }

    New-Item -Path $homeDirectory -Name $user.login -ItemType "directory"

    New-ADUser -Name $user.login `

    -SamAccountName $user.login `

    -GivenName $user.name `

    -Surname $user.lastName `

    -Title $user.position `

    -EmailAddress $user.email `

    -HomePhone $user.phone `

    -Department $user.department `

    -AccountPassword $password `

    -Path $path

    -HomeDirectory $homeDirectory `

    -Enabled $true

    $table['Object'] = 'User'

    $table['Name'] = $user.login

    $table['Location'] = $user.containerName

    $html += [PSCustomobject]$table| ConvertTo-Html -Fragment -As Table

    ForEach ($group in $user.groups) {

        $groupExists = Get-ADGroup -LDAPFilter "(SAMAccountName=$group)"

        if ($groupExists -eq $null){

            $location = 'OU=' + $user.containerName + ',DC=LAN,DC=local'

            New-ADGroup -Name $group `

            -GroupCategory Security `

            -GroupScope Global `

            -DisplayName $group `

            -Path $location

            $table['Object'] = 'Group'

            $table['Name'] = $group

            $table['Location'] = $user.containerName

            $html += [PSCustomobject]$table| ConvertTo-Html -Fragment -As Table

        }

        $str = "CN=" + $user.login + ",OU=" + $user.containerName + ",DC=LAN,DC=local"

        $u = Get-ADUser -Identity $str -Server "AD-SRV.LAN.local"

        Add-ADGroupMember -Identity $group -Members $u

    }

}

$html | Out-File .\log.html

start .\log.html

{

"users":[

{

"name":"Andrey",

"lastName":"Larionov",

"middleName":"Nikolaevich",

"position":"student",

"department":"CS",

"email":"nowiwr01@gmail.com",

"phone":"+79216583412",

"login":"nowiwr01",

"password":"Homework4",

"containerName":"unit-for-delete"

},

{

"name":"Dmitriy",

"lastname":"Melnikov",

"middleName":"Alexandrovich",

"position":"student",

"department":"CS",

"email":"melnikov@gmail.com",

"phone":"+78000000001",

"login":"melnikov",

"password":"melnikov01",

"containerName":"unit-for-delete"

},

{

"name":"Adam",

"lastname":"Parrish",

"middleName":" ",

"position":"student",

"department":"CS",

"email":"parrishad@gmail.com",

"phone":"+78000000000",

"login":"Parrish",

"password":"Magician01",

"containerName":"unit-for-delete"

},

{

"name":"Henry",

"lastname":"Cheng",

"middleName":"Henry",

"position":"student",

"department":"CS",

"email":"chenghenry@gmail.com",

"phone":"+78000000001",

"login":"HCheng",

"password":"TheFool12",

"containerName":"unit-for-delete"

},

{

"name":"Fifth",

"lastname":"Fifth",

"middleName":"Fifth",

"position":"student",

"department":"CS",

"email":"Fifth@gmail.com",

"phone":"+78000000001",

"login":"Fifth",

"password":"Fifth01",

"containerName":"unit-for-delete"

}

]

}

**4) Приведите конвейер команд из ч.6 п.3**

dsquery user OU=unit-for-delete,DC=LAN,DC=local | dsrm -noprompt

**5) Приведите конвейер команд из ч.6 п.4**

Get-ADObject -Filter {Deleted -eq $True} -IncludeDeletedObjects | where {$\_.ObjectClass -eq 'user'} | Restore-ADObject