

Лаб 4. Доменные службы Active Directory (AD DS). Установка и первоначальная настройка AD DS. Объекты AD. Групповые политики (GPO).

Задание.

Использовать виртуальные машины из предыдущих лабораторных работ. Установить на Windows Server 2019 роль «Доменные службы Active Directory», развернуть новый лес и новый домен AD. Подготовить структуру подразделений (OU) домена AD. Подключить Windows 10 к домену AD.

Создать несколько объектов групповых политик (GPO) на разных уровнях структуры домена, применить их к Windows 10. Протестировать механизм наследования групповой политики. Подготовить отчет результатов групповой политики.

Этапы выполнения.

- 1) Перед установкой роли «Доменные службы Active Directory» необходимо удалить ранее созданную зону DNS, либо при создании нового леса AD указать другое имя леса, не совпадающее с именем созданной ранее зоны DNS.
- 2) Установить на Windows Server 2019 роль «Доменные службы Active Directory». На последнем этапе установки выбрать пункт «Повысить роль этого сервера до уровня контроллера домена» (рис.1).

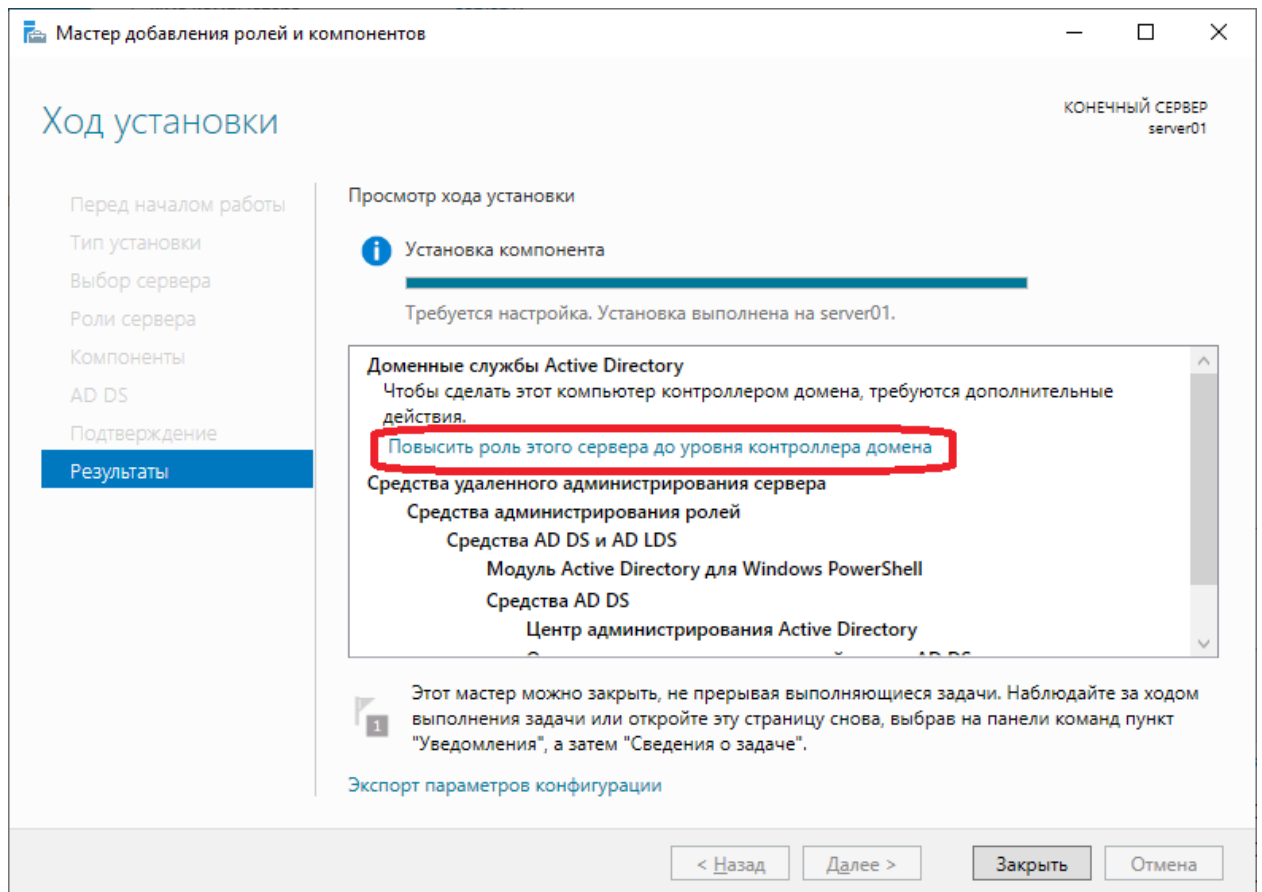


Рис.1. Установка Доменных служб Active Directory.

3) Создать новый лес (например, example.edu) (рис.2).

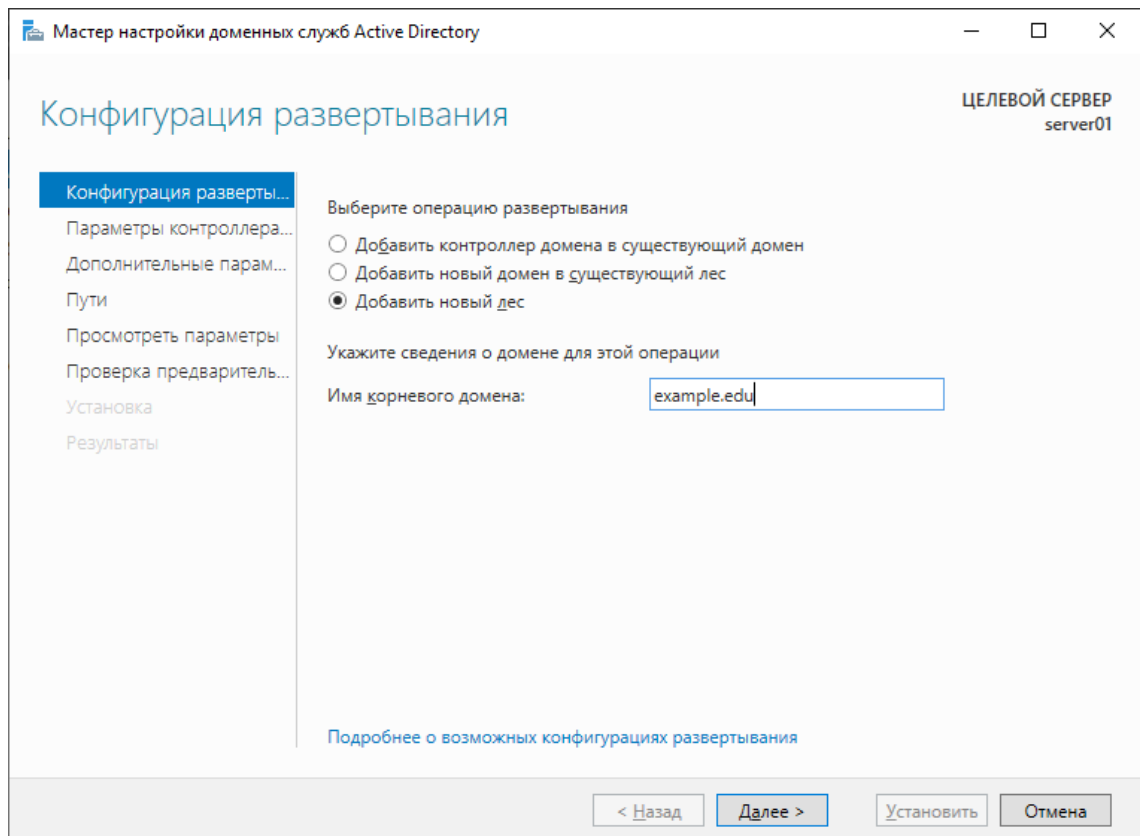


Рис.2. Создание нового леса.

Режим работы леса и режим работы домена оставить в значении «Windows Server 2016», задать пароль для режима восстановления служб каталогов, остальные параметры мастера настройки оставить в значениях по умолчанию (рис.3).

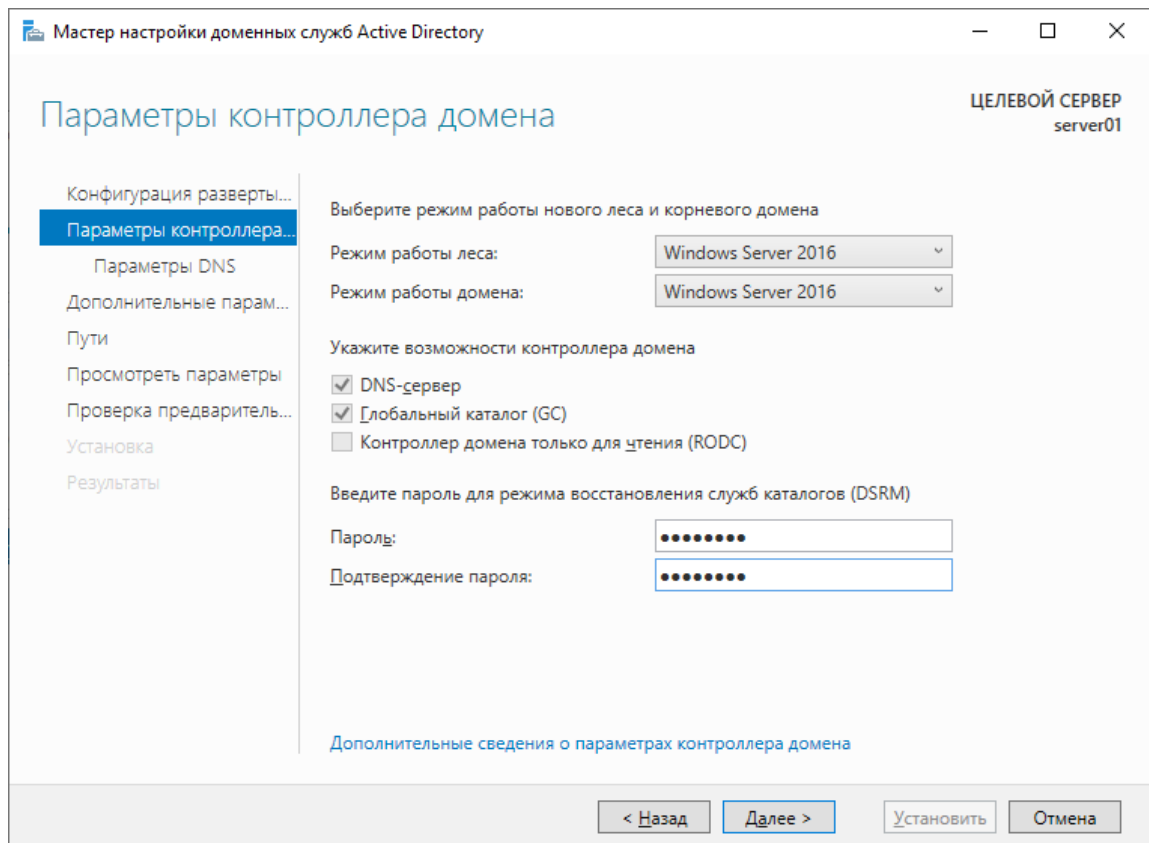


Рис.3. Параметры контроллера домена.

Задать NetBIOS-имя домена или оставить предложенный вариант (рис.4).

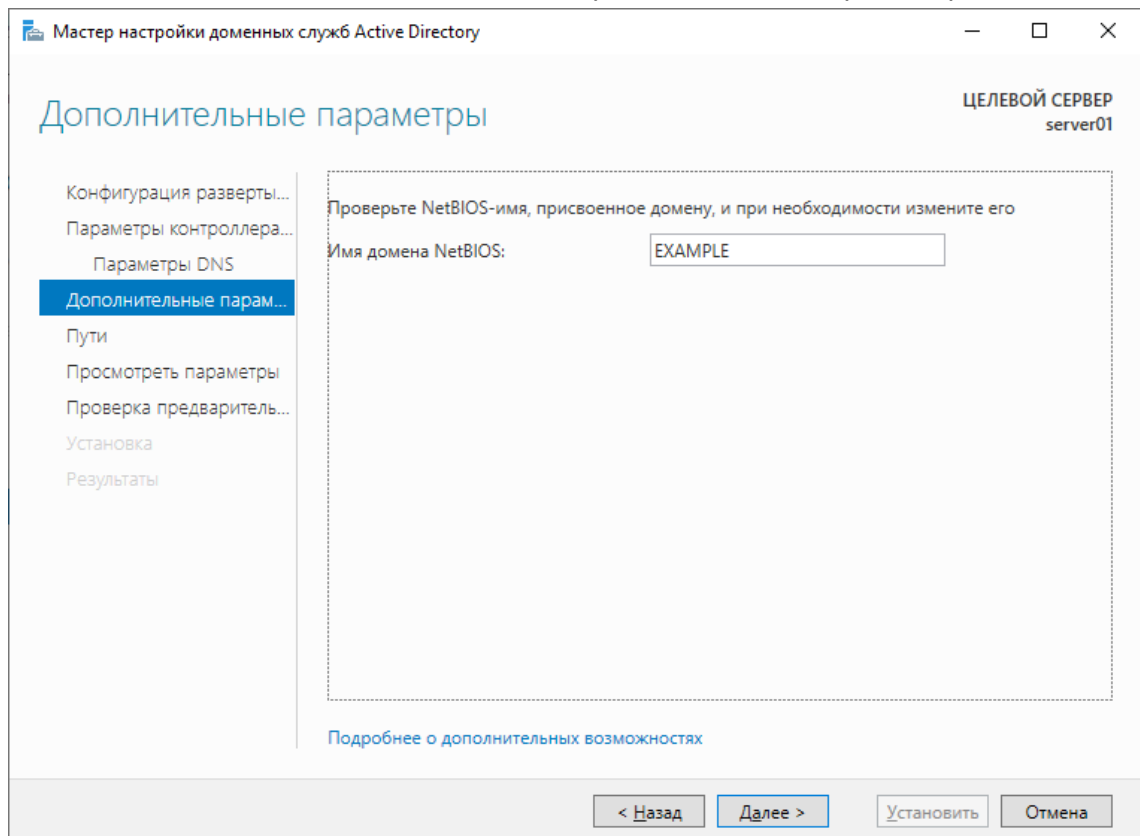


Рис.4. NetBIOS-имя домена.

На этапе «Проверка предварительных требований» выводится ряд предупреждений, некритичных для данного лабораторного стенда — нажать кнопку Установить (рис.5).

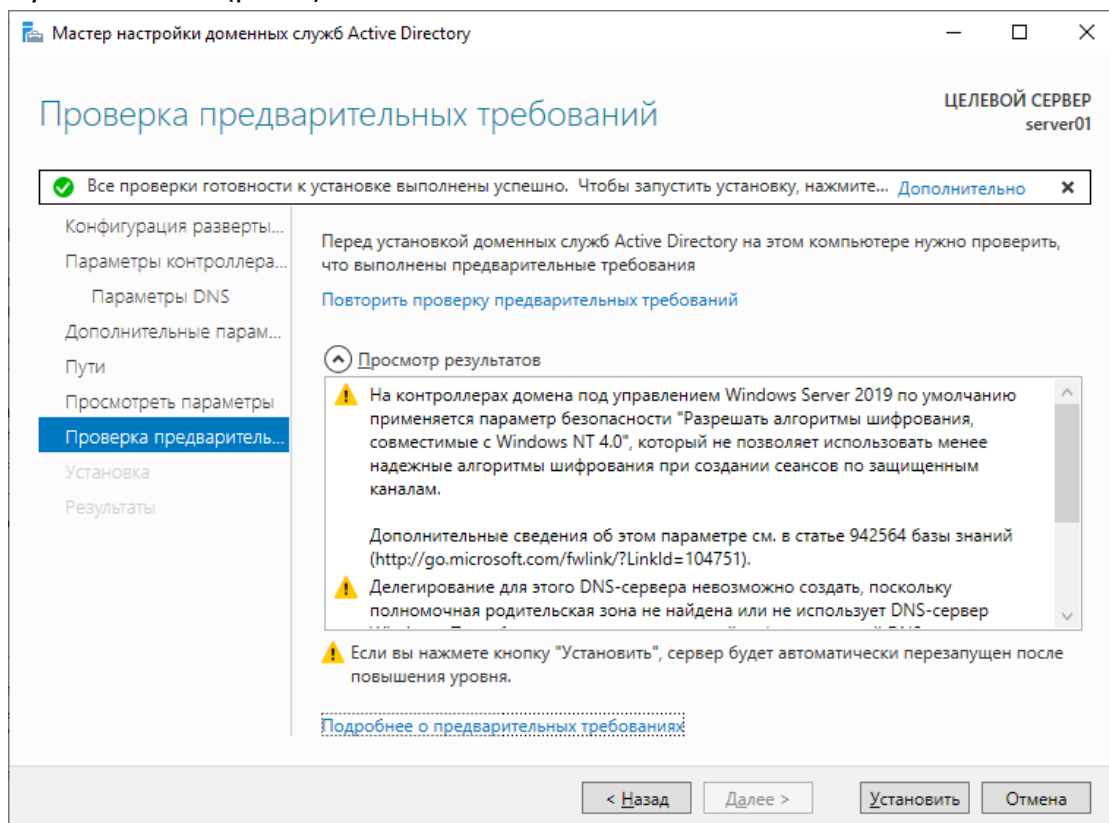


Рис.5. Проверка предварительных требований.

ОС будет перезагружена, локальная учетная запись Администратор получит полномочия администратора домена.

4) Выполнить авторизацию DHCP-сервера (рис.6).

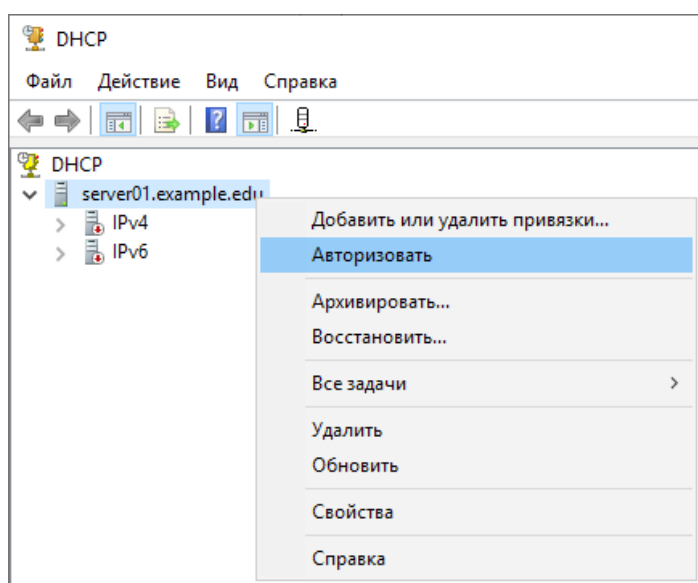


Рис. 6. Авторизация DHCP-сервера.

5) Перейти в оснастку «Пользователи и компьютеры Active Directory» через меню Средства в Диспетчере серверов.

6) Подготовить структуру подразделений (OU) домена AD. В корневом контейнере домена создать подразделение (OU) с названием организации (рис.7). Название выбрать самостоятельно (в качестве примера используется «Организация») (рис.8).

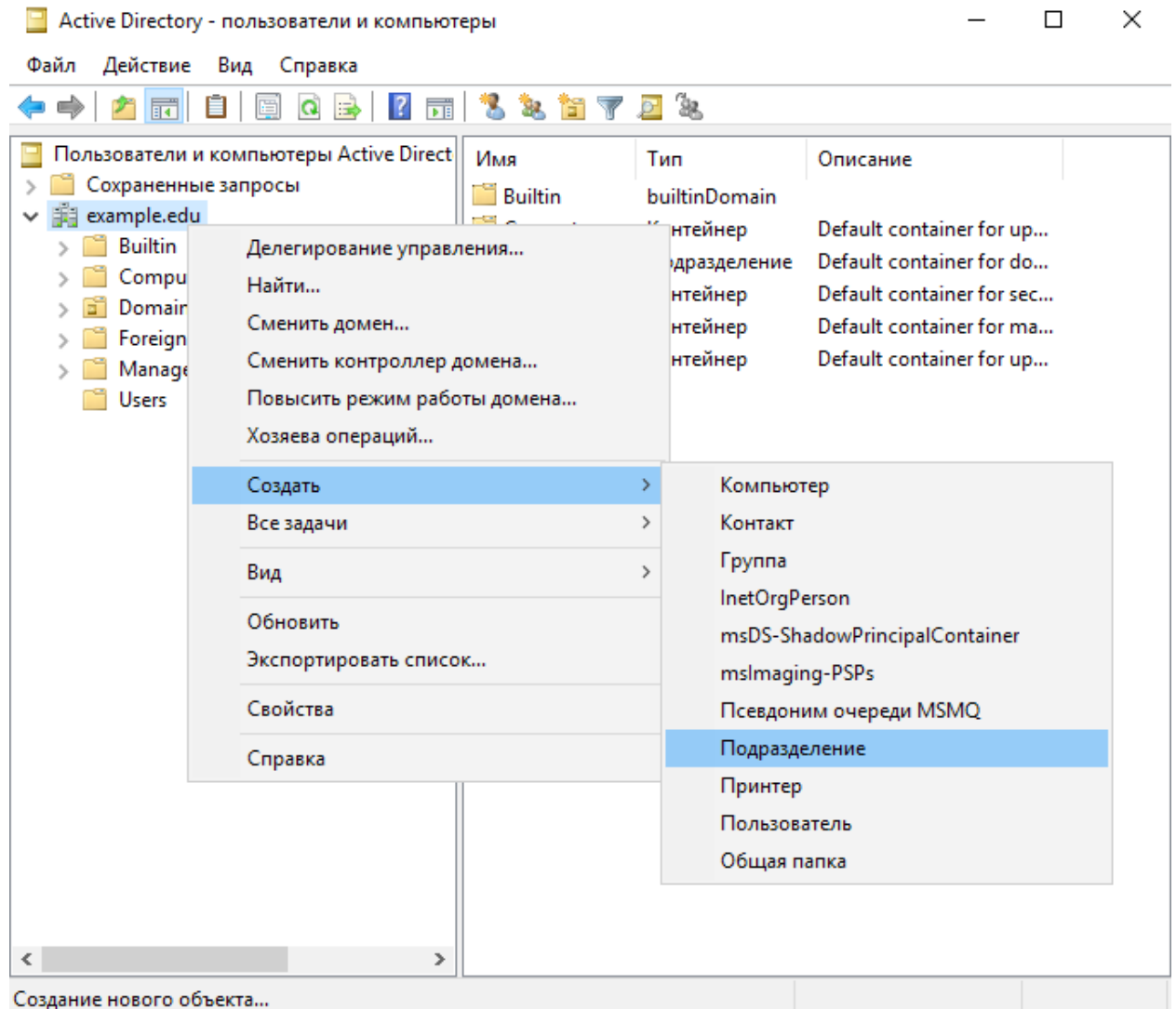
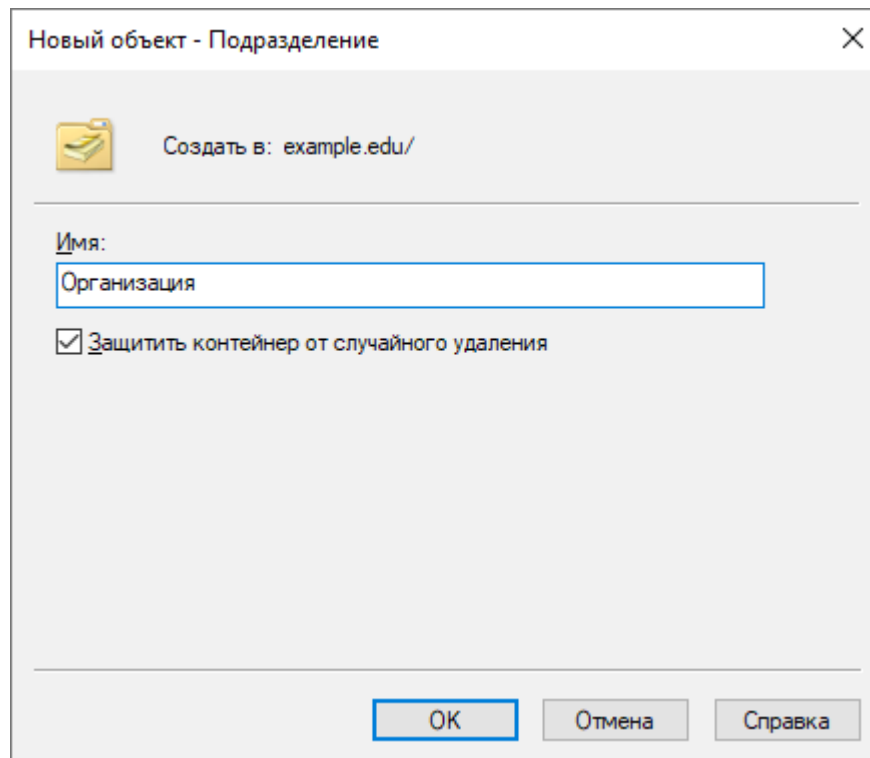


Рис.7. Создание подразделения (OU).



Новый объект - Подразделение

Создать в: example.edu/

Имя:

Организация

☒ Защитить контейнер от случайного удаления

OK Отмена Справка

Рис.8. Название подразделения.

7) В созданном подразделении создать несколько вложенных подразделений (названия выбрать самостоятельно; пример: «Управление 1», «Управление 2», «Управление 3»).

В каждом вложенном подразделении создать еще по два подразделения - «Пользователи» и «Компьютеры». Примерная структура подразделений — на рис.9.

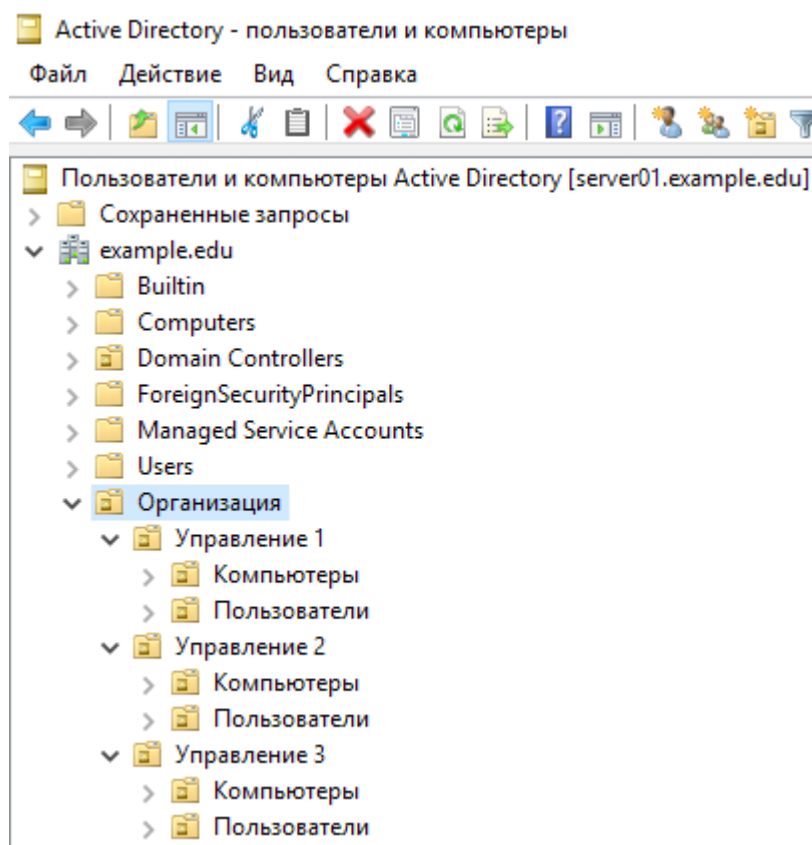


Рис.9. Структура подразделений.

Для удаления объекта (например, созданного ошибочно) с защитой от случайного удаления необходимо включить отображение дополнительных компонентов в меню Вид, а затем снять защиту в свойствах объекта.

Снимок окна «Active Directory – пользователи и компьютеры» со структурой созданных подразделений — в отчет.

8) Подключить Windows 10 к созданному домену AD (рис. 10). По запросу учетных данных указать логин и пароль пользователя с правами на подключение к домену. Учетная запись «Администратор» на контроллере домена с Windows Server 2019 (администратор домена) обладает такими полномочиями.

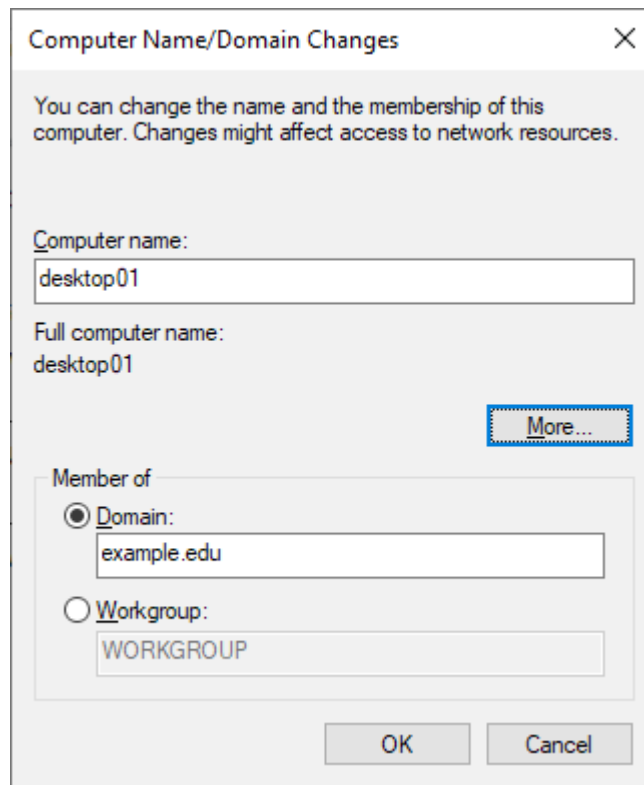


Рис.10. Подключение к домену.

9) На контроллере домена в оснастке «Active Directory – пользователи и компьютеры» перенести новый появившийся компьютер с Windows 10 из контейнера Computers в одно из созданных ранее подразделений (OU) «Компьютеры» (например, Организация/Управление 1/Компьютеры).

10) Перейти в оснастку «Управление групповой политикой» через меню Средства в Диспетчере серверов. Создать новый объект групповой политики (GPO) (например, «Test update») (рис.11).

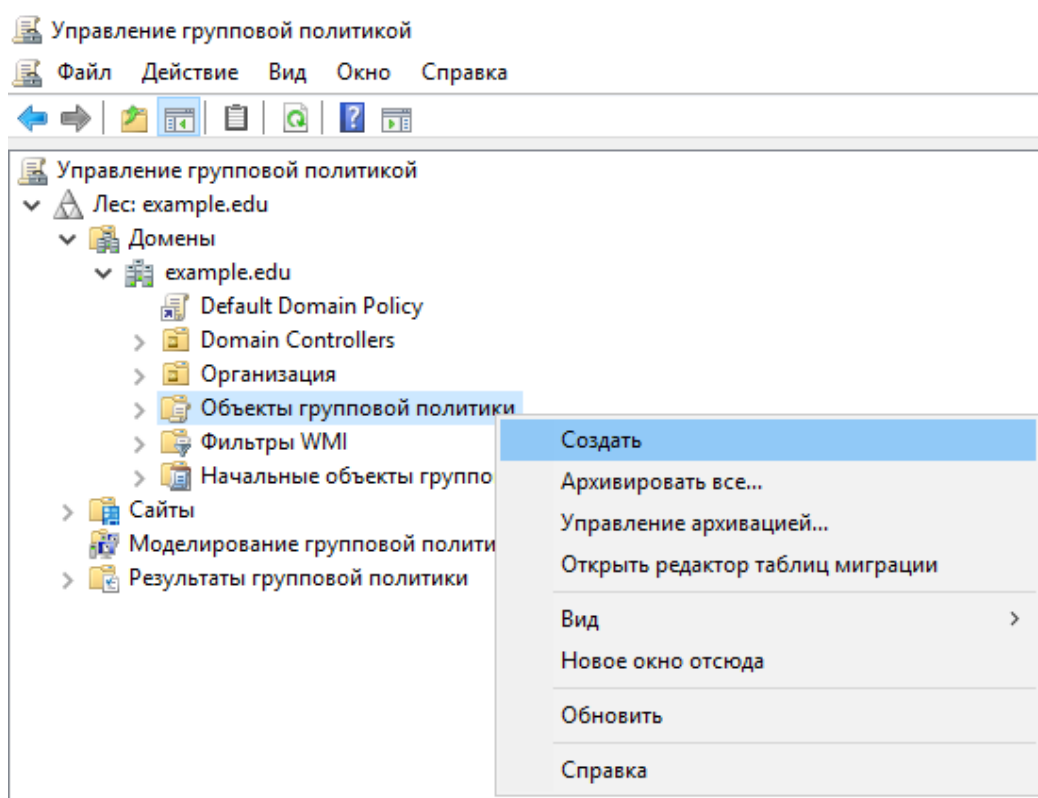


Рис.11. Создание объекта групповой политики.

11) В редакторе групповой политики (рис.12) изменить параметр: Конфигурация компьютера — Политики — Административные шаблоны — Компоненты Windows — Центр обновления Windows — Настройка автоматического обновления, установить значение «Отключено» (рисунки 13, 14).

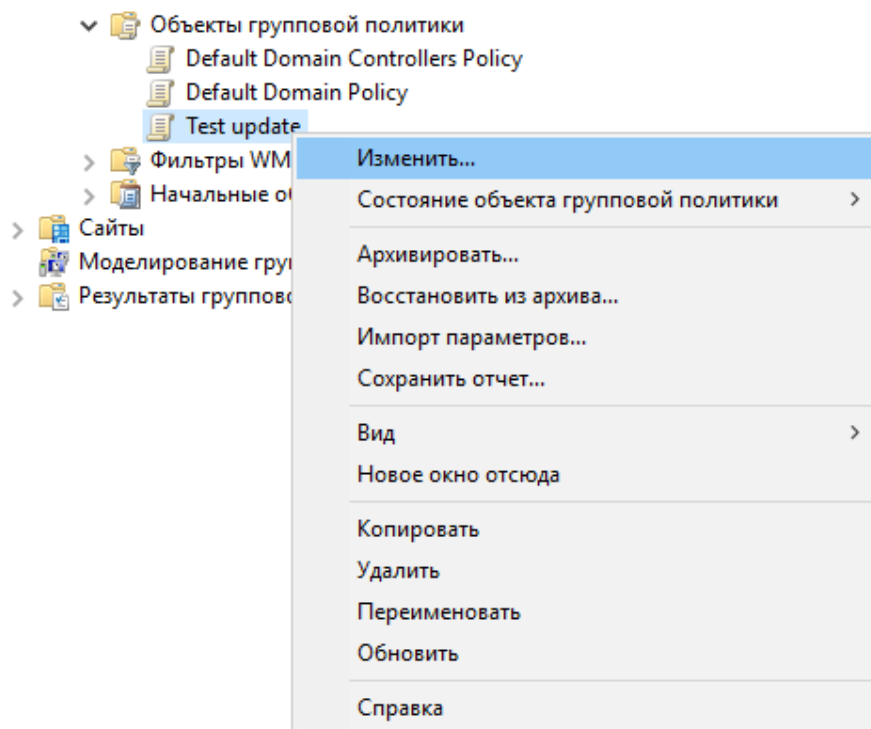


Рис.12. Вызов редактора управления групповыми политиками.

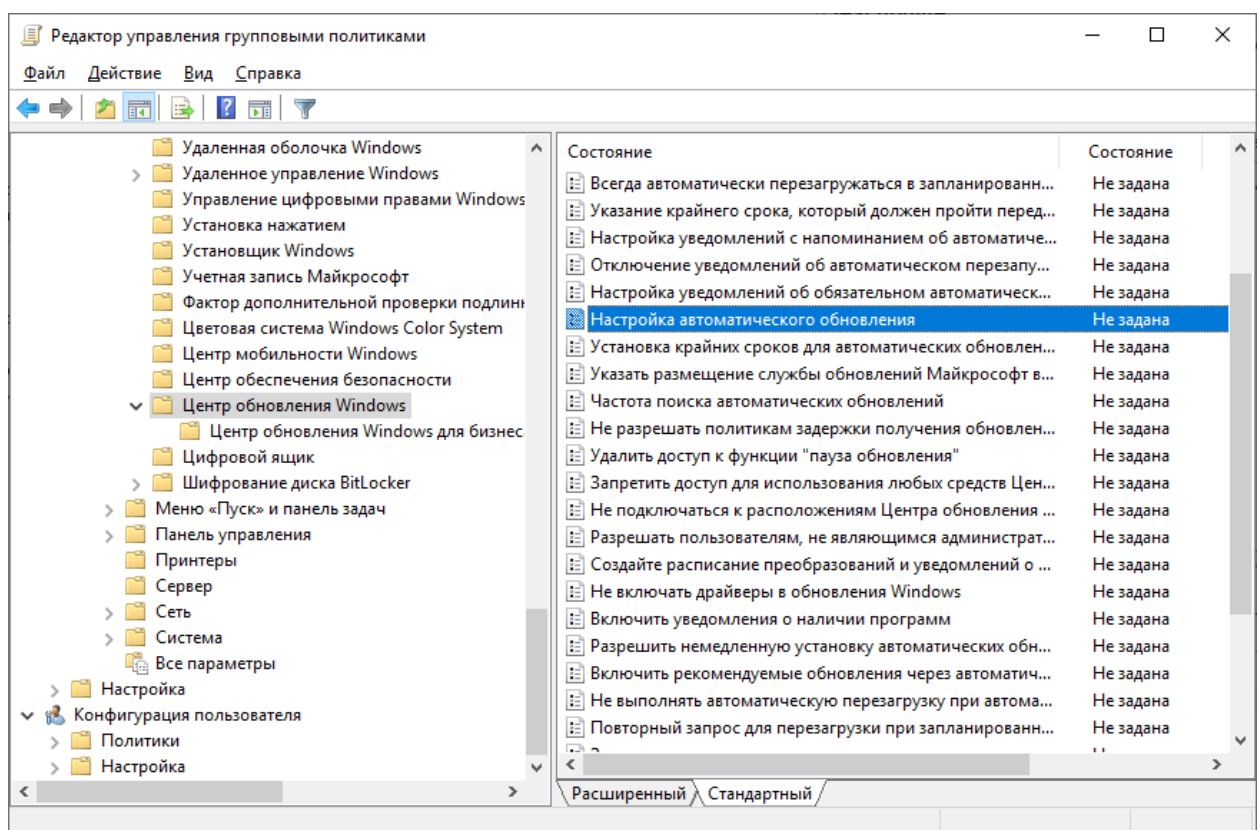


Рис.13. Список параметров групповой политики.

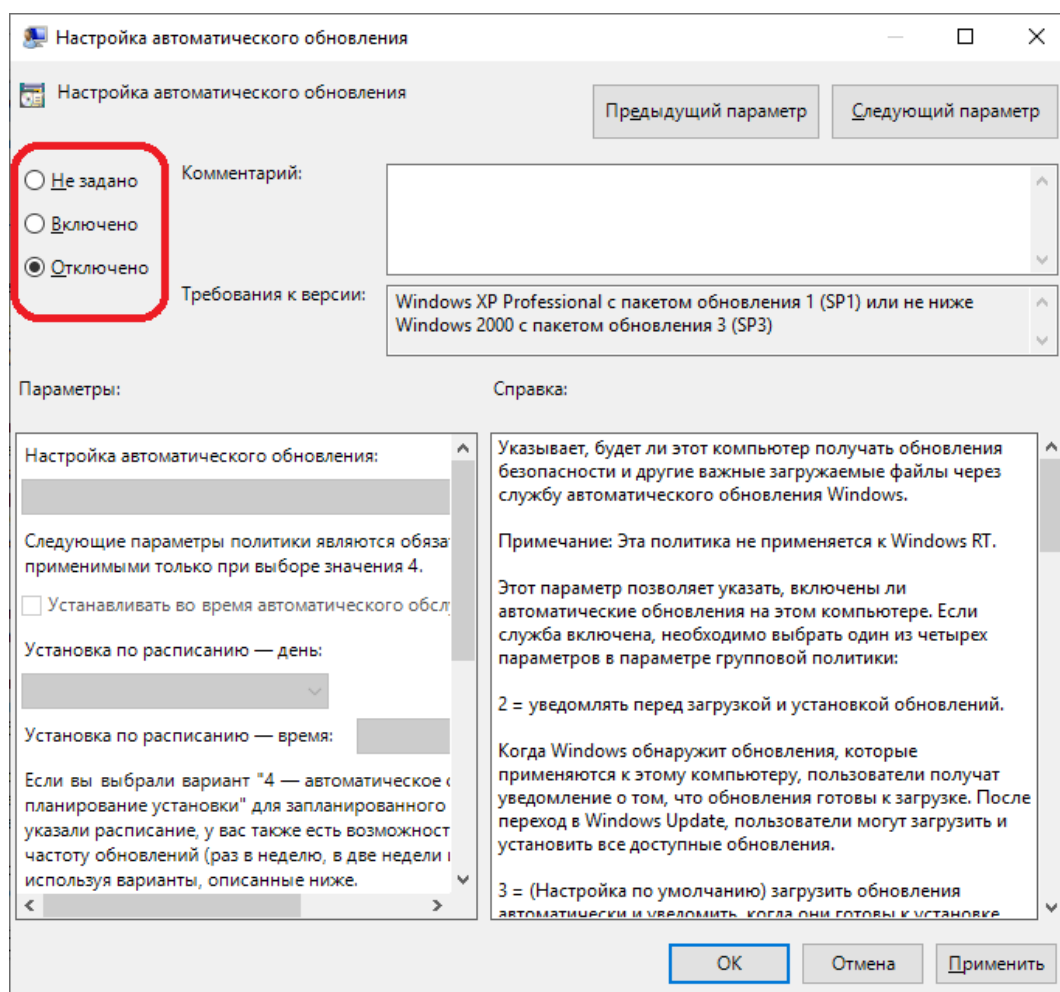


Рис.14. Настройка параметра групповой политики.

12) Связать созданную политику с подразделением, в котором находится компьютер с Windows 10 (например, Организация/Управление 1/Компьютеры) (рис.15).

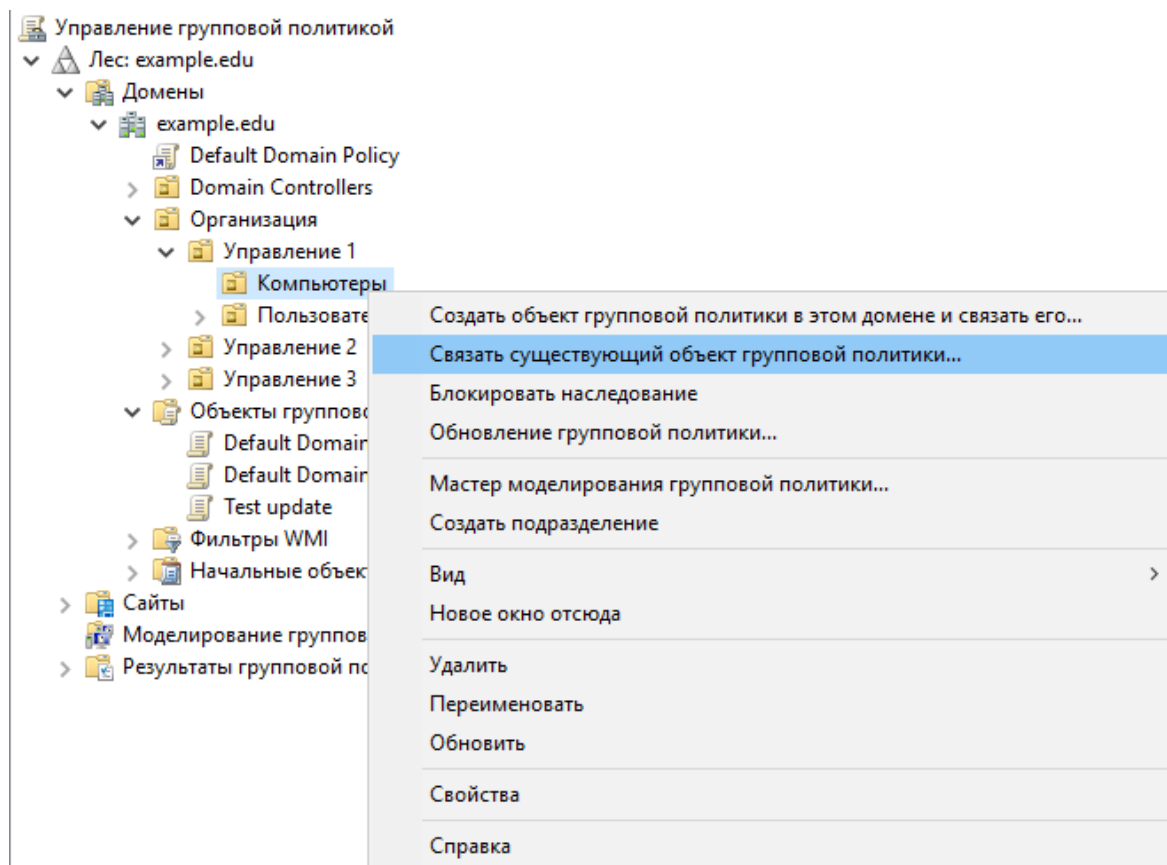


Рис.15. Связь GPO с подразделением.

Просмотреть параметры, которые задаются групповой политикой можно на вкладке «Параметры» в свойствах политики (рис.16).

Добавить в отчет снимок параметров созданной политики — показать раздел «Параметры компьютера».

В конфигурации по умолчанию при переходе на вкладку «Параметры» появляется сообщение о блокировке содержимого конфигурацией усиленной безопасности Internet Explorer. Отключить данную конфигурацию можно в Диспетчере серверов в разделе Локального сервера, параметр «Конфигурация усиленной безопасности Internet Explorer». После применения новых параметров необходимо перезапустить оснастку «Управление групповой политикой».

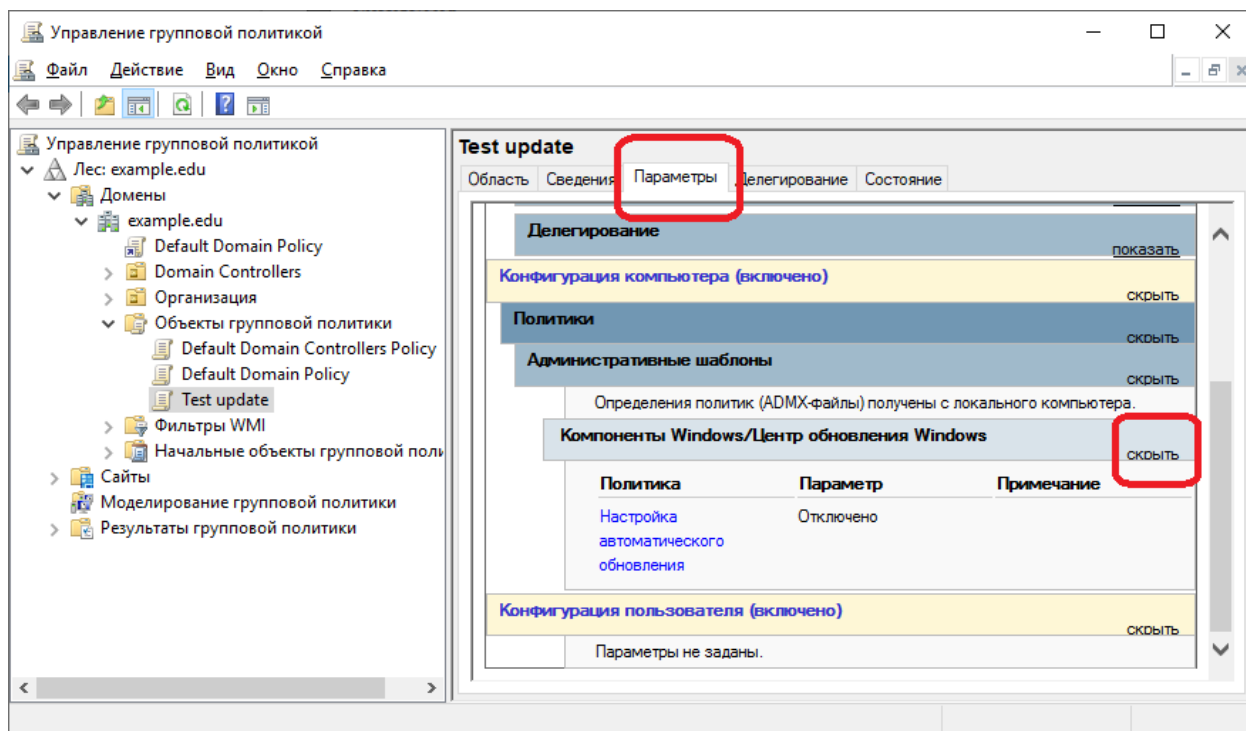


Рис.16. Параметры GPO

13) На Windows 10 форсировать применение групповых политик командой:
 gpupdate /force

Параметры обновлений Windows можно проверить в разделе Settings – Update & Security – Windows Update (рис.17). Снимок данного окна на Windows 10 – в отчет.

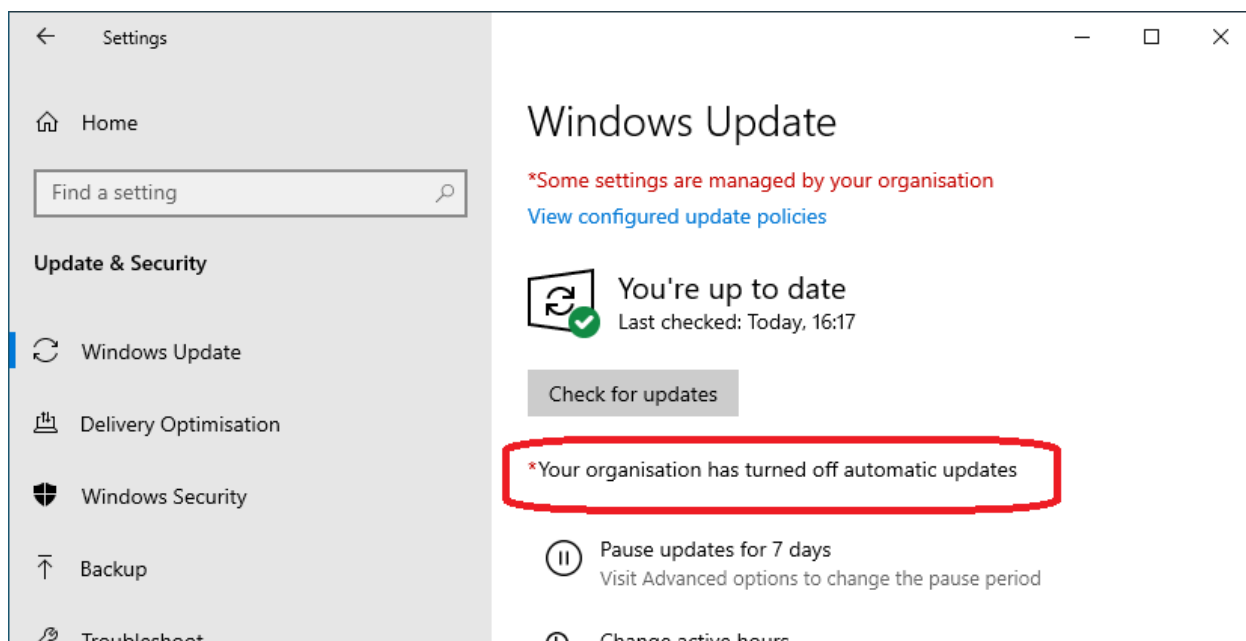


Рис. 17. Параметры обновлений Windows.

14) В оснастке «Управление групповой политикой» создать еще одну групповую политику (например, «Test update 2»). В редакторе политики изменить параметр

«Настройка автоматического обновления», установить значение «Включено», настройка автоматического обновления: «2 – Уведомление о загрузке и автоматическая установка» (рис.18).

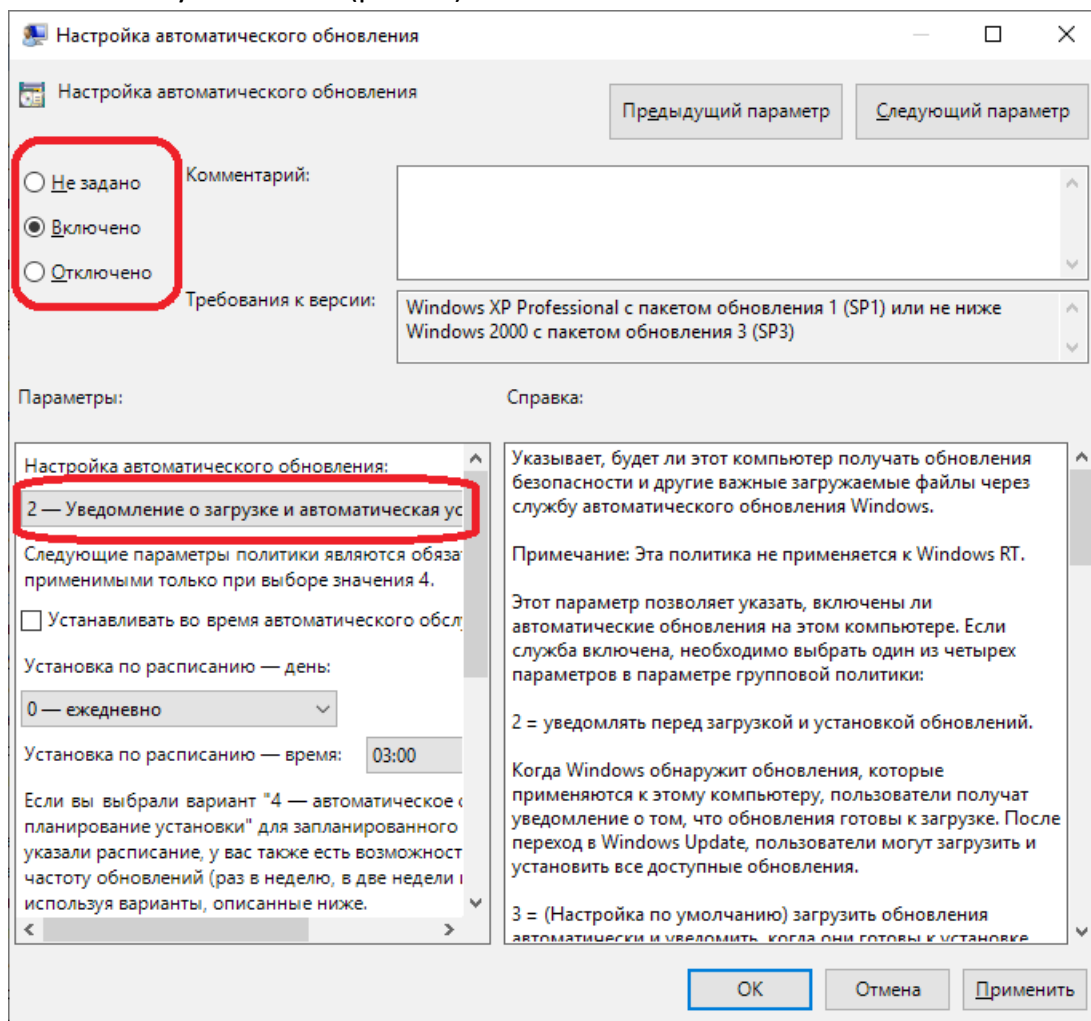


Рис.18. Настройка параметра групповой политики.

15) Применить вторую созданную политику (Test update 2) на уровне всего домена, т.е. связать политику с корневым контейнером домена (например, example.edu).

В той же оснастке открыть свойства подразделения, в котором находится компьютер с Windows 10 (например, Организация/Управление 1/Компьютеры) и проверить приоритет наследования политик на вкладке «Наследование групповой политики» (рис.19).

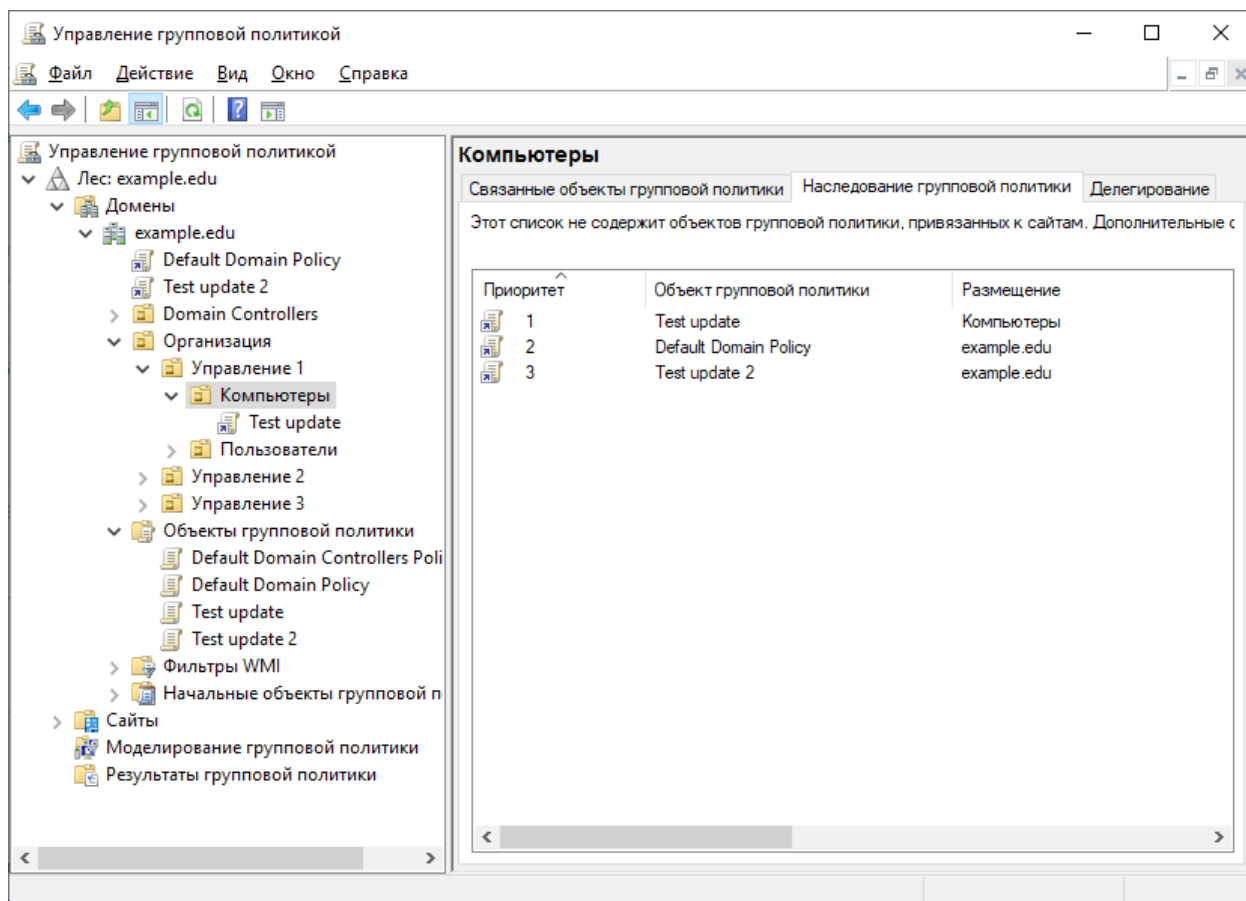


Рис.19. Наследование групповой политики.

Политика на уровне подразделения (OU) имеет приоритет выше, чем политика на уровне домена. Параметры обновления из второй созданной политики (Test update 2) не будут применяться для компьютера Windows 10.

16) Сделать вторую созданную политику (Test update 2) принудительной (рис.20).

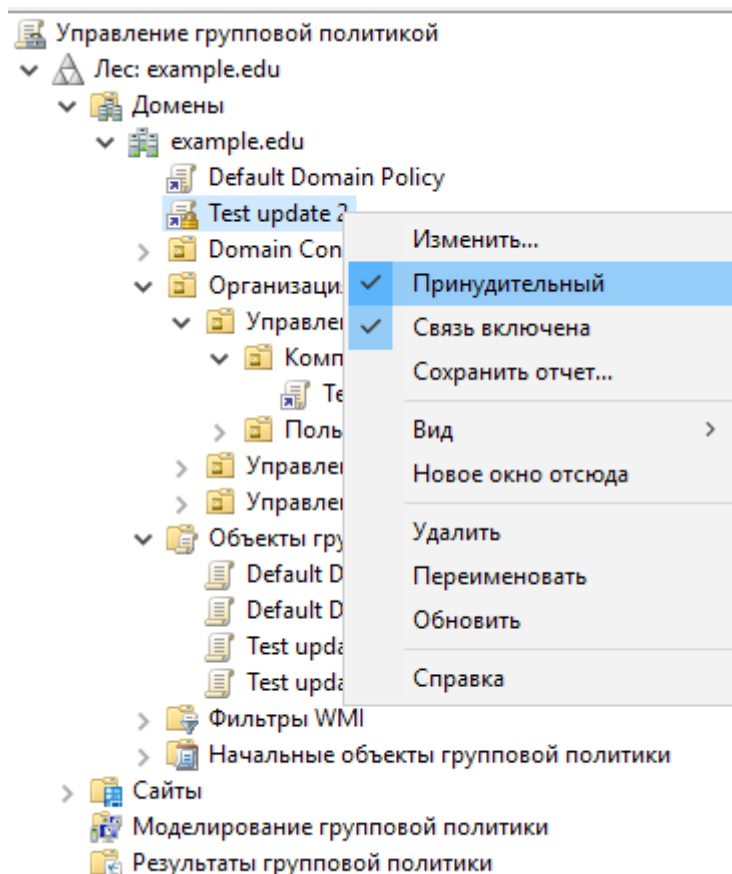


Рис.20. Установка атрибута «Принудительный» на GPO.

Вновь проверить приоритет наследования политик для подразделения с компьютером на Windows 10 (например, Организация/Управление 1/Компьютеры), убедиться в том, что вторая политика (Test update 2) получила максимальный приоритет.

Снимок вкладки «Наследование групповой политики» в свойствах OU с компьютером на Windows 10 – в отчет.

17) На Windows 10 форсировать применение групповых политик и проверить параметры обновлений Windows в разделе Settings – Update & Security – Windows Update. Должны применяться параметры из второй политики (Test update 2). Снимок данного окна на Windows 10 – в отчет.

18) В оснастке «Active Directory – пользователи и компьютеры» создать доменного пользователя (например, user1) (рисунки 21, 22). Перенести пользователя в одно из созданных ранее подразделений (OU) Пользователи (например, Организация/Управление 1/Пользователи).

Новый объект - Пользователь

Создать в: Организация/Управление 1/Пользователи

Имя: Пользователь 1 Инициалы:

Фамилия:

Полное имя: Пользователь 1

Имя входа пользователя:

User1 @example.edu

Имя входа пользователя (пред-Windows 2000):

EXAMPLE\ User1

< Назад Далее > Отмена

Рис.21. Создание пользователя.

Новый объект - Пользователь

Создать в: example.edu/Организация/Управление 1/Поль:

Пароль:

Подтверждение:

☒ Требуется смена пароля при следующем входе в систему

☐ Запретить смену пароля пользователем

☐ Срок действия пароля не ограничен

☐ Отключить учетную запись

< Назад Далее > Отмена

Рис.22. Параметры пароля пользователя.

19) В оснастке «Управление групповой политикой» создать третью групповую политику (например, «Test link»), привязать политику к подразделению пользователей (например, Организация/Управление 1/Пользователи).

В редакторе политики настроить создание ярлыка на рабочем столе пользователя. Для этого перейти в раздел Конфигурация пользователя — Настройка — Конфигурация Windows — Ярлыки, создать ярлык. Указать имя ярлыка, размещение — «Рабочий стол». Тип объекта — «Объект оболочки». Выбрать целевой объект — «Центр управления сетями и общим доступом». (рис.23.)

Новые свойства ярлыка

Общие Общие параметры

Действие: Обновить

Имя: Центр управления сетями

Тип объекта: Объект оболочки

Размещение: Рабочий стол

Целевой объект: Центр управления сетями и общим доступом

Аргументы:

Начать с:

Быстрый вызов: Нет

Выполнение: Обычный размер окна

Комментарий:

Путь к файлу значка:

Индекс значка: 0

OK Отмена Применить Справка

Рис.23. Создание ярлыка средствами GPO.

На вкладке общие параметры отметить пункт «Выполнять в контексте безопасности вошедшего пользователя» для создания ярлыка на рабочем столе пользователя (рис.24). Если в качестве размещения выбрана публичная директория (All Users/Рабочий стол), то данный параметр необходимо отключить.

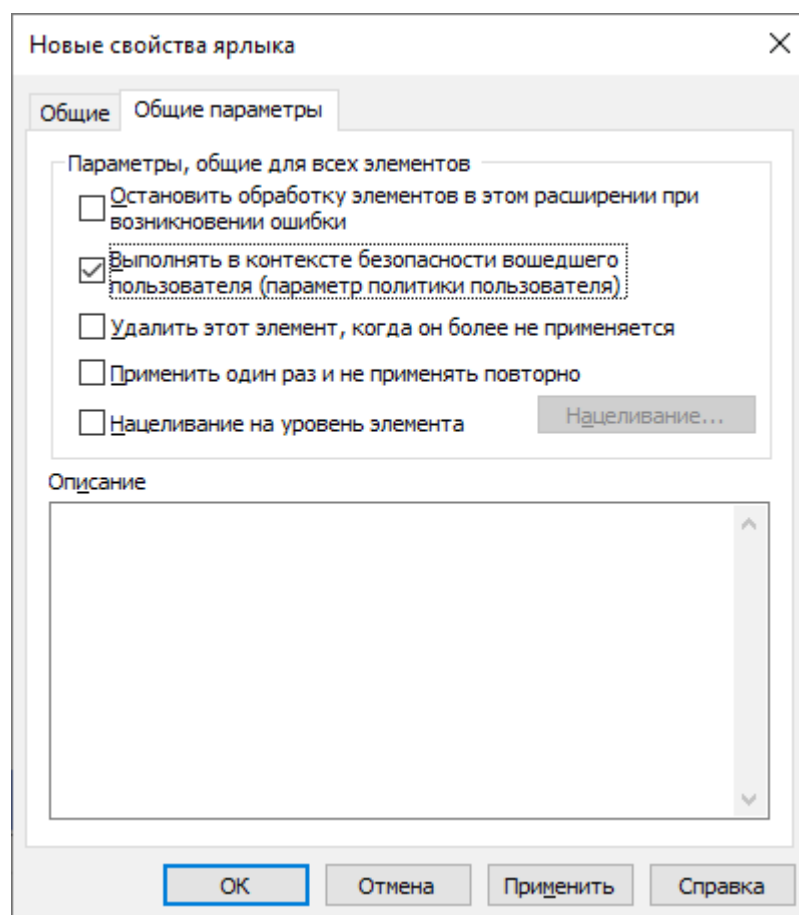


Рис.24. Параметры выполнения политики.

Добавить в отчет снимок параметров созданной политики в оснастке «Управление групповой политикой» - вкладка «Параметры», показать раздел «Параметры пользователя».

20) Выполнить вход в Windows 10 с доменной учетной записью. На экране приветствия выбрать «Other user», ввести имя и пароль доменной учетной записи (например, User1). Домен (NetBIOS имя домена) подставляется автоматически. Проверить появление ярлыка на рабочем столе.

По умолчанию доменные пользователи (члены группы «Пользователи домена») не обладают административными полномочиями на компьютерах домена (не входят в локальную группу «Администраторы»). При необходимости выполнить вход с локальной учетной записью на компьютере необходимо ввести имя пользователя в одном из форматов:

<имя ПК>\<имя локального пользователя> (например, «Desktop01\User»);
.\<имя локального пользователя> (например, «.\User»).

21) На Windows Server 2019 в оснастке «Управление групповой политикой» проверить результаты групповой политики (с помощью одноименного раздела)

для компьютера с Windows 10 (например, desktop01) и доменного пользователя (например, EXAMPLE\user1) (рисунки 25, 26).

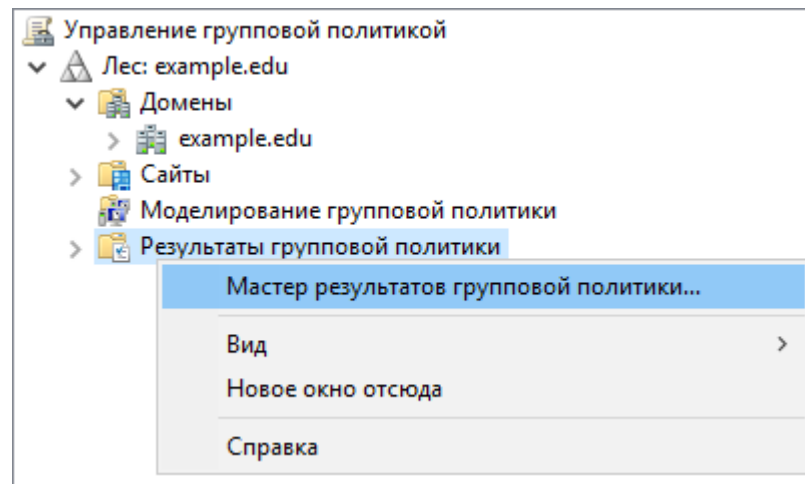


Рис.25. Вызов мастера результатов групповой политики.

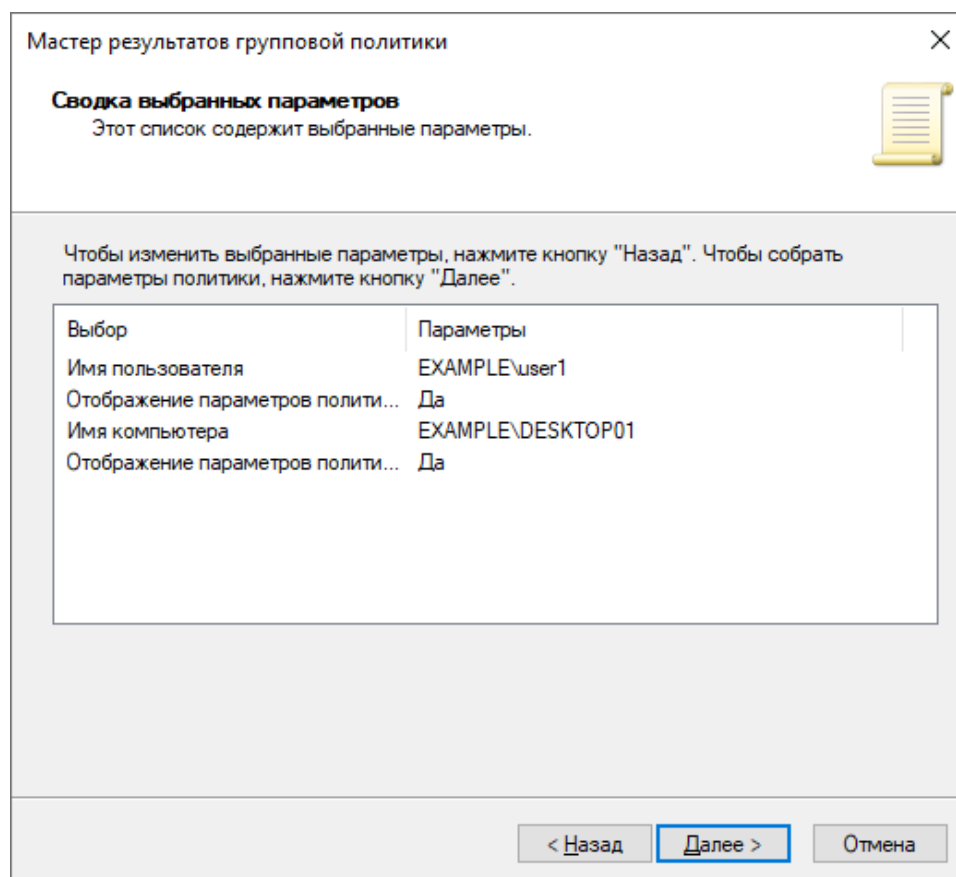


Рис. 26. Параметры результатов групповой политики

Сохранить результат групповой политики в файл и добавить к отчету по лабораторной работе.

Сформировать аналогичный отчет также можно на компьютере с Windows 10 с помощью команды:

gpresult /H <имя файла> (для сбора конфигурации компьютера необходимо выполнять с правами администратора).

Отчет:

- снимок окна «Active Directory – пользователи и компьютеры» со структурой созданных подразделений;
- снимок параметров объекта групповой политики в оснастке «Управление групповой политикой» на вкладке «Параметры» - показать раздел «Параметры компьютера» (этап 12, рис.16);
- снимок окна Settings – Update & Security – Windows Update на Windows 10 (этап 13);
- снимок вкладки «Наследование групповой политики» в свойствах OU с компьютером на Windows 10 (этап 16);
- снимок окна Settings – Update & Security – Windows Update на Windows 10 (этап 17);
- снимок параметров созданной политики в оснастке «Управление групповой политикой» - вкладка «Параметры» - показать раздел «Параметры пользователя» (этап 19).
- результат групповой политики в виде файла (этап 21).