

Санкт-Петербургское государственное бюджетное
профессиональное образовательное учреждение
«Академия управления городской средой, градостроительства и печати»

ПРИНЯТО

на заседании педагогического совета

Протокол № 2

«26» декабря 2023 г.



КОМПЛЕКТ КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ

по текущему контролю успеваемости
и промежуточной аттестации
по профессиональному модулю

**ПМ.04 ВЫПОЛНЕНИЕ РАБОТ ПО ОДНОЙ ИЛИ НЕСКОЛЬКИМ ПРОФЕССИЯМ
РАБОЧИХ, ДОЛЖНОСТЯМ СЛУЖАЩИХ**

по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Квалификация

Техник по защите информации

Форма обучения

очная

Санкт-Петербург
2023 год

Комплект контрольно-оценочных средств по профессиональному модулю ПМ.04
Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих
разработан на основе Федерального государственного образовательного стандарта по
специальности 10.02.05 Обеспечение информационной безопасности автоматизированных
систем, утвержденного приказом Минобрнауки России от 09.12.2016 № 1553.

СОГЛАСОВАНО

ООО «ДЖИ-ТИ ИНВЕСТ»

Генеральный директор

 П.С. Тюганов

«26» декабря 2023 г.

Комплект контрольно-оценочных средств по профессиональному модулю рассмотрен на
заседании методического совета СПб ГБПОУ «АУГСГиП»

Протокол № 2 от «29» ноября 2023 г.

Комплект контрольно-оценочных средств по профессиональному модулю рассмотрен на
заседании цикловой комиссии общетехнических дисциплин и компьютерных технологий

Протокол № 4 от «21» ноября 2023 г.

Председатель цикловой комиссии: Караченцева М.С.



СОДЕРЖАНИЕ

1. ПАСПОРТ КОМПЛЕКТА ОЦЕНОЧНЫХ СРЕДСТВ	4
2. СИСТЕМА КОНТРОЛЯ И ОЦЕНКИ ОСВОЕНИЯ ПРОГРАММЫ ПМ.04 ВЫПОЛНЕНИЕ РАБОТ ПО ПРОФЕССИИ 16199 ОПЕРАТОР ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫХ И ВЫЧИСЛИТЕЛЬНЫХ МАШИИ.....	7
2.1. Формы промежуточной аттестации по ППСЗ при освоении профессионального модуля ...	7
2.2. Организация контроля и оценки освоения программы ПМ.....	7
3. КОМПЛЕКТ МАТЕРИАЛОВ ДЛЯ ОСВОЕНИЯ УМЕНИЙ И УСВОЕНИЯ ЗНАНИЙ, ОЦЕНКИ СФОРМИРОВАННОСТИ ОБЩИХ И ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНЦИЙ ПО ВИДУ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ	8
3.1. Задания для оценки освоения теоретического курса профессионального модуля.....	8
3.1.1. Оценка освоения теоретического курса профессионального модуля по МДК.04.01...8	
3.2. Контрольно-оценочные материалы для промежуточной аттестации	108

1. ПАСПОРТ КОМПЛЕКТА ОЦЕНОЧНЫХ СРЕДСТВ

Результатом освоения профессионального модуля является готовность обучающегося к выполнению вида профессиональной деятельности по участию в планировании и организации работ по обеспечению защиты объекта и составляющих его профессиональных компетенций, а также общих компетенций, формирующихся в процессе освоения ППССЗ в целом.

Комплект контрольно-оценочных средств позволяет оценивать:

1. Освоение профессиональных компетенций (ПК), соответствующих виду профессиональной деятельности, и общих компетенций (ОК):

Код	Наименование результата обучения
ПК 4.1.	Подготавливать к работе, настраивать и обслуживать аппаратное обеспечение и операционную систему персонального компьютера.
ПК 4.2.	Подготавливать к работе, настраивать и обслуживать периферийные устройства персонального компьютера и компьютерную оргтехнику.
ПК 4.3.	Обрабатывать аудио и визуальный контент средствами звуковых, графических и видеоредакторов
ПК 4.4.	Обеспечивать меры по информационной безопасности.
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности
ОК 9.	Использовать информационные технологии в профессиональной деятельности
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках
ОК 11.	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере

2. Приобретение в ходе освоения профессионального модуля практического опыта:

Освоение практического опыта

Иметь практический опыт	Виды работ на учебной и/ или производственной практике и требования к их выполнению
подготовки к работе, настройки и обслуживанию сопровождению аппаратного, программного обеспечения и оргтехники	<p>Подготовка к работе серверной инфраструктуры на базе Windows Server</p> <p>Настройка контроллера домена в среде Windows.</p> <p>Настройка синхронизации по протоколу NTP</p> <p>Подготовка к работе и подключение сетевых периферийных устройств через Групповую политику в Windows Server</p> <p>Обеспечение применения технологии DirectAccess при осуществлении соединения клиента с корпоративной сетью.</p> <p>Обеспечить шифрования и расширенного аудита системы в ОС Windows Server 2012 R2</p> <p>Применение групповых политик для обеспечения политики безопасности</p> <p>Поиск уязвимостей информационной системы</p> <p>Выполнить установку, настройку, обновлений операционных систем и прикладного программного обеспечения на персональном компьютере.</p> <p>Подготовить рабочее место, настроить периферийные устройства персонального компьютера и компьютерной оргтехники.</p> <p>Обеспечить информационную безопасность рабочего места.</p>
обработки аудио, визуального и мультимедийного контента с помощью специализированных программ-редакторов	<p>Создание анимации текста в приложении GIMP</p> <p>Нормализация аудиофайла с помощью приложения Audacity</p> <p>Создание видеоролика в приложении MovAvi</p>

3. Освоение умений и усвоение знаний:

№	Освоенные умения, усвоенные знания
31	особенности установки, настройки и администрирования операционных систем
32	современные технологии поиска уязвимостей безопасности информационных систем
33	современные технологии анализа безопасности веб-сервисов и методы поиска уязвимостей веб-приложений
34	способы повышения защищенности веб-приложений
35	виды компьютерной графики
36	характеристики графических изображений
37	форматы графических, аудио и видео файлов

№	Освоенные умения, усвоенные знания
38	особенности восприятия изображения человеком
39	рынок современного программного обеспечения в области обработки различных видов информации
У1	производить установку, настройку и администрирование операционных систем
У2	производить настройку периферийных устройств
У3	осуществлять поиск уязвимостей информационных систем
У4	оценивать риски информационной безопасности с использованием классификации веб-угроз
У5	работать с растровыми и векторными изображениями
У6	осуществлять обработку аудиоинформации
У7	осуществлять обработку видеоинформации

Формой аттестации по профессиональному модулю является экзамен по профессиональному модулю. Итогом экзамена является однозначное решение: «вид профессиональной деятельности освоен/не освоен».

2. СИСТЕМА КОНТРОЛЯ И ОЦЕНКИ ОСВОЕНИЯ ПРОГРАММЫ ПМ.04 ВЫПОЛНЕНИЕ РАБОТ ПО ПРОФЕССИИ 16199 ОПЕРАТОР ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫХ И ВЫЧИСЛИТЕЛЬНЫХ МАШИН

2.1. Формы промежуточной аттестации по ППСЗ при освоении профессионального модуля

Элементы модуля, профессиональный модуль	Формы промежуточной аттестации
МДК 04.01 Выполнение работ по профессии 16199 «Оператор электронно-вычислительных и вычислительных машин»	Дифференцированный зачет
Производственная практика	Зачет
ПМ	Экзамен

2.2. Организация контроля и оценки освоения программы ПМ

Итоговый контроль освоения вида профессиональной деятельности Выполнение работ по профессии 16199 Оператор электронно-вычислительных и вычислительных машин осуществляется на экзамене. Условием допуска к экзамену является положительная аттестация по МДК, учебной практике и производственной практике.

Экзамен проводится в виде выполнения практического экзаменационного задания.

Условием положительной аттестации (вид профессиональной деятельности освоен) на экзамене квалификационном является положительная оценка освоения всех профессиональных компетенций по всем контролируемым показателям. При отрицательном заключении хотя бы по одной из профессиональных компетенций принимается решение «вид профессиональной деятельности не освоен».

Промежуточный контроль освоения профессионального модуля осуществляется при проведении экзамена по МДК и зачета по учебной практике. Предметом оценки освоения МДК являются умения и знания. Экзамен по МДК проводится по заранее подготовленным и утвержденным экзаменационным вопросам. Условием положительной аттестации является получение обучающимся на экзамене оценки «удовлетворительно», «хорошо», «отлично».

Предметом оценки по учебной и производственной практике является освоение общих и профессиональных компетенций, умений. Контроль и оценка по учебной и (или) производственной практике проводится на основе Аттестационного листа обучающегося с места прохождения практики.

Текущий контроль по МДК осуществляется в форме выполнения практических проверочных заданий, устных зачетов.

**3. КОМПЛЕКТ МАТЕРИАЛОВ ДЛЯ ОСВОЕНИЯ
УМЕНИЙ И УСВОЕНИЯ ЗНАНИЙ,
ОЦЕНКИ СФОРМИРОВАННОСТИ ОБЩИХ
И ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНЦИЙ
ПО ВИДУ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ**

3.1. Задания для оценки освоения теоретического курса профессионального модуля

3.1.1. Оценка освоения теоретического курса профессионального модуля по МДК.04.01

Дидактические единицы	Проверяемые ОК, ПК, У, З	Формы контроля (наименование контрольной точки)	
		Текущая аттестация	Промежуточная аттестация
Тема 1.1 Настройка аппаратного обеспечения и операционной системы персонального компьютера	У1, З1 ОК1-ОК9 ПК 4.1	Практическая работа № 2. Установка контроллера домена. Использование Windows PowerShell для администрирования AD DS.	Практические задания на экзамене
	У1, У2, З1 ОК1-ОК9 ПК 4.2	Практическая работа № 4. Подключение сетевых периферийных устройств через Групповую политику	
	З1 ОК1-ОК9 ПК 4.1, ПК 4.2	Устный зачет по теме 1.1	
Тема 1.2 Обработка видео- и аудиоконтента	У6, У7, З9 ОК1-ОК9 ПК 4.3	Практическая работа № 10. Создание ролика из фотографий	
		Устный зачет по теме 1.2	
	У6, У7, З9 ОК1-ОК9 ПК 4.3	Практическая работа № 13 Запись звука с микрофона. Резка аудиофайлов и удаление ненужных моментов	
Тема 1.3 Обработка графических изображений	У5, З5, З6, З7, З8 ОК1-ОК9 ПК 4.3	Практическая работа № 15. Работа со слоями	
		Устный зачет по теме 1.3	
Тема 1.4 Обеспечение информационной безопасности	У3, З4, ОК1-ОК9 ПК 4.4	Практическая работа № 19. Поиск уязвимостей информационных систем	
	У4, З3, ОК1-ОК9 ПК 4.4	Практическая работа № 20. Оценка рисков информационной безопасности с использованием классификации веб-угроз	
	З3, ОК1-ОК9 ПК 4.4	Устный зачет по теме 1.4	

Практическая работа № 2 «Установка контроллера домена. Использование Windows PowerShell для администрирования AD DS»

Инструкция для обучающихся

Внимательно прочитайте задание. Проведите обследование объектов на предмет состояния инженерно-технического укрепления.

Время выполнения – 90 минут.

Задание

1. Настройка имени сервера и статического IP-адреса

1.1 Откройте **Пуск > Компьютер (пр. кнопкой мыши) > Свойства** (Рис.12).

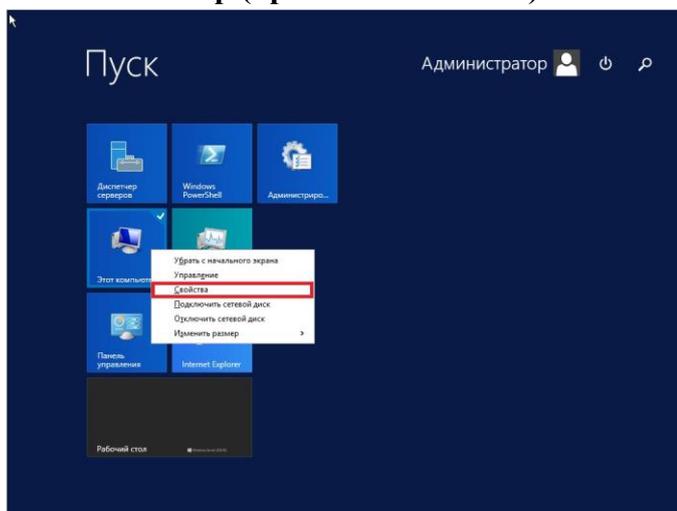


Рис. 1

1.2 В открывшемся окне выберите **Изменить параметры**.

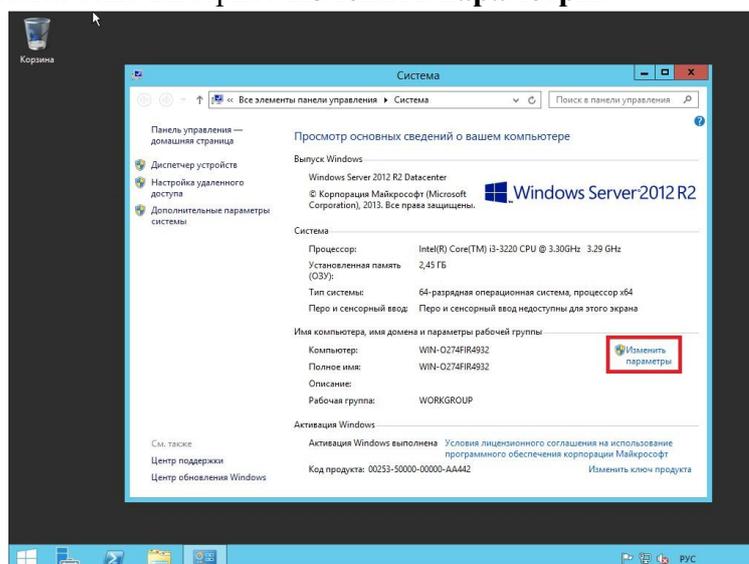


Рис. 2

1.3 В **Свойствах системы** выберите вкладку **Имя компьютера** и нажмите **Изменить...** . В появившемся окне укажите новое имя сервера в поле **Имя компьютера** (прим. в данном руководстве это **SERVER2012R2**), затем нажмите **ОК**.

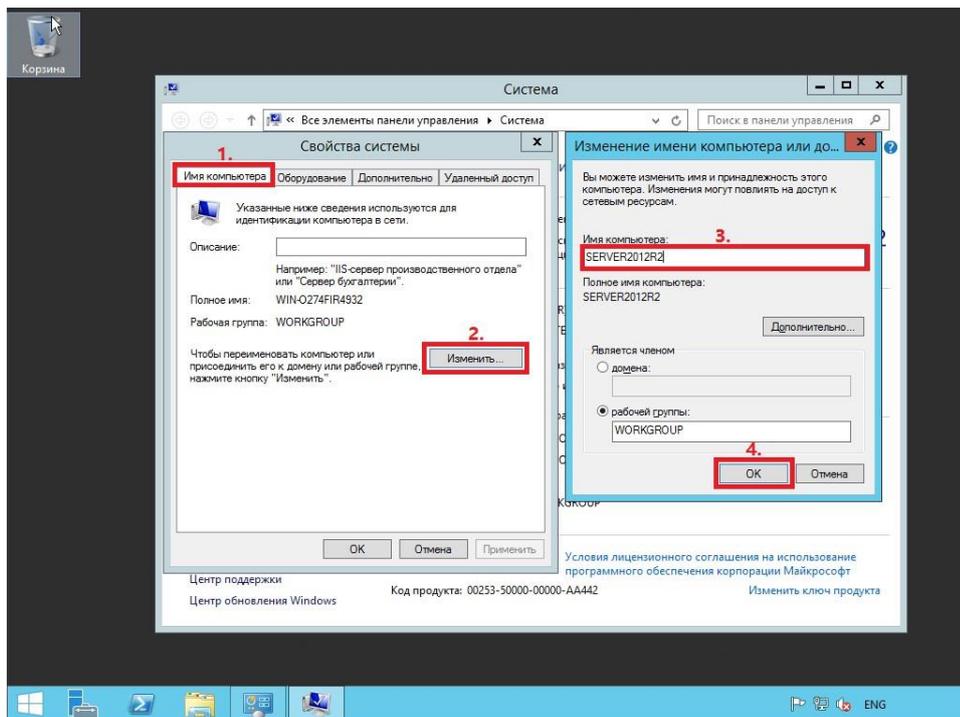
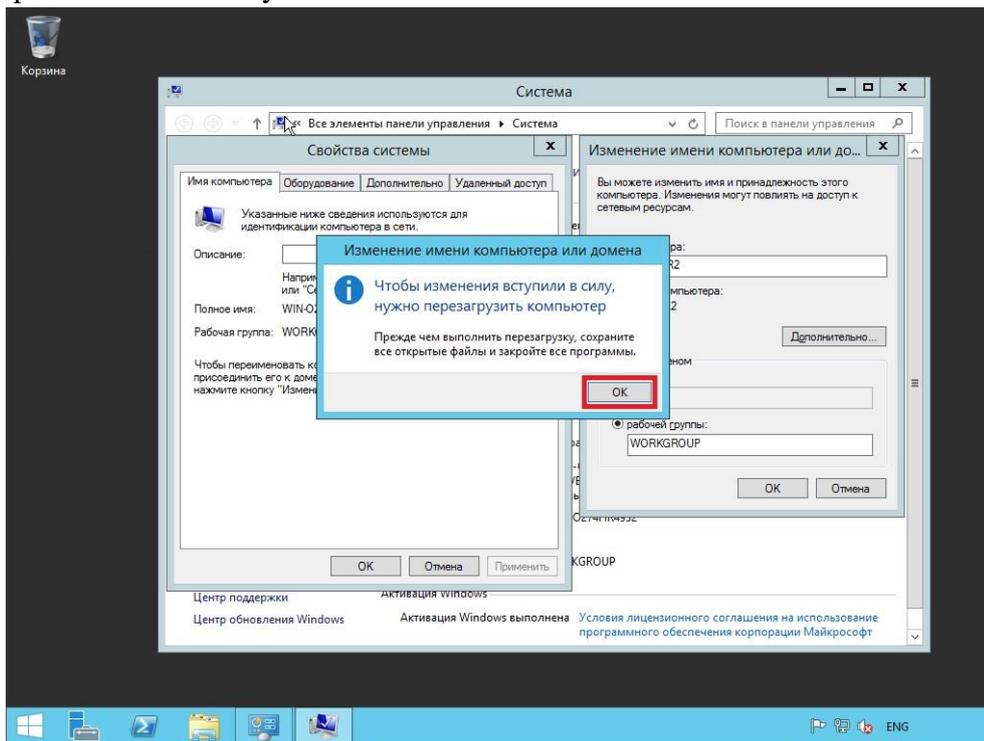


Рис. 3

1.4 Система предупредит о том, что для применения новых настроек необходимо перезагрузить сервер. Нажмите кнопку **ОК**



1.5

Рис. 4

1.6 После перезагрузки, в правом нижнем углу кликните (пр. кнопкой мыши) на иконке сетевого соединения. В открывшемся меню выберите **Центр управления сетями и общим доступом**

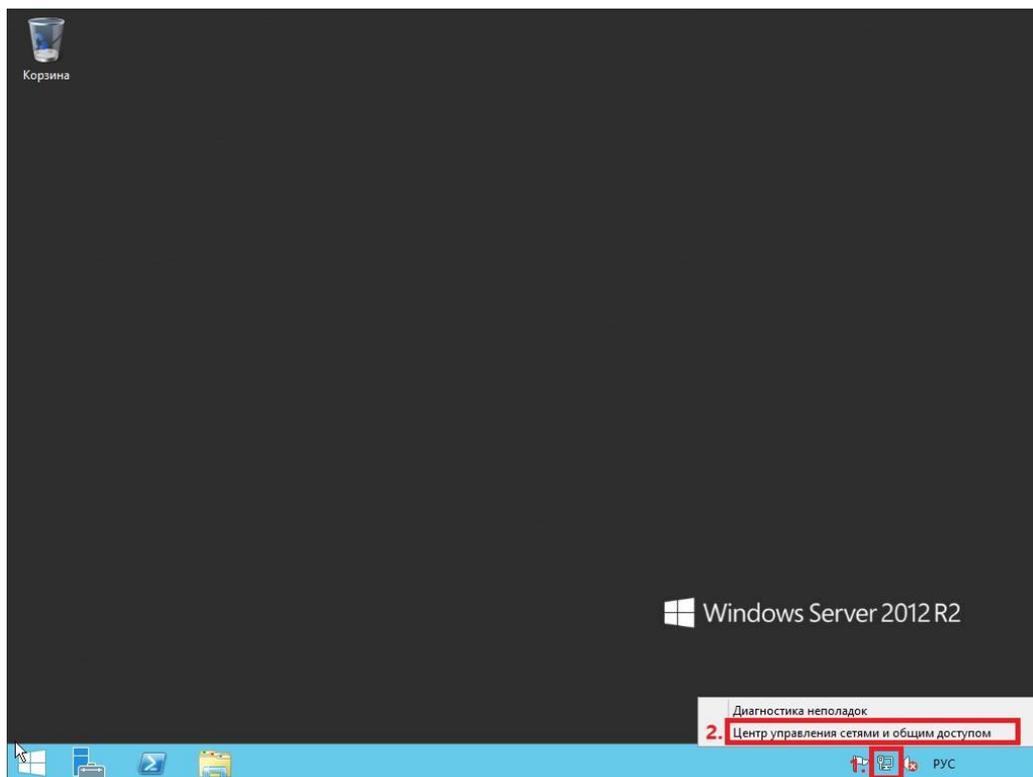


Рис. 5

1.7 В открывшемся окне выберите **Изменение параметров адаптера**

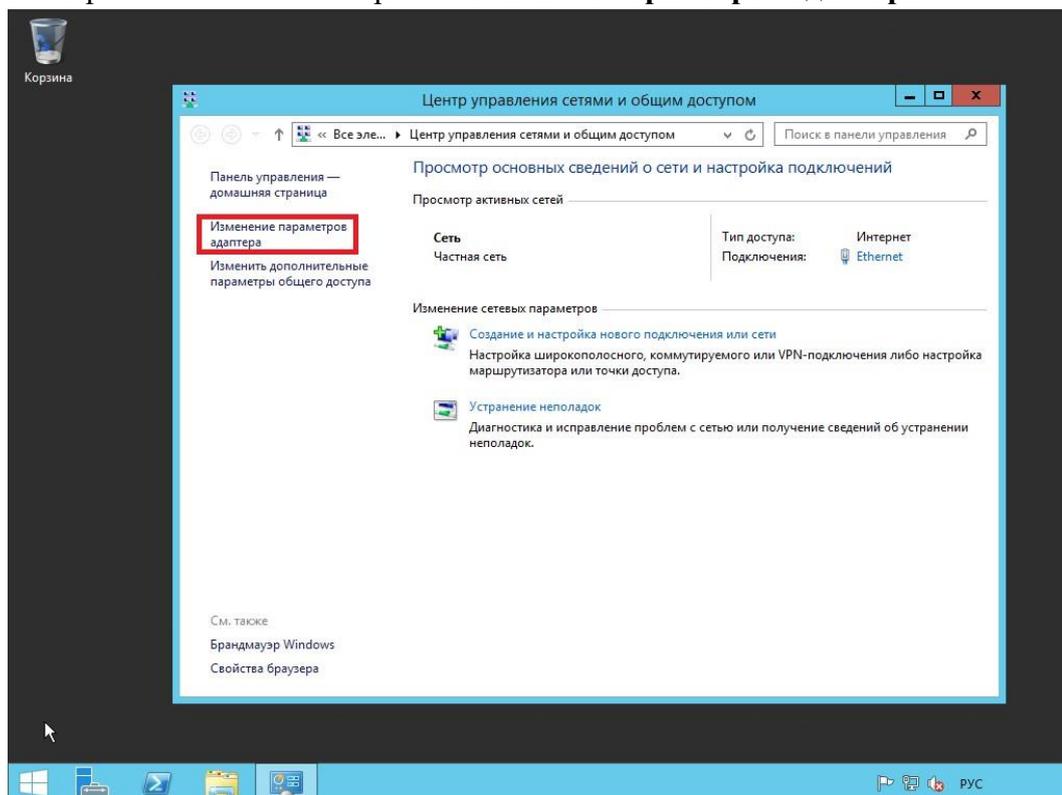


Рис. 6

1.8 В открывшемся окне Сетевые подключения нажмите правой кнопкой мыши на сетевом подключении и выберите пункт **Свойства**. В появившемся окне выделите **Протокол Интернета версии 4 (TCP/IPv4)** и нажмите **Свойства**

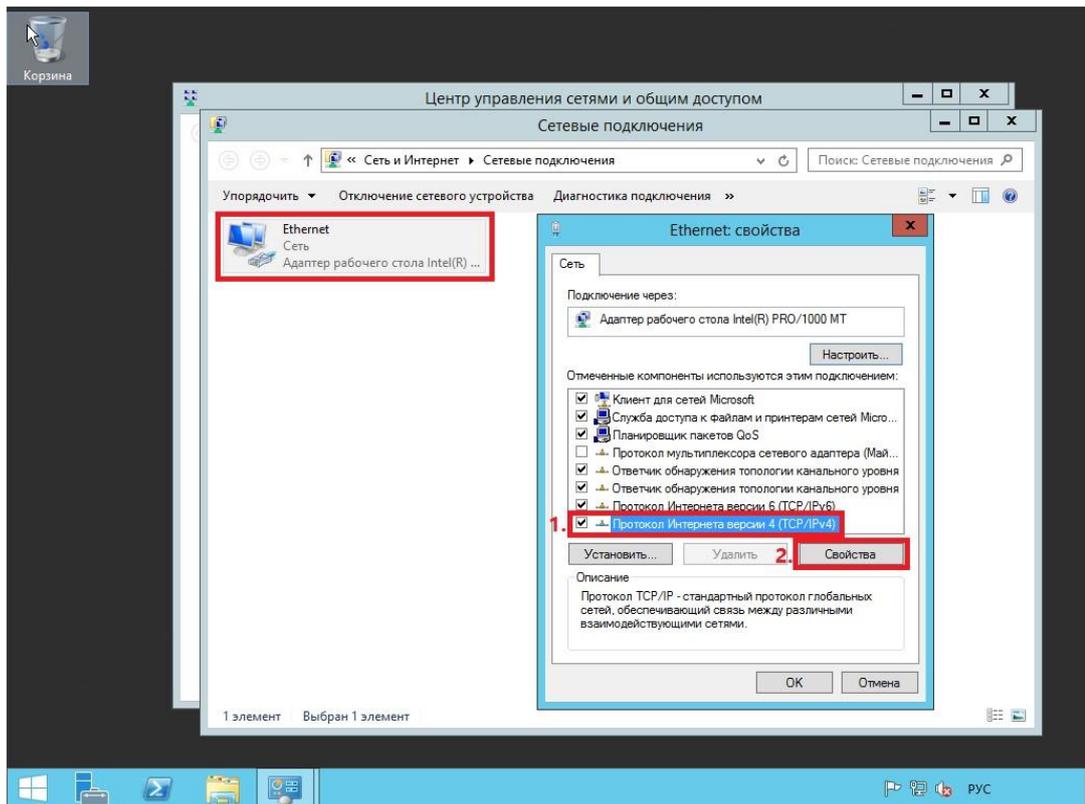


Рис. 7

1.9 В свойствах, на вкладке **Общие** выберите пункт **Использовать следующий IP-адрес**. В соответствующие поля введите **свободный IP-адрес**, **маску подсети** и **основной шлюз**. Затем выберите пункт **Использовать следующие адреса DNS-серверов**. В поле **предпочитаемый DNS-сервер** введите **IP-адрес сервера**, после чего нажмите **ОК**.

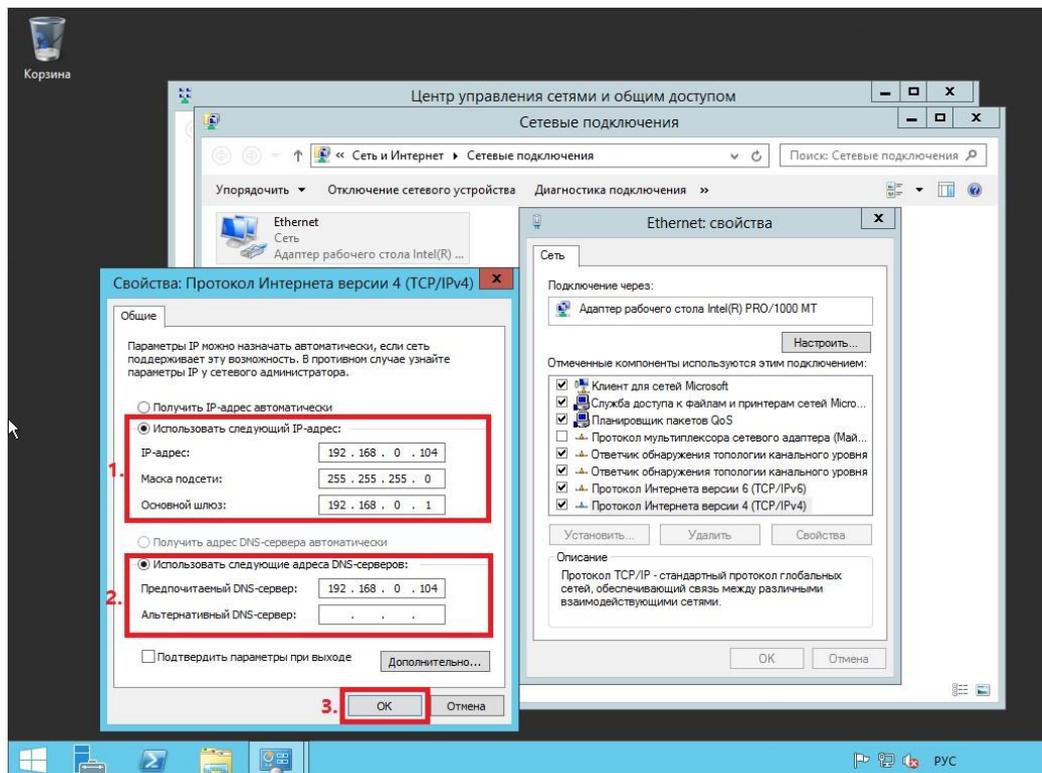


Рис. 8

Установка роли Active Directory Domain Services

2.1 Откройте окно диспетчера сервера и выберите пункт **Добавить роли и компоненты** (Рис.9).

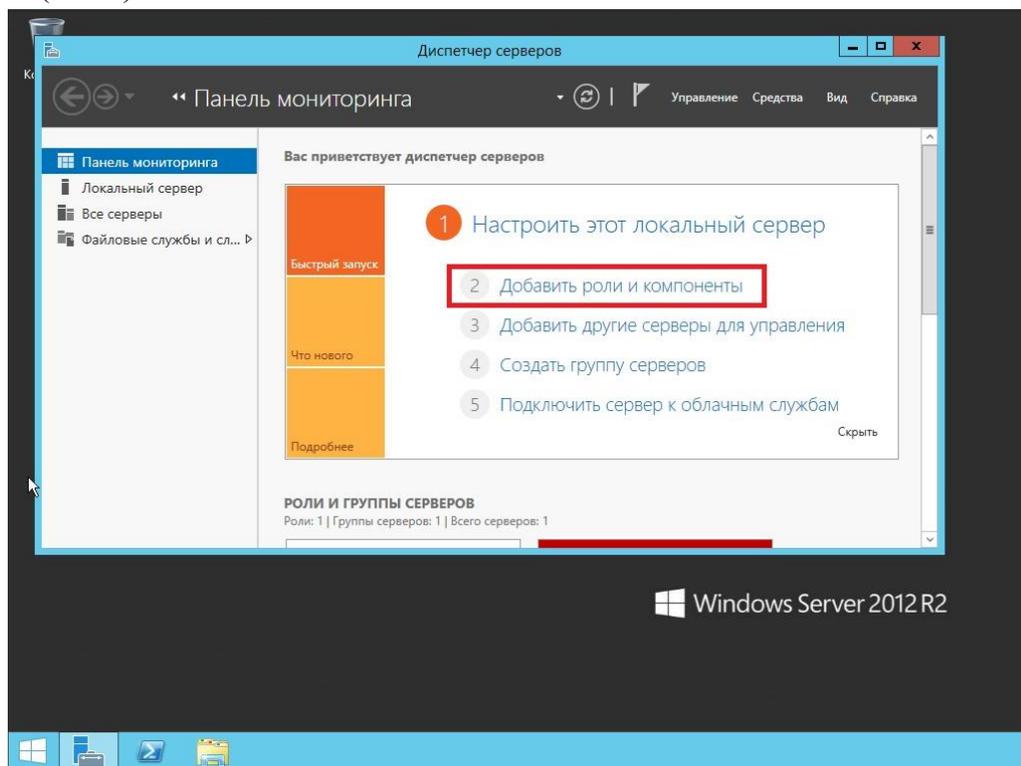


Рис. 9

2.2 В появившемся окне нажмите **Далее**

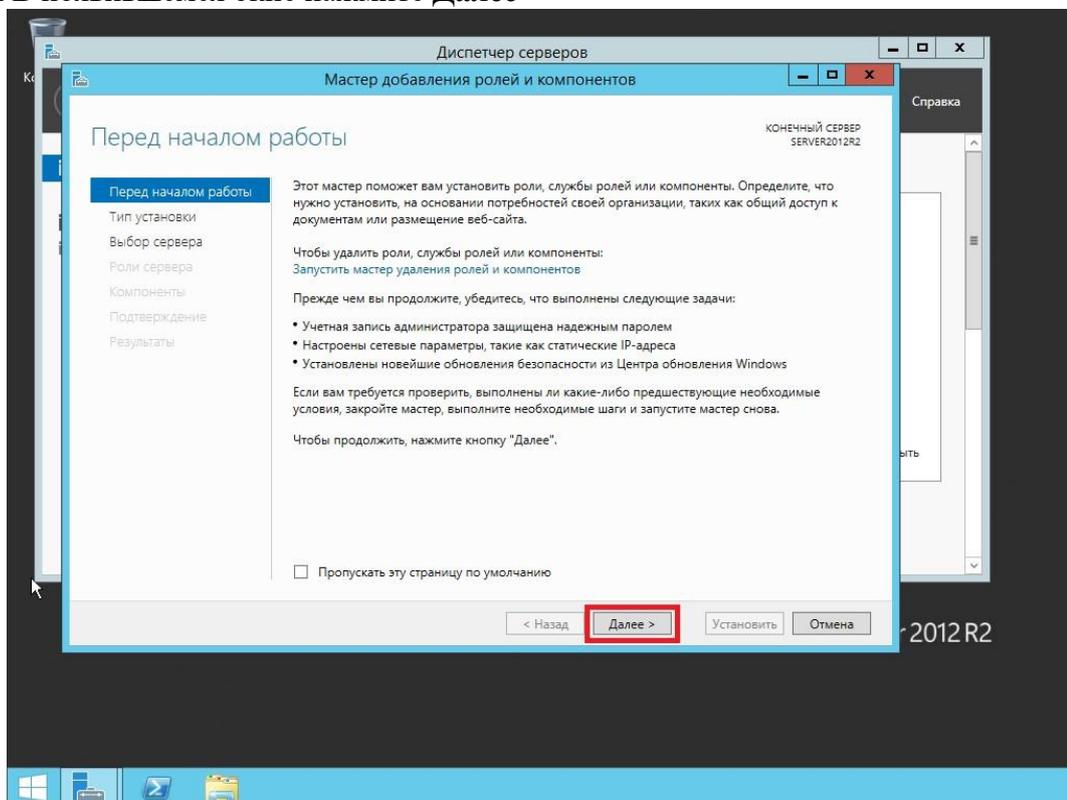


Рис. 10

2.3 Выберите пункт **Установка ролей и компонентов**, затем нажмите **Далее**

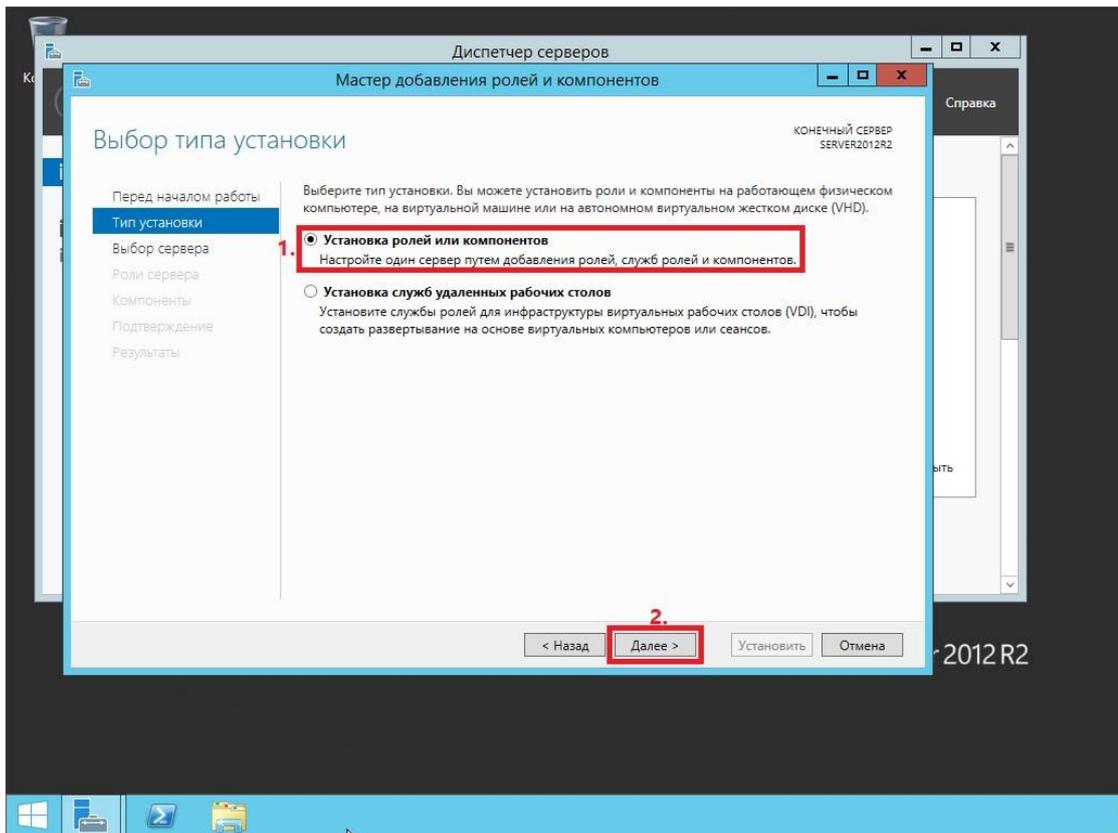


Рис. 11

2.4 Выберите сервер, на который будет производиться установка роли, затем нажмите **Далее**

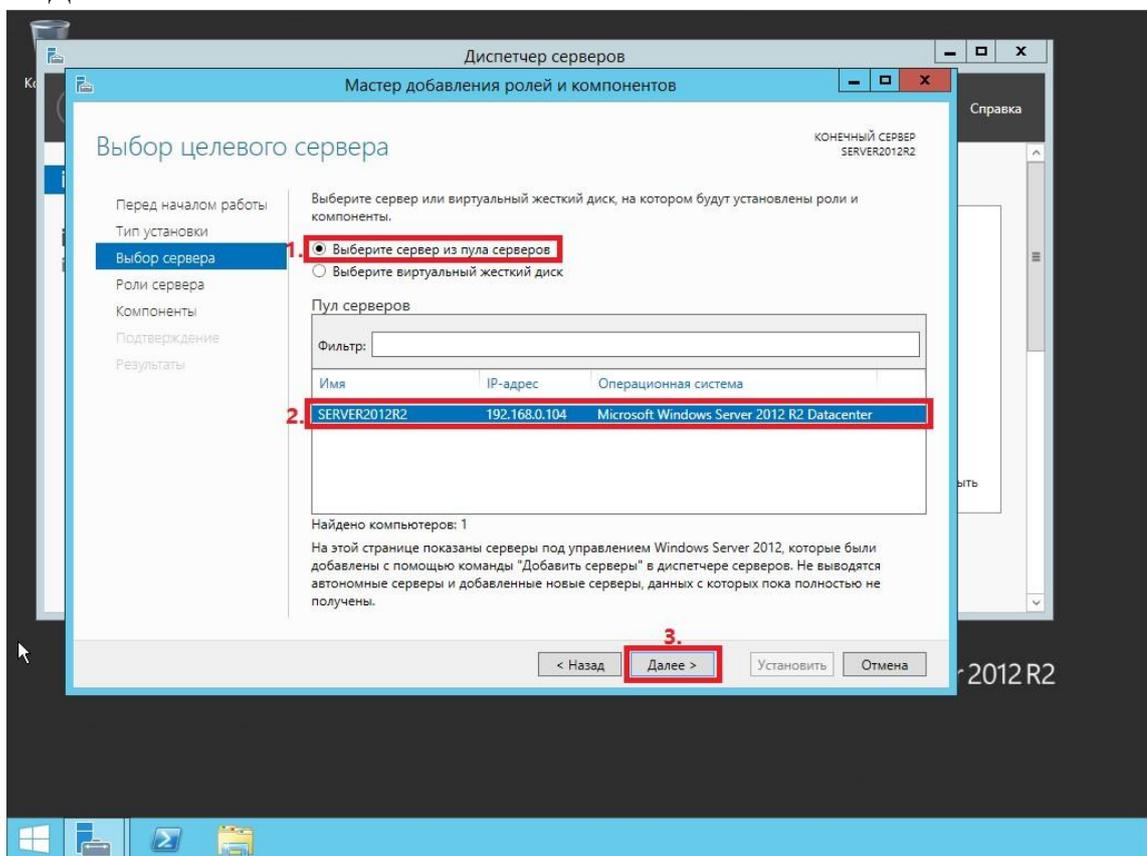


Рис. 12

2.5 Выберите роль **Доменные службы Active Directory**, на следующем этапе Мастер установки ролей предупредит, что для установки роли Доменные службы Active Directory нужно установить несколько компонентов. Нажмите **Добавить компоненты**

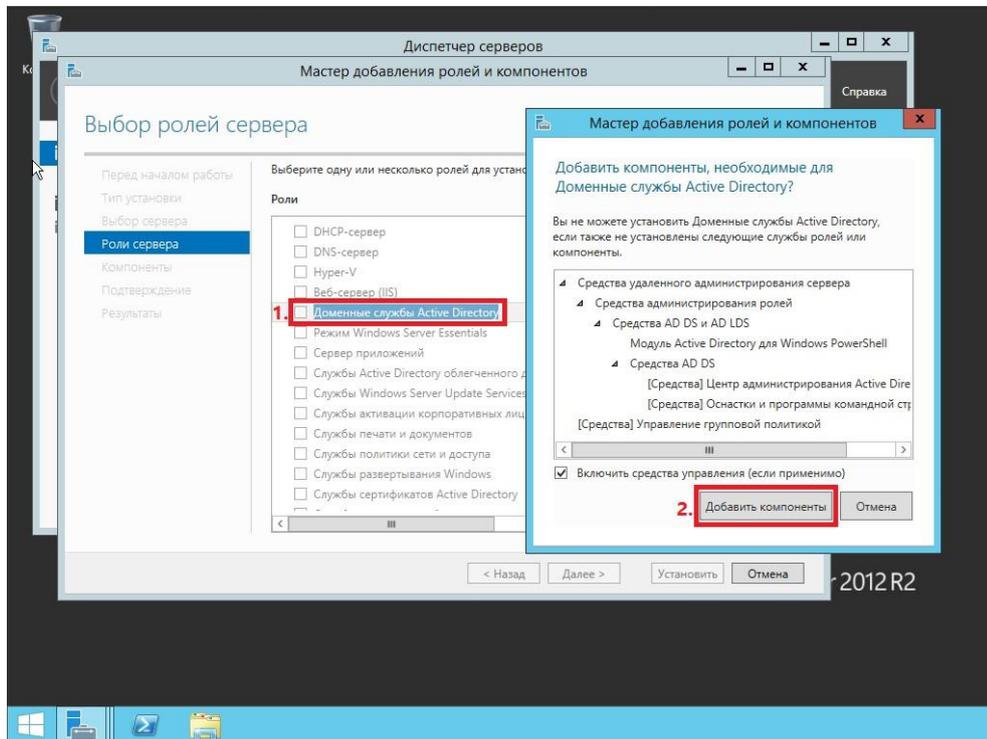


Рис. 13

2.6 Убедитесь, что после установки необходимых компонентов напротив **Доменные службы Active Directory** стоит галочка, затем нажмите **Далее**

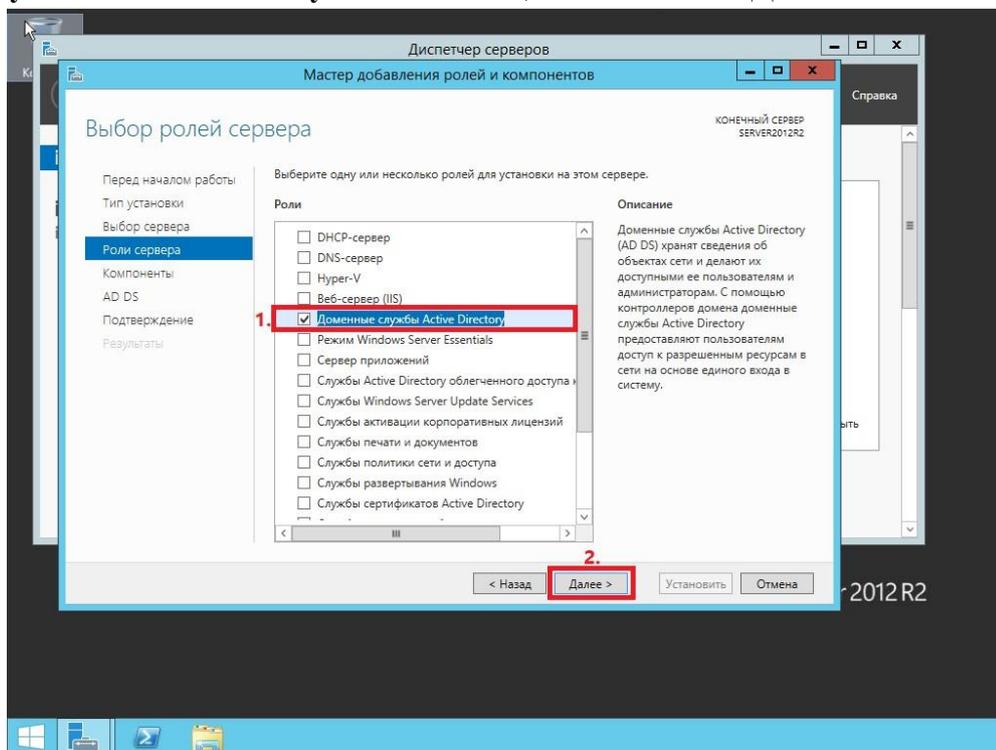


Рис. 14

2.7 На этапе добавления компонентов оставьте все значения по умолчанию и нажмите **Далее**

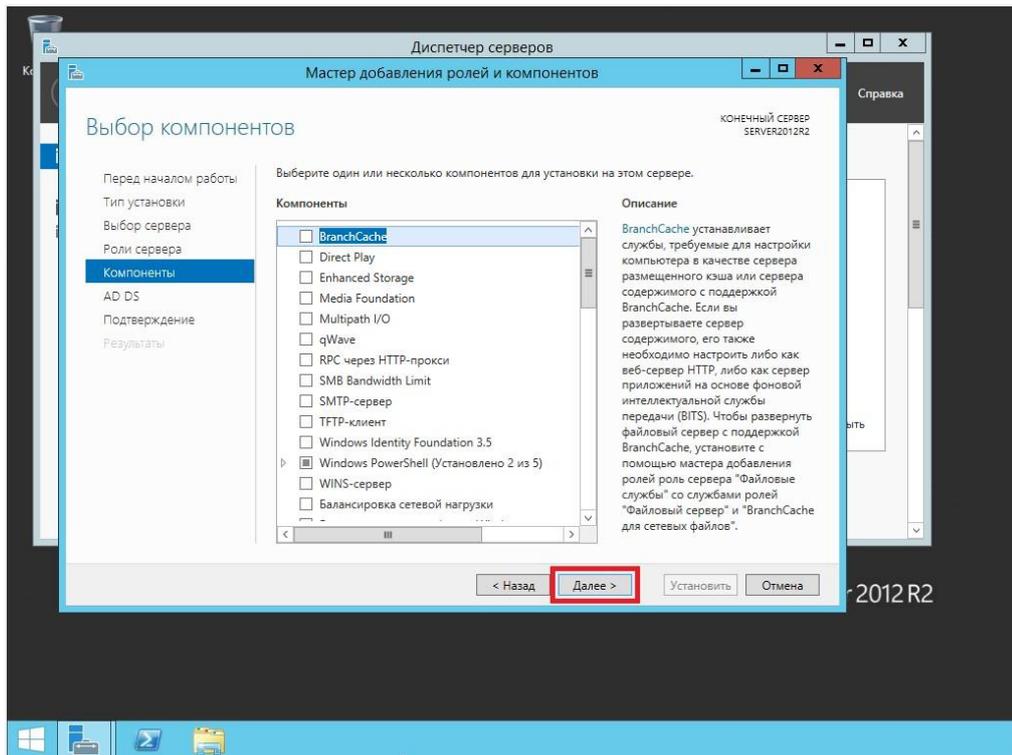


Рис. 15

2.8 Ознакомьтесь с дополнительной информацией касательно Доменных служб Active Directory, затем нажмите **Далее**

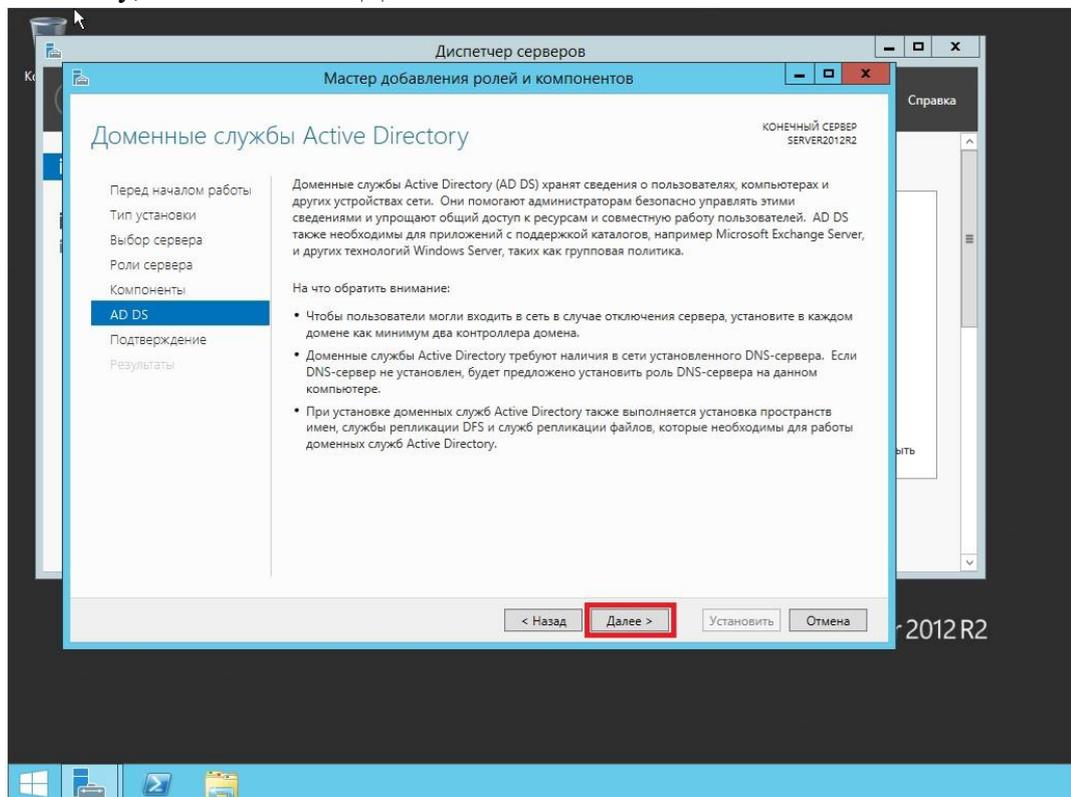


Рис. 16

2.9 Для начала установки роли нажмите **Установить**

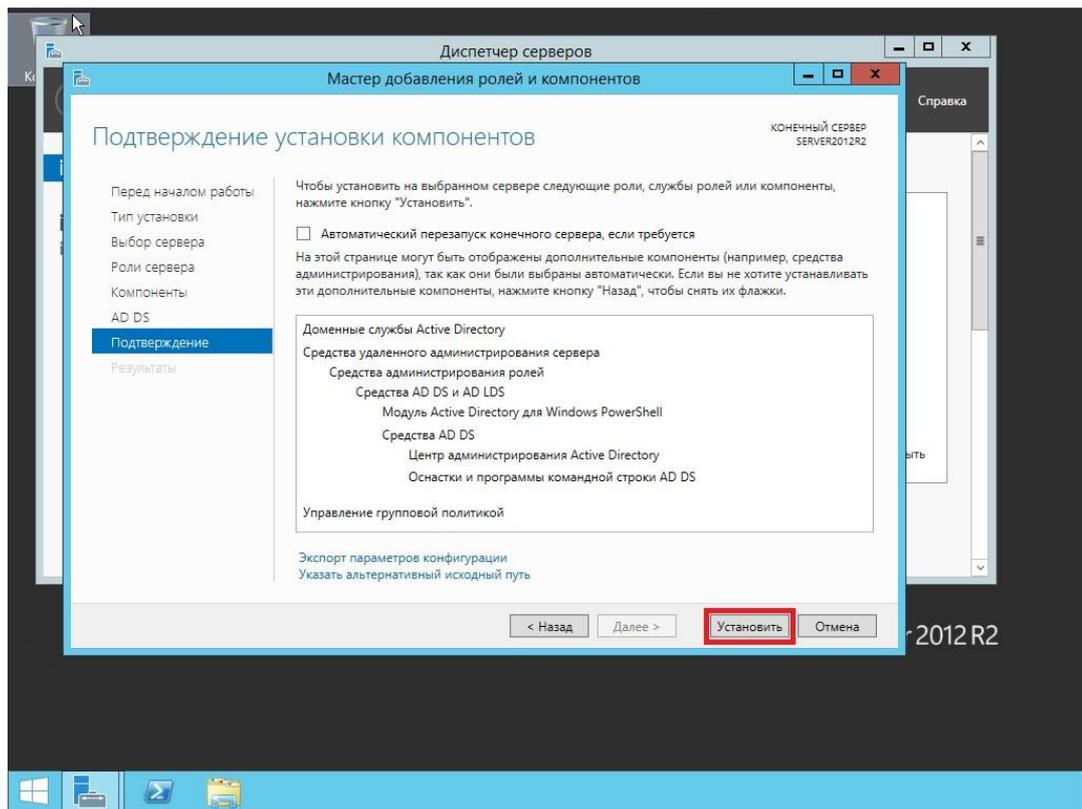


Рис. 17

2.10 После окончания установки нажмите **Повысить** роль этого сервера до уровня **контроллера домена**

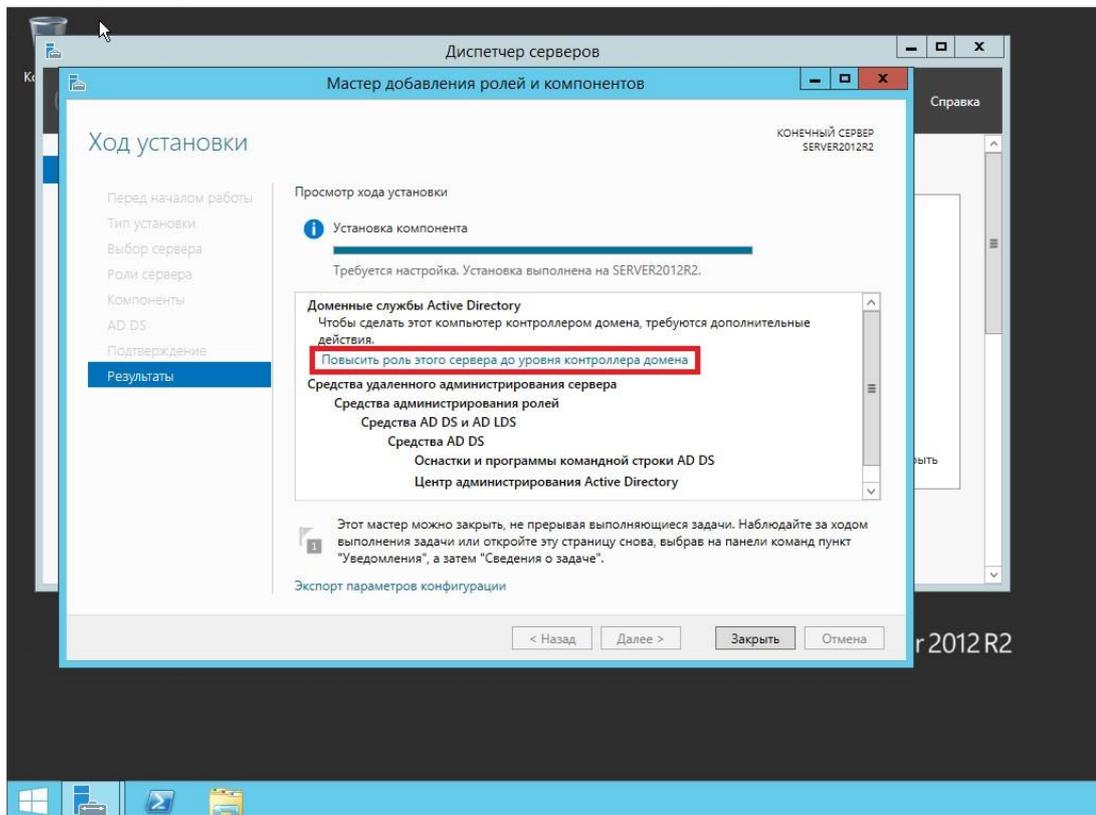


Рис. 18

2.11 Выберите пункт **Добавить новый лес**, затем в поле **Имя корневого домена** введите имя домена (*прим. в данном руководстве это example.local, Вы можете выбрать любое другое*), затем нажмите **Далее**

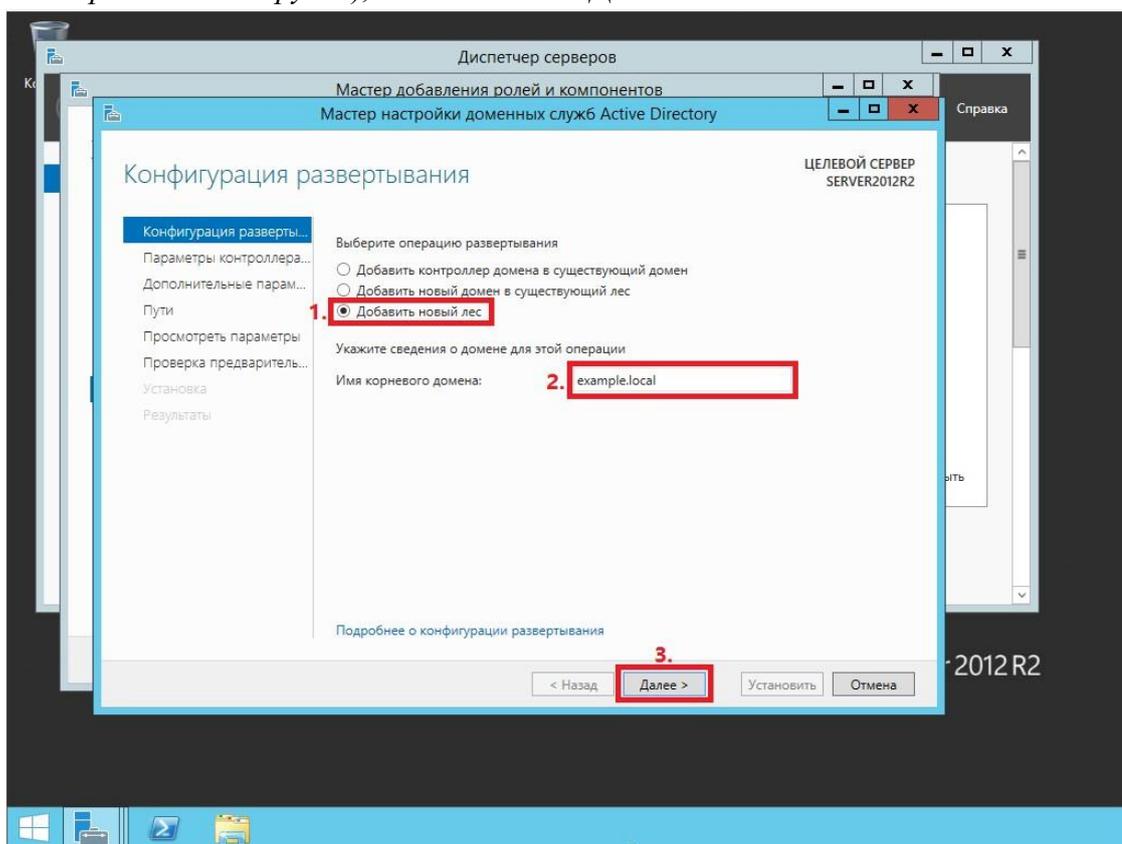


Рис. 19

2.12 На следующем шаге предлагается выбрать функциональный уровень нового леса и корневого домена. Если вы добавляете новый лес и планируете в дальнейшем использовать серверы на базе операционной системы Windows Server 2012 R2, то можете не менять функциональный уровень леса и корневого домена. Установите галочку напротив **DNS-сервер**, придумайте и введите пароль для режима восстановления служб каталогов в соответствующие поля, затем нажмите **Далее**

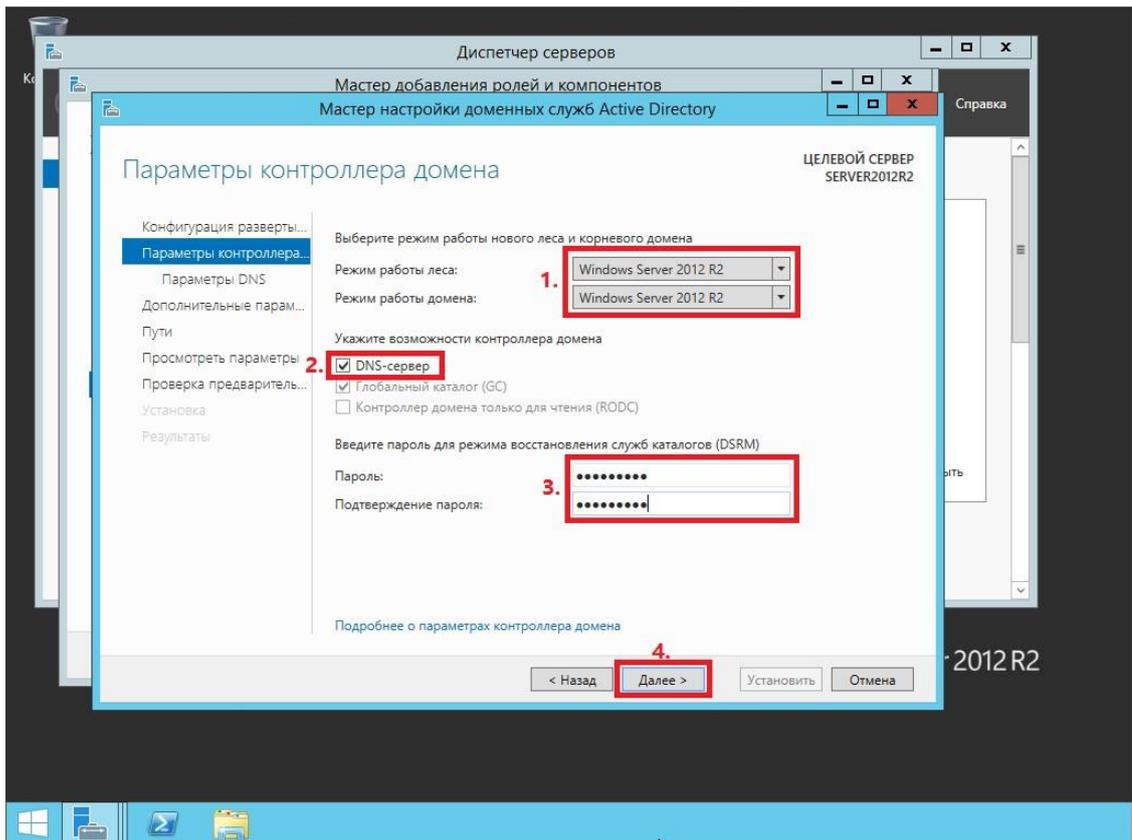


Рис. 20

2.13 Оставьте значение NetBIOS по умолчанию и нажмите **Далее**

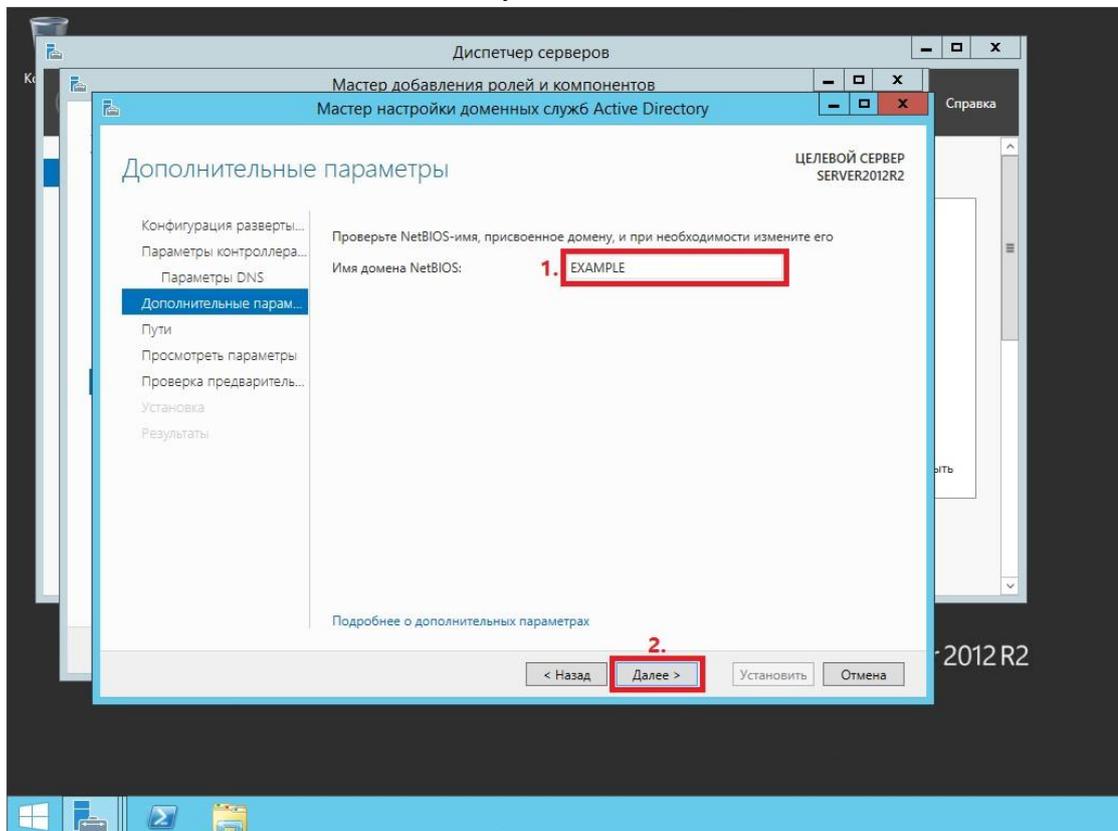


Рис. 21

2.14 Оставьте настройки по умолчанию и нажмите **Далее**

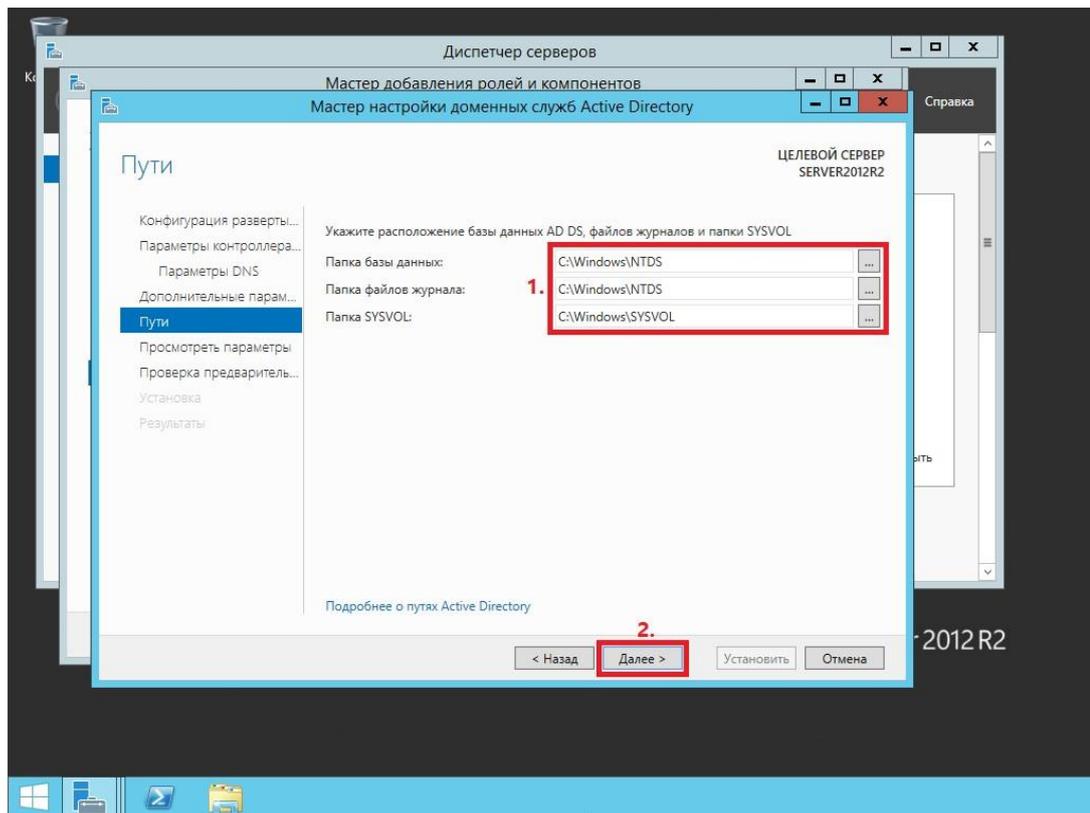


Рис. 22

2.15 В окне со сводной информацией по настройке сервера нажмите **Далее**

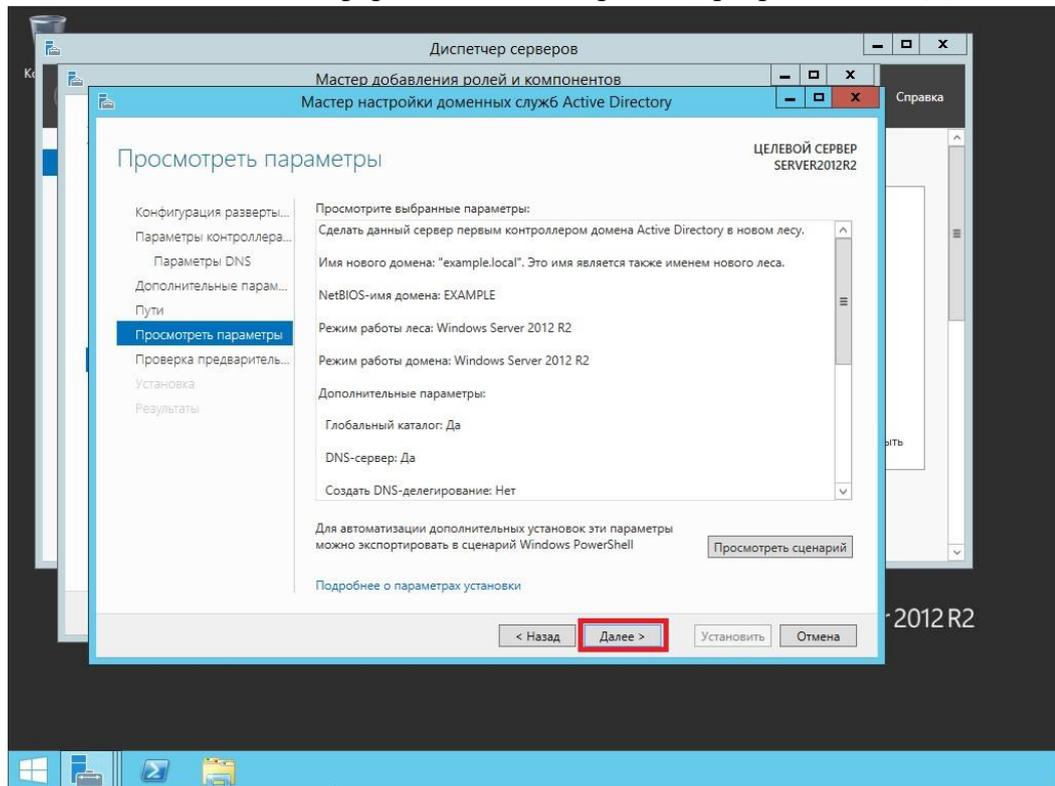


Рис. 23

2.16 Далее Мастер настройки доменных служб Active Directory проверит все ли предварительные требования соблюдены и выведет отчет. Нажмите **Установить** (Рис.24).

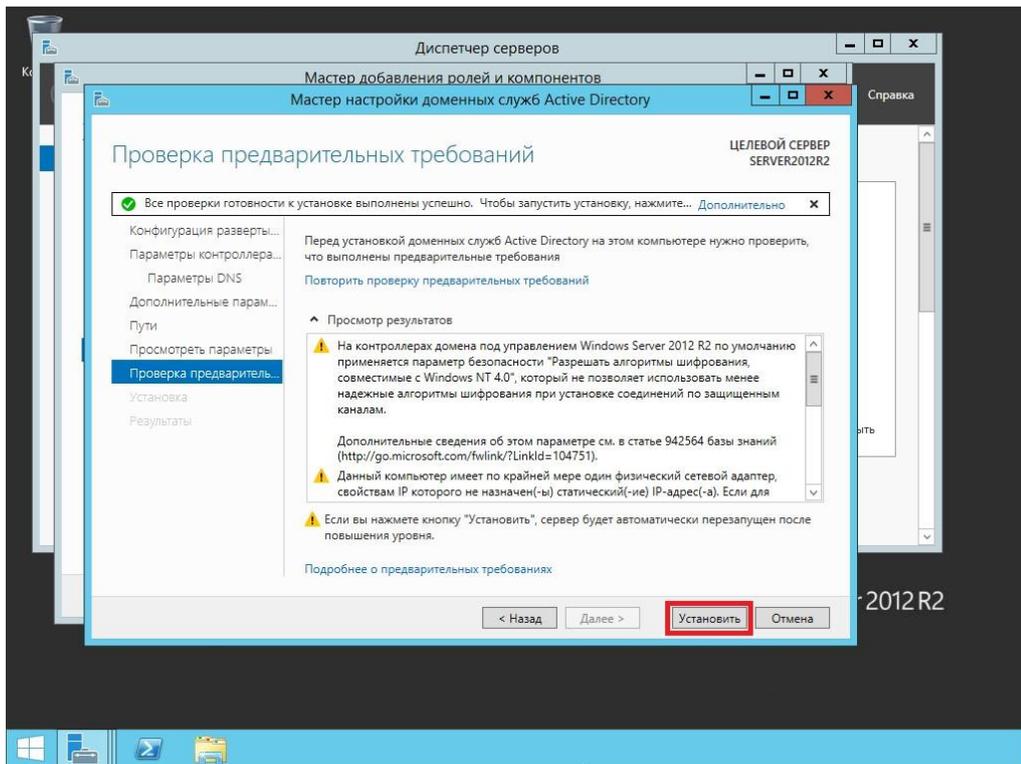


Рис. 24

2.17 После того как роль вашего сервера будет повышена до уровня контроллера домена, сервер автоматически перезагрузится. Перед тем как сервер начнет перезагружаться вы увидите предупреждение

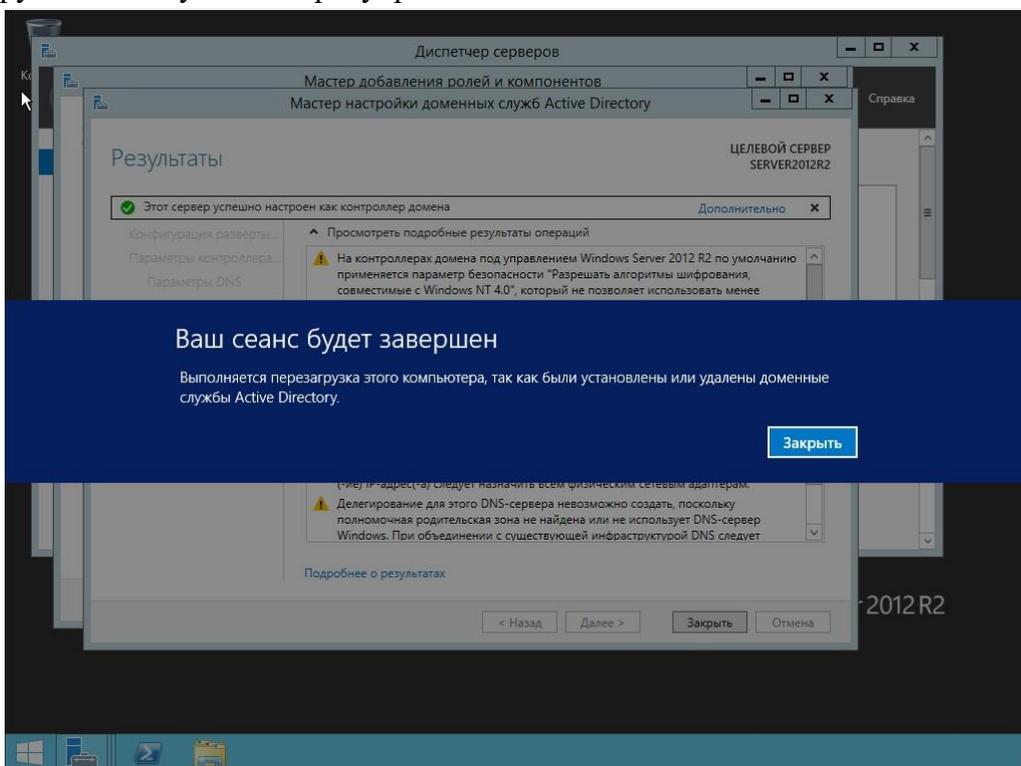


Рис. 25

2.18 После повышения роли сервера до уровня контроллера домена и перезагрузки — зайдите в систему под учетной записью с правами администратора домена

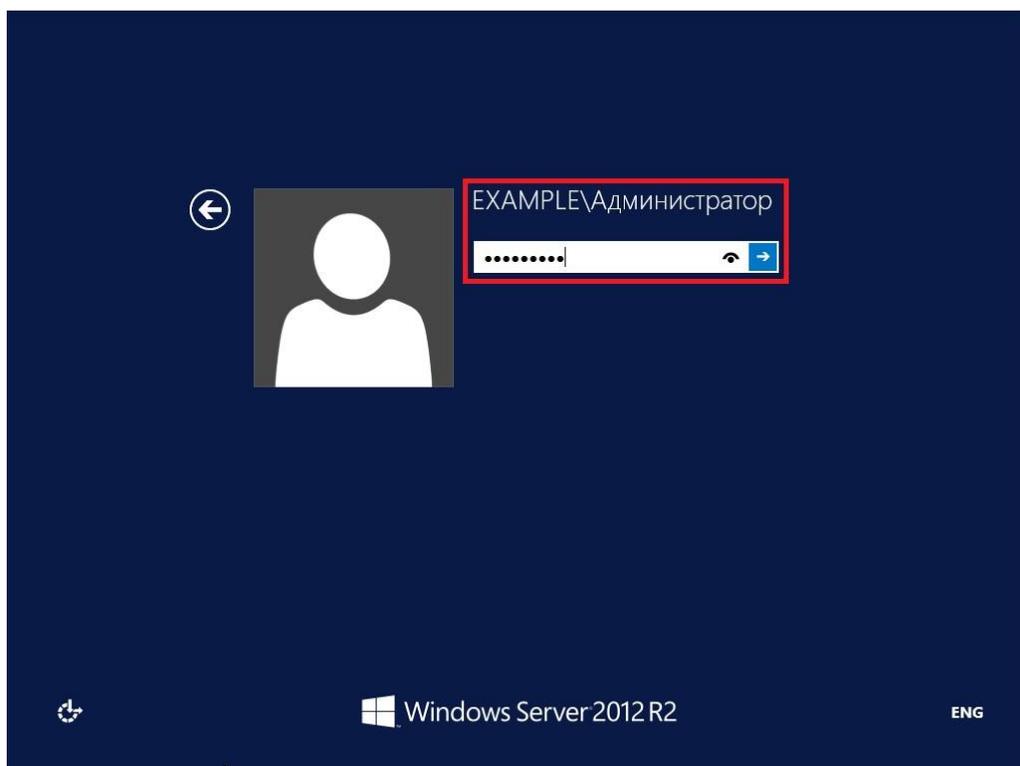


Рис. 26

Установка контроллера домена Active Directory в Windows Server 2012 R2 завершена!

Сделайте скриншоты (фотографии) процесса установки контроллера домена Active Directory и вставьте в отчёт.

Настройка политики паролей учетных записей в Active Directory

3.1 Что бы изменить политику паролей для пользователей, находящихся в домене, заходим в «Диспетчер серверов» далее в верхнем меню жмем "Средства" и переходим в раздел "Управления групповой политикой"

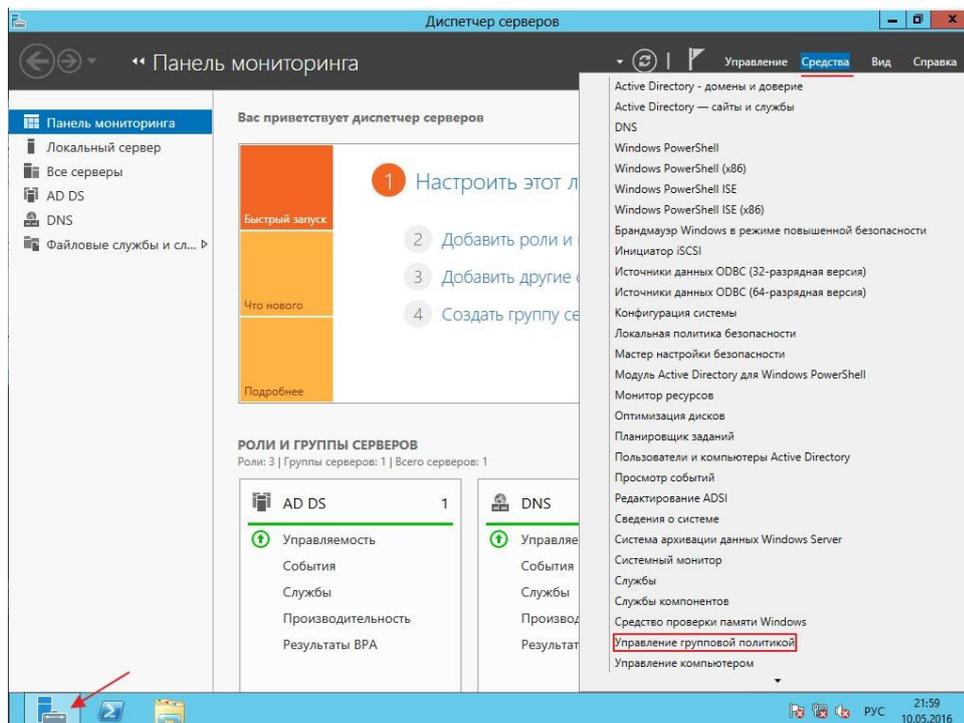


Рис. 27

3.2 Для того что бы изменить политику паролей необходимо изменить политику по умолчанию домена (Default Domain Policy) для этого нажмите ПКМ по данной политике и нажмите на пункт **"Изменить"**

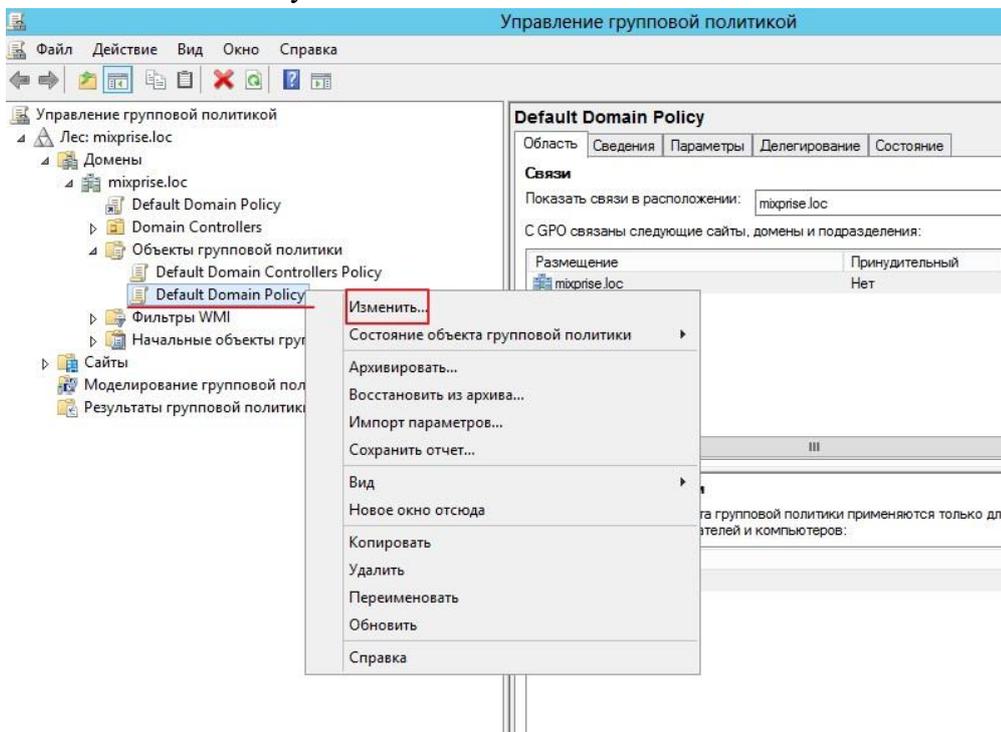


Рис. 28

3.3 В открывшемся окне открылся редактор, теперь необходимо найти где же изменять саму политику паролей, редактирование происходит в разделе **"Конфигурации компьютера"** далее разворачиваем папку **"Конфигурация Windows"** дальше открываем **"Параметры безопасности и политики учетных записей"**

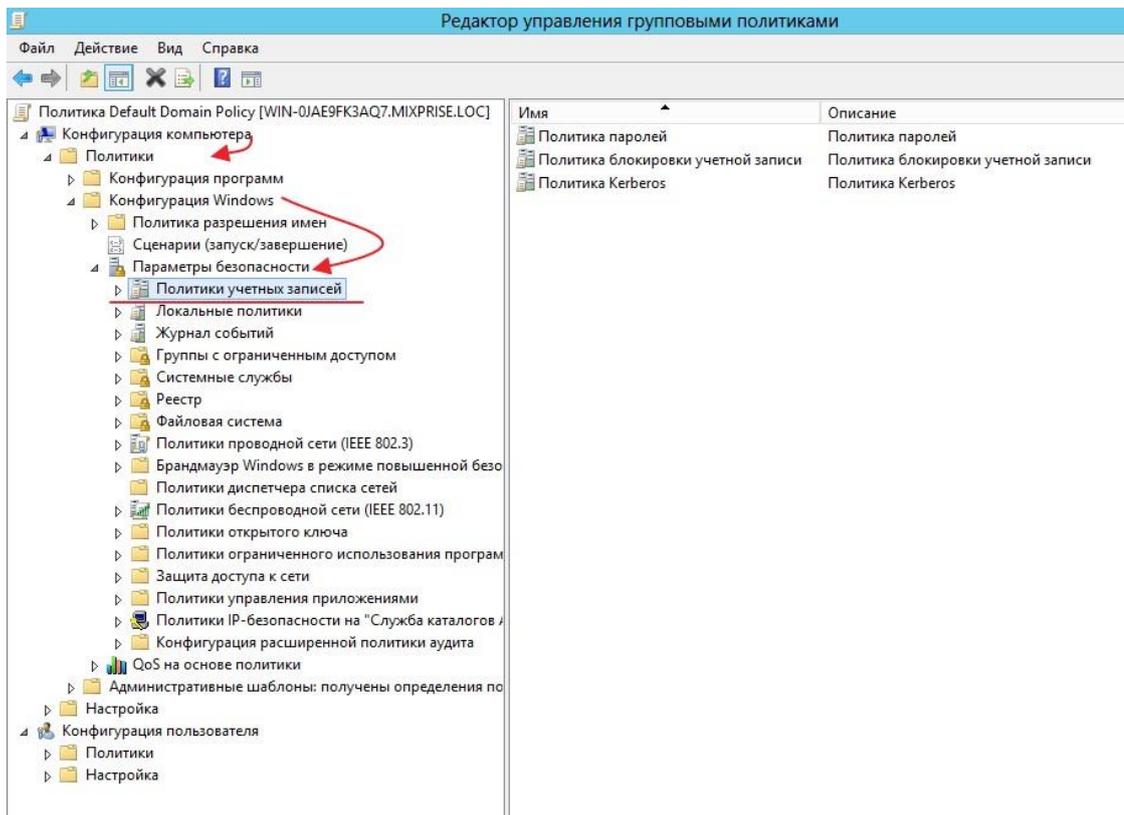


Рис. 29

Начнем настройку с первого раздела под названием "Политика паролей" открываем его

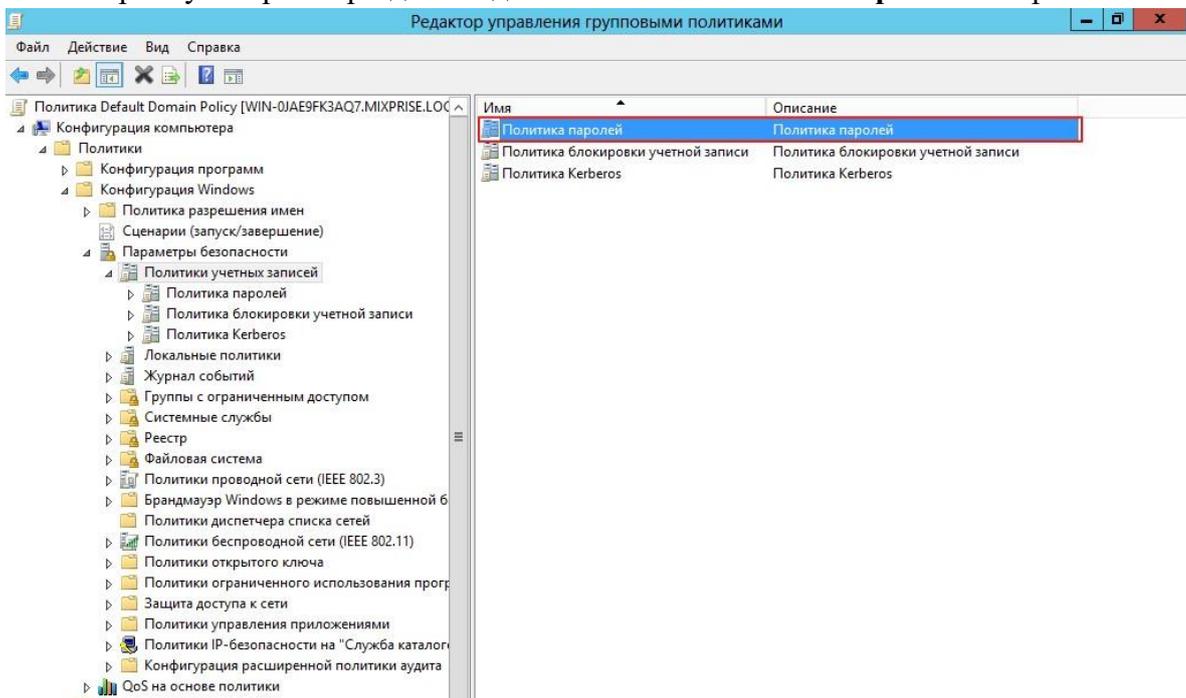


Рис. 30

В открывшемся окошке нам доступно для изменения 6 пунктов, каждый из них мы можем изменить, достаточно просто кликнуть на него.

3.4 Открываем вкладку "Вести журнал паролей" с помощью нее определяются числовое значение новых паролей, которые применяются к пользователю прежде чем он

сможет снова использовать предыдущий пароль, здесь я оставляем все по умолчанию.

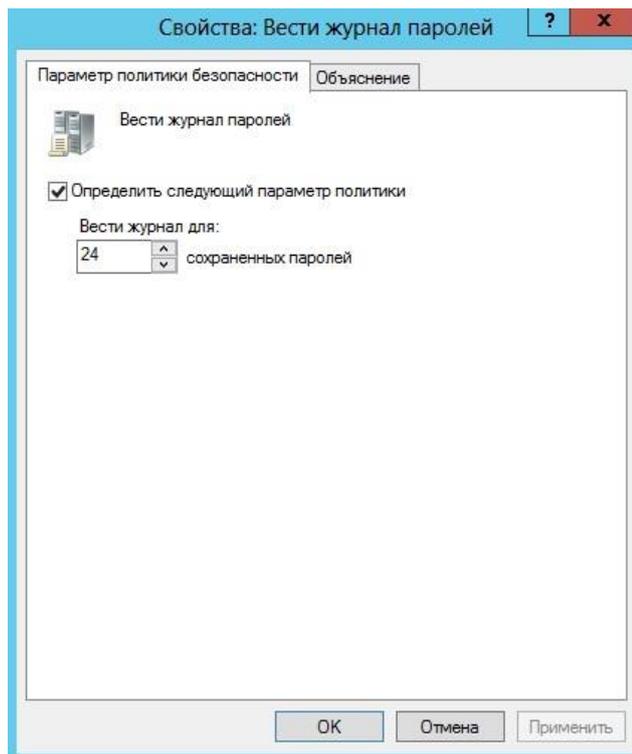


Рис. 31

3.5 Следующая вкладка "**Максимальный срок действия пароля**" по умолчанию это 42 дня, с помощью этой политики определяется временной интервал, в котором используется пароль прежде чем система вновь потребует от пользователя этот пароль поменять, убираем чекбокс и жмем "**Применить**"

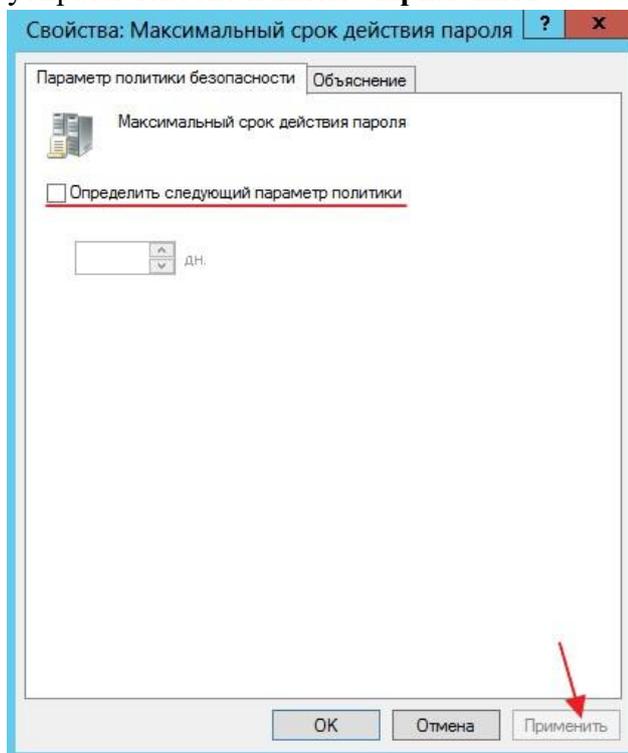


Рис. 32

Переходим на раздел "**Минимальная длина пароля**". По умолчанию это 7-8 символов, выставляем как минимум 4 символа

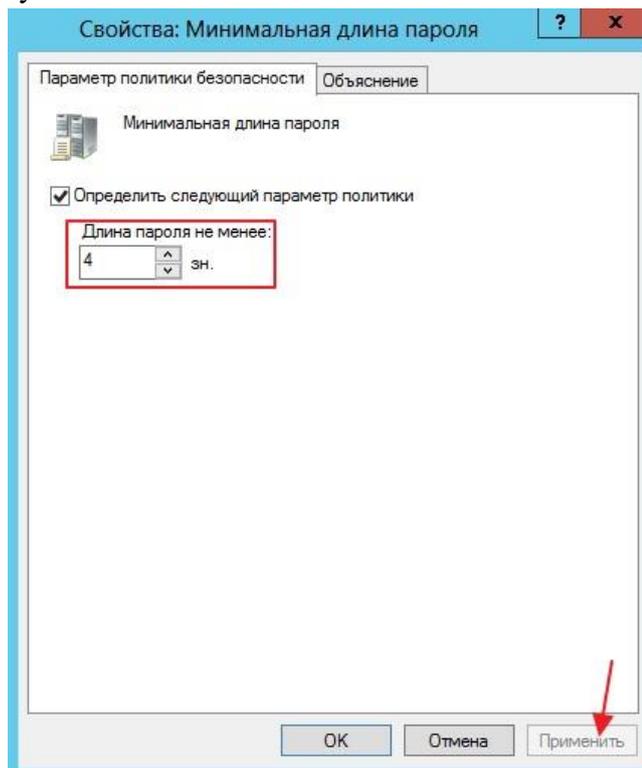


Рис. 33

3.6 Далее "**Минимальный срок действия пароля**" с помощью него определяется время, за которое пользователь не может изменить пароль по умолчанию значение ноль дней. Убираем галочку и применяем настройки

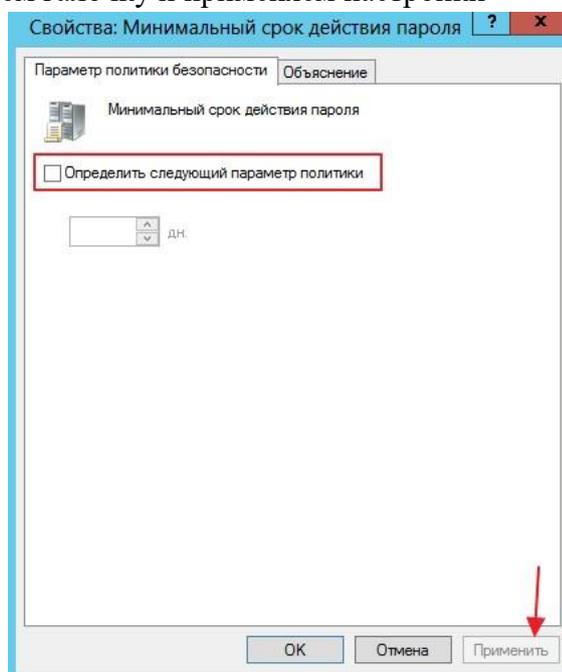


Рис. 34

3.7 Переходим к "**Пароль должен отвечать требованиям сложности**" это те требования, когда в пароле обязательно должны присутствовать английские буквы,

верхнего и нижнего регистра, цифры, не алфавитные символы и т.д. Ставим "Отключен" и кликаем "Применить".

ВАЖНО! При настройке «живого» сервера эти параметры должны быть включены!

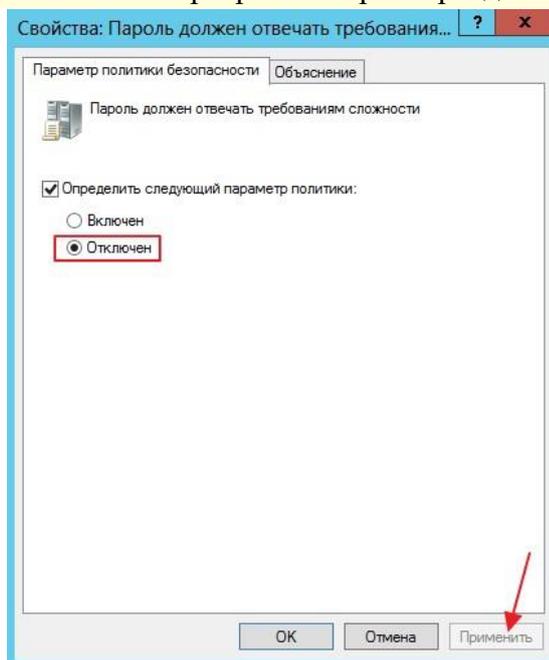


Рис. 35

3.8 Последняя политика "Хранить пароли", скажем лишь то, что если в ее включить пароли ваших пользователей в системе будут храниться в открытом виде и если злоумышленник доберется до вашей сети, то он легко сможет получить доступ к файлам!

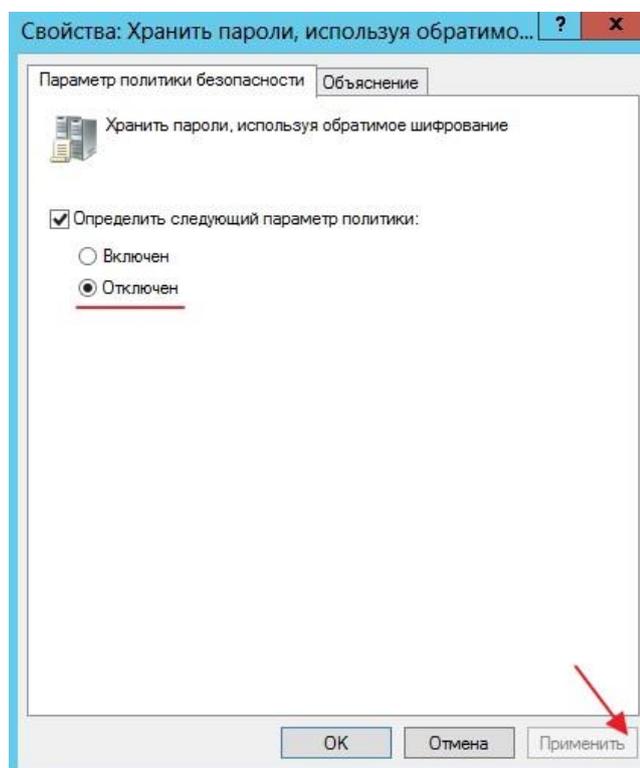


Рис. 36

3.9 Рассмотрим "Политику блокировки учетной записи". В данной политике доступны 3 блока это: "Время до сброса счетчика блокировки" выставляете время блокировки аккаунта, в качестве примера поставим значение равное 30 мин

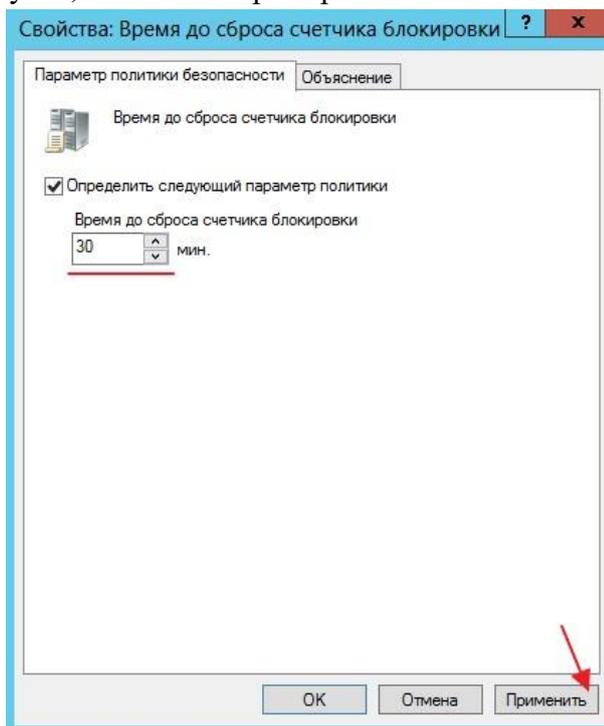


Рис. 37

"Пороговое значение блокировки» прежде, чем аккаунт будет заблокирован, грубо говоря выставляете попытки ввода неверного пароля, после чего наступит блокировка аккаунта пользователя, выставим в качестве примера 3 раза

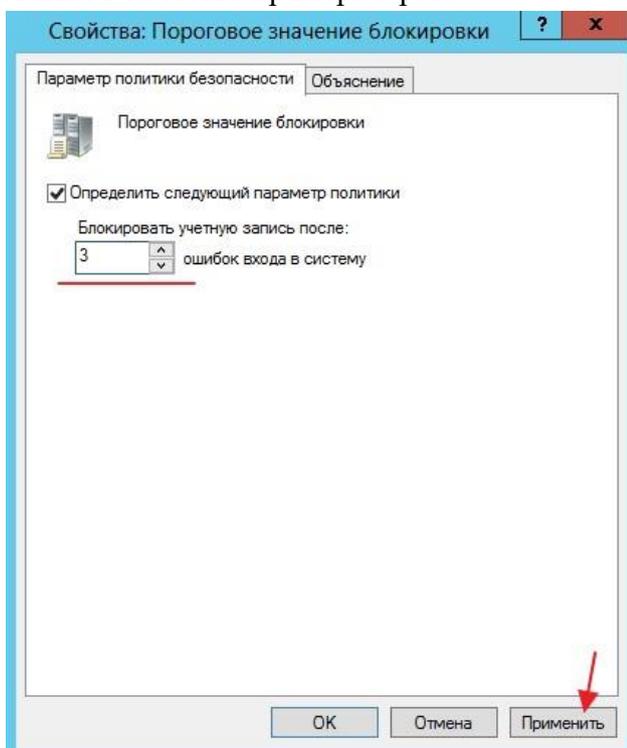


Рис. 38

"Продолжительность блокировки учетной записи" означает что если вы ввели скажем 4 раза неверный пароль, при такой настройке можете подождать 30 мин, и у вас снова будет доступно 3 попытки ввода пароля

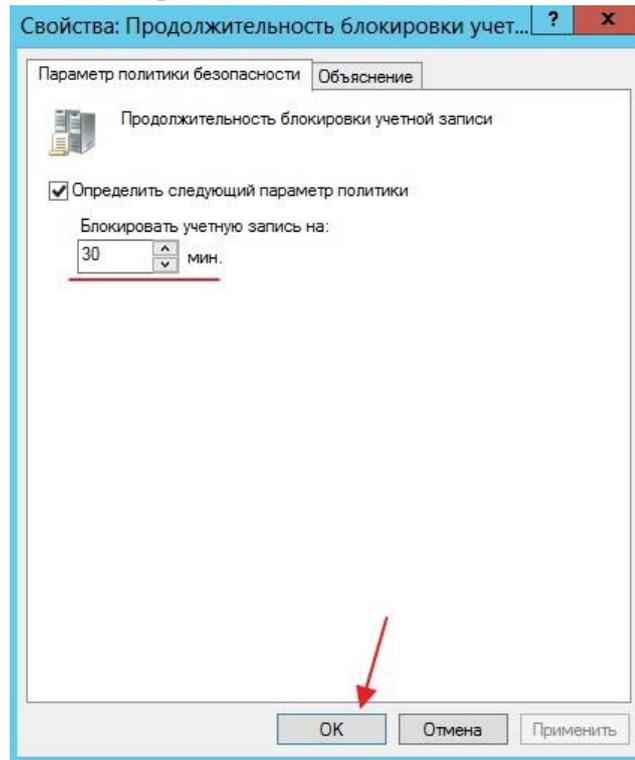


Рис. 39

3.10 Теперь что бы изменить пароль у пользователя заходим в **"Пользователи и компьютеры Active Directory"**

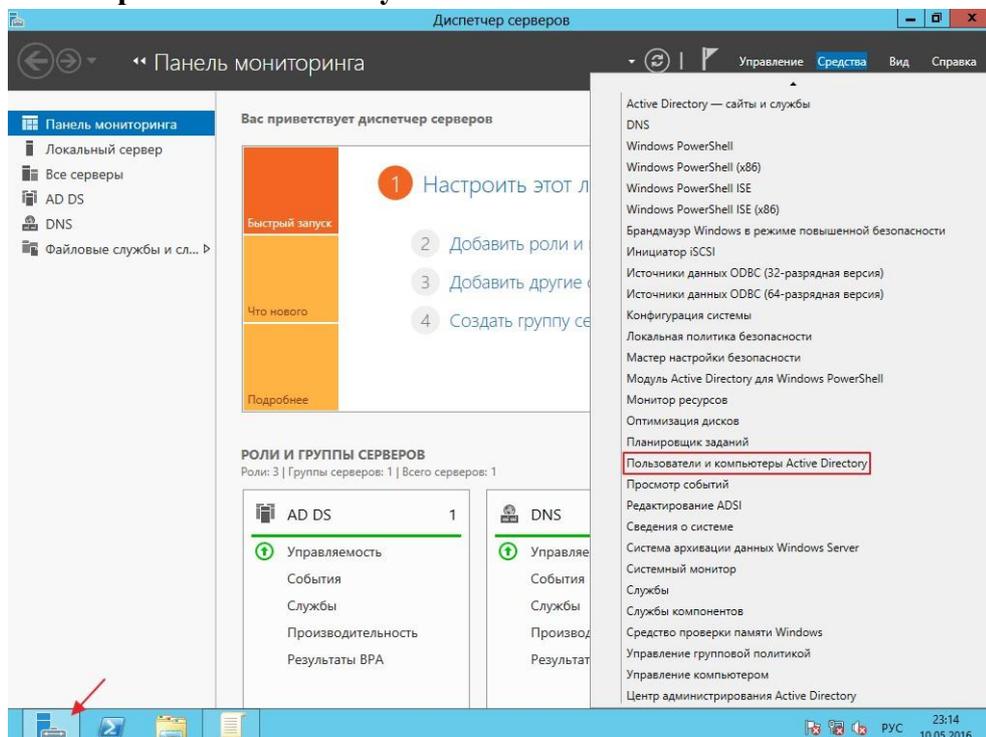


Рис. 40

Ищем учётную запись, для которой мы хотим изменить пароль, в нашем примере создайте учётную запись «Admin».

3.11 Теперь попробуем войти на сервер с новой учётной записью и новым паролем, для этого выполните "Выход из системы"

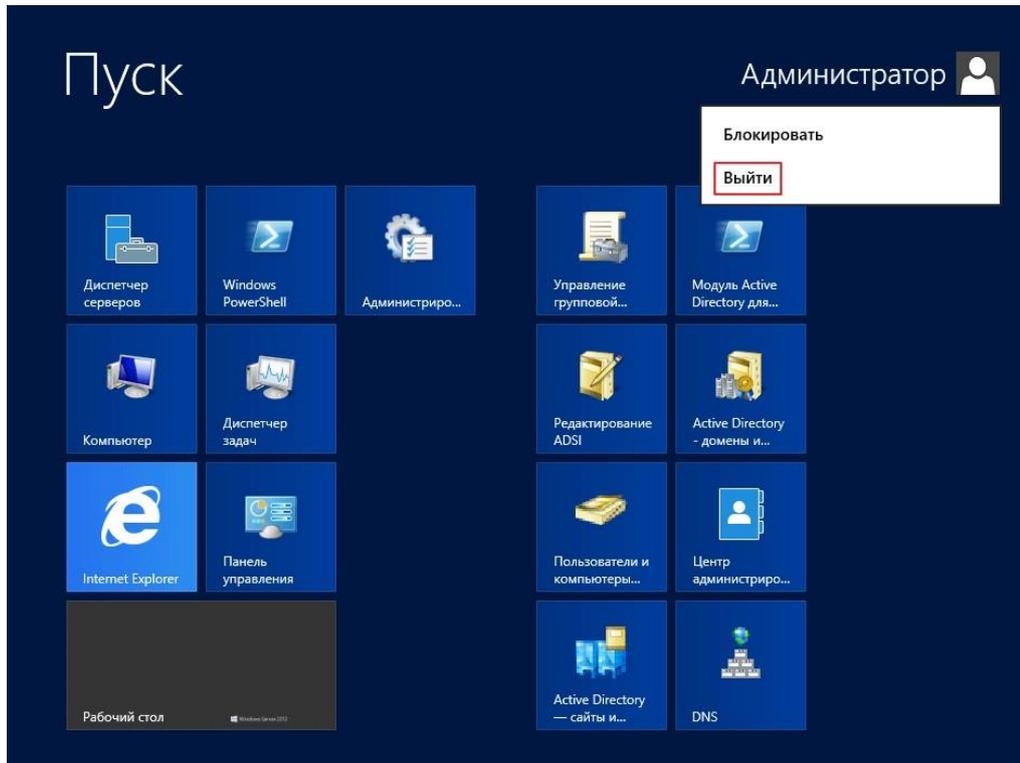


Рис. 41

Осуществляем вход с новой учётной записью

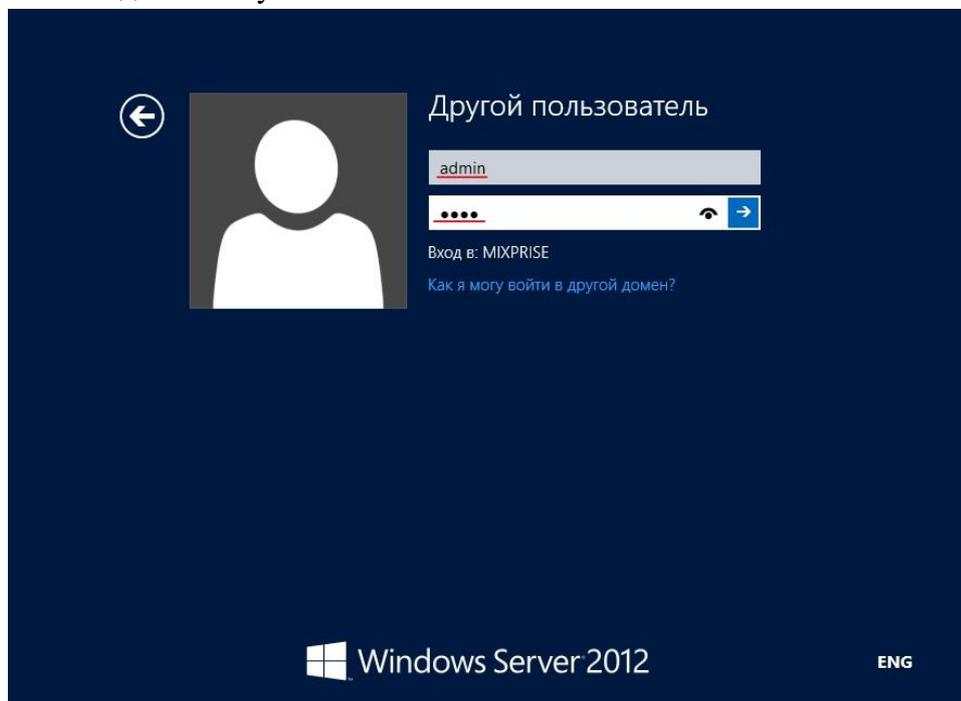


Рис. 42

Сделайте скриншоты (фотографии) процесса настройки контроллера домена Active Directory и вставьте в отчёт.

Создание пользователя в Powershell с параметрами New-ADUser

4.1 Итак, представим, что нам нужно срочно создать 50 однотипных учетных записей.

Пишем вот такой скрипт:

```
$org="OU=Students,DC=contoso,DC=com"  
$username="student" $count=1..50 foreach ($i in $count)  
{ New-ADUser -Name $username$i -Path $org -passThru }
```

Где:

- Name - логин
- GivenName - имя
- SurName - фамилия
- AccountPassword - пароль, который мы объявили в переменной
- Enabled - делает пользователя активным

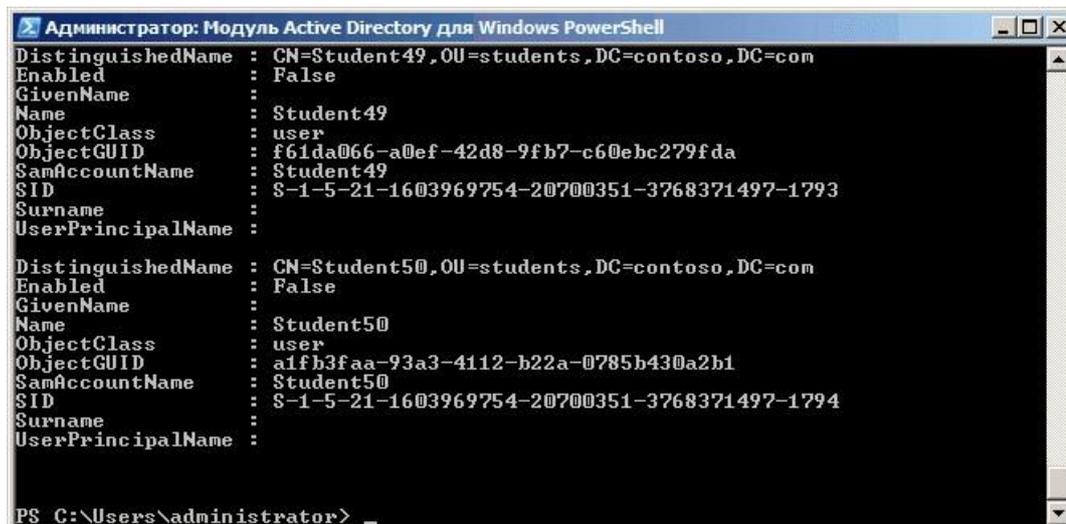


Рис. 43

Запускаем скрипт, и в подразделении Students создается 50 пользователей с именами student1-student50. По умолчанию учетки создаются отключенными, и пользователи все равно будут вынуждены к вам обращаться для их активации. Избежим этого:

```
$org="OU=Students,DC=contoso,DC=com"  
$username="student" $count=1..50 foreach ($i in $count)  
{ New-ADUser -Name $username$i -Path $org -Enabled $True -ChangePasswordAtLogon $True  
-AccountPassword (ConvertTo-SecureString «p@$$w0rd» -AsPlainText -force) -passThru }
```

Здесь создаем учетные записи уже активными и задаем `p@$$w0rd` как пароль по умолчанию, а также указываем сменить его при первом входе в систему. Чтобы не передавать пароль в открытом виде, используем командлет `ConvertTo-SecureString`, который переводит текстовую строку в защищенный формат.

4.2 Теперь сделаем наш скрипт чуть более гибким. Используя командлет *Read-Host* заставим наш скрипт запрашивать имя и количество пользователей:

```
$org="OU=Students,DC=contoso,DC=com"
$username=Read-Host "Enter name"
$number=Read-Host "Enter number"
$count=1..$number foreach ($i in $count)
{ New-AdUser -Name $username$i -Path $org -Enabled $True -ChangePasswordAtLogon $true
-AccountPassword (ConvertTo-SecureString "p@$w0rd" -AsPlainText -force) -passThru }
```

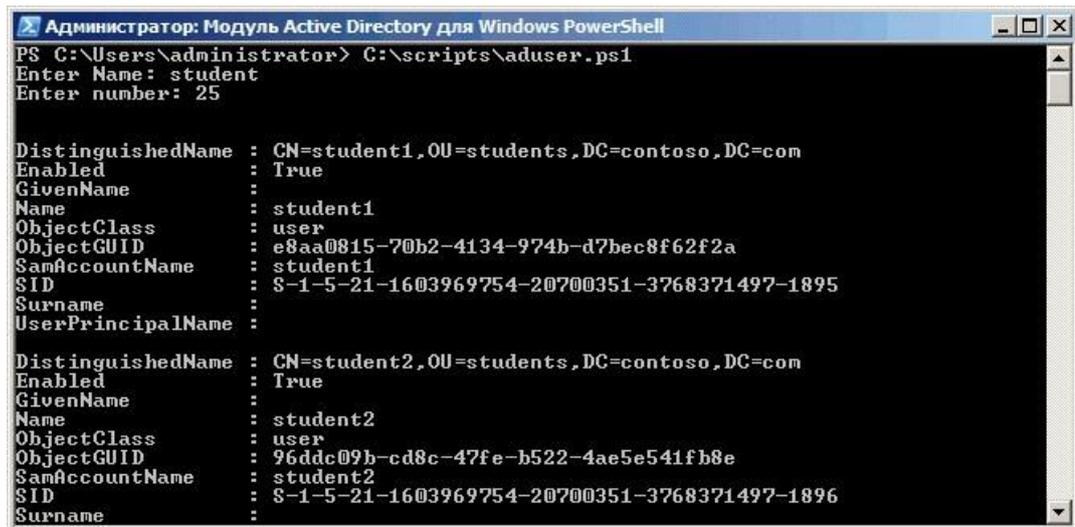


Рис. 44

Учетные записи созданы, пользователи могут заходить в систему и работать. Теперь их надо настроить — добавить в группы безопасности, прописать домашний каталог, сценарии входа и т.п. Сделать это можно с помощью шаблона. Проще говоря, создаем шаблонную учетную запись, полностью настраиваем ее, а затем делаем с нее нужное количество копий с помощью параметра *-Instance* :

```
$template = Get-AdUser -Identity "student" $org="OU=Students,DC=contoso,DC=com"
$username=Read-Host "Enter name"
$number=Read-Host "Enter number"
$count=1..$number foreach ($i in $count)
{ New-AdUser -Name $username$i -UserPrincipalName $username$i -Path $org -Instance `
$template -Enabled $True -ChangePasswordAtLogon $true `
-AccountPassword (ConvertTo-SecureString "p@$w0rd" -AsPlainText -force) -passThru }
```

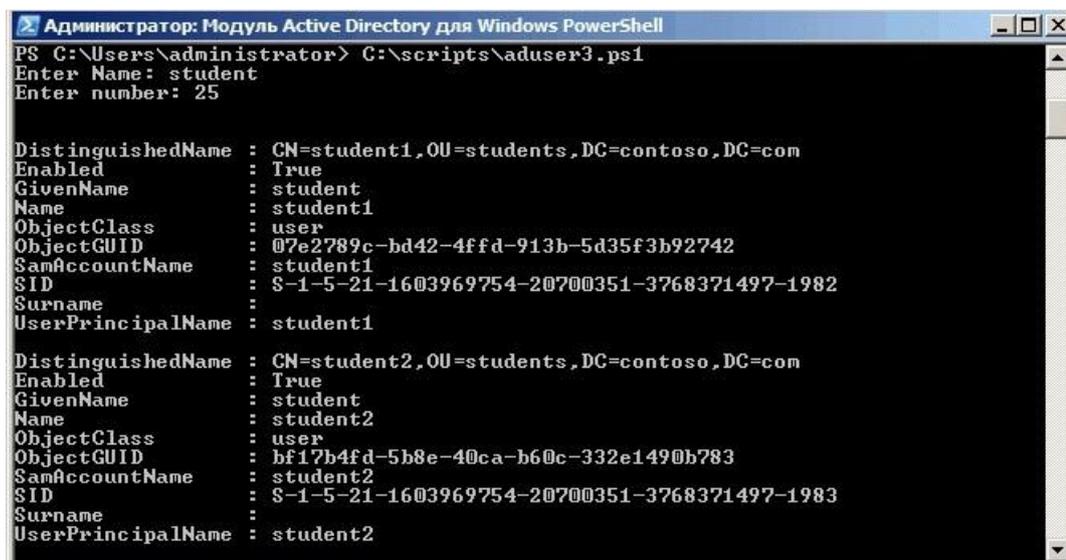


Рис. 45

4.3 Следующий способ автоматизировать создание учетных записей — импортировать их из CSV-файла. Этот способ подойдет в том случае, если вам предоставили список пользователей, и им надо завести учетные записи в соответствии с этим списком. Как правило, подобные списки создаются в Excel в виде таблицы со столбцами Имя, Должность, Отдел и т.п., примерно такого вида:

	A	B	C	D	E
1	Name	SamAccountName	DisplayName	Department	Title
2	GarsinT	GarsinT	Егор Тимофеевич Гаршин	sales	начальник отдела
3	DroninM	DroninM	Макар Трофимович Дронин	sales	менеджер по продажам
4	AlekseevA	AlekseevA	Антон Богданович Алексеев	sales	менеджер по продажам
5	NedozrelovP	NedozrelovP	Павел Григорьевич Недозрелов	sales	менеджер по продажам
6	DeryabinaP	DeryabinaP	Пелагея Степановна Дерябина	sales	менеджер по продажам
7	ShustrovaK	ShustrovaK	Клавдия Андреевна Шустрова	sales	менеджер по продажам
8	DevyatovG	DevyatovG	Георгий Валерьевич Деятов	accounting	главный бухгалтер
9	VarlovG	VarlovG	Георгий Николаевич Варлов	accounting	бухгалтер
10	SherbakovR	SherbakovR	Руслан Павлович Щербаков	accounting	бухгалтер
11	ZheleznyakovV	ZheleznyakovV	Владимир Викторович Железняков	accounting	бухгалтер
12	EmanovaP	EmanovaP	Прасковья Романовна Еманова	accounting	бухгалтер
13	AndrosovV	AndrosovV	Вадим Макарович Андросов	accounting	бухгалтер
14	BurobinM	BurobinM	Михаил Егорович Буробин	accounting	бухгалтер
15	ZlobinaS	ZlobinaS	Степанида Романовна Злобина	accounting	бухгалтер
16	OleynikovaS	OleynikovaS	Степанида Егоровна Олейникова	accounting	бухгалтер
17	MuravlevN	MuravlevN	Николай Фёдорович Муравлёв	accounting	бухгалтер
18	MolostnovaF	MolostnovaF	Фёкла Егоровна Молостнова	accounting	бухгалтер
19	LutovaV	LutovaV	Вероника Антоновна Лютова	accounting	бухгалтер
20	KadyshhevA	KadyshhevA	Афанасий Львович Кадышев	accounting	бухгалтер
21	SludachevF	SludachevF	Федот Львович Слюдачёв	accounting	бухгалтер

Рис. 46

Наша задача — сохранить его в формате CSV и затем указать в скрипте с помощью командлета *ImportCSV*. Если ваш CSV-файл содержит все необходимые столбцы, то *New-ADUser* автоматически свяжет их с правильными атрибутами пользователя :

```
$csv = Import-CSV -Path "C:\scripts\users.csv"
```

```
$csv | New-ADUser -Path $org -Enabled $True -ChangePasswordAtLogon $true `
-AccountPassword (ConvertTo-SecureString "p@$w0rd" -AsPlainText -force) -passThru
```

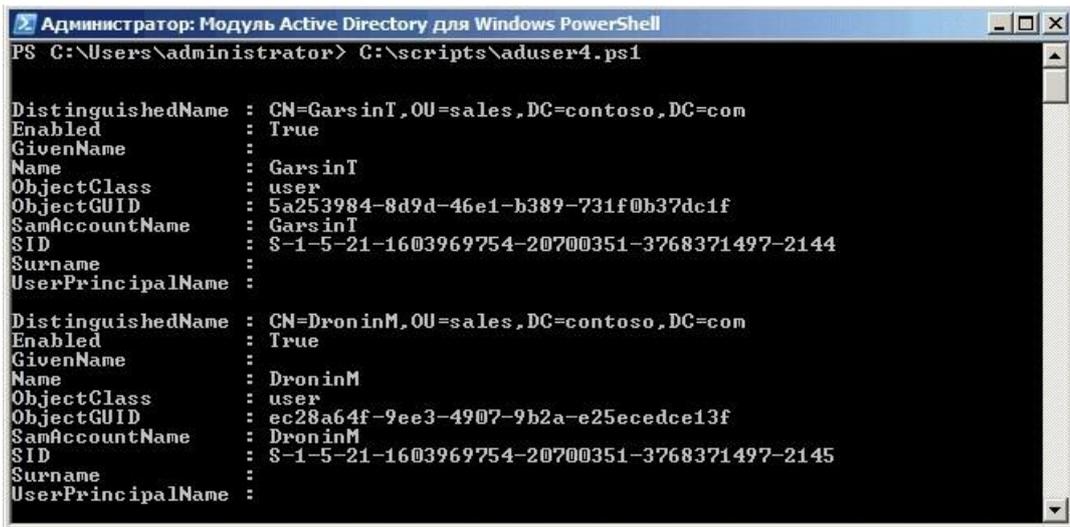


Рис. 47

Таким образом можно импортировать сотни новых пользователей за несколько секунд, но есть в этом методе и подводные камни:

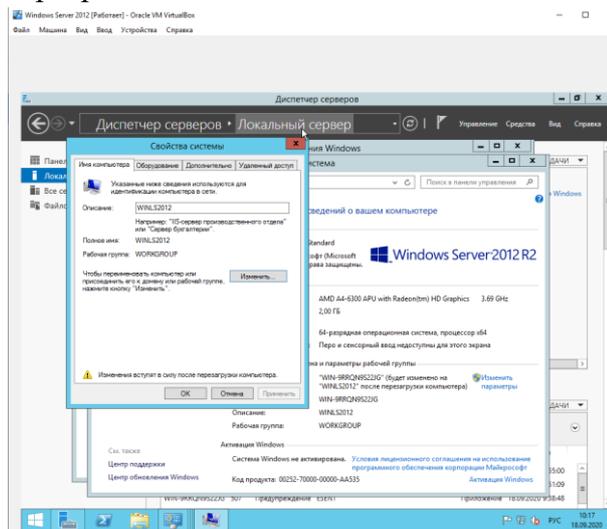
- Названия столбцов должны **полностью** совпадать с названиями атрибутов пользователя, например Name (Имя), Organization (Организация), Title (должность), иначе ничего не получится.

- В таблице **обязательно** нужно указать SamAccountName, в противном случае будет выдана ошибка о том, что учетная запись уже существует.

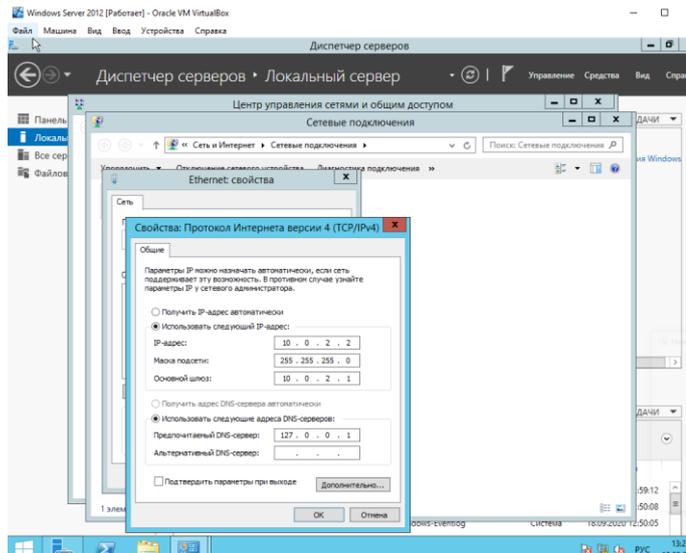
Если атрибуты задавать в русской раскладке, как в нашем примере, то могут возникнуть проблемы с кодировкой. В решении этой проблемы мне помогло извлечение содержимого CSV-файла с помощью командлета *Get-Content* и сохранение его в другой CSV-файл: *Get-Content users.csv >> users1.csv*. После этого все русскоязычные атрибуты стали отображаться нормально.

Эталоны ответов:

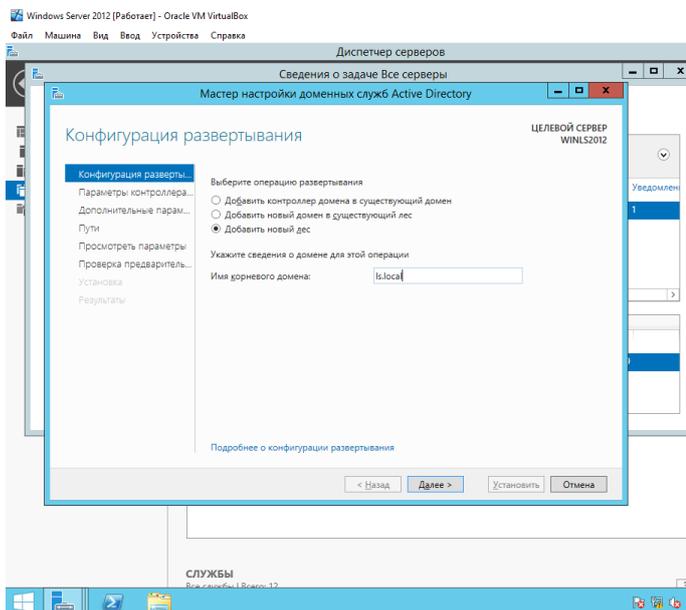
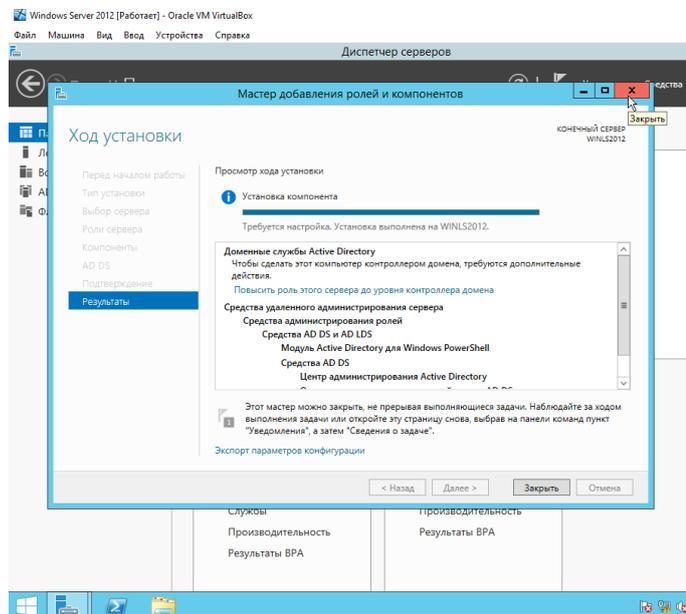
1. Смена названия сервера

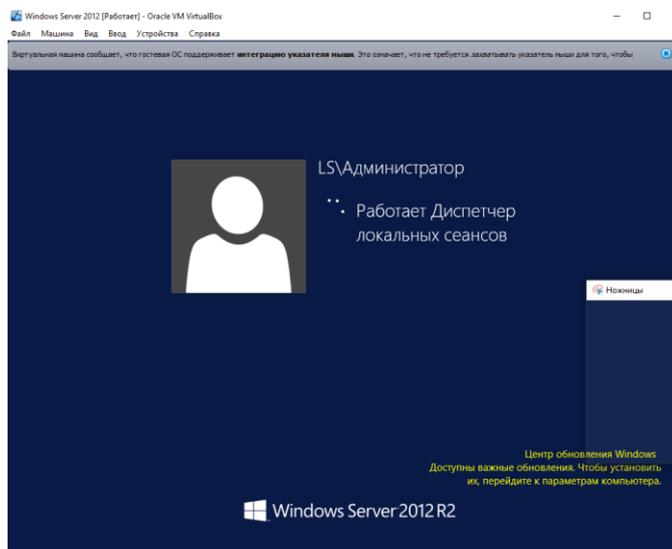
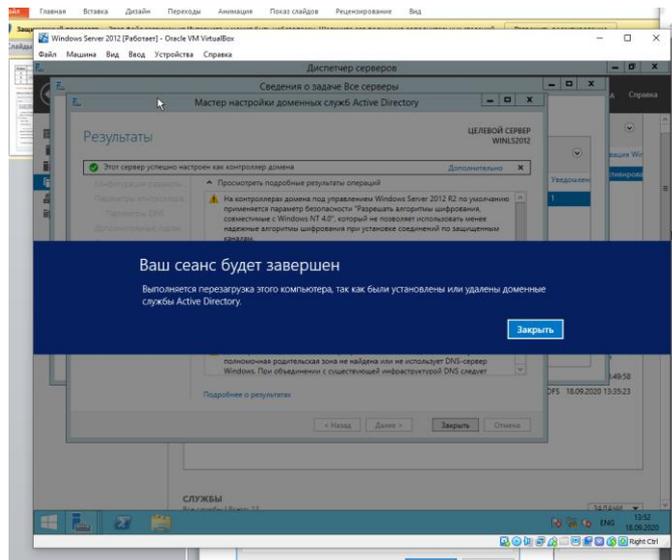


2. Выставление IP

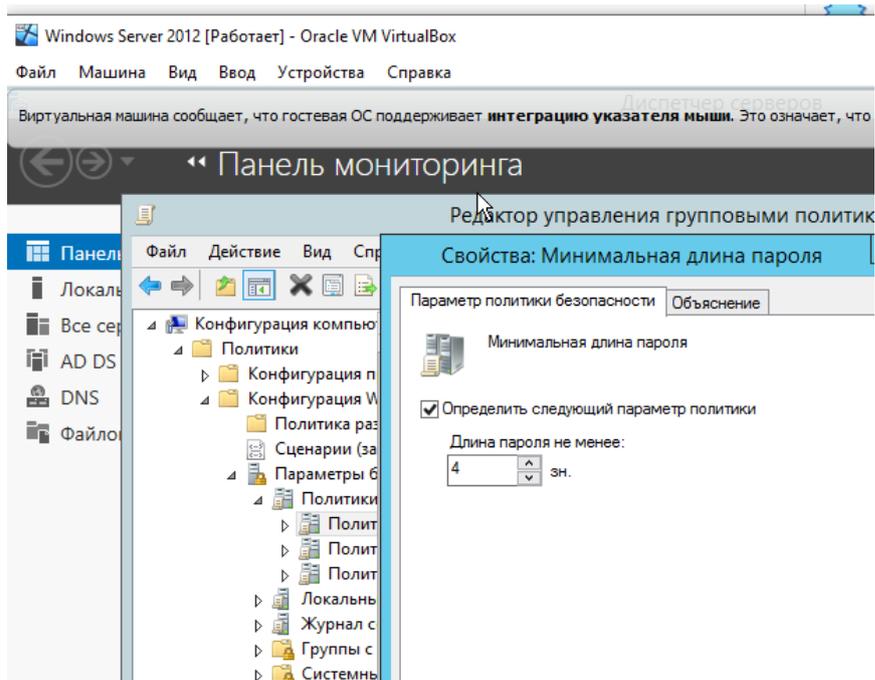
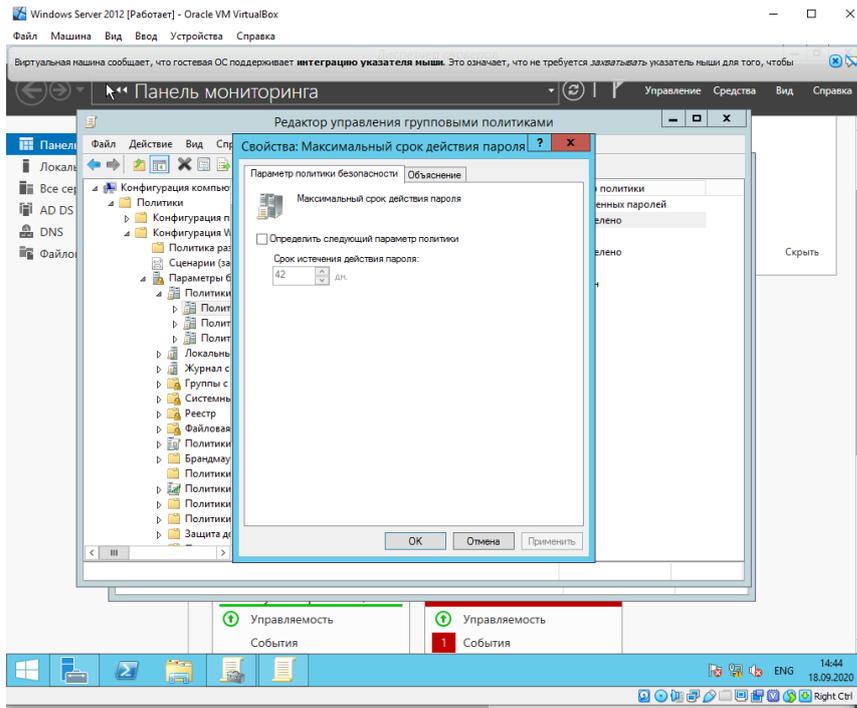


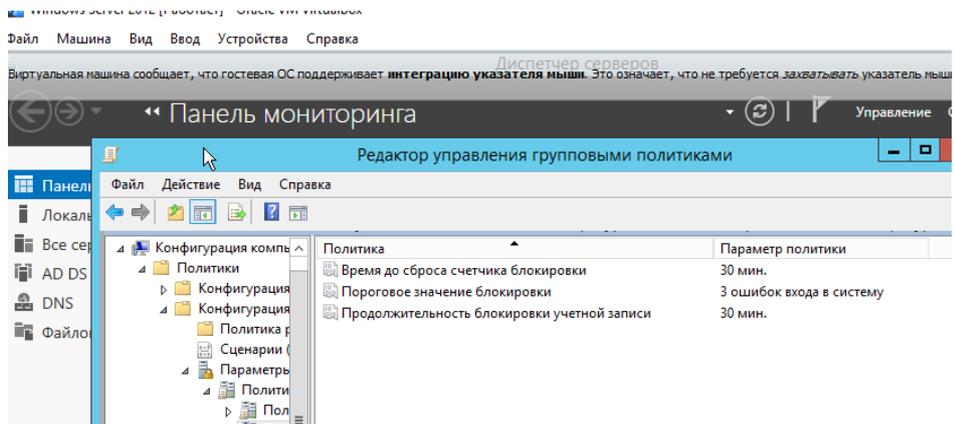
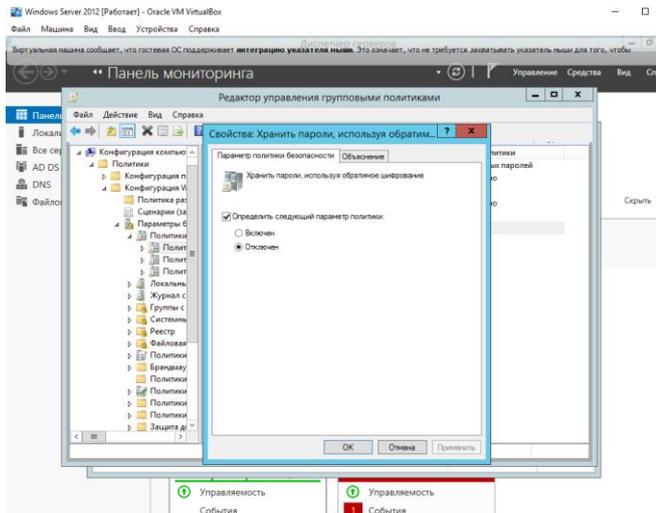
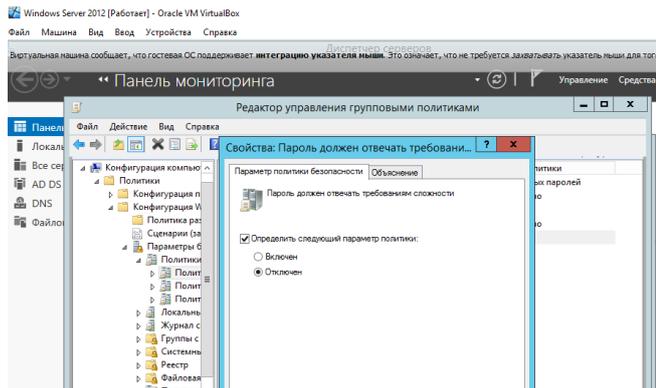
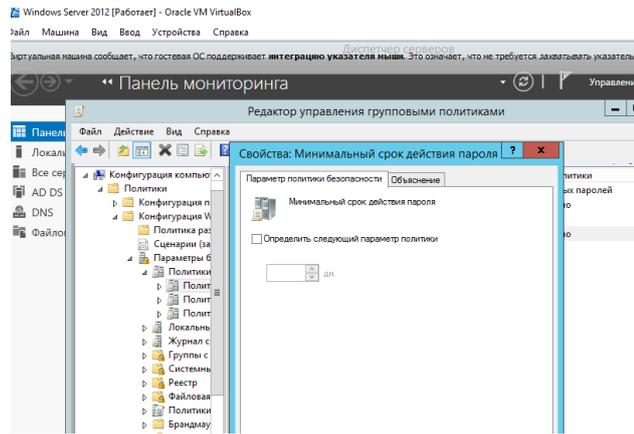
2.AD DS

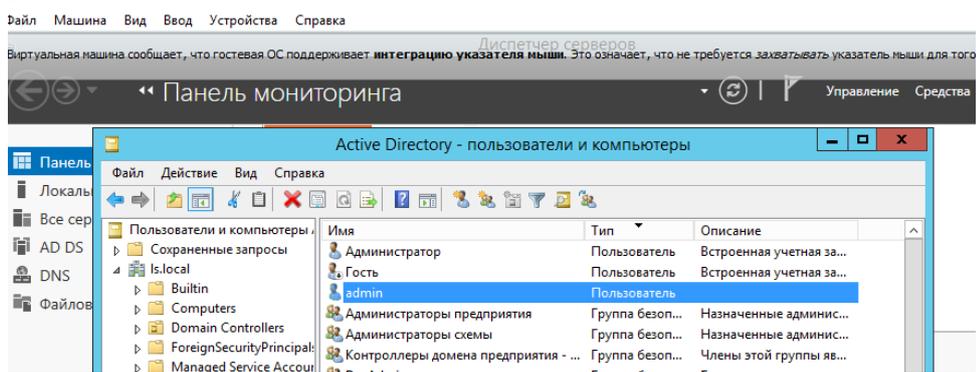




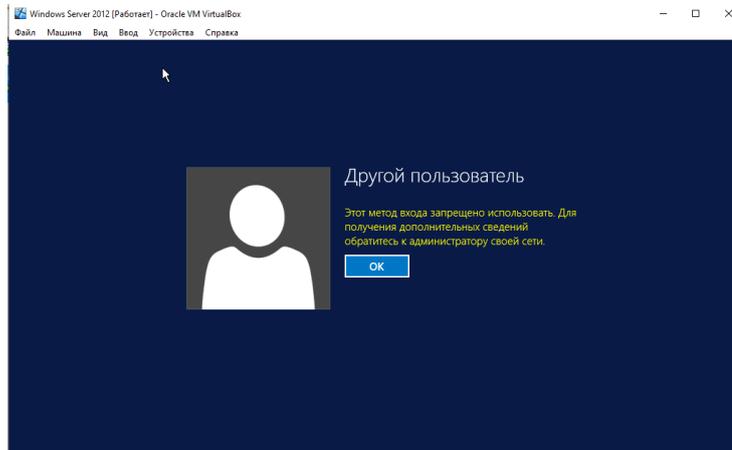
2. Настройка паролей



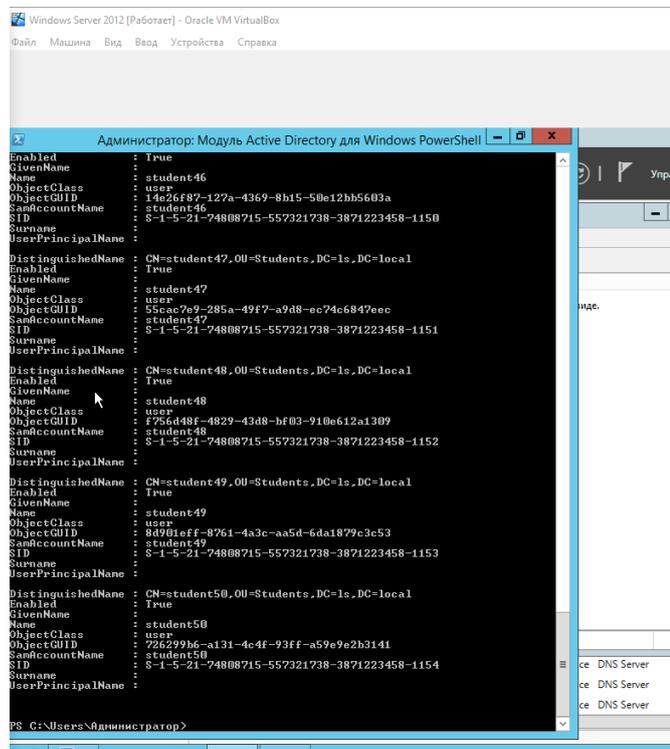




Пользователь не может войти на сервер, так как создан для работы в рабочей станции, подключенной к домену.



4. PowerShell



Практическая работа № 4 «Подключение сетевых периферийных устройств через Групповую политику»

Инструкция для обучающихся

Внимательно прочитайте задание. Проведите обследование объектов на предмет состояния инженерно-технического укрепления.

Время выполнения – 90 минут.

Задание

Установка принтеров пользователям домена AD с помощью групповых политик

Рассмотрим возможности автоматического подключения принтеров пользователям домена Active Directory с помощью групповых политик (GPO). Довольно удобно, когда при первом входе в систему у пользователя сразу устанавливаются и появляются в принтерах доступные ему устройства.

Рассмотрим следующую конфигурацию: в организации имеется 3 отдела, каждый отдел должен печатать документы на собственном цветном сетевом принтере. Ваша задача, как администратора, настроить автоматическое подключение сетевых принтеров пользователям в зависимости от отдела.

1. Подключение принтеров пользователям через GPO

1.1 Создайте три новые группы безопасности в AD (prn_HPColorSales, prn_HPColorIT, prn_HPColorManagers) и добавьте в нее пользователей отделов (наполнение групп пользователей можно автоматизировать по статье “Динамические группы в AD”). Вы можете создать группы в консоли ADUC, или с помощью командлета New-ADGroup:

```
New-ADGroup"prnHPColorSales"-path
```

```
'OU=Groups,OU=Moscow,DC=corp,dc=winitpro,DC=ru' -GroupScope Global -PassThru
```

1.2 Запустите консоль редактора доменных политик (GPMC.msc), создайте новую политику **prnt_AutoConnect** и прилинкуйте ее к OU с пользователями;

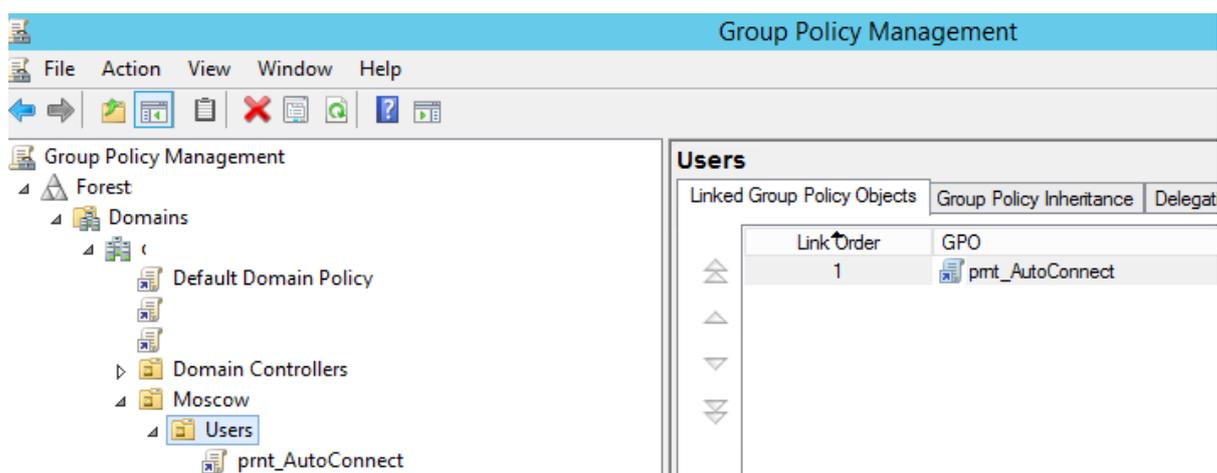


Рис. 48

Если у вас в домене используется небольшое количество сетевых принтеров (до 30-50), вы можете все их настраивать с помощью одной GPO. Если у вас сложная структура домена, есть сайты AD, используется делегирование прав администрато-

рам филиалов, лучше создать несколько политик подключения принтеров, например по одной политике на сайт или OU.

- 1.3 Перейдите в режим редактирования политики и разверните секцию **User Configuration -> Preferences -> Control Panel Setting -> Printers**. Создайте новый элемент политики с именем **Shared Printer**;

Если вы хотите подключать принтер по IP адресу (не через принт-сервер, а напрямую), выберите пункт **TCP/IP Printer**.

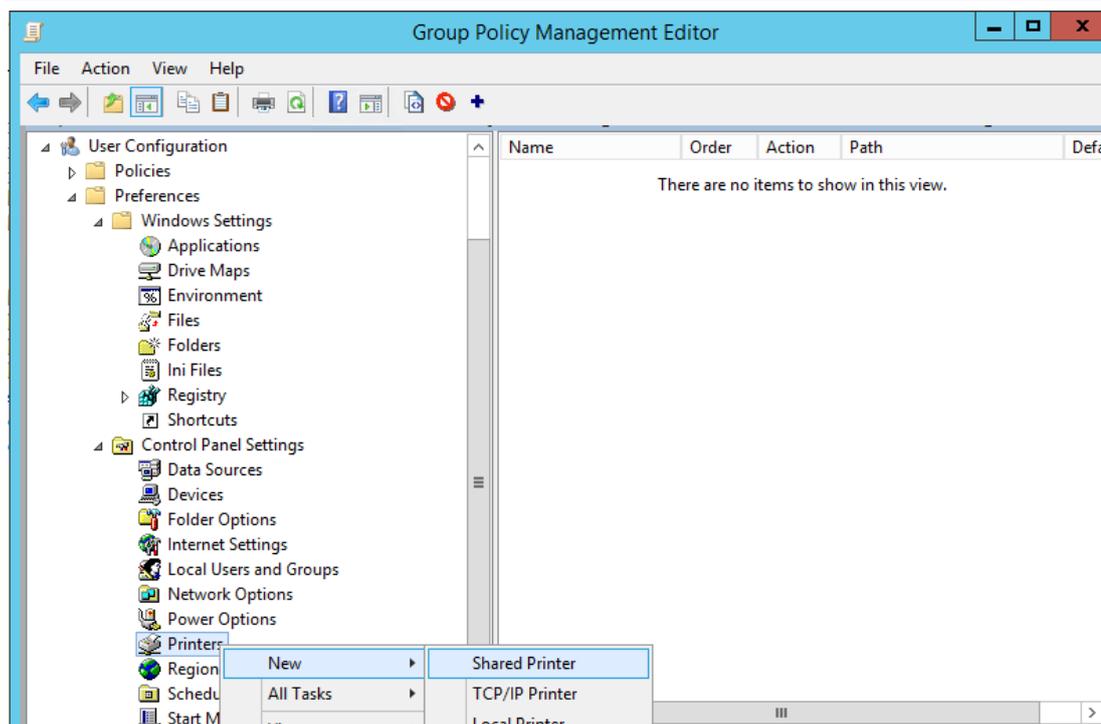


Рис. 49

- 1.4 Действие – **Update**. В поле **Shared Path** укажите UNC адрес принтера, например, `\\msk-prnt\hpcolorsales` (в моем примере все принтеры подключены к принт-серверу `\\msk-prnt`). Здесь же вы можете указать, нужно ли использовать этот принтер в качестве принтера по-умолчанию;

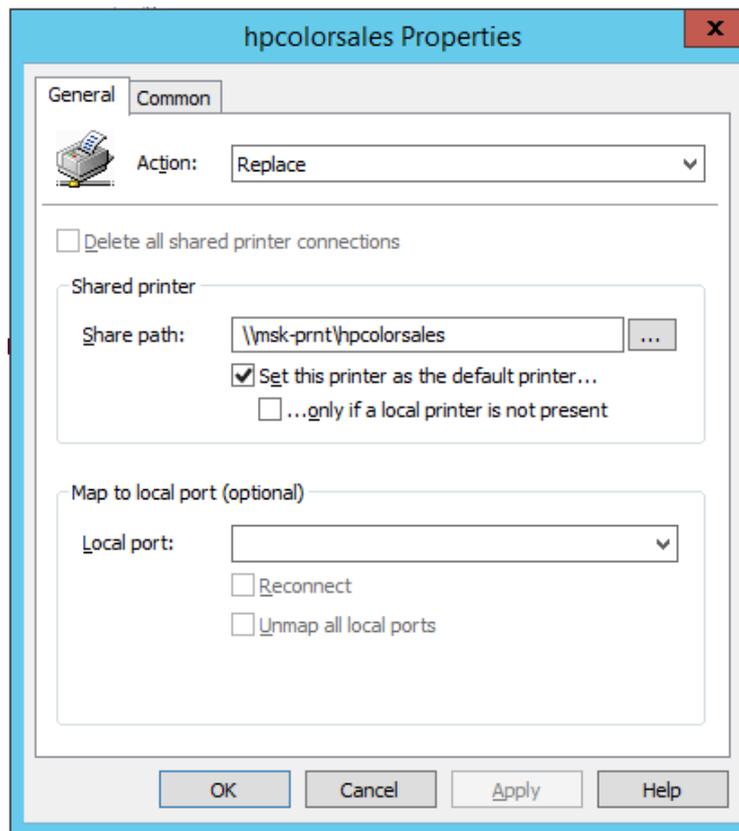


Рис. 50

- 1.5 Перейдите на вкладку **Common** и укажите, что принтер нужно подключать в контексте пользователя (опция **Run in logged-on user's security context**). Также выберите опцию **Item-level targeting** и нажмите на кнопку **Targeting**;
- 1.6 С помощью нацеливания GPP вам нужно указать, что данная политика подключения принтера применялась только для членов группы prn_HPColorSales. Для этого нажмите **New Item** -> **Security Group** -> в качестве имени группы укажите prn_HPColorSales;

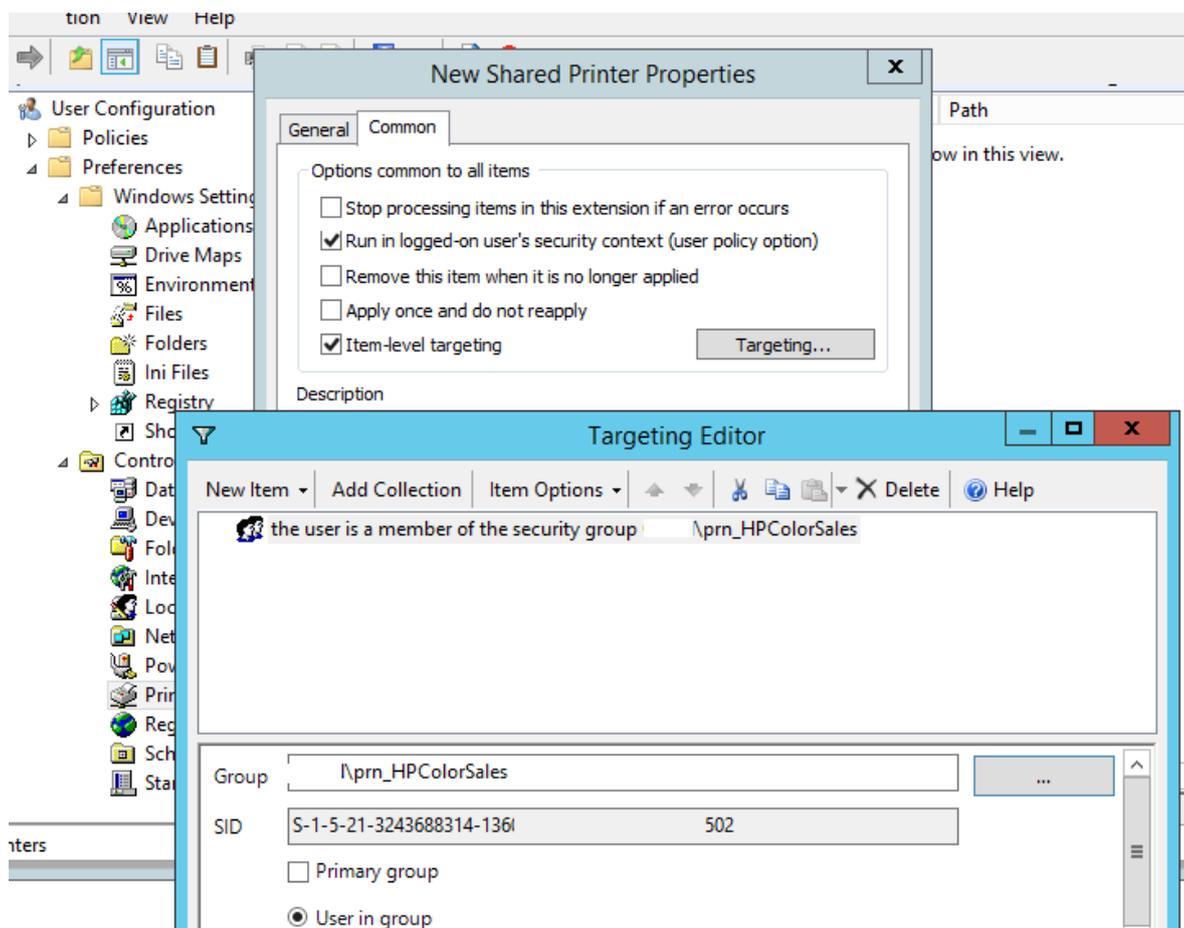


Рис. 51

Обратите внимание, что данное ограничение не запрещает любому пользователю домена подключить это принтер вручную в проводнике Windows. Чтобы ограничить доступ к принтеру, нужно изменить права доступа к нему на принт-сервере, ограничив возможность печати определенными группам.

1.7 Аналогичным образом создайте политики подключения принтеров для других групп пользователей.

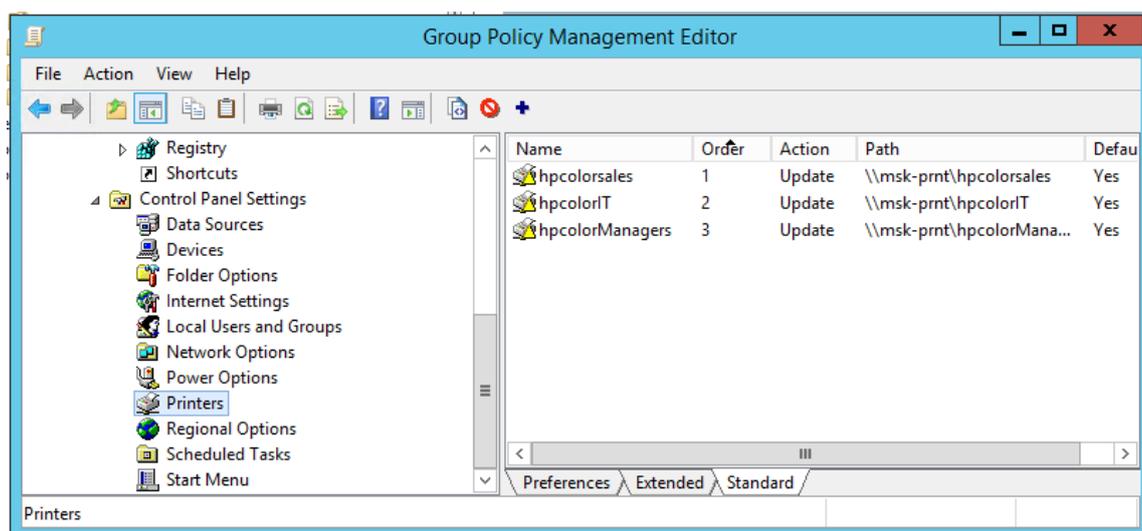


Рис. 52

Есть еще старый раздел политик для настройки принтеров — Computer Configuration -> Policies -> Windows Settings -> Deployed Printers, однако этот метод установки принтеров пользователям не такой гибкий, как рассмотренный выше способ с помощью GPP.

При использовании такой групповой политики, новые принтеры будут устанавливаться у пользователей, только если на их компьютере уже установлен соответствующий принтеру драйвер печати. Дело в том, что у обычных пользователей нет прав на установку драйверов.

2. Настройка политики подключения принтеров Point and Print Restrictions

2.1 Для корректного подключения принтеров у любого пользователя, вам необходимо настроить политику Point and Print Restrictions и настроить адреса принт-серверов серверов, с которых пользователей разрешено устанавливать принтеры.

Если вы подключаете принтеры через пользовательский раздел политики, перейдите в раздел GPO User Configuration -> Policy -> Administrative Templates -> Control Panel -> Printers -> Printer -> Point and Print Restriction. Включите политику (Enabled) и настройте ее следующим образом:

- **Users can only point and print to these servers** –укажите список принт-серверов, с которых разрешено устанавливать драйвера (указываются FQDN имена, разделитель точка с запятой);
- **When installing driver for new connection -> Do not show warning or elevation prompt**
- **When installing driver for existing connection -> Do not show warning or elevation prompt.**

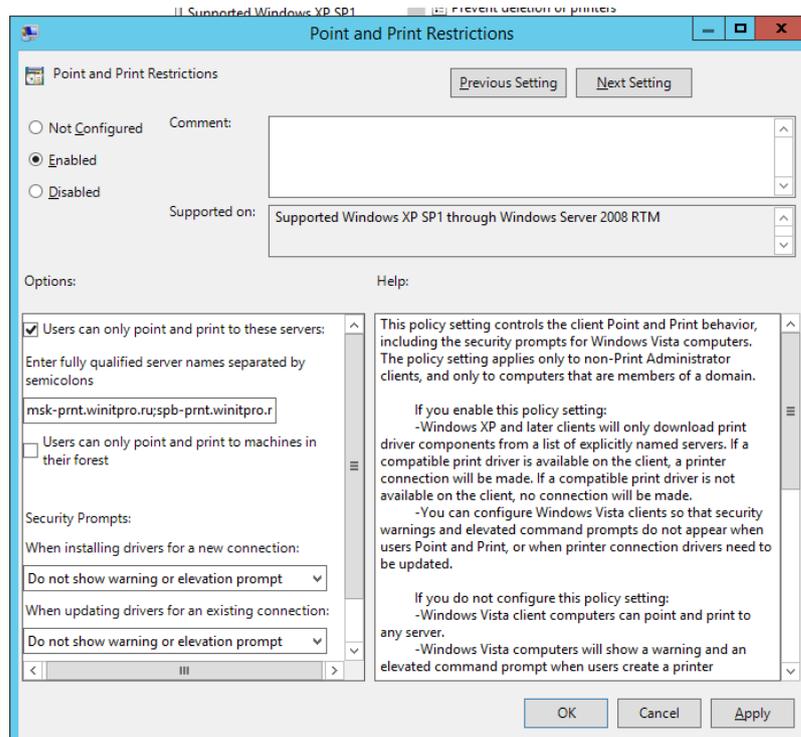


Рис. 53

Аналогичным образом нужно включить политику **Package Point and Print – Approved server** в разделе **User Configuration -> Policies -> Administrative Templates -> Printers** и задать в ней список доверенных принт-серверов.

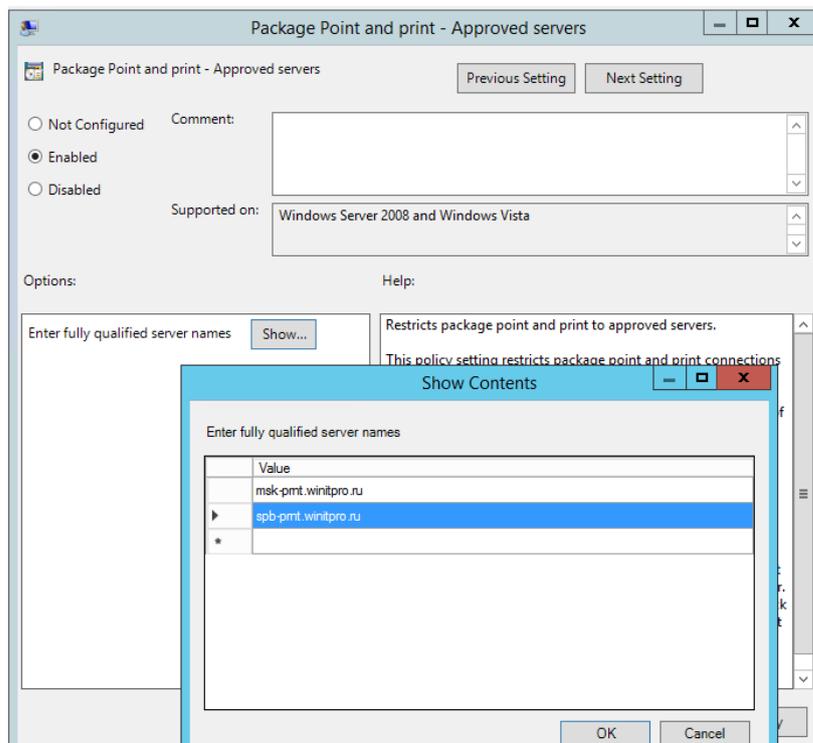


Рис. 54

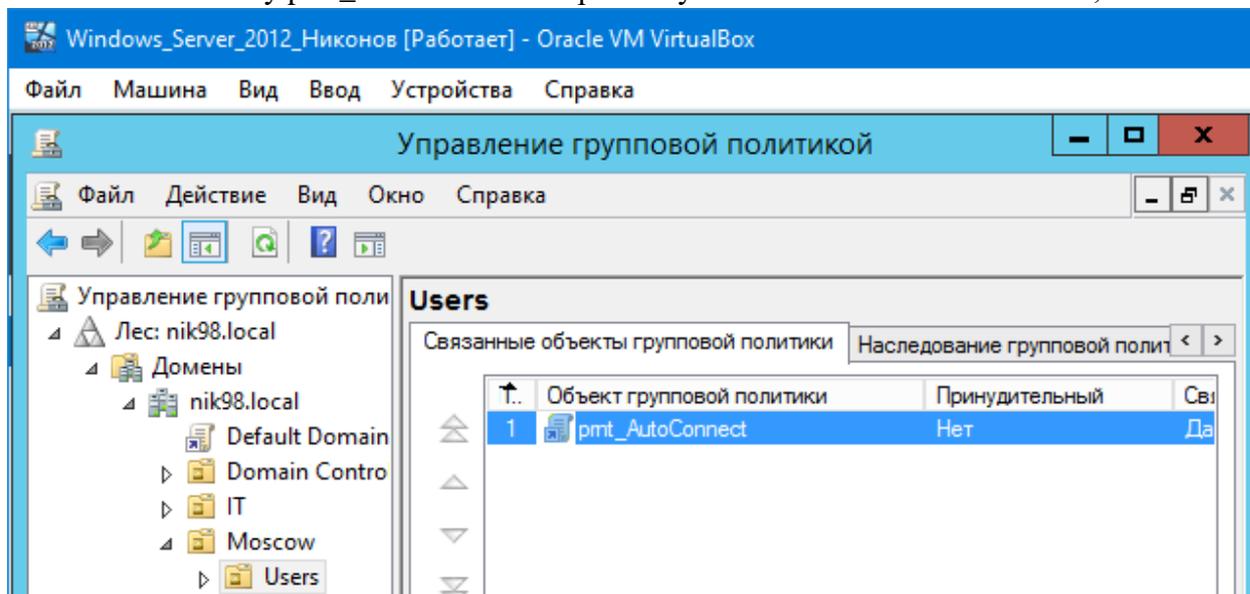
Теперь после перезагрузки компьютера при входе пользователя у него будет автоматически подключаться назначенный ему сетевой принтер.

Сделайте скриншоты (фотографии) процесса подключения сетевого принтера и вставьте в отчёт.

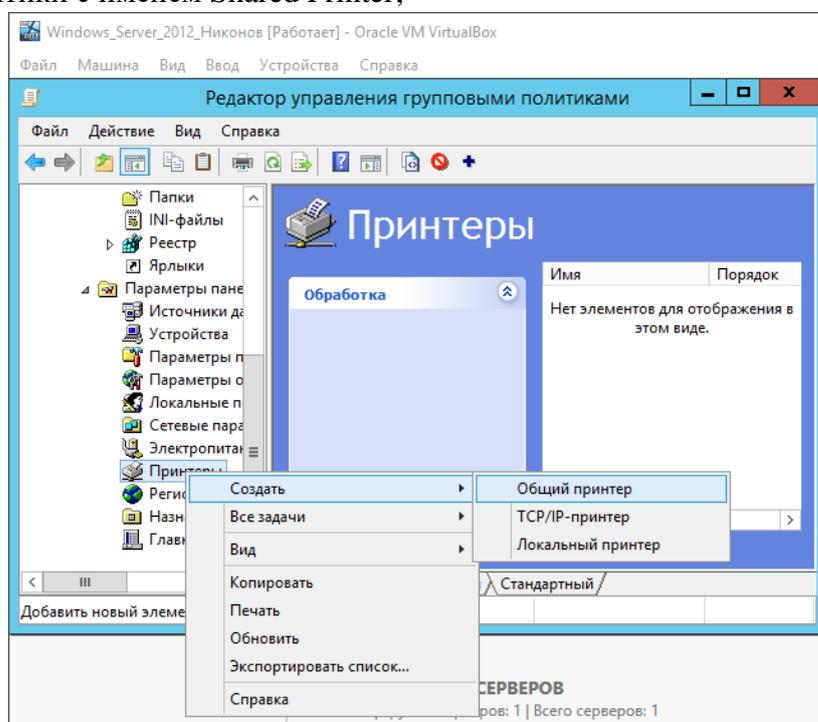
Эталон ответа

Создадим три новые группы безопасности в AD (prn_HPColorSales, prn_HPColorIT, prn_HPColorManagers) и добавим в нее пользователей отделов.

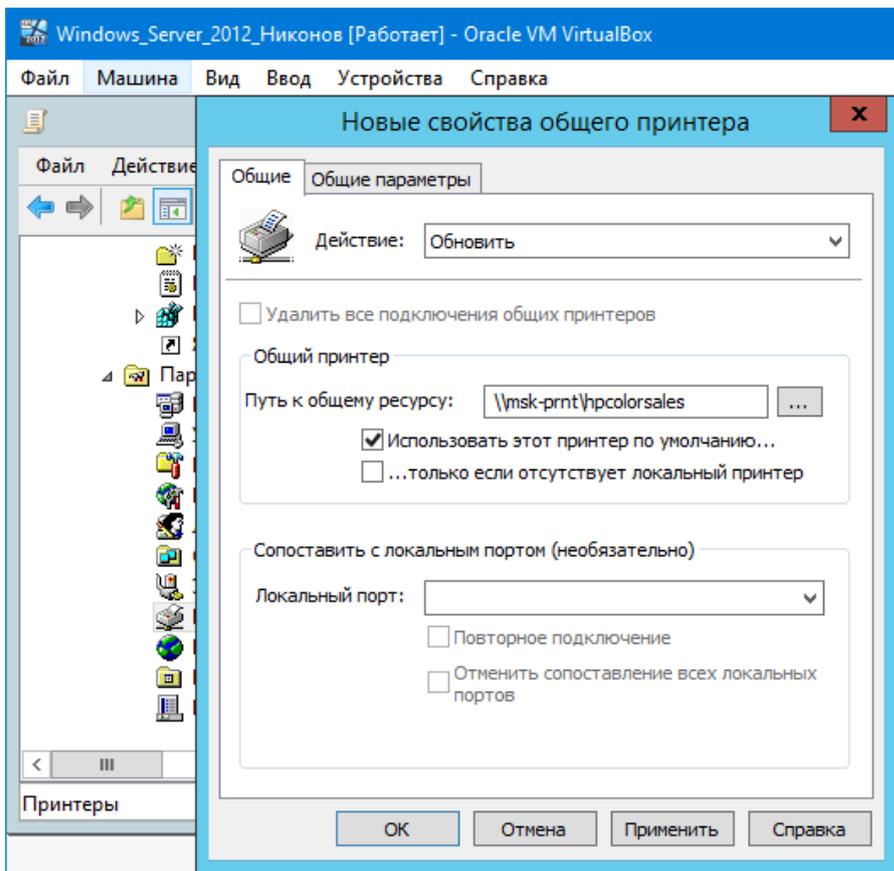
1. Запустим консоль редактора доменных политик (GPMC.msc), создадим новую политику prnt_AutoConnect и прилинкуем ее к OU с пользователями;



2. Перейдем в режим редактирования политики и развернем секцию User Configuration -> Preferences -> Control Panel Setting -> Printers. Создадим новый элемент политики с именем Shared Printer;

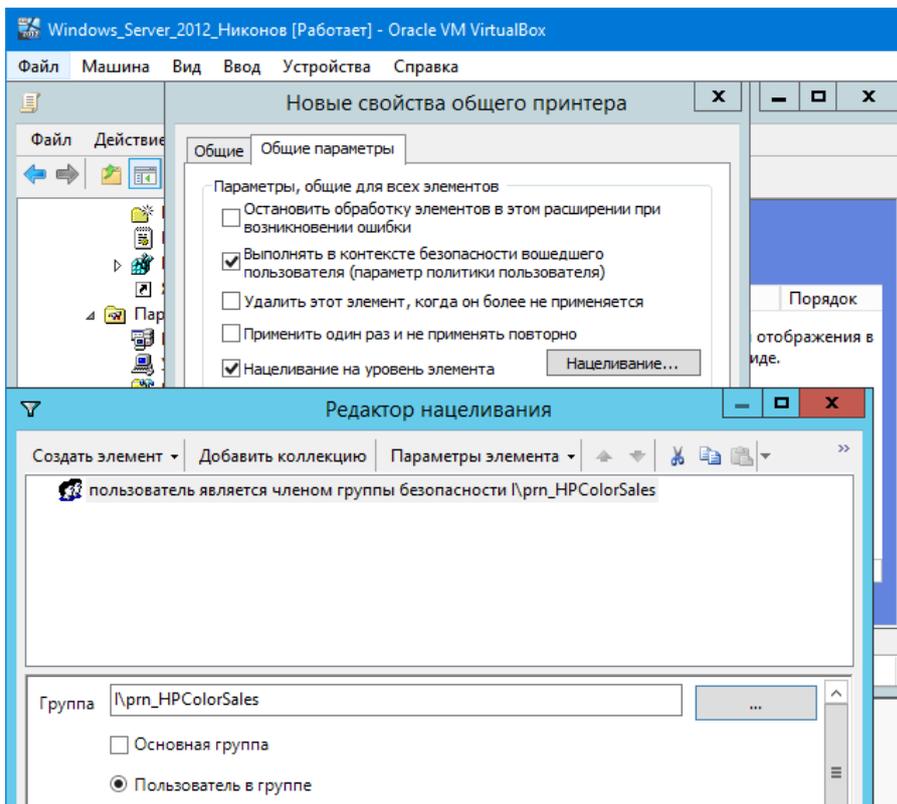


3. В поле Shared Path укажем UNC адрес принтера, « \\msk-prnt\hpcolorsales» Здесь же укажем, нужно ли использовать этот принтер в качестве принтера по умолчанию;

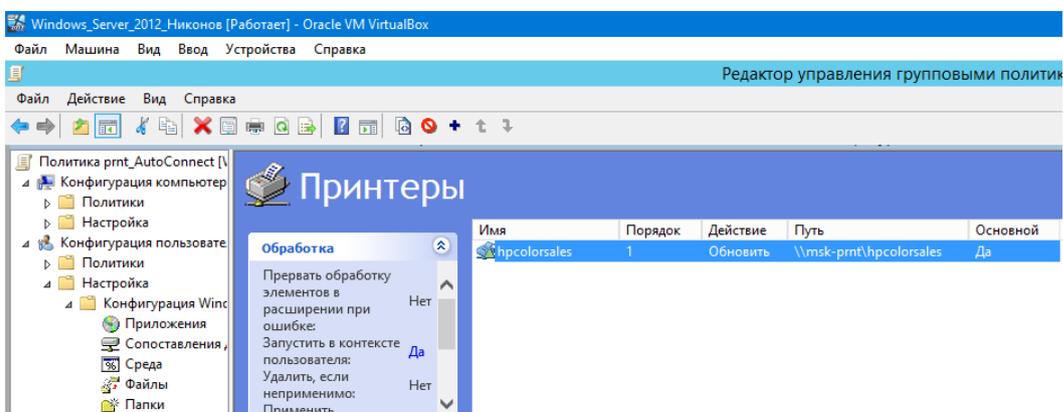


4. Перейдем на вкладку Common и укажем, что принтер нужно подключать в контексте пользователя. Также выберем опцию Item-level targeting и нажмем на кнопку Targeting;

5. С помощью нацеливания GPP укажем, что данная политика подключения принтера применялась только для членов группы prn_HPCOLORSales. Для этого нажмем New Item -> Security Group -> в качестве имени группы укажем prn_HPCOLOR Sales;



6. Аналогичным образом создадим политики подключения принтеров для других групп пользователей.



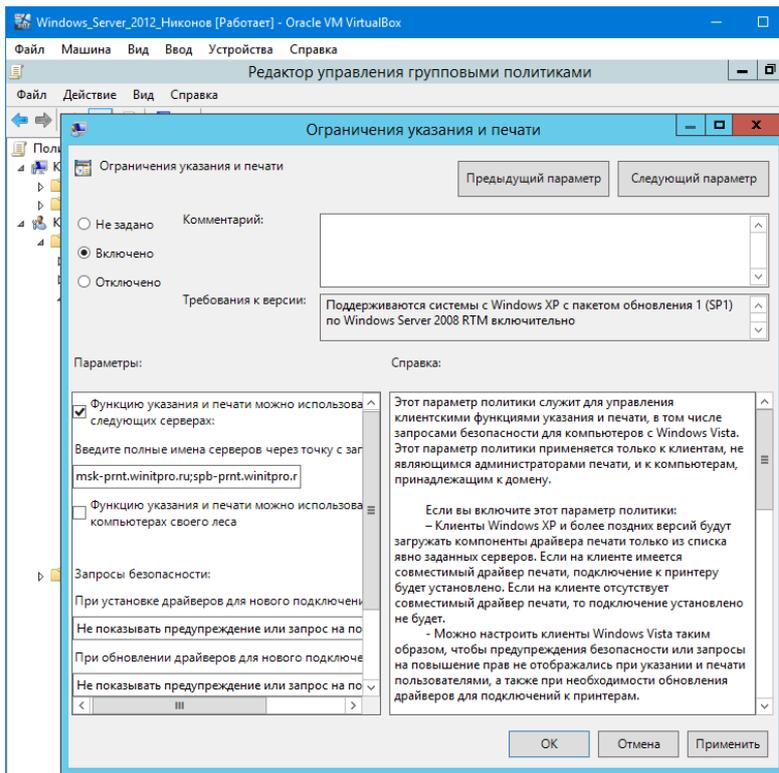
Настройка политики подключения принтеров Point and Print Restrictions

Для корректного подключения принтеров у любого пользователя, придется настроить политику Point and Print Restrictions и настроить адреса принт-серверов серверов, с которых пользователей разрешено устанавливать принтеры.

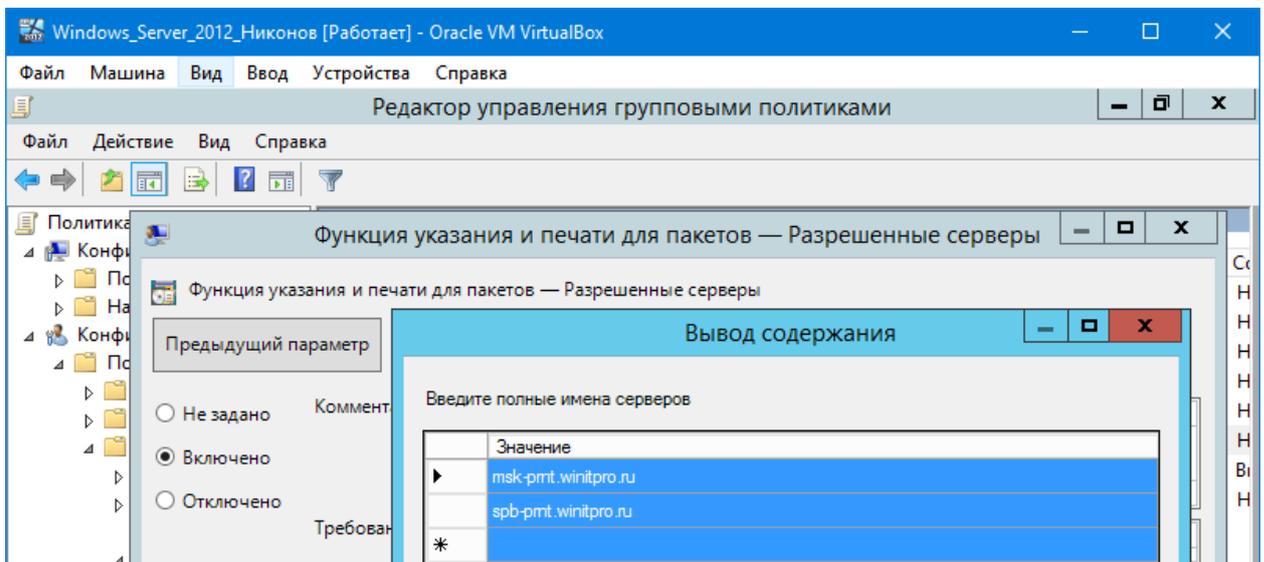
Перейдем в раздел GPO User Configuration -> Policy -> Administrative Templates -> Control Panel -> Printers -> Printer -> Point and Print Restriction. Включим политику (Enabled) и настроим ее следующим образом:

- Users can only point and print to these servers –укажите список принт-серверов, с которых разрешено устанавливать драйвера (указываются FQDN имена, разделитель точка с запятой);

- When installing driver for new connection -> Do not show warning or elevation prompt
- When installing driver for existing connection -> Do not show warning or elevation prompt.



Аналогичным образом включим политику Package Point and Print – Approved server в разделе User Configuration -> Policies -> Administrative Templates -> Printers и зададим в ней список доверенных принт-серверов.



Теперь после перезагрузки компьютера при входе пользователя у него будет автоматически подключаться назначенный ему сетевой принтер.

3. Устный зачет по теме 1.1.

Инструкция для обучающихся

Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 2 вопроса.

Выполнение задания: одному студенту на ответ выделяется 3 мин., группа сдает зачет за одно учебное занятие.

Перечень вопросов:

1. Что такое виртуализация?
2. Как в Windows Server 2012 реализуется Мультиотенантный шлюз VPN?
3. Что такое Групповая работа сетевых адаптеров?
4. Что такое архитектура неоднородной памяти (Non-Uniform Memory Architecture, NUMA)?
5. Как обеспечивается защита доступа и информации в Windows Server 2012?
6. Как обеспечивается контролируемый доступ к корпоративной информации?
7. Что представляет собой диск профиля пользователя?
8. Что такое каталог (AD)?
9. Каковы функции службы каталогов?
10. Что понимается под масштабируемостью службы каталогов?

Эталоны ответов: приведены в Учебном пособии по МДК.04.01 «Эксплуатация аппаратного обеспечения, операционной системы, периферийных устройств и оргтехники»

Практическая работа № 19 «Поиск уязвимостей информационных систем»

Инструкция для обучающихся

Внимательно прочитайте задание. Проведите поиск уязвимостей информационной системы.

Время выполнения – 90 минут.

Задание

Kali включает в себя очень способный OpenVAS, который является бесплатным и с открытым исходным кодом.

Это просто потому, что сканеры уязвимостей часто имеют слабую репутацию, прежде всего потому, что их роль и цель неправильно поняты.

Сканеры Vulnerabilty сканируют уязвимости – но они не являются волшебными машинами эксплойта и должны быть одним из многих источников информации, используемых в оценке безопасности.

Слепой запуск сканера уязвимостей на цель почти наверняка закончится разочарованием и горем, с десятками (или даже сотнями) результатов низкого уровня или неинформативных результатов.

1. Системные Требования

Основная жалоба, которую получают о OpenVAS (или любом другом сканере уязвимостей), можно резюмировать как «она слишком медленная и сбойная и не работает, и это плохо, и очень плохо».

Почти во всех случаях медленность и / или сбои связаны с недостаточными системными ресурсами.

OpenVAS имеет десятки тысяч сигнатур, и если вы не дадите вашей системе достаточного количества ресурсов, особенно оперативной памяти, вы окажетесь в мире страданий.

Для некоторых коммерческих сканеров уязвимостей требуется как минимум 8 ГБ ОЗУ и рекомендуется еще больше.

OpenVAS не требует около такого объема памяти, но чем больше вы можете предоставить ему, тем более плавно система сканирования будет работать.

Для этого урока наша виртуальная машина Kali имеет 3 процессора и 3 ГБ оперативной памяти, что обычно достаточно для сканирования небольшого количества хостов одновременно.

2. Начальная установка OpenVAS в Кали

У OpenVAS много движущихся частей, и настройка вручную может быть проблемой.

К счастью, Kali содержит простую в использовании утилиту под названием «openvas-setup», которая занимается настройкой OpenVAS, загрузкой сигнатур и созданием пароля для пользователя admin.

Эта первоначальная настройка может занять довольно много времени, даже при быстром подключении к Интернету, можно просто сидеть сложа руки.

В конце настройки будет отображаться автоматически созданный пароль для пользователя admin.

Обязательно сохраните этот пароль где-нибудь в безопасности.

```
root@kali:~# openvas-setup
ERROR: Directory for keys (/var/lib/openvas/private/CA) not found!
ERROR: Directory for certificates (/var/lib/openvas/CA) not found!
ERROR: CA key not found in /var/lib/openvas/private/CA/cakey.pem
ERROR: CA certificate not found in /var/lib/openvas/CA/cacert.pem
ERROR: CA certificate failed verification, see /tmp/tmp.7G2IQWtqwj/openvas-manage-
certs.log for details. Aborting.ERROR: Your OpenVAS certificate infrastructure did NOT pass
validation.
See messages above for details.
```

```
Generated private key in /tmp/tmp.PerU51G2tl/cakey.pem.  
Generated self signed certificate in /tmp/tmp.PerU51G2tl/cacert.pem.  
...  
/usr/sbin/opensvamd  
User created with password 'xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx'.
```

3. Работа с ошибками установки

Иногда скрипт «openvas-setup» будет отображать ошибки в конце загрузки NVT, аналогичные приведенным ниже.

```
(openvassd:2272): lib kb_redis-CRITICAL **: get_redis_ctx: redis connection error: No such  
file or directory  
(openvassd:2272): lib kb_redis-CRITICAL **: redis_new: cannot access redis at  
'/var/run/redis/redis.sock'  
(openvassd:2272): lib kb_redis-CRITICAL **: get_redis_ctx: redis connection error: No such  
file or directory  
openvassd: no process found
```

Если вам посчастливилось столкнуться с этой проблемой, вы можете запустить «openvas-check-setup», чтобы узнать, какой компонент вызывает проблемы.

В этом конкретном случае мы получаем следующее из скрипта:

```
...  
ERROR: The number of NVTs in the OpenVAS Manager database is too low.  
FIX: Make sure OpenVAS Scanner is running with an up-to-date NVT collection and run 'open-  
vasmd --rebuild'.  
...
```

Скрипт «openvas-check-setup» обнаруживает проблему и даже предоставляет команду для запуска (надеюсь) решения этой проблемы.

После восстановления коллекции NVT рекомендуется пройти все проверки.

```
root@kali:~# openvasmd --rebuild  
root@kali:~# openvas-check-setup  
openvas-check-setup 2.3.7  
Test completeness and readiness of OpenVAS-9  
...
```

It seems like your OpenVAS-9 installation is OK.

...

4. Управление пользователями OpenVAS

Если вам нужно (или хотите) создать дополнительных пользователей OpenVAS, запустите 'openvasmd' с параметром -create-user, который добавит нового пользователя и отобразит случайно сгенерированный пароль.

```
root@kali:~# openvasmd --create-user=dookie
```

```
User created with password 'уууууууу-уууу-уууу-уууу-уууууууууууу'.
```

```
root@kali:~# openvasmd --get-users
```

```
admin
```

```
dookie
```

К счастью, изменение паролей пользователей OpenVAS легко осуществляется с помощью опции «openvasmd» и «new-password».

```
root@kali:~# openvasmd --user=dookie --new-password=s3cr3t
```

```
root@kali:~# openvasmd --user=admin --new-password=sup3rs3cr3t
```

5. Запуск и остановка OpenVAS

Сетевые службы по умолчанию отключены в Kali Linux, поэтому, если вы не настроили OpenVAS для запуска при загрузке, вы можете запустить необходимые службы, запустив «openvas-start».

```
root@kali:~# openvas-start
```

Starting OpenVas Services После того, как у вас есть список хостов, вы можете импортировать их в разделе «Цели» в меню «Конфигурация».

Когда службы завершают инициализацию, вы должны найти TCP-порты 9390 и 9392, которые прослушивают ваш loopback-интерфейс.

```
root@kali:~# ss -ant
```

```
State Recv-Q Send-Q Local Address:Port Peer Address:Port
```

```
LISTEN 0 128 127.0.0.1:9390 *:*
```

```
LISTEN 0 128 127.0.0.1:9392 *:*
```

Из-за нагрузки на системные ресурсы вы, вероятно, захотите остановить OpenVAS, когда вы закончите использовать его, особенно если вы не используете специальную систему для сканирования уязвимостей.

OpenVAS можно остановить, запустив «openvas-stop».

```
root@kali:~# openvas-stop
```

6. Использование Greenbone Security Assistant

Greenbone Security Assistant – это веб-интерфейс OpenVAS, доступный на вашем локальном компьютере (после запуска OpenVAS) на **https://localhost: 9392**.

После принятия самоверенного сертификата вам будет представлена страница входа в систему и после аутентификации вы увидите основную панель.



Рис. 55

7. Настройка учетных данных

Сканеры уязвимостей обеспечивают наиболее полные результаты, когда вы можете предоставить механизму сканирования учетные данные для использования на сканируемых системах.

OpenVAS будет использовать эти учетные данные для входа в сканируемую систему и выполнения подробного перечисления установленного программного обеспечения, патчей и т. д.

Вы можете добавить учетные данные через запись «Credentials» в меню «Configuration».

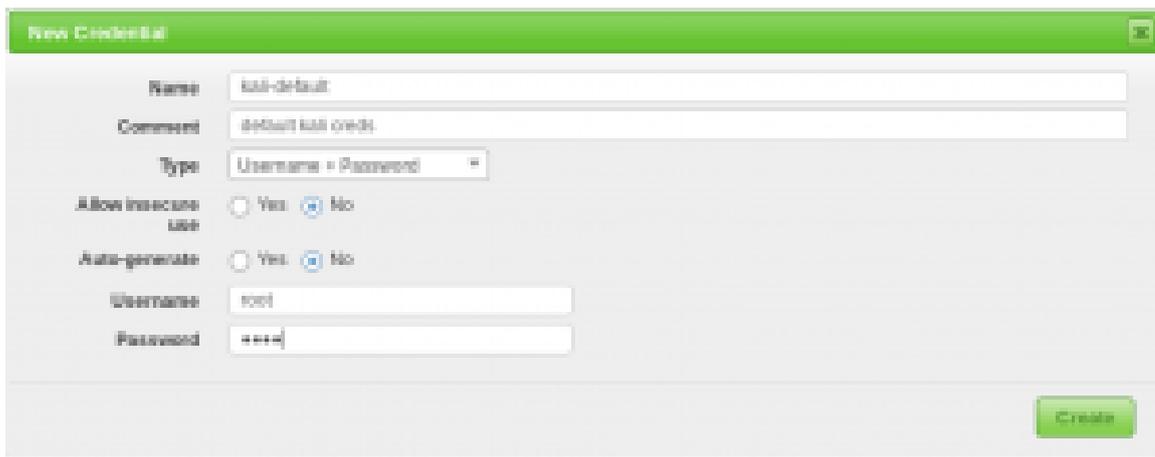


Рис. 56

8. Конфигурация цели

OpenVAS, как и большинство сканеров уязвимостей, может сканировать удаленные системы, но это сканер уязвимостей, а не сканер портов.

Вместо того, чтобы полагаться на сканер уязвимостей для идентификации хостов, вы значительно упростите свою жизнь с помощью специализированного сетевого сканера, такого как Nmap или Masscan, и импортируйте список целей в OpenVAS.

```
root@kali:~# nmap -sn -oA nmap-subnet-86 192.168.86.0/24
```

```
root@kali:~# grep Up nmap-subnet-86.gnmap | cut -d " " -f 2 > live-hosts.txt
```

После того, как у вас есть список хостов, вы можете импортировать их в разделе «target» в меню «Configuration».

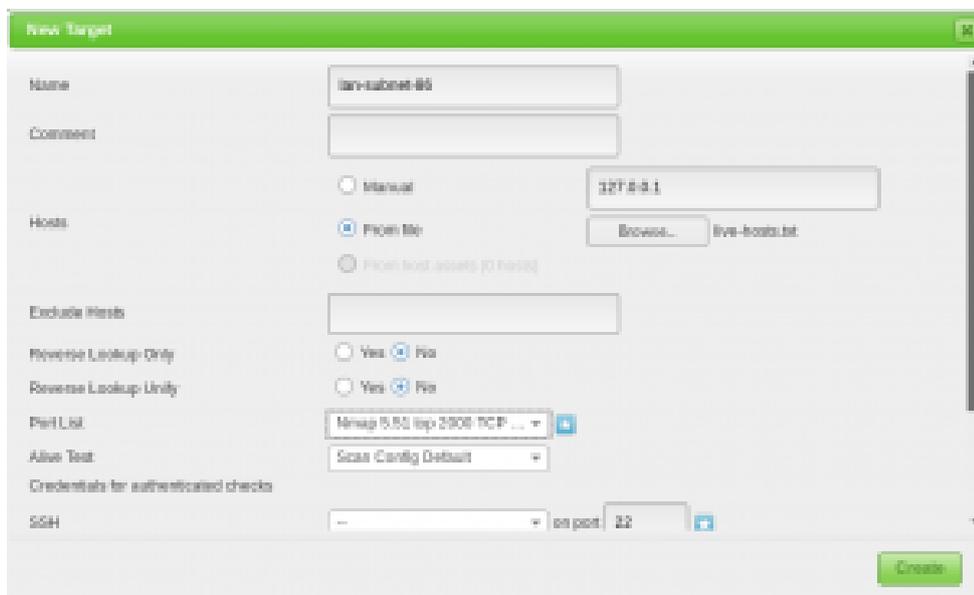


Рис. 57

Name	Hosts	IPs	Port List	Credentials - auth type	Actions
subnet-00	192.168.0.1, 192.168.0.2, 192.168.0.3, 192.168.0.4, 192.168.0.5, 192.168.0.6, 192.168.0.7, 192.168.0.8, 192.168.0.9, 192.168.0.10, 192.168.0.11, 192.168.0.12, 192.168.0.13, 192.168.0.14, 192.168.0.15, 192.168.0.16, 192.168.0.17, 192.168.0.18, 192.168.0.19, 192.168.0.20, 192.168.0.21, 192.168.0.22, 192.168.0.23, 192.168.0.24, 192.168.0.25, 192.168.0.26, 192.168.0.27, 192.168.0.28, 192.168.0.29, 192.168.0.30, 192.168.0.31, 192.168.0.32, 192.168.0.33, 192.168.0.34, 192.168.0.35, 192.168.0.36, 192.168.0.37, 192.168.0.38, 192.168.0.39, 192.168.0.40, 192.168.0.41, 192.168.0.42, 192.168.0.43, 192.168.0.44, 192.168.0.45, 192.168.0.46, 192.168.0.47, 192.168.0.48, 192.168.0.49, 192.168.0.50, 192.168.0.51, 192.168.0.52, 192.168.0.53, 192.168.0.54, 192.168.0.55, 192.168.0.56, 192.168.0.57, 192.168.0.58, 192.168.0.59, 192.168.0.60, 192.168.0.61, 192.168.0.62, 192.168.0.63, 192.168.0.64, 192.168.0.65, 192.168.0.66, 192.168.0.67, 192.168.0.68, 192.168.0.69, 192.168.0.70, 192.168.0.71, 192.168.0.72, 192.168.0.73, 192.168.0.74, 192.168.0.75, 192.168.0.76, 192.168.0.77, 192.168.0.78, 192.168.0.79, 192.168.0.80, 192.168.0.81, 192.168.0.82, 192.168.0.83, 192.168.0.84, 192.168.0.85, 192.168.0.86, 192.168.0.87, 192.168.0.88, 192.168.0.89, 192.168.0.90, 192.168.0.91, 192.168.0.92, 192.168.0.93, 192.168.0.94, 192.168.0.95, 192.168.0.96, 192.168.0.97, 192.168.0.98, 192.168.0.99, 192.168.0.100	01	all listed, assigned TCP 2001-40-10	SSH	   

Рис. 58

9. Конфигурация сканирования

Перед запуском сканирования уязвимостей вы должны точно настроить Scan Config/,

Это можно сделать в разделе “Scan Configs” в меню “Config”.

Вы можете клонировать любую конфигурацию сканирования по умолчанию и редактировать ее параметры, отключая любые службы или проверки, которые вам не нужны.

Если вы используете Nmap для проведения предварительного анализа ваших целевых объектов, вы можете сэкономить время сканирования уязвимости.

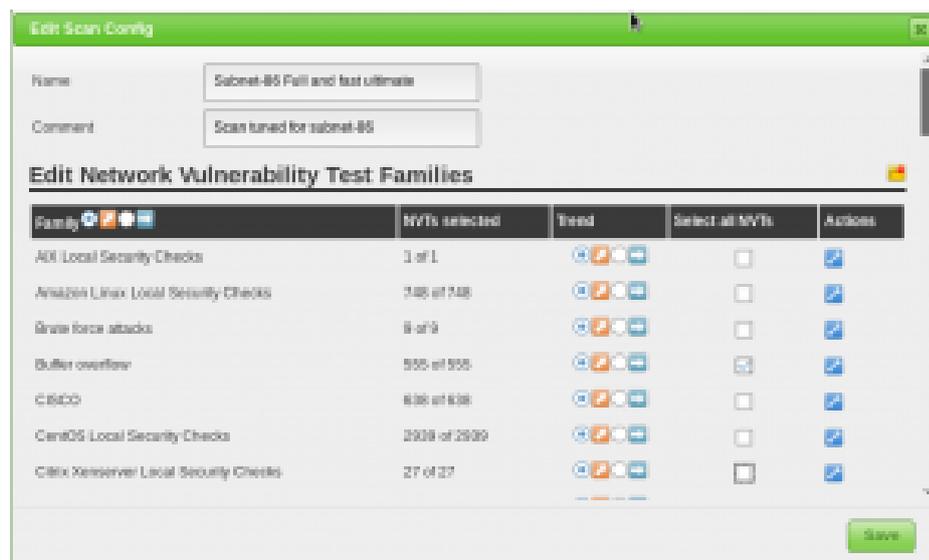


Рис. 59

10. Конфигурация задачи

Ваши учетные данные, цели и конфигурации сканирования настроены таким образом, что теперь вы готовы собрать все вместе и запустить сканирование уязвимостей.

В OpenVAS сканирование уязвимостей проводится как «tasks».

Когда вы настраиваете новую задачу, вы можете дополнительно оптимизировать сканирование путем увеличения или уменьшения одновременных действий, которые происходят.

С нашей системой с 2 ГБ оперативной памяти мы скорректировали наши настройки задач, как показано ниже.



Рис. 60

Благодаря нашим более точно настроенным параметрам сканирования и целевому выбору результаты нашего сканирования намного полезнее.



Рис. 61

11. Автоматизация OpenVAS

Одной из менее известных функций OpenVAS является интерфейс командной строки, с которым вы взаимодействуете с помощью команды «omr».

Его использование не совсем интуитивно, но мы не единственные поклонники OpenVAS, и мы столкнулись с несколькими базовыми скриптами, которые вы можете использовать и расширить сканирование для автоматизации OpenVAS.

Первый – `openvas-automate.sh` от `mgeeky`, полуинтерактивный скрипт Bash, который предлагает вам тип сканирования и заботится обо всем остальном.

Конфигурации сканирования жестко закодированы в сценарии, поэтому, если вы хотите использовать свои настроенные конфиги, их можно добавить в разделе «targets».

```
root@kali:~# apt -y install pcregrep
```

```
root@kali:~# ./openvas-automate.sh 192.168.86.61:: OpenVAS automation script.
```

```
mgeeky, 0.1[>] Please select scan type:
```

1. Discovery
2. Full and fast
3. Full and fast ultimate
4. Full and very deep
5. Full and very deep ultimate
6. Host Discovery
7. System Discovery
9. Exit

```
-----
```

```
Please select an option: 5
```

```
[+] Tasked: 'Full and very deep ultimate' scan against '192.168.86.61'
```

```
[>] Reusing target...
```

```
[+] Target's id: 6ccbb036-4afa-46d8-b0c0-acbd262532e5
```

```
[>] Creating a task...
```

```
[+] Task created successfully, id: '8e77181c-07ac-4d2c-ad30-9ae7a281d0f8'
```

```
[>] Starting the task...
```

```
[+] Task started. Report id: 6bf0ec08-9c60-4eb5-a0ad-33577a646c9b
```

```
[.] Awaiting for it to finish. This will take a long while...
```

```
8e77181c-07ac-4d2c-ad30-9ae7a281d0f8 Running 1% 192.168.86.61
```

Мы также наткнулись на сообщение в блоге по code16, которое представляет и объясняет их скрипт Python для взаимодействия с OpenVAS.

Подобно скрипту Bash выше, вам нужно будет внести некоторые изменения в скрипт, если вы хотите настроить тип сканирования.

```
root@kali:~# ./code16.py 192.168.86.27
```

```
-----
```

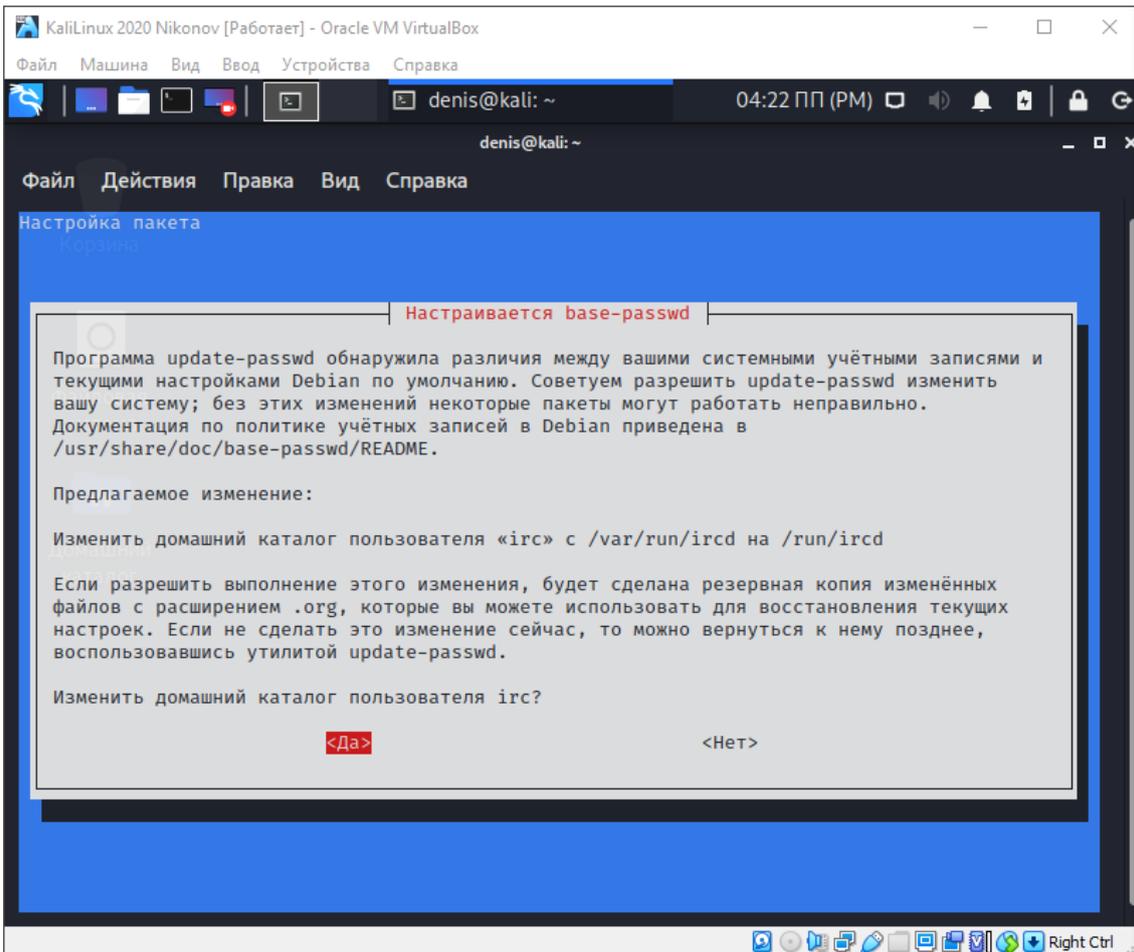


```
KaliLinux 2020 Nikonov [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
denis@kali: ~ 03:24 ПП (PM)
denis@kali: ~
Файл Действия Правка Вид Справка
denis@kali:~$ sudo apt-get update
[sudo] пароль для denis:
Сущ:1 http://mirror-1.truenetwork.ru/kali kali-rolling InRelease
Чтение списков пакетов... Готово
denis@kali:~$ sudo apt-get dist-upgrade
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Расчёт обновлений... Готово
Следующие пакеты устанавливались автоматически и больше не требуются:
 libarmadillo9 libcdio18 libcfitsio8 libgtksourceview2.0-common libgtksourceview2.0-common
 libjsoncpp1 libmpdec2 libobjc-9-dev libpgm-5.2-0 libpoppler82 libprotobuf22 libproxychains3
 libpython2-stdlib libsnmp35 libsrtp1-gnutls libtsk13 libx264-155 libx264-159 libyara3
 openjdk-8-jre proxychains python-cairo python-dbus python-enchant python-gi
 python-gobject-2 python-numpy python-pkg-resources python2 python2-minimal
 python3-flask-restless python3-grequests python3-mimeparse python3-mimerender
Для их удаления используйте «sudo apt autoremove».
Следующие пакеты будут УДАЛЕНЫ:
 libgc1c2 libpython-stdlib python python-chardet python-gtk2 python-gtksourceview2
 python-minimal
Следующие НОВЫЕ пакеты будут установлены:
 calendar cpp-10 g++-10 gcc-10 gir1.2-harfbuzz-0.0 ipp-usb kali-defaults-desktop
 kali-linux-headless kali-wallpapers-2020.4 kismet-capture-ubertooth-one libarmadillo10
 libasan6 libayatana-ido3-0.4-0 libbfio1 libbtbb1 libcdio19 libcfitsio9 libclang-cpp10
 libgc1 libgcc-10-dev libgspell-1-2 libgspell-1-common libgtksourceviewmm-3.0-0v5 libjson-c5
 libnsl-dev libnsl2 libnss-nis libnss-nisplus libobjc-10-dev libpgm-5.3-0 libpoppler102
 libproxychains4 libpython3.9-minimal libpython3.9-stdlib librtlsdr0 librttopo1 libsane1
 libstdc++-10-dev libtbb2 libtirpc-dev libtsk19 libubertooth1 libudfread0 libvhd1 libvmdk1
 libx264-160 libxml++2.6-2v5 libyara4 linux-compiler-gcc-10-x86
 linux-headers-5.9.0-kali1-amd64 linux-headers-5.9.0-kali1-common
 linux-image-5.9.0-kali1-amd64 linux-kbuild-5.9 llvm-10 llvm-10-dev llvm-10-runtime
```

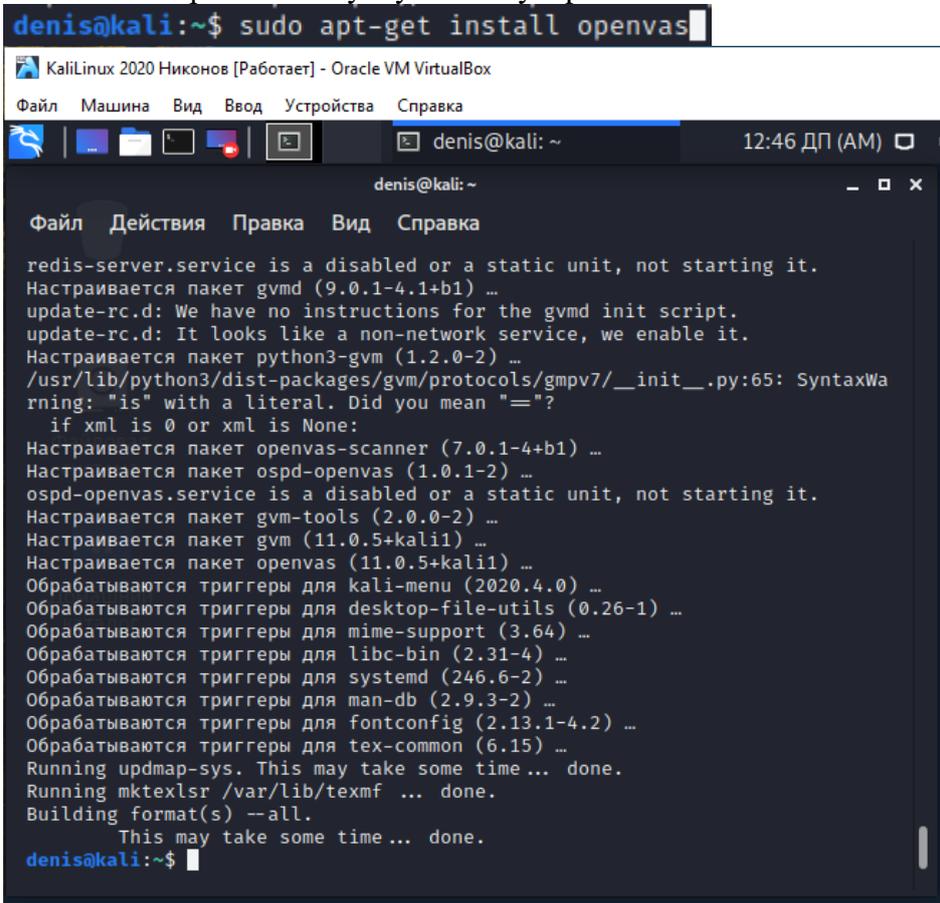
Соглашаемся:

```
KaliLinux 2020 Nikonov [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
denis@kali: ~ 04:06 ПП (PM)
denis@kali: ~
Файл Действия Правка Вид Справка
Package configuration
Configuring libc6:amd64
There are services installed on your system which need to be restarted when certain
libraries, such as libpam, libc, and libssl, are upgraded. Since these restarts may
cause interruptions of service for the system, you will normally be prompted on each
upgrade for the list of services you wish to restart. You can choose this option to
avoid being prompted; instead, all necessary restarts will be done for you
automatically so you can avoid being asked questions on each library upgrade.
Restart services during package upgrades without asking?
<Yes> <No>
```

Соглашаемся:



Выполним первоначальную установку OpenVAS:



```

denis@kali:~$ sudo apt-get update && sudo apt-get install -y openvas
Пол:1 http://mirror-1.truenetwork.ru/kali kali-rolling InRelease [30,5 kB]
Пол:2 http://mirror-1.truenetwork.ru/kali kali-rolling/main amd64 Packages
[16,9 MB]
Получено 16,9 MB за 4с (4 688 kB/s)
Чтение списков пакетов... Готово
Чтение списков пакетов... Готово
Построение дерева зависимостей

```

Зайдем под root:

```

denis@kali:~$ sudo -s
root@kali:/home/denis#

```

```

root@kali:~# apt-get install openvas
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Следующие пакеты устанавливались автоматически и больше не требуются:
 cython dconf-cli dh-python easy-rsa enchant finger fonts-glyphicons-halflings
 hashcat-data kde-style-qtcurve-qt5 kdelibs5-data lib32gcc-s1 lib32stdc++6
 libbind9-161 libboost-iostreams1.67.0 libboost-regex1.67.0 libc6-i386 libclang1-6.0
 libclang1-7 libcodecd2-0.8.1 libcrococ3 libcrystalhd3 libcupsfilters1 libcupsimage2
 libdc1394-22 libdirstrestrictions1 libdns1104 libdns1110 libdvdrread4 libebml4v5
 libenchant1c2a libevent-2.1-6 libevent-core-2.1-6 libevent-openssl-2.1-6
 libevent-pthreads-2.1-6 libexiv2-14 libgeos-3.7.2 libgit2-27 libgps23 libgssglue1
 libgtkmm-2.4-1v5 libgtksourceview2.0-0 libgtksourceview2.0-common libhavege1
 libhwloc5 libigdgmm9 libilmbase23 libirs161 libisc1100 libisc1105 libisccc161
 libisccfg163 libisl19 libjim0.77 libkf5jsembed-data libkf5jsembed5

```

```

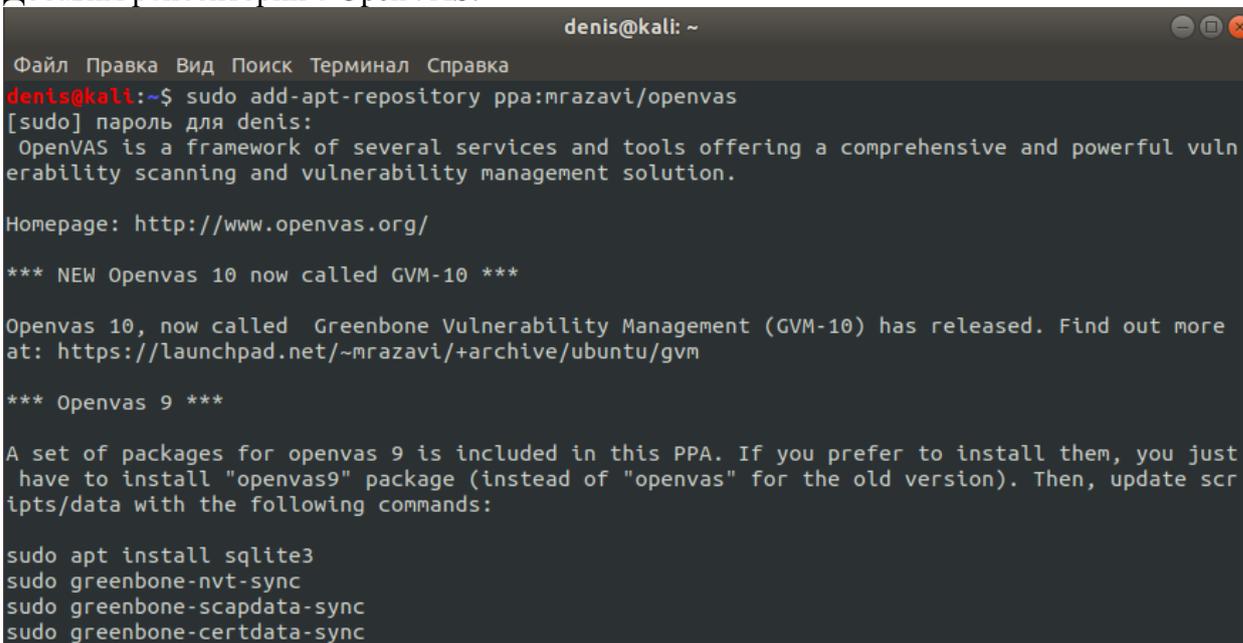
Настраивается пакет texlive-fonts-recommended (2020.20200925-1) ...
Настраивается пакет tipa (2:1.3-20) ...
Regenerating '/var/lib/texmf/fmtutil.cnf-DEBIAN'... done.
Regenerating '/var/lib/texmf/fmtutil.cnf-TEXLIVEDIST'... done.
update-fmtutil has updated the following file(s):
 /var/lib/texmf/fmtutil.cnf-DEBIAN
 /var/lib/texmf/fmtutil.cnf-TEXLIVEDIST
If you want to activate the changes in the above file(s),
you should run fmtutil-sys or fmtutil.
Настраивается пакет gvm-tools (2.0.0-2) ...
Настраивается пакет texlive-latex-extra (2020.20200925-1) ...
Настраивается пакет openvas-scanner (7.0.1-4+b1) ...
Настраивается пакет ospd-openvas (1.0.1-2) ...
ospd-openvas.service is a disabled or a static unit, not starting it.
Настраивается пакет gvm (11.0.5+kali1) ...
Настраивается пакет openvas (11.0.5+kali1) ...
Обрабатываются триггеры для fontconfig (2.13.1-4.2) ...
Обрабатываются триггеры для kali-menu (2020.4.0) ...
Обрабатываются триггеры для mime-support (3.64) ...
Обрабатываются триггеры для libc-bin (2.31-4) ...
Обрабатываются триггеры для systemd (246.6-2) ...
Обрабатываются триггеры для man-db (2.9.3-2) ...
Обрабатываются триггеры для install-info (6.7.0.dfsg.2-5) ...
Обрабатываются триггеры для tex-common (6.15) ...
Running updmap-sys. This may take some time... done.
Running mktexlsr /var/lib/texmf ... done.
Building format(s) --all.
This may take some time... done.
root@kali:~#

```

Запустим установочный пакет OpenVAS:

```
root@kali:~# openvas-setup
bash: openvas-setup: команда не найдена
root@kali:~#
```

Добавим репозиторий с OpenVAS:



```
denis@kali: ~
Файл Правка Вид Поиск Терминал Справка
denis@kali:~$ sudo add-apt-repository ppa:mrazavi/openvas
[sudo] пароль для denis:
OpenVAS is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution.

Homepage: http://www.openvas.org/

*** NEW Openvas 10 now called GVM-10 ***

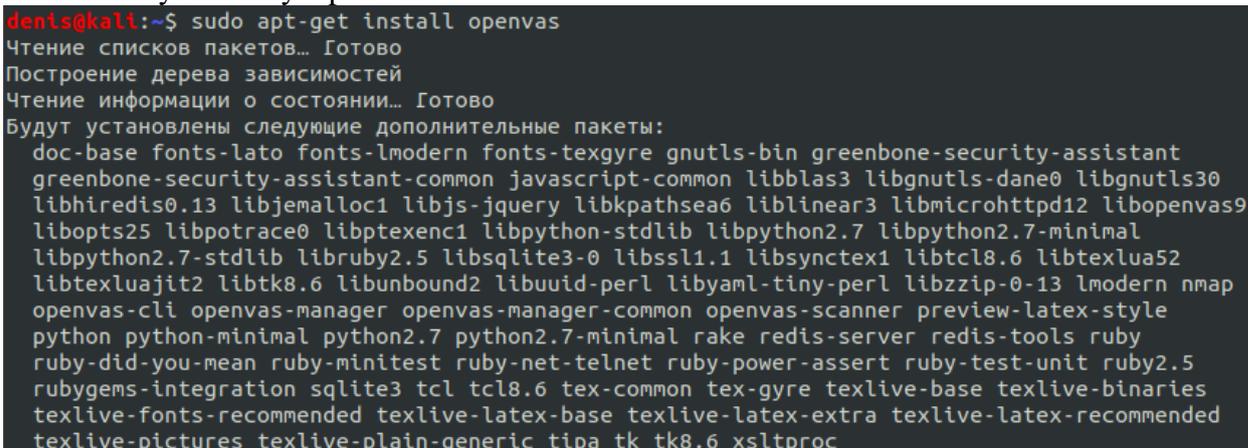
Openvas 10, now called Greenbone Vulnerability Management (GVM-10) has released. Find out more at: https://launchpad.net/~mrazavi/+archive/ubuntu/gvm

*** Openvas 9 ***

A set of packages for openvas 9 is included in this PPA. If you prefer to install them, you just have to install "openvas9" package (instead of "openvas" for the old version). Then, update scripts/data with the following commands:

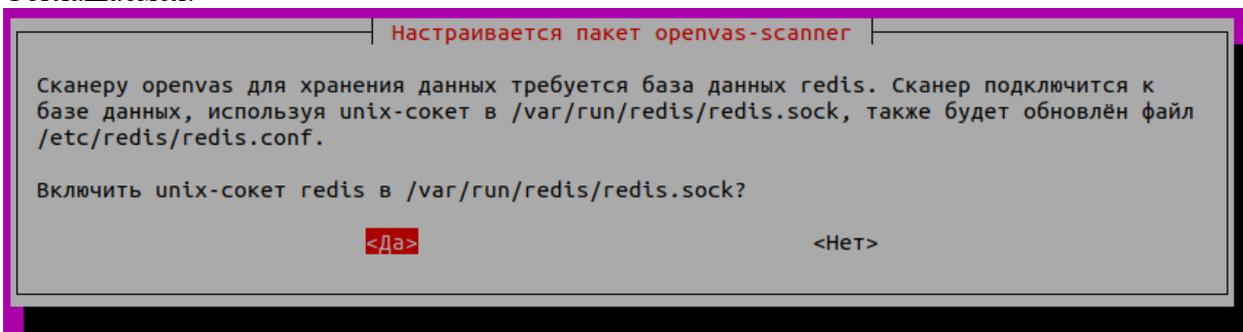
sudo apt install sqlite3
sudo greenbone-nvt-sync
sudo greenbone-scandata-sync
sudo greenbone-certdata-sync
```

Выполним установку OpenVAS:



```
denis@kali:~$ sudo apt-get install openvas
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Будут установлены следующие дополнительные пакеты:
 doc-base fonts-lato fonts-lmodern fonts-texgyre gnutls-bin greenbone-security-assistant
 greenbone-security-assistant-common javascript-common libblas3 libgnutls-dane0 libgnutls30
 libhiredis0.13 libjemalloc1 libjs-jquery libkpathsea6 liblinear3 libmicrohttpd12 libopenvas9
 libopts25 libpotrace0 libptexenc1 libpython-stdlib libpython2.7 libpython2.7-minimal
 libpython2.7-stdlib libruby2.5 libsqlite3-0 libssl1.1 libsyntax1 libtcl8.6 libtexlua52
 libtexluajit2 libtk8.6 libunbound2 libuuid-perl libyaml-tiny-perl libzip-0-13 lmodern nmap
 openvas-cli openvas-manager openvas-manager-common openvas-scanner preview-latex-style
 python python-minimal python2.7 python2.7-minimal rake redis-server redis-tools ruby
 ruby-did-you-mean ruby-minitest ruby-net-telnet ruby-power-assert ruby-test-unit ruby2.5
 rubygems-integration sqlite3 tcl tcl8.6 tex-common tex-gyre texlive-base texlive-binaries
 texlive-fonts-recommended texlive-latex-base texlive-latex-extra texlive-latex-recommended
 texlive-pictures texlive-plain-generic tipa tk tk8.6 xsltproc
```

Соглашаемся:



```
Настраивается пакет openvas-scanner

Сканеру openvas для хранения данных требуется база данных redis. Сканер подключится к
базе данных, используя unix-сокет в /var/run/redis/redis.sock, также будет обновлен файл
/etc/redis/redis.conf.

Включить unix-сокет redis в /var/run/redis/redis.sock?

<Да> <Нет>
```

```

denis@kali:~$ sudo apt-get install openvas9
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Следующие пакеты устанавливались автоматически и больше не требуются:
 doc-base fonts-lato fonts-texgyre greenbone-security-assistant
 greenbone-security-assistant-common javascript-common libjs-jquery libruby2.5 libuuid-perl
 libyaml-tiny-perl openvas-cli openvas-manager-common preview-latex-style rake ruby
 ruby-did-you-mean ruby-minitest ruby-net-telnet ruby-power-assert ruby-test-unit ruby2.5
 rubygems-integration tex-gyre texlive-fonts-recommended texlive-latex-extra
 texlive-latex-recommended texlive-pictures texlive-plain-generic tipa

```

Выполним обновление Security Контента:

```
sudo openvas-nvt-sync
```

```
sudo openvas-scapdata-sync
```

```
sudo openvas-certdata-sync
```

Установка завершилась успешно, но команды не сработали из-за того, что openvas – не известная команда

Так как на KaliLinux 2020 и KaliLinux 2019 не удалось установить OpenVAS, попробуем установить OpenVAS на Ubuntu 16.04 LTS

Шаг 1: Обновим систему и выполним перезагрузку:

```
# apt-get update -y
```

```
# apt-get upgrade -y
```

```
# sudo reboot
```

Шаг 2: Установим требуемые зависимости

Прежде, чем установить OpenVAS, мы должны будем установить его требуемые зависимости.

Чтобы установить их, выполним следующую команду:

```
# apt-get install python-software-properties
```

```

Ubuntu 2016 Nikonov [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Terminal File Edit View Search Terminal Help
denis@denis-VirtualBox:~$ sudo -s
[sudo] password for denis:
root@denis-VirtualBox:~# apt-get install python-software-properties
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
 libdbusmenu-gtk4 libpango1.0-0 libpangox-1.0-0 ubuntu-core-launcher
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
 python-apt python-pycurl
Suggested packages:
 python-apt-dbg python-apt-doc libcurl4-gnutls-dev python-pycurl-dbg python-pycurl-doc
The following NEW packages will be installed:
 python-apt python-pycurl python-software-properties
0 upgraded, 3 newly installed, 0 to remove and 55 not upgraded.
Need to get 211 kB of archives.
After this operation, 966 kB of additional disk space will be used.
Do you want to continue? [Y/n] y

```

Затем, установим SQLite для менеджера OpenVAS:

```
# apt-get install sqlite3
```

```

root@denis-VirtualBox:~# apt-get install sqlite3
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libdbusmenu-gtk4 libpango1.0-0 libpangox-1.0-0 ubuntu-core-launcher
Use 'sudo apt autoremove' to remove them.
Suggested packages:
  sqlite3-doc
The following NEW packages will be installed:
  sqlite3
0 upgraded, 1 newly installed, 0 to remove and 55 not upgraded.
Need to get 518 kB of archives.
After this operation, 1 939 kB of additional disk space will be used.
Get:1 http://ru.archive.ubuntu.com/ubuntu xenial-updates/main amd64 sqlite3 amd64 3.11.0-1ubuntu1
.5 [518 kB]
Fetched 518 kB in 0s (1 234 kB/s)
Selecting previously unselected package sqlite3.
(Reading database ... 173272 files and directories currently installed.)
Preparing to unpack .../sqlite3_3.11.0-1ubuntu1.5_amd64.deb ...
Unpacking sqlite3 (3.11.0-1ubuntu1.5) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up sqlite3 (3.11.0-1ubuntu1.5) ...
root@denis-VirtualBox:~#

```

Шаг 3: установка OpenVAS

По умолчанию пакет OpenVAS не доступен в репозитории Ubuntu 16.04, таким образом, мы должны будем добавить OpenVAS PPA к списку репозитория своей системы.

add-apt-repository ppa:mrazavi/openvas

```

root@denis-VirtualBox:~# add-apt-repository ppa:mrazavi/openvas
OpenVAS is a framework of several services and tools offering a comprehensive and powerful vulne
rability scanning and vulnerability management solution.

Homepage: http://www.openvas.org/

*** NEW Openvas 10 now called GVM-10 ***

Openvas 10, now called Greenbone Vulnerability Management (GVM-10) has released. Find out more a
t: https://launchpad.net/~mrazavi/+archive/ubuntu/gvm

*** Openvas 9 ***

A set of packages for openvas 9 is included in this PPA. If you prefer to install them, you just
have to install "openvas9" package (instead of "openvas" for the old version). Then, update scrip
ts/data with the following commands:

sudo apt install sqlite3
sudo greenbone-nvt-sync
sudo greenbone-scapdata-sync
sudo greenbone-certdata-sync

```

и обновим репозиторий:

apt-get update

```

root@denis-VirtualBox:~# apt-get update
Hit:1 http://ru.archive.ubuntu.com/ubuntu xenial InRelease
Hit:2 http://ru.archive.ubuntu.com/ubuntu xenial-updates InRelease
Hit:3 http://ru.archive.ubuntu.com/ubuntu xenial-backports InRelease
Get:4 http://ppa.launchpad.net/mrazavi/openvas/ubuntu xenial InRelease [17,5 kB]
Hit:5 http://security.ubuntu.com/ubuntu xenial-security InRelease
Get:6 http://ppa.launchpad.net/mrazavi/openvas/ubuntu xenial/main amd64 Packages [2 936 B]
Get:7 http://ppa.launchpad.net/mrazavi/openvas/ubuntu xenial/main i386 Packages [2 944 B]
Get:8 http://ppa.launchpad.net/mrazavi/openvas/ubuntu xenial/main Translation-en [1 044 B]
Fetched 24,5 kB in 0s (24,6 kB/s)
Reading package lists... Done
root@denis-VirtualBox:~# █

```

Наконец, установка OpenVAS.

apt-get install openvas

```

root@denis-VirtualBox:~# apt-get install openvas
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libdbusmenu-gtk4 libpango1.0-0 libpangox-1.0-0 ubuntu-core-launcher
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  fonts-lato fonts-lmodern javascript-common libblas-common libblas3 libhiredis0.13
  libjemalloc1 libjs-jquery liblinear3 libmicrohttpd10 libopenvas8 libpotrace0 libptexenc1
  libruby2.3 libsyntax1 libtexlua52 libtexluajit2 libzip-0-13 lmodern lua-lpeg ndiff nmap
  openvas-cli openvas-gsa openvas-manager openvas-scanner python-bs4 python-chardet
  python-html5lib python-lxml python-pkg-resources python-six rake redis-server redis-tools
  ruby ruby-did-you-mean ruby-minitest ruby-net-telnet ruby-power-assert ruby-test-unit ruby2.3
  rubygems-integration tex-common texlive-base texlive-binaries texlive-latex-base
  texlive-latex-base-doc xsltproc
Suggested packages:
  apache2 | lighttpd | httpd liblinear-tools liblinear-dev xmlstarlet python-genshi
  python-xml-dbg python-lxml-doc python-setuptools ruby-redis ri ruby-dev bundler debhelper
  perl-tk
The following NEW packages will be installed:
  fonts-lato fonts-lmodern javascript-common libblas-common libblas3 libhiredis0.13
  libjemalloc1 libjs-jquery liblinear3 libmicrohttpd10 libopenvas8 libpotrace0 libptexenc1
  libruby2.3 libsyntax1 libtexlua52 libtexluajit2 libzip-0-13 lmodern lua-lpeg ndiff nmap
  openvas openvas-cli openvas-gsa openvas-manager openvas-scanner python-bs4 python-chardet
  python-html5lib python-lxml python-pkg-resources python-six rake redis-server redis-tools
  ruby ruby-did-you-mean ruby-minitest ruby-net-telnet ruby-power-assert ruby-test-unit ruby2.3
  rubygems-integration tex-common texlive-base texlive-binaries texlive-latex-base
  texlive-latex-base-doc xsltproc
0 upgraded, 50 newly installed, 0 to remove and 55 not upgraded.
Need to get 102 MB of archives.
After this operation, 268 MB of additional disk space will be used.
Do you want to continue? [Y/n] █

```

Как только OpenVAS установился, запустим службу OpenVAS следующими командами:

```

root@denis-VirtualBox:~# systemctl start openvas-scanner
root@denis-VirtualBox:~# systemctl start openvas-manager
root@denis-VirtualBox:~# systemctl start openvas-gsa
root@denis-VirtualBox:~#

```

Шаг 4: Разрешим выполнение OpenVAS через системный брандмауэр

По умолчанию OpenVAS работает на порте 443, таким образом, мы должны будем позволить использовать этот порт через брандмауэр UFW.

```

root@denis-VirtualBox:~# ufw allow https
Rules updated
Rules updated (v6)
root@denis-VirtualBox:~#

```

Шаг 5: Доступ веб-интерфейс OpenVAS

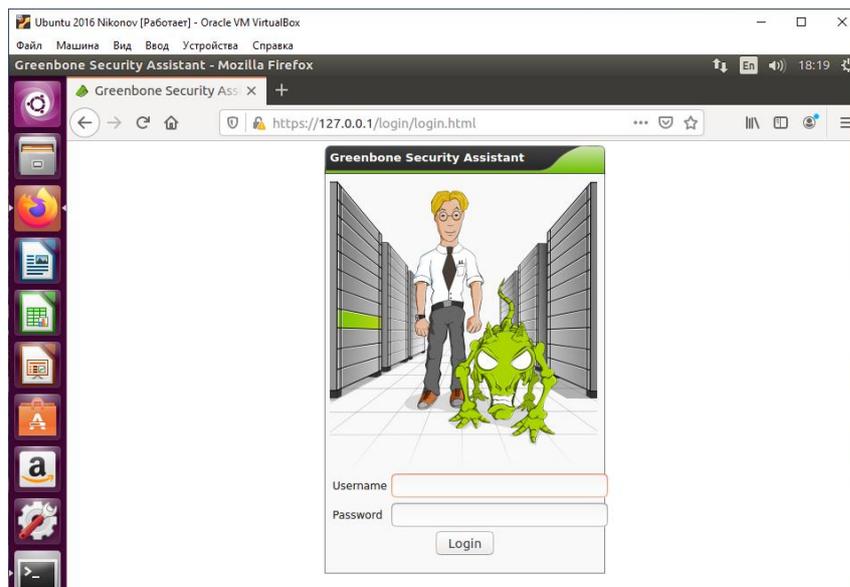
Прежде, чем получить доступ к OpenVAS, мы должны будем обновить его базу данных уязвимости.

```
# openvas-nvt-sync
```

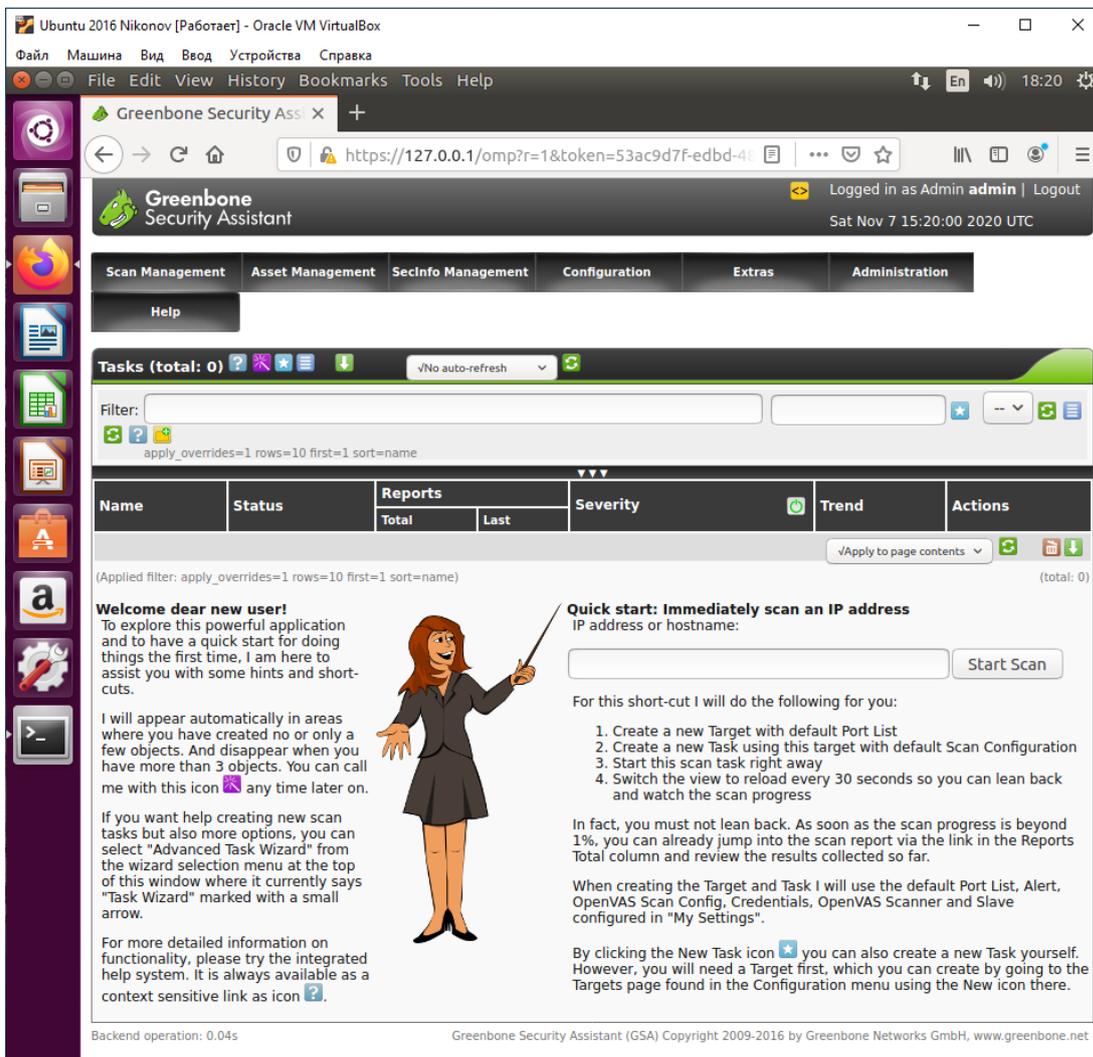
```
root@denis-VirtualBox:~# openvas-nvt-sync
[i] This script synchronizes an NVT collection with the 'OpenVAS NVT Feed'.
[i] The 'OpenVAS NVT Feed' is provided by 'The OpenVAS Project'.
[i] Online information about this feed: 'http://www.openvas.org/openvas-nvt-feed.html'.
[i] NVT dir: /var/lib/openvas/plugins
[w] Could not determine feed version.
[i] rsync is not recommended for the initial sync. Falling back on http.
[i] Will use wget
[i] Using GNU wget: /usr/bin/wget
[i] Configured NVT http feed: http://www.openvas.org/openvas-nvt-feed-current.tar.bz2
[i] Downloading to: /tmp/openvas-nvt-sync.n2EXm50qNs/openvas-feed-2020-11-07-7825.tar.bz2
--2020-11-07 18:18:02-- http://www.openvas.org/openvas-nvt-feed-current.tar.bz2
Resolving www.openvas.org (www.openvas.org)... 45.135.105.67, 2a0e:6b40:10::67
Connecting to www.openvas.org (www.openvas.org)|45.135.105.67|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.openvas.org/openvas-nvt-feed-current.tar.bz2 [following]
--2020-11-07 18:18:02-- https://www.openvas.org/openvas-nvt-feed-current.tar.bz2
Connecting to www.openvas.org (www.openvas.org)|45.135.105.67|:443... connected.
HTTP request sent, awaiting response... 404 Not Found
2020-11-07 18:18:03 ERROR 404: Not Found.

[i] Checking dir: ok
[i] Checking MD5 checksum: /usr/bin/md5sum: /var/lib/openvas/plugins/md5sums: No such file or dir
ectory
not ok
Error: md5sums not correct. Your NVT collection might be broken now.
Please try this for details: cd "/var/lib/openvas/plugins" ; /usr/bin/md5sum -c "/var/lib/openvas
/plugins/md5sums" | less
```

Как только база данных стала актуальна, откроем свой веб-браузер и введем URL <https://127.0.0.1/>.



На странице входа в систему введем имя пользователя по умолчанию (admin) и пароль (admin).



После входа в систему нам подарят инструментальную панель OpenVAS.

Для того, чтобы изменить административный пароль пользователя из командной строки, следует выполнить следующую команду:

```
# openvasmd - user=admin - новый пароль = &lt;новый пароль&gt;
```

1. Управление пользователями OpenVAS

Создадим дополнительного пользователя OpenVAS, запустим 'openvasmd' с параметром - create-user, который добавит нового пользователя и отобразит случайно сгенерированный пароль.

```
root@denis-VirtualBox:~# openvasmd --create-user=denis
User created with password '850ea62c-4950-42d8-926f-ecb46b57d24c'.
root@denis-VirtualBox:~#
```

```
root@denis-VirtualBox:~# openvasmd --get-users
admin
denis
root@denis-VirtualBox:~#
```

Изменение паролей пользователей OpenVAS легко осуществляется с помощью опции «openvasmd» и «new-password».


```
Nmap scan report for 127.0.1.243
Host is up.
Nmap scan report for 127.0.1.244
Host is up.
Nmap scan report for 127.0.1.245
Host is up.
Nmap scan report for 127.0.1.246
Host is up.
Nmap scan report for 127.0.1.247
Host is up.
Nmap scan report for 127.0.1.248
Host is up.
Nmap scan report for 127.0.1.249
Host is up.
Nmap scan report for 127.0.1.250
Host is up.
Nmap scan report for 127.0.1.251
Host is up.
Nmap scan report for 127.0.1.252
Host is up.
Nmap scan report for 127.0.1.253
Host is up.
Nmap scan report for 127.0.1.254
Host is up.
Nmap scan report for 127.0.1.255
Host is up.
Nmap done: 256 IP addresses (256 hosts up) scanned in 26.46 seconds
root@denis-VirtualBox:~#
```

```
root@denis-VirtualBox:~# grep Up nmap-subnet-0.gnmap | cut -d " " -f 2 > live-hosts.txt
root@denis-VirtualBox:~#
```

```
root@denis-VirtualBox:~# nmap -sn -oA nmap-subnet-2 10.0.2.1/24

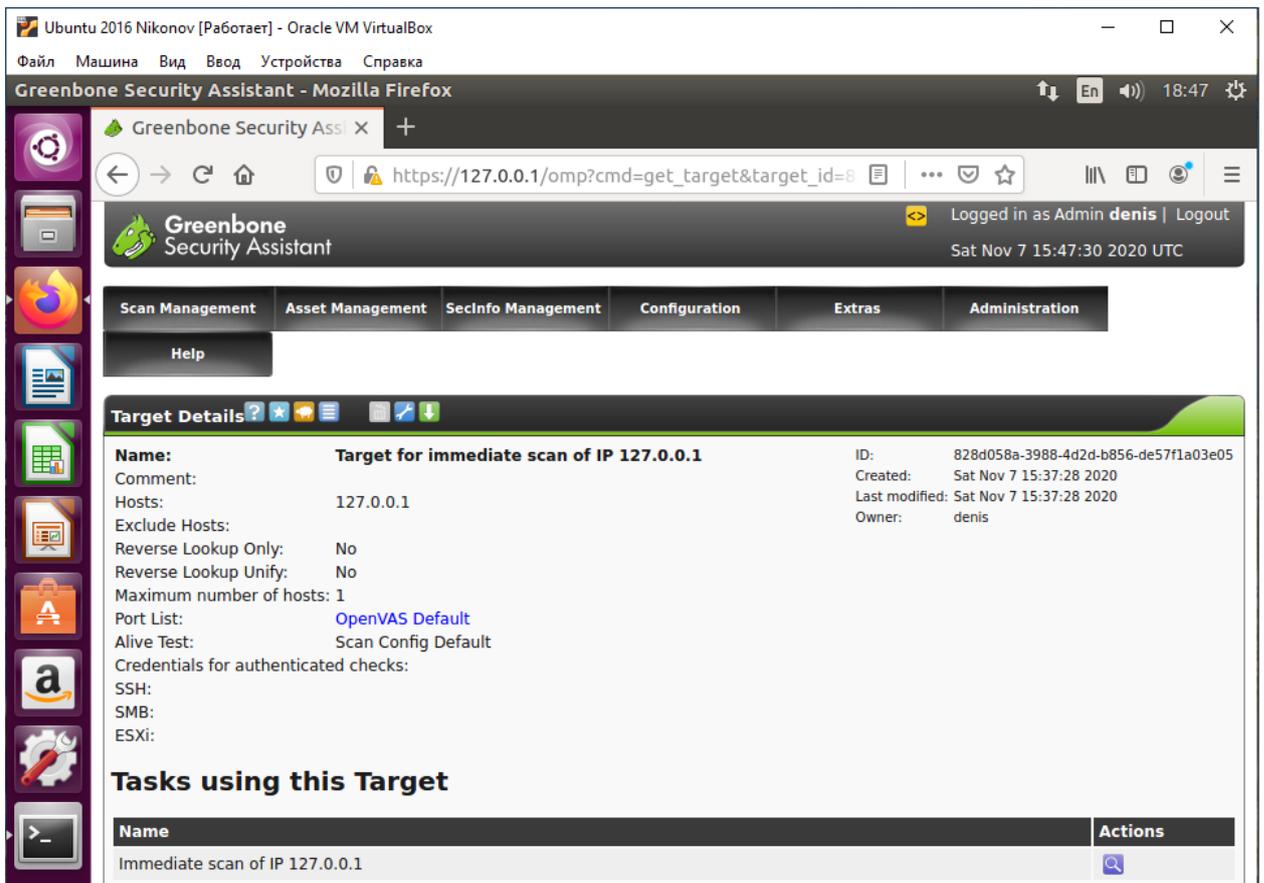
Starting Nmap 7.01 ( https://nmap.org ) at 2020-11-07 18:56 MSK
Nmap scan report for 10.0.2.2
Host is up (0.00053s latency).
MAC Address: 52:54:00:12:35:02 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00054s latency).
MAC Address: 52:54:00:12:35:03 (QEMU virtual NIC)
Nmap scan report for 10.0.2.4
Host is up (0.00052s latency).
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.03 seconds
root@denis-VirtualBox:~# grep Up nmap-subnet-0.gnmap | cut -d " " -f 2 > live-hosts.txt
root@denis-VirtualBox:~#
```

```
root@denis-VirtualBox:~# nmap -sn -oA nmap-subnet-100 192.168.100.1/24

Starting Nmap 7.01 ( https://nmap.org ) at 2020-11-07 19:09 MSK
```

```
root@denis-VirtualBox:~# grep Up nmap-subnet-100.gnmap | cut -d " " -f 2 > live-hosts100.txt
root@denis-VirtualBox:~# cat live-hosts100.txt
192.168.100.0
192.168.100.1
192.168.100.2
192.168.100.3
192.168.100.4
192.168.100.5
192.168.100.6
192.168.100.7
192.168.100.8
192.168.100.9
192.168.100.10
```

После того, как у нас есть список хостов, мы можем импортировать их в разделе «target» в меню «Configuration».



Ubuntu 2016 Nikonov [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security Assi X +

https://127.0.0.1/omp?cmd=new_target&next=get_

Greenbone Security Assistant

Logged in as Admin denis | Logout

Sat Nov 7 15:49:06 2020 UTC

Scan Management Asset Management Secinfo Management Configuration Extras Administration

Help

New Target

Name: 127.0.1.1

Comment (optional): Demo Link

Hosts:

- Manual localhost
- From file Browse... live-hosts.txt

Exclude Hosts:

Reverse Lookup Only: Yes No

Reverse Lookup Unify: Yes No

Port List: All IANA assigned TCP 2012-02-10

Alive Test: Scan Config Default

Credentials for authenticated checks (optional):

SSH: -- on port 22

SMB: --

ESXi: --

Create Target

Backend operation: 0.07s Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net

Ubuntu 2016 Nikonov [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security Assi X +

https://127.0.0.1/omp

Greenbone Security Assistant

Logged in as Admin denis | Logout

Sat Nov 7 15:50:04 2020 UTC

Scan Management Asset Management Secinfo Management Configuration Extras Administration

Help

Target Details

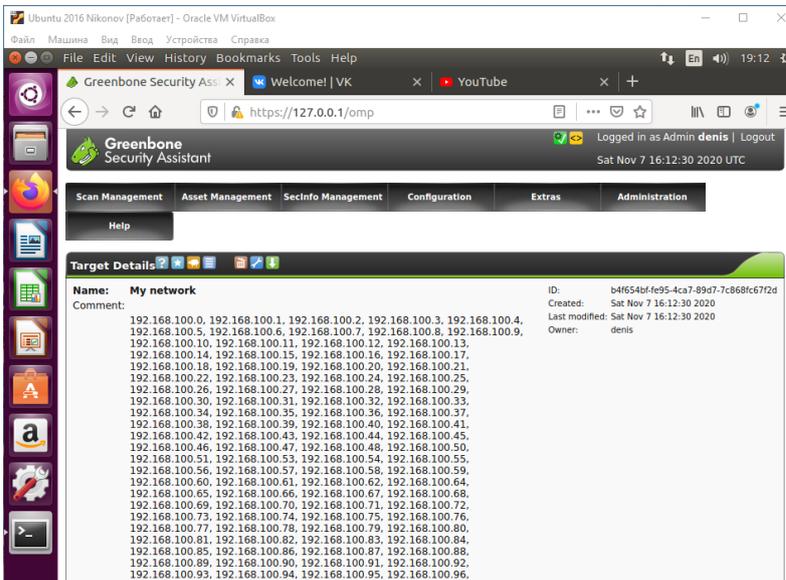
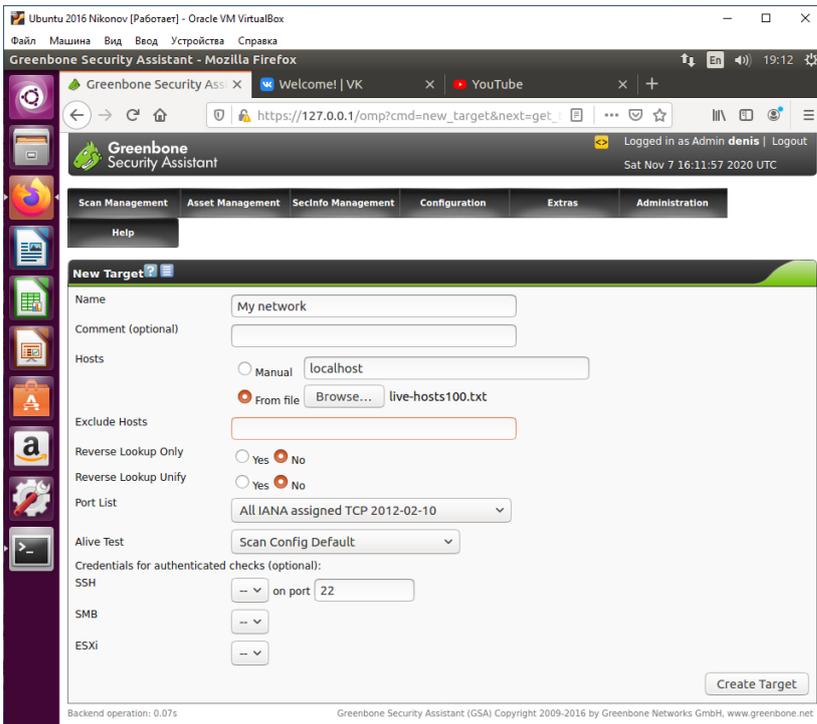
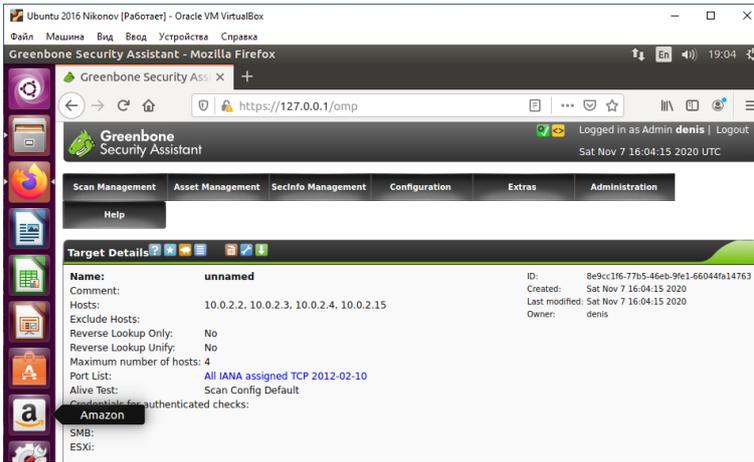
Name: 127.0.1.1 ID: a1b9c1bb-496e-407d-8bb3-06d3c05e885b

Comment: Demo Link Created: Sat Nov 7 15:50:04 2020

Owner: denis Last modified: Sat Nov 7 15:50:04 2020

Hosts:

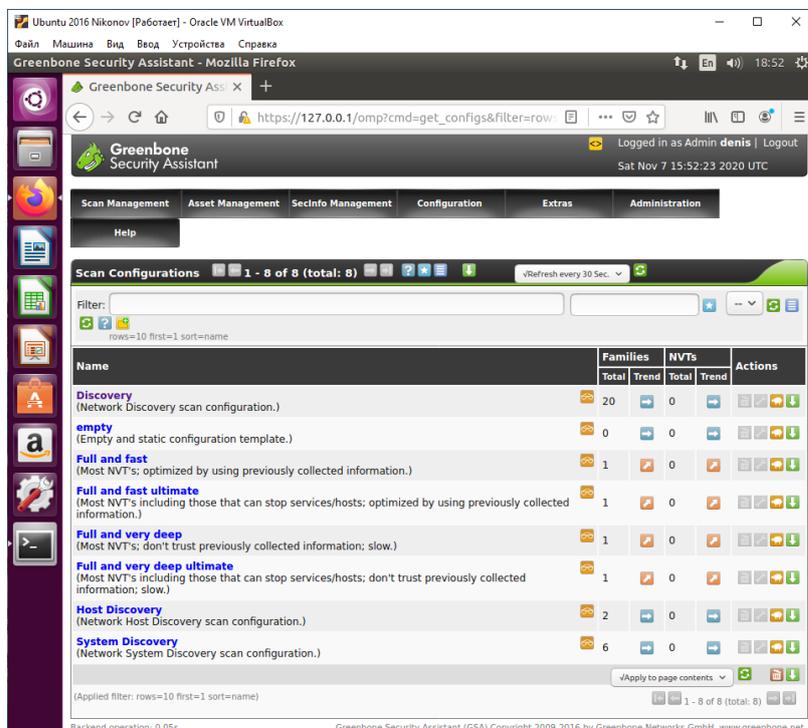
127.0.1.0, 127.0.1.1, 127.0.1.2, 127.0.1.3, 127.0.1.4, 127.0.1.5, 127.0.1.6, 127.0.1.7, 127.0.1.8, 127.0.1.9, 127.0.1.10, 127.0.1.11, 127.0.1.12, 127.0.1.13, 127.0.1.14, 127.0.1.15, 127.0.1.16, 127.0.1.17, 127.0.1.18, 127.0.1.19, 127.0.1.20, 127.0.1.21, 127.0.1.22, 127.0.1.23, 127.0.1.24, 127.0.1.25, 127.0.1.26, 127.0.1.27, 127.0.1.28, 127.0.1.29, 127.0.1.30, 127.0.1.31, 127.0.1.32, 127.0.1.33, 127.0.1.34, 127.0.1.35, 127.0.1.36, 127.0.1.37, 127.0.1.38, 127.0.1.39, 127.0.1.40, 127.0.1.41, 127.0.1.42, 127.0.1.43, 127.0.1.44, 127.0.1.45, 127.0.1.46, 127.0.1.47, 127.0.1.48, 127.0.1.49, 127.0.1.50, 127.0.1.51, 127.0.1.52, 127.0.1.53, 127.0.1.54, 127.0.1.55, 127.0.1.56, 127.0.1.57, 127.0.1.58, 127.0.1.59, 127.0.1.60, 127.0.1.61, 127.0.1.62, 127.0.1.63, 127.0.1.64, 127.0.1.65, 127.0.1.66, 127.0.1.67, 127.0.1.68, 127.0.1.69, 127.0.1.70, 127.0.1.71, 127.0.1.72, 127.0.1.73, 127.0.1.74, 127.0.1.75, 127.0.1.76, 127.0.1.77, 127.0.1.78, 127.0.1.79, 127.0.1.80, 127.0.1.81, 127.0.1.82, 127.0.1.83, 127.0.1.84, 127.0.1.85, 127.0.1.86, 127.0.1.87, 127.0.1.88, 127.0.1.89, 127.0.1.90, 127.0.1.91, 127.0.1.92, 127.0.1.93, 127.0.1.94, 127.0.1.95, 127.0.1.96, 127.0.1.97, 127.0.1.98, 127.0.1.99, 127.0.1.100, 127.0.1.101, 127.0.1.102, 127.0.1.103, 127.0.1.104, 127.0.1.105, 127.0.1.106, 127.0.1.107, 127.0.1.108, 127.0.1.109, 127.0.1.110, 127.0.1.111, 127.0.1.112, 127.0.1.113, 127.0.1.114, 127.0.1.115, 127.0.1.116, 127.0.1.117, 127.0.1.118, 127.0.1.119, 127.0.1.120, 127.0.1.121, 127.0.1.122, 127.0.1.123, 127.0.1.124, 127.0.1.125, 127.0.1.126, 127.0.1.127, 127.0.1.128, 127.0.1.129, 127.0.1.130, 127.0.1.131, 127.0.1.132, 127.0.1.133, 127.0.1.134, 127.0.1.135, 127.0.1.136, 127.0.1.137, 127.0.1.138, 127.0.1.139, 127.0.1.140, 127.0.1.141, 127.0.1.142, 127.0.1.143, 127.0.1.144, 127.0.1.145, 127.0.1.146, 127.0.1.147, 127.0.1.148, 127.0.1.149, 127.0.1.150, 127.0.1.151, 127.0.1.152, 127.0.1.153, 127.0.1.154, 127.0.1.155, 127.0.1.156, 127.0.1.157, 127.0.1.158, 127.0.1.159, 127.0.1.160, 127.0.1.161, 127.0.1.162, 127.0.1.163, 127.0.1.164, 127.0.1.165, 127.0.1.166, 127.0.1.167, 127.0.1.168, 127.0.1.169, 127.0.1.170, 127.0.1.171, 127.0.1.172, 127.0.1.173, 127.0.1.174, 127.0.1.175, 127.0.1.176, 127.0.1.177, 127.0.1.178, 127.0.1.179, 127.0.1.180, 127.0.1.181, 127.0.1.182, 127.0.1.183, 127.0.1.184, 127.0.1.185, 127.0.1.186, 127.0.1.187, 127.0.1.188, 127.0.1.189, 127.0.1.190, 127.0.1.191, 127.0.1.192, 127.0.1.193, 127.0.1.194, 127.0.1.195, 127.0.1.196, 127.0.1.197, 127.0.1.198, 127.0.1.199, 127.0.1.200, 127.0.1.201, 127.0.1.202, 127.0.1.203, 127.0.1.204, 127.0.1.205, 127.0.1.206, 127.0.1.207, 127.0.1.208, 127.0.1.209, 127.0.1.210, 127.0.1.211, 127.0.1.212, 127.0.1.213, 127.0.1.214, 127.0.1.215, 127.0.1.216, 127.0.1.217, 127.0.1.218, 127.0.1.219, 127.0.1.220, 127.0.1.221, 127.0.1.222, 127.0.1.223, 127.0.1.224, 127.0.1.225, 127.0.1.226, 127.0.1.227, 127.0.1.228, 127.0.1.229, 127.0.1.230, 127.0.1.231, 127.0.1.232, 127.0.1.233, 127.0.1.234, 127.0.1.235, 127.0.1.236, 127.0.1.237, 127.0.1.238, 127.0.1.239, 127.0.1.240, 127.0.1.241, 127.0.1.242, 127.0.1.243, 127.0.1.244, 127.0.1.245, 127.0.1.246, 127.0.1.247, 127.0.1.248, 127.0.1.249, 127.0.1.250, 127.0.1.251, 127.0.1.252, 127.0.1.253, 127.0.1.254, 127.0.1.255



3. Конфигурация сканирования

Перед запуском сканирования уязвимостей следует точно настроить Scan Config/, Это можно сделать в разделе “Scan Configs” в меню “Config”.

Мы будем клонировать любую конфигурацию сканирования по умолчанию и редактировать ее параметры, отключая любые службы или проверки, которые нам не нужны.

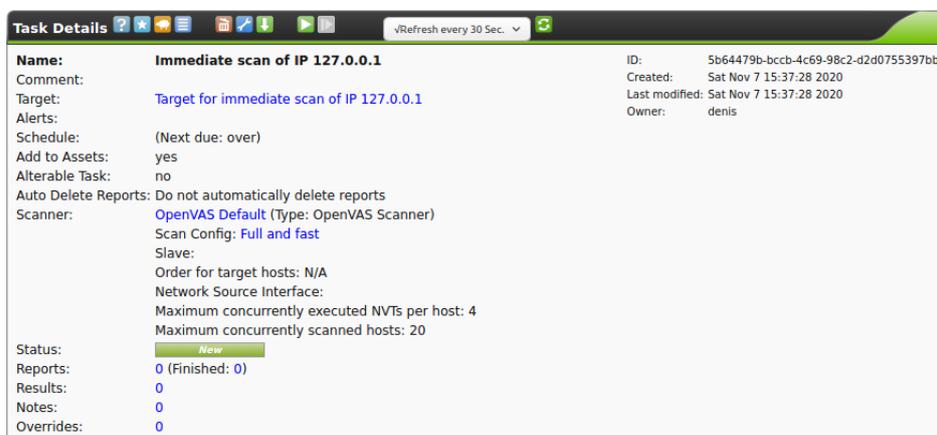


4. Конфигурация задачи

Наши учетные данные, цели и конфигурации сканирования настроены таким образом, что теперь можно запустить сканирование уязвимостей.

В OpenVAS сканирование уязвимостей проводится как «tasks».

Когда мы настраиваем новую задачу, мы можем дополнительно оптимизировать сканирование путем увеличения или уменьшения одновременных действий, которые происходят.



Task Details		Refresh every 30 Sec.	
Name:	Immediate scan of IP 10.0.2.15	ID:	ae29edf4-248d-4378-b18c-eb4dcf3ff8bd
Comment:		Created:	Sat Nov 7 15:57:08 2020
Target:	Target for immediate scan of IP 10.0.2.15	Last modified:	Sat Nov 7 15:57:08 2020
Alerts:		Owner:	denis
Schedule:	(Next due: over)		
Add to Assets:	yes		
Alterable Task:	no		
Auto Delete Reports:	Do not automatically delete reports		
Scanner:	OpenVAS Default (Type: OpenVAS Scanner)		
	Scan Config: Full and fast		
	Slave:		
	Order for target hosts: N/A		
	Network Source Interface:		
	Maximum concurrently executed NVTs per host: 4		
	Maximum concurrently scanned hosts: 20		
Status:	New		
Reports:	0 (Finished: 0)		
Results:	0		
Notes:	0		
Overrides:	0		

Благодаря нашим более точно настроенным параметрам сканирования и целевому выбору результаты нашего сканирования намного полезнее.

Практическая работа № 20 «Создание ролика из фотографий»

Инструкция для обучающихся

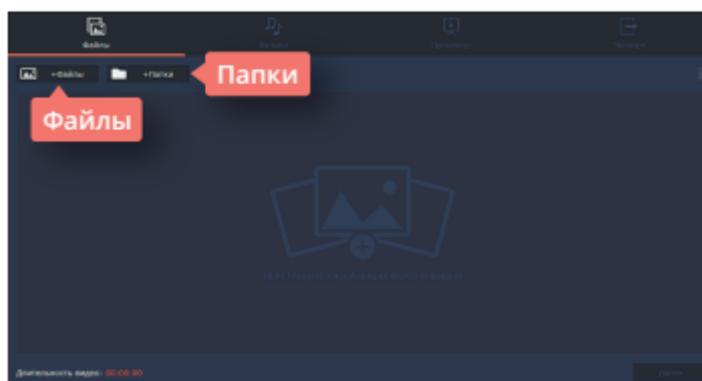
Внимательно прочитайте задание. Выполните необходимые операции.

Время выполнения – 90 минут.

Задание

1. Ролик из фотографий (Часть 1)

Откроем программу Movavi Видеоредактор, на этот раз в простом режиме - появится окно с названием «Мастер создания клипов». Активной будет первая вкладка «Файлы» с двумя кнопками: «Файлы» и «Папки».

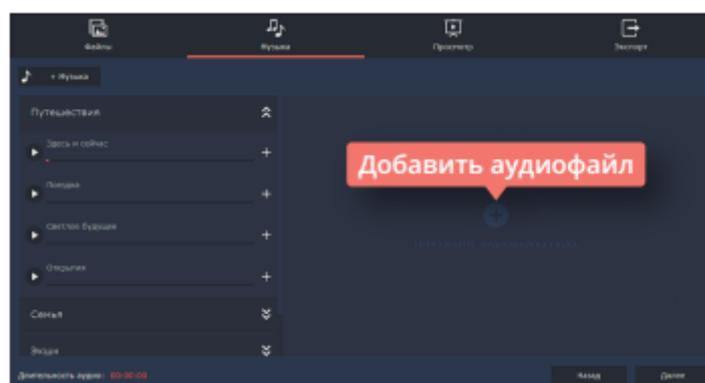


Если фотографий очень много, и выбрать для создания проекта нужно только некоторые, удобнее воспользоваться кнопкой «Файлы». Она пригодится и в том случае, если фотографии лежат в разных папках компьютера. При нажатии на кнопку программа откроет обычное окно поиска, с помощью которого можно найти все необходимые фотографии, выбрать сразу несколько или открыть их по одной. Если вы заранее выбрали файлы и поместили их в отдельную папку, то удобнее будет воспользоваться кнопкой «Папки», которая позволяет перемещать в окно проекта все файлы из папки одновременно.



Итак, выбор сделан, и необходимые фотографии появились в окне создания клипов. Теперь их состав и количество можно окончательно отредактировать. Лишние фотографии легко удалить, выделив фото и кликнув либо на крестик на самом фото, либо на изображение корзины в правом верхнем углу окна. Кстати, этот режим работы с видео очень упрощен, поэтому редактировать размеры или расположение фотографий в нем не получится. Не стоит открывать, например, фотографии, «перевернутые набок», лучше сразу подобрать файлы, оптимально подходящие для размещения.

Обратите внимание, как только первый файл появился в окне рабочего стола, сразу стали активными и остальные вкладки в верхней части окна. Перейдем к следующей вкладке «Музыка», она отвечает за аудио сопровождение ролика. В этой вкладке можно воспользоваться кнопкой «Музыка», открыть окно поисковика и добавить к ролику заранее подобранную мелодию. Однако быстрее, проще и удобнее воспользоваться библиотекой программы.



Movavi Видеоредактор предлагает выбор из мелодий на популярные темы: «Путешествия», «Семья», «Экшн» или «Романтика». Эти музыкальные треки достаточно короткие, яркие и ритмичные, они отлично подойдут в качестве музыкального сопровождения к ролику из фотографий. Чтобы добавить необходимый аудиофайл, нужно кликнуть по знаку «+» в правой части файла. При выборе музыкального сопровождения учтите общее настроение фотографий. Видео будет смотреться гармонично, если фото и музыка хорошо сочетаются друг с другом: фотографиям из путешествия подойдет мажорный настрой, а осенним фотографиям природы - лиричный лад.

Дальше выбираем вкладку «Просмотр». Умный мастер создания видео предложит самостоятельно его подкорректировать, обрезав фото под длительность музыки. Имейте в виду, что, если фотографий много, а музыкальное сопровождение короткое, программа просто уберет из видео часть фотографий, а не сократит время размещения фотографии в кадре. Но можно и самостоятельно задать необходимое количество минут и секунд для длительности видео. Сделать это можно, передвигая бегунок на линии, расположенной

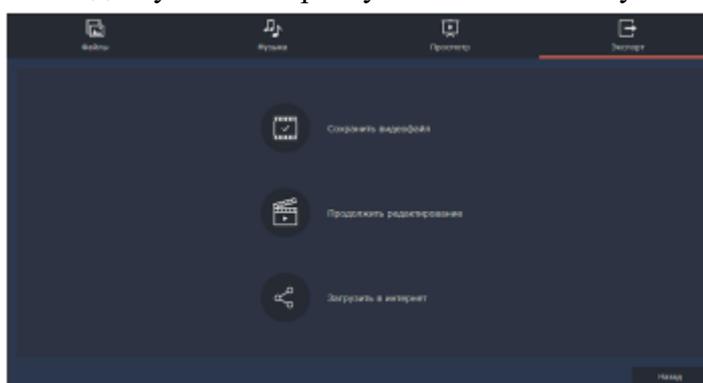
под текстом об умном мастере создания видео. В этой вкладке можно отрегулировать и баланс громкости, также передвигая соответствующий бегунок.



К каждой фотографии программа добавит дополнительные настройки, такие как «Приближение», «Отдаление» или «Панорама», однако переходы между кадрами останутся в виде простой склейки.

Хотите узнать, каким получится ролик? Перед оцифровкой можно посмотреть его от начала до конца в окне предпросмотра.

Вкладка «Экспорт» позволит сохранить ролик (если вы не умеете это делать правильно, можно прочитать предыдущий урок) или вернуться к его редактированию. Программа также предоставляет возможность выложить готовое видео сразу на YouTube, с условием наличия открытого доступа к Интернету и активного аккаунта.



2. Ролик из фотографий (Часть 2)

Одна из самых актуальных проблем при создании ролика из фотографий - вертикальные фото. Фотографии в таком формате встречаются достаточно часто, иногда они просто красивые, и их хочется вставить, иногда их по какой-то причине необходимо показать. Если оставить вертикальную фотографию как есть, то задний фон будет черным, а это смотрится не очень красиво. Для того, чтобы не искать фон для каждой фотографии отдельно, или не вставлять один фон для всего видео ряда (он может не подходить к некоторым фотографиям), можно воспользоваться фильтрами. В фильтрах нужно выбрать вкладку «Коррекция» и фильтр с названием «Заполнение краев».

Зажмите его правой кнопкой мыши и перетащите на вертикальную фотографию, расположенную на монтажном столе. Программа автоматически создаст размытый задний фон из основных цветов фотографии.

Обратите внимание, что в этом режиме программы можно работать с перестановкой фотографий, так что можно легко подобрать для каждой нужное место.

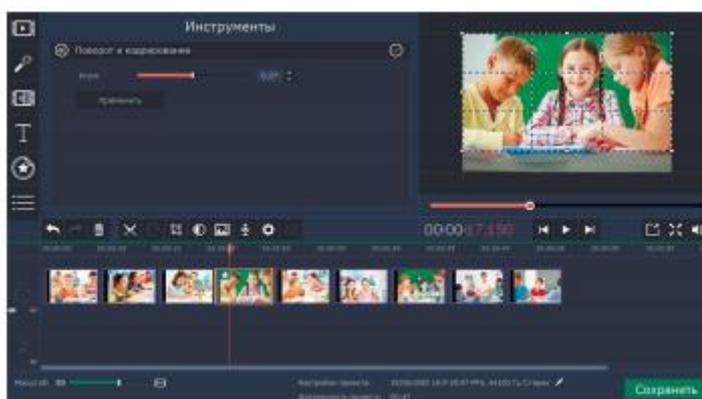
Можно редактировать и длительность одного кадра. Определитесь, сколько времени вам необходимо на ролик. Можно добавить аудиофайл на монтажный стол (из компьютера или библиотеки программы) и ориентироваться на его продолжительность.

При создании видеоролика из фотографий для красоты можно использовать переходы. Если выделить на дорожке один кадр, в верхней части тайм-линии станет активной кнопка с изображением картинки. Если нажать на нее, программа откроет окно «Мастер переходов». Здесь можно задать один переход для всего ролика или дать программе автоматически подобрать разные переходы к каждому снимку.



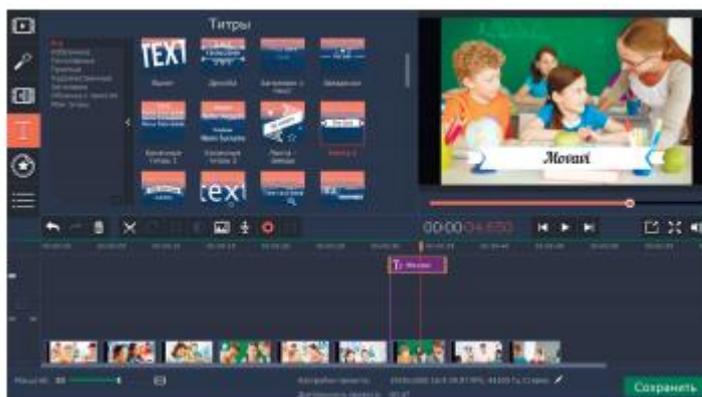
А еще можно задать длительность переходов и продолжительность самих фотографий в кадре. Если вы хотите вручную задать переходы для каждой фотографии, откройте вкладку «Переходы» и разместите их, перетаскивая на нужные файлы.

Если фотография горизонтальная, но все-таки не подходит полностью под видео формат, можно применить к ней кадрирование. Кликните по фотографии два раза, программа откроет в верхнем окне вкладку «Инструменты». Во вкладке выберите «Поворот и кадрирование».



Программа откроет рамку в окне предпросмотра, с ее помощью, уменьшая или увеличивая кадр, можно подобрать оптимальный вариант размещения фотографии. Кроме того, с помощью строки «Угол», можно исправить «заваленный горизонт». Нажмите кнопку «Применить», чтобы программа приняла новые параметры для фотографии.

Программа Movavi Видеоредактор позволяет добавлять на видео титры и различные надписи. Давайте добавим название к началу ролика. Перейдите во вкладку «Титры» и выберите подходящий вариант: простой или художественный. Зажмите его левой кнопкой мыши и перетащите на монтажный стол. Кликните по титрам дважды. В окне предпросмотра программа предоставит возможность менять текст титров, оставляя выбранный стиль. Добавьте необходимый текст и нажмите кнопку «Применить».



Программа позволяет размещать на видео не только титры, но и различные картинки и стикеры. При создании видеоряда из фотографий, этой функцией как раз можно воспользоваться, она позволит сделать ролик более интересным и ярким. Перейдите к вкладке «Стикерсы». Выберите строку «Смайлы» или «Школьное». Нажмите левой кнопкой мыши необходимую картинку и перетащите ее на монтажный стол. Программа разместит дополнительную картинку над основной и расположит ее как титры. Если кликнуть по смайлу, в окне предпросмотра программа откроет возможность его редактировать. Картинку можно увеличить или уменьшить, переместить в кадре и поставить на нужное место, задать длительность. После выбора всех параметров нажмите кнопку «Применить», чтобы программа запомнила заданное.

В библиотеке программы есть также вкладка «Фигуры». С ее помощью в кадр можно поместить различные геометрические фигуры, сделать подложки под надписи или добавить стрелки. При желании они могут послужить дополнительной анимацией в кадре. Кроме того, во вкладке «Титры» есть строка «Облачка с текстом», которая поможет рассказать о мыслях героя и сделать из фоторяда настоящую историю.

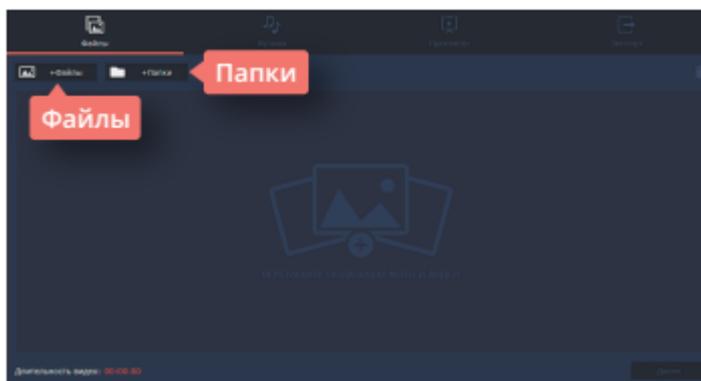
При создании ролика можно воспользоваться собственными картинками. Чтобы их было легко поместить поверх видео, они должны быть сделаны на прозрачном фоне. Таким образом можно поместить на видео, например, логотип.

Вставьте скриншот полученных результатов.

Эталон ответа:

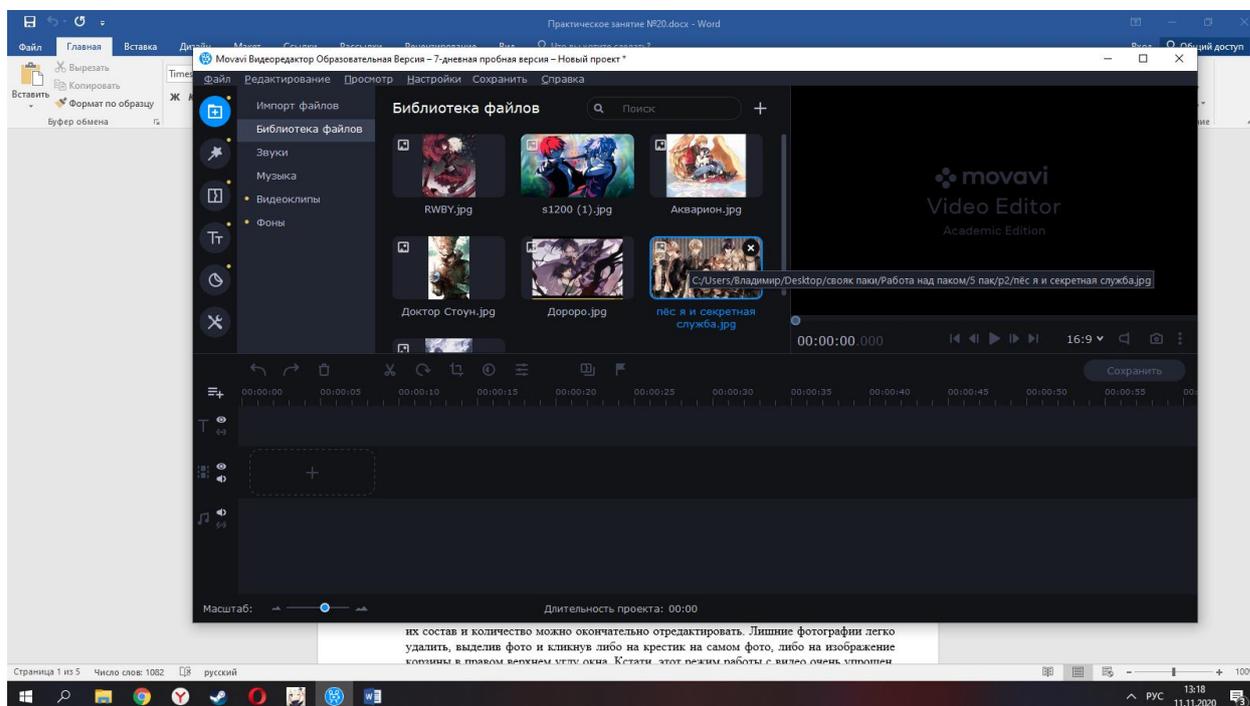
1. Ролик из фотографий (Часть 1)

Откроем программу Movavi Видеоредактор, появится окно с названием «Мастер создания клипов». Активна первая вкладка «Файлы» с двумя кнопками: «Файлы» и «Папки».

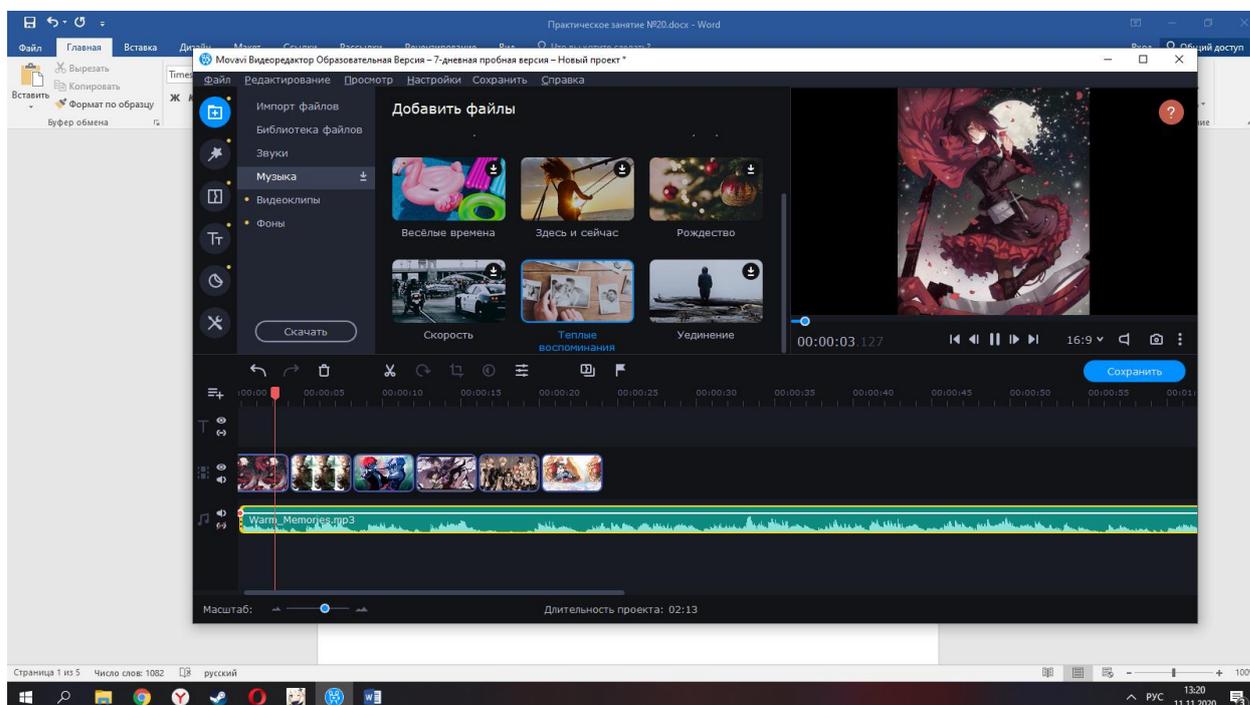


Если фотографий очень много, и выбрать для создания проекта нужно только некоторые, удобнее воспользоваться кнопкой «Файлы». Она пригодится и в том случае, если фото-

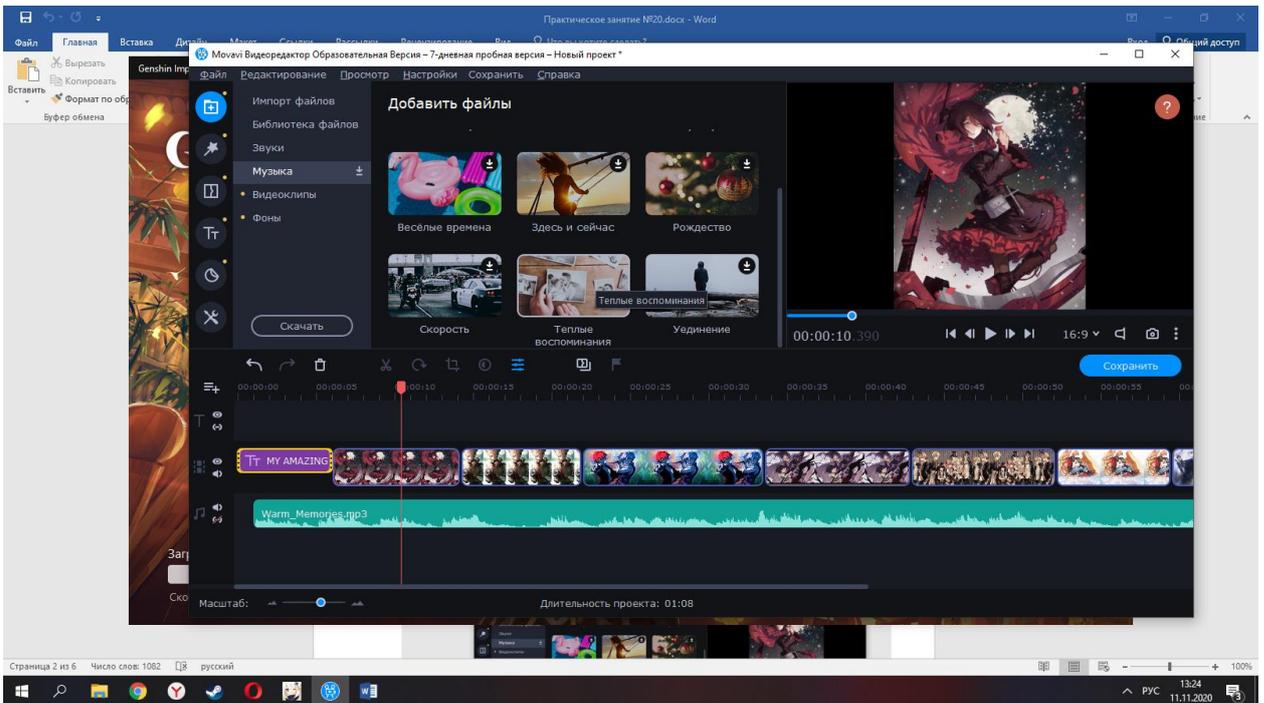
графии лежат в разных папках компьютера. При нажатии на кнопку программа откроет обычное окно поиска, с помощью которого можно найти все необходимые фотографии, выбрать сразу несколько или открыть их по одной.



Итак, выбор сделан, и необходимые фотографии появились в окне создания клипов. Теперь их состав и количество можно окончательно отредактировать.

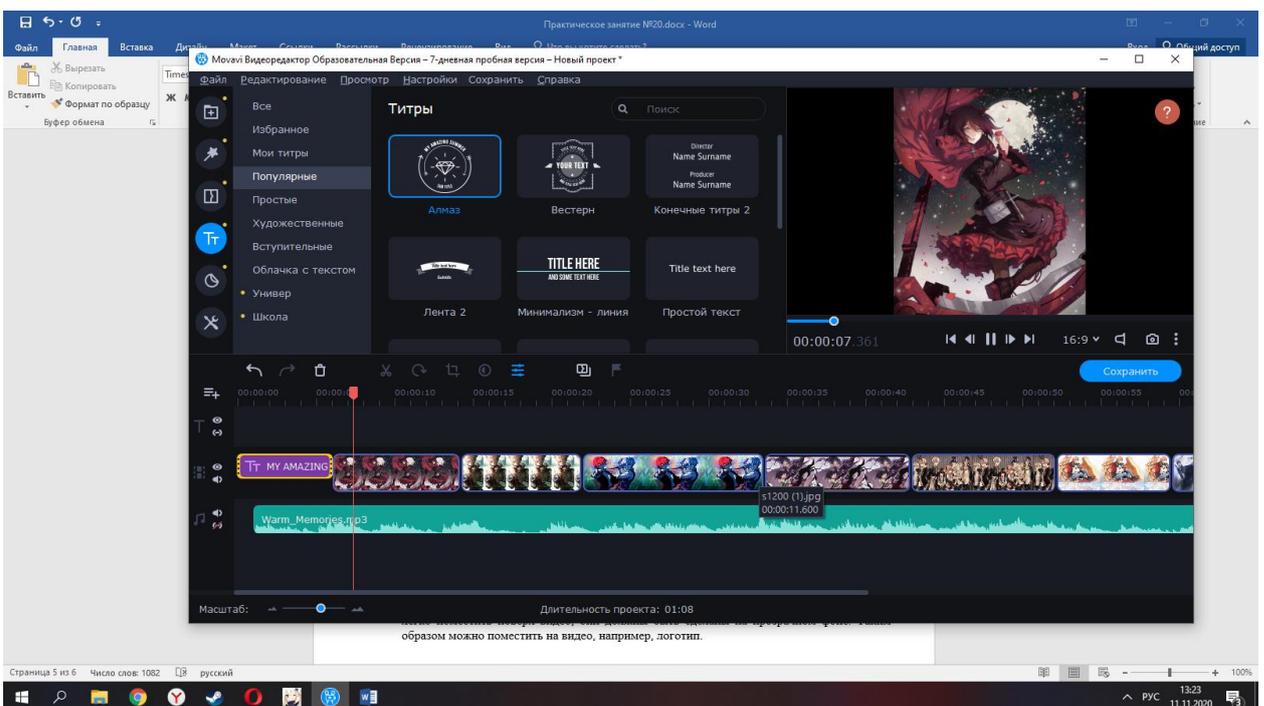


К каждой фотографии программа добавила дополнительные настройки, такие как «Приближение», «Отдаление» или «Панорама», однако переходы между кадрами остались в виде простой склейки.



2. Ролик из фотографий (Часть 2)

Одна из самых актуальных проблем при создании ролика из фотографий - вертикальные фото. Фотографии в таком формате встречаются достаточно часто, иногда они просто красивые, и их хочется вставить, иногда их по какой-то причине необходимо показать. Если оставить вертикальную фотографию как есть, то задний фон будет черным, а это смотрится не очень красиво. Для того, чтобы не искать фон для каждой фотографии отдельно, или не вставлять один фон для всего видео ряда (он может не подходить к некоторым фотографиям), можно воспользоваться фильтрами. В фильтрах выбираем вкладку «Коррекция» и фильтр с названием «Заполнение краев».



4. Устный зачет по теме 2.4.

Инструкция для обучающихся

Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 2 вопроса.

Выполнение задания: одному студенту на ответ выделяется 3 мин., группа сдает зачет за одно учебное занятие.

Перечень вопросов:

1. Назовите области применения цифрового видео?
2. Назовите источники видеосигнала?
3. Что такое анимация?
4. Что такое мультипликация?
5. Назовите основные форматы видеоданных?
6. Назовите основные характеристики видеосигнала?
7. Что такое потоковое видео?
8. Дайте определение ширине (скорости) видеопотока?
9. Назовите основные цветовые модели?
10. Что такое чересстрочная развёртка?

4. Практическое занятие № 13 Запись звука с микрофона. Резка аудиофайлов и удаление ненужных моментов.

Инструкция для обучающихся

Внимательно прочитайте задание. Выполните необходимые операции.

Время выполнения – 90 минут.

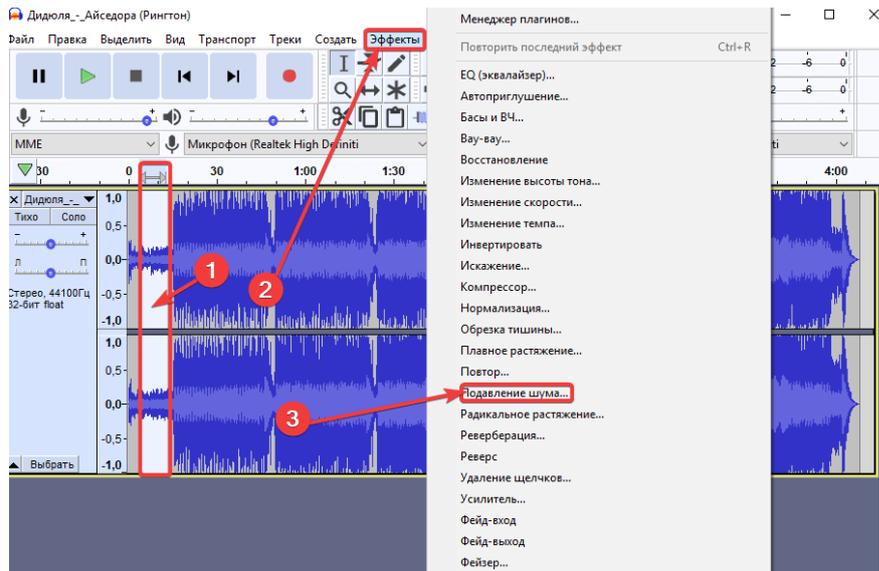
Задание

1. Удаление шума

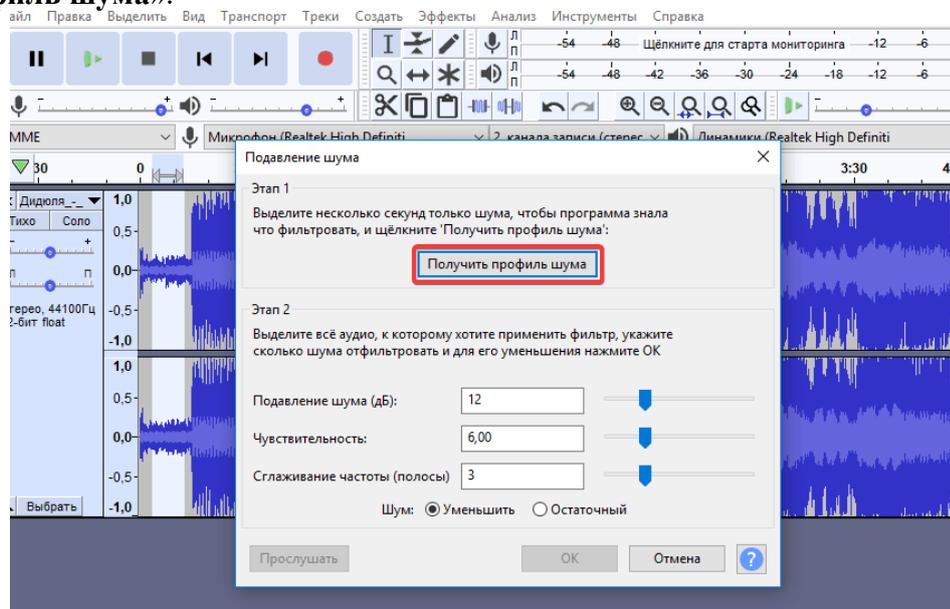
Удаление шума обычно требуется для треков, записанных с микрофона или записей, оцифрованных со старых пленок.

Как вырезать шум с записи

1. Выделить участок трека, где присутствует только шум, без музыки и голоса.
2. Нажать на вкладку «**Эффекты**».
3. В выпадающем меню выбрать пункт «**Подавление шума**».

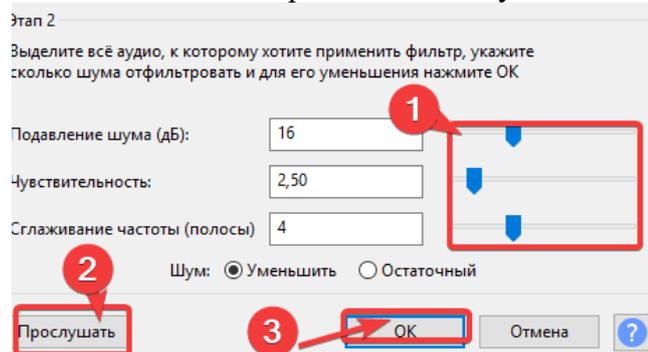


Следующий шаг – генерация модели шума. Это поможет редактору определить, какие звуки следует оставлять, а от каких избавляться. Для этого кликаем мышкой на «**Получить профиль шума**».



Снова выделите весь трек и опять нажмите на «**Эффекты**» и «**Подавление шума**».

- В заключении выполните следующие действия:
- В открывшемся окне с помощью перемещения ползунков и кнопки добейтесь желаемого качества записи
 - Результат можно узнать, нажав на «**Прослушать**».
 - Для сохранения окончательного варианта используйте «**ОК**».



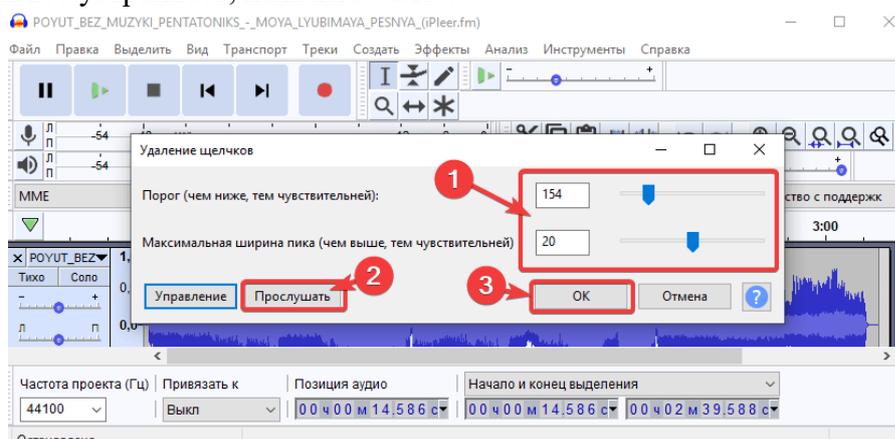
Таким же образом можно убрать фрагменты трека с плохо записанным голосом, например, писком.

Как удалить голос

- Выделите мышкой участок неудачной записи.
- Сгенерируйте модель шума.
- Выделите весь трек.
- Корректируйте качество с помощью бегунков и нажмите «Ок».

Как удалить помехи

Кроме шума можно удалить щелчки и треск. Для этого тоже выделите весь трек, потом откройте раздел «Эффекты» и выберите «Удаление щелчков». В появившемся окне также, как и при удалении шума, отрегулируйте чувствительность ползунками, прослушайте и, если все устраивает, нажмите «Ок».



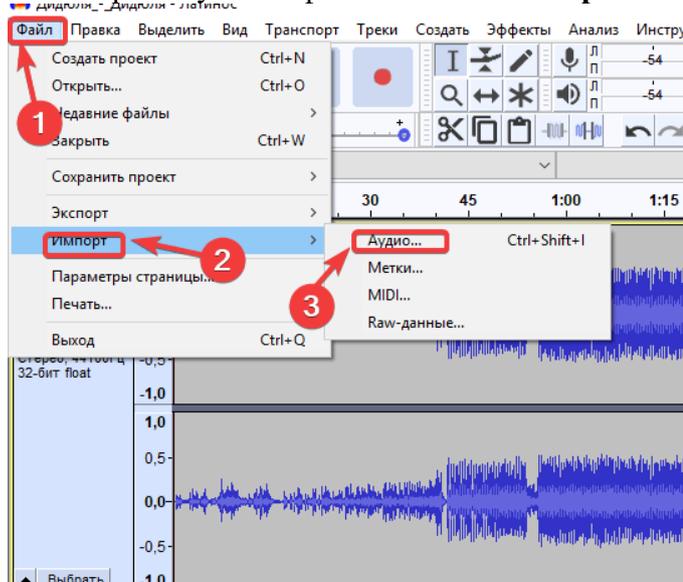
Как наложить голос

Наложение голоса поверх музыки может понадобиться, в случае если у вас есть минусовка и отдельно запись голоса. Вначале загрузите трек в редактор. Для этого повторите действия из раздела «Обрезка».

Теперь нужно добавить голос, не создавая при этом новый проект:

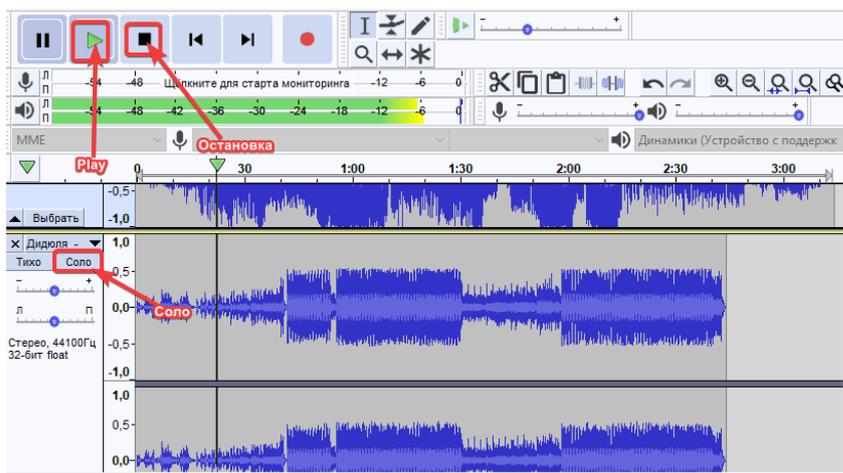
1. Нажмите на пункт в меню «Файл»
2. В выпадающем списке выберите «Импорт».
3. В следующем разделе кликните на «Аудио».

Осталось указать путь и выбрать нужный файл и нажать «Открыть».



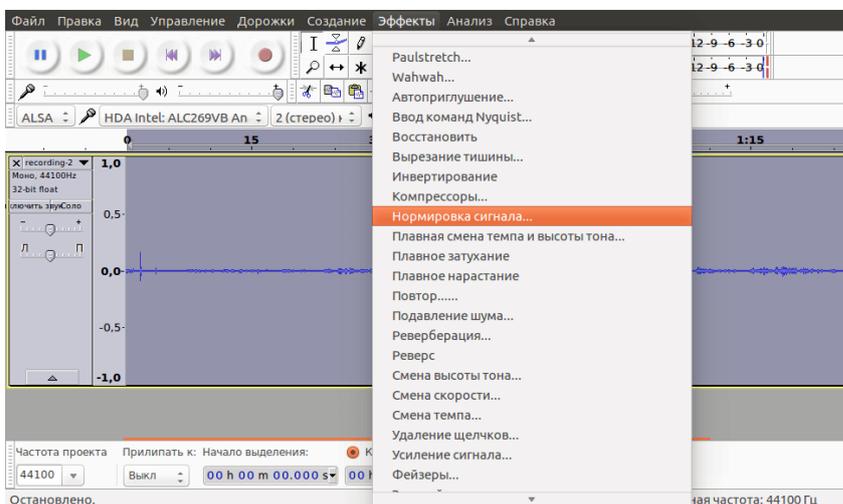
Кроме этого, можно просто перетащить мышкой нужные файлы в рабочую область программы.

Треки можно прослушать, нажав на «Play». Чтобы проиграть каждую мелодию отдельно, необходимо остановить режим воспроизведения, включить режим «Соло» и щелкнуть курсором по дорожке с нужным треком.

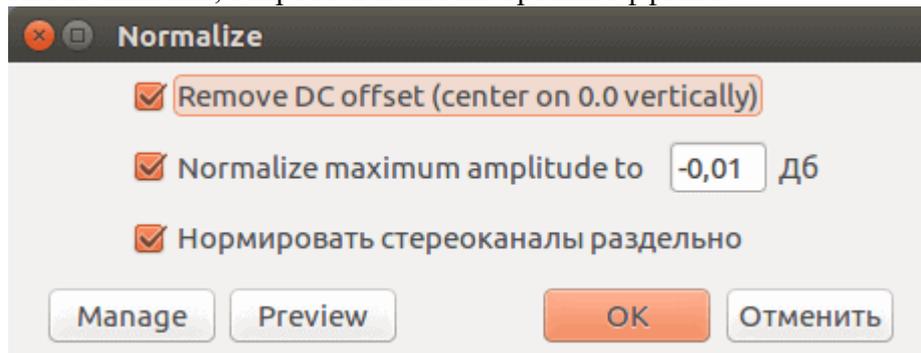


Усиление сигнала.

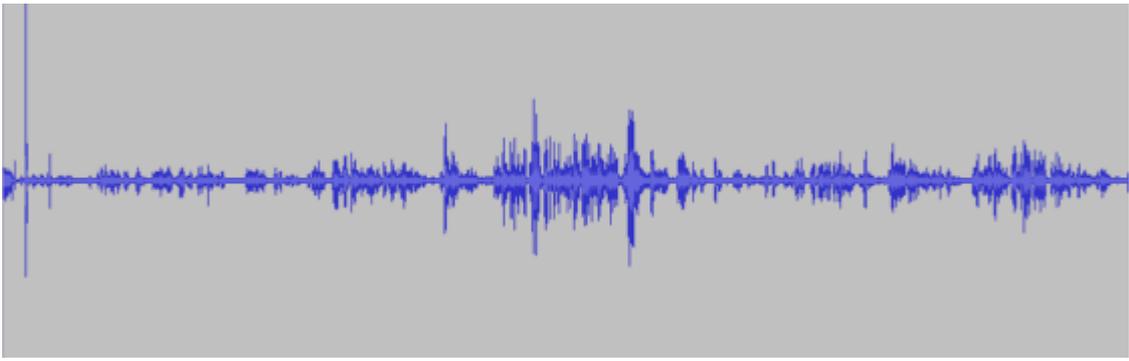
Чтобы повысить качество звука, первым делом необходимо увеличить громкость записи. Для этого двойным щелчком левой кнопки мыши по дорожке (либо комбинацией **Ctrl+a**) выделяем ее. Затем открываем вкладку меню **Эффекты** и выбираем пункт **Нормировка сигнала...**



После нажатия, откроется меню настройки эффекта:

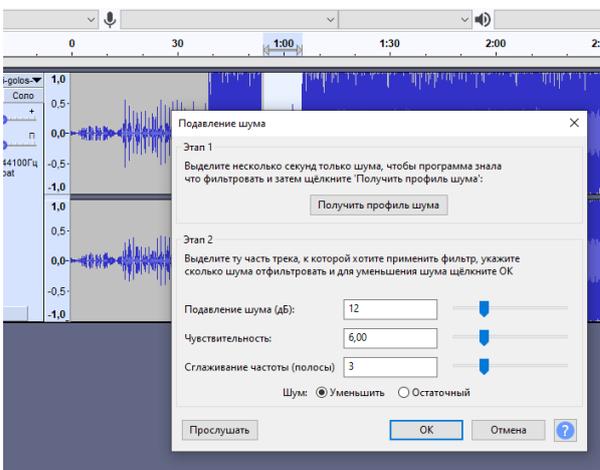
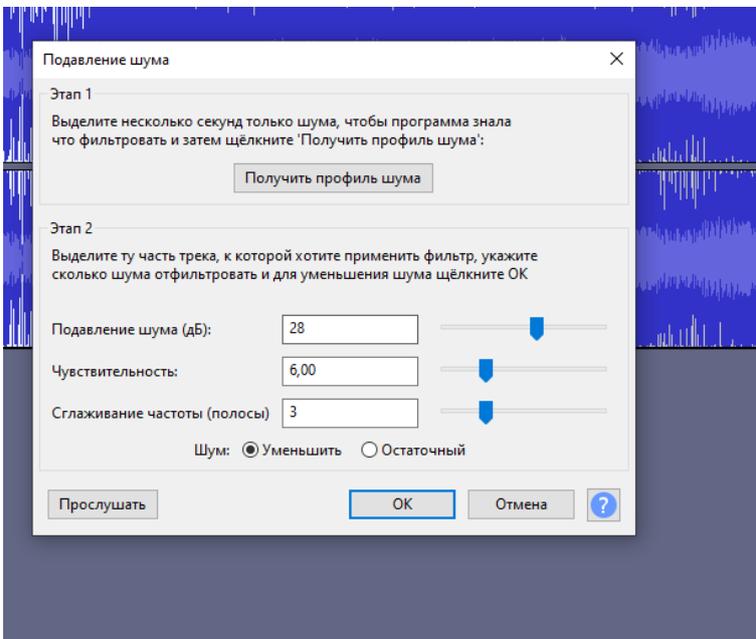


Стандартные настройки нас вполне устроят. В окошке указывается значение громкости, которое будет у самого громкого пика вашей записи. Нормировка повысит уровень громкости записи, никак больше не влияя на запись.

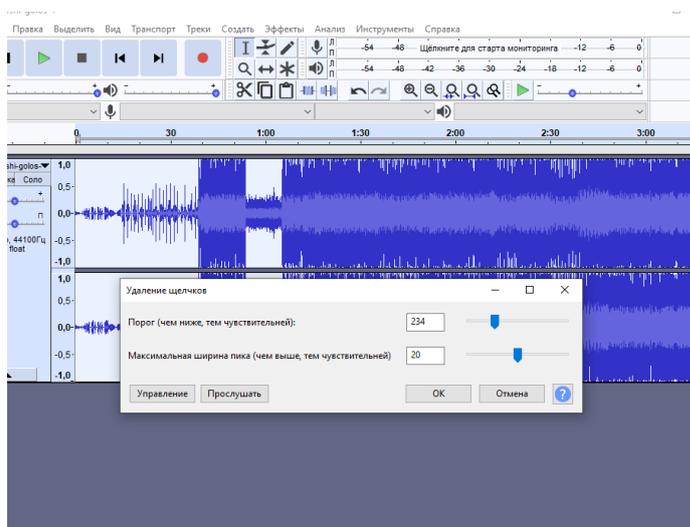


Эталон ответа

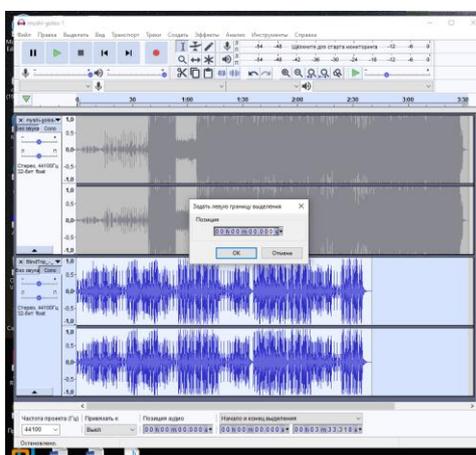
Удаление шума



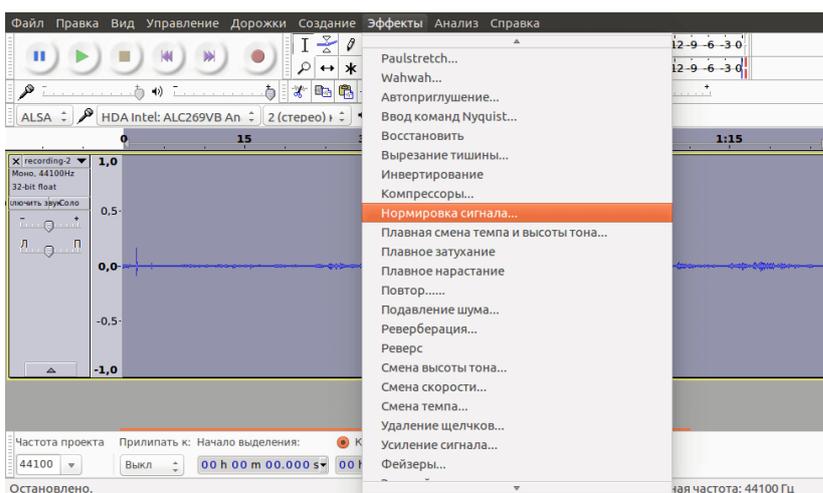
Удаление помех



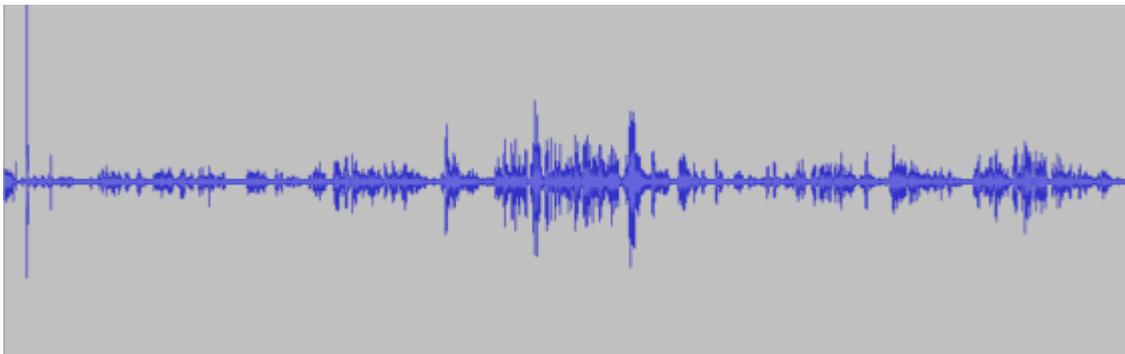
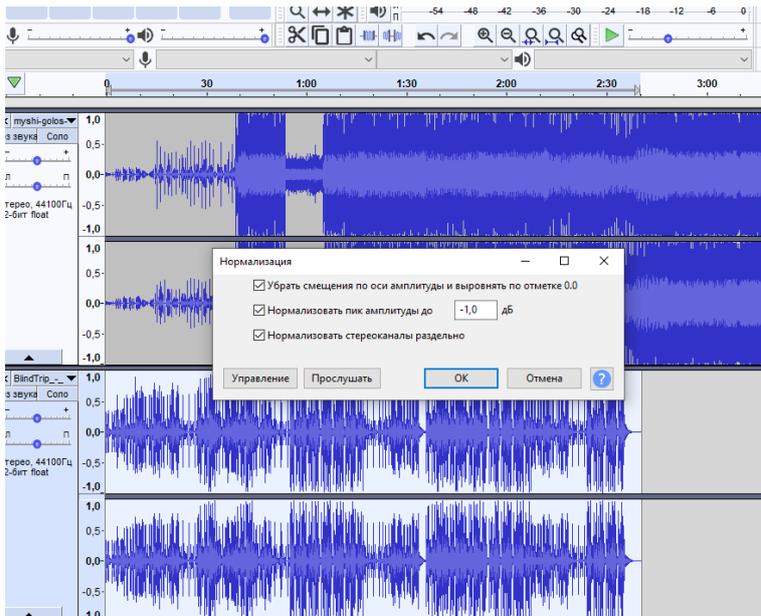
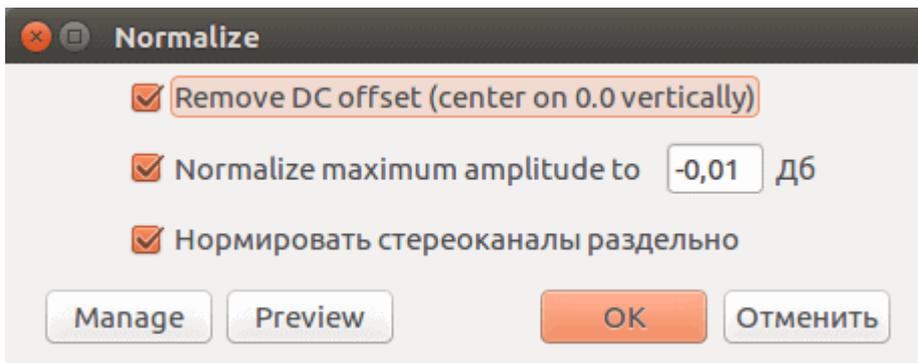
Наложение голоса



Усиление сигнала.



После нажатия, откроется меню настройки эффекта:



Практическая работа № 2 «Работа со слоями»

Инструкция для обучающихся

Внимательно прочитайте задание. Проведите обследование объектов на предмет состояния инженерно-технического укрепления.

Время выполнения – 90 минут.

Задание

1. Черно-белое изображение.

Рассмотрим выделение цветом на фотографии *единичного объекта с несложными краями*, у которой нет особо завышенных требований по качеству к заключительному результату.

- Выберите в меню **Файл – Открыть**. Загрузите в GIMP изображение, с которым намерены работать.
- Для примера оставим цветным только красный шарик на картинке, а остальную часть изображения обесцветим.
- Возьмите инструмент **Свободное выделение (Лассо)** и с его помощью обведите на фото объект, который желаете оставить цветным, расставляя контрольные точки вдоль его границы. Замкните контур, кликнув по первоначальной точке выделения.



Рис. 62

Чем чаще вы расставите контрольные точки вдоль границы объекта, тем качественнее будет выделение. Для удобства работы с инструментом Лассо, *зажмите клавишу Ctrl и покрутите колёсико мыши в нужную сторону*, увеличивая изображение в рабочей области фоторедактора.

- Выберите в меню **Выделение – Инvertировать**. В результате этого, выделенной станет остальная часть изображения вне границы элемента, который вы замыслили сделать цветовым акцентом.
- Через меню **Выделение – Растушевать** сделайте растушёвку границ выделенного объекта. Ширину размывания можно оставить по умолчанию. Нажмите ОК.

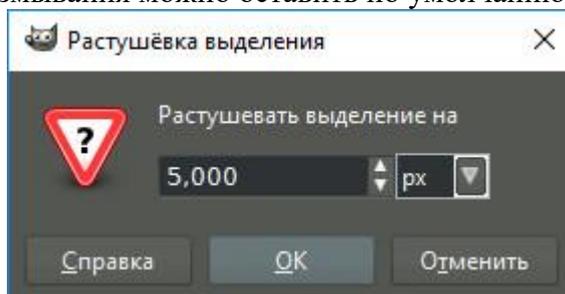


Рис. 63

- В меню **Цвет** выберите команду **Обесцвечивание**. В диалоговом окне инструмента переключитесь на пункт **Светимость**. Нажмите ОК.

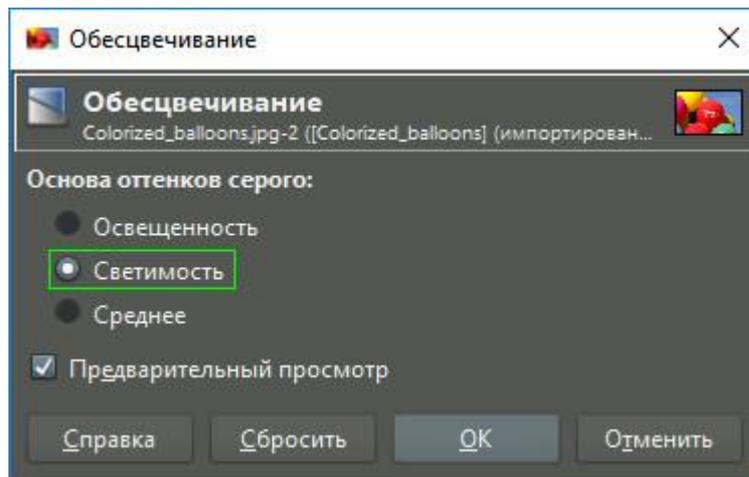


Рис. 64

- Кликните в меню **Выделение – Снять выделение** и оцените готовый результат. **Готовое чёрно-белое фото с красным элементом:**

Вставьте скриншот результата.

- Сохраните получившийся результат в формате .jpg

2. Рамка для фото.

Рассмотрим, как можно добавить рамку к изображению в GIMP.

- Выберите в меню **Файл – Открыть**. Загрузите в GIMP изображение, с которым намерены работать. Загрузите в GIMP изображение, которое получилось в работе «Чёрно-белое фото».
- Выберите в меню **Фильтры – Декорация – Добавить рамку**.

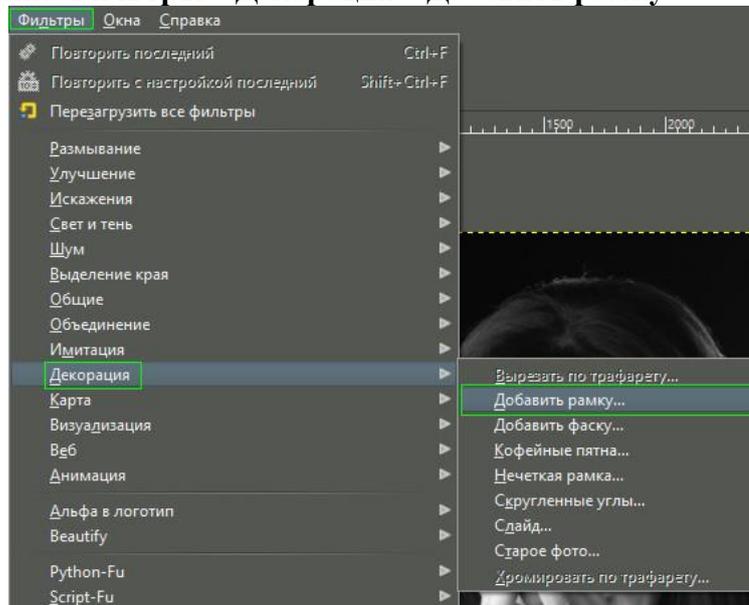


Рис. 65

- В диалоговом окне фильтра задайте следующие параметры:

- Ширина горизонтальной планки – **50 px**;
- Ширина вертикальной планки – **50 px**;

- Цвет рамки – **Белый**;
- Рельефность рамки – **1 px**.

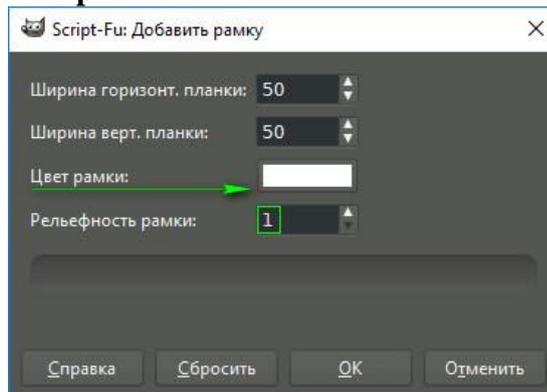


Рис. 66

Чтобы изменить цвет рамки на белый, кликните по кнопке, указанной на верхнем скриншоте стрелкой. В открывшейся палитре в строке HTML-разметка введите код **FFFFFF**. Нажмите **ОК**.

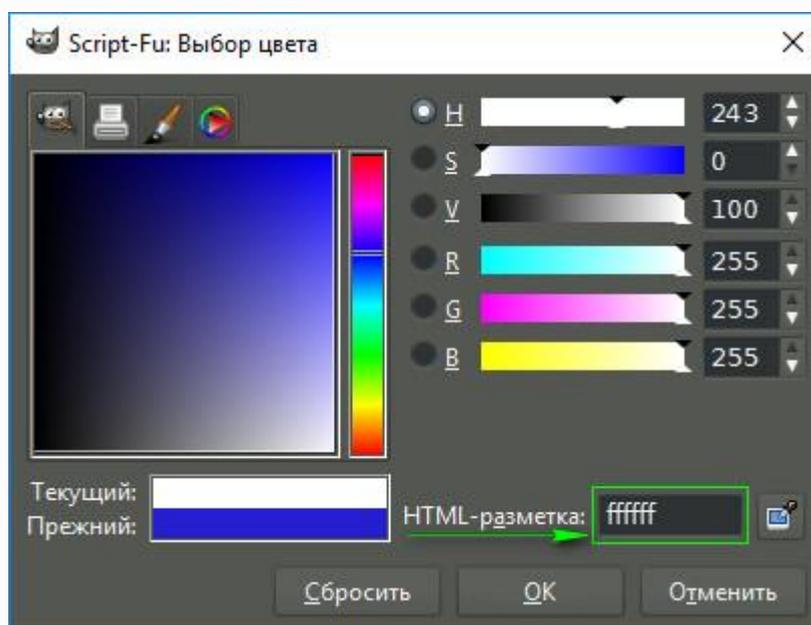


Рис. 67

- В диалоговом окне **Слои** сделайте клик правой клавишей мыши по слою **Border Layer** и выберите **Объединить с предыдущим**.

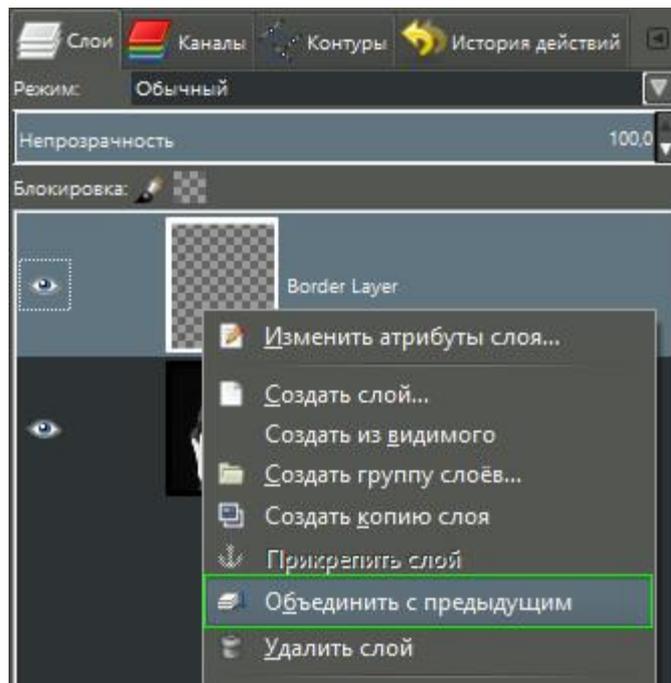


Рис. 68

- Сохраните получившийся результат в формате .jrg

3. Наложение слоев. Режимы смешивания.

Рассмотрим режимы наложения двух слоев друг на друга.

- Выберите в меню **Файл – Открыть**. Загрузите в GIMP изображение, которое получилось в первой работе «Правка горизонта».
- В диалоговом окне **Слой** добавьте новый прозрачный слой.

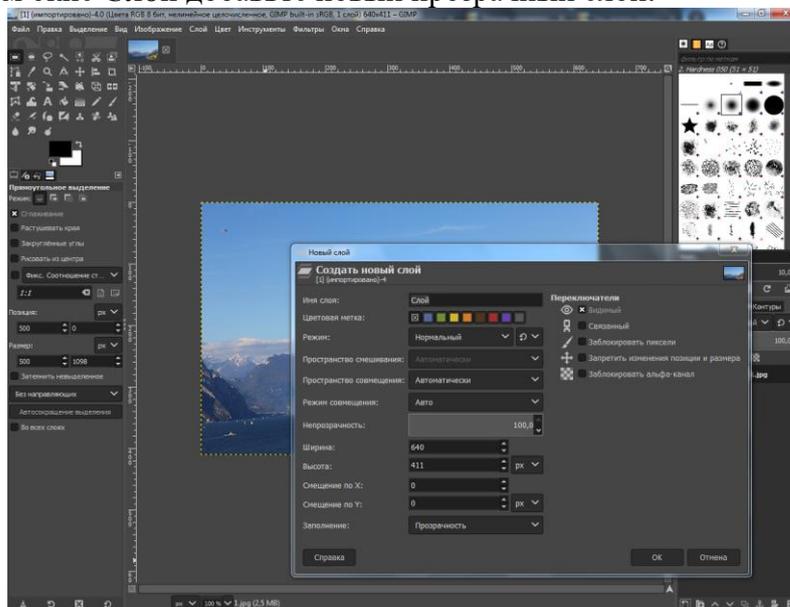


Рис. 69

- Создадим на новом слое 4 вертикальные направляющие линии. Размер данной картины по ширине 640, следовательно, каждая направляющая располагается через 160px. Для этого выбираем инструмент **Прямоугольное выделение** и строим прямоугольник с позиции 160 и размером 160.

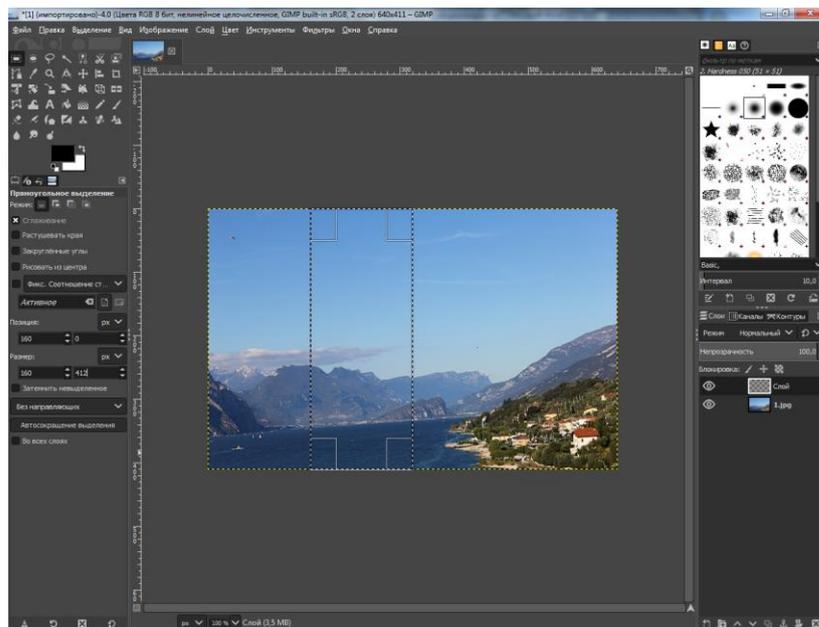


Рис. 70

- Выберите в меню **Изображение – Направляющие – Создать из выделенного**

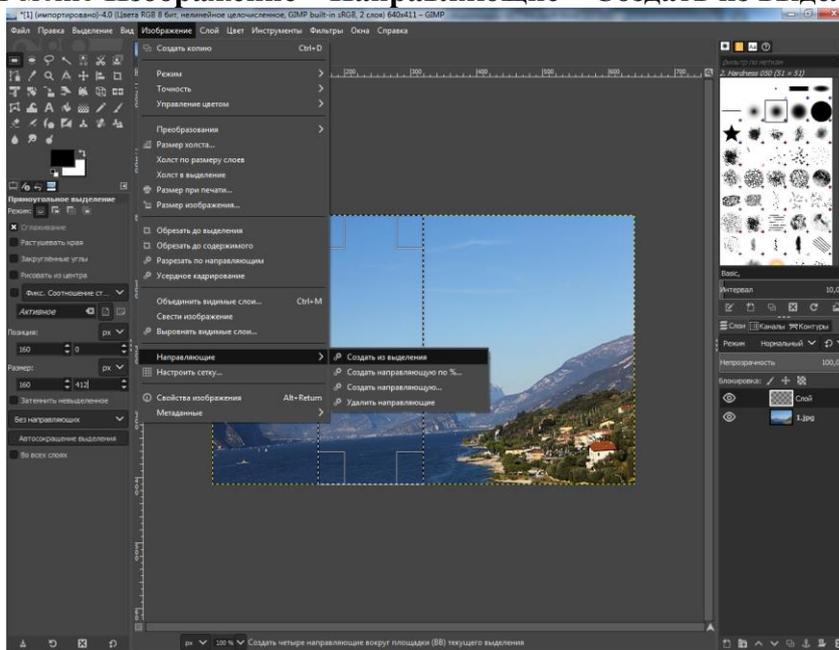


Рис. 71

- Аналогичным образом создаем последнюю направляющую.

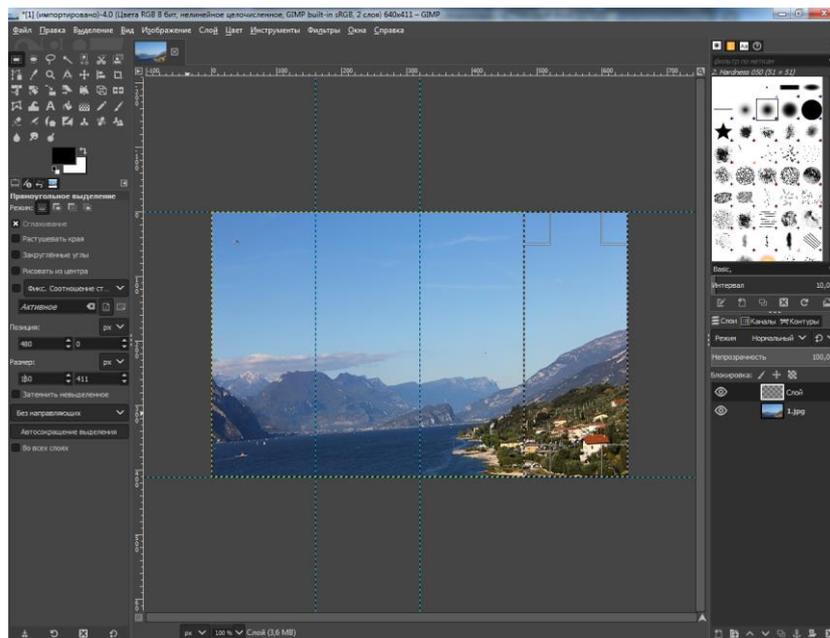


Рис. 72

- Берем инструмент **Плоская заливка** и закрашиваем каждую область. Для того, чтобы закрасить область, необходимо выбирать нужную прямоугольную область (с помощью инструмента **Прямоугольное выделение**).

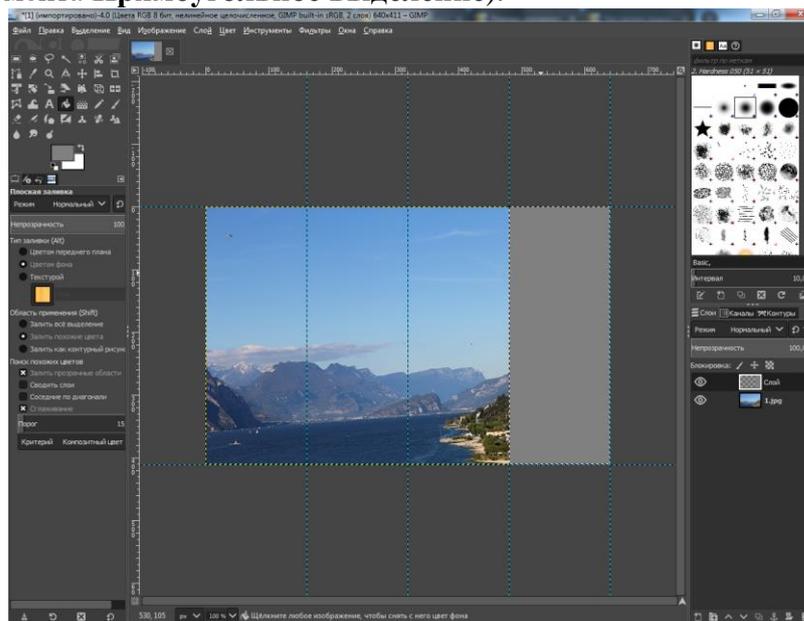


Рис. 73

- В конечном счете должен получиться четырехцветный фон.

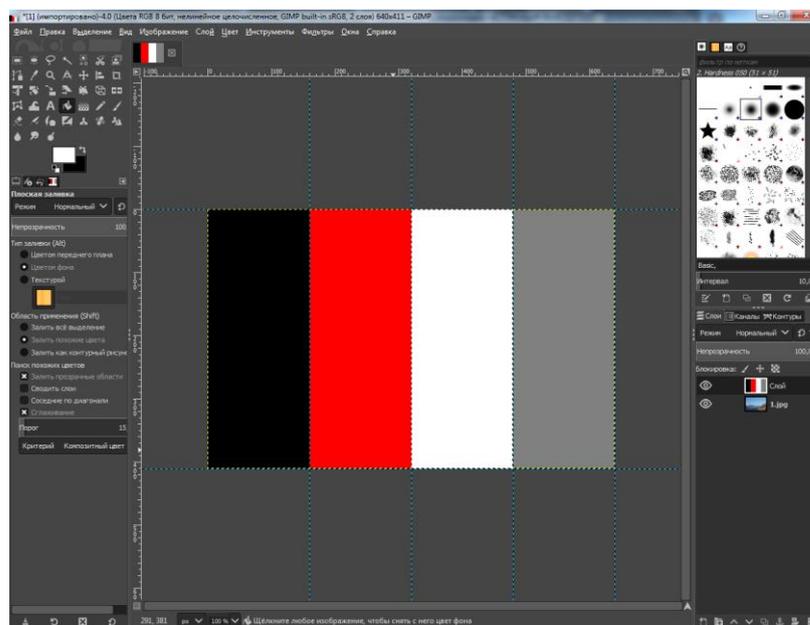


Рис. 74

- Теперь, для того чтобы выбрать режим наложения (смешивания) слоев необходимо: На диалоговом окне **Слой** установить **Непрозрачность** – «50» и в открывшемся меню выбрать желаемый режим.

При создании нового слоя автоматически устанавливается режим наложения «Нормальный».

Вставьте скриншот результата.

Эталон ответа:

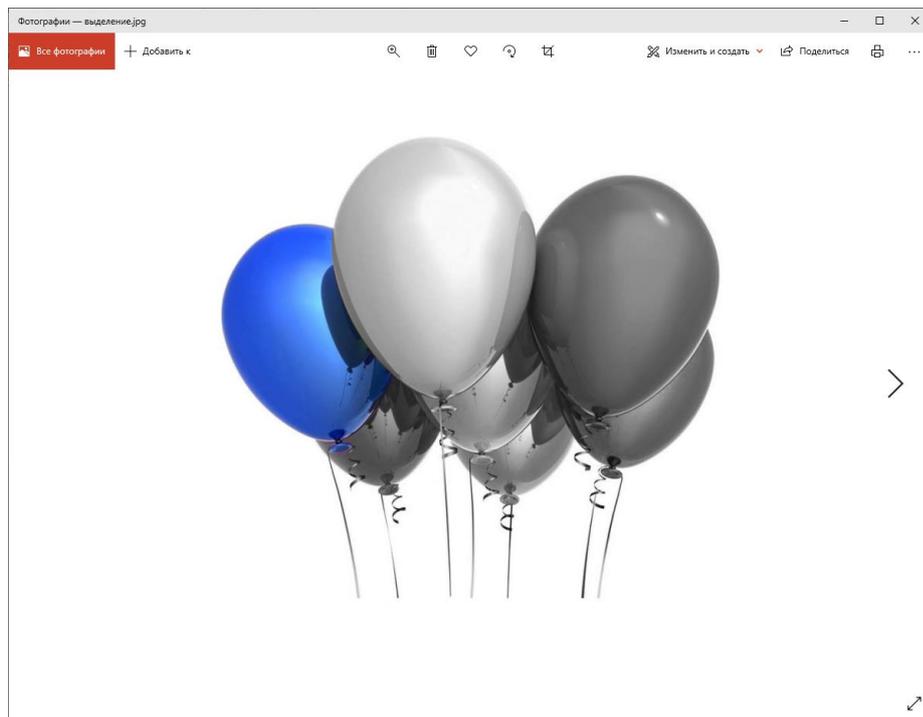
Инструмент **Свободное выделение (Лассо)**

Выделение – Инvertировать. В результате этого, выделенной станет остальная часть изображения вне границы элемента, который вы замыслили сделать цветовым акцентом.

Выделение – Растушевать

Цвет - Обесцвечивание - Светимость.

Выделение – Снять выделение

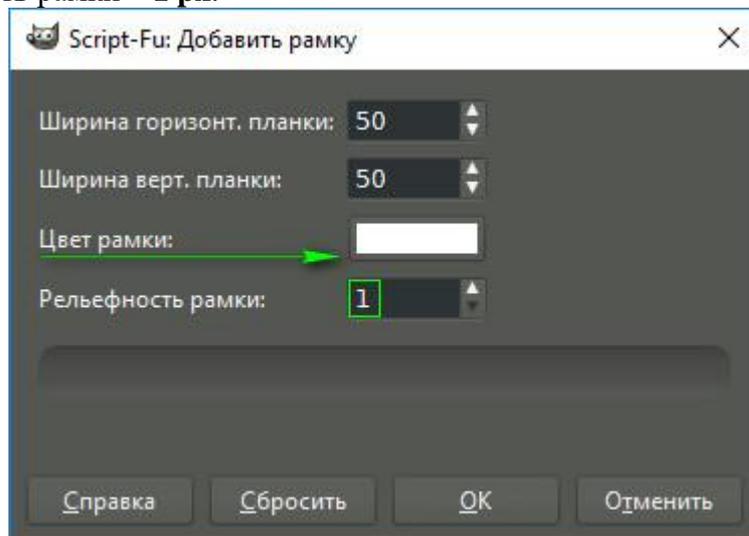


Задание 2. Рамка для фото.

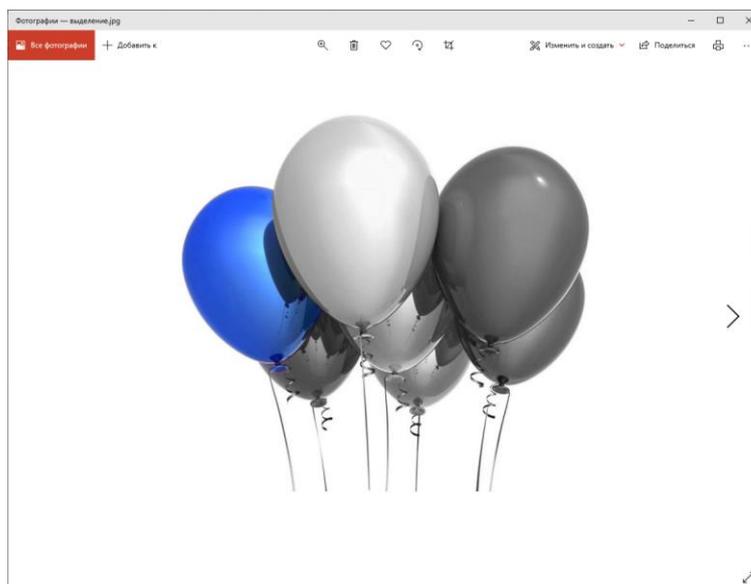
Фильтры – Декорация – Добавить рамку.

Параметры:

- Ширина горизонтальной планки – **50 px**;
- Ширина вертикальной планки – **50 px**;
- Цвет рамки – **Белый**;
- Рельефность рамки – **1 px**.

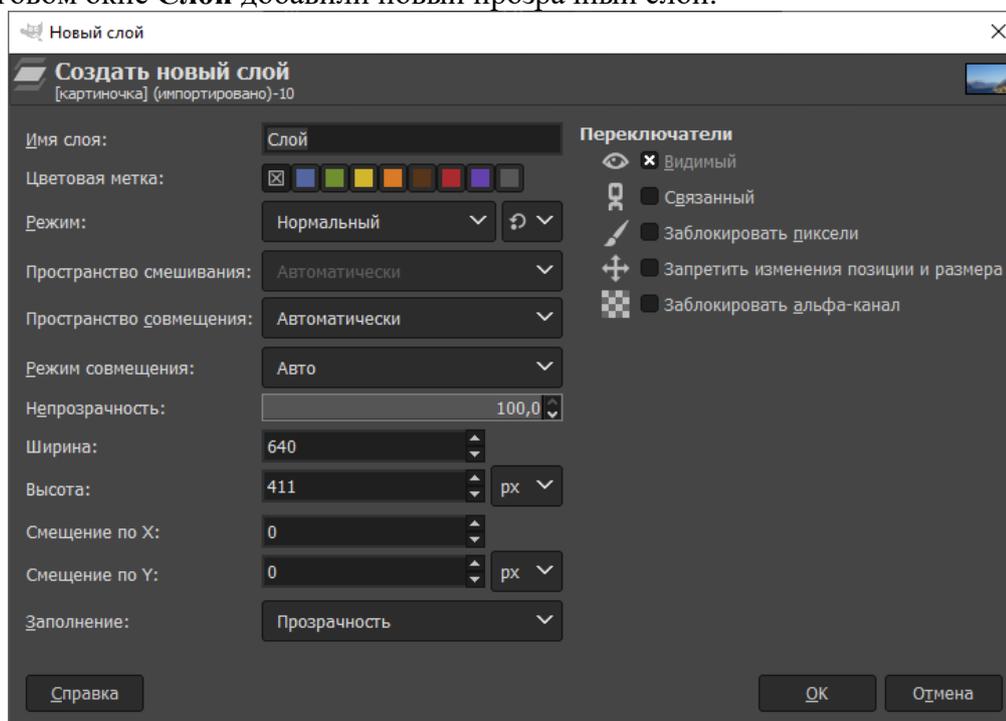


Слой правой клавишей мыши **Border Layer - Объединить с предыдущим.**

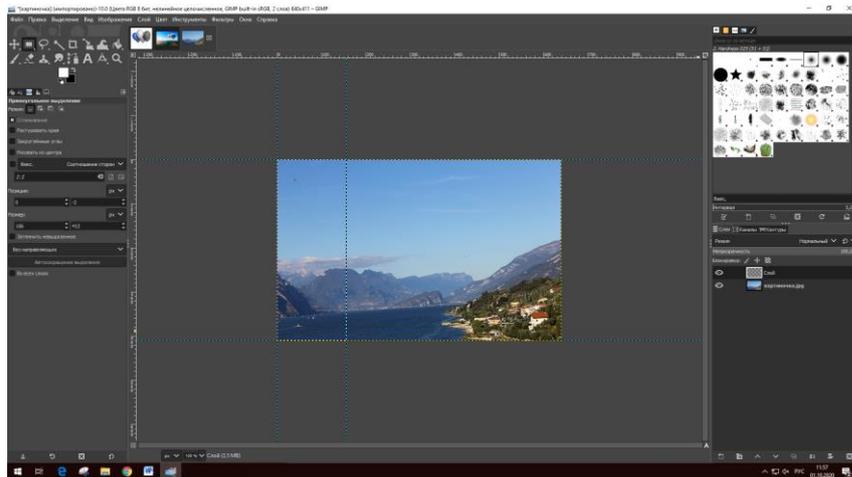


Задание 3. Наложение слоев. Режимы смешивания.

В диалоговом окне **Слой** добавили новый прозрачный слой.

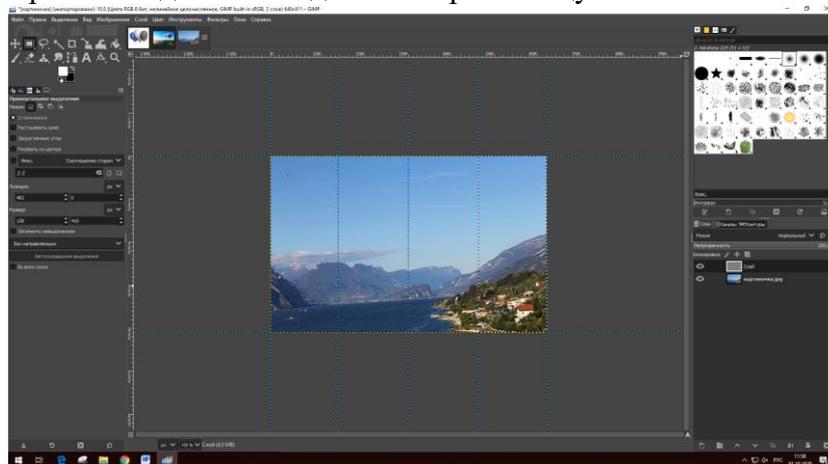


Создадим на новом слое 4 вертикальные направляющие линии. Размер данной картины по ширине 640, следовательно, каждая направляющая располагается через 160px. Для этого выбираем инструмент **Прямоугольное выделение** и строим прямоугольник с позиции 160 и размером 160.

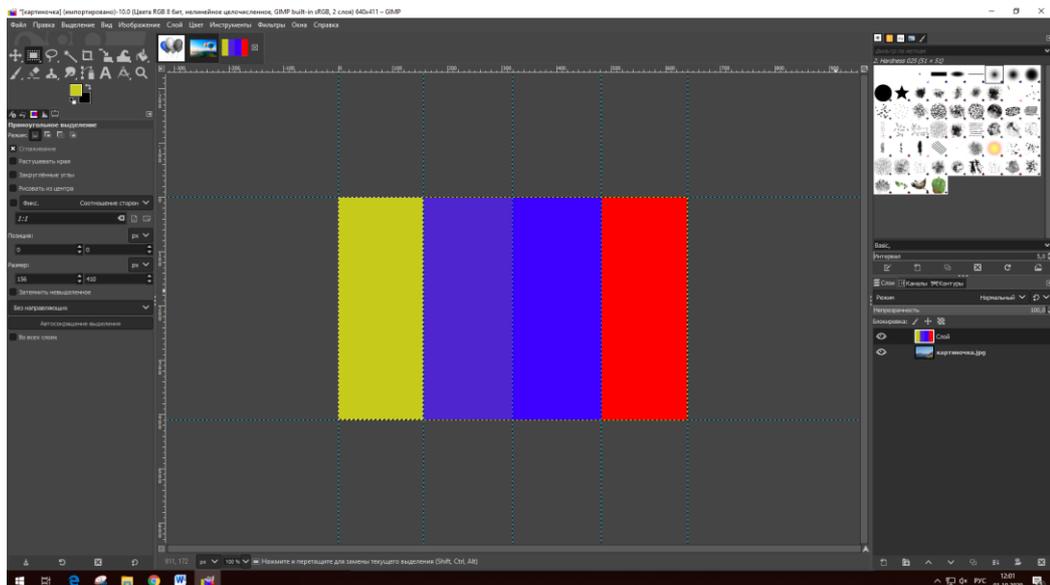


Изображение – Направляющие – Создать из выделенного

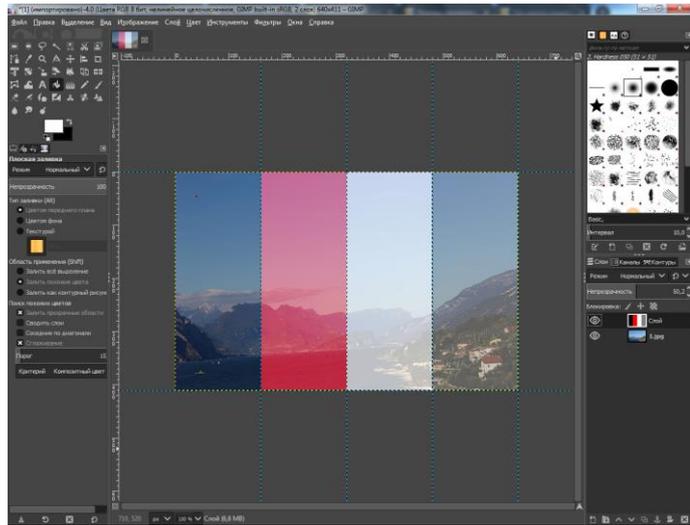
Аналогичным образом создаем последнюю направляющую.



Берем инструмент **Плоская заливка** и закрашиваем каждую область. Для того, чтобы закрасить область, необходимо выбрать нужную прямоугольную область (с помощью инструмента **Прямоугольное выделение**).

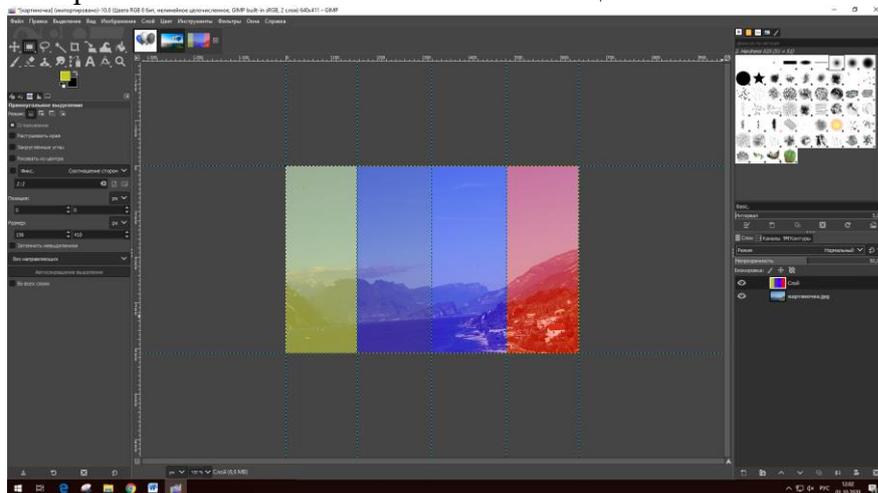


Теперь, для того чтобы выбрать режим наложения (смешивания) слоев необходимо: На диалоговом окне **Слои** установить **Непрозрачность** – «50» и в открывшемся меню выбрать желаемый режим.

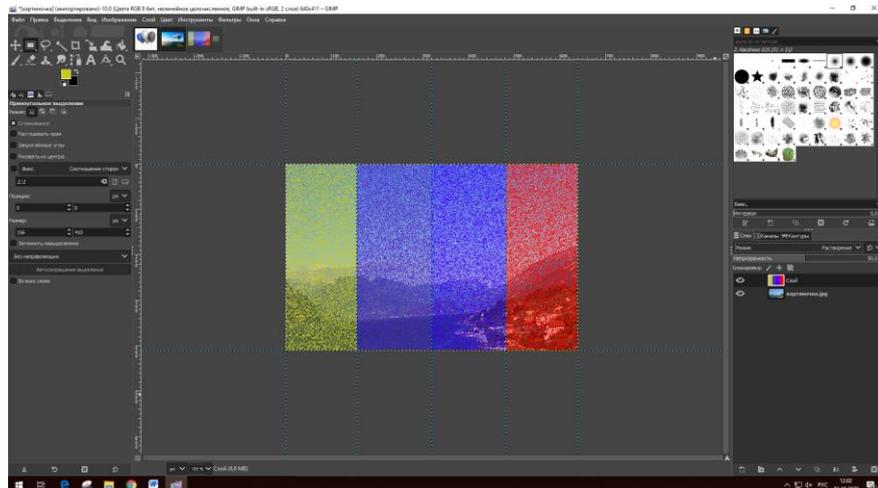


При создании нового слоя автоматически устанавливается режим наложения «Нормальный».

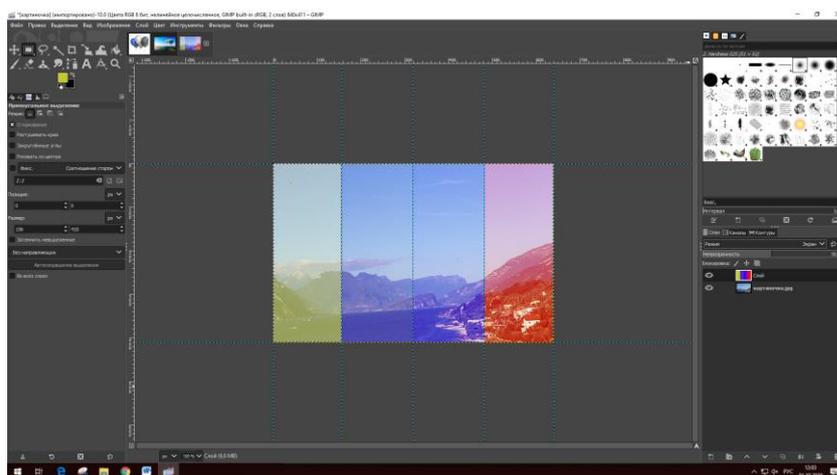
В GIMP существует около 20 режимов наложения слоя. Выбор режима изменяет внешний вид слоя или изображения в зависимости от нижележащих слоёв.



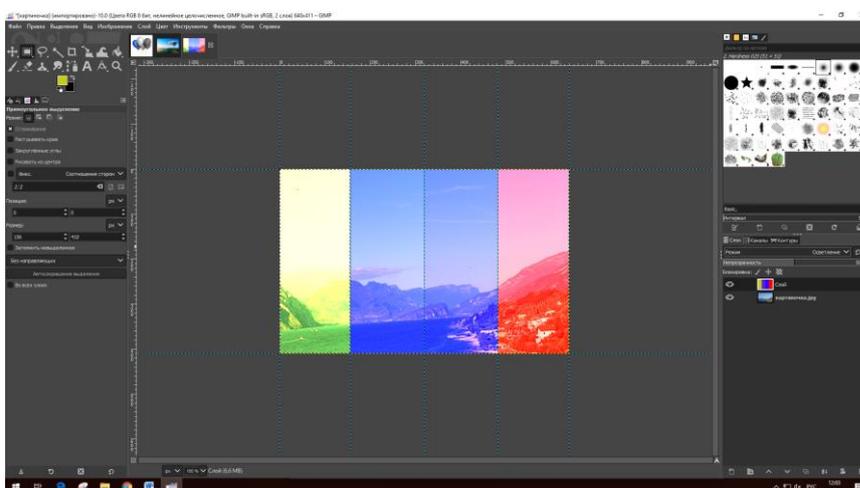
Растворение



Экран



Осветление



2. Устный зачет по теме 2.1.

Инструкция для обучающихся

Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 2 вопроса.

Выполнение задания: одному студенту на ответ выделяется 3 мин., группа сдает зачет за одно учебное занятие.

Перечень вопросов:

1. Назовите виды компьютерной графики?
2. Назовите форматы растровой графики?
3. Что такое растровая графика?
4. Что такое векторная графика?
5. Назовите форматы векторной графики?
6. Как человек воспринимает цвета?
7. Что такое цветовая модель?
8. Назовите особенности палитры RGB?
9. Где используется палитра CMYK?
10. Что такое свет и цвет?

Практическая работа № 20 «Оценка рисков информационной безопасности с использованием классификации веб-угроз»

Инструкция для обучающихся

Внимательно прочитайте задание. Проведите поиск уязвимостей информационной системы.

Время выполнения – 90 минут.

Задание

Провести «светофорную» оценку риска каждой веб-угрозы для смоделированной организации используя полученные результаты из практической работы №29. Заполнить таблицу. (Воспользоваться таблицей выше)

Название угрозы	Возможность угрозы	Последствия	Уровень риска

В настоящий момент существует множество методик оценки опасности уязвимости, но наиболее распространены следующие подходы:

- классическая «светофорная» оценка, выделяющая уязвимости «высокой», «средней» и «низкой» степени риска;
- пятиуровневая модель, принятая в стандарте PSI DSS и определяющая уровни «критичный», «неотложный», «высокий», «средний» и «низкий» (Urgent, Critical, High, Medium, Low)
- метод Common Vulnerability Scoring System (CVSS) , оценивающий степень риска как число от 0 до 10.

Классы атак

1. Аутентификация (Authentication)

Раздел, посвященный аутентификации, описывает атаки направленные на используемые Web-приложением методы проверки идентификатора пользователя, службы или приложения. Аутентификация использует как минимум один из трех механизмов (факторов): "что-то, что мы имеем", "что-то, что мы знаем" или "что-то, что мы есть". В этом разделе описываются атаки, направленные на обход или эксплуатацию уязвимостей в механизмах реализации аутентификации Web-серверов.

1. Подбор (Brute Force)

автоматизированный процесс проб и ошибок, использующийся для того, чтобы угадать имя пользователя, пароль, номер кредитной карточки, ключ шифрования и т.д.

2. Недостаточная аутентификация (Insufficient Authentication)

эта уязвимость возникает, когда Web-сервер позволяет атакующему получать доступ к важной информации или функциям сервера без должной аутентификации

3. Небезопасное восстановление паролей (Weak Password Recovery Validation)

эта уязвимость возникает, когда Web-сервер позволяет атакующему несанкционированно получать, модифицировать или восстанавливать пароли других пользователей

2. Авторизация (Authorization)

Данный раздел посвящен атакам, направленным на методы, которые используются Web-сервером для определения того, имеет ли пользователь, служба или приложение необходимые для совершения действия разрешения. Многие Web-сайты разрешают только определенным пользователям получать доступ к некоторому содержимому или функциям приложения. Доступ другим пользователям должен быть ограничен. Используя различные техники, злоумышленник может повысить свои привилегии и получить доступ к защищенным ресурсам.

1. Предсказуемое значение идентификатора сессии (Credential/Session Prediction)
предсказуемое значение идентификатора сессии позволяет перехватывать сессии других пользователей

2. Недостаточная авторизация (Insufficient Authorization)
недостаточная авторизация возникает, когда Web-сервер позволяет атакующему получать доступ к важной информации или функциям, доступ к которым должен быть ограничен

3. Отсутствие таймаута сессии (Insufficient Session Expiration)
в случае если для идентификатора сессии или учетных данных не предусмотрен таймаут или его значение слишком велико, злоумышленник может воспользоваться старыми данными для авторизации

4. Фиксация сессии (Session Fixation)
используя данный класс атак, злоумышленник присваивает идентификатору сессии пользователя заданное значение

3. Атаки на клиентов (Client-side Attacks)

Этот раздел описывает атаки на пользователей Web-сервера. Во время посещения сайта, между пользователем и сервером устанавливаются доверительные отношения, как в технологическом, так и в психологическом аспектах. Пользователь ожидает, что сайт предоставит ему легитимное содержимое. Кроме того, пользователь не ожидает атак со стороны сайта. Эксплуатируя это доверие, злоумышленник может использовать различные методы для проведения атак на клиентов сервера.

1. Подмена содержимого (Content Spoofing)
используя эту технику, злоумышленник заставляет пользователя поверить, что страницы сгенерированы Web-сервером, а не переданы из внешнего источника

2. Межсайтовое выполнение сценариев (Cross-site Scripting, XSS)
наличие уязвимости Cross-site Scripting позволяет атакующему передать серверу исполняемый код, который будет перенаправлен браузеру пользователя

3. Расщепление HTTP-запроса (HTTP Response Splitting)
при использовании данной уязвимости злоумышленник посылает серверу специальным образом сформированный запрос, ответ на который интерпретируется целью атаки как два разных ответа

4. Выполнение кода (Command Execution)

Эта секция описывает атаки, направленные на выполнение кода на Web-сервере. Все серверы используют данные, переданные пользователем при обработке запросов. Часто эти данные используются при составлении команд, применяемых для генерации динамического содержимого. Если при разработке не учитываются требования безопасности, злоумышленник получает возможность модифицировать исполняемые команды.

1. Переполнение буфера (Buffer Overflow)

эксплуатация переполнения буфера позволяет злоумышленнику изменить путь исполнения программы путем перезаписи данных в памяти системы

2. Атака на функции форматирования строк (Format String Attack)

при использовании этих атак путь исполнения программы модифицируется методом перезаписи областей памяти с помощью функций форматирования символьных переменных

3. Внедрение операторов LDAP (LDAP Injection)

атаки этого типа направлены на Web-серверы, создающие запросы к службе LDAP на основе данных, вводимых пользователем

4. Выполнение команд ОС (OS Commanding)

атаки этого класса направлены на выполнение команд операционной системы на Web-сервере путем манипуляции входными данными

5. Внедрение операторов SQL (SQL Injection)

эти атаки направлены на Web-серверы, создающие SQL запросы к серверам СУБД на основе данных, вводимых пользователем

6. Внедрение серверных сценариев (SSI Injection)

атаки данного класса позволяют злоумышленнику передать исполняемый код, который в дальнейшем будет выполнен на Web-сервере

7. Внедрение операторов XPath (XPath Injection)

эти атаки направлены на Web-серверы, создающие запросы на языке XPath на основе данных, вводимых пользователем

5. Разглашение информации (Information Disclosure)

Атаки данного класса направлены на получение дополнительной информации о Web-приложении. Используя эти уязвимости, злоумышленник может определить используемые дистрибутивы ПО, номера версий клиента и сервера и установленные обновления. В других случаях, в утекающей информации может содержаться расположение временных файлов или резервных копий. Во многих случаях эти данные не требуются для работы пользователя. Большинство серверов предоставляют доступ к чрезмерному объему данных, однако необходимо минимизировать объем служебной информации. Чем большими знаниями о приложении будет располагать злоумышленник, тем легче ему будет скомпрометировать систему.

1. Индексирование директорий (Directory Indexing)

атаки данного класса позволяют атакующему получить информацию о наличии файлов в Web каталоге, которые недоступны при обычной навигации по Web сайту

2. Идентификация приложений (Web Server/Application Fingerprinting)

определение версий приложений используется злоумышленником для получения информации об используемых сервером и клиентом операционных системах, Web-северах и браузерах

3. Утечка информации (Information Leakage)

эти уязвимости возникают в ситуациях, когда сервер публикует важную информацию, например, комментарии разработчиков или сообщения об ошибках, которая может быть использована для компрометации системы

4. Обратный путь в директориях (Path Traversal)

данная техника атак направлена на получение доступа к файлам, директориям и командам, находящимся вне основной директории Web-сервера.

5. Предсказуемое расположение ресурсов (Predictable Resource Location)

позволяет злоумышленнику получить доступ к скрытым данным или функциональным возможностям

6. Логические атаки (Logical Attacks)

Атаки данного класса направлены на эксплуатацию функций приложения или логики его функционирования. Логика приложения представляет собой ожидаемый процесс функционирования программы при выполнении определенных действий. В качестве примеров можно привести восстановление пролей, регистрацию учетных записей, аукционные торги, транзакции в системах электронной коммерции. Приложение может требовать от пользователя корректного выполнения нескольких последовательных действий для выполнения определенной задачи. Злоумышленник может обойти или использовать эти механизмы в своих целях.

1. Злоупотребление функциональными возможностями (Abuse of Functionality)
данные атаки направлены на использование функций Web-приложения с целью обхода механизмов разграничения доступа
2. Отказ в обслуживании (Denial of Service)
данный класс атак направлен на нарушение доступности Web-сервера
3. Недостаточное противодействие автоматизации (Insufficient Anti-automation).
Эти уязвимости возникают в случае, если сервер позволяет автоматически выполнять операции, которые должны проводиться вручную
4. Недостаточная проверка процесса (Insufficient Process Validation). Уязвимости этого класса возникают, когда сервер недостаточно проверяет последовательность выполнения операций приложения.

3. Пример

Уровень риска

Возможность	Последствия				
	Незначительные	Легкие	Средние	Серьезные	Катастрофа
Редко	Н	Н	С	ВС	В
Маловероятно	Н	Н	С	ВС	В
Средне	Н	С	ВС	В	В
Вероятно	С	ВС	В	В	В
Определенно	С	В	В	В	В

В	Высокий риск	Детальное исследование и план управления
ВС	Риск выше среднего	Необходимо вмешательство высшего руководства
С	Средний риск	Должны быть назначены ответственные
Н	Низкий риск	Управляется внутренними документами и процедурами

Эталон ответа:

1. Провести «световую» оценку риска каждой веб-угрозы для смоделированной организации. Заполнить таблицу. (Воспользоваться таблицей выше)

Название угрозы	Возможность угрозы	Последствия	Уровень риска
Подбор	Маловероятно	Средние	С
Недостаточная аутентификация	Маловероятно	Серьезные	ВС
Небезопасное восстановление паролей	Маловероятно	Серьезные	ВС
Предсказуемое значение	Редко	Средние	С

идентификатора сессии			
Недостаточная авторизация	Редко	Средние	С
Отсутствие таймаута сессии	Средне	Серьёзные	В
Фиксация сессии	Маловероятно	Средние	С
Подмена содержимого	Вероятно	Катастрофа	В
Межсайтовое выполнение сценариев	Маловероятно	Легкие	Н
Расщепление HTTP-запроса	Маловероятно	Средние	С
Переполнение буфера	Вероятно	Катастрофа	В
Атака на функции форматирования строк	Редко	Легкие	Н
Внедрение операторов LDAP	Маловероятно	Средние	С
Выполнение команд ОС	Маловероятно	Серьёзные	ВС
Внедрение операторов SQL	Средне	Катастрофа	В
Внедрение серверных сценариев	Маловероятно	Средние	С
Внедрение операторов XPath	Средне	Средние	ВС
Индексирование директорий	Маловероятно	Незначительные	Н
Идентификация приложений	Маловероятно	Незначительные	Н
Утечка информации	Средне	Серьёзные	В
Обратный путь в директориях	Средне	Средние	ВС
Предсказуемое расположение ресурсов	Редко	Незначительные	Н
Злоупотребление функциональными возможностями	Средне	Средние	ВС
Отказ в обслуживании	Вероятно	Средние	ВС
Недостаточное противодействие автоматизации	Маловероятно	Незначительные	Н
Недостаточная проверка процесса	Средне	Легкие	С

6. Устный зачет по теме 1.4

Инструкция для обучающихся

Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 2 вопроса.

Выполнение задания: одному студенту на ответ выделяется 3 мин., группа сдает зачет за одно учебное занятие.

Перечень вопросов:

1. Что такое Аутентификация (Authentication)?

2. Как реализуются атаки на клиентов (Client-side Attacks)?
3. Что такое Логические атаки (Logical Attacks)?
4. Какие атаки называются Выполнение кода (Command Execution)?
5. Назовите основные поисковые признаки уязвимостей ИС?
6. На какие классы подразделяются Уязвимости ИС по области происхождения?
7. На какие классы подразделяются Уязвимости ИС по месту возникновения?
8. Назовите этапы аудита информационной безопасности?
9. Назовите методы тестирования веб-сервисов?
10. Что понимается под Фаззингом параметров?

3.2. Контрольно-оценочные материалы для промежуточной аттестации

Формой промежуточной аттестации по МДК.04.01 является **дифференцированный зачет**.

Перечень вопросов для дифференциального зачета:

1. Определение каталога и службы каталогов
2. Назначение службы каталогов
3. Функции службы каталогов
4. Преимущества active directory
5. Логическая структура AD
6. Виды компьютерной графики.
7. Что такое растровая графика. Форматы растровой графики.
8. Что такое векторная графика. Форматы векторной графики
9. Восприятие цвета человеческим глазом.
10. Цветовая модель. Разновидности цветовых моделей
11. Особенности палитры RGB.
12. Палитра CMYK. Применение
13. Понятие света и цвета.
14. Области применения цифрового видео.
15. Основные характеристики звуковой информации
16. Разновидности шумов и их спектры
17. Основные принципы цифровых преобразований звуковых сигналов
18. Анимация и мультипликация.
19. Основные форматы видеоданных. Основные характеристики видеосигнала.
20. Потокое видео. Ширина(скорость) видеопотока.

Эталон ответов: приведен в Учебном пособии по МДК 04.01

Условия выполнения

1. Количество билетов для экзаменуемого: 1
2. Время подготовки к ответу: 20 минут
3. Требования к устным ответам:
Полное овладение содержанием учебного материала, в котором обучающийся легко ориентируется, владение понятийным аппаратом.
4. Оборудование: учебная аудитория, стол, стул, пишущая ручка, бумага.

Результаты промежуточной аттестации фиксируются в протоколе.

Критерии оценки устных ответов

В системе оценки знаний и умений используются **следующие критерии:**

«Отлично» – за глубокое и полное овладение содержанием учебного материала, в котором обучающийся легко ориентируется, владение понятийным аппаратом за умение связывать теорию с практикой, решать практические задачи, высказывать и обосновывать

свои суждения. Отличная отметка предполагает грамотное, логичное изложение ответа (как в устной, так и в письменной форме), качественное внешнее оформление.

«Хорошо» – если обучающийся полно освоил учебный материал, владеет понятийным аппаратом, ориентируется в изученном материале, грамотно излагает ответ, но содержание и форма ответа имеют некоторые неточности.

«Удовлетворительно» – если обучающийся обнаруживает знание и понимание основных положений учебного материала, но излагает его неполно, непоследовательно, допускает неточности в определение понятий, не умеет доказательно обосновать свои суждения.

«Неудовлетворительно» – если обучающийся имеет разрозненные, бессистемные знания, не умеет выделять главное и второстепенное, допускает ошибки в определение понятий, искажает их смысл, беспорядочно и неуверенно излагает материал, за полное незнание и непонимание учебного материала или отказ отвечать.