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

УТВЕРЖДАЮ
Заместитель директора
по учебно-производственной работе
О.В. Фомичева
«__» _____ 2023 г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по выполнению практических работ
по МДК.02.02 Программное обеспечение компьютерных сетей
ПМ.02 ОРГАНИЗАЦИЯ СЕТЕВОГО АДМИНИСТРИРОВАНИЯ ОПЕРАЦИОННЫХ СИСТЕМ

для специальности

09.02.06 Сетевое и системное администрирование

Санкт-Петербург
2023 г.

Методические рекомендации рассмотрены на заседании методического совета СПб ГБПОУ «АУГСГиП»
Протокол № 2 от «29» 11 202 3 г.

Методические рекомендации одобрены на заседании цикловой комиссии информационных технологий
Протокол № 4 от «21» 11 202 3 г.

Председатель цикловой комиссии: Караченцева М.С. _____

Разработчики: преподаватели СПб ГБПОУ «АУГСГиП»

С О Д Е Р Ж А Н И Е

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая тетрадь по выполнению практических работ предназначены для организации работы на практических занятиях по МДК 02.02 «Программное обеспечение компьютерных сетей», которая является важной составной частью в системе подготовки специалистов среднего профессионального образования по специальности 09.02.06 «Сетевое и системное администрирование».

Практические занятия являются неотъемлемым этапом изучения учебной дисциплины и проводятся с целью:

- формирования практических умений в соответствии с требованиями к уровню подготовки обучающихся, установленными рабочей программой учебной дисциплины;
- обобщения, систематизации, углубления, закрепления полученных теоретических знаний;
- готовности использовать теоретические знания на практике.

Практические занятия по МДК 02.02 «Программное обеспечение компьютерных сетей» способствуют формированию в дальнейшем при изучении профессиональных модулей, следующих общих и профессиональных компетенций:

ОК 1. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;

ОК 2. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;

ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях;

ОК 4. Эффективно взаимодействовать и работать в коллективе и команде;

ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;

ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;

ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, 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. Пользоваться профессиональной документацией на государственном и иностранном языках.

ПК 2.1 Администрировать локальные вычислительные сети и принимать меры по устранению возможных сбоев.

ПК 2.2 Администрировать сетевые ресурсы в информационных системах.

В рабочей тетради предлагаются к выполнению практические работы, предусмотренные учебной рабочей программой по МДК02.02 «Программное обеспечение компьютерных сетей».

При разработке содержания практических работ учитывался уровень сложности освоения студентами соответствующей темы, общих и профессиональных компетенций, на формирование которых направлена дисциплина.

Выполнение практических работ в рамках МДК02.02 «Программное обеспечение компьютерных сетей» позволяет освоить комплекс работ по выполнению практических заданий по всем темам МДК02.02 «Программное обеспечение компьютерных сетей».

Методические рекомендации по МДК02.02 «Программное обеспечение компьютерных сетей» имеют практическую направленность и значимость

Рабочая тетрадь предназначена для студентов колледжа, изучающих МДК02.02 «Программное обеспечение компьютерных сетей».

Оценки за выполнение практических работ выставляются по пятибалльной системе. Оценки за практические работы являются обязательными текущими оценками по учебной дисциплине и выставляются в журнале теоретического обучения.

1. Перечень практических работ по МДК 02.02 «Программное обеспечение компьютерных сетей»

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов
Тема 1. Реализация клиентской инфраструктуры	- локализовать отказ и инициировать корректирующие действия; - пользоваться нормативно-технической документацией в области инфокоммуникационных технологий; - использовать различные средства и режимы установки и обновления программного обеспечения информационно-коммуникационной системы, в том числе автоматические; - выполнять плановое архивирование программного обеспечения пользовательских устройств согласно графику	ОК 1-9 ПК 2.1 - 2.5	Практическая работа№ 1 Оценка и определение параметров развертывания	2
			Практическая работа№ 2 Планирование стратегии управления образами	2
			Практическая работа№ 3 Настройка безопасности клиентских систем	2
			Практическая работа№ 4 Настройка шифрования файлов с помощью EFS	2
			Практическая работа№ 5 Подготовка образа и среды предустановки Установка Windows ADK	2
			Практическая работа№ 6 Создание эталонного образа с помощью Windows SIM и Sysprep Создание файла ответов с помощью Windows SIM	2
			Практическая работа№ 7 Создание и обслуживание эталонного образа	2
			Практическая работа№ 8 Настройка и управление Windows Deployment Services	2

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов
			Планирование среды Windows Deployment Services	
			Практическая работа№ 9 Планирование и реализация миграции пользовательской среды	2
			Практическая работа№ 10 Миграция состояния пользователя с созданием жестких ссылок	2
			Практическая работа№ 11 Планирование и развертывание клиентских ОС с помощью MDT	2
			Практическая работа№ 12 Подготовка среды для развертывания операционной системы	2
			Практическая работа№ 13 Использование MDT и Configuration Manager для подготовки Zero-Touch Installation	2
			Практическая работа№ 14 Планирование и реализация инфраструктуры Remote Desktop Services	2
			Практическая работа№ 15 Расширение доступа к Интернет для инфраструктуры RDS	2
			Практическая работа№ 16	2

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов
			Развертывание и поддержка виртуализации профиля пользователя	
			Практическая работа№ 17 Проектирование и реализация файловых служб	2
			Практическая работа№ 18 Реализация Client Endpoint Protection Настройка точки Endpoint Protection	2
			Практическая работа№ 19 Настройка Data Protection для данных клиентского компьютера	2
			Практическая работа№ 20 Мониторинг производительности и работоспособности инфраструктуры клиентских ОС Настройка	2

,

2. ОПИСАНИЕ ПОРЯДКА ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ РАБОТ

2.1 Практическая работа№ 1
Оценка и определение параметров развертывания

Задание:

1. Установить и запустить Acronis Snap Deploy 5;
2. Создать эталонный образ машины;

Шаг 1. Установка Acronis Snap Deploy 5

На этом этапе устанавливается Acronis Snap Deploy 5 в типичной конфигурации. Полное описание способов установки и процедур см. в разделе, посвященном установке.

Перед установкой убедитесь в том, что выполнены следующие условия.

На машине имеется современная версия Windows, такая как Windows 10 Pro. Список операционных систем, на которые можно установить Acronis Snap Deploy 5, см. в разделе «Поддерживаемые операционные системы».

Имеется программа установки. Ее можно загрузить с веб-страницы загрузки продукта Acronis.

Имеется один или несколько лицензионных ключей на Acronis Snap Deploy 5. Можно приобрести лицензионные ключи полной версии или получить пробные ключи на веб-странице Acronis Snap Deploy 5. Тип лицензии («для сервера» или «для рабочей станции») определяет тип операционной системы, которую можно развертывать.

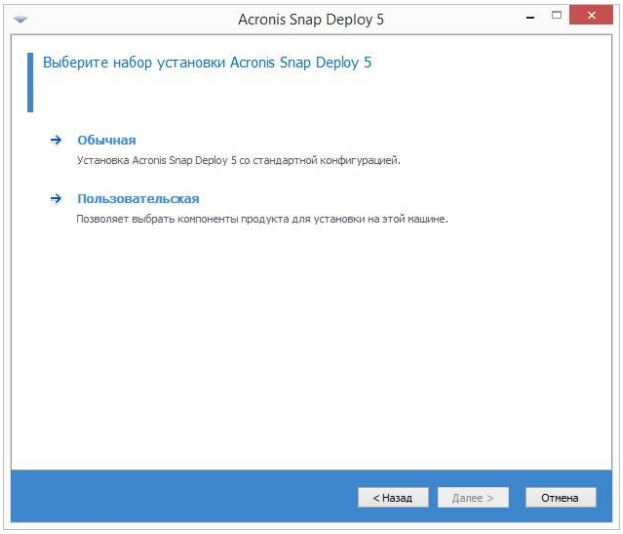
На машине, на которую нужно установить Acronis Snap Deploy 5, выполните следующие действия:

Войдите в систему с учетной записью администратора и запустите программу установки.

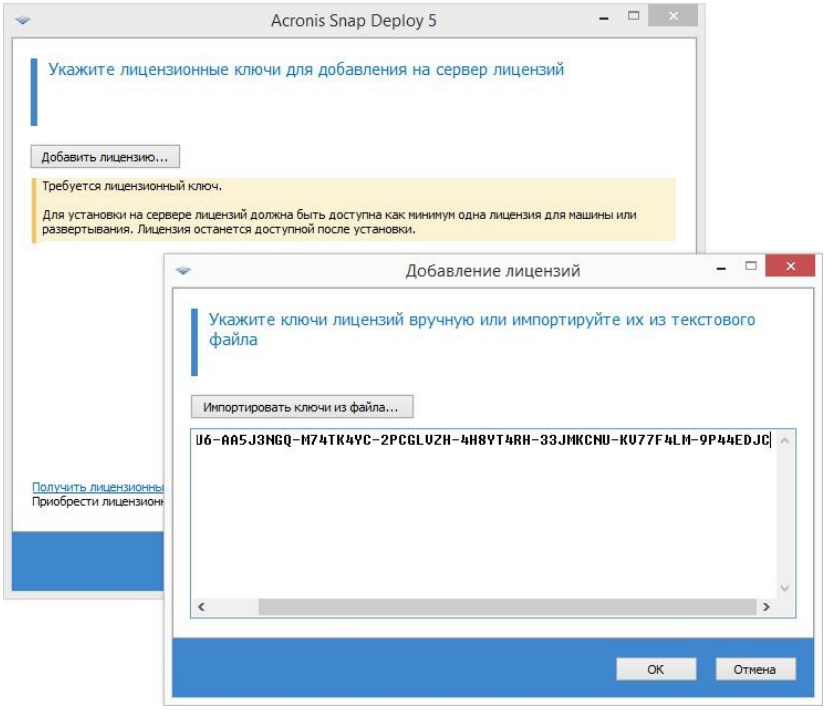
Нажмите Установить Acronis Snap Deploy 5.

Примите условия лицензионного соглашения и нажмите кнопку Далее.

Выберите Обычная.



Щелкните Добавить лицензию, а затем укажите лицензионные ключи. Можно ввести лицензионные ключи вручную или импортировать их из текстового файла.



Укажите, будет ли машина участвовать в программе улучшения качества программного обеспечения.

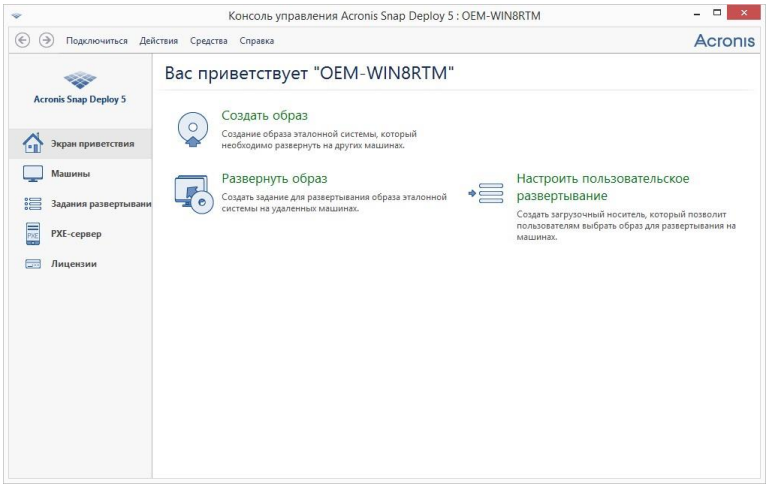
Нажмите кнопку Установить.

Шаг 2. Запуск Acronis Snap Deploy 5

На машине, на которой установлен Acronis Snap Deploy 5, выполните следующие действия.

На рабочем столе щелкните Acronis Snap Deploy 5.

После запуска Acronis Snap Deploy 5 появится экран приветствия.



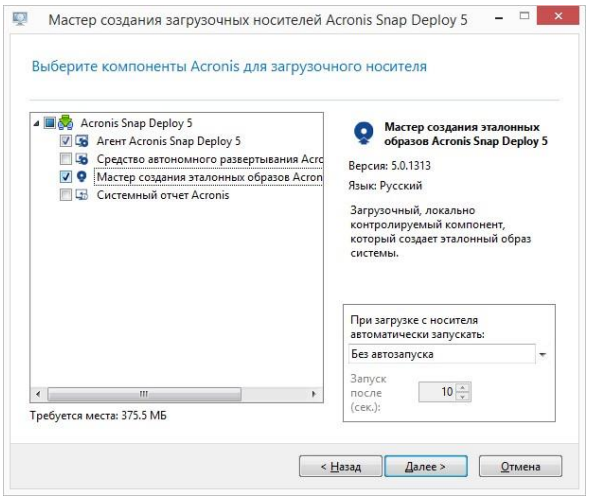
Шаг 3. Создание загрузочного носителя

На этом этапе создается загрузочный носитель, позволяющий создавать эталонные образы и выполнять развертывание.

На машине, на которой установлен и запущен Acronis Snap Deploy 5, выполните следующие действия.

В меню Средства выберите пункт Создать загрузочный носитель.

В списке компонентов выберите Агент и Мастер создания эталонных образов.



В окне Сетевые настройки в поле Имя/IP адрес сервера укажите имя машины, на которой установлен Acronis Snap Deploy 5.

Выберите создание носителя на CD или DVD. Вставьте чистый диск CD-R/RW или DVD-R/RW.

Совет. Если на машине нет оптического дисковода CD-RW, DVD-RW, можно выбрать создание ISO-файла, который затем можно будет записать на оптический диск на другой машине. Также можно создать носитель на USB-накопителе. Дополнительные сведения см. в разделе «Создание загрузочного носителя».

Нажмите кнопку Создать.

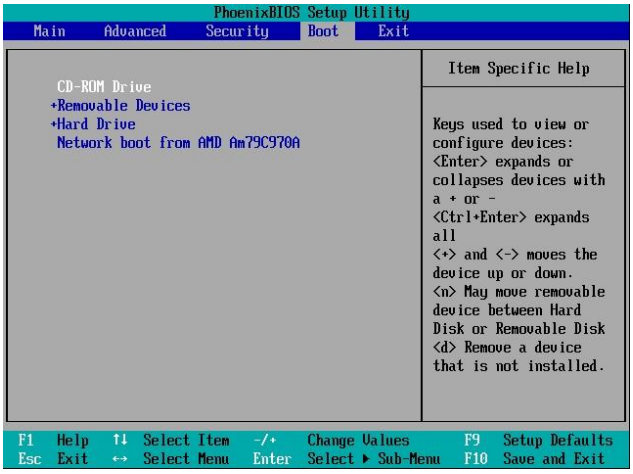
Шаг 4. Создание эталонного образа

На этом этапе образ машины создается и сохраняется на жестком диске с USBинтерфейсом.

Выберите машину, образ которой нужно создать. Для создания образа машины лицензии не требуется. Однако для развертывания машины будет использована лицензия для сервера или для рабочей станции в зависимости от того, работает ли на машине серверная операционная система (например, Windows 2008 Server или Linux) или операционная система для рабочей станции (например, Windows 7). Список операционных систем для серверов и рабочих станций см. в разделе «Поддерживаемые операционные системы для создания образов и развертывания».

На машине, образ которой нужно создать, выполните следующие действия.

Убедитесь, что загрузка с CD или DVD имеет более высокий приоритет, чем загрузка с жесткого диска. Может потребоваться открыть средство настройки BIOS этой машины и установить приоритет загрузки, как показано на следующем рисунке.



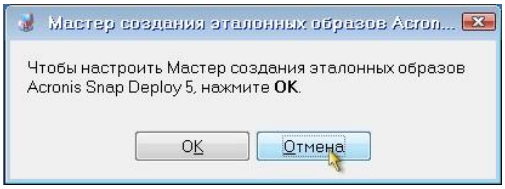
Подключите к машине жесткий диск с USB-разъемом.

Совет. Как вариант, можно сохранить образ в сетевую папку, как описано далее в этой процедуре.

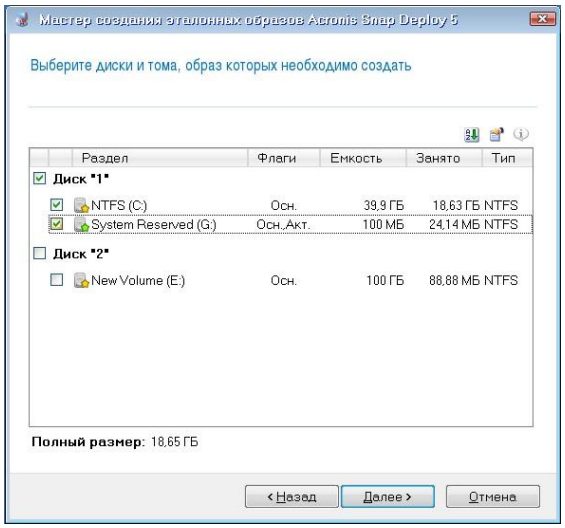
Загрузите машину с созданного загрузочного носителя.

В меню загрузки выберите Мастер создания эталонных образов.

Во всплывающем окне нажмите кнопку Отмена или дождитесь закрытия окна.



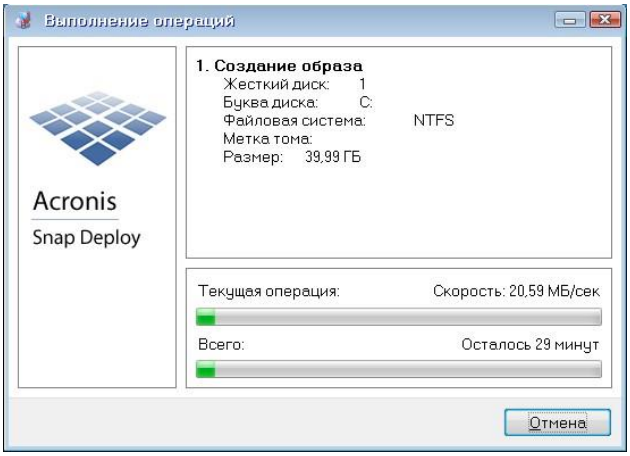
Выберите тома, которые нужно включить в эталонный образ. Можно оставить вариант по умолчанию, при котором в образ включаются тома, содержащие операционную систему.



Укажите папку на жестком диске USB, в которую нужно сохранить образ, или укажите сетевую папку, а также имя пользователя и пароль для доступа к этой папке.

Нажимайте кнопку Далее, пока не откроется итоговое окно. В этом окне нажмите кнопку Создать.

Acronis Snap Deploy 5 начнет создание образа.



После создания образа будет выполнена перезагрузка машины.

2.2 Практическая работа№ 2
Планирование стратегии управления образами

Задание:

Подготовка целевой машины

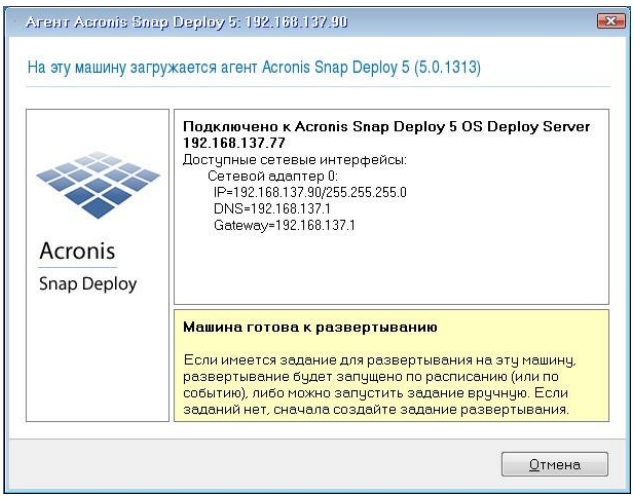
На целевой машине выполните следующие действия.

Убедитесь, что загрузка с CD или DVD имеет более высокий приоритет, чем загрузка с жесткого диска. Может потребоваться открыть средство настройки BIOS этой машины и установить приоритет загрузки.

Загрузите машину с созданного загрузочного носителя.

В меню загрузки щелкните Агент.

Во всплывающем окне нажмите кнопку Отмена или дождитесь закрытия окна. Убедитесь, что машина готова к развертыванию. Окно должно выглядеть, примерно как на следующем рисунке.



Подробно. Целевая машина готова к развертыванию после подключения к OS Deploy Server. Этот сервер является частью Acronis Snap Deploy 5. Если машина не подключается к серверу, может потребоваться настроить параметры сети, как описано в разделе «Загрузка целевых машин».

Когда целевая машина готова, можно развертывать на нее эталонный образ.

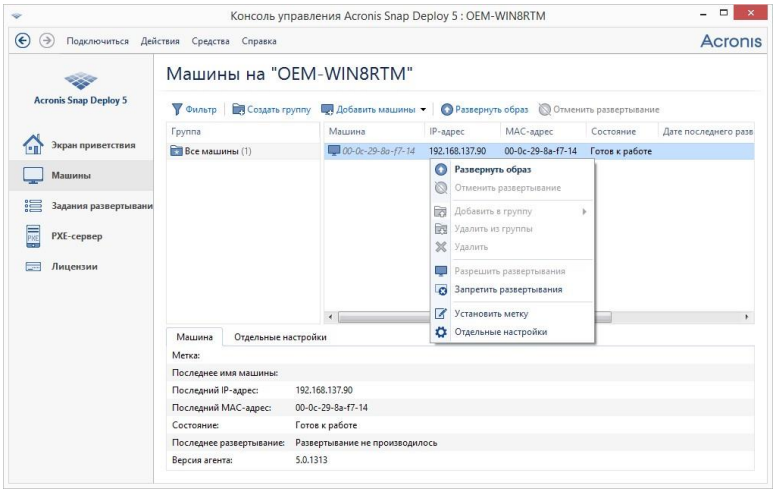
Развертывание эталонного образа

На машине, на которой установлен Acronis Snap Deploy 5, выполните следующие действия.

Подключите к машине жесткий диск USB, содержащий эталонный образ. Можно скопировать образ на локальный жесткий диск машины.

Щелкните представление Машины. Убедитесь, что подготовленная целевая машина отображается в списке с состоянием Готовые к работе.

Щелкните целевую машину правой кнопкой мыши и нажмите Развернуть образ.



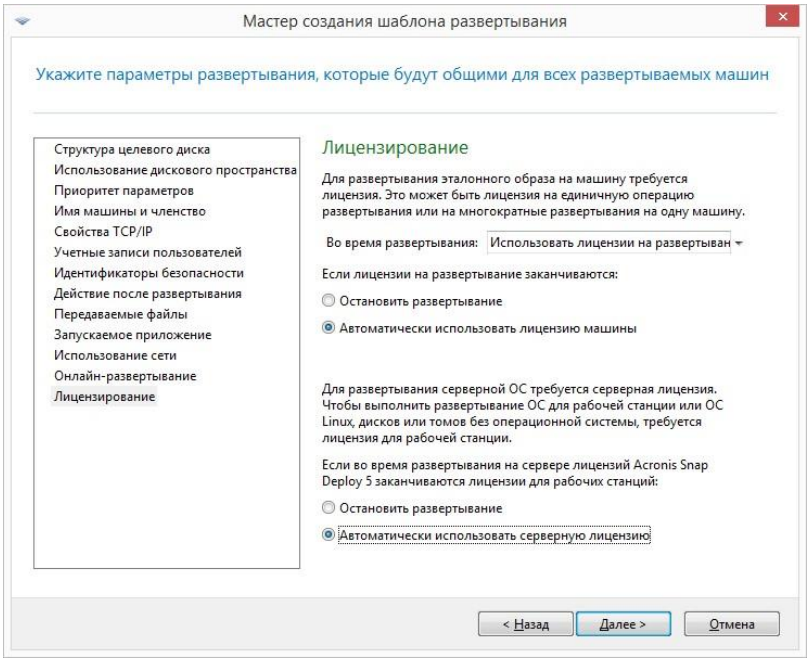
Нажимайте кнопку Далее, пока не откроется окно выбора шаблона. В этом окне нажмите кнопку Создать новый.

Щелкните Создать новый шаблон, а затем нажмите кнопку Далее.

Выберите созданный эталонный образ (TIB-файл) и нажмите кнопку Далее.

В окне настроек развертывания нажмите кнопку Далее.

Примечание. Если был создан образ машины с операционной системой для рабочих станций (например, Windows 7), но имеются только серверные лицензии (например, Acronis Snap Deploy 5 для сервера — лицензия пробной версии), может потребоваться разрешить программе использовать этот тип лицензии для развертывания машины. Для этого в окне настроек развертывания щелкните Лицензирование и выберите Автоматически использовать серверную лицензию.

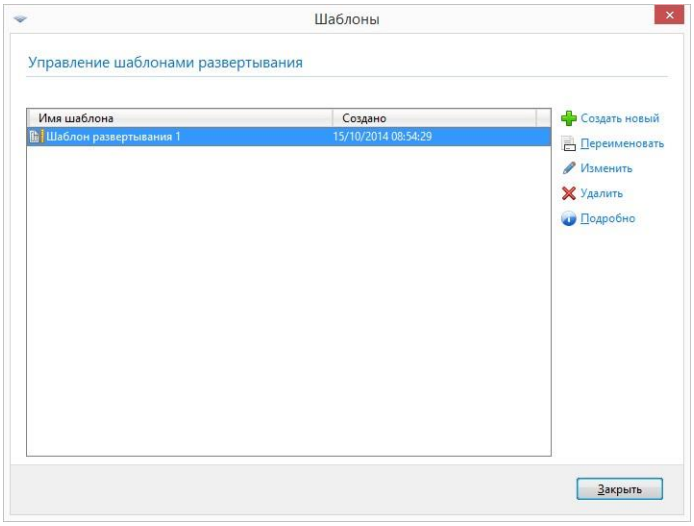


Можно добавить лицензию для рабочей станции перед началом развертывания. Для этого откройте представление Лицензии и нажмите кнопку Добавить лицензию на панели инструментов.

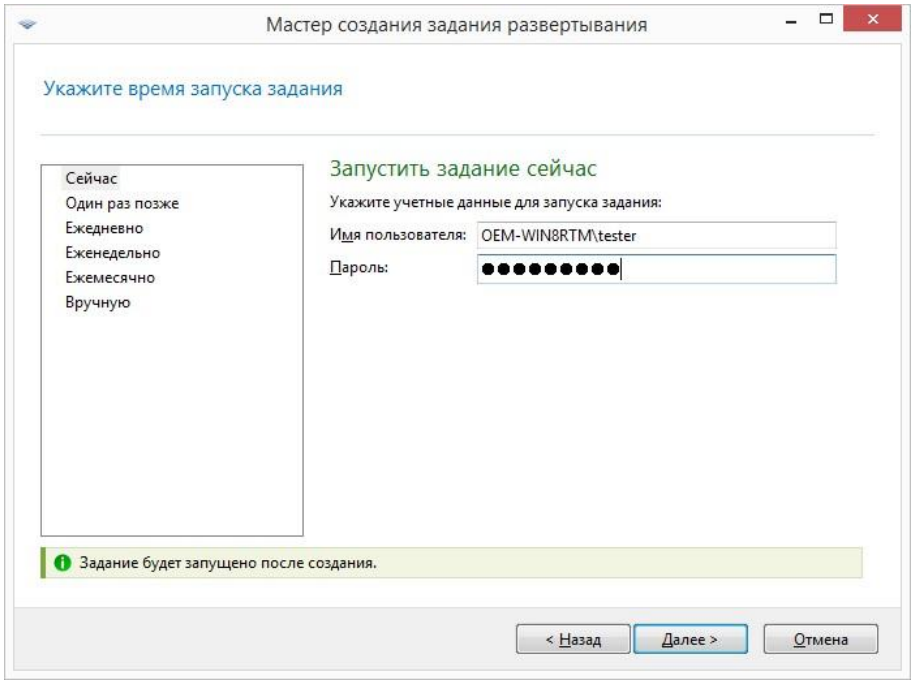
Нажимайте кнопку Далее, пока не откроется итоговое окно. В этом окне нажмите кнопку Сохранить.

Подробно. Создан шаблон развертывания. Он определяет порядок выполнения развертывания. Этот шаблон можно использовать повторно в других заданиях развертывания.

Выберите созданный шаблон развертывания, а затем нажмите кнопку Далее.

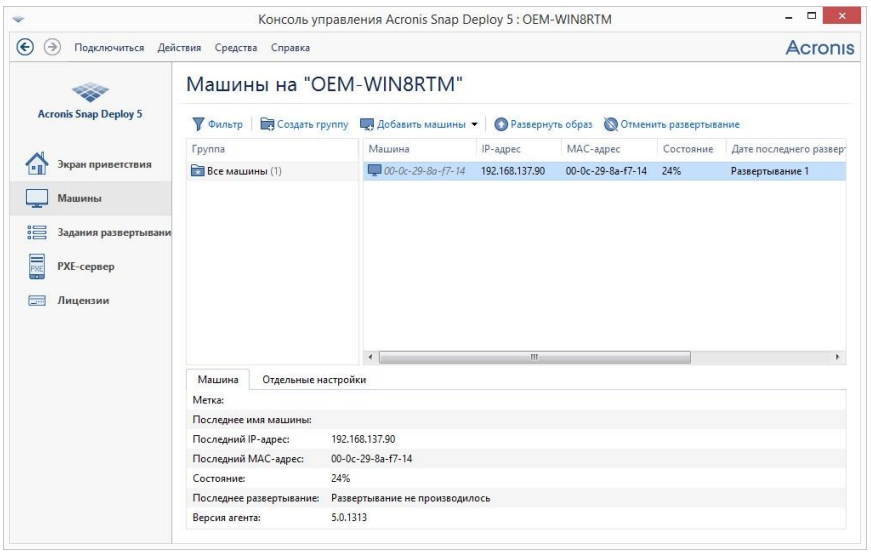


В ответ на вопрос, когда запустить развертывание, выберите Сейчас и введите имя пользователя и пароль, необходимые для входа в Windows.

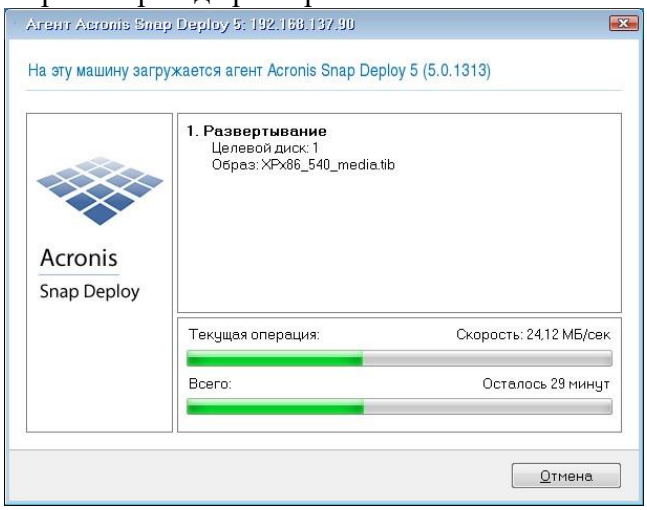


Нажимайте кнопку Далее, пока не откроется итоговое окно. В этом окне нажмите кнопку Создать.

Ход выполнения развертывания можно увидеть как на машине, где установлен Acronis Snap Deploy 5, так и на целевой машине.



Просмотр хода развертывания на машине с Acronis Snap Deploy 5



Просмотр хода развертывания на целевой машине

2.3 Практическая работа№ 3
Настройка безопасности клиентских систем

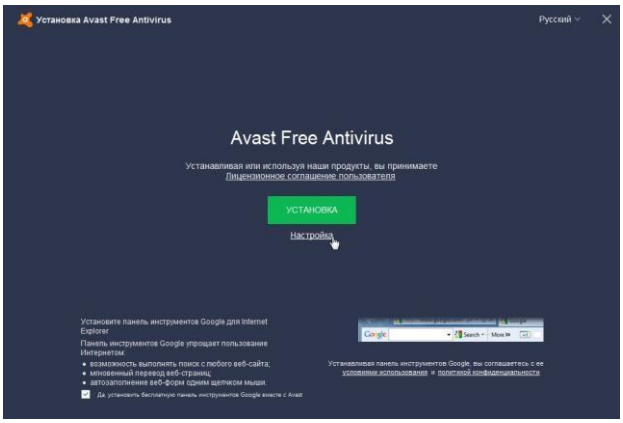
Задание:

Установка Avast Free Antivirus

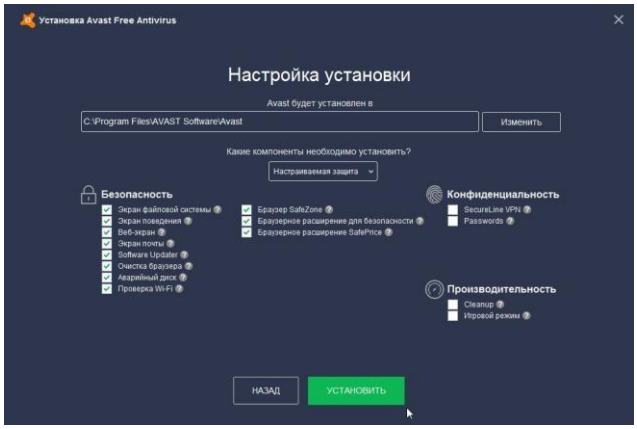
Первый этап в настройке - установка программы на ваше устройство. Убедитесь, что на вашем устройстве отсутствуют антивирусная программа (иначе удалите ее). Загрузите Avast Free Antivirus

Запустите скачанный файл, дайте положительный ответ на вопрос системы о разрешении внести изменения данной программе. Пошла распаковка установщика

Окно установки. Установка панели Google - отметить галкой на свое усмотрение. Заметим, что все продукты Google удобны и функциональны.



Можно, конечно, на данном этапе просто нажать на большую зеленую кнопку “Установка”, и просто установить антивирусную программу, и она будет хорошо работать, НО настройки производителя могут сильно отличаться от ваших потребностей и задач. Потому мы выбираем опцию “Настройка”!



Заметим, что ко всем пунктам можно получить пояснения, просто наведите курсор на знак вопроса справа.

Панель Безопасность

Для полноценной защиты нужно оставить все пункты, однако некоторыми опциями в домашних сетях пользуются редко, например, Аварийным диском - это удел профессионалов. Потому данную галку снимаем.

SoftwareUpdater - проверяет остальные программы на новизну версий. Полезная опция, когда твой софт безопасно, своевременно и самостоятельно обновляется, НО иногда для работы нужна именно такая версия программы. Потому данную опция рекомендуем использовать с осторожностью или снимаем галку.

Экран поведения. Очень часто пользователи отключают его для скорости работы, НО сейчас именно он становиться основным инструментом противодействия вирусам-шифровальщикам и новым вирусам. Он анализирует активность программ для обнаружения подозрительных или вредоносных действий. Обязательно ставим галку.

Браузер SafeZone + два браузерных расширения. Функциональные и простые решения для проведения безопасных платежей и внесения конфиденциальных данных. Оставляем галку.

Панель Конфиденциальность

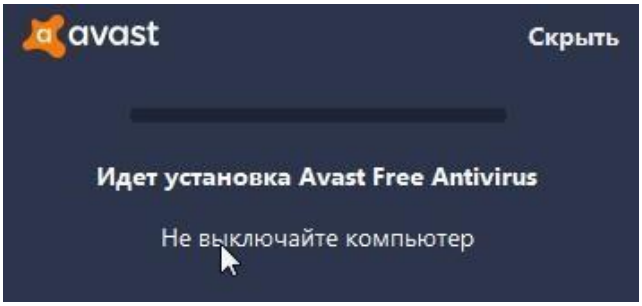
SecureLine VPN - виртуальная частная сеть. Как правило кому это нужно - уже подключены к корпоративным решениям или своим настроенным программам. Снимаем галку.

Passwords - безопасное хранилище паролей с подстановкой и одним мастерпаролем. Удобная опция. Однако, мы уверены, что хранение паролей - это нарушение безопасности и контроля. Пароли надо помнить и знать где и как они используются. Лучший способ забыть пароль - поставить галочку “запомнить пароль”. Рекомендации наших инженеров относительно создания и использования паролей в одном из наших следующих материалов. Снимаем галку.

Панель производительность

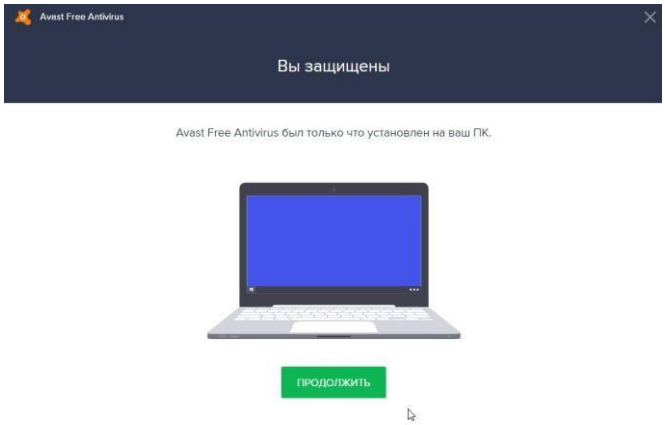
Удобные и функциональные инструменты! Существующие специализированные решения, по нашему опыту, лучшая альтернатива.

Нажимаем “Установить”



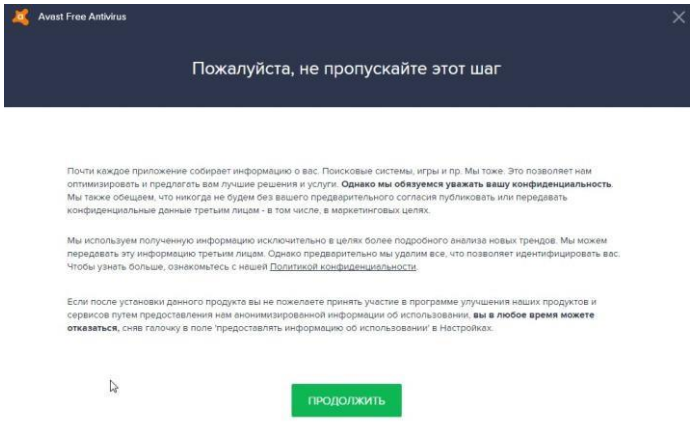
Ждем...Идет установка, время которой зависит от “железа” компьютера. Avast заявляет параллельную работу, но мы рекомендуем не мешать и дать ему установиться.

Запустите программу, если после установки она не открылась самостоятельно.



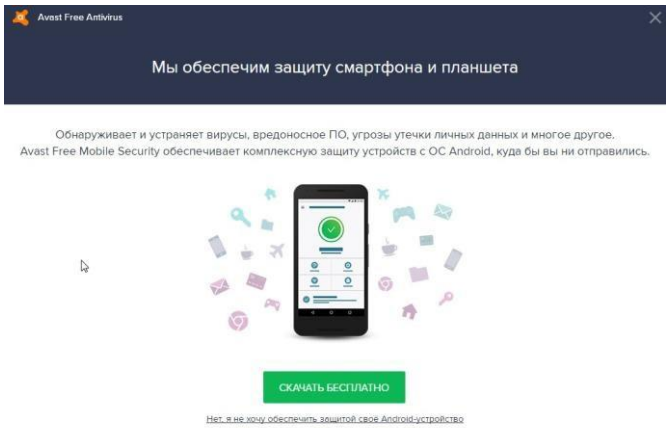
Нажмите “Продолжить”

Ознакомьтесь с окном о предоставлении информации, прочитайте! Прониклись?

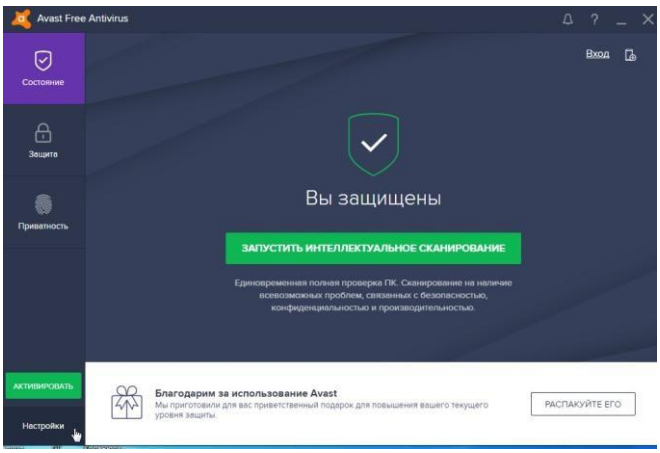


Жмите “Продолжить”

Аваст предлагает скачать дополнительно защиту для Андроид устройств, если актуально, то действуйте - нажмите “Скачать”. Иначе нажимайте “Нет, я не хочу обеспечить защитой свое Android-устройство”



Основное окно программы



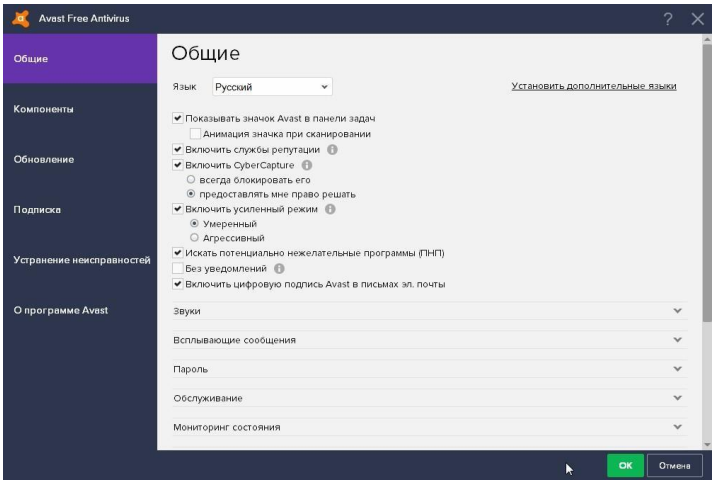
Установка антивирусной программы Avast Free Antivirus завершена.

Настройка Avast Free Antivirus

Переходим к его настройке, нажмите слева внизу кнопку “Настроить”

Панель слева - Общие

Общие

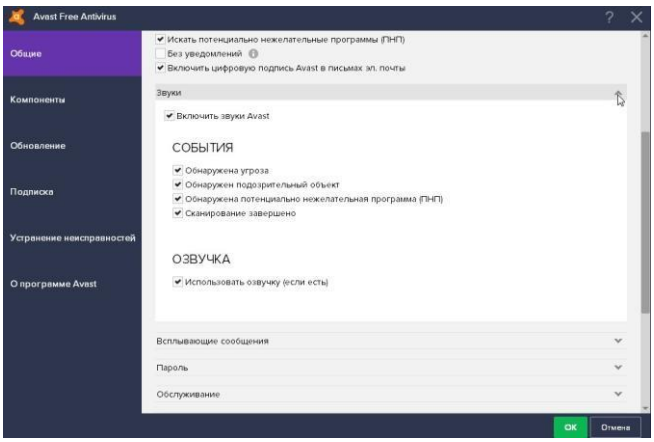


Тут рекомендуем включить усиленный режим (умеренный), CyberCapture (предоставлять мне право решать), “искать потенциально нежелательные программы”. Данные опции являются основой защиты от вирусов-шифровальщиков, хотя замедляют работу компьютера.

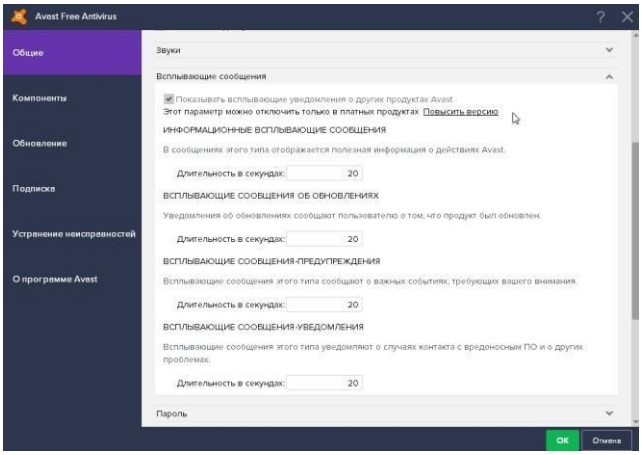
Об опасностях лучше узнавать незамедлительно, сейчас все происходит быстро, потому убираем галку “Без уведомлений”.

Прочие пункты тут очевидны и могут быть настроены по своему вкусу

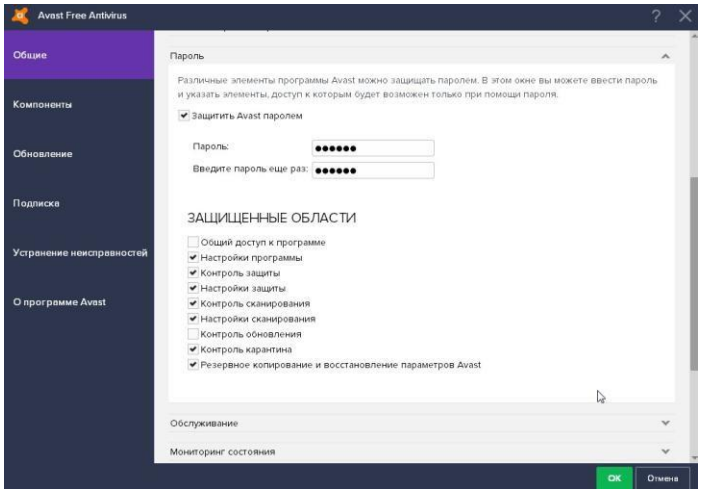
Пункт “Звук” позволяет включить звуковые оповещения об угрозах.



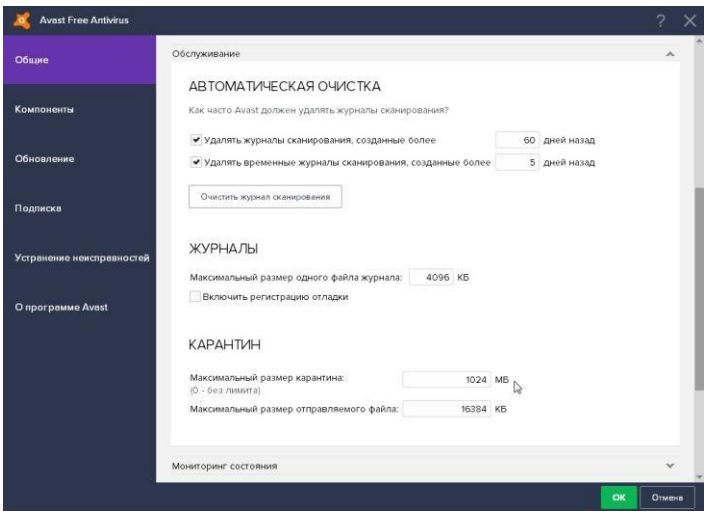
Пункт “Всплывающие сообщения” Сообщения отключаются только в платной версии, но можно уменьшить время их показа.



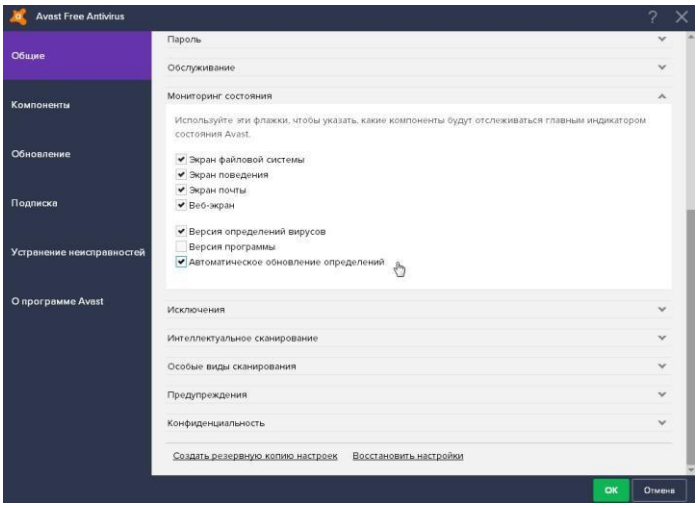
Пункт “Пароль”. ОБЯЗАТЕЛЬНО защитить антивирус паролем. Галочки советуем включить как на скриншоте



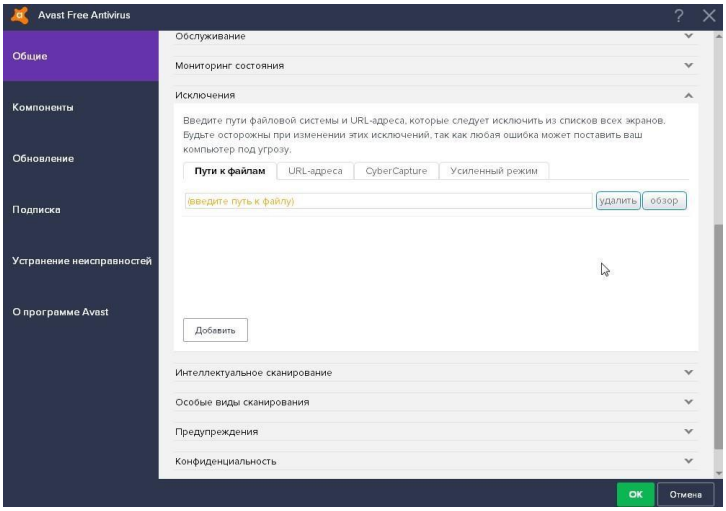
Пункт “Обслуживание”. Увеличиваем время хранение журналов сканирования и размеры карантина, как на скриншоте



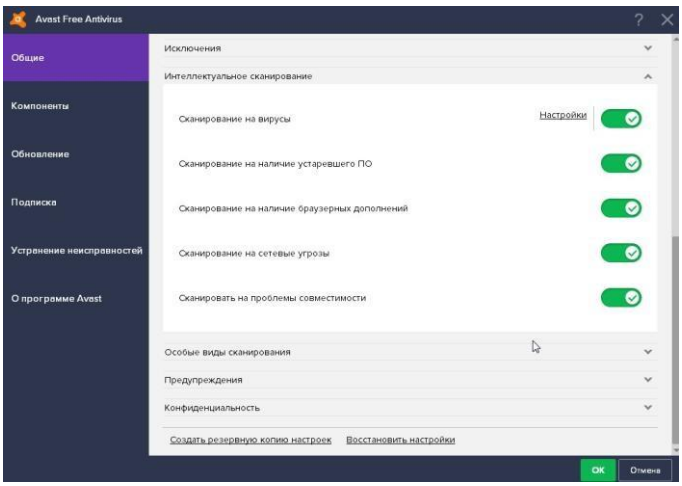
В пункте “Мониторинг” выставить настройки как на экране



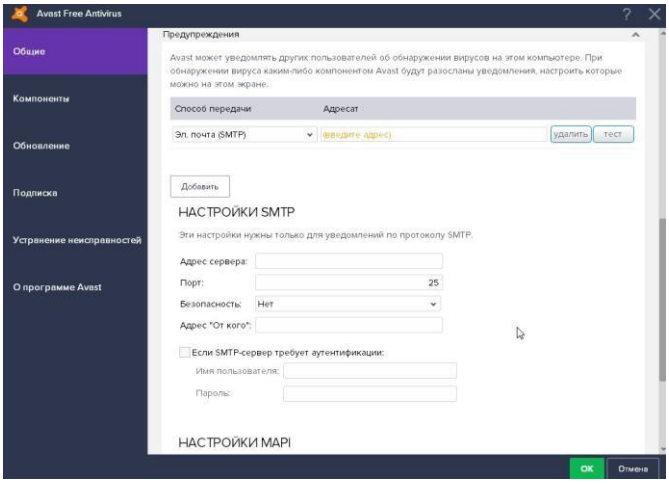
Пункт “Исключения” позволяет исключить заданные Вами URL адреса из всех экранов. Даже известные сайты не могут быть на 100% безопасны. Потому добавляя исключения вы повышаете производительность, но снижаете безопастность системы.



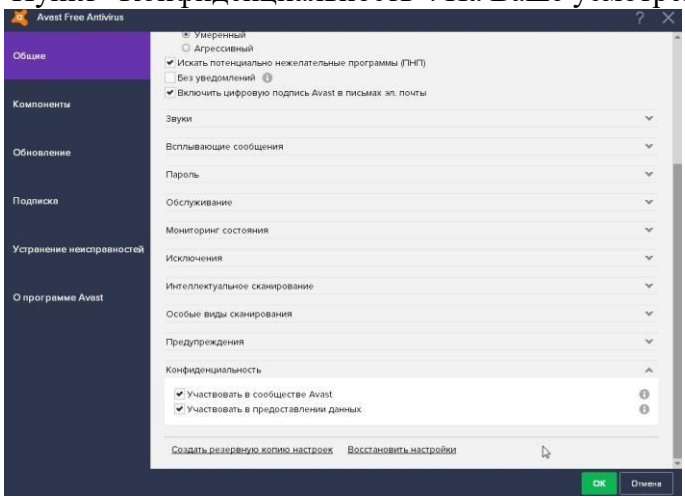
Пункт “Интеллектуальное сканирование” - все опции должны быть включены.



Пункт “Предупреждения”. Avast может уведомлять других пользователей по электронной почте об обнаружении вирусов на этом компьютере. Для разбирающихся настройки просты.

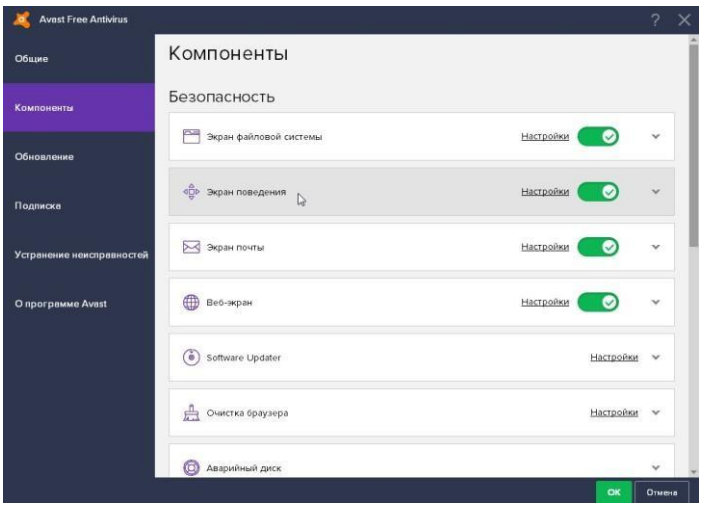


Пункт “Конфиденциальность”. На Ваше усмотрение.



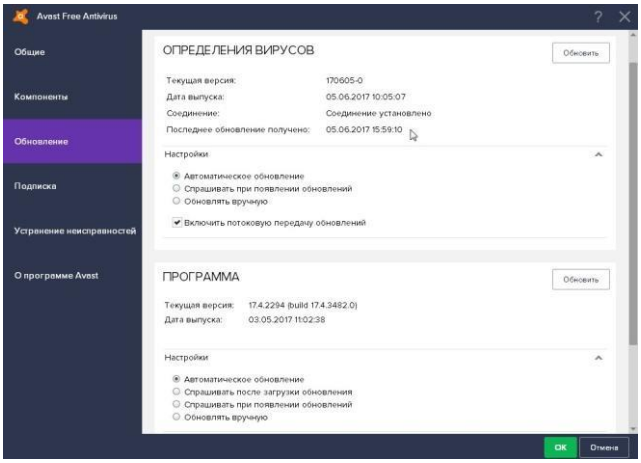
Ниже пункты “Создать резервную копию настроек” и “Восстановить настройки” полезны для забывчивых и тех у кого несколько компьютеров.

Панель слева - Компоненты



Все опции необходимо включить! Основные настройки мы сделали ранее, здесь настройки можно проверить.

Панель слева - Обновление



Включите автоматическое обновление.

2.4 Практическая работа№ 4
Настройка шифрования файлов с помощью EFS

а. Для включения режима шифрования выполните следующие действия.

1. Укажите файл или папку (например, создайте файл шифр.doc в папке Мои документы), которую требуется зашифровать, нажмите правую кнопку мыши и выберите в контекстном меню команду **Свойства.**

2. В появившемся окне свойств на вкладке Общие нажмите кнопку Другие. Появится окно диалога Дополнительные атрибуты.

3. В группе **Атрибуты сжатия и шифрования** установите флажок **Шифровать содержимое для защиты данных** и нажмите кнопку «**Ок**».

4. Нажмите кнопку ОК в окне свойств зашифровываемого файла или папки, в появившемся окне диалога укажите режим шифрования: **только к этой папке или к этой папке и всем вложенным папкам и файлам.**

Внимание! *После выполнения этих действий файл с Вашей информацией будет автоматически зашифровываться. Просмотр его на другой ПЭВМ будет невозможен.*

b. Для выключения режима шифрования выполните следующие действия.

1. Выделите файл шифр.doc в папке **Мои документы**.

2. Нажмите правую кнопку мыши и выберите пункт **Свойства.**

3. На вкладке **Общие** нажмите кнопку **Другие.**

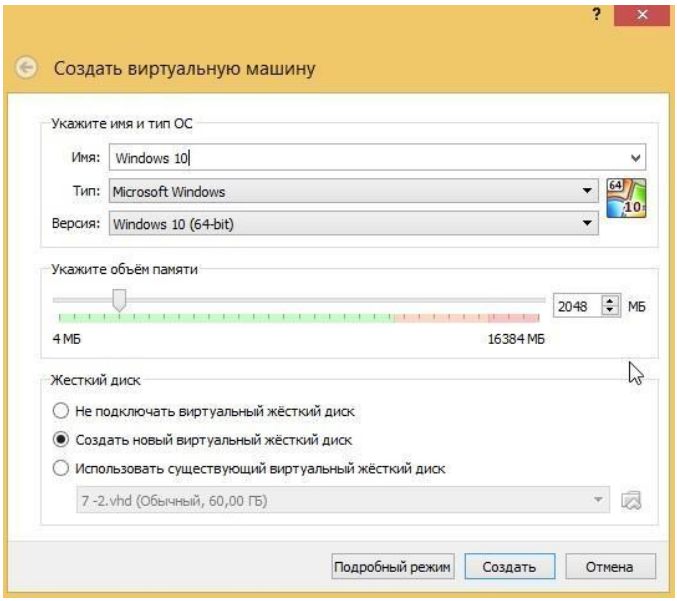
4. В открывшемся окне диалога в группе атрибуты сжатия и шифрования сбросьте флажок **Шифровать содержимое для защиты данных**.

Внимание! *После Выполнения тих действий файл с Вашей информацией не будет зашифровываться.*

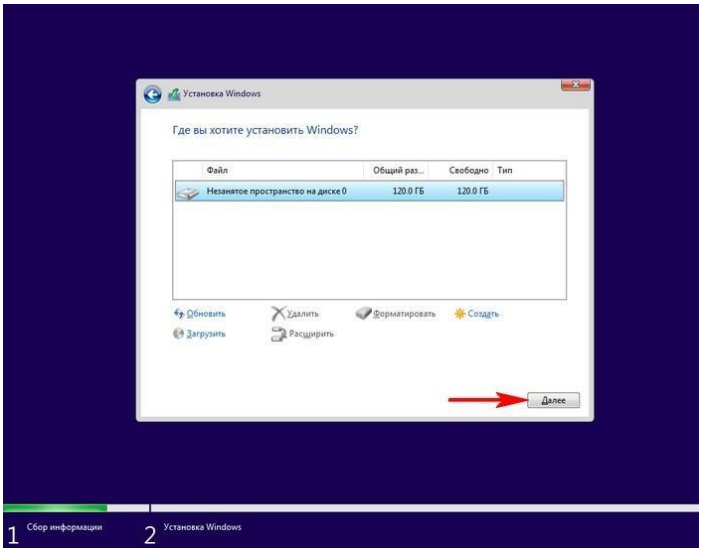
2.5 Практическая работа№ 5
Подготовка образа и среды предустановки Установка Windows ADK

Установим на наш компьютер виртуальную машину VirtualBox. Уверяю вас, способ с виртуальной машиной самый простой и использовать его для создания собственной сборки Windows сможет даже начинающий пользователь. Уверен, у большей части наших читателей она давно установлена. Ещё нам пригодиться USB-флешка объёмом не менее 8 Гб.

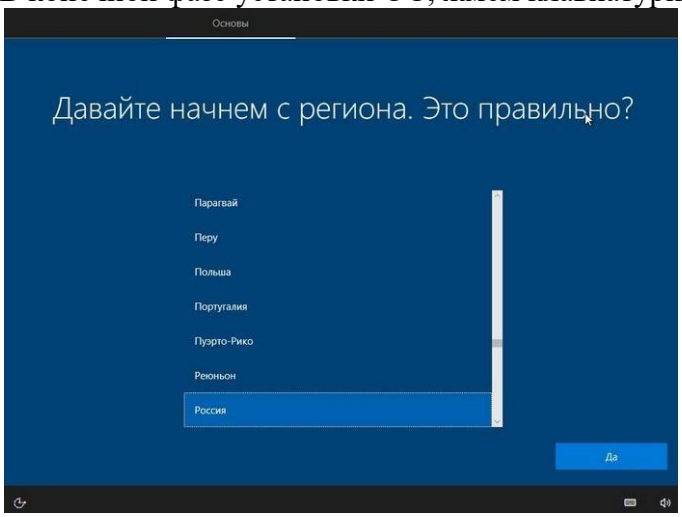
В VirtualBox создаём виртуальную машину Windows 10.



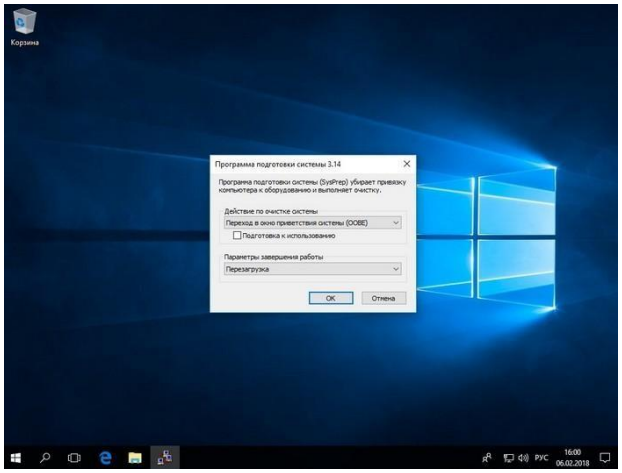
Загружаем виртуальную машину с ISO-образа Windows 10 и как обычно устанавливаем ОС на виртуалку.



В конечной фазе установки ОС, жмём клавиатурное сочетание Ctrl+Shift+F3.

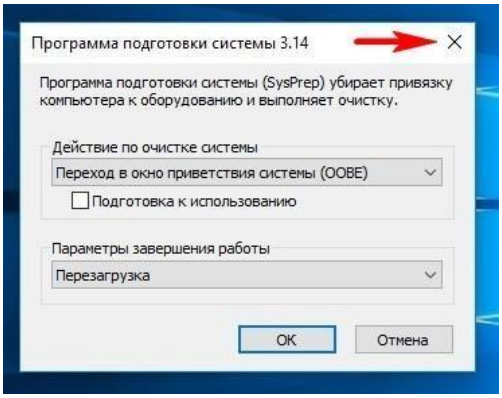


Операционная система переходит в режим аудита.



Можете нажать на крестик и закрыть данное окно (после установки всех необходимых программ мы откроем его снова). В режиме аудита вы можете устанавливать и

удалять программы, перезагружаться и завершать работу компьютера, одним словом экспериментируйте с Windows как хотите.

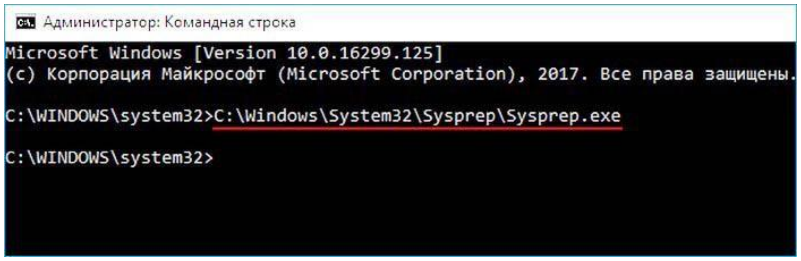


Устанавливаем все те программы, которые мы хотим иметь в дистрибутиве Win 10.

Программы устанавливаем, но не запускаем, нужно чтобы они не прописались в папке Appdata, которой не будет после sysprep.

После установки софта запускаем командную строку от имени администратора и вводим команду:

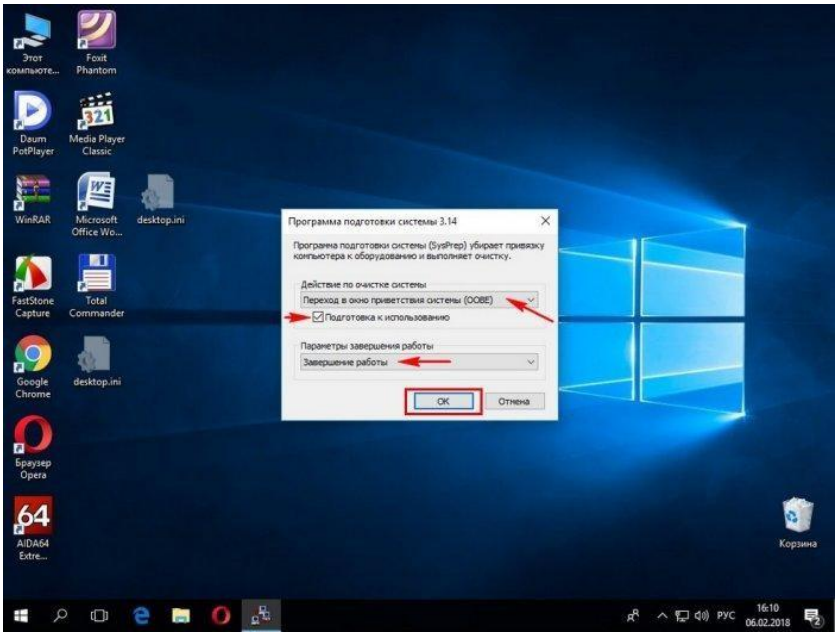
C:\Windows\System32\Sysprep\Sysprep.exe

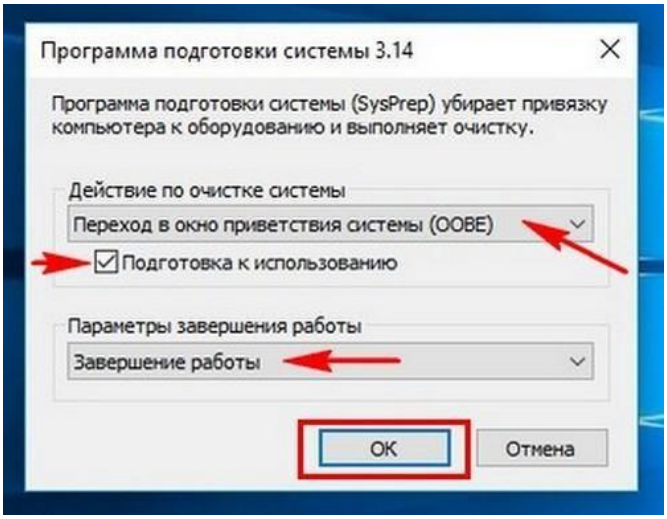


Запускается утилита "sysprep"

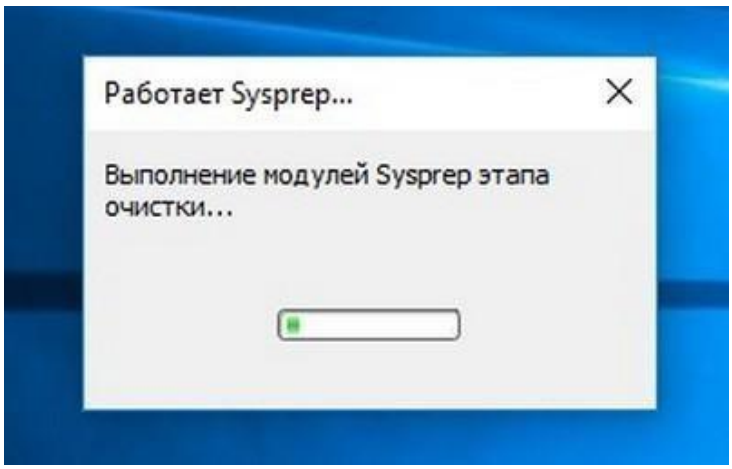
В появившемся окне с параметрами выставляем всё так, как на скришноте Перевод системы в режим (OOBE).

Отмечаем пункт - Подготовка к использованию. Завершение работы и нажимаем ОК.



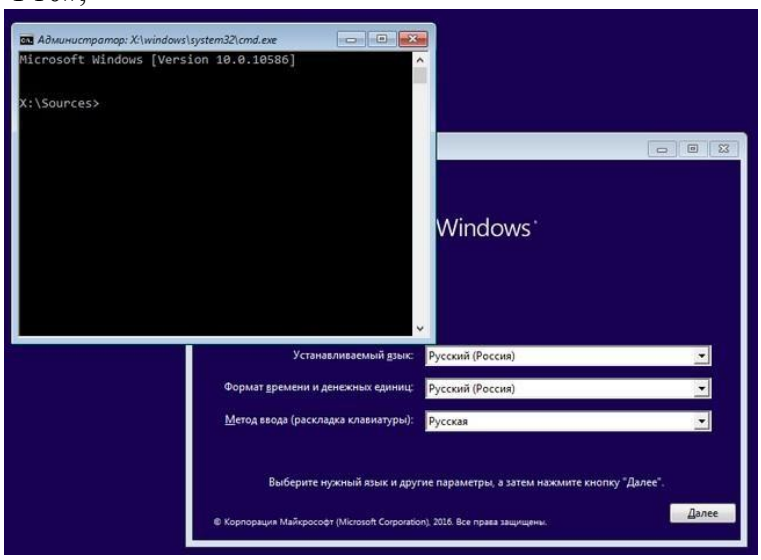


Windows 10 подготавливается утилитой "sysprep" несколько минут и затем виртуальная машина выключается.

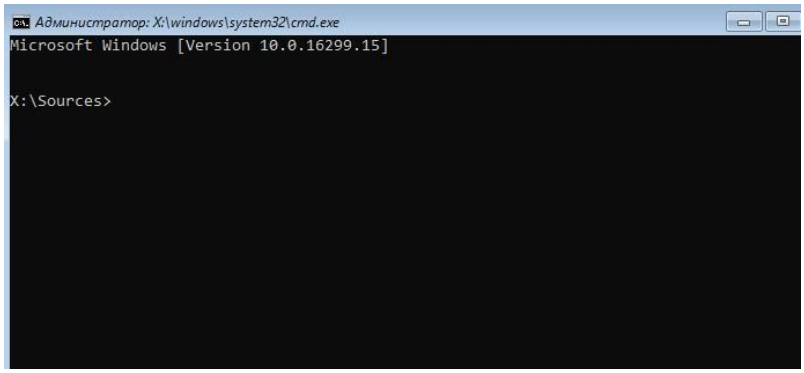


Опять загружаем виртуальную машину с ISO-образа Windows 10.

В начальном окне установки Windows 10 жмём клавиатурное сочетание «Shift+F10»,

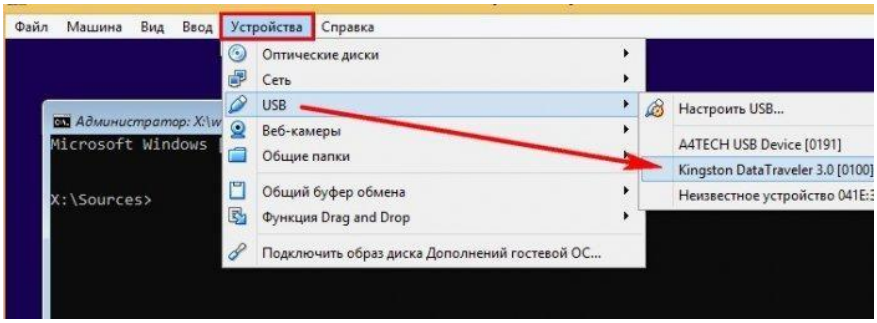


открывается командная строка Среды предустановки Windows PE.



На данном этапе подсоедините USB-флешку к вашему компьютеру.

Затем подключите USB-флешку к виртуальной машине. Устройства>USB выберите свою флешку.



в командной строке вводим команды:

diskpart

lis vol (данной командой выводим список разделов жёсткого диска, видим, что разделу с установленной Windows 10 присвоена буква диска C:, а USB-флешке буква (F:).

exit (выходим из DiskPart)

вводим следующую команду, которая произведёт захват диска (C:) с установленной Windows 10 в файл-образ формата ESD и сохранит его на USB-флешке (буква диска (F:).

Dism /Capture-Image /ImageFile:F:\install.esd /CaptureDir:C:\ /Name:Windows /compress:max где, install.esd: — это название будущего ESD-образа диска (C:)

с Windows 10.

F:\ — место сохранения ESD-образа. C:\ — раз-

дел с установленной Windows 10. сжатие

/compress:maximum (максимальное сжатие)

```
Microsoft Windows [Version 10.0.16299.15]


X:\Sources>diskpart

Microsoft DiskPart, версия 10.0.16299.15

(C) Корпорация Майкрософт (Microsoft Corporation).
На компьютере: MINWINPC
```

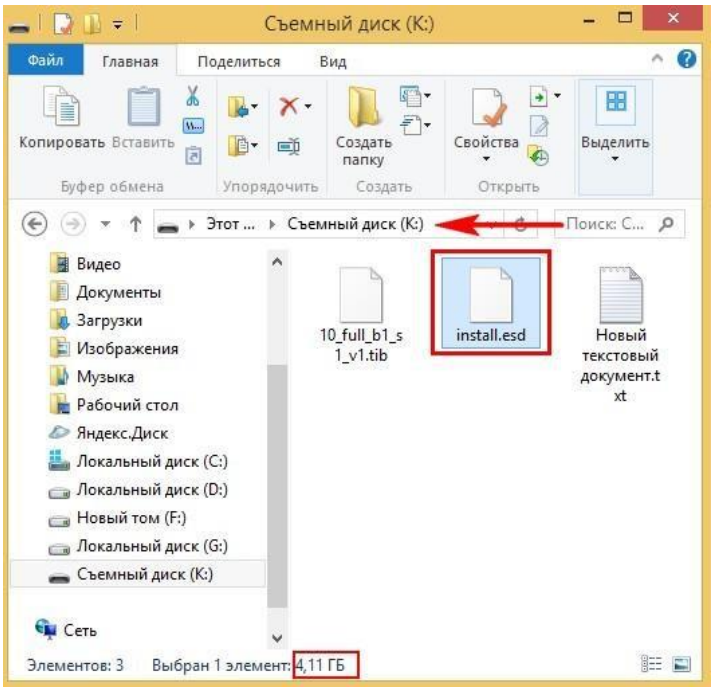
```
DISKPART> lis vol

  Том    ###  Имя  Метка        ФС     Тип         Размер   Состояние  Сведения
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
    Том 0     E   ESD-ISO      UDF    CD-ROM      3468 Мб  Исправен
    Том 1     C                NTFS   Раздел       119 Gб  Исправен
    Том 2     D   Восстановит  NTFS   Раздел       499 Мб  Исправен   Скрытый
    Том 3                      FAT32  Раздел       100 Мб  Исправен   Скрытый
    Том 4     F                NTFS   Сменный       29 Gб  Исправен

DISKPART> exit

Завершение работы DiskPart...

X:\Sources>Dism /Capture-Image /ImageFile:F:\install.esd /CaptureDir:C:\ /Name:Windows
/compress:max

Система DISM
Версия: 10.0.16299.15

Сохранение образа
[==========================100.0%==========================]
Операция успешно завершена.

X:\Sources>_
```

Выключаем виртуальную машину.

Создание дистрибутива Windows 10

В итоге всех вышеприведённых манипуляций мы имеем на нашей флешке файл install.esd (размер 4.11 Гб), содержащий файлы операционной системы Windows 10 с предустановленным программным обеспечением и следующим шагом нам нужно собрать на основе его дистрибутив Win 10.

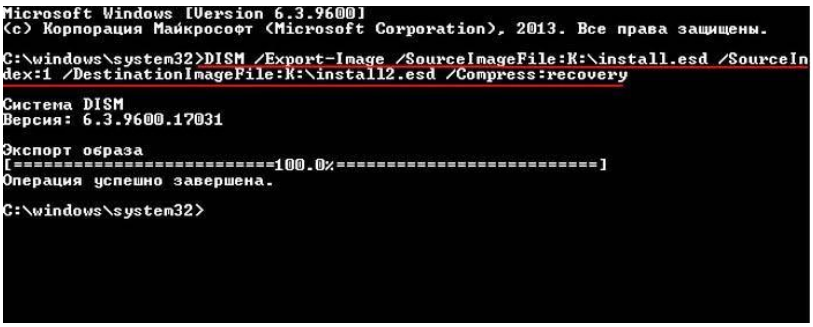
Виртуальную машину мы выключили и теперь в основной операционной системе наша флешка имеет букву диска (K:). На флешке находится файл install.esd размером 4.11 Гб.



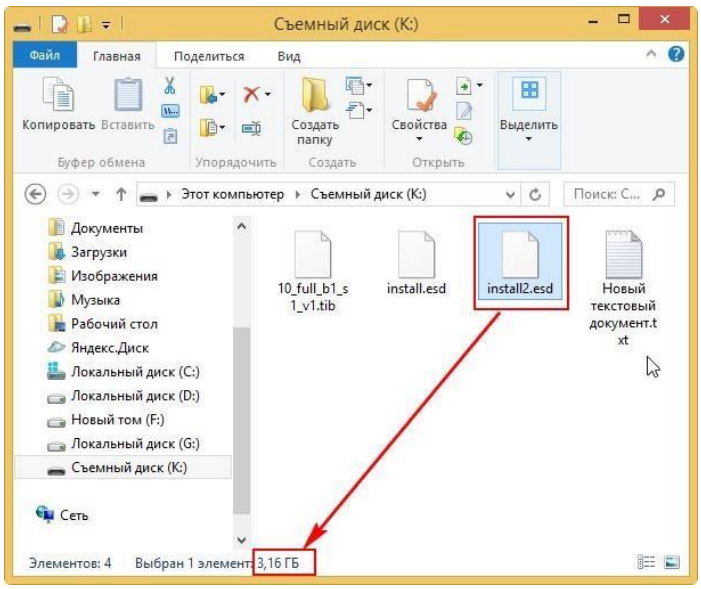
Compress:recovery

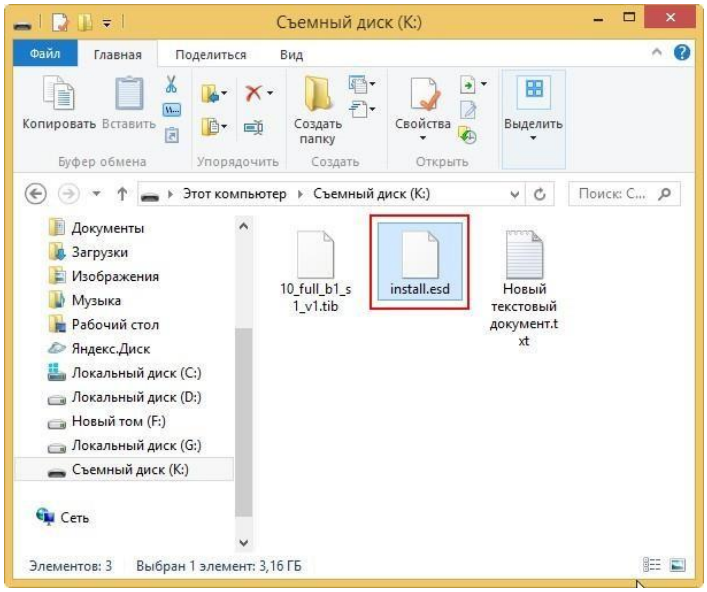
Ещё больше сожмём файл-образ Windows 10 - install.esd командой (делать это необязательно, просто я хочу дополнительно уменьшить образ Win 10)

Dism /Export-Image /SourceImageFile:K:\install.esd /SourceIndex:1 /DestinationImageFile:K:\install2.esd /Compress:recovery где K:, это буква нашей флешки с файлом install.esd. То есть, этой командой мы создаём ещё один файл этого образа с именем файла install2.esd и сжатием recovery. Или умными словами - конвертируем файл install.esd в новый файл install2.esd, применив новый тип сжатия Compress:recovery (сжатие архива обычно называют конвертированием).



Теперь на флешке (K:) появляется второй файл-образ Windows 10 - install2.esd размером 3,1 Гб. Первый файл install.esd 4,11 Гб удаляем, а второй файл install2.esd 3,1 Гб переименовываем в install.esd. Итого, на переносном винчестере USB (диск K:) находится один файл install.esd размером 3,1 Гб.

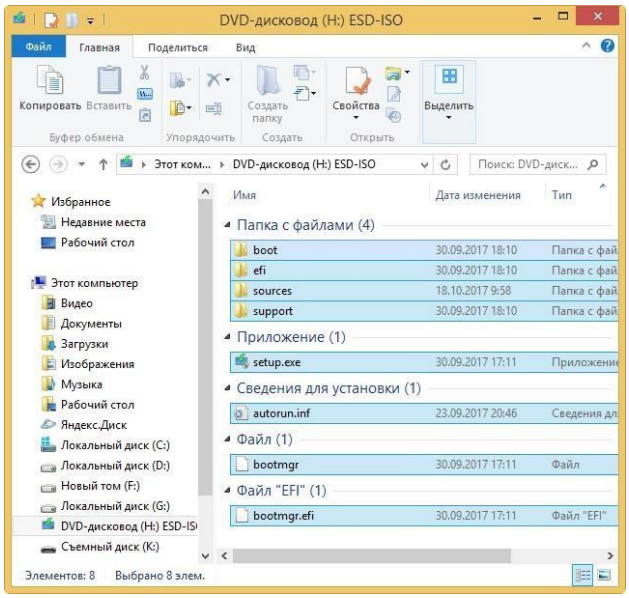




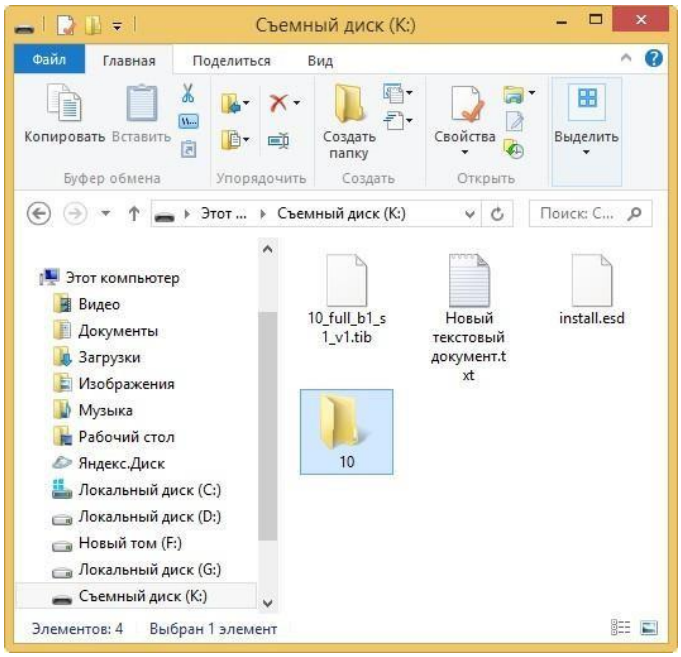
Собираем ISO-образ Windows 10 с новым файлом install.esd

Скачиваем ISO-образ Windows 10

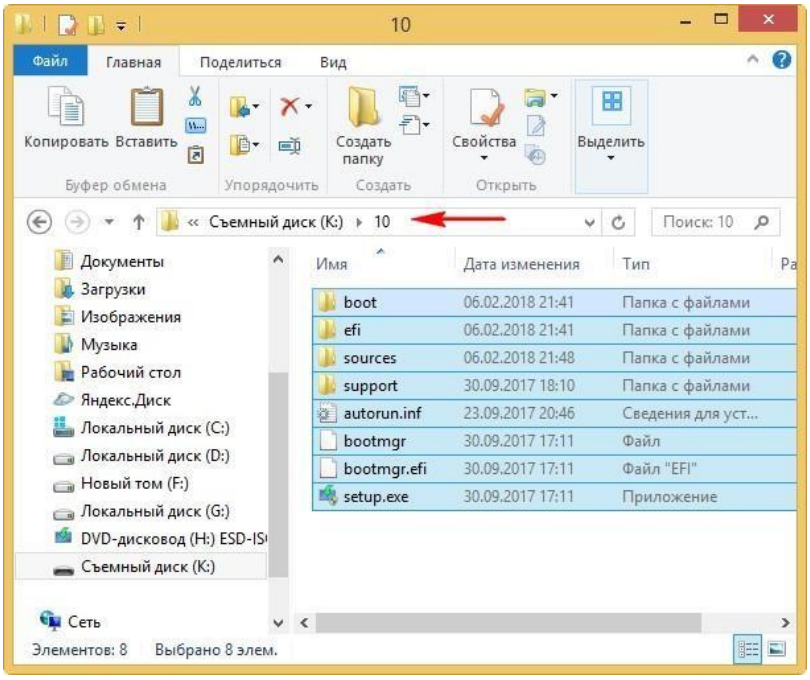
открываем его (подсоединяем к виртуальному дисководу) и копируем его содержимое.



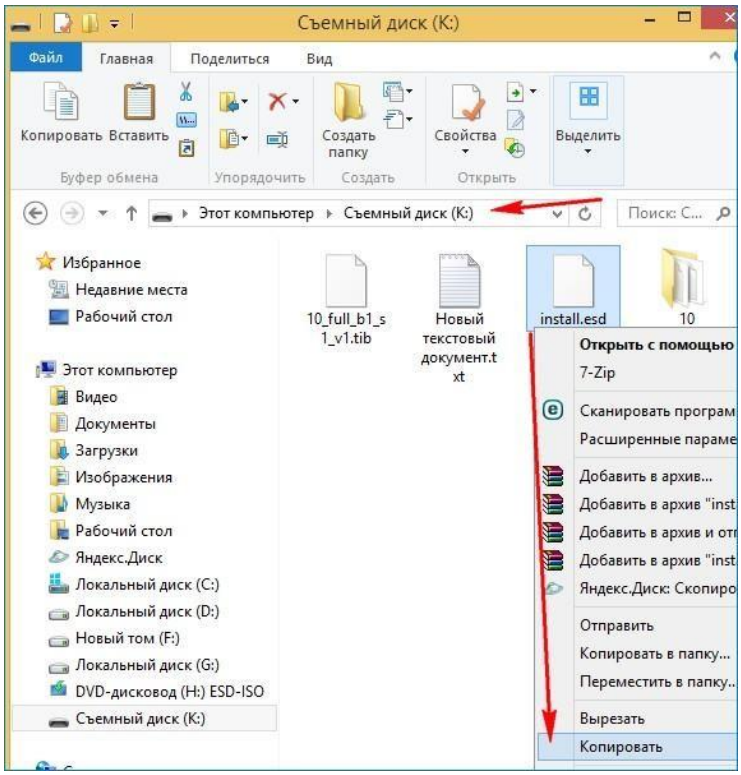
Затем создаём папку на флешке (K:) и называем её 10.



Вставляем в неё скопированное содержимое ISO-образа Windows 10.

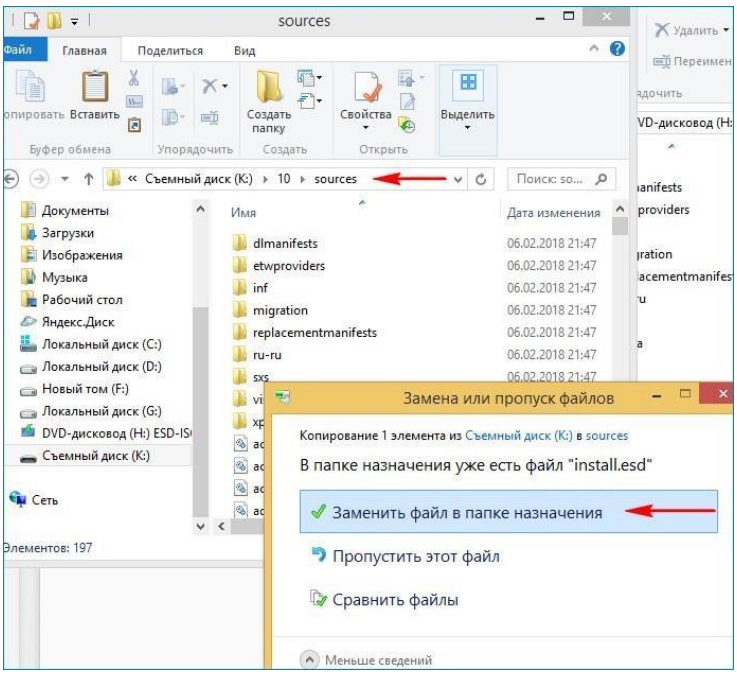


После того, как файлы скопировались, заходим на диск (K:) и копируем файл install.esd.

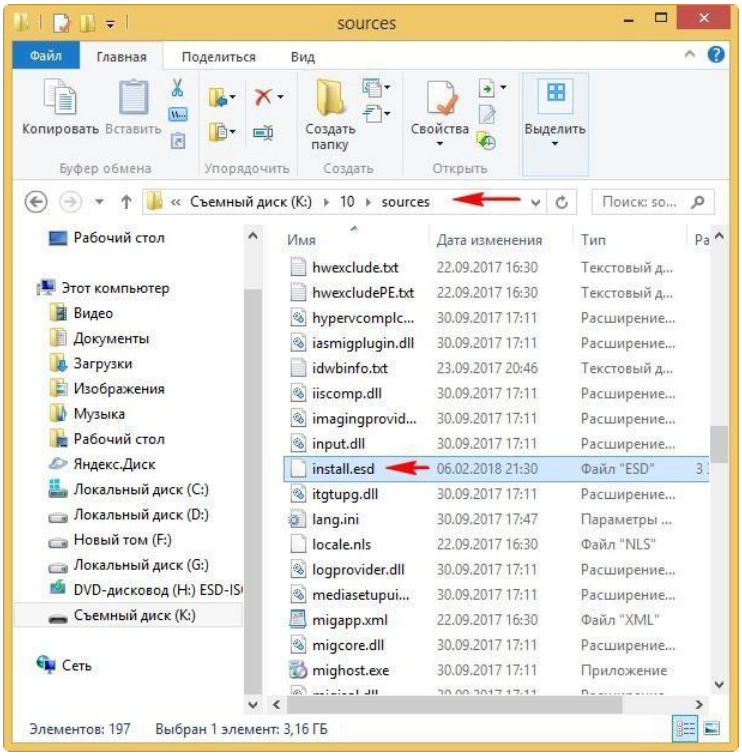


Заходим в папку K:\10\sources, щёлкаем правой мышью и выбираем Вставить.

Выбираем Заменить файл в папке назначения.



Оригинальный файл install.esd из дистрибутива Windows 10 заменён нашим файлом install.esd, содержащим программное обеспечение.



Комплект средств для развертывания Windows (Windows ADK)

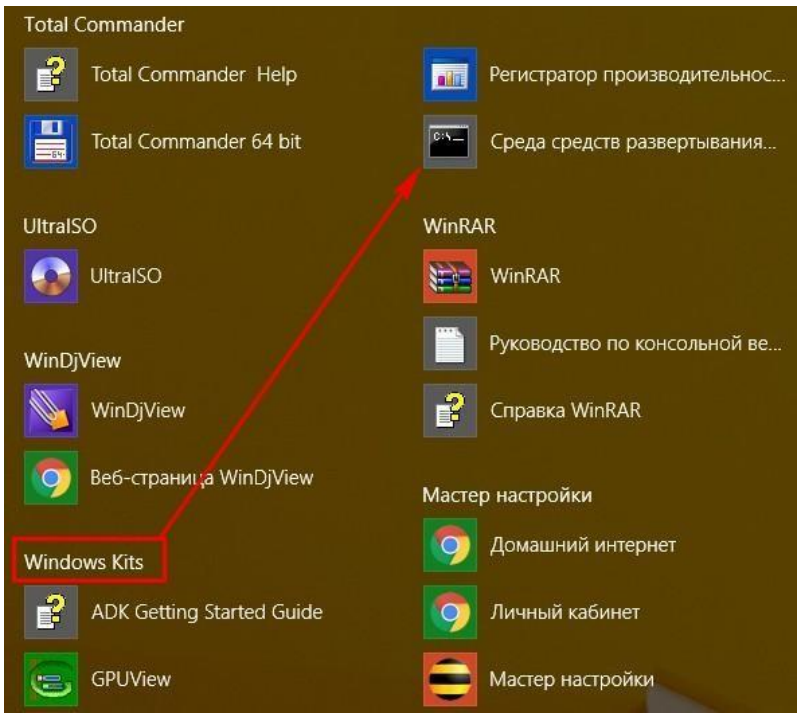
Нам осталось превратить папку 10 с файлами Windows 10 в установочный ISOдистрибутив с предустановленным программным обеспечением.

Если Вы опытный пользователь, то наверняка на вашем компьютере установлен Комплект средств для развертывания Windows (Windows ADK), если нет, то скачайте его по ссылке и установите.

Для Windows 8.1
https://www.microsoft.com/ru-ru/download/details.aspx?id=39982

Для Windows 10 https://developer.microsoft.com/ru-ru/windows/hardware/windows-assessment-
deployment-kit

После установки запускаем среду средств развёртывания и работы с образами.



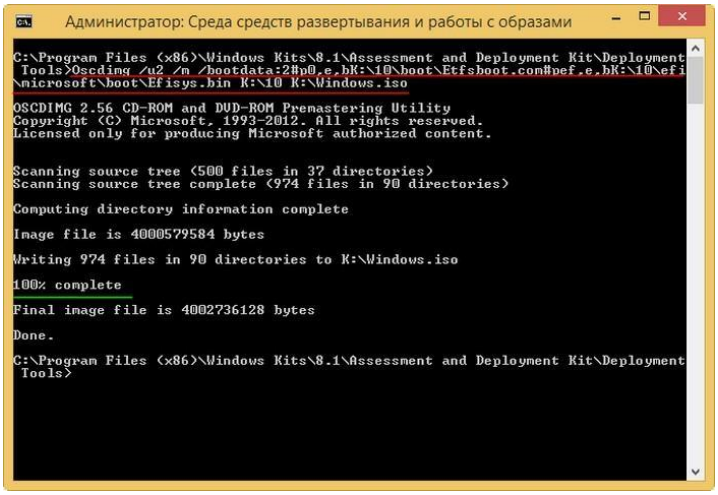
вводим команду:

Oscdimg /u2 /m /bootdata:2#p0,e,bK:\10\boot\Etfsboot.com#pef,e,bK:\10\efi\microsoft\boot\Efisys.bin K:\10 K:\Windows.iso где: u2, это файловая система UDF, а m - размер образа без ограничений.

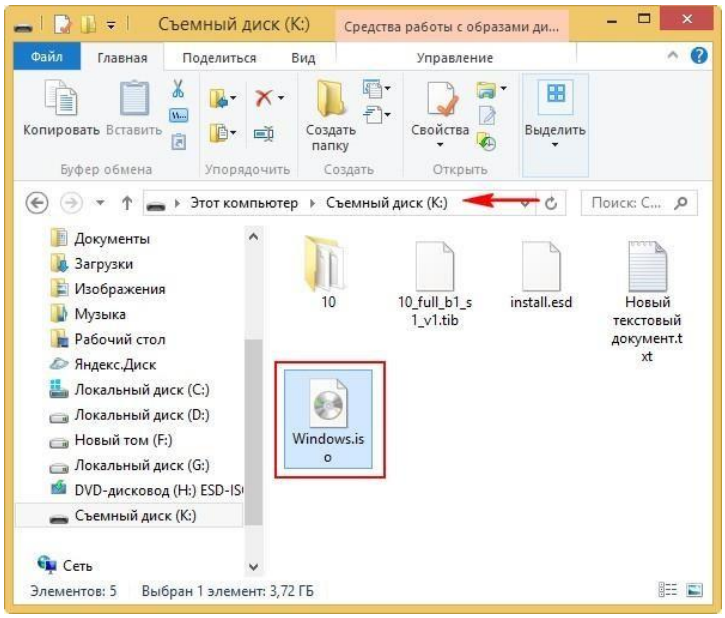
b - загрузочный сектор записать etfsboot.com, путь к файлу etfsboot.com при указании b(boot) пишется без пробела bI:\10\boot\etfsboot.com

bK: - где K: - буква диска.

K:\10 - создать ISO-образ из файлов и папок, находящихся на разделе K: в папке 10 K:\Windows.iso - созданный образ Win 10 разместить на разделе K:. присвоить имя образу Win 10 - Windows.



Дистрибутив Windows.iso на флешке (K:) готов.



Создание загрузочной флешки

Предлагаю создать загрузочную флешку Windows 10 программой WinSetupFromUSB, с помощью неё можно создать универсальную флешку, с помощью которой получится установить Windows 10 на новый ноутбук с БИОСом UEFI, а также на простой компьютер с обычным БИОС. Подробно на этом останавливаться мне бы не хотелось, всё очень хорошо описано в этой статье.

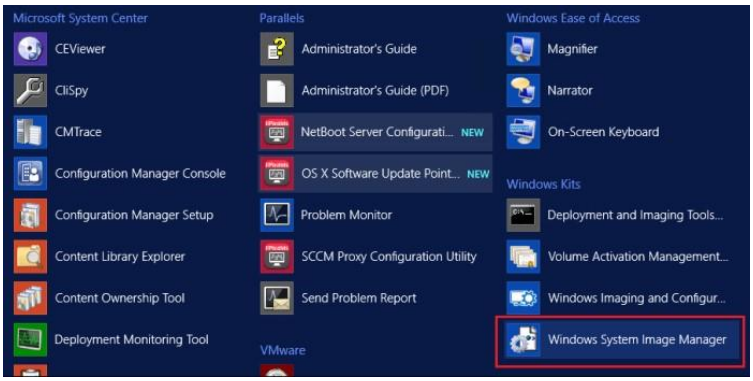
Установка Windows 10

Процесс установки собственного дистрибутива Windows 10 ничем не отличается от обычного процесса установки описанного в этой статье. Установить такую сборку вы можете на любой компьютер. Когда Windows 10 установится, то все программы будут тоже установлены.

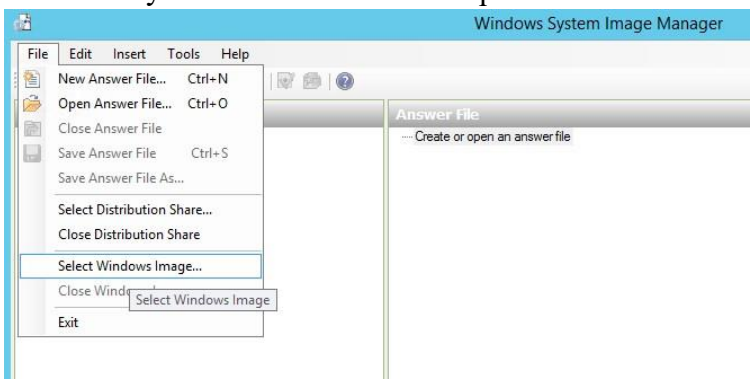
2.7 Практическая работа№ 6
Создание эталонного образа с помощью Windows SIM и Sysprep Создание файла ответов с помощью Windows SIM

Задание:

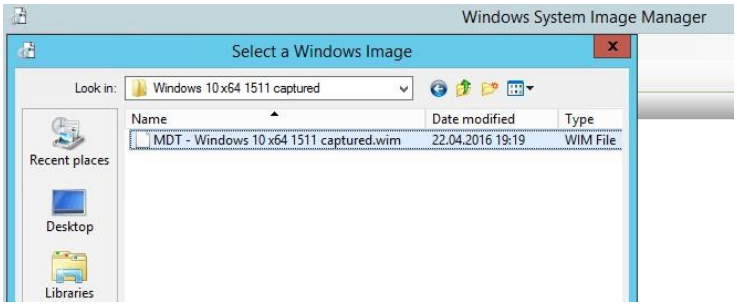
Открываем Windows Assessment and Deployment Kit (Windows ADK).



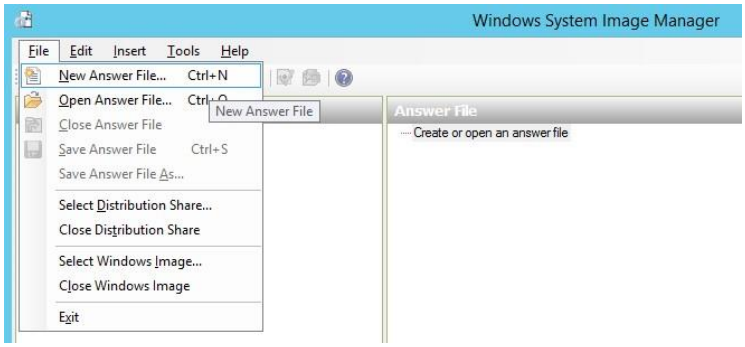
После запуска Windows SIM выбираем Select Windows Image



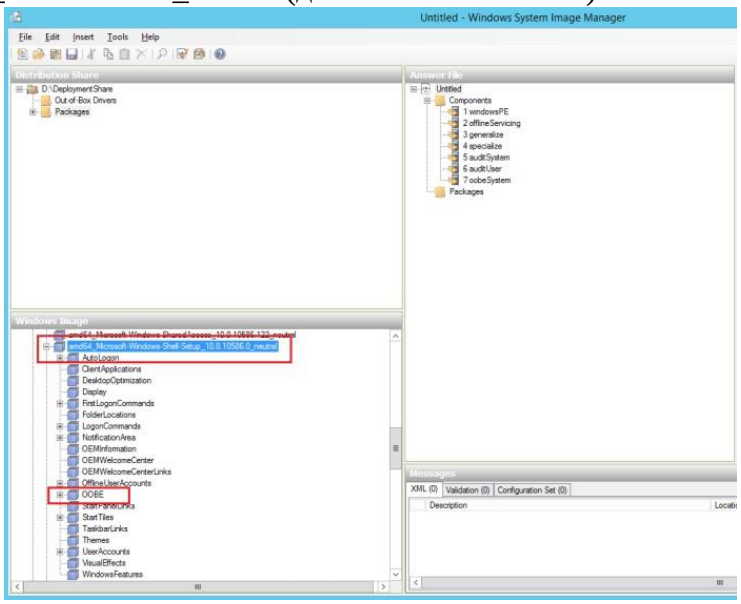
Можно взять wim файл с Windows 10 media (с диска/iso) или захваченный WIM файл Windows 10. Если вы это делаете первый раз, то получите сообщение о «Catalog File being missing», ничего страшного, соглашаемся и ждем пока он будет создан.



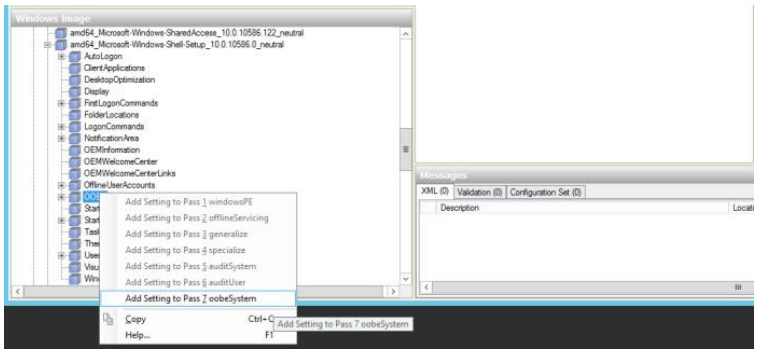
Из меню выберем New Answer File



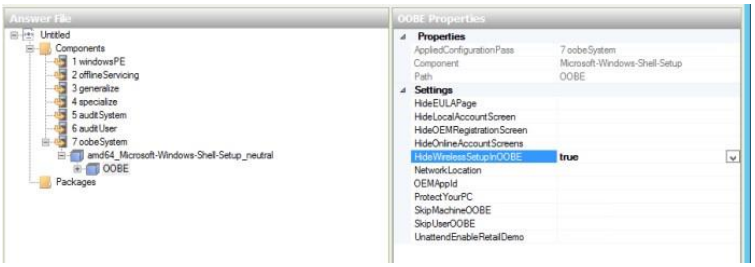
В разделе Windows Image, разворачиваем Components и ищем amd64_MicrosoftWindows-Shell-Setup_6.2.9200.16384_neutral (для Windows 8.1) и amd64_MicrosoftWindows-Shell-Setup_10.0.10586.0_neutral (для Windows 10 1511).



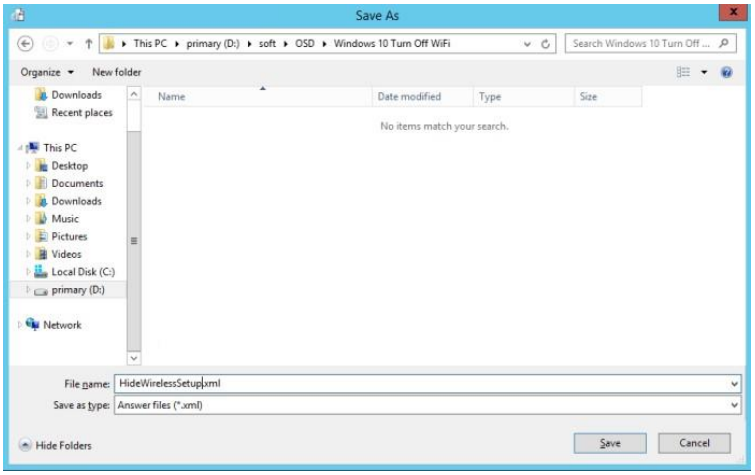
Правой кнопкой по разделу OOBE и выбираем Add Setting to Pass 7 oobeSystem



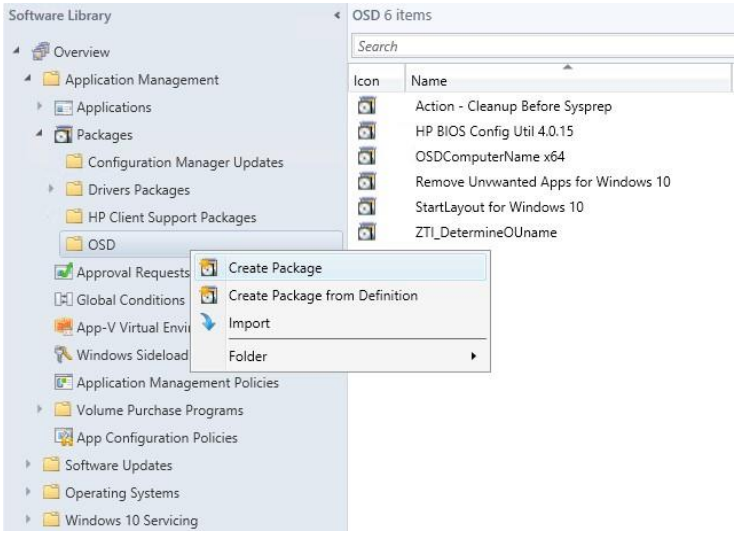
Нас интересует значение HideWirelessSetupInOOBE в значении true, это настройка и спрячет не нужный нам экран



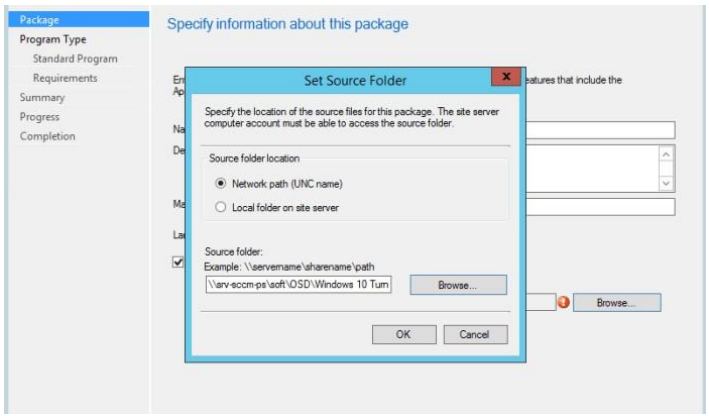
Далее, сохраняем файл ответов, чтобы создать пакет в SCCM



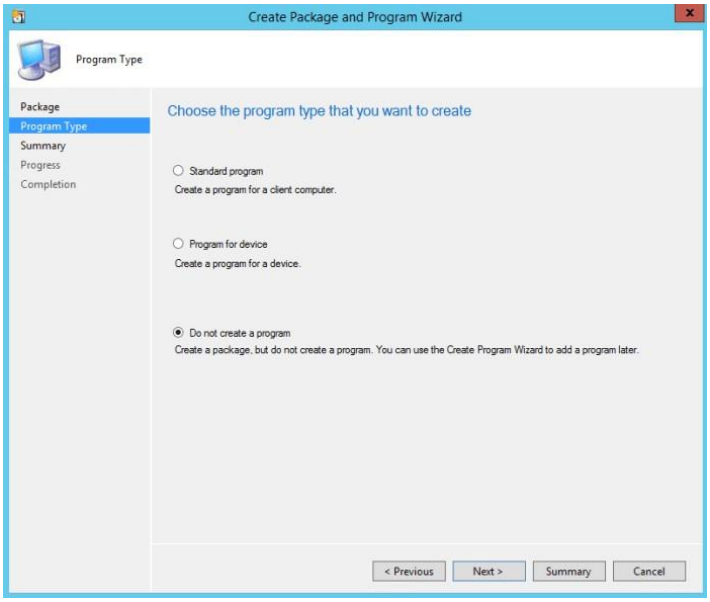
Создаем пакет (Create Package) в SCCM, чтобы в дальнейшем его использовать в последовательности задач с Windows 10



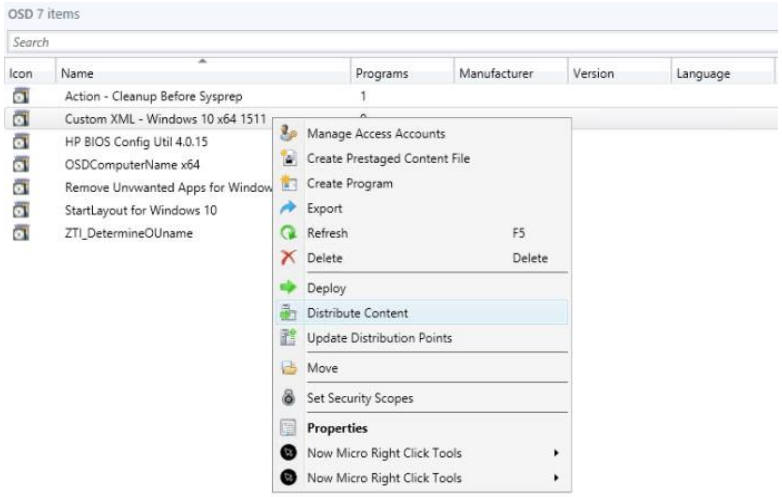
Указываем путь до папки с xml файлом



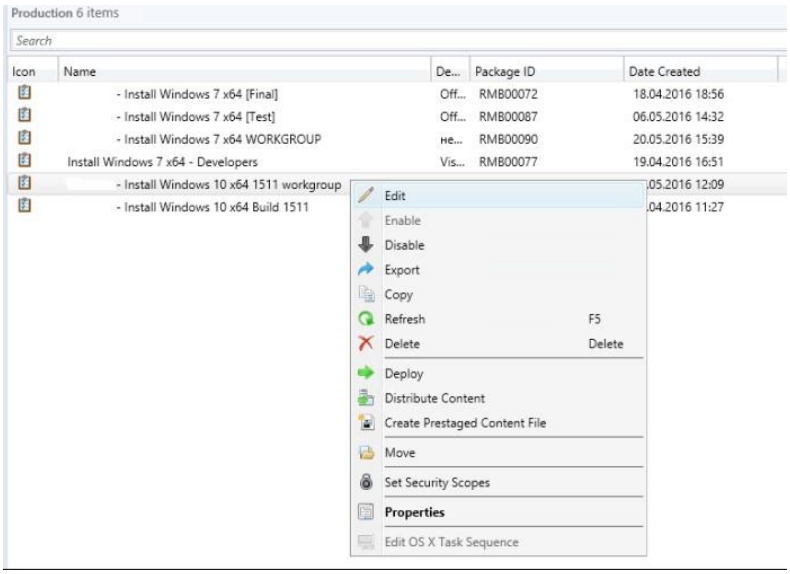
Выбираем опцию Do not create a program, т.к. внутри мы ничего устанавливать не будем



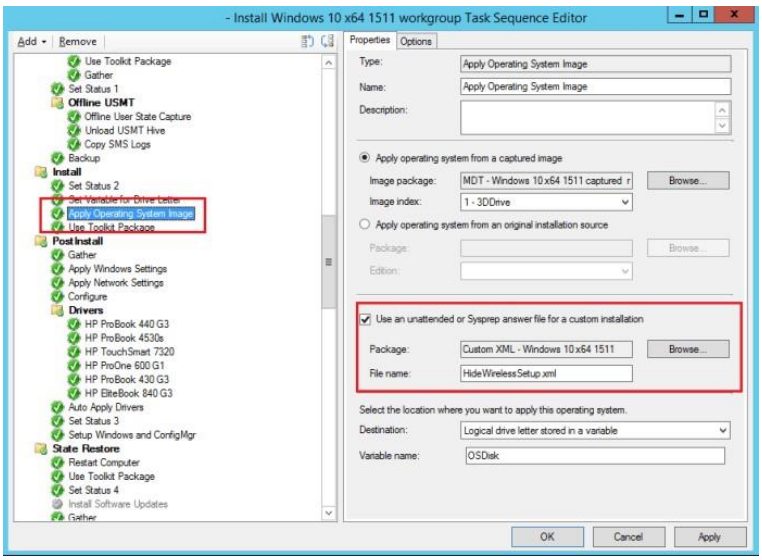
И обязательно не забываем выполнить доставку пакета (Distribute Content) на точку распространения



Теперь пора добавить этот пакет внутрь последовательности задач



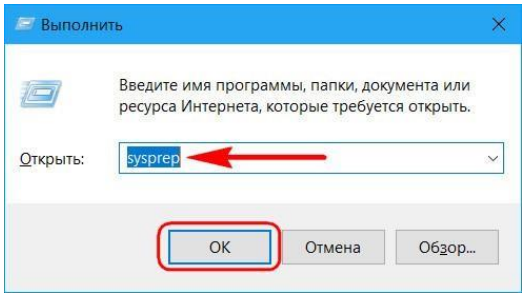
Нас интересует шаг Apply Operating System Image и раздел с файлом автоответа. Через Browse выбираем пакет, которой только что создали и в поле File Name указываем имя xml файла.



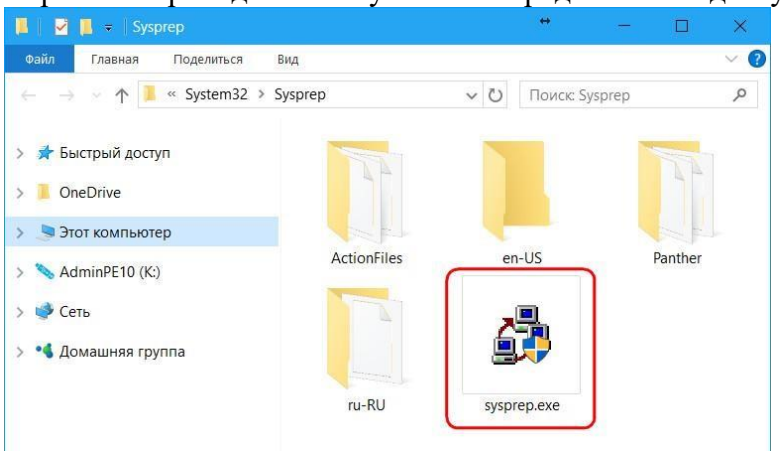
Всё.

Запуск утилиты

Запуск Sysprep проще всего осуществить с помощью команды Win+R.

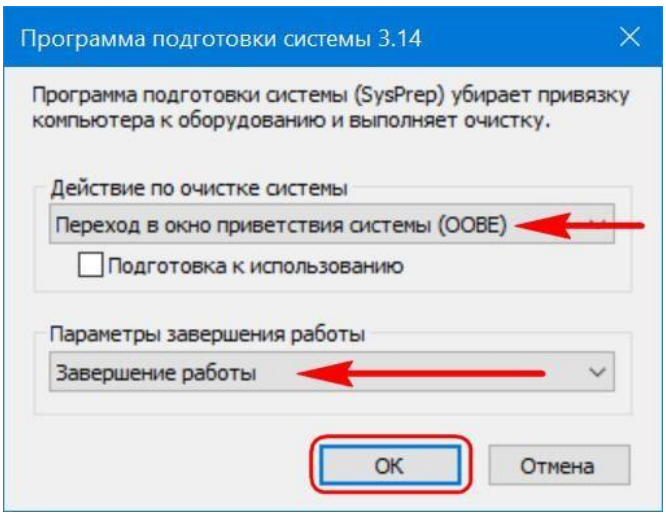


Таким образом в проводнике получим непосредственный доступ к файлу её запуска.



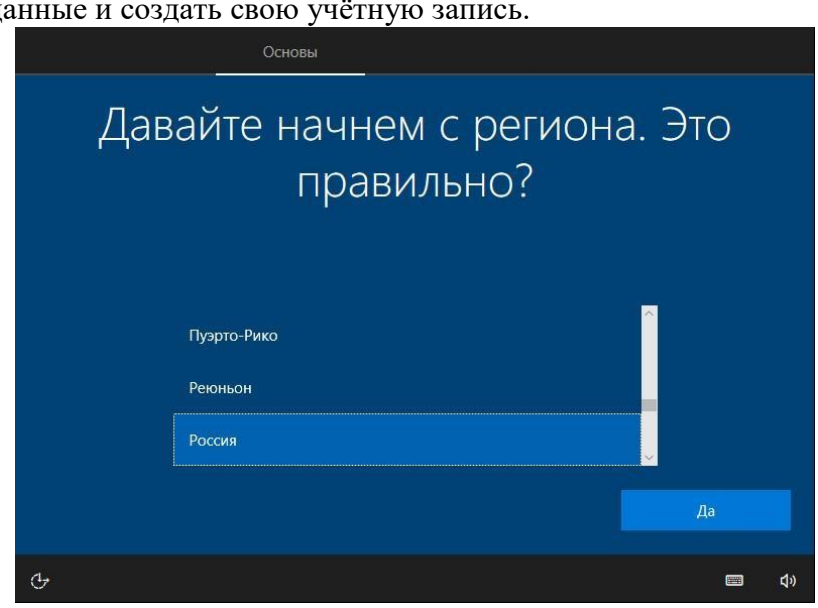
Отвязка от комплектующих

Чтобы отвязать Windows от текущих комплектующих перед их заменой или созданием бэкапа системы для переноса на другое устройство, используем «Переход в окно OOBE» и выбираем завершение работы.

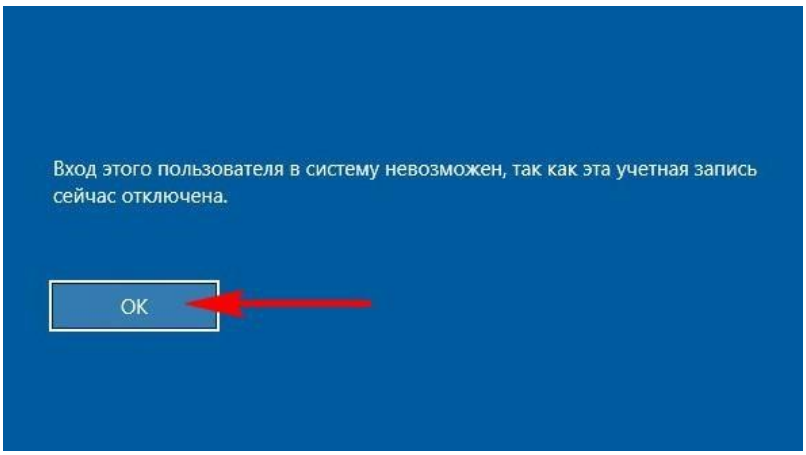


При таком раскладе утилита осуществит только сброс драйверов комплектующих. Если же выставить галочку опции «Подготовка к использованию», будет проведён ряд мероприятий для передачи системы новому пользователю - чистка системного журнала и временных файлов, удаление точек восстановления, обнуление SID, сброс активации и т.п.

Утилита выполнит свою работу, и компьютер выключится. Далее можно приступать к тем или иным действиям – менять комплектующие, бэкапить систему с загрузочного носителя. С новым включением – как на исходном устройстве, так и на том, куда система переносилась с помощью восстановления из бэкапа – сначала будем лицезреть, как устанавливаются драйверы на новые комплектующие, а затем попадём в окно OOBE. Окно OOBE - это не что иное, как экран приветствия системы, который мы обычно видим на завершающем этапе установки Windows, где нужно указать региональные данные и создать свою учётную запись.



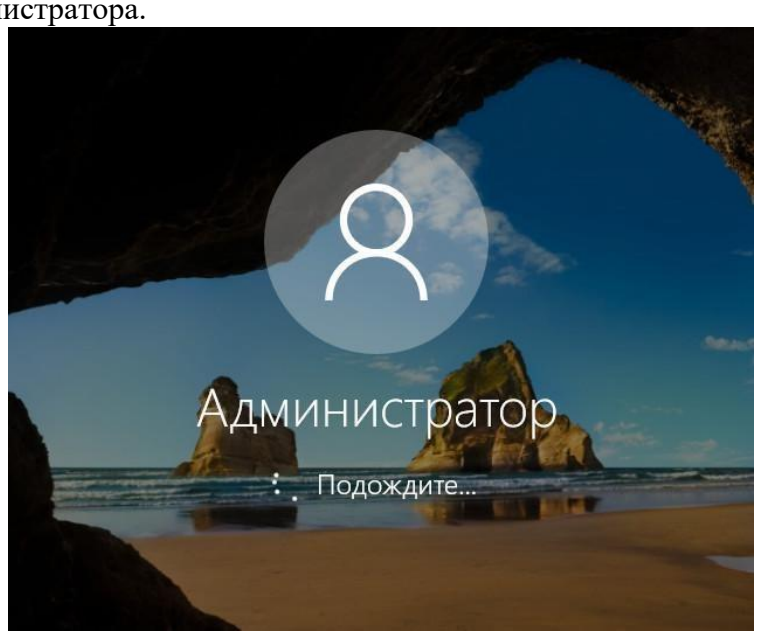
И поскольку при замене комплектующих или восстановлении Windows на других компьютерах в создании новой учётной записи нужды нет, спокойно можем сбросить этот процесс клавишами Ctrl+Shift+F3. Это клавиши входа в скрытую учётную запись администратора. Система попробует подгрузить её, но в доступе откажет. Жмём «Ок».



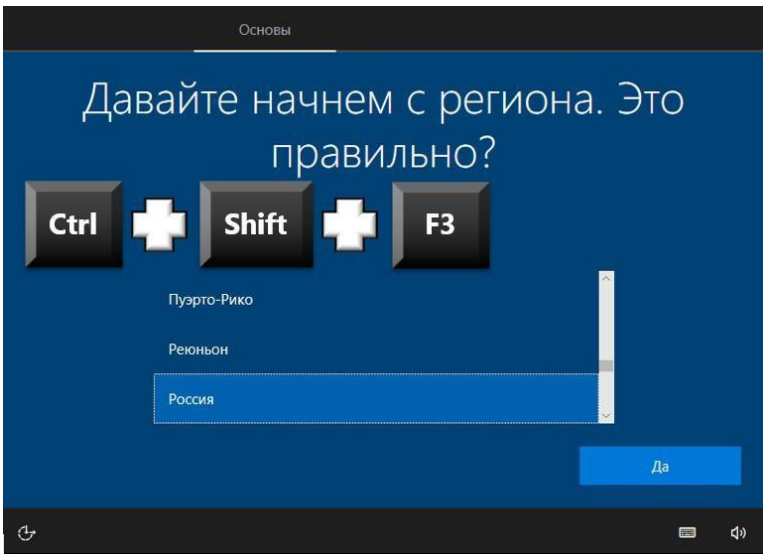
И после перезапуска увидим привычный экран блокировки со всеми существующими учётными записями.

Режим аудита

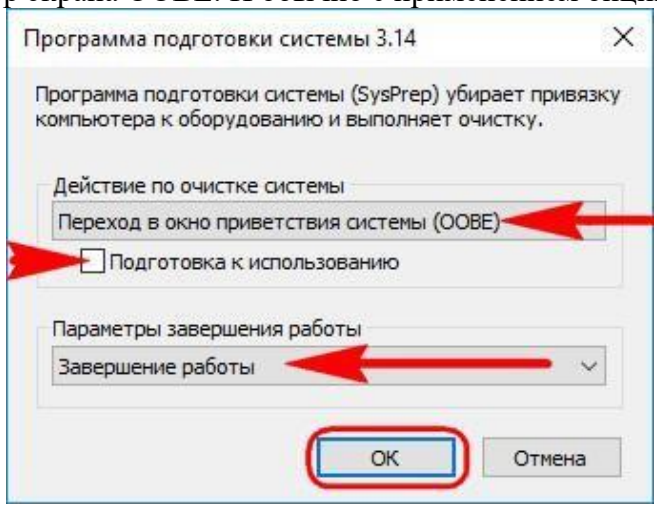
Режим аудита предоставляет возможность получить доступ к среде Виндовс без создания учётной записи конкретного пользователя, в режиме упомянутой учётной записи администратора.



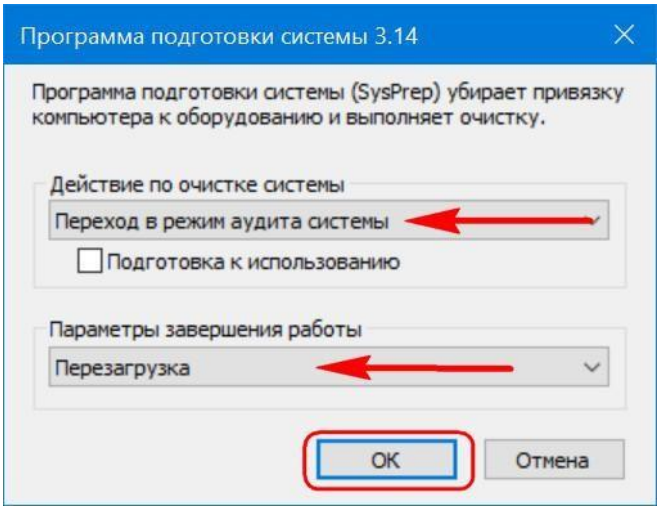
В этом режиме, собственно, и проводится OEM-производителями и IT-специалистами компаний настройка эталонного образа системы с нужными драйверами, параметрами и внедрённым софтом. Первичный вход в режим аудита выполняется на этапе установки Windows - той, что впоследствии должна стать эталонным образом, и на которой не должно существовать никаких пользовательских учётных записей и идентифицирующих данных. После этапа подготовки устройств попадём на завершающий этап установки системы, начинающийся с задания региональных настроек. И здесь жмём клавиши Ctrl+Shift+F3.



После перезагрузки попадём в режим аудита. Последний загружается с по умолчанию запущенным окном Sysprep для удобства. Вот, собственно, в таком режиме и можно приступать к модификации Windows. Если в процессе внесения правок в систему, например, при установке определённого софта потребуется перезагрузка, всё, что нужно сделать – это закрыть окно утилиты. И осуществить перезагрузку привычным образом. После перезагрузки система вновь запустится в режиме аудита. Завершается работа в этом режиме так, как было рассмотрено в предыдущем пункте статьи – выбором в окне Sysprep экрана OOBE. И обычно с применением опции подготовки к использованию.



Эталонную модифицированную Windows обычно делают с чистой, только что установленной системы. Но возможен вариант создания эталона на базе наработанной системы. Для этого внутри рабочей Виндовс необходимо запустить Sysprep и выбрать в её окне переход в режим аудита. Завершающий работу параметр - перезагрузка.

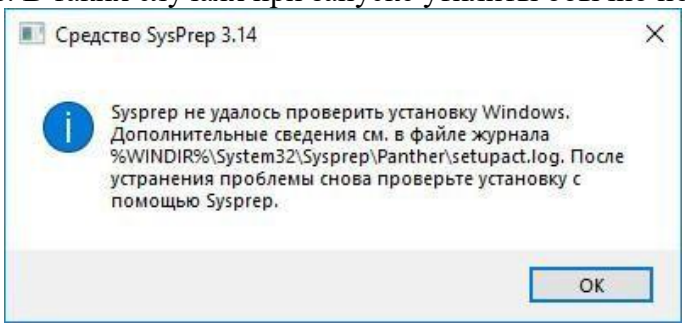


Войдя в режим аудита, можем удалить учётные записи тех пользователей, которые досе-ле работали с системой, донастроить что нужно, а затем выполнить отвязку от комплек-тующих (и при необходимости от идентифицирующих данных) с переходом в окно OOBE.

Вот только не с каждой рабочей системы удастся сделать эталонный образ. У этого ме-ханизма есть свои ограничения.

Решение проблем с запуском Sysprep

Sysprep, увы, не сработает, если Windows была не установлена начисто, а обновлена с предыдущей версии, клонирована или восстановлена из бэкапа, созданного на другом железе. В таких случаях при запуске утилиты обычно получим такое вот уведомление.



В таком случае можно кое-что предпринять, правда, без гарантированного успеха во всех 100% случаев.

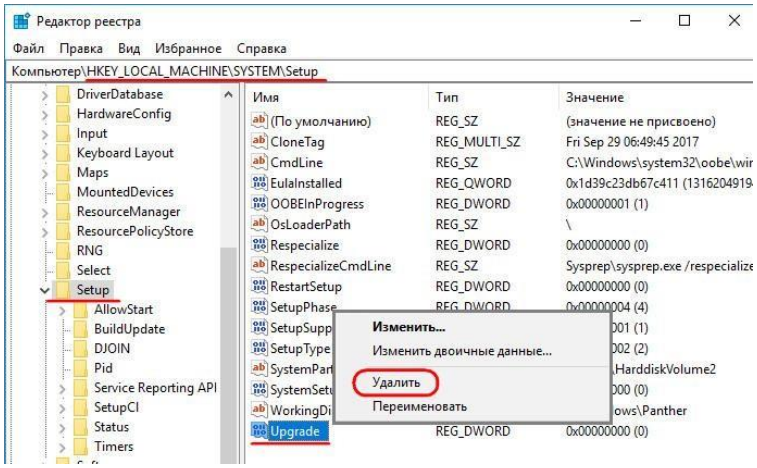
Создаём бэкап системы или хотя бы запасаемся точкой восстановления, поскольку далее будем работать с системным реестром.

Запускаем его.

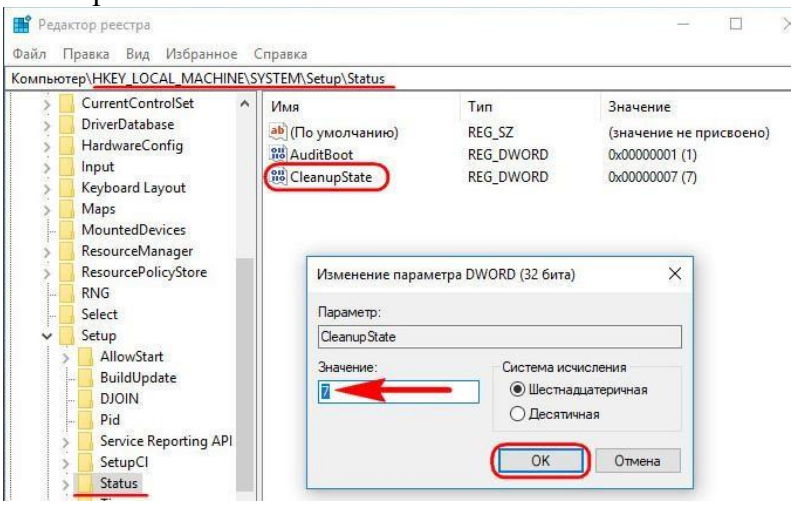
Раскрываем путь:

HKEY_LOCAL_MACHINE\SYSTEM\Setup

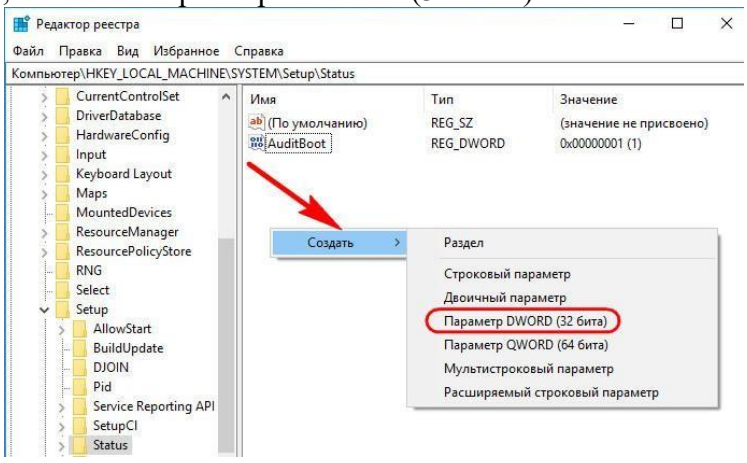
Если система обновлялась с предыдущей версии, в первую очередь в самом каталоге «Setup» удаляем параметр ~~«Upgrade»~~.



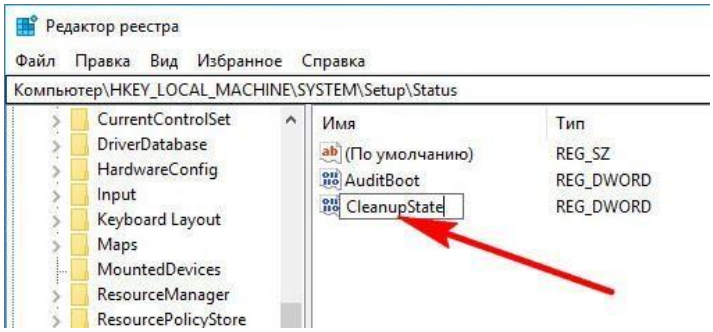
Затем раскрываем каталог «Setup», кликаем подкаталог «Status», здесь нам нужен параметр «CleanupState». Устанавливаем его значение 7.



Если такого параметра нет, создаём его. В контекстном меню окна реестра жмём «Создать», затем – «Параметр DWORD (32 бита)».



Даём имя параметру «CleanupState».

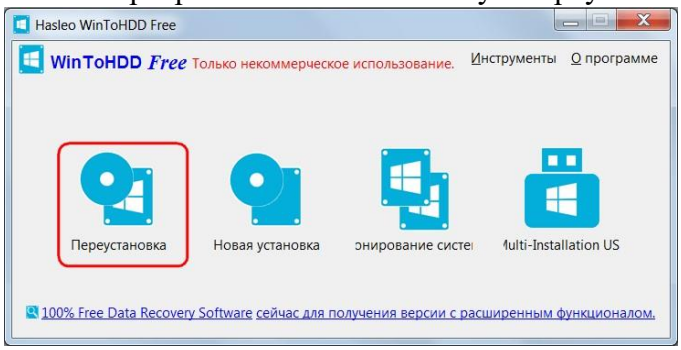


Устанавливаем его значение 7. После перезагрузки снова пробуем запустить Sysprep.

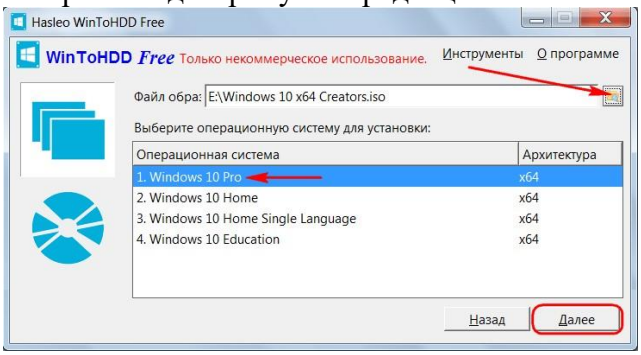
2.7 Практическая работа№ 7
Создание и обслуживание эталонного образа

Задание:

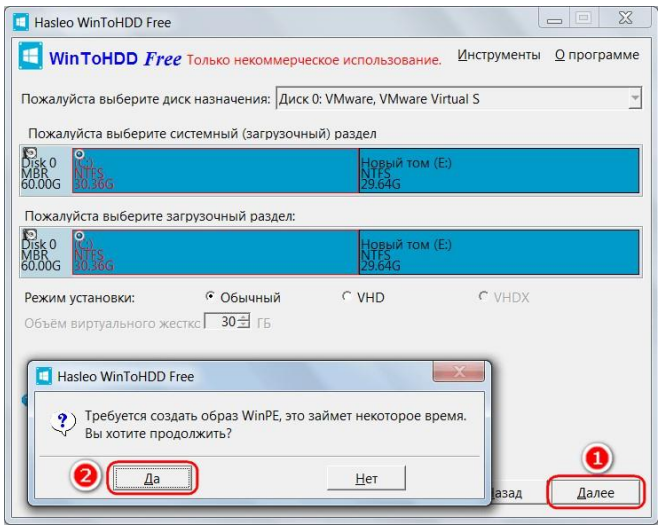
В окне программы кликаем кнопку «Переустановка».



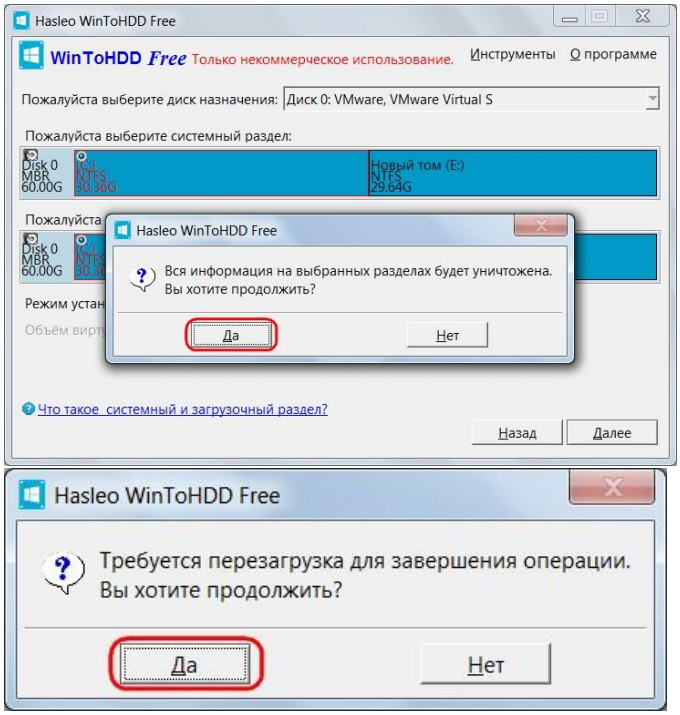
С помощью обзорной опции указываем путь к образу, в окошке ниже выбираем доступные в конкретном дистрибутиве редакции Windows. Жмём «Далее».



Следующее окошко является универсальным для всех операций, проводимых программой, оно предполагает выбор дисков и разделов новой системы. Однако в случае с переустановкой выбор уже предопределён. Ничего не меняем, просто жмём «Далее» и подтверждаем операцию в следующем диалоговом окошке.



Затем ещё раз даём добро на старт процесса и соглашаемся на перезагрузку.



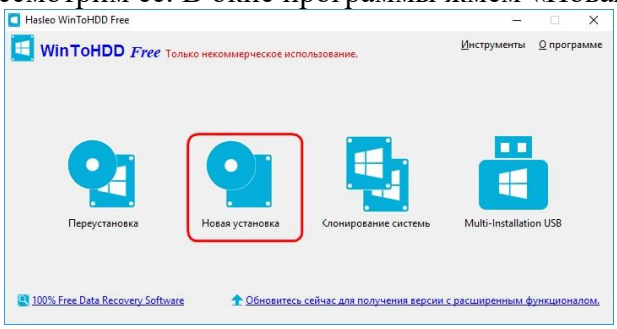
После перезагрузки компьютер запустится в предзагрузочном режиме с индикатором процесса установки.

По завершении снова произойдёт перезагрузка, и запустится уже новая, переустановленная система на этапе подготовки устройств компьютера. Затем останется проделать лишь несколько привычных шагов – выбрать локационные параметры, создать учётную запись и т.п.

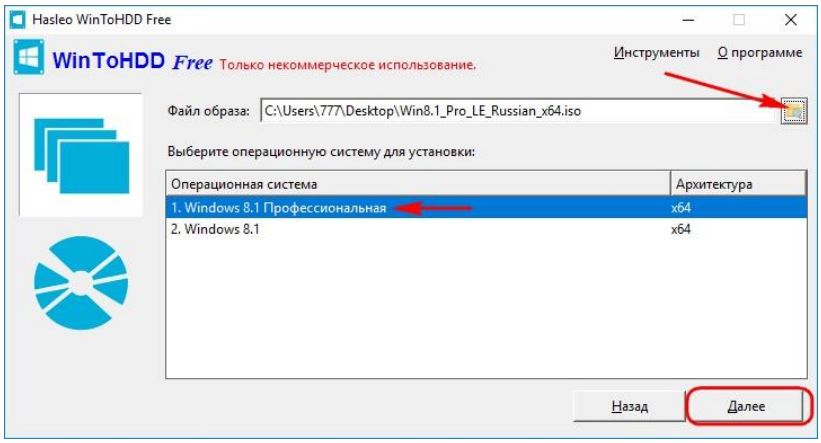
WinToHDD избавляет от необходимости ввода ключа продукта в официальных дистрибутивах Windows 8.1 (как минимум временного, пригодного только для установочного процесса). Напомним, мастер обычной установки позволяет отложить ввод ключа только для версии 10, для версии 8.1 этот момент, увы, не предусматривается. WinToHDD решает вопрос: больше не нужно искать в Интернете временный ключ продукта. Или заморачиваться по поводу вырезания этого этапа из дистрибутива в процессе перепаковки образа, как предлагается на некоторых компьютерных сайтах для гиков.
Но программа учитывает не все обстоятельства: она откажется проводить переустановку, если загрузочный и системный разделы текущей Windows расположены на разных жёстких дисках. Всё должно быть только по стандартному шаблону.

Установка на другой носитель

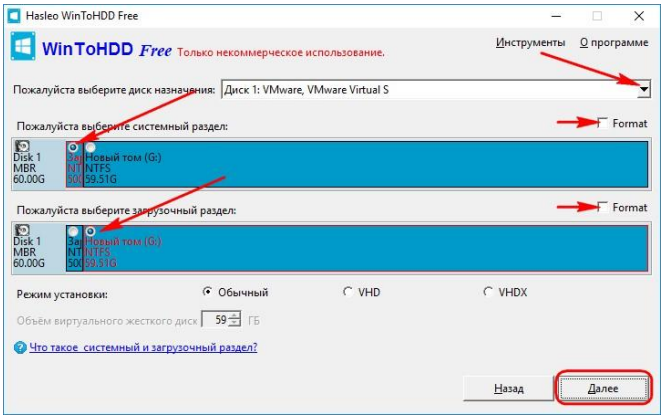
В плане возможностей установки Windows на отличный от системного раздел диска WinToHDD уступает своему аналогу – программе WinNTSetup. Последняя может устанавливать систему и на другие диски, и на другие разделы одного и того же диска. А вот в WinToHDD реализована только функция установки на другой HDD, SSD, USB-HDD и т.п.
Обычному установочному процессу с флешки или DVD WinToHDD уступает неспособностью автоматического формирования нужной структуры разделов на чистом диске. Носитель с нераспределённым пространством программа попросту не захочет принимать в качестве целевого. От пользователя, соответственно, потребуются навыки разметки дискового пространства.
Такие условности сводят к минимуму случаи задействования этой функции. Тем не менее рассмотрим её. В окне программы жмём «Новая установка».



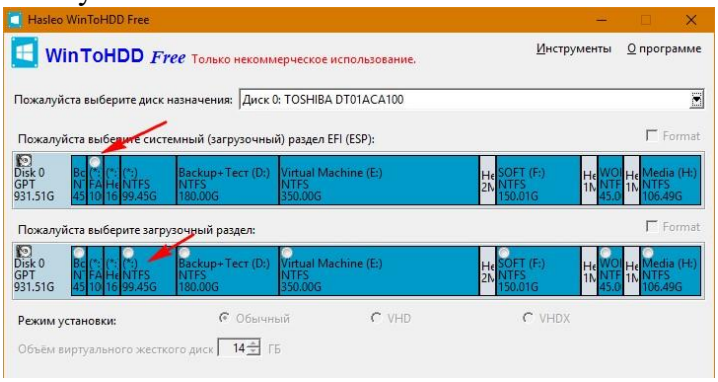
Выбираем образ с дистрибутивом, определяемся с редакцией. Жмём «Далее».



Указываем диск назначения. Далее в окне программы появятся два визуальных блока со структурой разделов. В первом блоке указываем раздел «Зарезервировано системой» на 350-500 Мб, который Windows при установке автоматически создаёт на MBR-дисках. Во втором блоке отмечаем галочкой будущий диск C. Если на этих двух разделах содержатся данные, дополнительно ставим галочку опции «Format». Жмём «Далее».

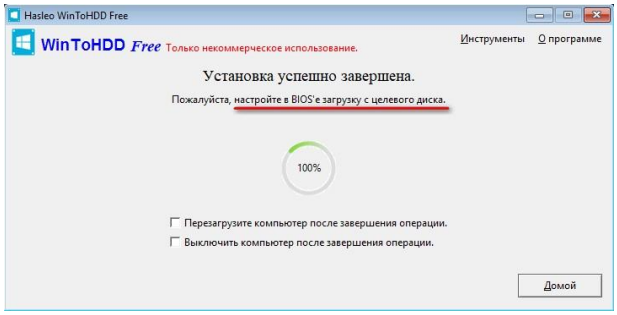


Кстати, на компьютерах с UEFI всё обстоит проще: EFI-раздел в первом визуальном блоке значится как единственный возможный выбор. Лишь во втором блоке нужно указать диск С устанавливаемой Windows.



И ещё нюанс: на этом этапе при необходимости вместо физического накопителя можно выбрать файлы VHD/VHDX. Для этого нужно выставить галочку возле одного из форматов и указать размер файла.

Далее запустится процесс копирования файлов новой Windows. По завершении операции перезапускаем компьютер. В отчётном окошке WinToHDD заботливо напоминает о том, что нужно не забыть выставить в BIOS загрузку с диска, на который только что установилась система.

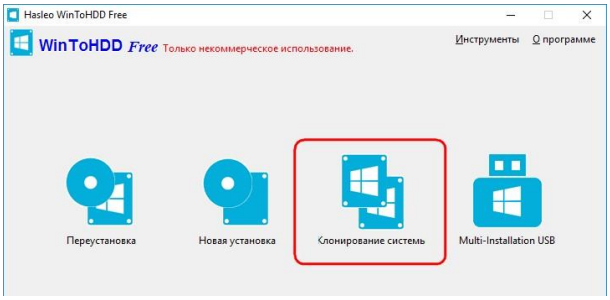


Затем будем наблюдать череду завершающих установочных этапов.

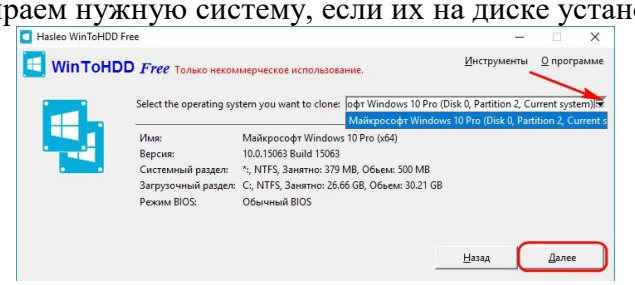
Клонирование

Из преимуществ функции клонирования операционной системы на другой накопитель – увы, только возможность бесплатного осуществления этой операции. Для проведения этой операции программа также требует подготовленных ранее разделов. Она не умеет переносить имеющуюся структуру исходного диска на диск целевой, как это могут делать другие программы, предусматривающие в числе функционала операцию по клонированию Windows.

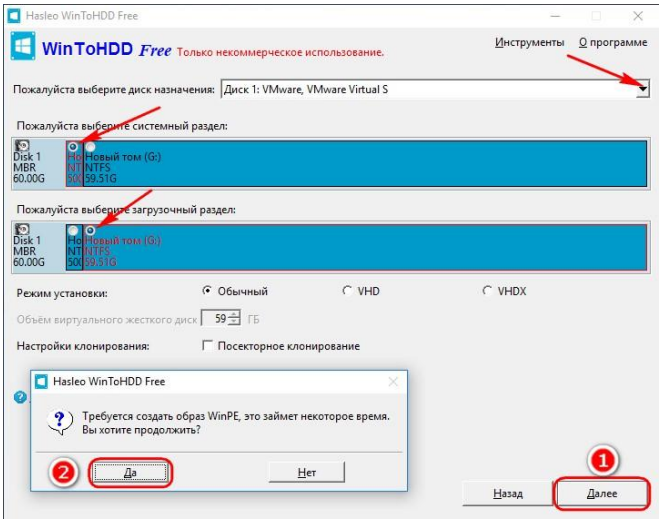
В главном окне программы кликаем «Клонирование системы».



Выбираем нужную систему, если их на диске установлено несколько. Жмём «Далее».



Указываем диск назначения. На визуальных блоках структуры диска отмечаем технический раздел и диск С по принципу, рассмотренному в предыдущем пункте статьи. Жмём «Далее» и подтверждаем операцию.

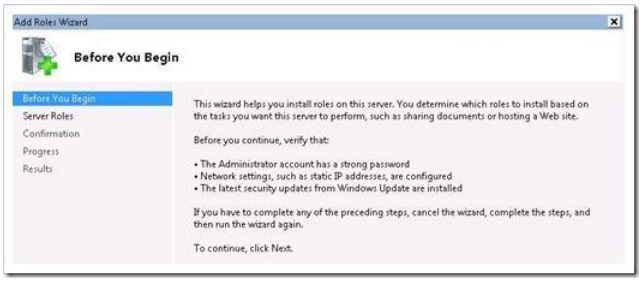


Далее нужно ещё раз подтвердить запуск операции и согласиться на перезагрузку компьютера. Клонирование проводится в предзагрузочном режиме. По завершении операции компьютер перезапускаем и выбираем в BIOS загрузку с диска, на который клонирована система.

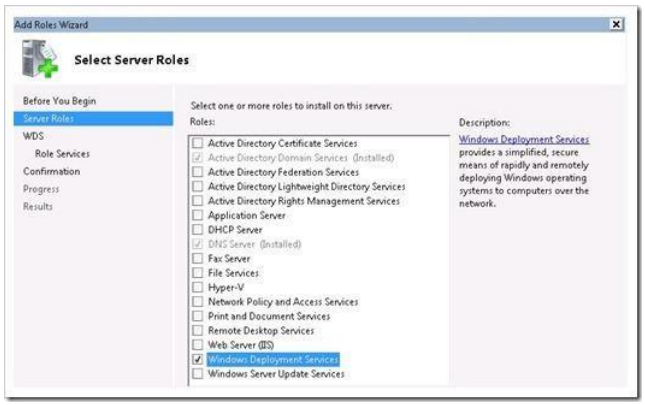
2.8 Практическая работа№ 8
Настройка и управление Windows Deployment Services Планирование среды Windows Deployment Services

Задание

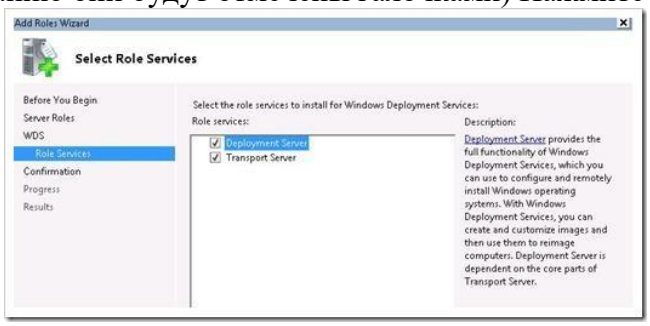
Чтобы установить WDS, перейдите в консоль Server Manager и нажмите кнопку Add Role. В результате появится мастер установки ролей.

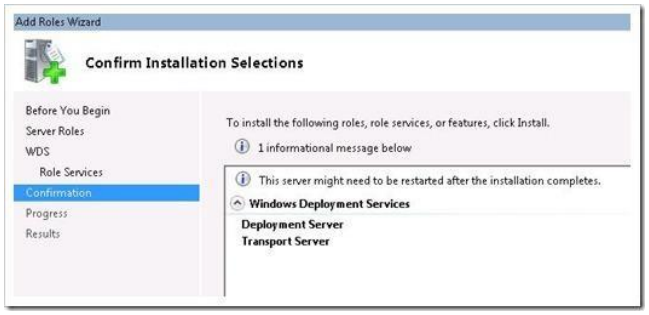


Нажмите кнопку Next. Выберите роль Windows Deployment Services и опять Далее.

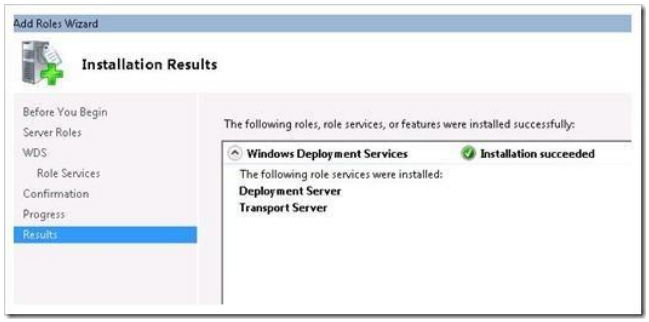


Необходимо доставить следующие службы: Deployment Server и Transport Server (по умолчанию они будут отмечены галочками) Нажмите кнопку Далее.



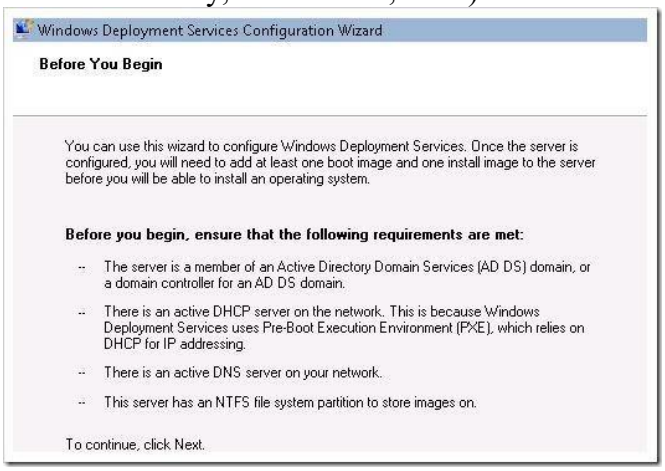


В общем-то, все, дальше начнется установка с отображением результатов установки на экран.

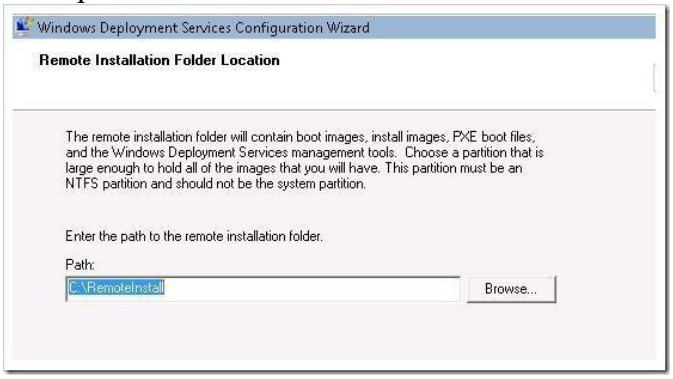


После окончания установки перейдите в Administrative Tools и откройте консоль Windows Deployment Services. При первом нажатии на ваш сервер, появится окно с предупреждением, в котором говорится, что служба WDS еще не настроена: Windows Deployment Services is not configured.
This server is not configured. To configure this server, first verify that you are a local administrator.

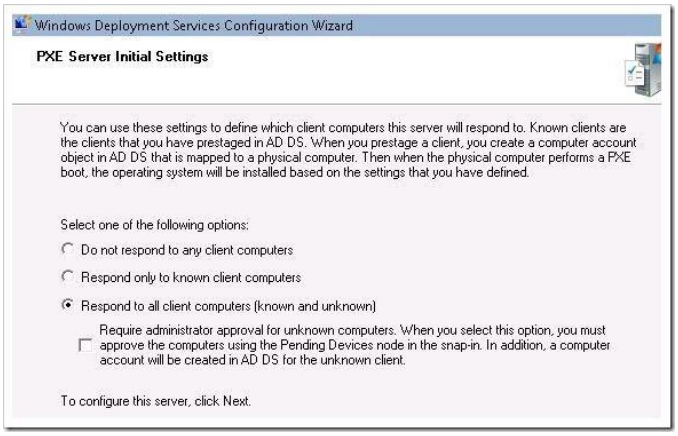
Щелкните правой кнопкой мыши по серверу и выберите пункт «configure» (настроить). Запустится очередной мастер, прежде чем приступить к настройке WDS, вы должны убедиться, что ваша инфраструктура соответствует указанным требованиям (установлен домен Active Directory, есть DHCP, DNS). Нажмите кнопку Далее.



Укажите папку для файлов Remote Installation. Согласно требованиям, указанным ниже, вы должны убедиться, что размер выбранного раздела достаточно большой для хранения файлов – образов.

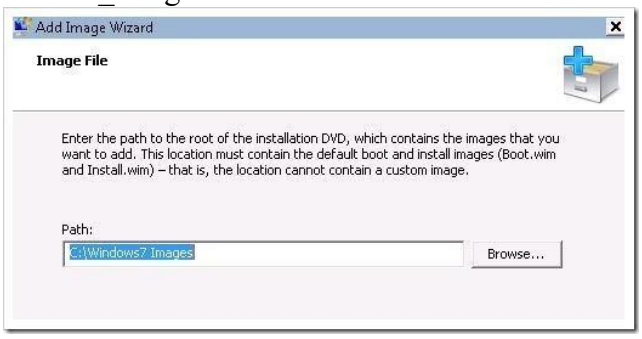


Дальше настраиваем PXE. В данном случае у нас есть возможность настроить автоматическое создание учетных записей компьютера в Active Directory, и связать в дальнейшем эту учетку с физическим ПК. Для простоты я выбрал «Respond to all computers».



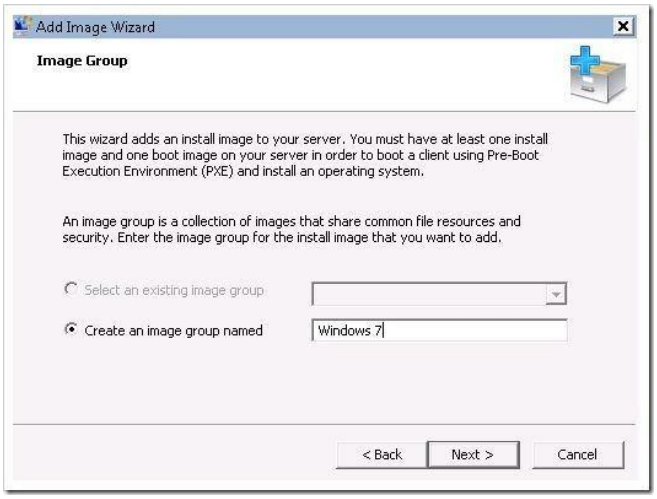
Затем нам предоставляется возможность добавить установочные образы на сервер. Я оставил галочку «Add images to the server now», в результате появится мастер добавления образов.

На этом этапе я добавлю образ загрузчика и установщика для Windows 7. Эти образы можно найти на DVD дистрибутиве Windows 7 в папке sources. Вам понадобятся 2 файла install.wim и boot.wim. Я скопировал эти два файла на сервер WDS в папку «C:Windows7_Images».

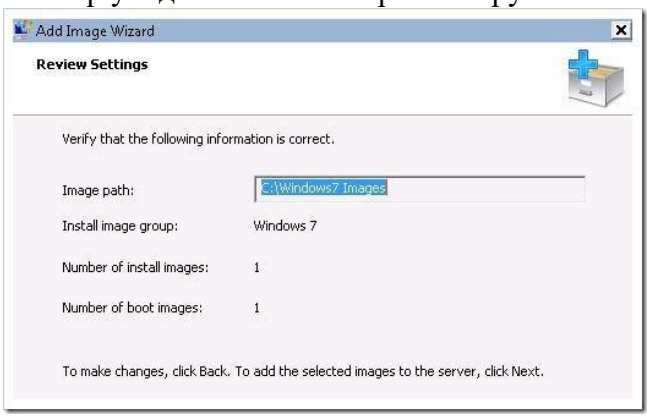


Теперь мы можем создать новую группу образов или выбрать уже существующую.

Я создал новую группу для образов с именем «Windows 7».

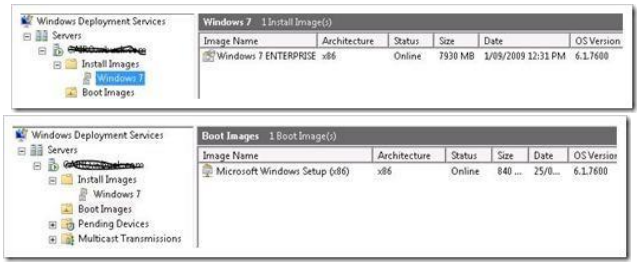


Мастер увидел оба моих образа: загрузочный — boot.wim и установочный — install.wim.



Теперь оба образа добавлены на сервер и будут отображены в консоли WDS.

На первом скриншоте виден установочной образ Windows 7. На втором отображен образ загрузчика.



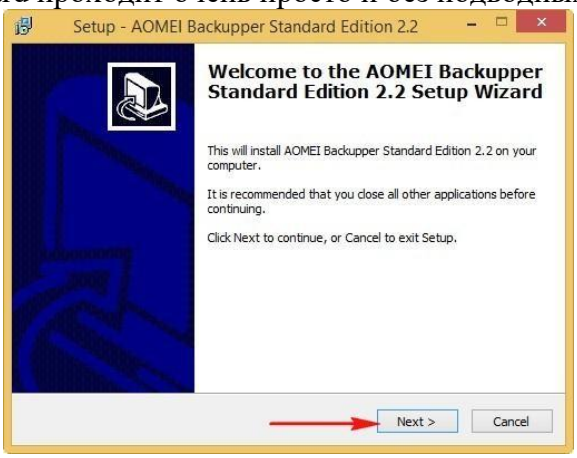
2.9 Практическая работа№ 9
Планирование и реализация миграции пользовательской среды

Задание

Установка программы AOMEI Backupper Standard

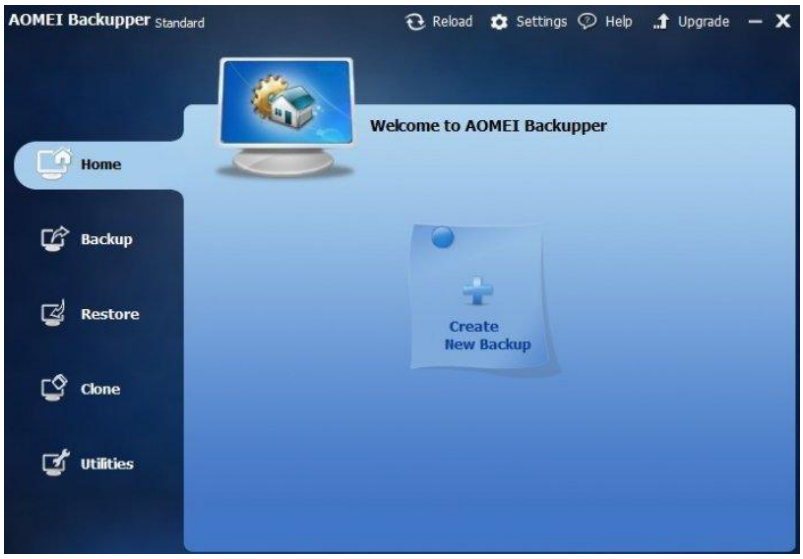
Идём на официальный сайт программы AOMEI Backupper Standard и выбираем Aomei Backupper Standard. Лицензия: Freeware. Платформа: Windows 8.1, Windows 8, Windows 7, Vista, XP (32/64-бит). Скачать

Запускаем установку программы. Инсталляция AOMEI Backupper Standard проходит очень просто и без подводных камней, жмите всегда Next

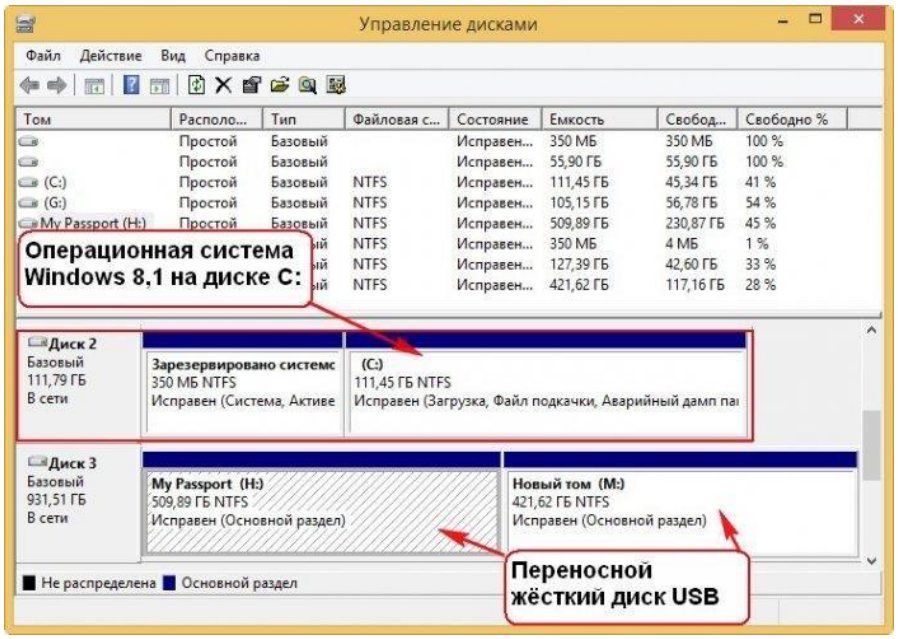


После установки запускаем программу

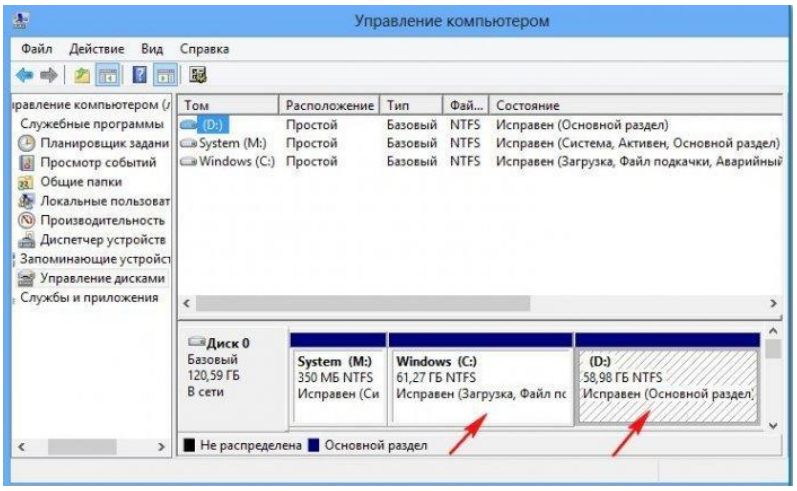
И она запускается на английском языке



Создавать будем резервную копию операционной системы Windows 8.1 (Раздел C:). Резервную копию сохраним на переносном жёстком диске USB (Раздел H:).

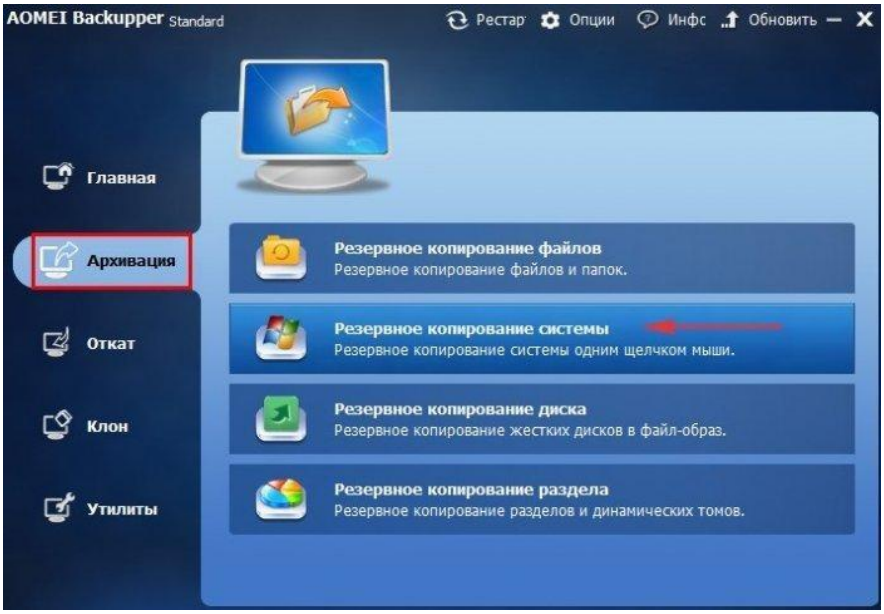


Если у Вас нет переносного жёсткого диска USB, тогда создайте на простом жёстком диске ещё один раздел (например раздел D:) и сохраните резервную копию на нём.



Выбираем "Создать новую копию" или "Архивация",

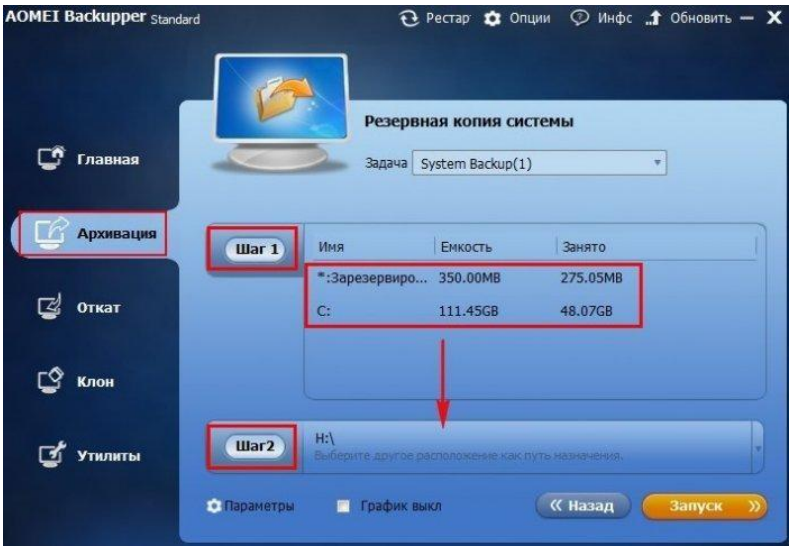
откроется одно и тоже окно Архивации. Выбираем "Резервное копирование системы"



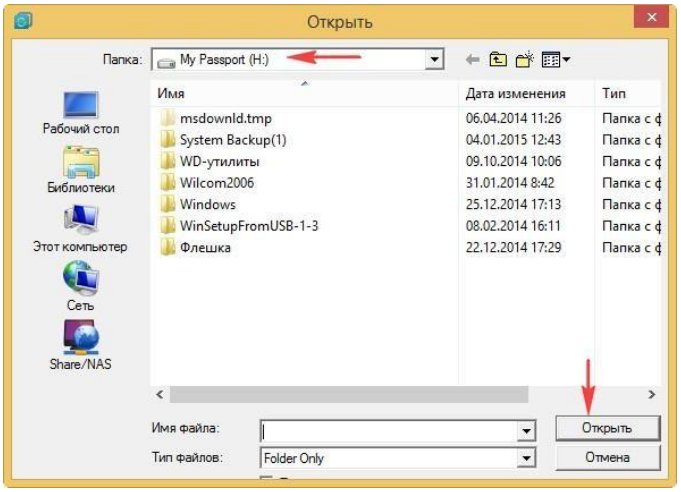
Шаг 1. Программа сразу предлагает нам создать резервную копию операционной системы. Сколько бы у Вас не было разделов на жёстком диске, для создания резервного образа Windows программа AOMEI Backupper Standard всегда выберет два раздела. Первый - скрытый раздел System Reserved (Зарезервировано системой), имеющий объём 100 МБ (Windows 7) и 350 МБ (Windows 8). Также программа выберет диск C: с установленной Windows.

Если Вы хотите включить в резервный образ несколько разделов жёсткого диска, то Вам нужно выбрать не "Архивацию", а "Резервное копирование разделов". Если Вы хотите включить в резервный образ все разделы жёсткого диска, то это тоже можно сделать по другой нашей статье.

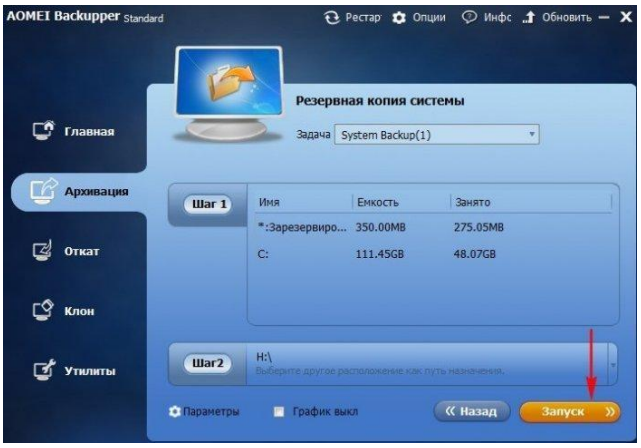
Шаг 2. Обратите внимание, программа предлагает Вам сохранить резервный образ на диске H:, Вы можете не соглашаться и нажать на кнопку выбора раздела.



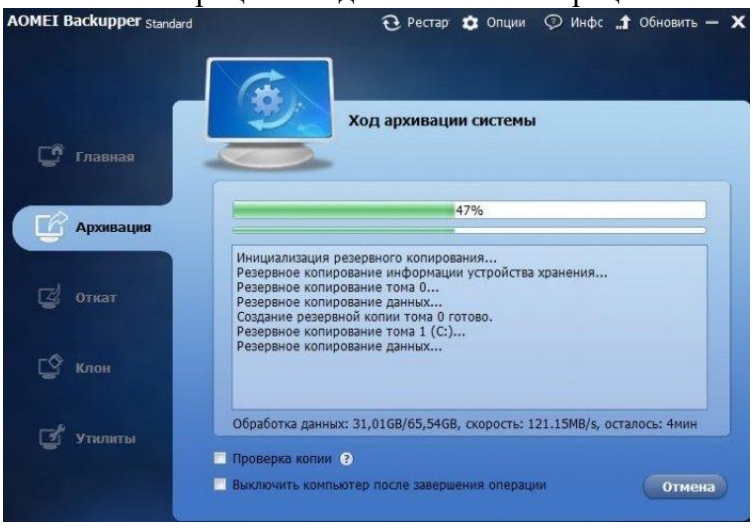
Откроется проводник, в котором Вы сможете выбрать нужный раздел для сохранения резервного образа операционной системы. Выбераем диск H: и жмём кнопку "Открыть".



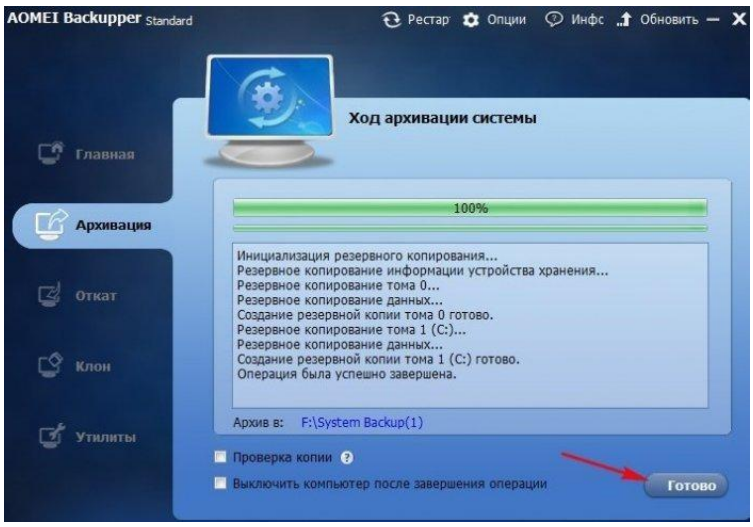
После выбора раздела для содания резервной копии Windows жмём на кнопку "Запуск"

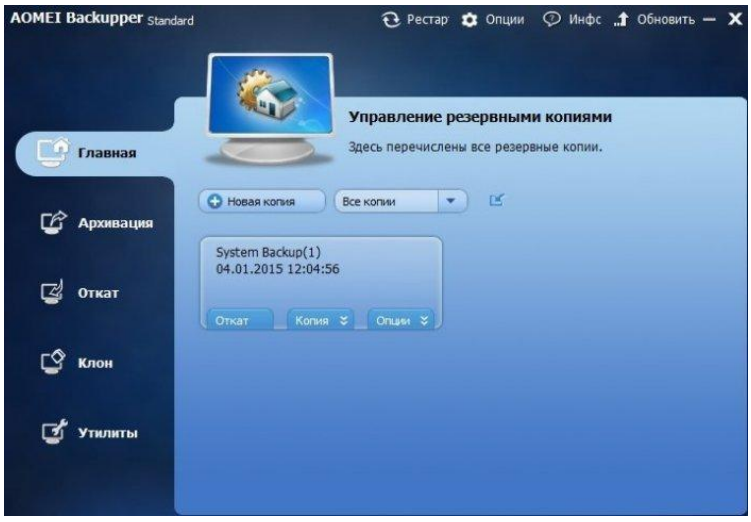


Начинается процесс создания бэкапа операционной системы

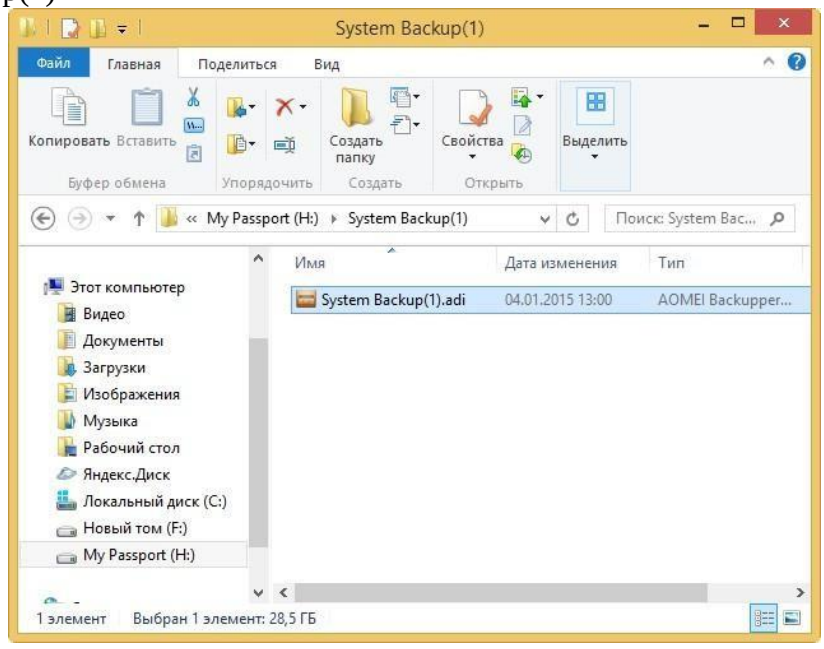


Резервная копия создана, жмём Готово.





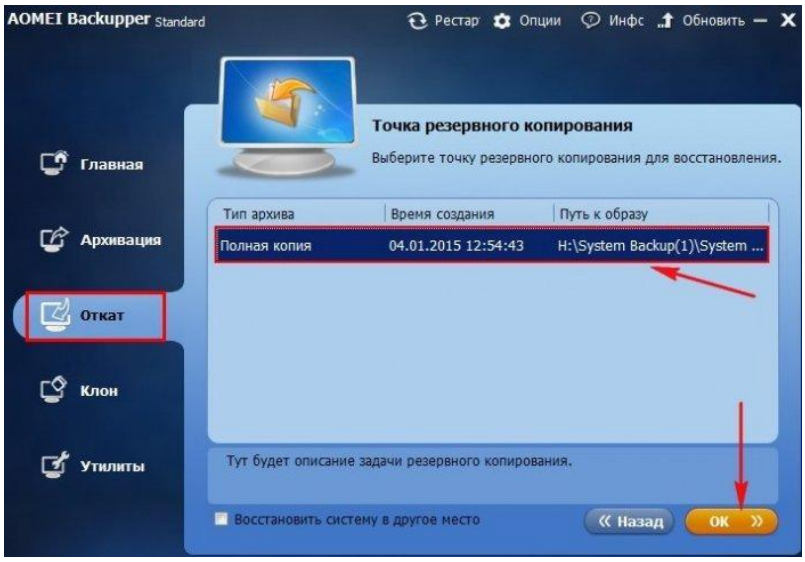
Как мы и планировали резервная копия находится на диске H: в папке H:\System Backup(1)



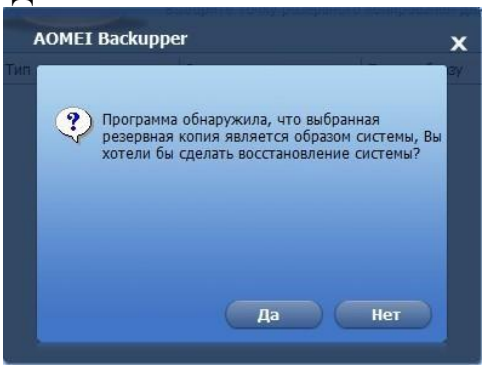
Разворачивание резервной копии

Допустим прошло некоторое время и Ваша операционная система стала работать нестабильно и Вы решили не переустанавливать её заново, а восстановить из заранее созданной резервной копии (восстановить Windows Вы сможете даже в том случае, если она не загружается, читайте статью далее).

Запускаем программу AOMEI Backupper Standard и идём на вкладку "Откат", в правой части окна выбираем нужную резервную копию (если Вы их создавали несколько) и выделяем её левой мышью, затем жмём ОК.

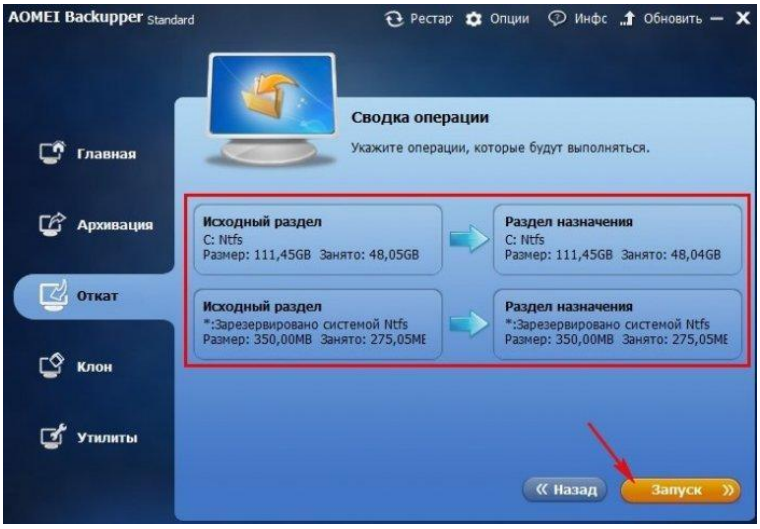


Да

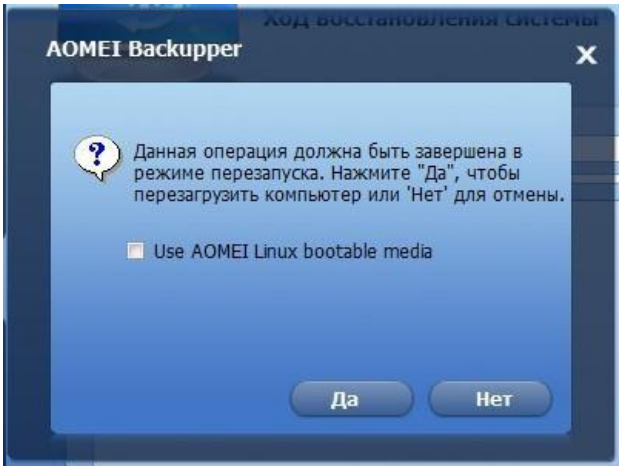


Смотрим все ли наши настройки правильные и жмём Запуск.

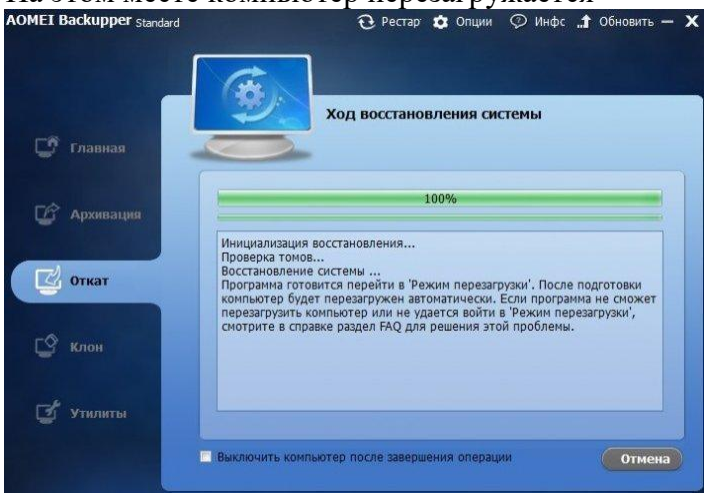
Все Ваши данные на диске C: будут замещены данными из резервной копии.



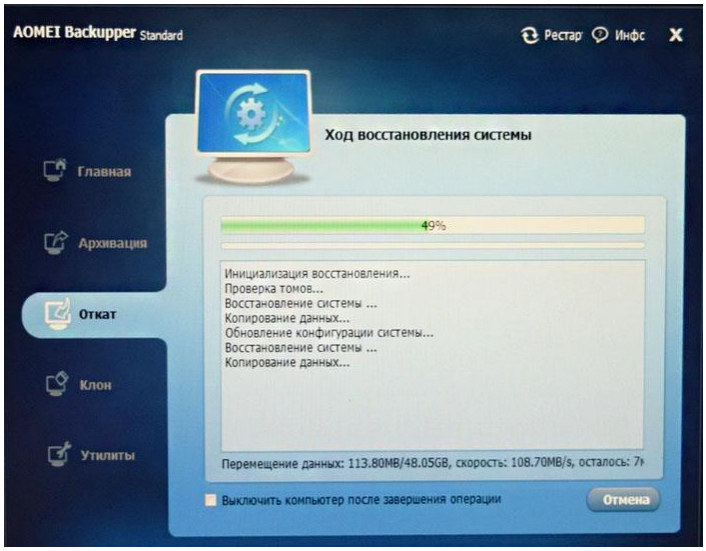
Соглашаемся на перезагрузку компьютера. Да.



На этом месте компьютер перезагружается



Процесс восстановления продолжается в ДОС режиме



Через пару минут компьютер автоматически перезагружается

И загружается восстановленная из резервной копии Windows 8.1.

2.10 Практическая работа№ 10
Миграция состояния пользователя с созданием жестких ссылок

Задание:

Использование миграции с жесткими связями для 32-разрядных операционных систем
В консоли Configuration Manager выберите System Center Configuration Manager / База данных сайта / Управление компьютером / Развертывание операционной системы / Последовательности задач.
Щелкните правой кнопкой мыши последовательность задач, в которую необходимо добавить запись пользовательской среды с жесткими связями, и выберите пункт Редактировать.
В редакторе последовательности задач выберите шаг последовательности задач, который идет перед шагом Хранилище состояния пользователей, нажмите кнопку Добавить, щелкните пункт Общие и выберите действие Задать переменную последовательности задач. В полях Переменная последовательности задач и Значение укажите значения для миграции с жесткими связями. Повторите это действие для каждой переменной последовательности задач.
В редакторе последовательности задач нажмите кнопку Добавить, щелкните пункт Общие и выберите действие Выполнить из командной строки.

Введите x86\usmtutils.exe /rd %OSDStateStorePath% в поле Командная строка.

Установите флажок Пакет.

В диалоговом окне Выберите пакет выберите пакет USMT 4.0 и нажмите кнопку ОК.
Если последовательность задач будет развертываться как в операционных системах x86, так и x64, на вкладке Параметры нажмите кнопку Добавить условие, выберите Версия операционной системы, а затем выберите версии операционной системы x86, чтобы указать операционные системы, для которых предназначена последовательность задач.
После того как USMT восстановит пользовательскую среду, данные с жесткими ссылками должны быть удалены. Для этого используется программа USMTUTILS.exe, которая входит в состав пакета USMT 4.0.
Использование миграции с жесткими связями для 64-разрядных операционных систем
В консоли Configuration Manager выберите System Center Configuration Manager / База данных сайта / Управление компьютером / Развертывание операционной системы / Последовательности задач.

Щелкните правой кнопкой мыши последовательность задач, в которую необходимо добавить запись пользовательской среды с жесткими связями, и выберите пункт Редактировать.
В редакторе последовательности задач выберите шаг последовательности задач, который идет перед шагом Хранилище состояния пользователей, нажмите кнопку Добавить, щелкните пункт Общие и выберите действие Задать переменную последовательности задач. В полях Переменная последовательности задач и Значение укажите значения для миграции с жесткими связями. Повторите это действие для каждой переменной последовательности задач.
В редакторе последовательности задач нажмите кнопку Добавить, щелкните пункт Общие и выберите действие Выполнить из командной строки.

Введите amd64\usmtutils.exe /rd %OSDStateStorePath% в поле Командная строка.

Установите флажок Пакет.

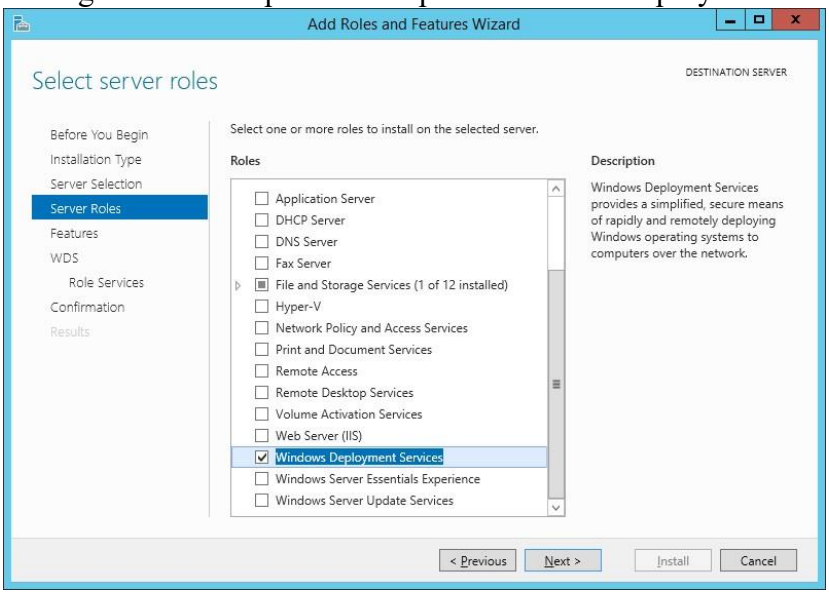
Выберите пакет USMT 4.0.

Если последовательность задач будет развертываться как в операционных системах x86, так и x64, на вкладке Параметры нажмите кнопку Добавить условие, выберите Версия операционной системы, а затем выберите версии операционной системы x64, чтобы указать операционные системы, для которых предназначена последовательность задач.
После того как USMT восстановит пользовательскую среду, жесткие связи должны быть удалены. Для этого используется программа USMTUTILS.exe, которая входит в состав пакета USMT 4.0.

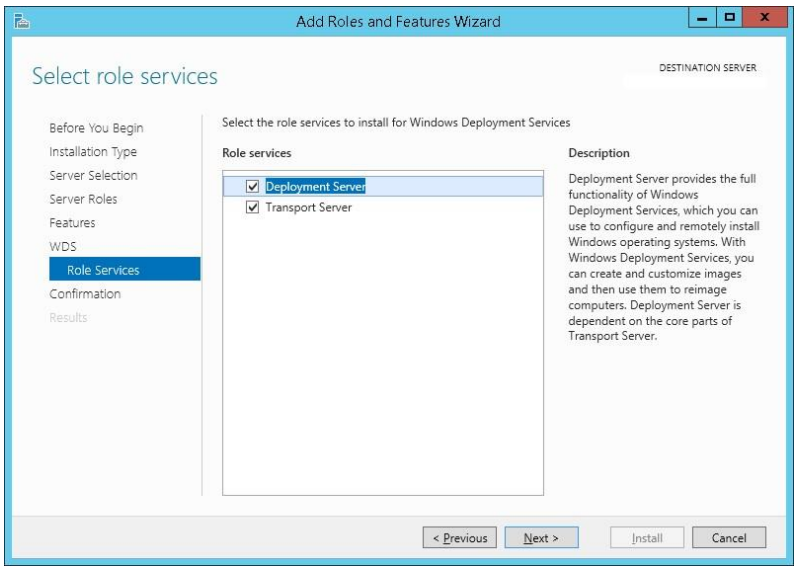
2.11 Практическая работа№ 11
Планирование и развертывание клиентских ОС с помощью MDT

Задание:

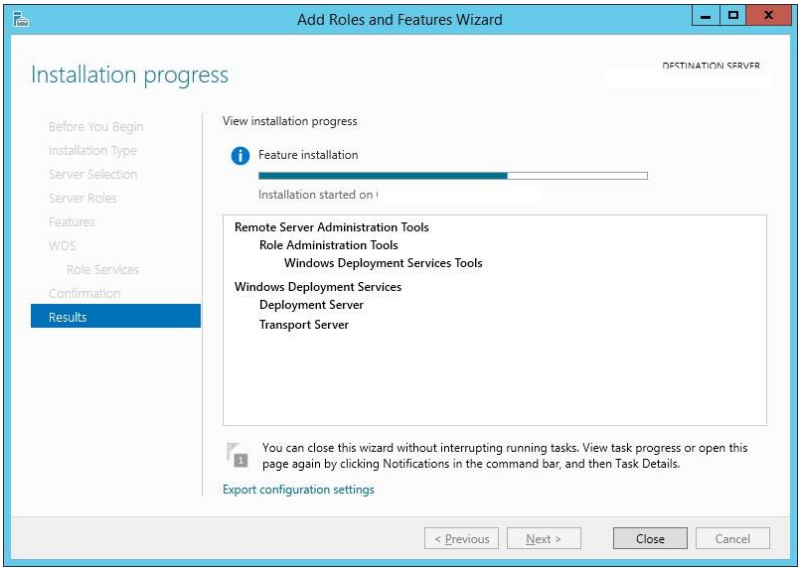
В первую очередь нужно на сервере под управлением Windows Server 2012 R2 установить роль Windows Deployment Services. Установку роли можно выполнить из консоли Server Manager. В списке ролей выберите Windows Deployment Services и нажмите Next.



В списке устанавливаемых компонентов роли WDS отметьте службы Deployment Server и Transport Server.



Запустите установку роли WDS (занимает пару минут).

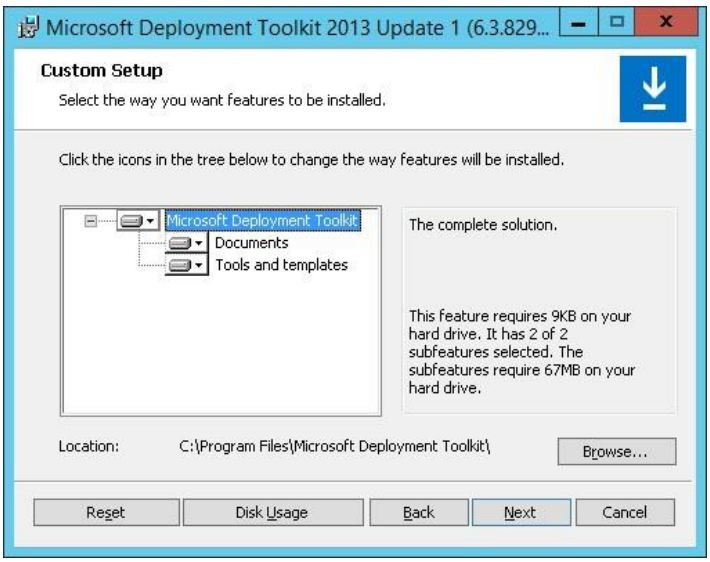


Совет. Роль Windows Deployment Services можно установить с помощью всего одной команды PowerShell:

```
Install-WindowsFeature -Name WDS -IncludeManagementTools
```

Установка Microsoft Deployment Toolkit 2013

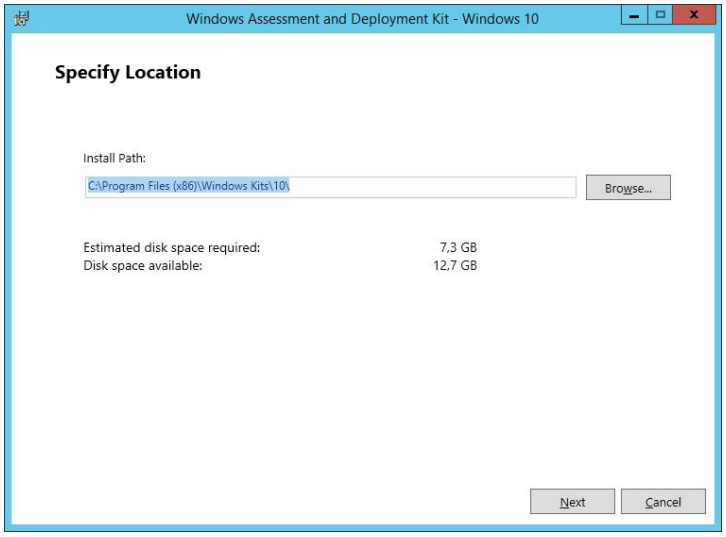
Установите Microsoft Deployment Toolkit (MDT) 2013 Update 1 со стандартными настройками, для чего достаточно скачать и запустить с правами администратора файл MicrosoftDeploymentToolkit2013_x64.



Установка Windows Assessment and Deployment Kit

Далее нужно установить Windows Assessment and Deployment Kit (Windows ADK) для Windows 10. Скачайте и запустите файл adksetup.exe.

Укажите каталог для установки (по умолчанию C:\Program Files (x86)\Windows Kits\10\).

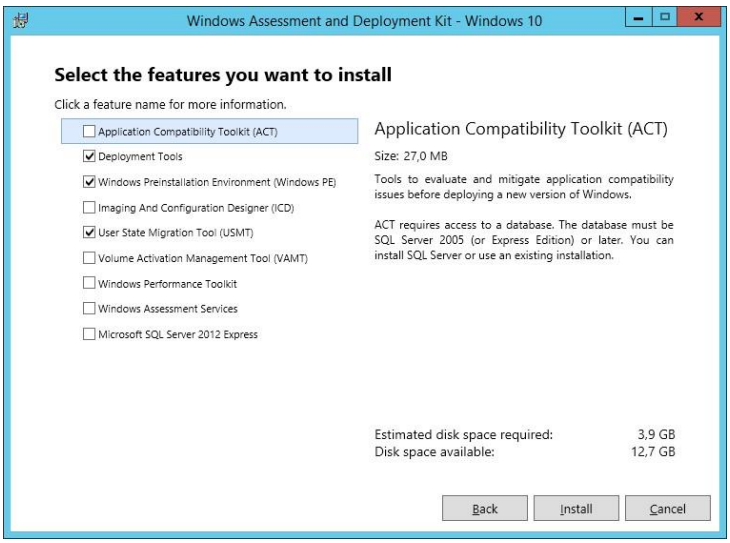


В списке компонентов ADK для установки отметьте:

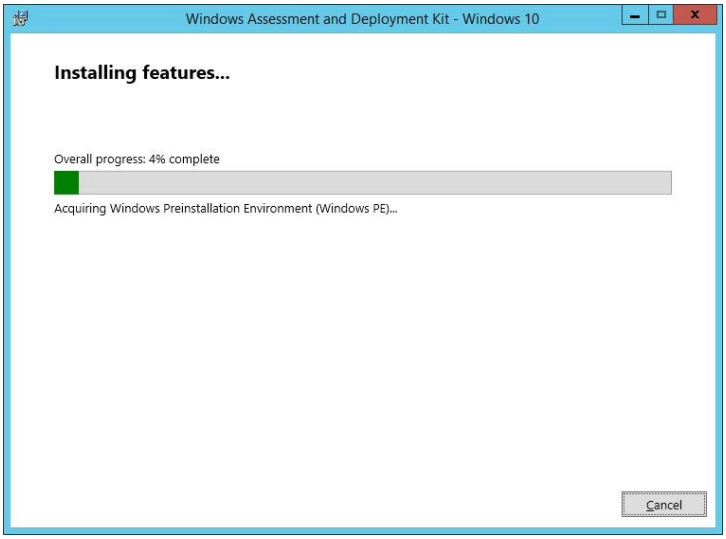
Deployment tools –используется для настройки образа Windows и автоматизации развертывания образа

Windows Preinstallation Environment (Windows PE) – среда WinPE — минимальная ОС, разработанная для подготовки компьютера к установке Windows или обслуживания

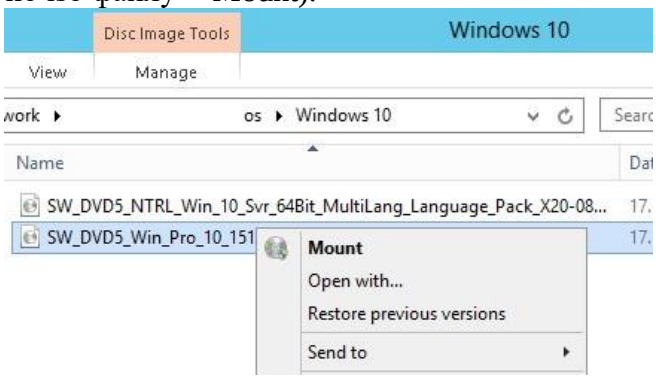
User State Migration tool (USMT) – набор инструментов для миграции данных пользователей между системами



Запустите установке Windows ADK.

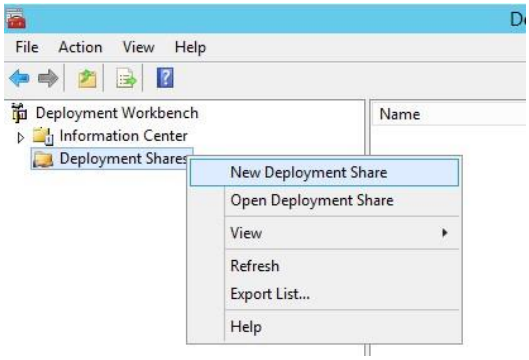


Теперь нам нужен дистрибутив Windows 10. В нашем примере это будет Windows 10 x64 Pro. Т.к. MDT не позволяет напрямую работать с iso файлами образа Windows, необходимо распаковать установочные файлы. Самый простой вариант – смонтировать файл с iso образом Windows 10 через File Explorer (Проводник) в отдельный виртуальный драйв (ПКМ по iso файлу-> Mount).

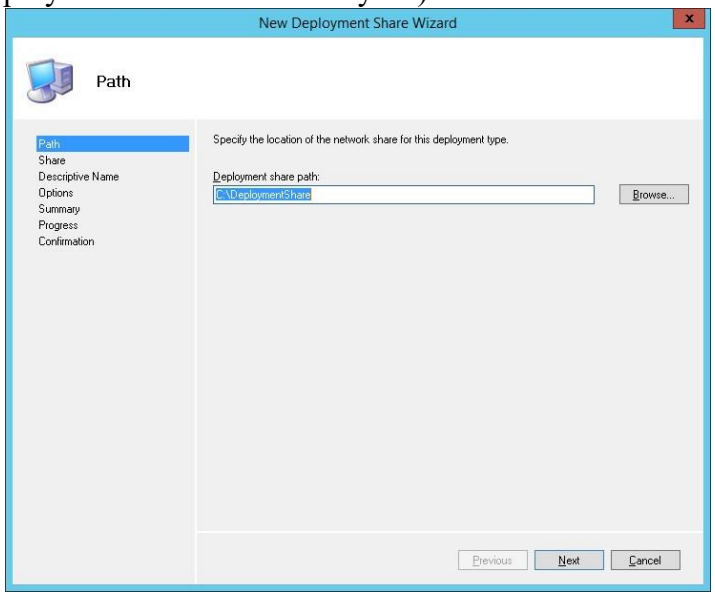


Настройка MDT 2013

Приступим к настройке MDT 2013. Запустим консоль Deployment Workbench, щелкнем ПКМ по Deployment Share и создадим новый каталог (New Deployment Share).



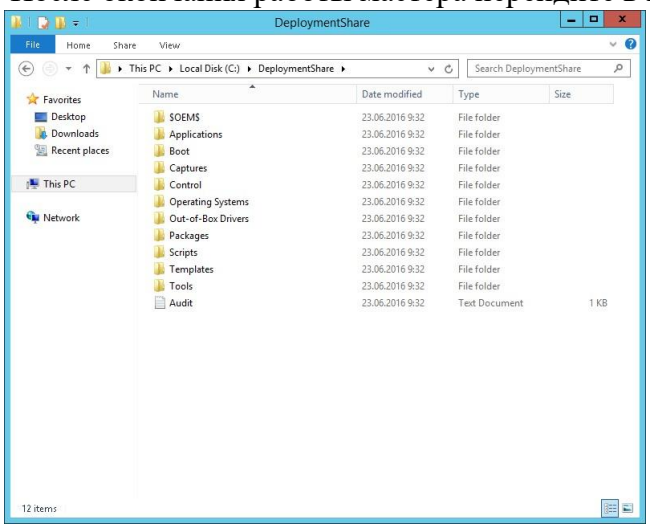
В окне мастера создания нового каталога распространения укажите путь к папке (C:\DeploymentShare в нашем случае).



Укажите сетевое имя каталога (мы оставили имя по умолчанию DeploymentShare$) и нажмите Next.

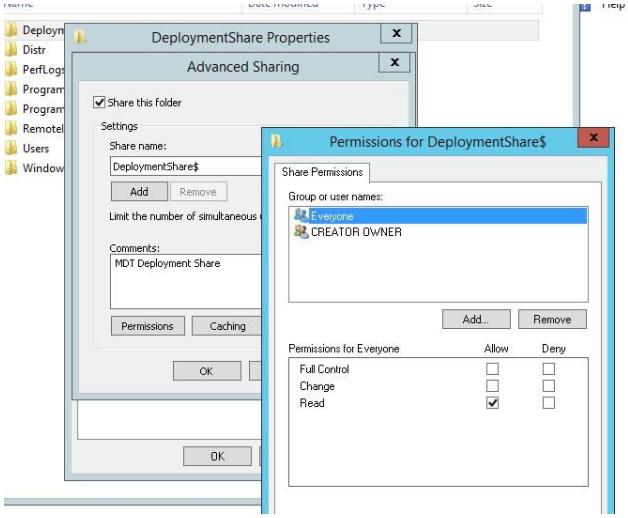
Совет. Знак “$” в имени сетевой папки означает, что она будет скрыта от пользователей.

После окончания работы мастера перейдите в папку C:\DeploymentShare.



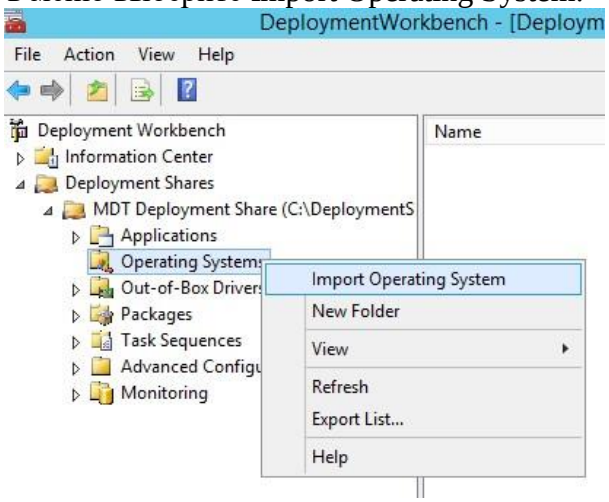
В этой папке хранятся образы ОС, драйвера, настройки, пакеты с приложениями и т.д. Папка является портабельной и может быть легко перенесена на другой MDT сервер.

Чтобы все сетевые клиенты (в том числе анонимные) могли обращаться к содержимому этой папке, в свойствах сетевой папки DeploymentShare$, нужно добавить группу Everyone с разрешением на чтение.

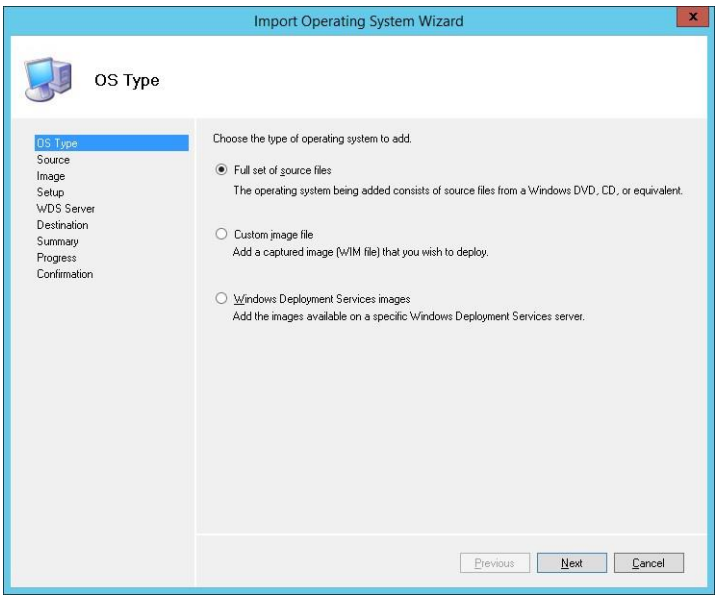


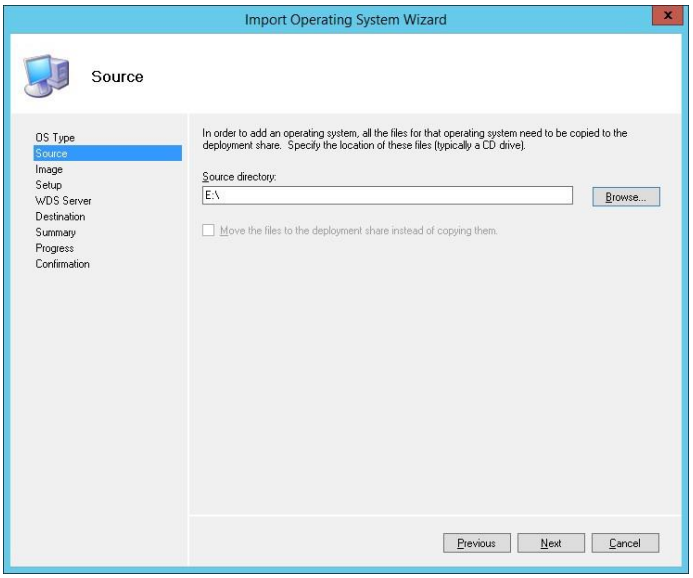
На следующем шаге нам нужно импортировать образ Windows 10. MDT поддерживает импорт образа операционной системы непосредственно с диска дистрибутива, wim файла или образа wds.

Разверните Deployment Shares -> MDT Deployment share. ПКМ по разделу Operating systems и в меню выберите Import Operating System.

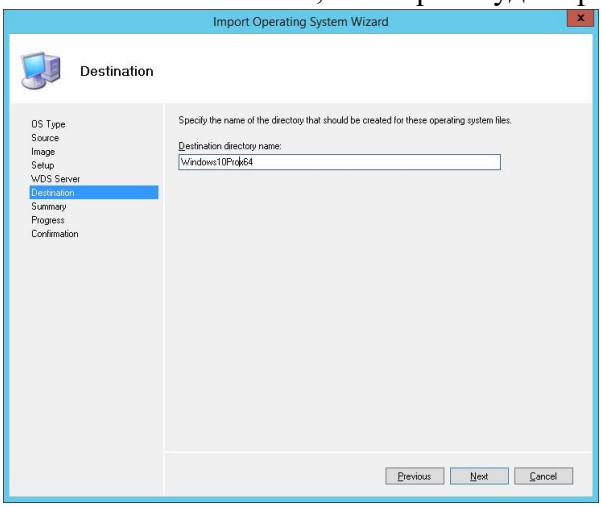


Выберите пункт Full set of source files и укажите имя драйва, на который был смонтирован iso образ Windows 10.

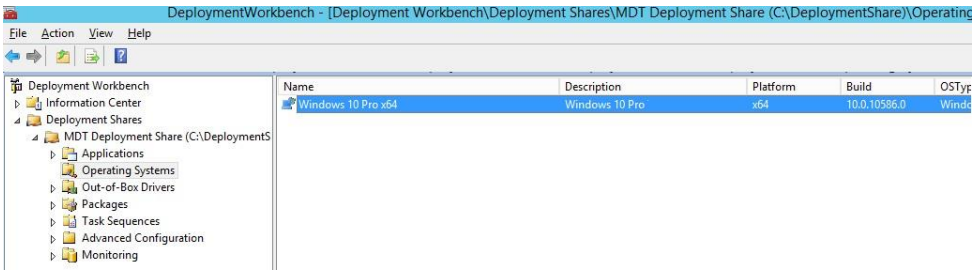




Укажите имя каталога, в котором будет храниться импортируемый образ.



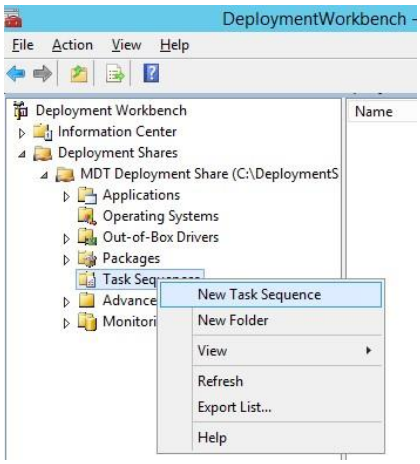
Мастер скопирует файлы дистрибутива Windows 10 в каталог C:\DeploymentShare\Operating Systems\Windows10Prox64, а в разделе Operating Systems появится новый запись, указывающая на образ Windows 10 Pro x64.



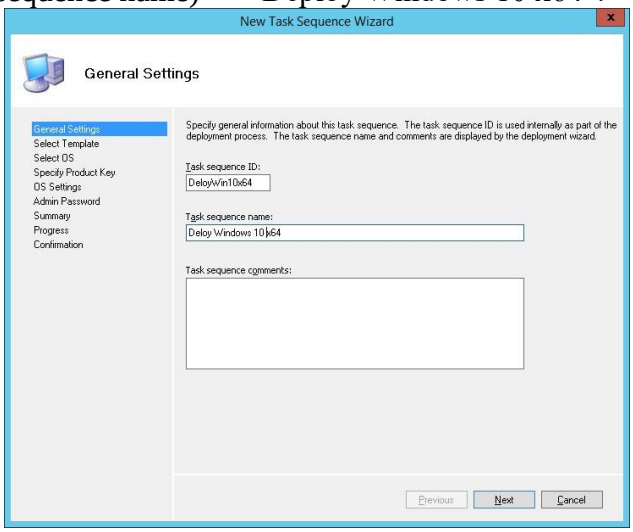
Создание задания установки MDT

Теперь нужно создать задание установки (Task Sequence), представляющее собой последовательность действий, необходимых для разворачивания Windows (это установка ОС, драйверов, приложений, конфигурация системы, обновлений, запуск различных скриптов настройки и т.п.).

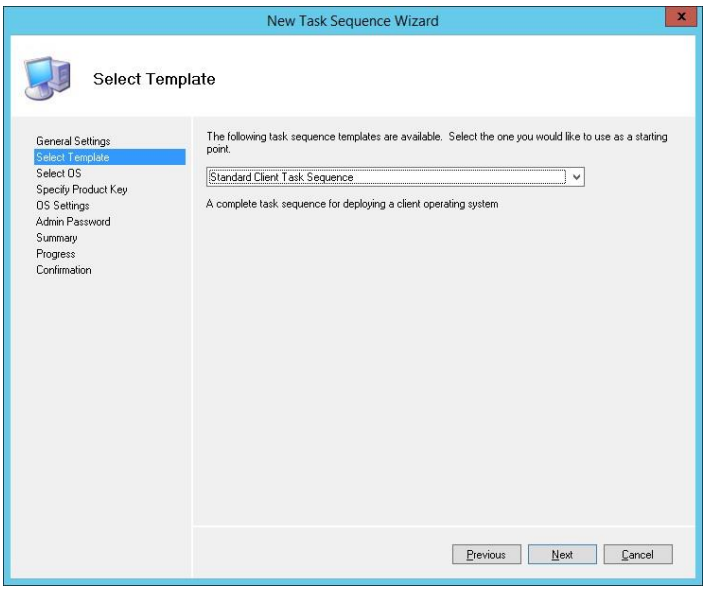
Щелкните ПКМ по разделу Task Sequences и выберите New Task Sequence.



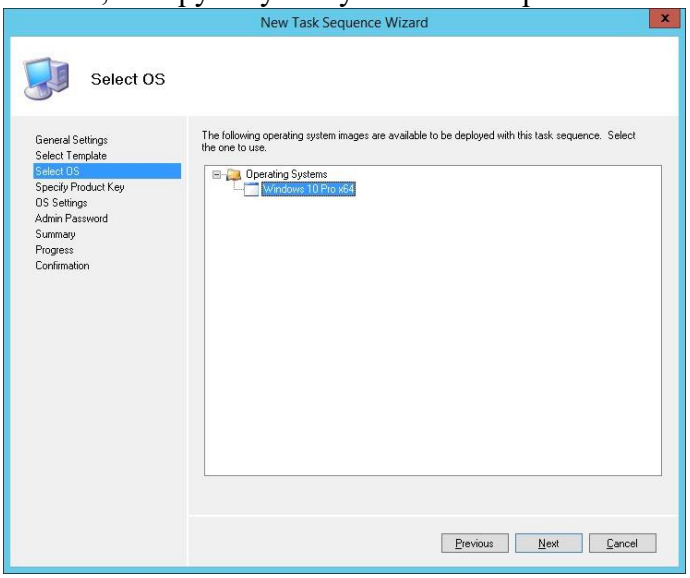
В качестве идентификатора задания (Task sequence ID) укажем DeployWin10x64, а имени (Task sequence name) — “Deploy Windows 10 x64”.



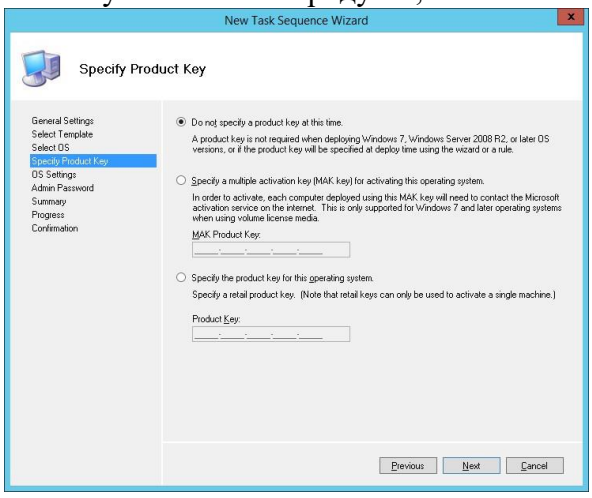
В выпадающем меню нужно выбрать один из существующих шаблонов заданий установки. В нашем случае это будет Standard Client Task Sequence.



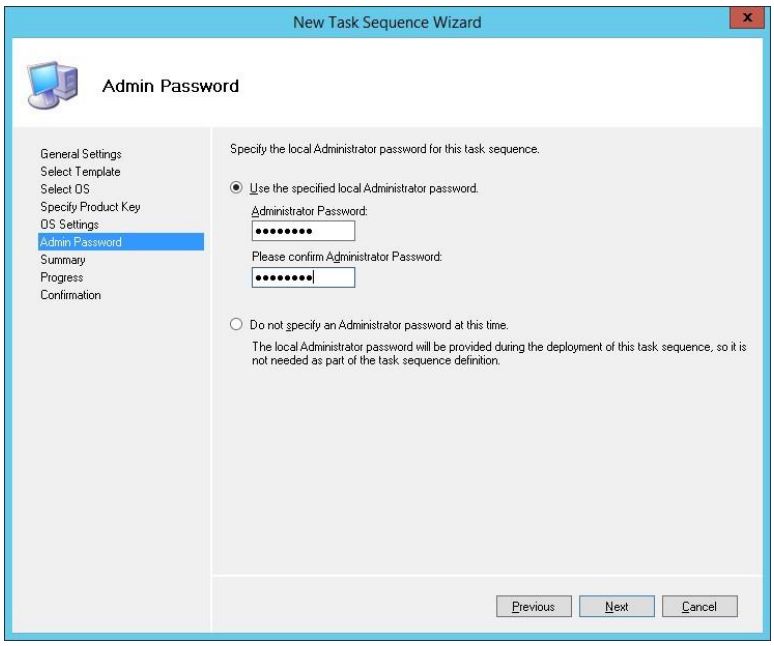
Выберите ОС, которую нужно установить в рамках этого задания (Windows 10 Pro x64).



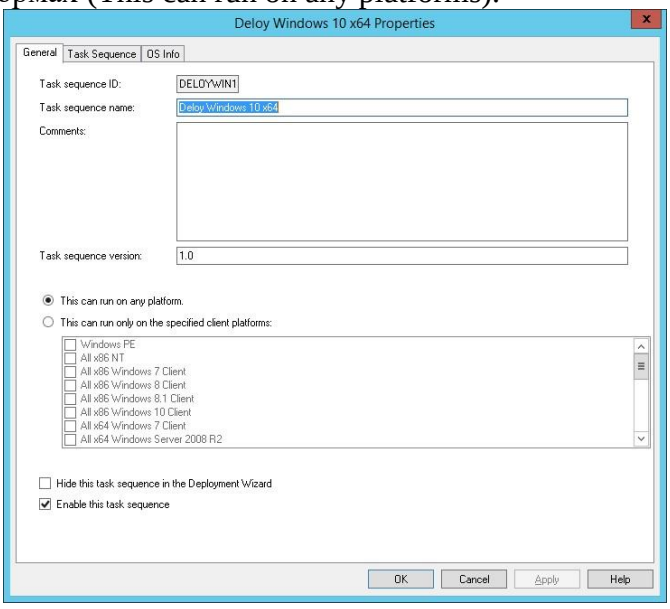
Затем можно указать ключ продукта, это может быть как retail, MAK или KMS ключ.



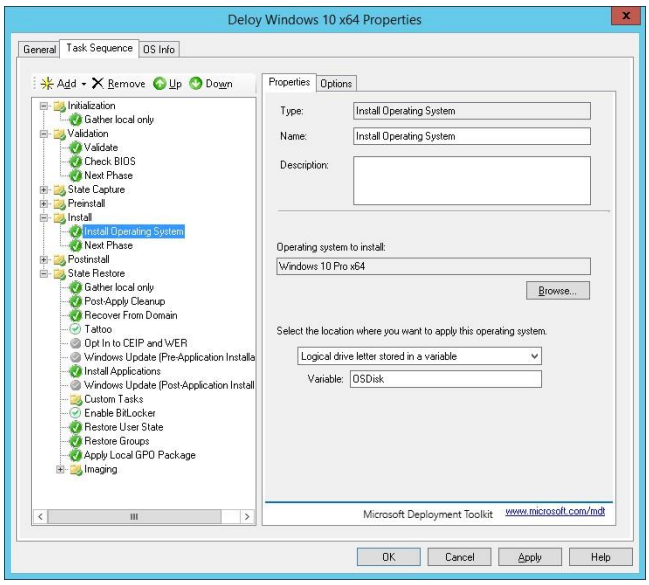
Далее можно задать пароль локального администратора на устанавливаемой системе. Совет. Имейте в виду, что пароль хранится в открытом виде в файле Unattend.xml, поэтому стоит задать простой пароль локального администратора, который после ввода компьютера в домен будет автоматически измен с помощью MS LAPS.



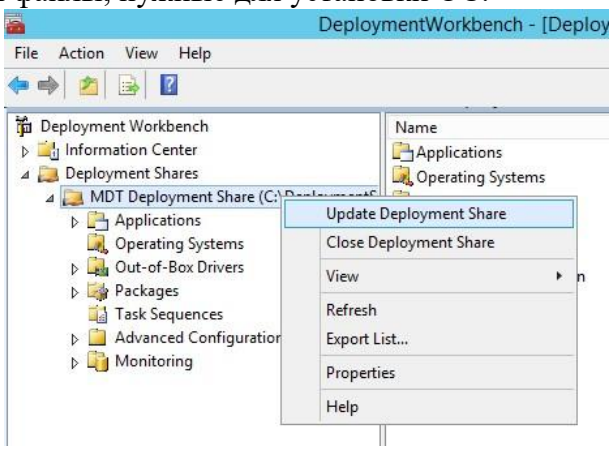
Откройте свойства созданного задания и проверьте, что его запуск разрешён на любых платформах (This can run on any platforms).



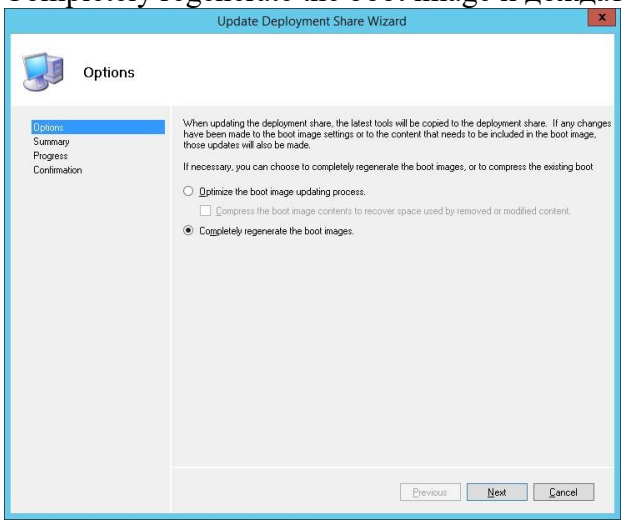
На вкладке Task Sequence отображается последовательность шагов, определенных в шаблоне, которые нужно выполнить при разворачивании ОС на клиенте. Здесь можно добавить собственные шаги, либо оставить все по-умолчанию.



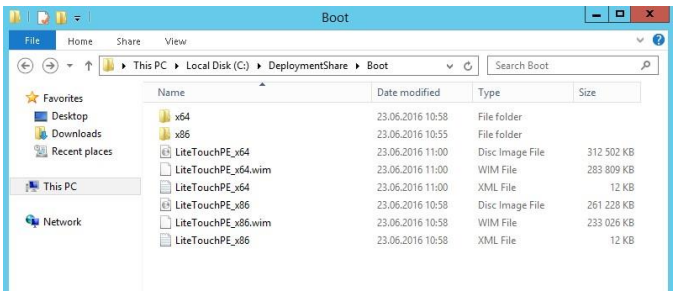
Далее нужно обновить каталок распространения MDT. Щелкните ПКМ по MDT Deployment Share и выберите Update Deployment Share. MDT сгенерирует загрузочные образы и файлы, нужные для установки ОС.



При первом запуске каталог C:\DeploymentShare\Boot пуст, поэтому нужно выбрать пункт Completely regenerate the boot image и дождаться генерации образов ОС.



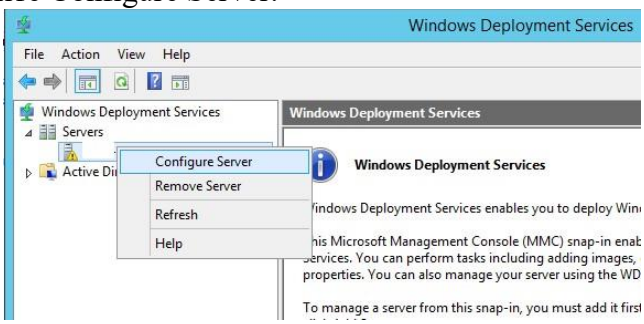
В каталоге C:\DeploymentShare\Boot должны появится iso и wim образы Windows PE для x86 и x64 платформ. Эти образы могут быть использованы для загрузки физических или виртуальных машин при разворачивании образа. При разворачивании образа Windows по сети (PXE boot) с помощью Windows Deployment Services могут быть использованы wim файлы.



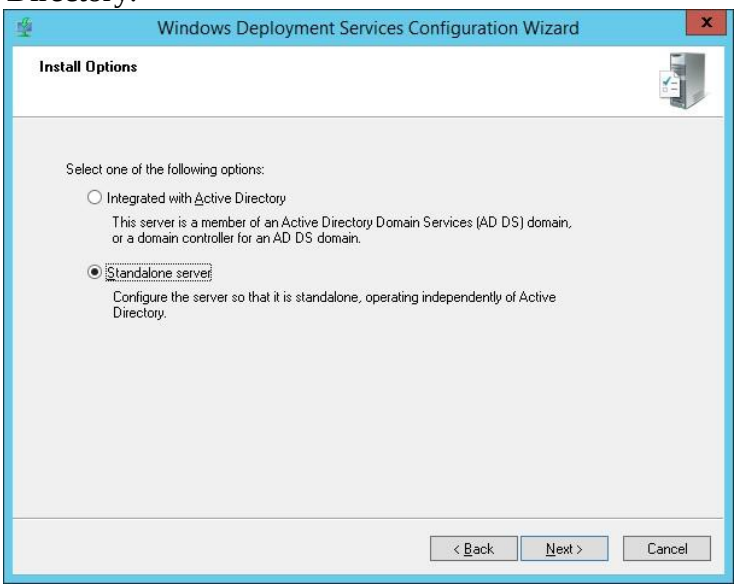
Совет. Т.к. мы планируем использовать загрузку PXE booting, нам понадобятся только wim файлы LiteTouchPE_x64.wim и LiteTouchPE_x86.wim.

Настройка загрузочного образа в Windows Deployment Services

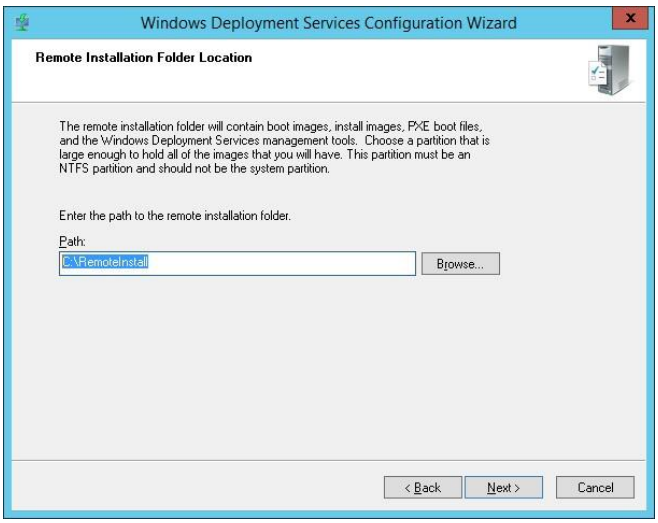
Следующий этап – настройка сервера WDS, который должен обслуживать запросы клиентов PXE. Откройте консоль Windows Deployment Services (Server Manager -> Tools > Windows Deployment Services), разверните ветку Servers и в контекстном меню сервера выберите Configure Server.



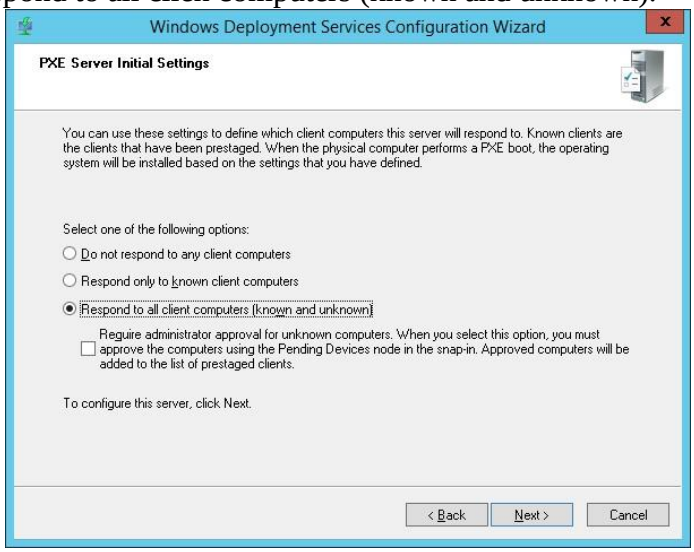
Укажем, что это будет отдельный WDS сервер (Standalone Server), не зависимый от Active Directory.



Каталог установки оставим без изменений — C:\RemoteInstall.

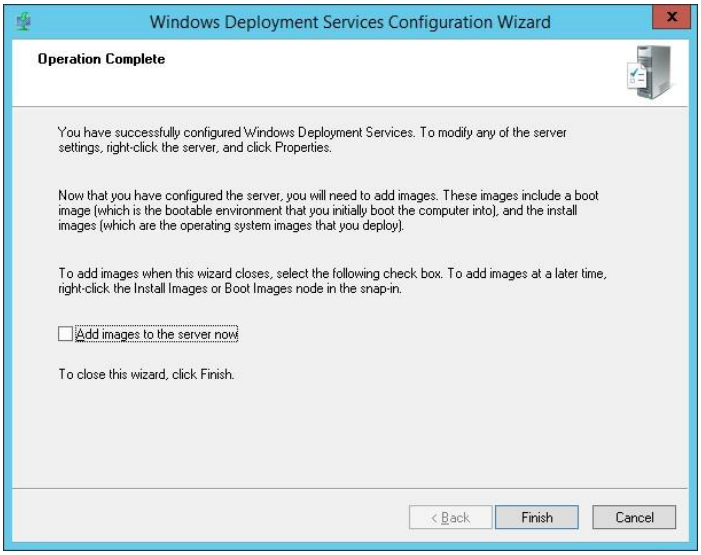


В настройках клиента PXE нужно указать, что нужно отвечать на запросы всех клиентов — Respond to all clien computers (known and unknown).

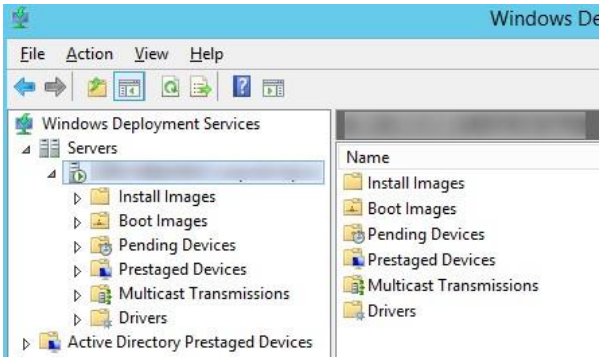


Совет. В среде Active Directory было бы безопаснее использовать опцию Respond only to known client computer.

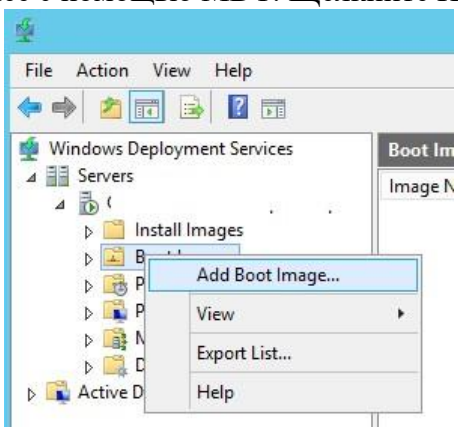
Снимите галку– Add images to the server now.



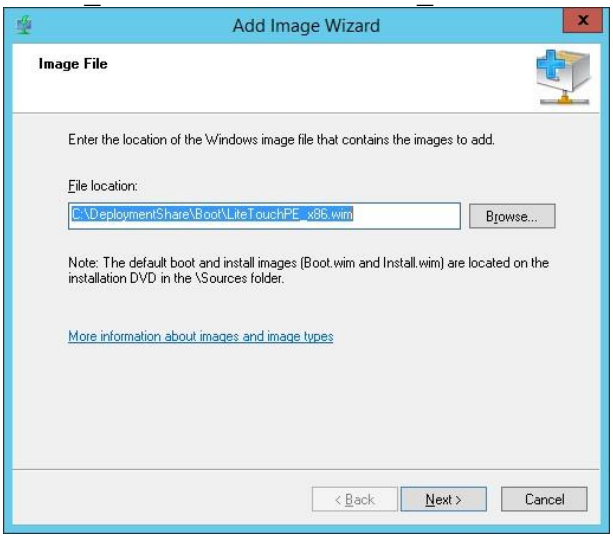
Зеленый треугольник на имени WDS сервера означает, что он настроен и запущен.

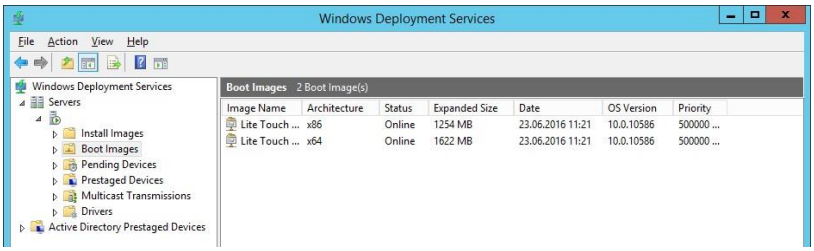


Теперь нам нужно импортировать на WDS сервер загрузочный образ, который мы создали ранее с помощью MDT. Щелкните ПКМ по Boot Image –> Add boot image.



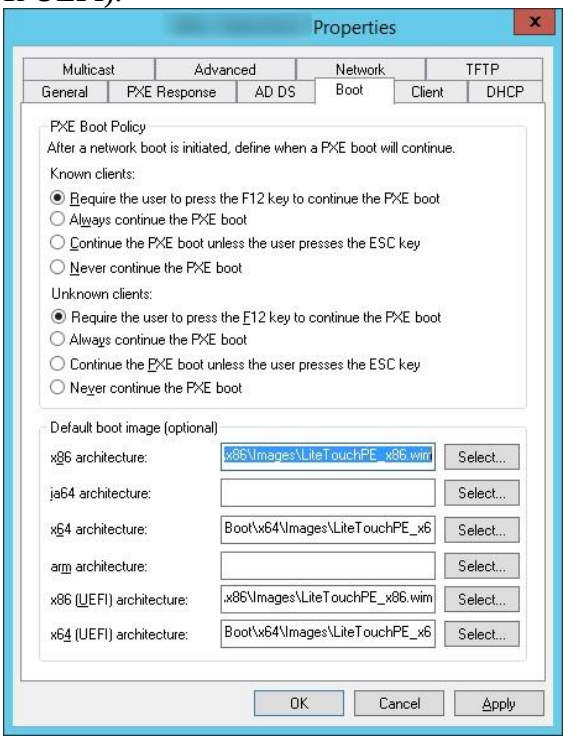
Перейдите в каталог C:\DeploymentShare\Boot и последовательно добавьте файлы LiteTouchPE_x86.wim и LiteTouchPE_x64.wim.



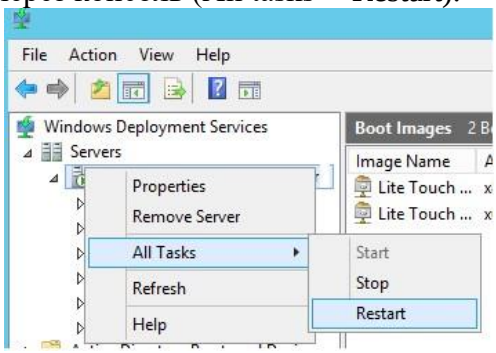


Последнее, что осталось выполнить – открыть свойства WDS сервера и перейти на вкладку Boot. Чтобы предотвратить случайную загрузку клиентов через PXE и автоматическую установку Windows, зададим обязательное использование клавиши F12 для использования PXE-загрузки. Для этого в секции PXE Boot Policy нужно выбрать опцию Require the user to press the F12 key to continue the PXE boot.

Здесь же укажите загрузочные образы для архитектур x86 и x64 (в том числе для архитектуры UEFI).



Все остальные настройки WDS сервера оставим по-умолчанию. Перезапустите службу WDS через консоль (All tasks ->Restart).

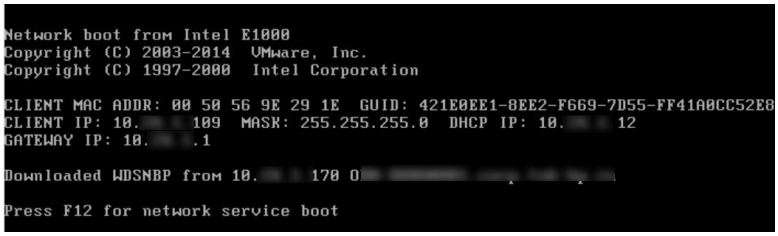


Важно. WDS сервер и клиентский компьютер, на который вы хотите установить ОС через PXE, должны находится в одной подсети (VLAN). Если они расположены в разных подсетях, нужно настроить DHCP-relay (IP Helper) с дополнительными DHCP опциями 60 и 67.

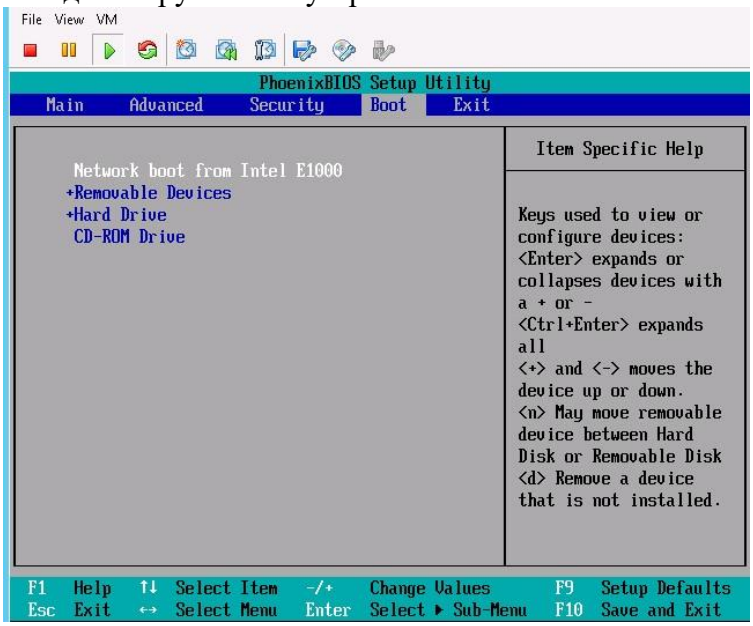
Тестирование установки Windows 10 по сети

Теперь мы готовы протестировать сетевую загрузку компьютера клиента с wim образа, расположенного на WDS сервере (PXE boot). В этом тесте это будет виртуальная машина VMWare. Запустите ВМ и в процессе загрузи несколько раз нажмите клавишу F12 для начала загрузки через PXE.

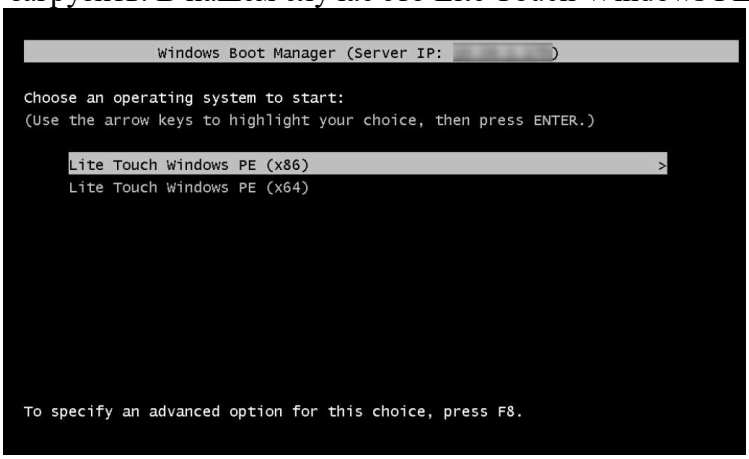
Press F12 for network service boot



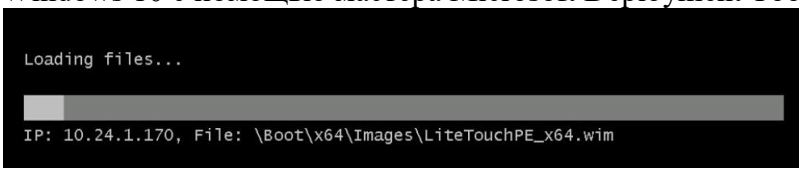
Совет. Т.к. экран загрузки в ВМ проскакивает слишком быстро, практически нереально успеть нажать кнопку F12. Поэтом в настройках ВМ предпочтительно задать наивысший приоритет для загрузочного устройства Network boot from Intel E1000.



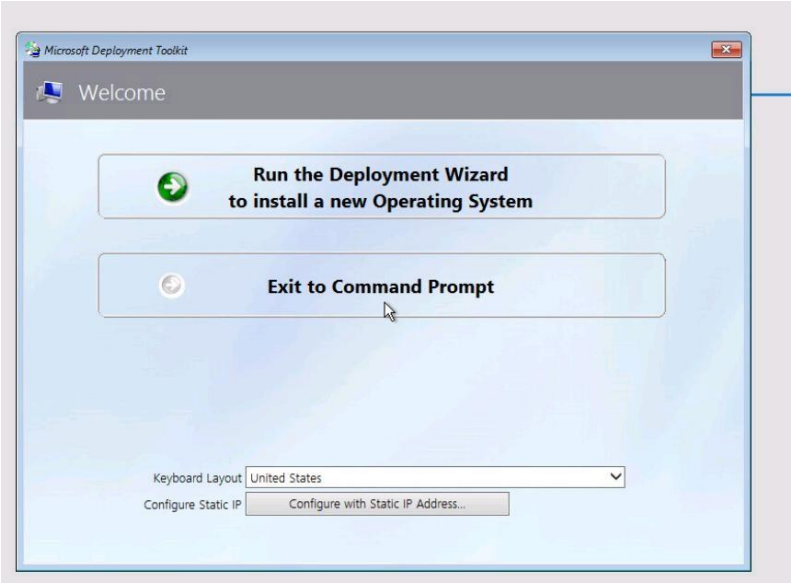
Машина подключится к WDS серверу и получит список доступных загрузочных образов Windows PE. В стандартном диалоге Boot Manager нужно быте выбрать ОС, которую нужно загрузить. В нашем случае это Lite Touch Windows PE (x86).



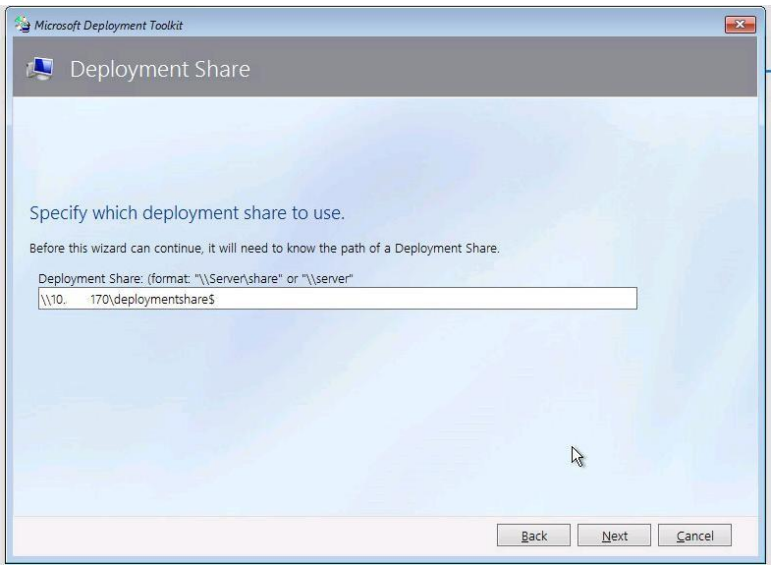
Система начнет загрузку по сети wim образа со средой WinPE и предложит начать установку Windows 10 с помощью мастера Microsoft Deployment Tool Wizard.



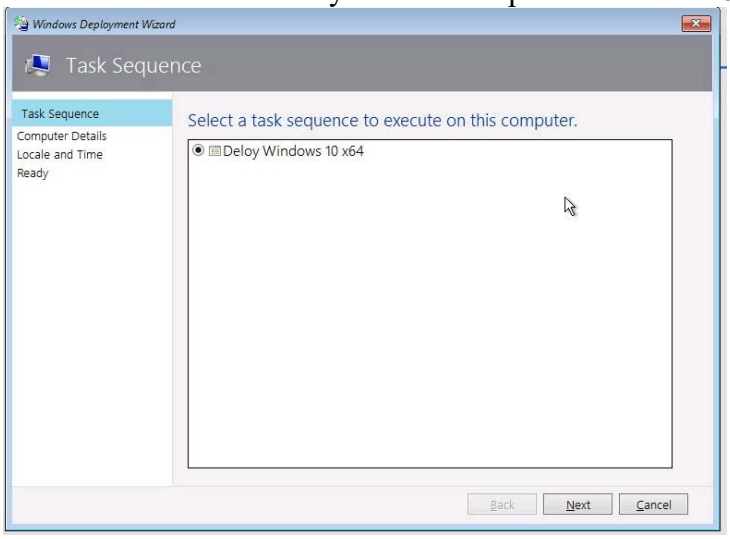
Нажмите на кнопку Run the Deployment Wizard to install a new Operating System для запуска пошагового мастера установки образа Windows 10 на компьютер клиента.



В нашем примере также понадобилось указать UNC путь к сетевой папке DeploymentShare$ на MDT сервере(\\10.1.24.170\DeploymentShare$) и имя+пароль пользователя для доступа к ней.



Осталось среди доступных заданий выбрать созданное ранее Deploy Windows 10 x64 и дождаться окончания сетевой установки образа Windows 10 на этот компьютер.

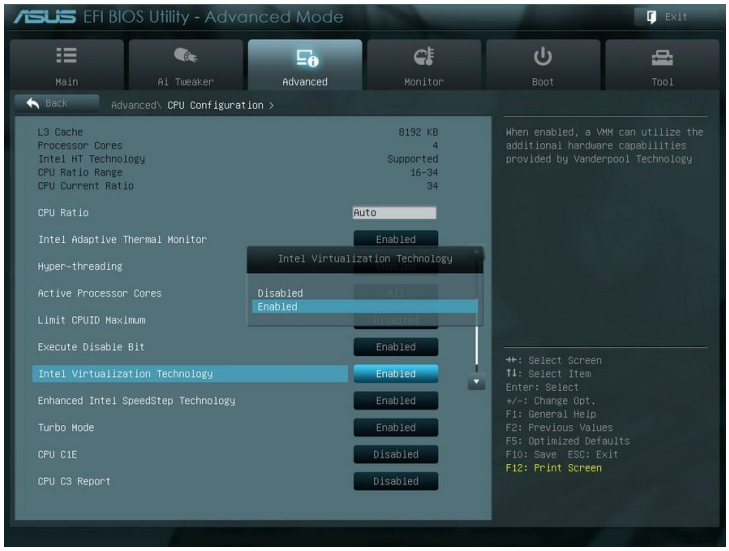


Итак, в этой статье мы показали, как воспользоваться функционалом MDT 2013 и WDS сервера для создания инфраструктуры, позволяющей в автоматическом режиме по сети развернуть образ Windows 10 на клиентах.

2.12 Практическая работа№ 12
Подготовка среды для развертывания операционной системы

Задание:

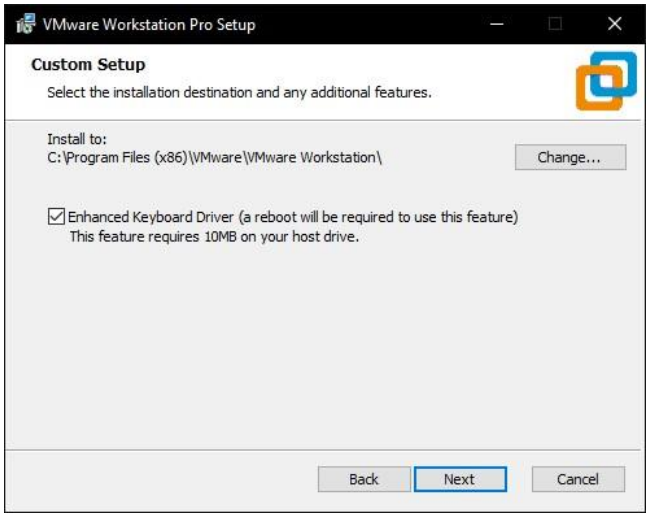
Для функционирования виртуальной машины VMware Workstation Pro нужна 64разрядная система, поддержка аппаратной виртуализации вашим компьютером и активация технологии "Intel Virtualization Technology" или "AMD Virtualization Technology" в BIOS материнской платы



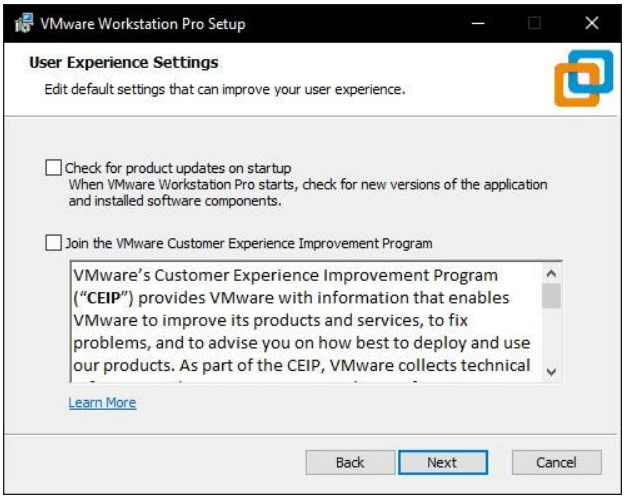
Как установить VMware Workstation Pro

Скачайте VMware Workstation Pro, запустите исполняемый файл и следуйте дальнейшим инструкциям. Мы покажем важные аспекты.

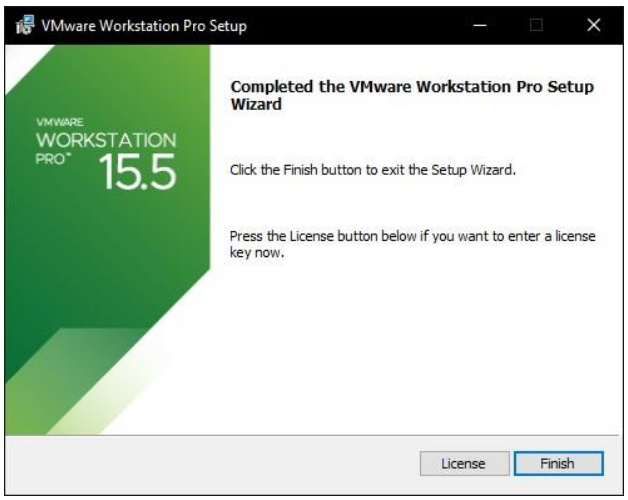
Отметьте галочкой и разрешите установку драйвера клавиатуры.



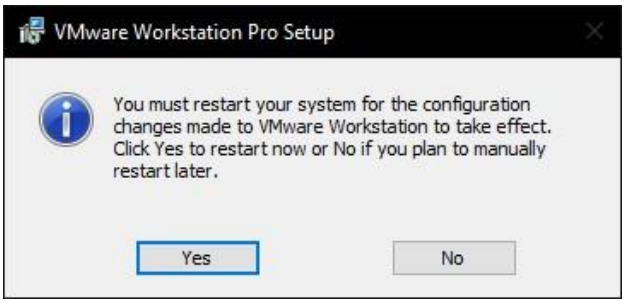
Если необходимо отменить автоматические обновления, отключите верхнюю опцию. А если нет желания принимать участие в программе улучшения качества отправляя анонимные данные и статистику использования VMware Workstation Pro, снимите галочку с нижнего пункта и продолжайте.



На последнем этапе активируйте лицензию нажав по соответствующей кнопке и нажмите "Finish".

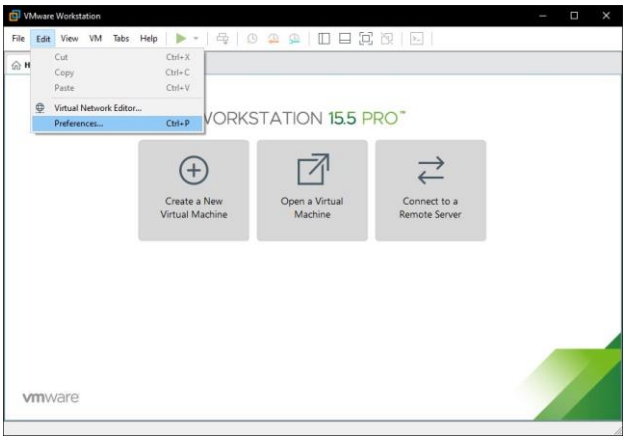


После чего, согласитесь на перезагрузку компьютера.

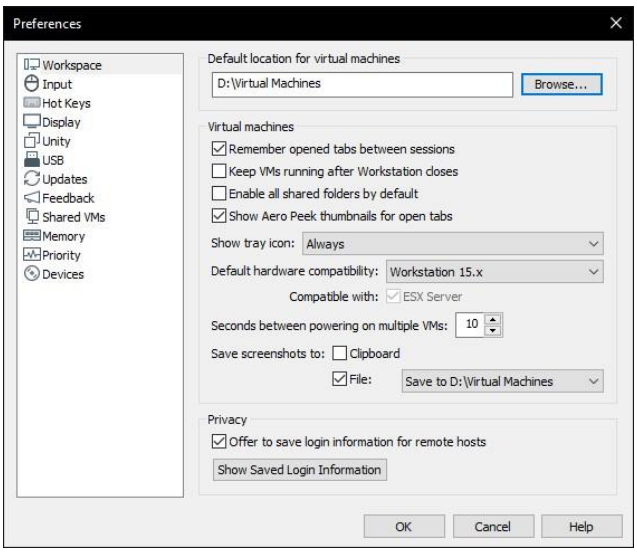


Начальная настройка VMware Workstation Pro

Откройте виртуальную машину, разверните меню "Edit" и зайдите в настройки нажав "Preferences".

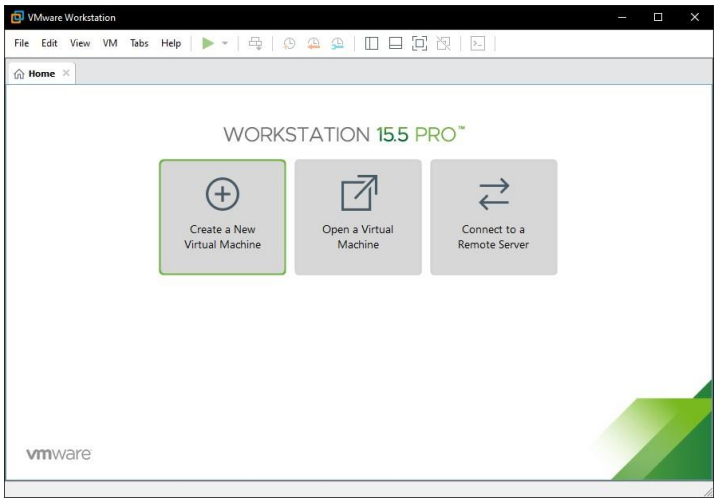


Если требуется изменить расположение виртуальных машин, например из-за нехватки места на основном диске, нажмите кнопку "Browse" и сделайте это.



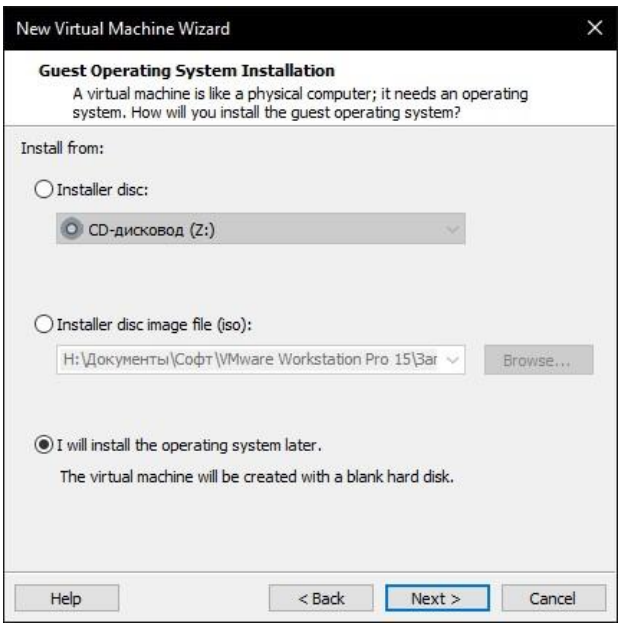
Остальные настройки можно не трогать, по умолчанию отлично подойдет. Как установить Windows 10 в VMware Workstation Pro

Перед началом установкой "Скачайте Windows 10" на компьютер и в главном окне VMware Workstation Pro нажмите большую кнопку "Create a New Virtual Machine".

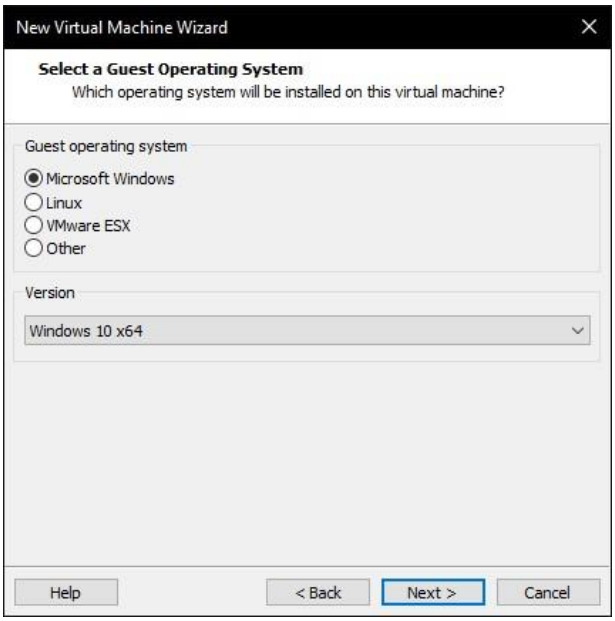


В появившемся окне нажмите мышкой "Next".

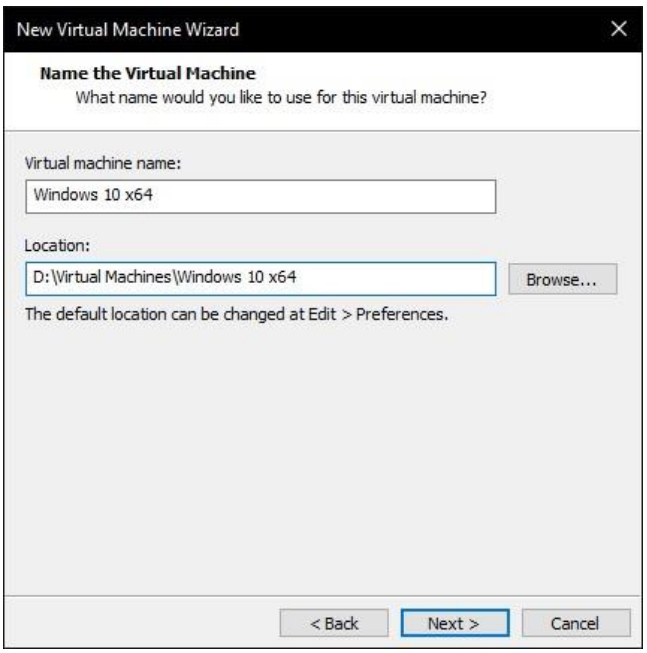
Образ пока выбирайте, просто продолжайте дальше.



Укажите операционную систему и версию.

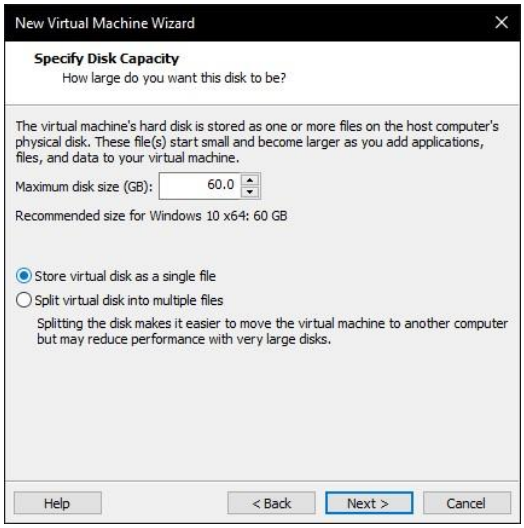


Если необходимо, выберите другую локацию.

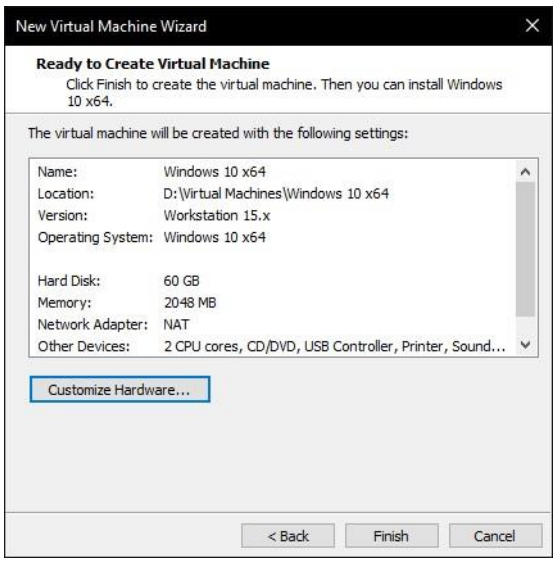


Укажите размер диска и отметьте как сохранить диск:

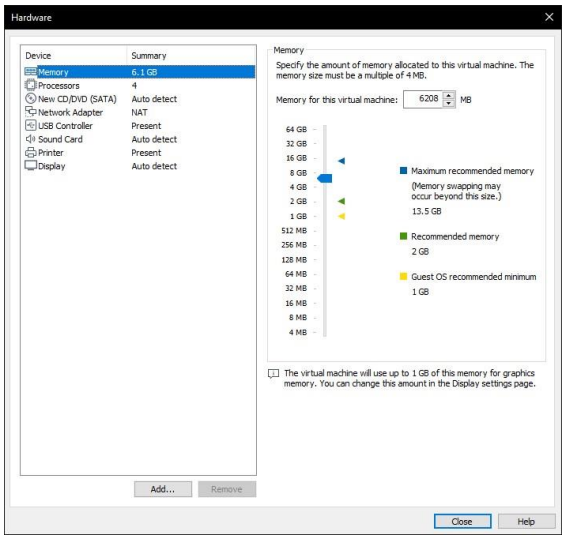
1. Сохранение диска в виде одного файла.
2. Разделение диска на несколько файлов.
3. Если перенос виртуальной машины не планируется и важна производительность, советуем выбрать первый вариант.



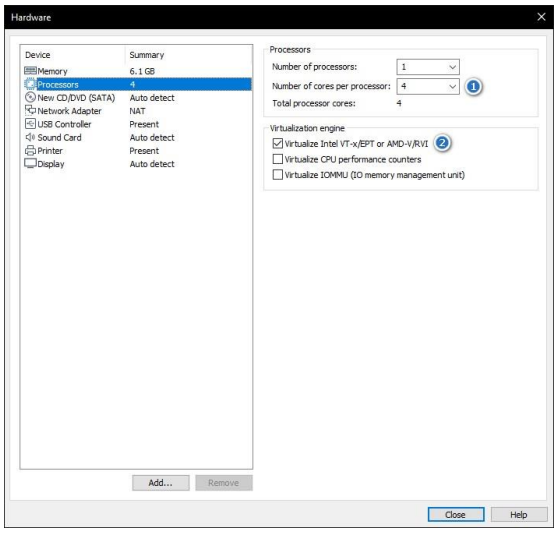
Теперь нажмите "Customize Hardware".



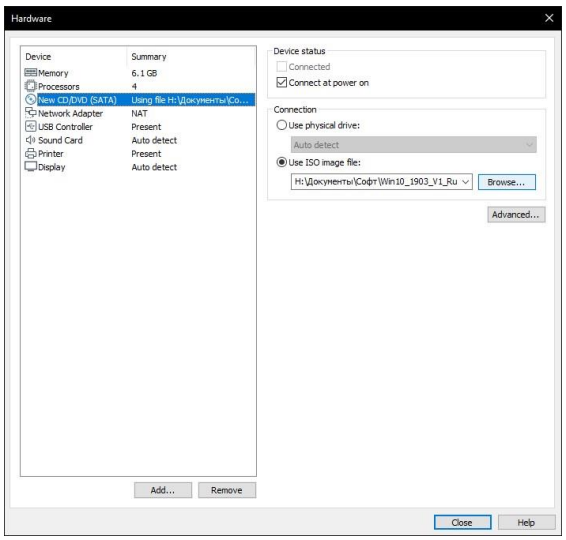
Задайте объём оперативной памяти (рекомендуем 4 гигабайта и более).



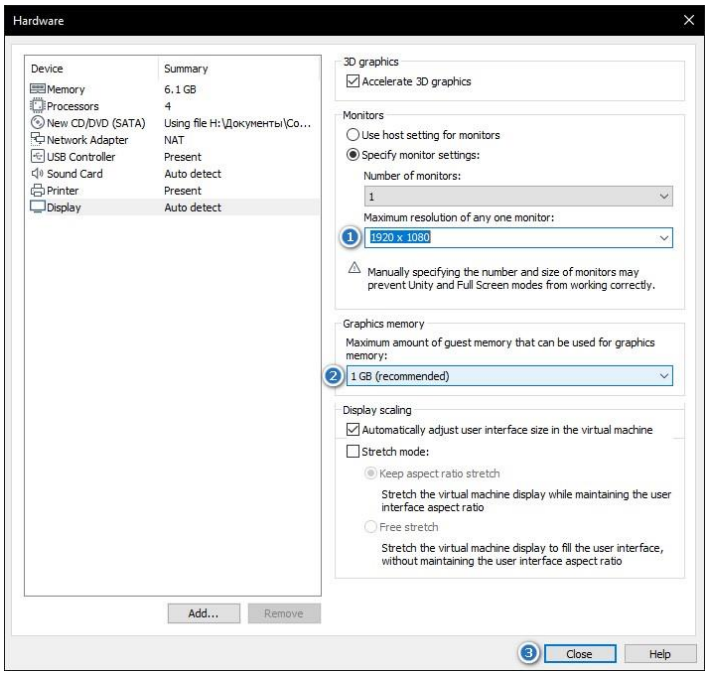
Укажите количество ядер процессора, и активируйте виртуализацию.



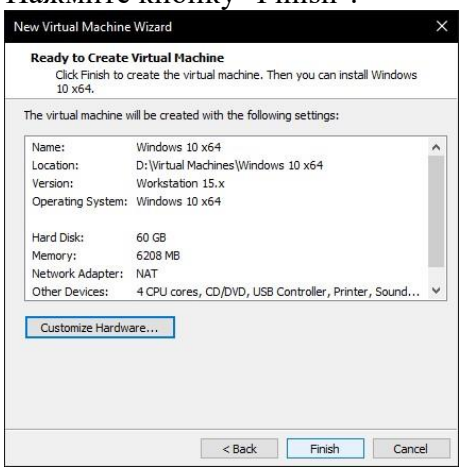
В меню "New CD/DVD (SATA)" отметьте "Use ISO image file" и выберите образ диска Windows 10 через кнопку "Browse".



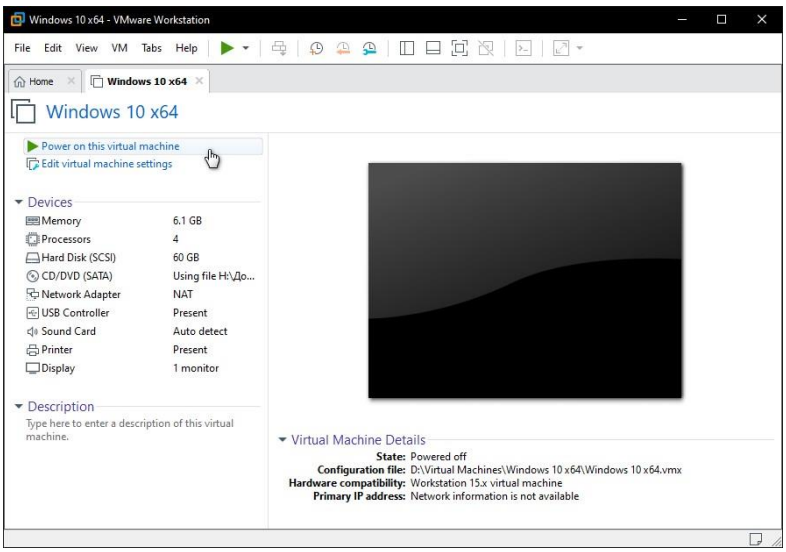
Перейдите в "Display", выберите разрешение экрана, укажите нужный объем графической памяти (можно оставить рекомендованный, но чем больше тем лучше) и закройте данное окно.



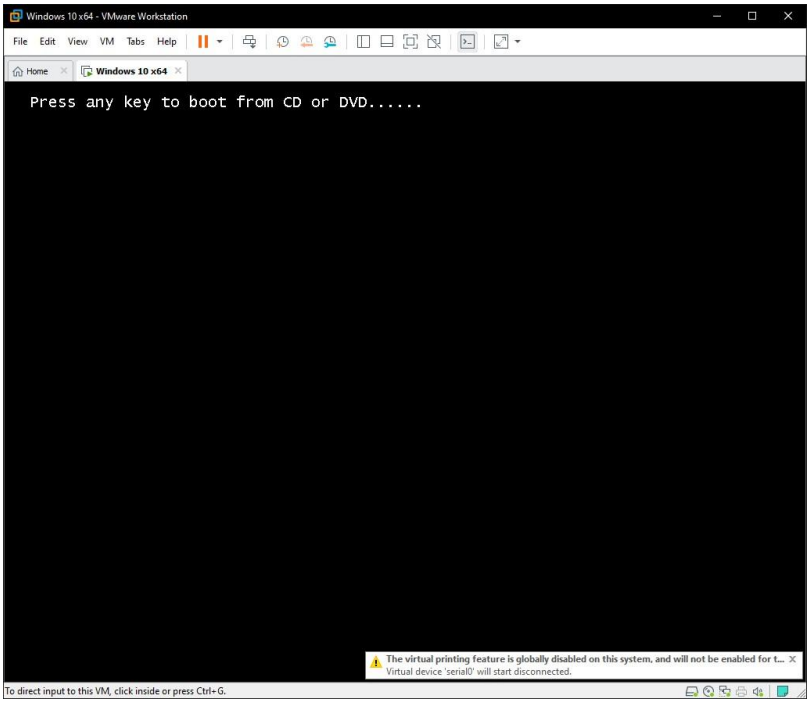
Нажмите кнопку "Finish".



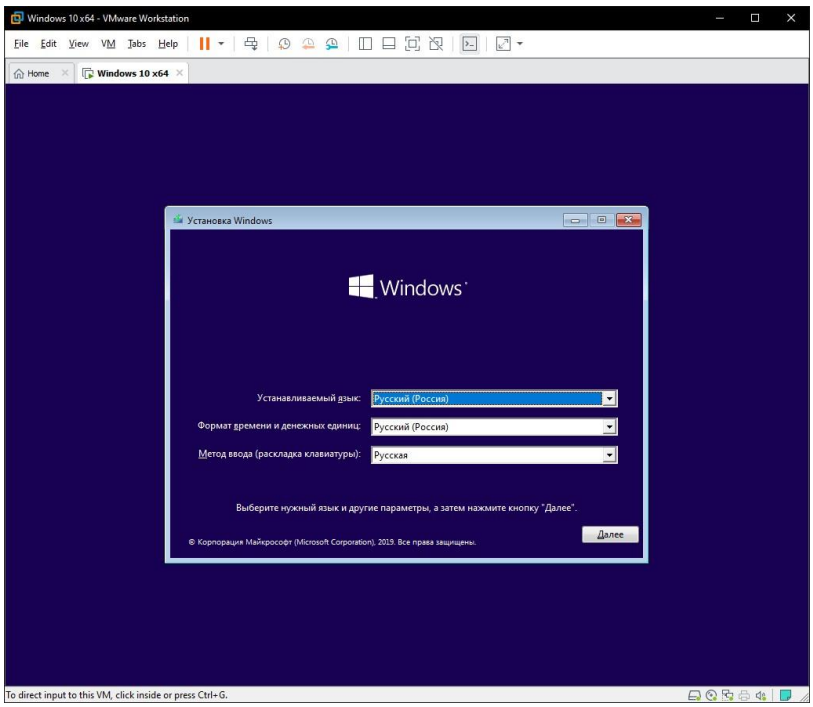
Запустите виртуальную машину нажав "Power on this virtual machine".



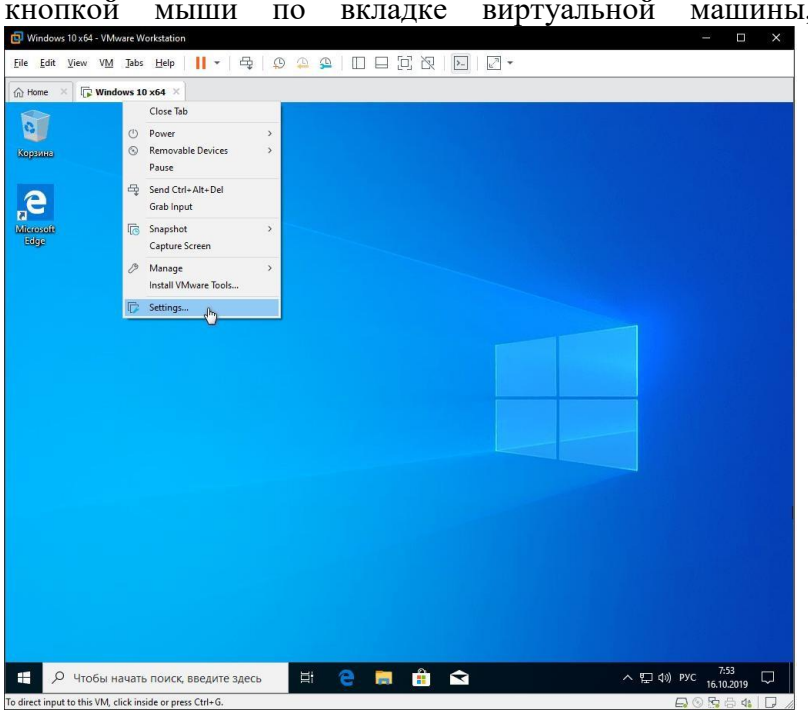
Когда появиться надпись загрузки с компакт-диска нажмите на клавиатуре несколько раз "Enter".



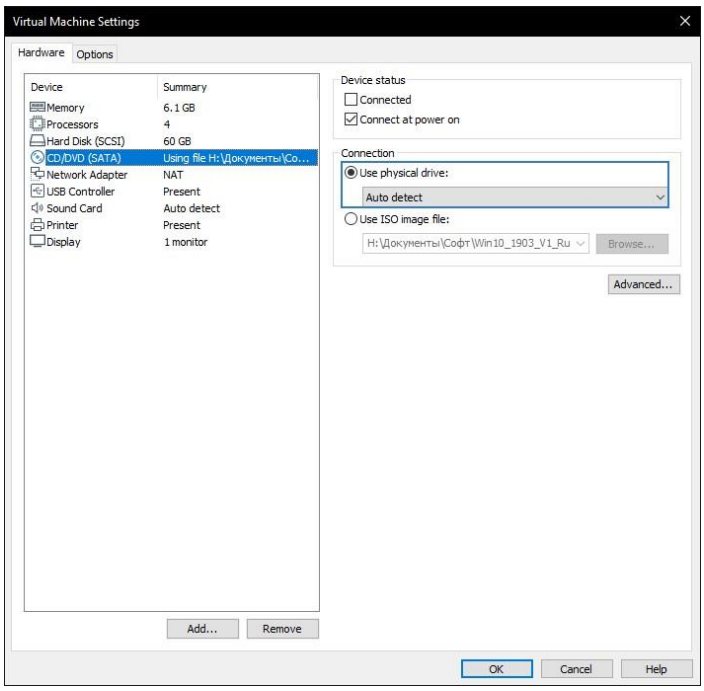
И выполните "Установку Windows 10".



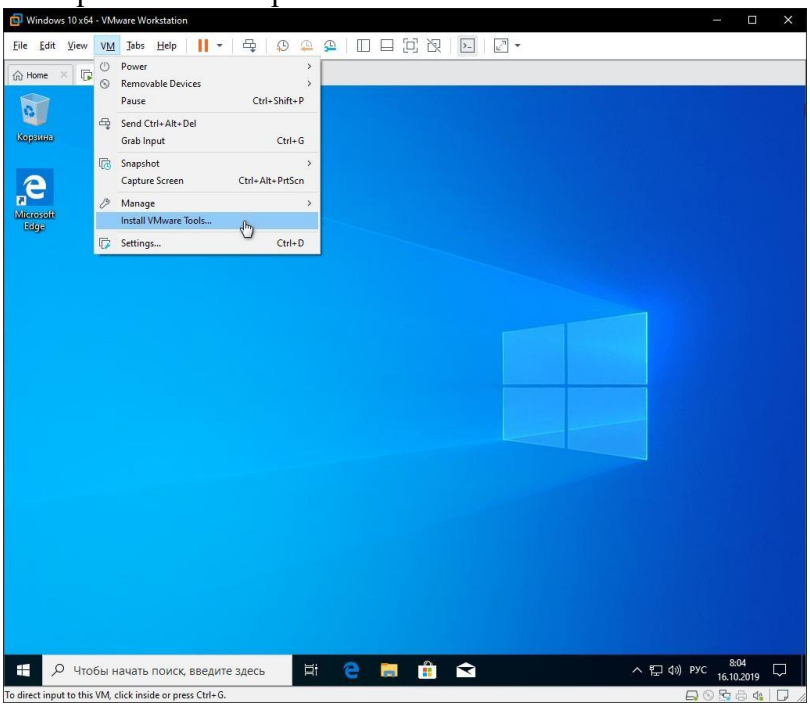
По окончании установки Windows 10 извлеките образ диска, щелкнув правой кнопкой мыши по вкладке виртуальной машины, зайдя в настройки.



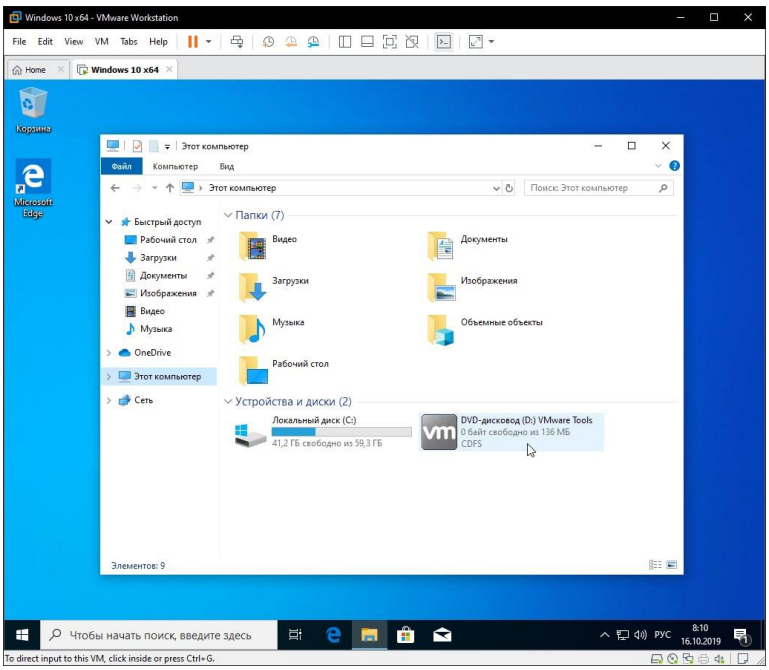
И выбрав в параметрах привода дисков автоопределение.



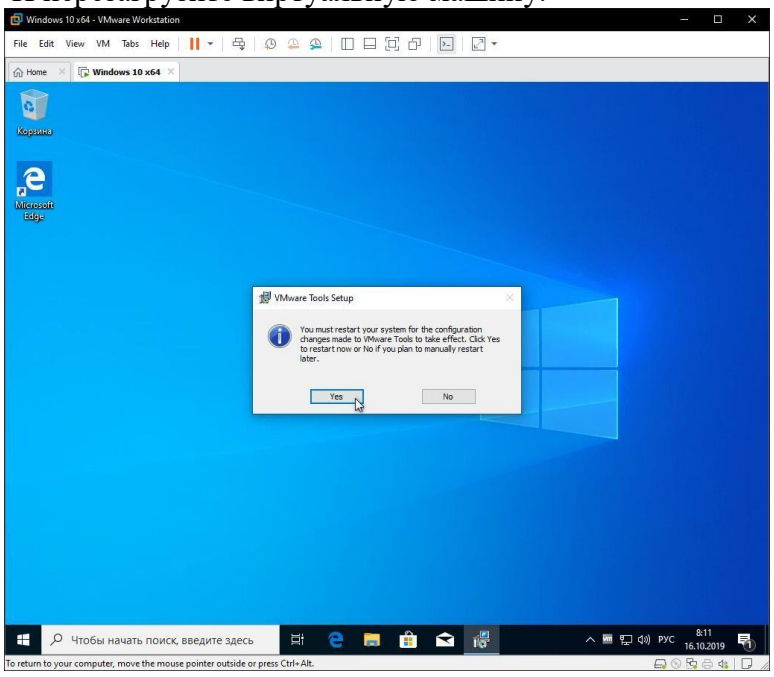
Теперь нажмите верхнее меню "VM" и нажмите "Install VMware Tools".



Зайдите в Проводник > Этот компьютер и запустите установку "VMware Tools" нажав смонтированный образ.

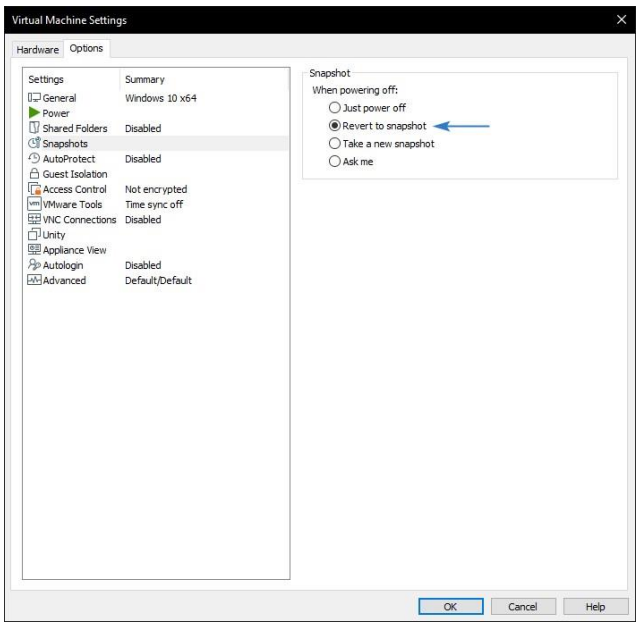


И перезагрузите виртуальную машину.

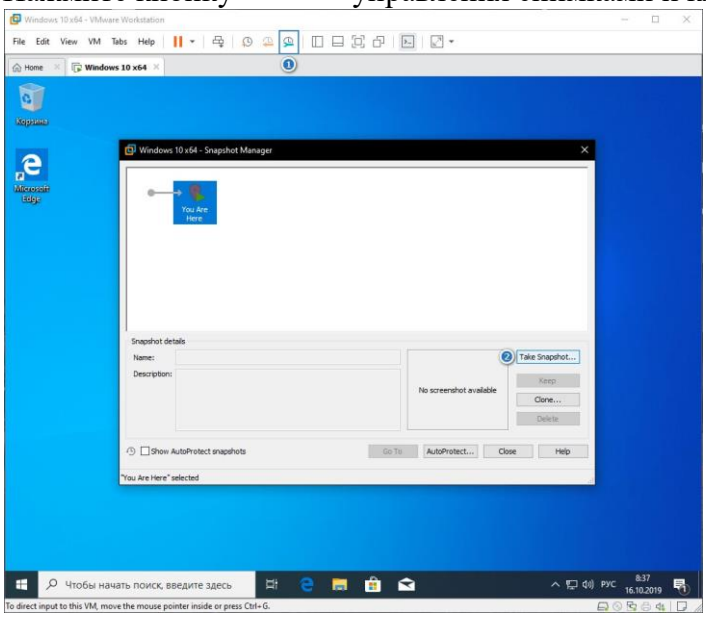


Создание снимка состояния системы в VMware Workstation Pro

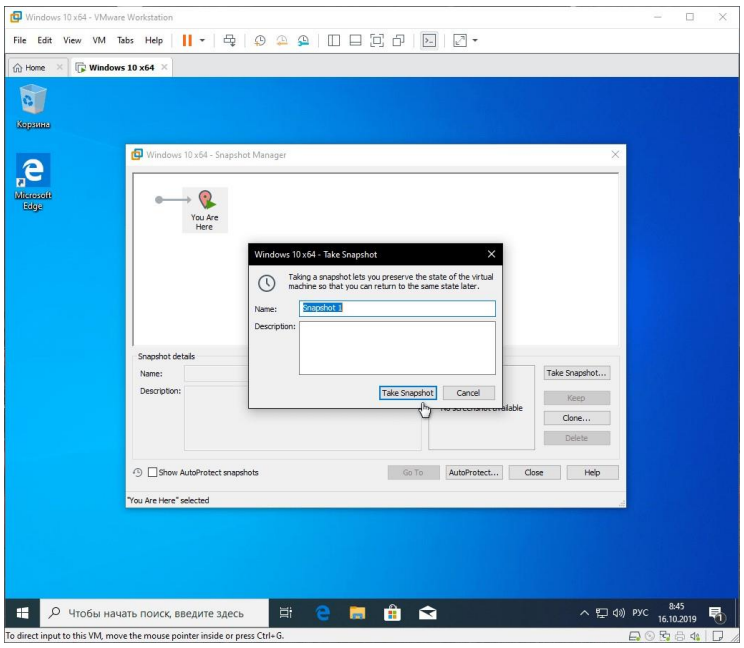
Перед созданием снимка "Настройте Windows 10" под себя. Зайдите в настройки виртуальной машины как было показано немного выше и перейдите на вкладку "Options", нажмите меню "Snapshots", отметьте "Revent to snapshot" и сохраните изменения. Это позволит при выключении машины всегда возвращаться к снимку.



Нажмите кнопку управления снимками и кликните мышкой "Take Snapshot".



Задайте имя снимку и снова нажмите "Take Snapshot".

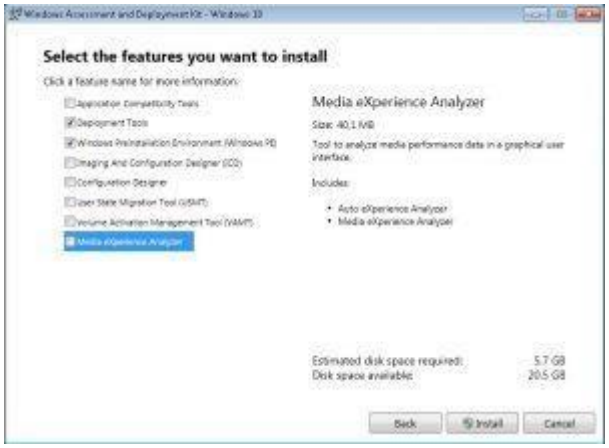


2.13 Практическая работа№ 13
Использование MDT и Configuration Manager для подготовки Zero-Touch Installation

Задание:

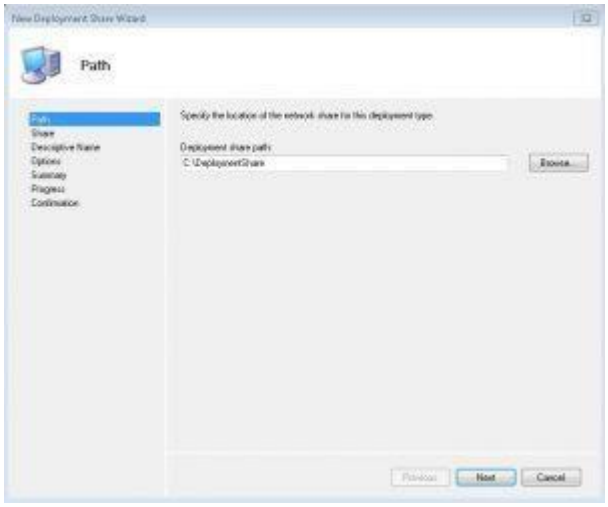
Скачиваем и устанавливаем Windows Assessment and Deployment Kit (Windows ADK) последней версии.

При установке данного средства нужно выбирать обязательно компоненты «средства развертывания» и «среда предустановки Windows PE».



Скачиваем и устанавливаем Microsoft Deployment Toolkit (MDT) со всеми компонентами.

Через интерфейс MDT создаем новый «Deployment Share». Чтобы не было проблем в дальнейшем рекомендуется не менять путь по умолчанию.



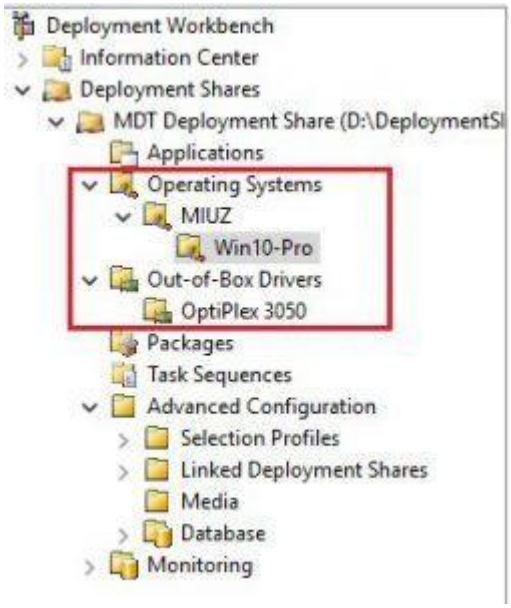
Подготавливаем драйвера для дистрибутива. В моем примере дистрибутив подготавливается для системного блока Dell Optiplex 3050. По сервис-номеру находим нужный системный блок:

http://www.dell.com/support/home/ru/ru/rubsdc/product-support/servicetag/h18cdk2/drivers

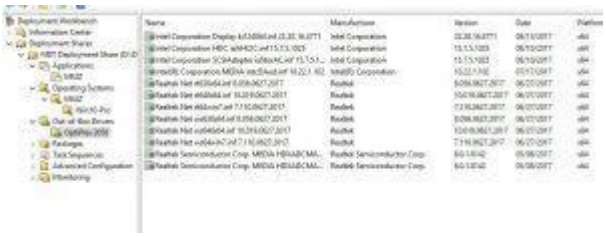
Скачиваем необходимые драйвера для выбранной операционной системы и сохраняем в заранее подготовленные директории:

Распаковываем каждый файл, скачанный с сайта DELL, запустив инсталлятор и нажав на кнопку “Extract” и выбрав соответствующую папку, созданную на предыдущем шаге.

Создаем каталоги в Workbench для дистрибутива операционной системы и для драйверов. Если не планируется в дальнейшем создавать дистрибутивы для других систем или компьютеров, то каталоги можно не создавать.

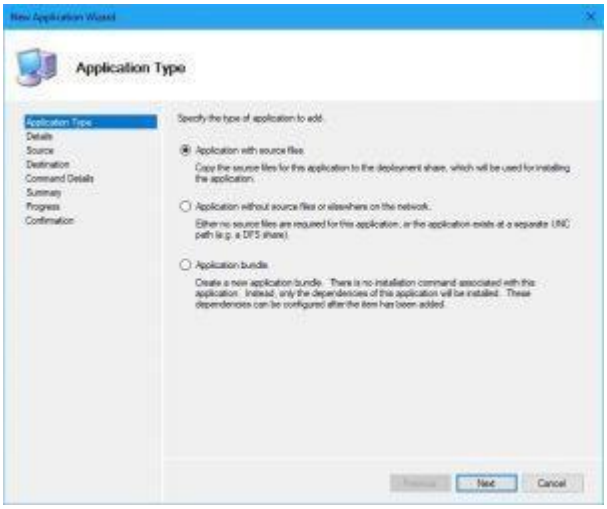


Импортируем драйверы в созданную директорию «Optiplex 3050», после импорта удаляем драйвера для 32-ух битных систем, т.к. планируем распространять только 64битную систему.



В каталог с операционными системами добавляем нужный дистрибутив (образ должен содержать WIM образ, а не ESD)

Добавляем приложения, которые требуется установить в каталог приложений, указав при этом командную строку для тихой установки программ

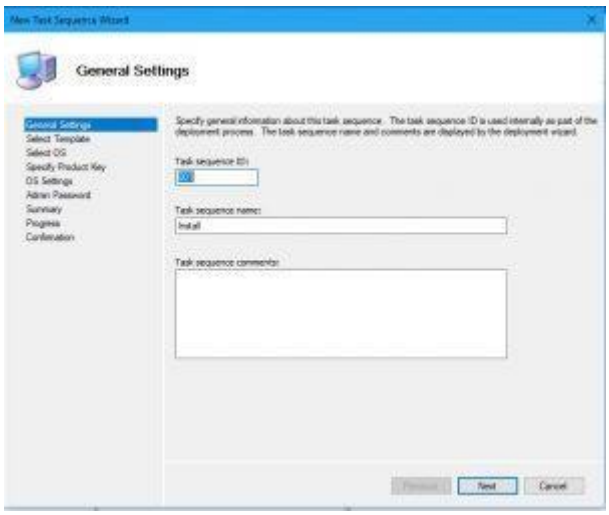


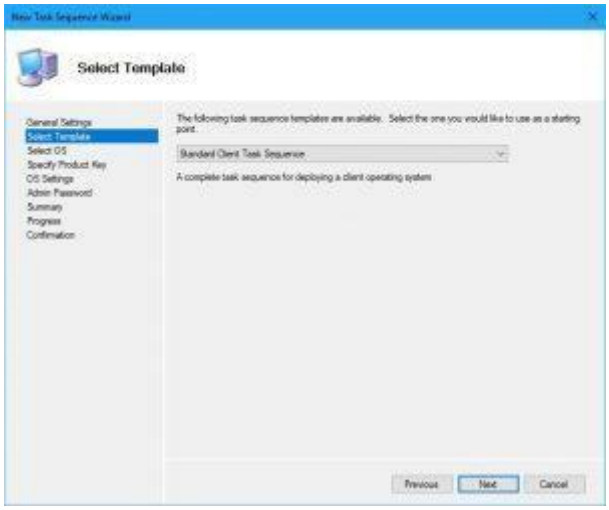
Отдельно стоит упомянуть про установку MS Office 2010. Для его тихой установки при запуске setup.exe нужно добавить ключ, в котором указывается путь до файла config.xml, в котором прописаны некоторые настройки:

```
<Configuration Product="Standard">
<Display Level="none" CompletionNotice="no" SuppressModal="yes"  cceptEu-
la="yes" />
<PIDKEY Value="AAAAABBBBBCCCCCDDDDDEEEEE" />
<USERNAME Value= '%username%' />
<COMPANYNAME Value="Рога и Копыта" />
<INSTALLLOCATION Value="%programfiles%\Microsoft Office" />
<Setting Id="SETUP_REBOOT" Value="NEVER" />
</Configuration>
```

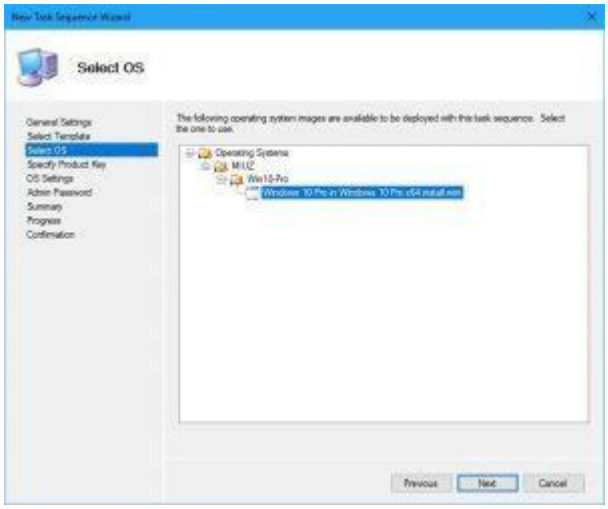
PIDKEY – это ключ активации MS Office

Создаем новый стандартный Task Sequence. Task sequence ID – используется в автоматизации установки, поэтому лучше создавать его числовым.

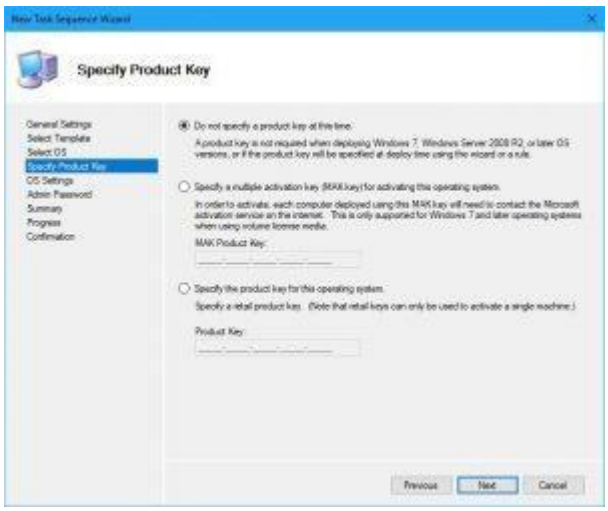




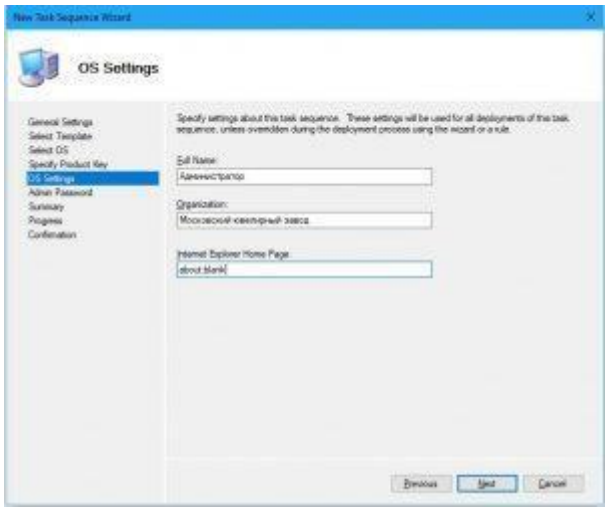
Указываем wim-файл из дистрибутива, который будет использоваться в этом task sequence. В дальнейшем его можно будет поменять.



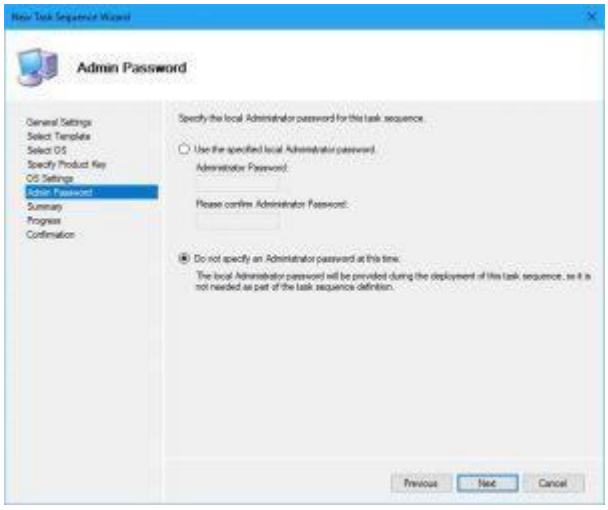
Можно сразу указать ключ установки.



Указываем владельца дистрибутива. Строчка с домашней страницей в Internet Explorer не работает для Windows 10

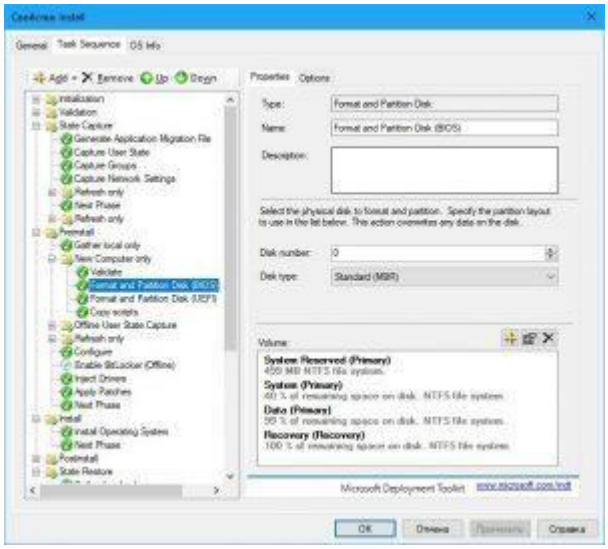


Указываем пароль локального администратора. Для русского дистрибутива учетная запись будет называться «Администратор». Выбирая 2-ой пункт учетная запись не будет иметь пароля.

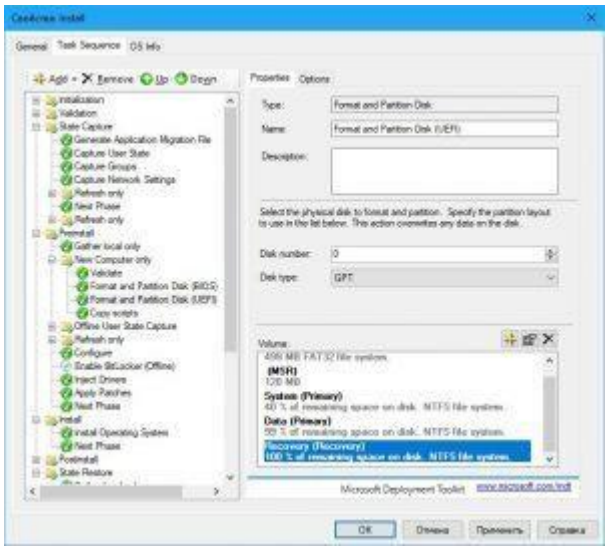


Открываем свойства только что созданного Task Sequence и во вкладке «Task Sequence» находим слева строку «Format and Partition Disk (BIOS)». Здесь надо указать

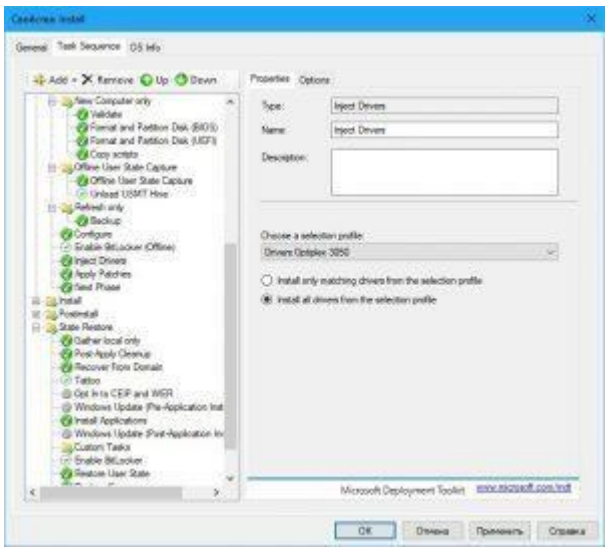
как будет разбиваться диск на компьютере с BIOS. Я сделал настройки так, как представлены на скриншоте: 40% пространства диска выделяется на системный раздел, из оставшегося пространства берется 99% и забирается под раздел с данными. Оставшаяся часть – раздел восстановления. В начале диска оставляем раздел для загрузки.



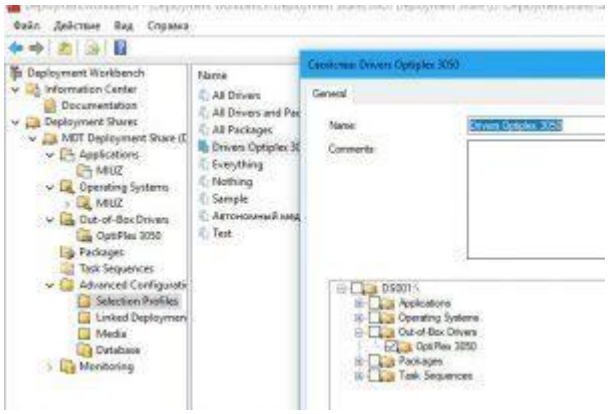
Тоже самое проделываем и для компьютеров с UEFI, только разделы в начале диска будут другие – EFI и MSR.



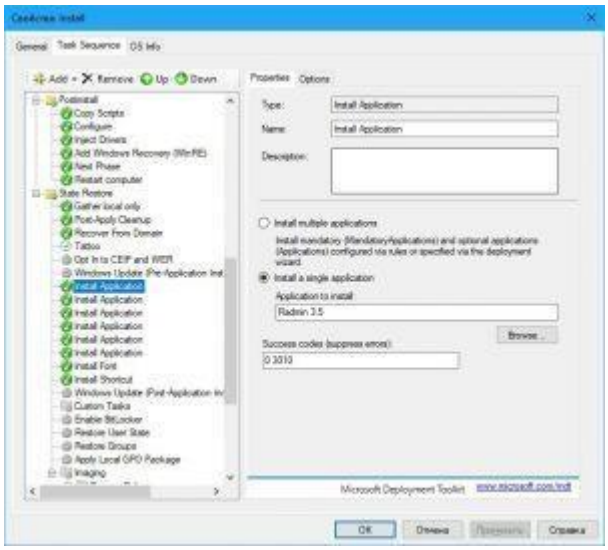
В разделе Inject Drivers нужно указать профиль, в котором выбраны драйверы, которые в свою очередь, требуется внедрить в настраиваемый дистрибутив. Если нужно указать несколько профилей, то через меню Add – General – Inject Drivers добавляем еще одну задачу добавления драйверов.



Профиль заранее создаем в соответствующем разделе.



Ниже в разделе слева находим строку «Install Application». Указываем приложение, которое требуется установить. Если требуется установить несколько приложений, то добавляем такие задачи через меню Add – General – Install Application

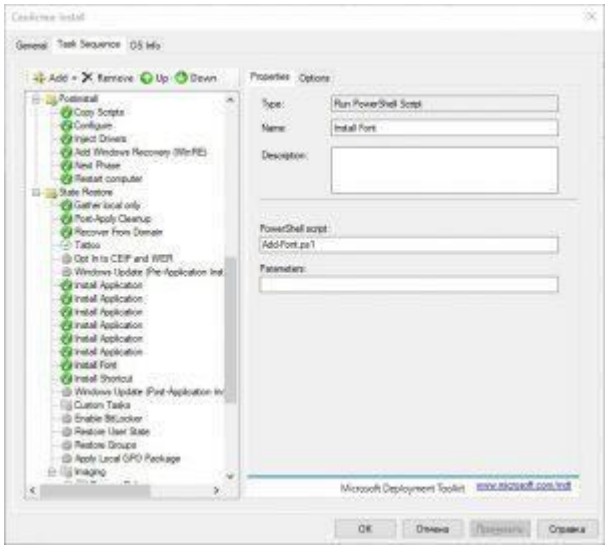


Если требуется установить шрифт, то предварительно требуется создать Powershell-скрипт, например, «Add-Font.ps1» со следующим содержимым:

```
Set-ExecutionPolicy RemoteSigned -Force
```

```
$fonts = (New-Object -ComObject Shell.Application).Namespace(0x14)
dir *.ttf | %{ $fonts.CopyHere($_.fullname) }
```

Скрипт ищет шрифт с расширением ttf в той же директории, где располагается и сам скрипт. Сам скрипт и шрифт копируем в папку «..\DeploymentShare\Scripts».В Task Sequence через меню Add – General – Run Powershell Script добавляем задачу по запуску PS-скрипта. Указываем в ней название скрипта без параметров. Название задачи вписываем английскими буквами, иначе при инсталляции будут отображаться некорректно символы. Если в PS-скрипте требуется выполнить команду, которая доступна только из командной строки, то тогда вписываем ее в таком виде: cmd /c «команда», иначе выполнение всего скрипта прервется и установка завершится ошибкой



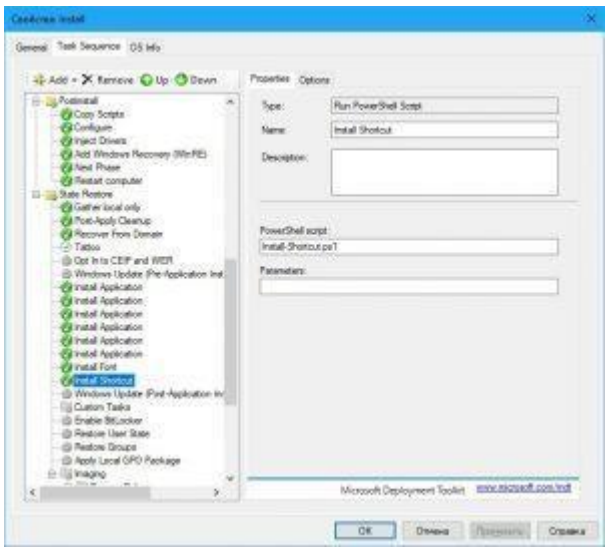
Для создания ярлыков добавим еще один PS-скрипт, который назовем «Install-Shortcut.ps1». В нем будет записаны команды: cp "Портал.url" "C:\Users\Default\Desktop" cp "Портал.url" "C:\Users\Администратор\Desktop" del "C:\Users\Public\Desktop\Adobe Reader 9.lnk"

добавляем ярлык в общий профиль и в профиль Администратора и удаляем ярлык Adobe Reader, который устанавливается на рабочем столе каждого пользователя. Оригинальный ярлык должен находиться там же, где и сам скрипт. Копируем скрипт и ярлык в директорию «..\DeploymentShare\Scripts».

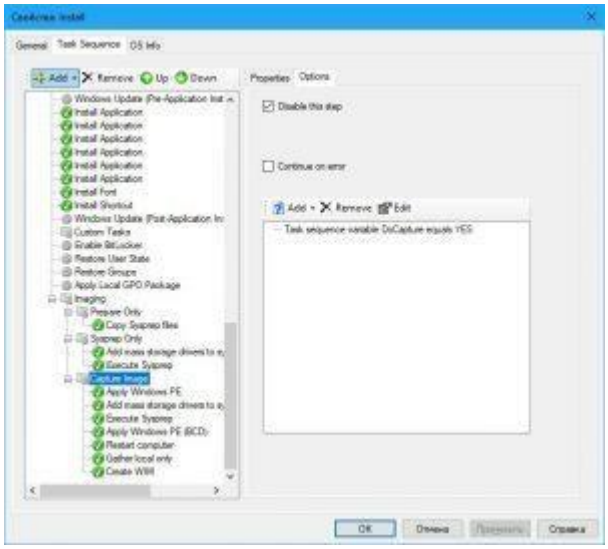
Если требуется изменить значение реестра, то тогда создаем файл .reg и делаем его импорт командой:

reg import Edit_Reestr.reg

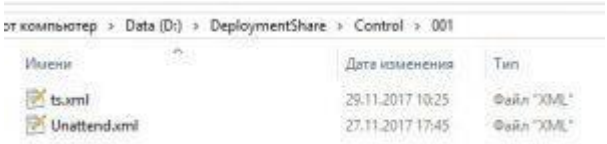
В результате в Task Sequence нужно указать только имя скрипта



Все задачи после запуска скриптов можно отключить, потому что они не требуются, если надо только установить систему (без sysprep и захвата). Для этого берем, например, задачу «Capture Image» и в Options ставим галочку «Disable this step».

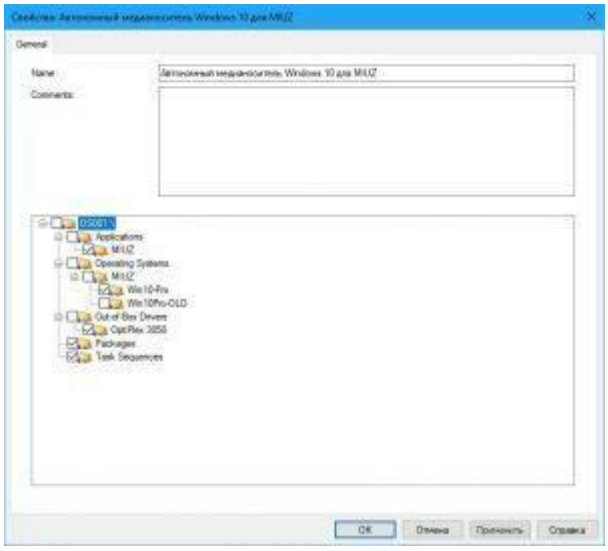


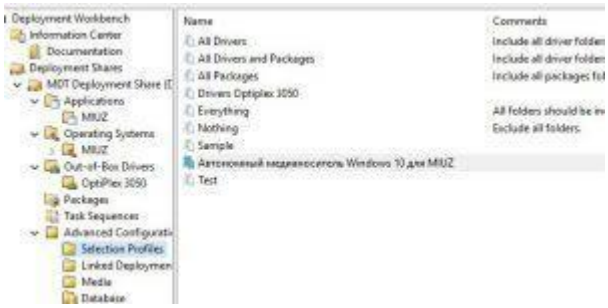
Если требуется изменить параметры, которые вводились в момент создания Task Sequence, то для этого нужно найти файл Unattend.xml, который лежим в папке с именем, совпадающим с идентификатором этого Task Sequence, которая в свою очередь лежит в папке «Control». В нем, например, можно поменять пароль администратора, который был ранее задан.



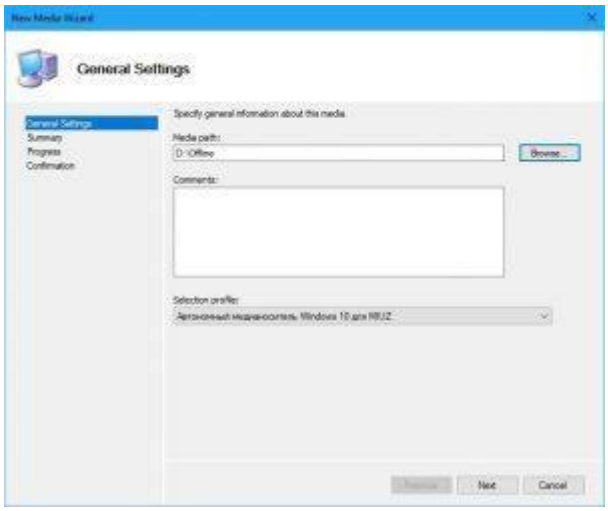
В папке с профилями создаем еще один профиль, назовем ее «Автономный медиаоноситель Windows 10 для MIUZ». В нем указываем те директории, которые необходимо

скомпоновать в один ISO-файл, с которого и будет происходить установка системы: указываем приложения, операционные системы, драйвера, пакеты и Task Sequence.

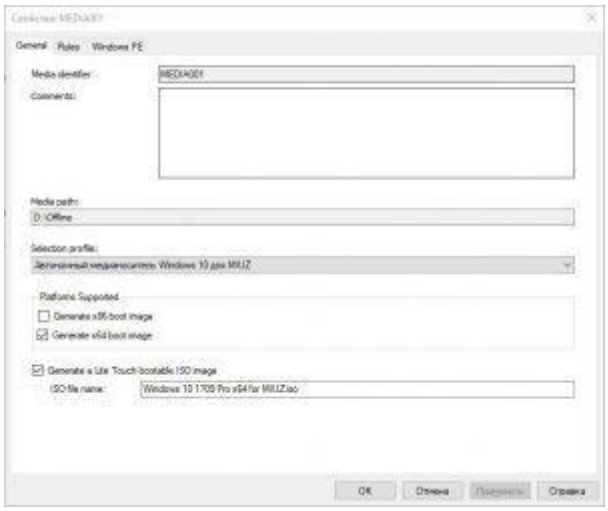




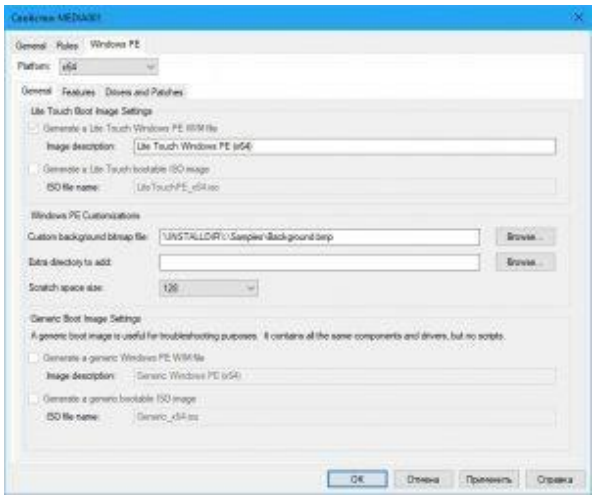
В разделе «Media» через команду «New Media» создаем новый носитель, в котором указываем путь, где будут храниться файлы, из которых будет создаваться ISO-образ и указываем профиль, который создали на предыдущем шаге. Важно: путь в строке «Media path» не должен содержать русские символы, иначе будут ошибки в дальнейшем.

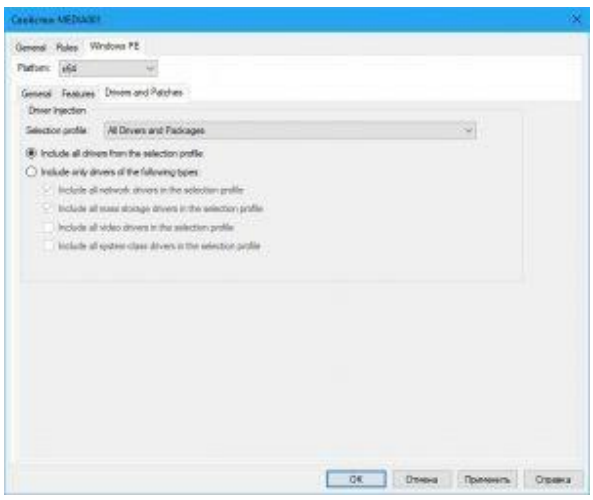


После создания нового «Media» заходим в его свойства. Указываем, что загрузочный образ будет генерироваться только 64-битный (т.к. система, которую требуется устанавливать, только 64-битная). Указываем имя ISO-файла, которое будет создаваться.

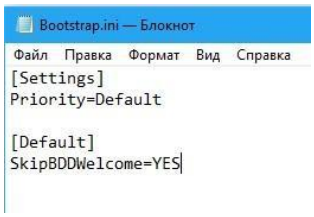


Во вкладке Windows PE для платформы x64 указываем «Scratch space size» указываем значение 128. Во вкладке «Drivers and Patches» можно выбрать какие драйвера добавлять в образ Windows PE.





Во вкладке «Rules» прописываются настройки, которые исполняются в момент запуска Windows PE из создаваемого ISO-файла. Причем настройки в файле Bootstrap.ini исполняются до момента запуска Windows PE. Поэтому в нем может быть прописано, где брать сам загрузчик с Windows PE (в случаях если он распространяется не через ISO-файл, а через PXE). Для нашего случая в нем прописываем только одну строку, которая отключает показ сообщения после запуска Windows PE.



Все настройки, которые прописаны в самой вкладке «Rules», находятся в файле CustomSettings.ini в папке Control. Все они нужны, чтобы установка дистрибутива происходила без вопросов (режим ZTI):

[Settings]
Priority=Default
Properties=MyCustomProperty
[Default]
_SMSTSORGNAME=MIUZ
DeploymentType=NEWCOMPUTER
OSDComputerName=Temp001
TaskSequenceID=001
SkipTaskSequence=YES
SkipDomainMembership=YES
TimeZone=145
TimeZoneName=Russia TZ 2 Standard Time
SkipTimeZone=YES
SkipLocaleSelection=YES
FinishAction=Reboot
DoCapture=NO
OSInstall=Y
SkipCapture=YES
SkipAdminPassword=YES
SkipProductKey=YES
SkipComputerBackup=YES
SkipComputerName=YES
SkipBitLocker=YES

JoinWorkgroup=MIUZ

SkipUserData=YES
SkipFinalSummary=YES

BdeInstallSuppress=YES

UserDataLocation =NONE

USMTOfflineMigration=FALSE

SkipSummary=YES

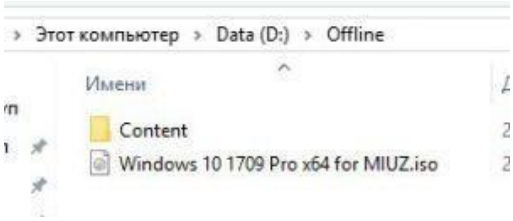
UserLocale=ru-ru

UILanguage=ru-ru

KeyboardLocale=ru-ru

HideShell=YES

После того, как все настройки в «Media» сделаны, необходимо «обновить» контент в нем. Для этого нажимаем правой кнопкой мыши на «MEDIA001» и нажимаем на «Update Media Content». Будет обновлена директория, которая указана в свойствах этого носителя (скопированы все файлы и настройки, указанные в профиле, из папки DeploymentShare). После этого заходим в директорию этого «Media». В ней можно увидеть папку Content и ISO-файл.



ISO-файл можно записывать на DVD-болванку и идти устанавливать систему. Этот ISOфайл генерируется из папок и файлов, содержащихся в папке «Content». Если требуется записать полученный ISO на флешку, то требуется выполнить следующие действия:

а) на физическом компьютере под управлением Windows 7 или более поздних версий вставьте нужный USB-накопитель.

б) скопируйте содержимое папки Offline\Content в корень USB-накопителя.

в) запустите командную строку от имени администратора и выполните команду diskpart

г) введите list vol, чтобы перечислить тома

д) введите sel vol [номер тома, являющимся USB-накопителем]

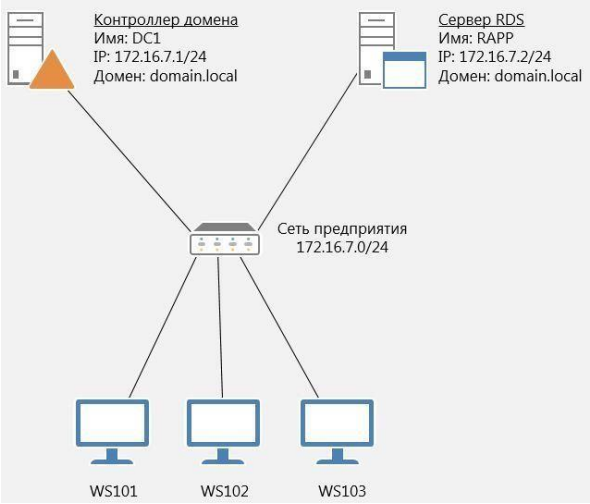
е) введите active, а затем введите exit

После этих манипуляций загрузочная флешка с вашим кастомным образом Windows 10 будет готова. Ко всему прочему Windows будет устанавливаться автоматически без дополнительных вопросов.

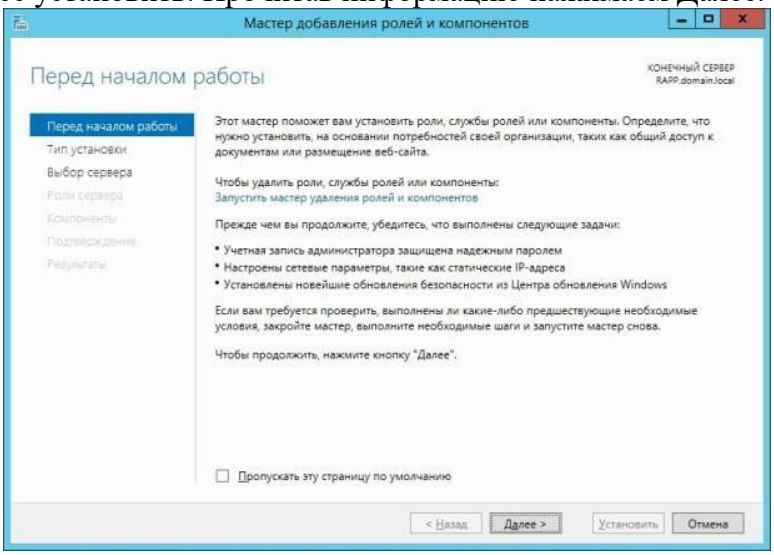
2.14 Практическая работа№ 14
Планирование и реализация инфраструктуры Remote Desktop Services

Задание:

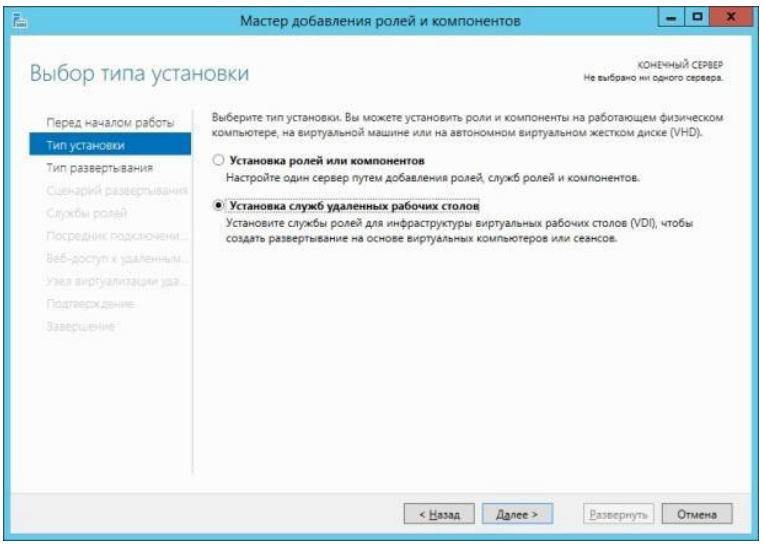
Перед тем, как начать установку RDS на сервер необходимо ознакомиться с существующей инфраструктурой сети. В данном случае, это тестовая сеть, состоящая из контроллера домена DC1 со статическим адресом 172.16.7.1/24, сервера на который будут установлены службы RDS — RAPP, с адресом 172.16.7.2/24 и рабочих станций WS101, WS102, WS103, получающих IP-адреса по DHCP. Все компьютеры сети подключены к домену domain.local



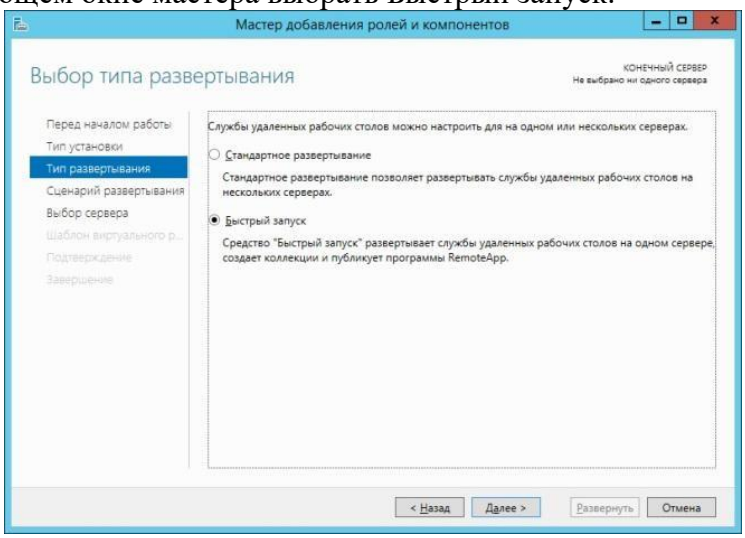
На сервере RAPP необходимо открыть Диспетчер серверов. Для этого можно нажать на соответствующую иконку на панели задач или выполнить команду servermanager.exe В окне диспетчера выбираем Управление — Добавить роли и компоненты, после чего откроется окно мастера добавления ролей и компонентов. В первом его окне предлагается ознакомиться с основными требованиями к серверам, на которые будут устанавливаться роли. Также здесь можно установить галочку, которая позволит пропускать эту информацию при добавлении новых компонентов и ролей. При частой установке бывает полезно её установить. Прочитав информацию нажимаем Далее.



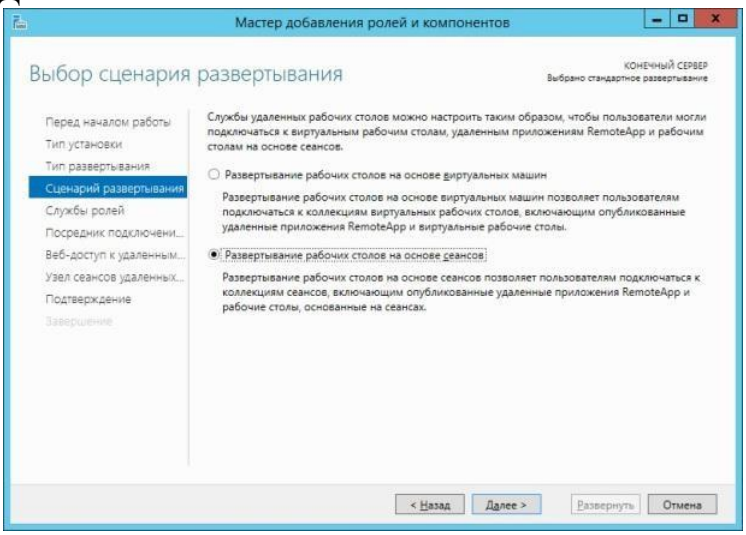
В следующем окне предлагается выбрать тип установки. Отмечаем пункт Установка служб удалённых рабочих столов.



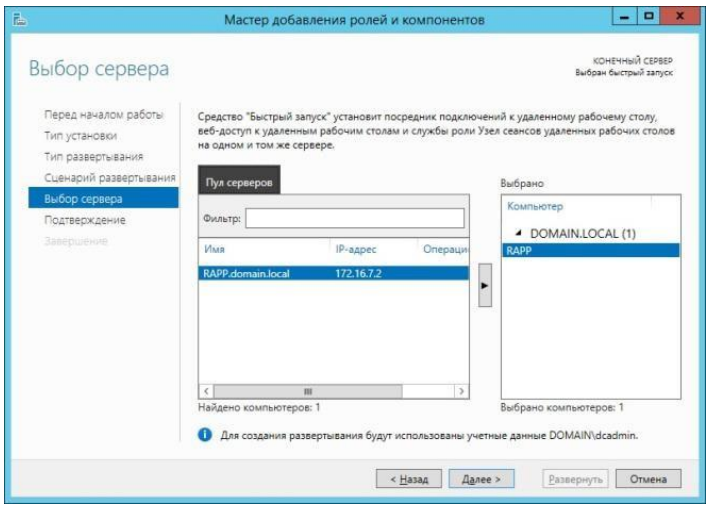
Так как мы производим установку всех служб RDS на один сервер, то целесообразно в следующем окне мастера выбрать Быстрый запуск.



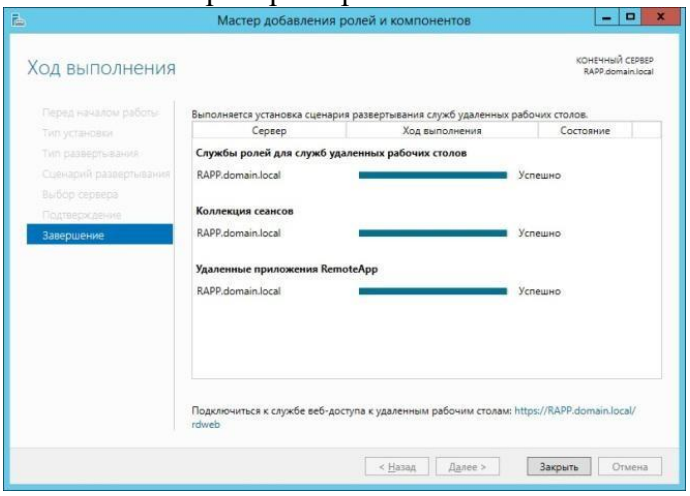
Далее выбираем сценарий развертывания RDS. Нас интересует создание среды удалённых рабочих столов на основе сеансов. Поэтому выбираем соответствующую опцию и жмём Далее.



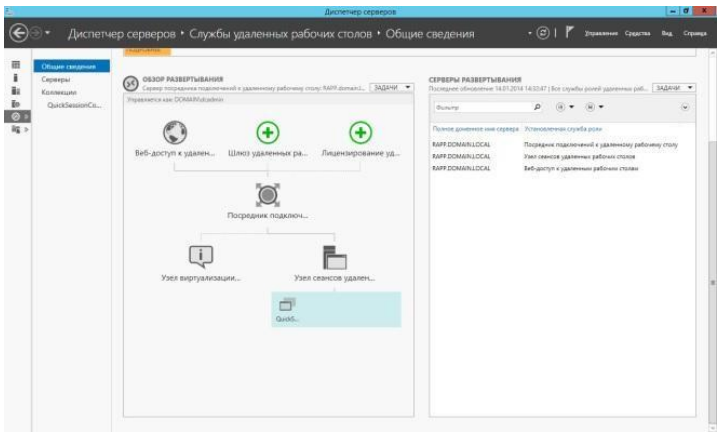
В следующем окне мастера предлагается выбрать сервер, на котором будут развернуты службы RDS. В нашем случае это сервер RAPP.domain.local. После того, как выбор сделан, жмём Далее.



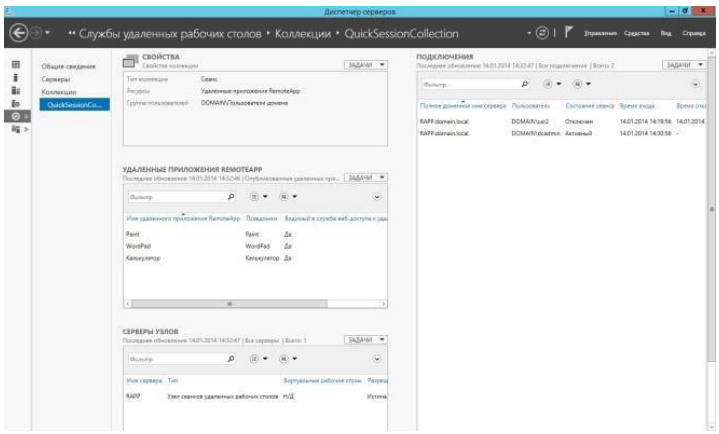
После выбора сервера мы увидим окно с подтверждением выбранных служб и именем сервера, на который будут установлены эти службы. Тут же необходимо согласиться с тем, что сервер будет перезагружен, поставив соответствующую галочку и нажать кнопку Развернуть, после чего откроется окно в котором будет отображен процесс развёртывания ролей RDS. В процессе выполнения установки сервер будет перезагружен. После перезагрузки сервера, необходимо зайти под той же учётной записью, под которой был начат процесс установки (в данном случае это domain\dcadmin) и спустя некоторое время откроется окно мастера и развёртывание возобновится автоматически.



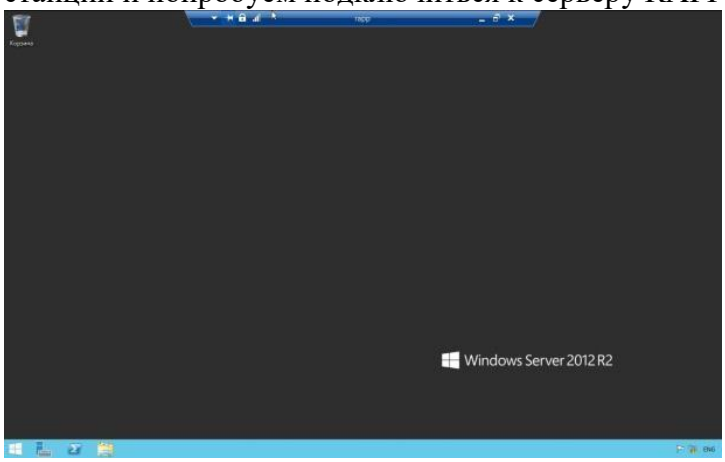
После завершения установки, мастер отрапортует о состоянии всех служб и сообщит ссылку для организации веб-доступа к удалённым рабочим столам.
Когда мастер завершит развёртывание RDS, можно будет посмотреть какие роли установлены. Для этого заходим в диспетчер серверов и выбираем в левой панели пункт Службы удалённых рабочих столов. На вкладке Общие сведения мы можем увидеть, что сервер RAPP в данном развёртывании будет выступать в роли посредника подключений к удалённому рабочему столу, узла сеансов удалённых рабочих столов и узла веб-доступа к удалённым рабочим столам.



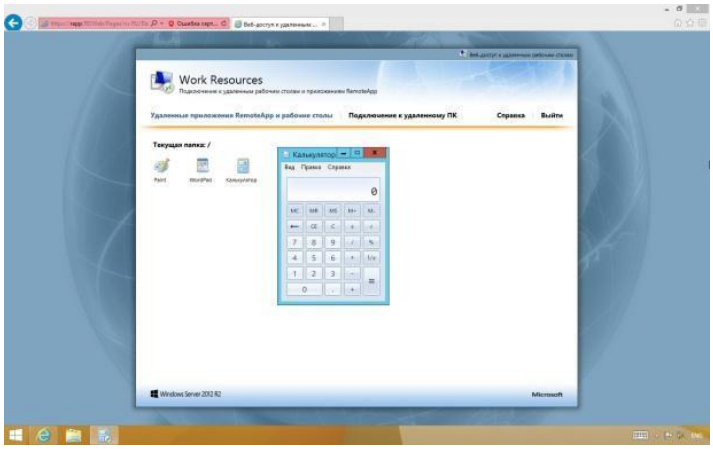
Так же мы видим, что кроме этих служб была установлена коллекция QuickSessionCollection в которую входят несколько стандартных приложений RemoteApp, а именно Paint, WordPad и Калькулятор.



Проверим работоспособность установленной системы. Для этого зайдём на одну из рабочих станций и попробуем подключиться к серверу RAPP.



Проверим работу веб-доступа к удалённым приложениям. Для этого перейдем по ссылке, которую мы получили в процессе работы мастера установки ролей и компонентов — https://rapp.domain.local/rdweb



Как видим, подключение удалось. Это значит, что все роли служб удалённых рабочих столов настроены корректно и могут обслуживать клиентов. Единственное что осталось сделать, перед тем как давать доступ для клиентов — это установить службу лицензирования, но об этом далее в этой статье.
Следует помнить, что в доменной среде пользователей не обязательно добавлять в группу «Пользователи удалённого рабочего стола» т.к. при развёртывании RDS в эту группу автоматически добавляется группа «Пользователи домена».

2.15 Практическая работа№ 15
Расширение доступа к Интернет для инфраструктуры RDS

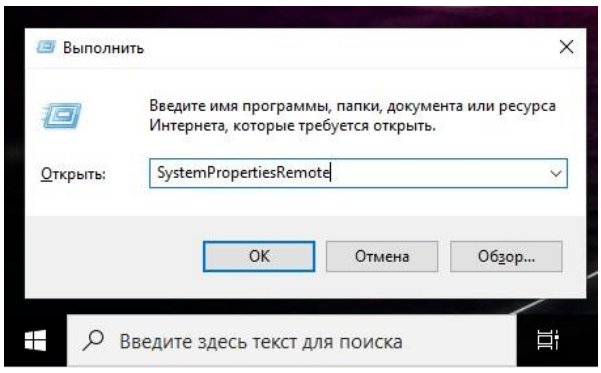
Задание:

Клиент и сервер присутствуют по умолчанию во всех версиях Windows. Для запуска клиента не требуется дополнительная настройка.
Что касается сервера, то он может быть отключён и/или доступ к порту RDP может быть заблокирован файерволом.

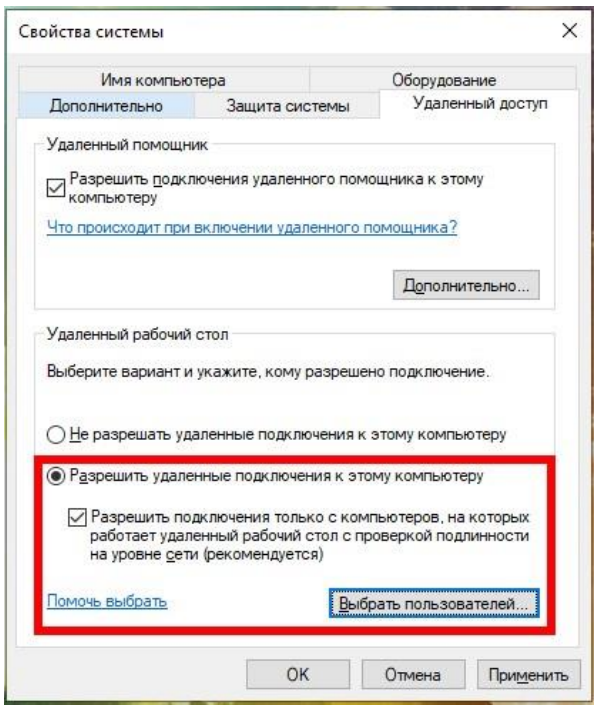
Как включить удалённый рабочий стол на Windows 10 в командной строке

Нажмите Win+r и введите:

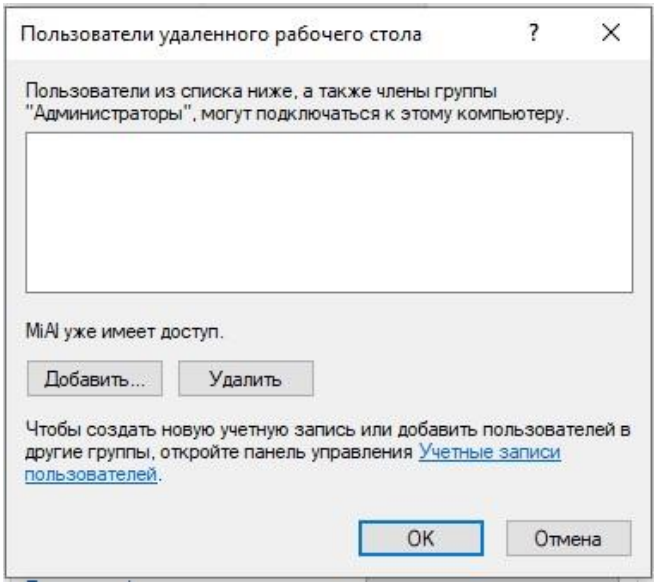
SystemPropertiesRemote



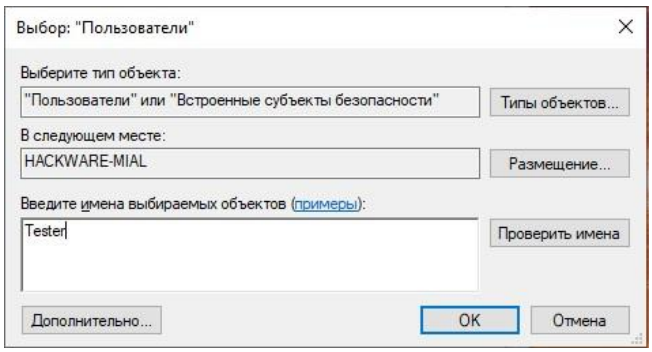
В открывшемся окне выберите «Разрешить удалённые подключения к этому компьютеру»:



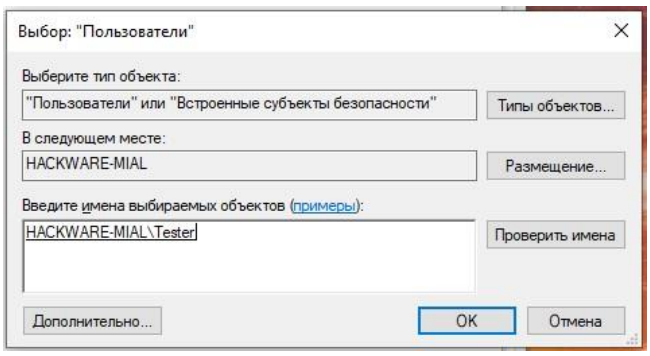
При необходимости добавьте пользователей, которые могут удалённо подключиться, щёлкнув «Выбрать пользователей». Члены группы «Администраторы» получают доступ автоматически:



Чтобы правильно добавить пользователя, введите его имя:



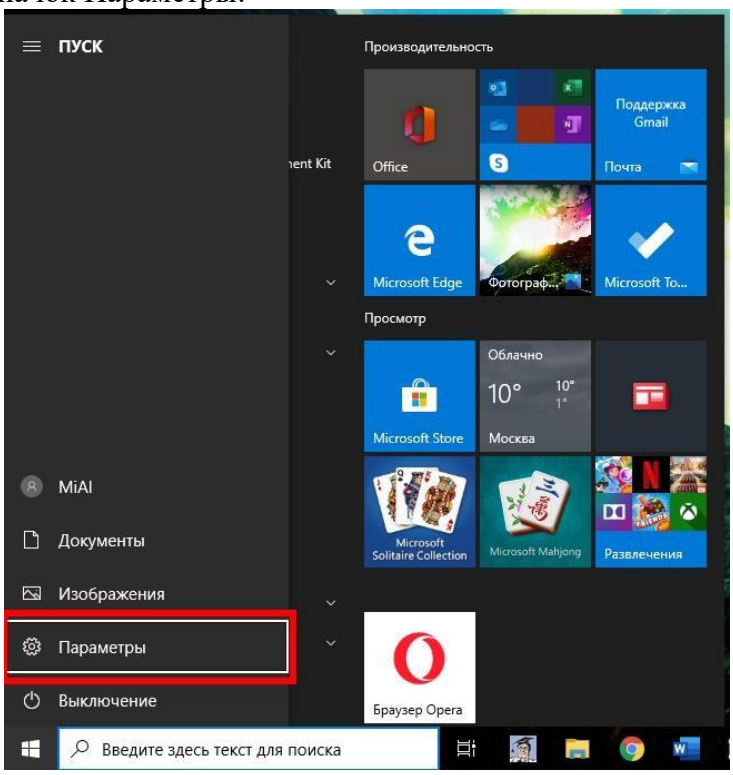
И нажмите кнопку «Проверить имена»:



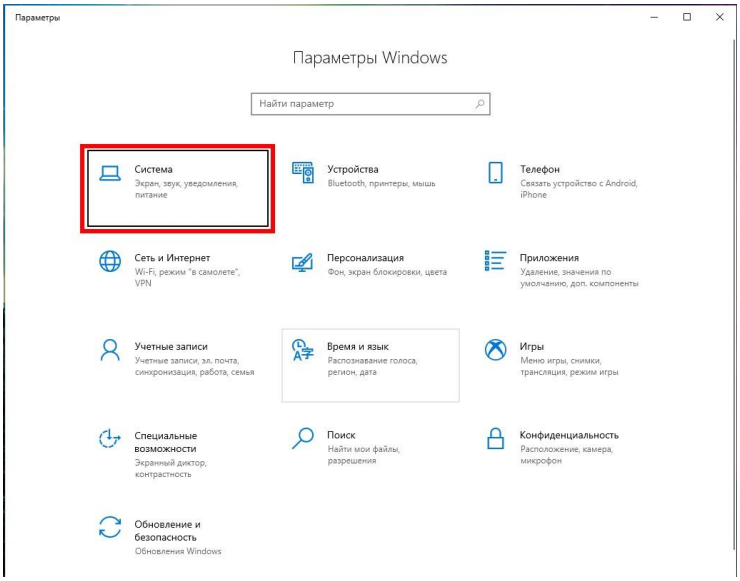
Команду SystemPropertiesRemote также можно запустить в командной строке, либо в PowerShell.

Как включить удалённый рабочий стол на Windows 10 в графическом интерфейсе

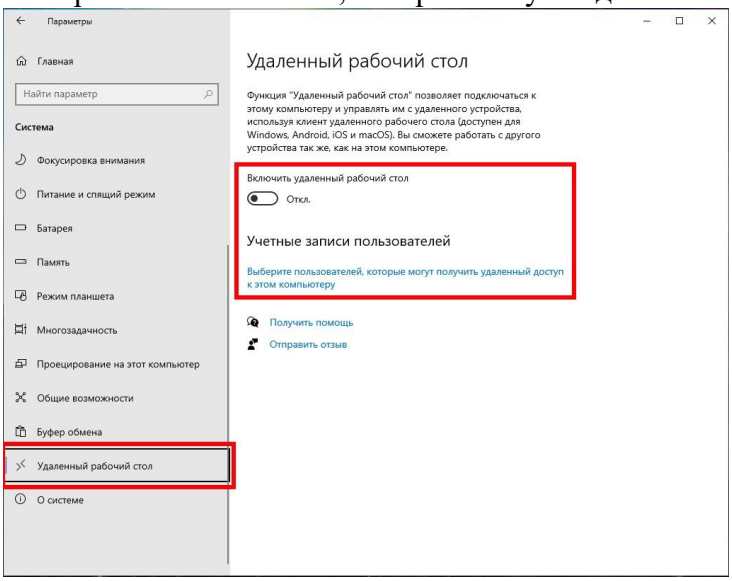
На устройстве, с которого вы собираетесь подключиться, откройте меню Пуск и щёлкните значок Параметры:



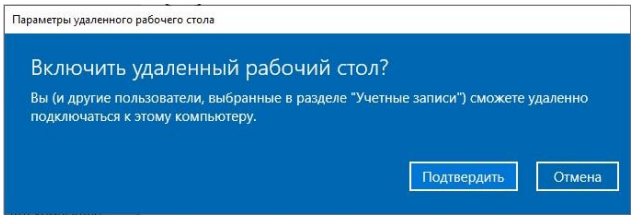
Выберите Система:



На вкладке «Удалённый рабочий стол» включите соответствующий ползунок. Также вы можете выбрать пользователей, которые могут подключаться удалённо к компьютеру.

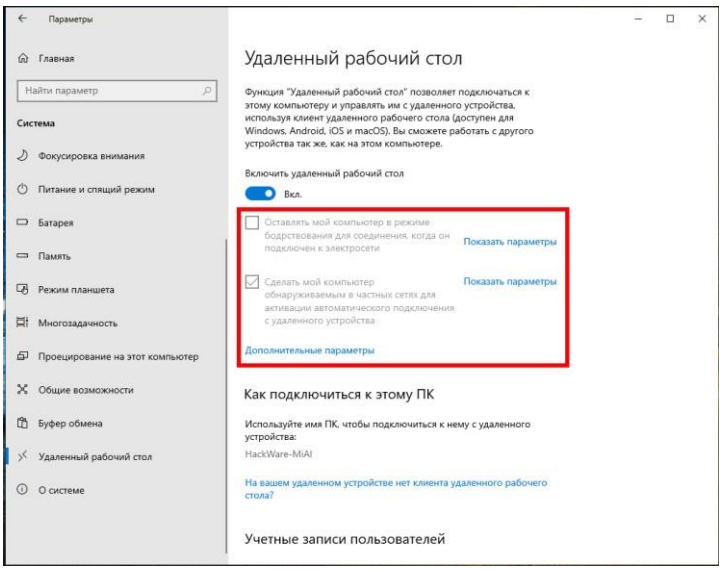


Подтвердите выбранное действие:

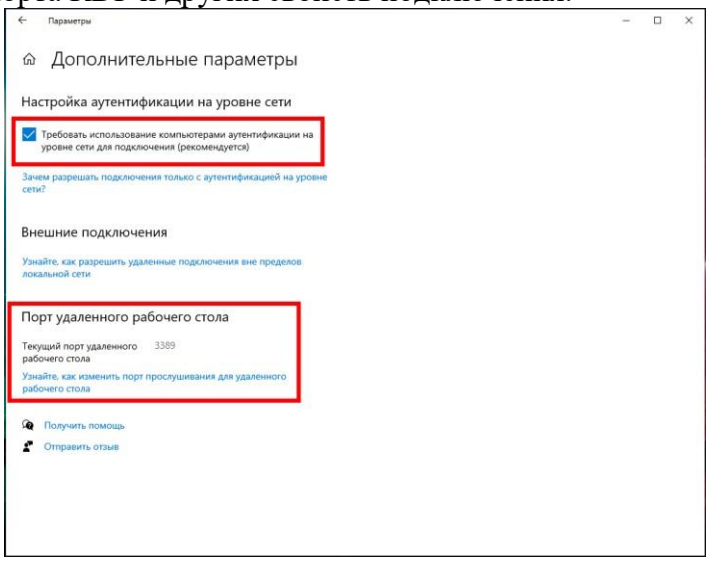


Дополнительно вы можете включить настройки:

Оставлять мой компьютер в режиме бодрствования для соединения, когда он подключён к электросети
Сделать мой компьютер обнаруживаемым в частных сетях для активации подключения с удалённым доступом



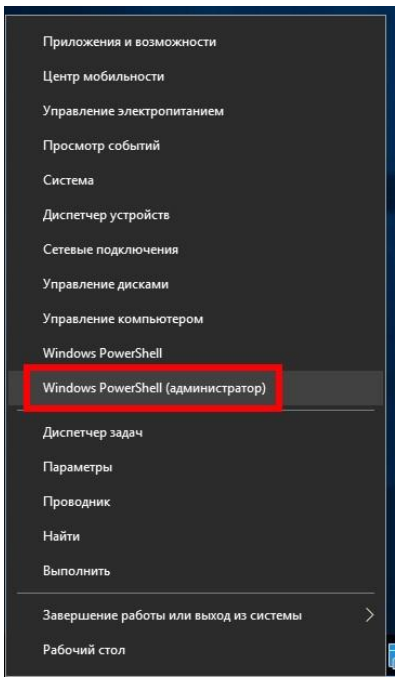
Кликнув «Дополнительные параметры» вы увидите настройки для изменения стандартного порта RDP и других свойств подключения.



Описанные выше способы также будут работать и на Windows Server 2019. В дополнении к ним есть ещё несколько способов включения RDP на Windows Server 2019.

Как включить удалённый рабочий стол на Windows Server 2019 в PowerShell

Разрешение службы удалённых рабочих столов в Windows Server 2019 быстрее сделать в PowerShell, чем в графическом интерфейсе. Для этого параметра мы будем использовать командлет Set-ItemPropery для изменения параметра флага реестра.
Запустите сеанс PowerShell от имени администратора. Для этого нажмите Win+x и выберите Windows PowerShell (администратор):



Затем выполните следующую команду:

```
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server' name
"fDenyTSConnections" -value 0
```

Файервол Windows не разрешает удалённые подключения к RDP Нам нужно настроить файервол, чтобы он разрешал удалённые подключения RDP, для этого выполните команду:

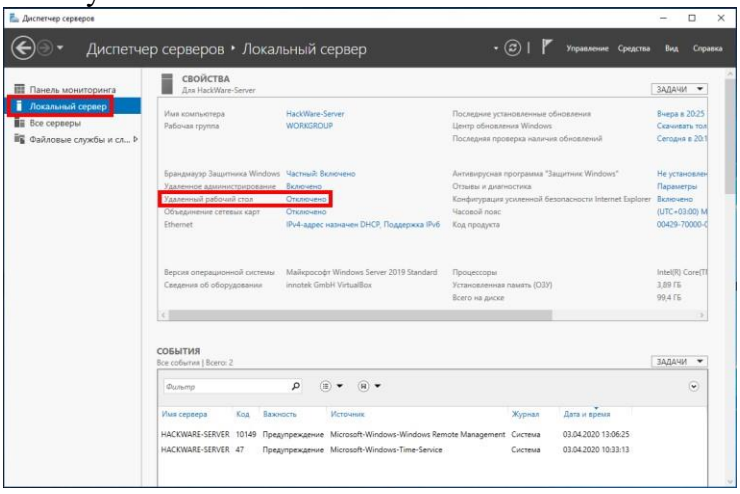
```
Enable-NetFirewallRule -DisplayGroup "Remote Desktop"
```

Для отключения RDP запустите:

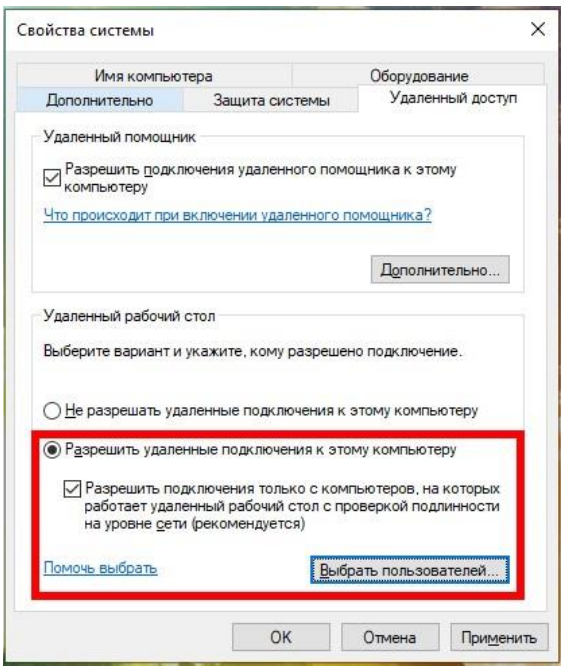
```
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server' name
"fDenyTSConnections" -value 1
```

Как включить удалённый рабочий стол на Windows Server 2019 в настройках (графический интерфейс)

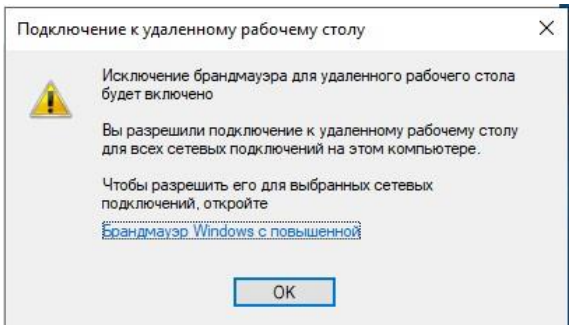
Если вы не дружите с терминалом, вы также можете включить службу RDP из графического интерфейса сервера. Откройте Диспетчер серверов из меню «Пуск» и нажмите на «Локальный сервер» в левой части. Найдите пункт «Удалённый рабочий стол» и кликните по слову «Отключено»:



В открывшемся окне выберите «Разрешить удалённые подключения к этому компьютеру»:



Согласитесь с изменением правила файервола:

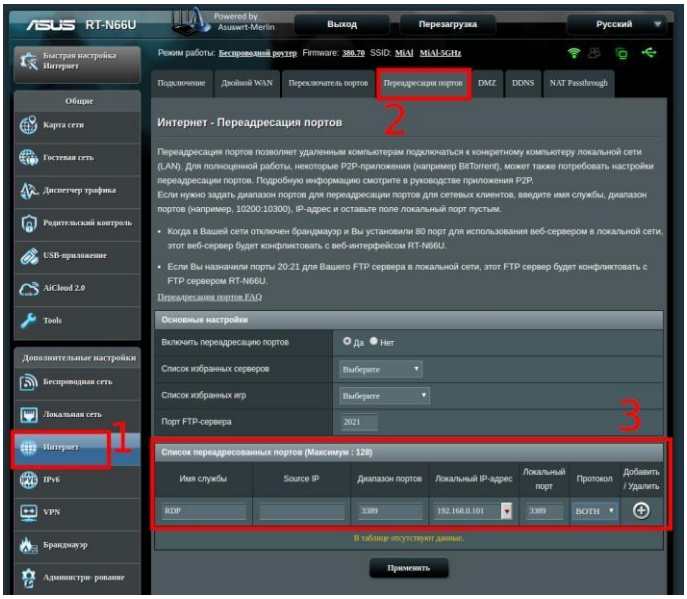


Как настроить подключение к RDP из Интернета

RDP разрешает любые подключения, будь то из локальной сети или из Интернета. Для подключения из Интернета требуется, чтобы у вашего компьютера был белый IP.
Если же ваш Интернет-провайдер использует NAT, то вам нужно арендовать внешний (белый) IP адрес.
Если вы подключены к роутеру (они тоже всегда используют NAT), то вам нужно настроить проброску (форвардинг, переадресацию) портов следующим образом:

1. Начать нужно с «Настройки постоянного IP в Windows».
2. Последующие настройки нужно делать в роутере. Поскольку у всех разные модели роутеров, то конкретные действия и названия вкладок в панели администрирования роутеров могут различаться. Главное понять суть и найти соответствующую вкладку в роутере. Помните, что нужно перенаправить порты TCP и UDP с номером 3389.

Перейдите в панель управления роутером. В настройках роутера перейдите в раздел «Интернет» (может называться WAN), затем во вкладку «Переадресация портов» (может называться «Перенаправление портов», «Port Forwarding»):



3. Добавьте новое правило:

Имя службы — введите любое

Source IP (исходный IP адрес) оставьте пустым

Диапазон портов — укажите порт 3389

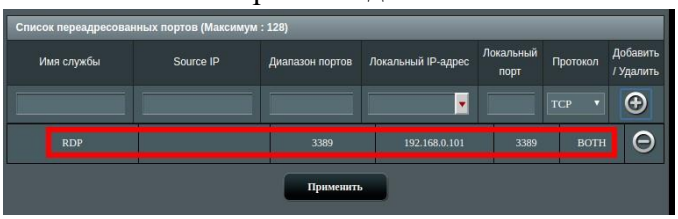
Локальный IP адрес — укажите IP адрес компьютера Windows, к которому будет выполняться подключение по RDP

Локальный порт — укажите порт 3389

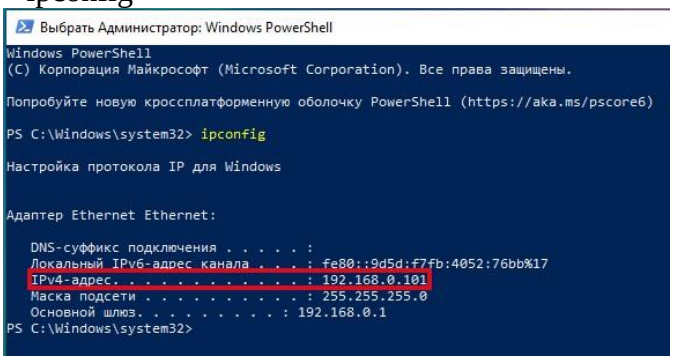
Протокол — укажите Both (оба)

4. И нажмите кнопку «Добавить».

5. Сохраните сделанные изменения.



IP адрес компьютера Windows можно посмотреть командой:
ipconfig

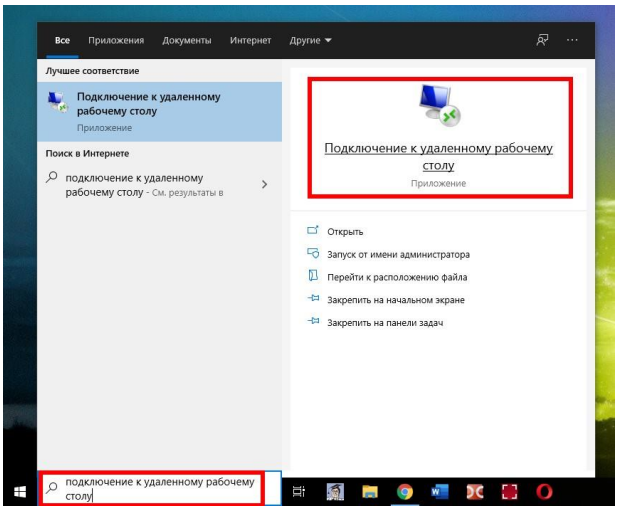


Про переадресацию портов, о том, что это такое (на примере веб сервера), дополнительно читайте в статье «Apache Forwarding — проброска портов веб-сервера».

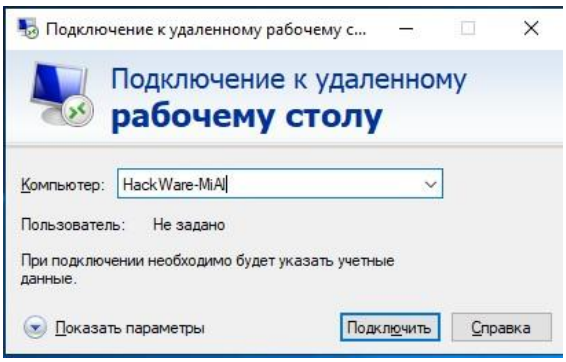
Ещё одним вариантом является использование VPN (виртуальной частной сети), в которой каждому компьютеру присваивается локальный адрес, но сама виртуальная частная сеть включает компьютеры которые могут быть размещены за пределами реальной частной сети. Подробности о VPN смотрите в статье «Доступ к службам компьютера через NAT и с серым IP с помощью OpenVPN».

Как подключиться к другому компьютеру и видеть его экран по RDP

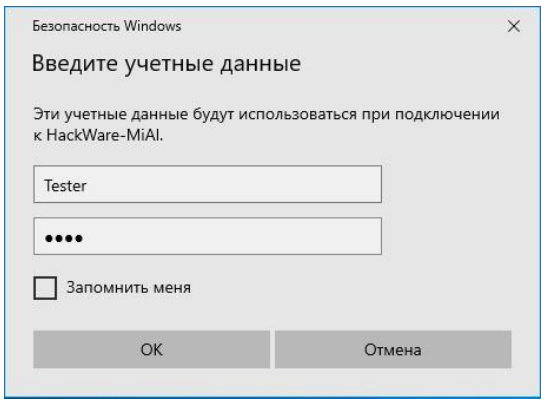
Удалённый рабочий стол можно использовать для подключения к Windows 10 Pro и Windows 10 Корпоративная, Windows 8.1, Windows 8 Корпоративная и Windows 8 Pro, Windows 7 Pro, Windows 7 Корпоративная и Windows 7 Максимальная, а также для подключения к версиям выше Windows Server 2008. Подключиться к компьютерам под управлением выпуска "Домашняя" (например, Windows 10 Домашняя) нельзя. Предварительная настройка или включение клиента RDP не требуется. Откройте командную строку (либо Win+r) и запустите: mstsc
Либо нажмите кнопку «Пуск» и начните набирать «подключение к удаленному рабочему столу»:



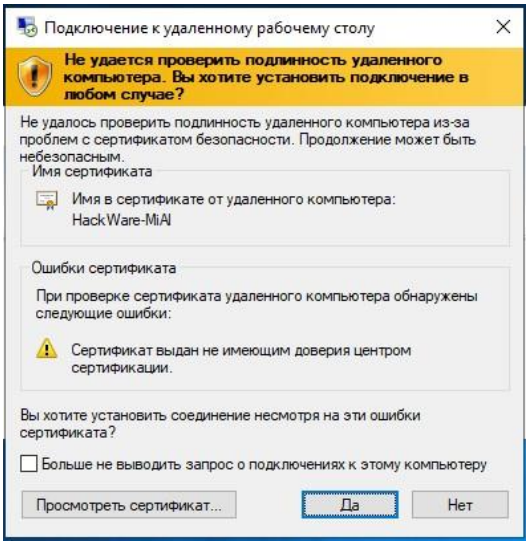
Для подключения можно использовать IP либо имя компьютера. Если вы не знаете, что это такое, то смотрите статью «Имя компьютера Windows: как изменить и использовать».
Введите IP либо имя компьютера, я буду использовать имя компьютера и подключусь к HackWare-MiAl:



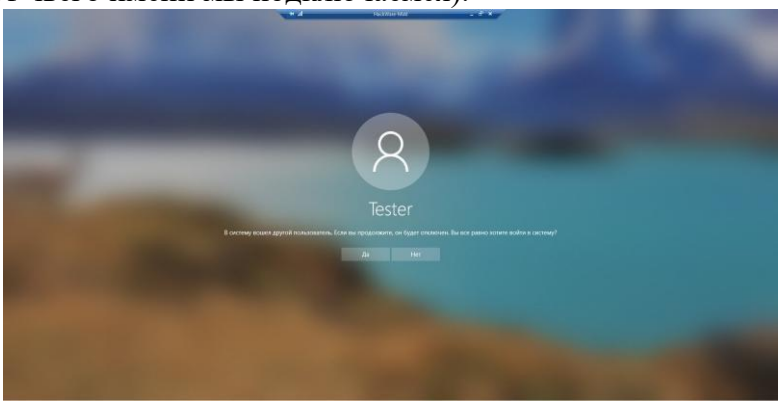
Вводим имя пользователя и пароль учётной записи на удалённом компьютере, то есть на том, к которому мы подключаемся. Можете поставить галочку «Запомнить меня», чтобы не вводить эти учётные данные в следующий раз:



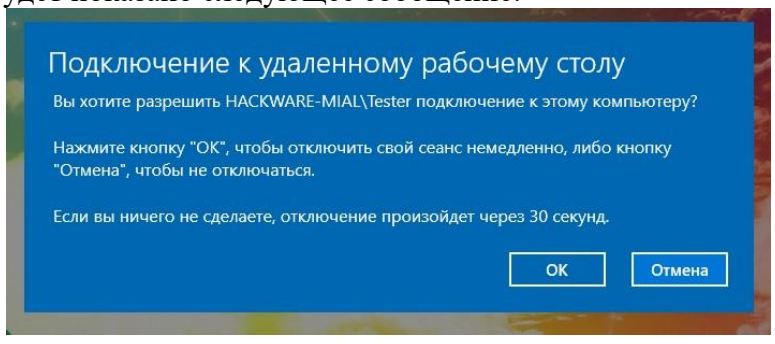
Нажимаем «Да»:



Система пишет, что в систему вошёл другой пользователь. Дело в том, что при подключении к удалённому компьютеру выполняется выход всех пользователей (в том числе того, от чьего имени мы подключаемся).



Если на удалённом компьютере выполнил вход какой-либо другой пользователь, то для него будет показано следующее сообщение:



Дело в том, что на одном компьютере Windows не могут одновременно работать несколько пользователей (имеется в виду по RDP, либо обычный вход и вход по RDP). Теперь мы видим экран удалённого компьютера: работа с ним ничем не отличается, можно запускать программы, выполнять настройки и любые другие действия:

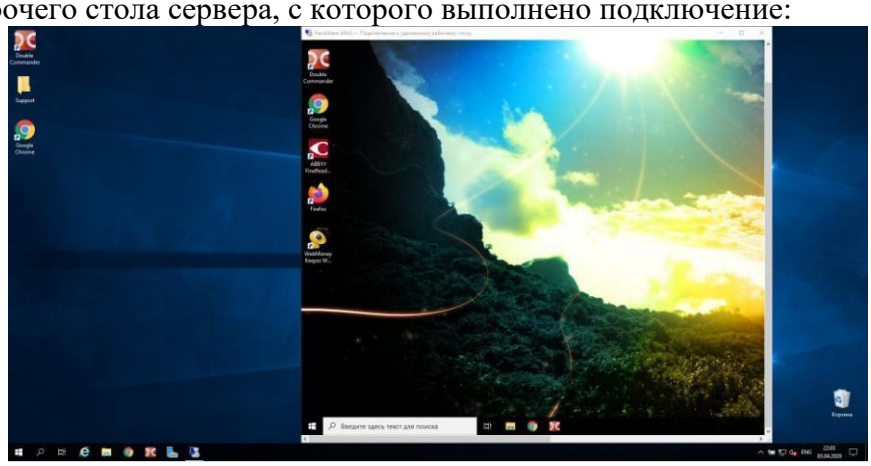
Обратите внимание на панель вверху в центре экрана:

С помощью этой панели можно:

проверить качество подключения до удалённого компьютера;

свернуть удалённый рабочий стол без отключения (работает как с любым приложением — для открытия рабочего стола достаточно кликнуть на его иконку на панели приложений); изменить размер экрана удалённого компьютера (то есть выйти из полноэкранного режима, либо войти в полноэкранный режим снова); закрыть подключение к удалённому рабочему столу.

На следующем скриншоте удалённый рабочий стол не в полный экран на фоне основного рабочего стола сервера, с которого выполнено подключение:



2.16 Практическая работа№ 16
Развертывание и поддержка виртуализации профиля пользователя

Задание:

Открываем Пуск -> Панель управления -> Система, слева жмем на «Изменить параметры«. В «Свойствах системы» на вкладке «Имя компьютера» нажимаем кнопку «Изменить» и в поле «Имя компьютера» вводим имя (я ввел ADserver) и жмем «ОК«. Появится предупреждение о необходимости перезагрузки системы, что бы изменения

вступили в силу, соглашаемся нажав «ОК«. В «Свойствах системы» жмем «Закрыть» и соглашаемся на перезагрузку.

2) Задать настройки сети

Открываем Пуск -> Панель управления -> Центр управления сетями и общим доступом > Изменить параметры адаптера. После нажатия правой кнопкой на подключении выбираем пункт «Свойства» из контекстного меню. На вкладке «Сеть» выделяем «Протокол интернета версии 4 (TCP/IPv4)» и жмем «Свойства«.

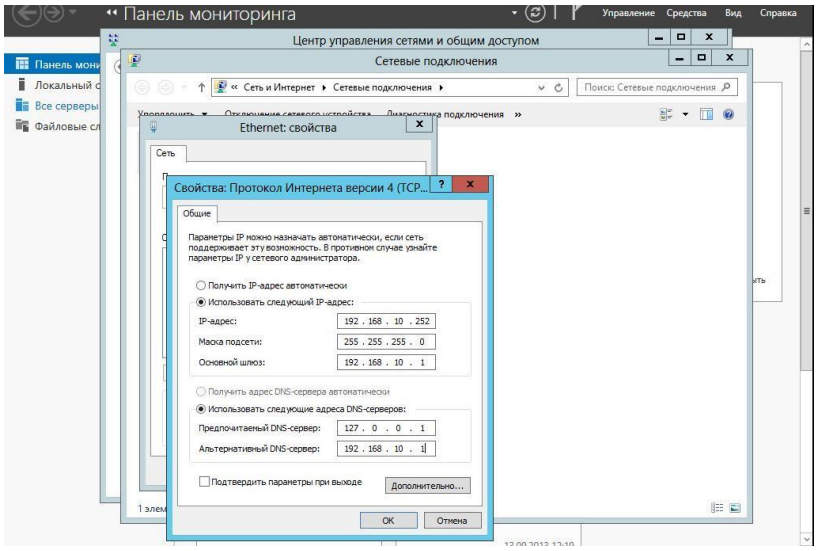
Я задал:
IP-адрес: 192.168.10.252

Маска подсети: 255.255.255.0

Основной шлюз: 192.168.10.1

Предпочтительный DNS-сервер: 127.0.0.1 (так как тут будет располагаться локальный DNS-сервер)

Альтернативный DNS-сервер: 192.168.10.1



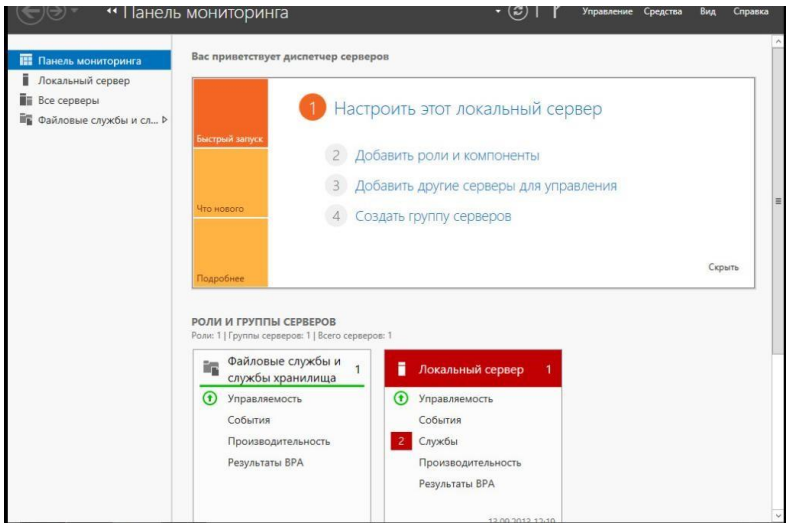
После чего жмем «ОК» и «Закрыть«.

Подготовка закончилась, теперь преступим к установке роли.

3. Установки роли

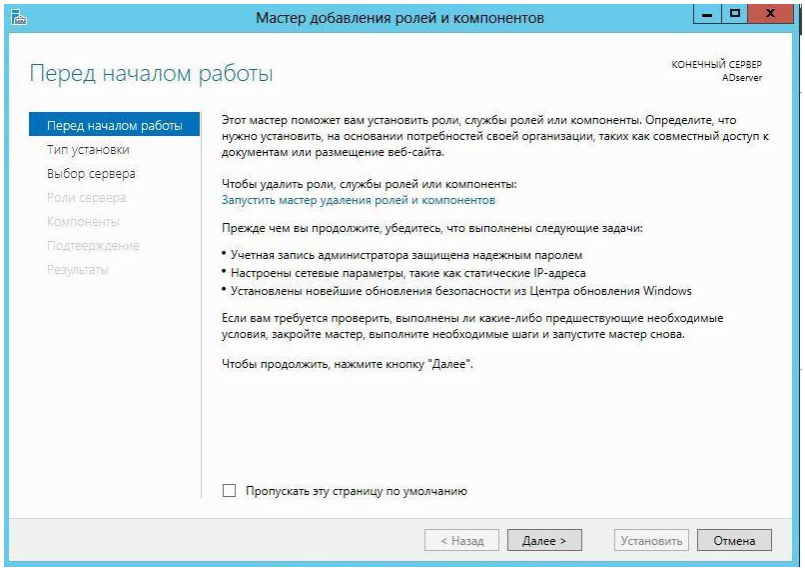
Для установки роли AD на компьютер откроем Пуск -> Диспетчер сервера.

Выберем «Добавить роли и компоненты«.

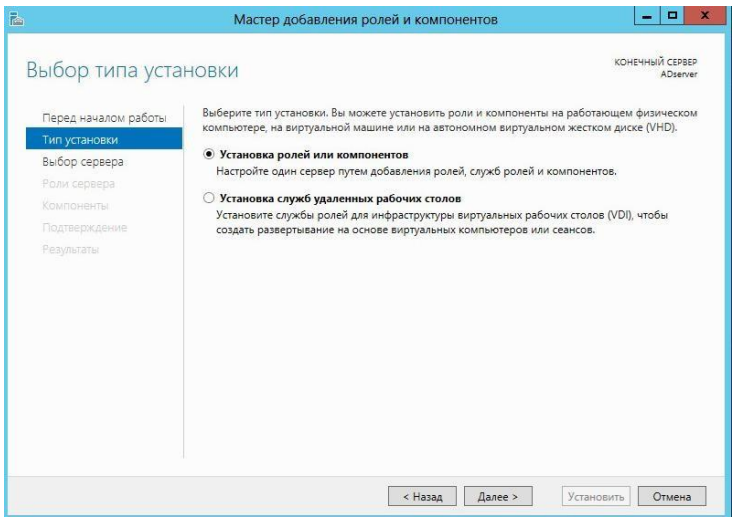


После чего запустится «Мастер добавления ролей и компонентов«.

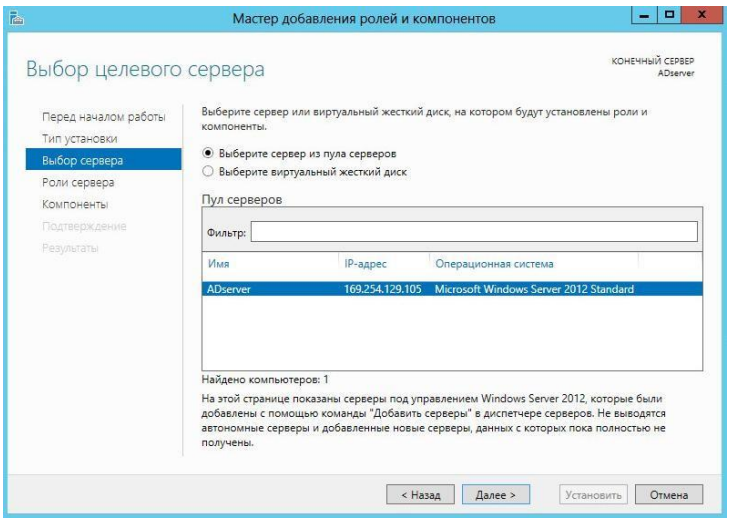
3.1 На первом этапе мастер напоминает, что нужно сделать перед началом добавления роли на компьютер, просто нажимаем «Далее«.



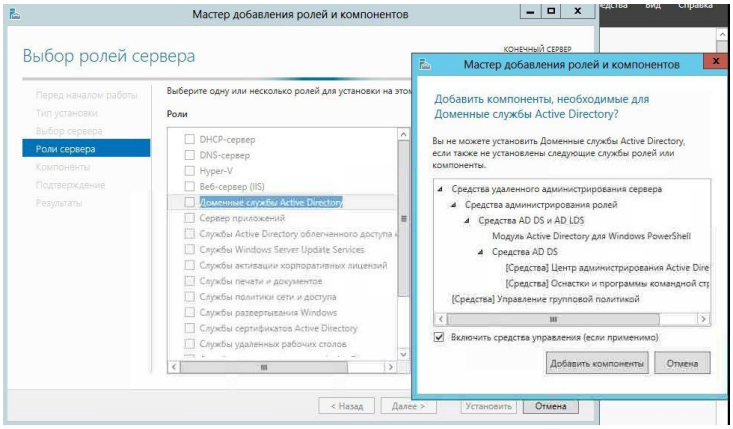
3.2 Теперь выбираем «Установка ролей и компонентов» и жмем «Далее«.



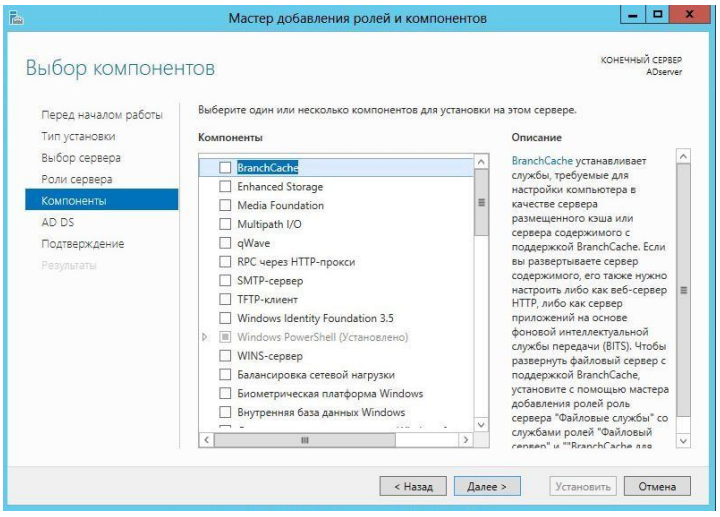
3.3 Выберем компьютер, на котором хотим установить роль AD и опять «Далее«.



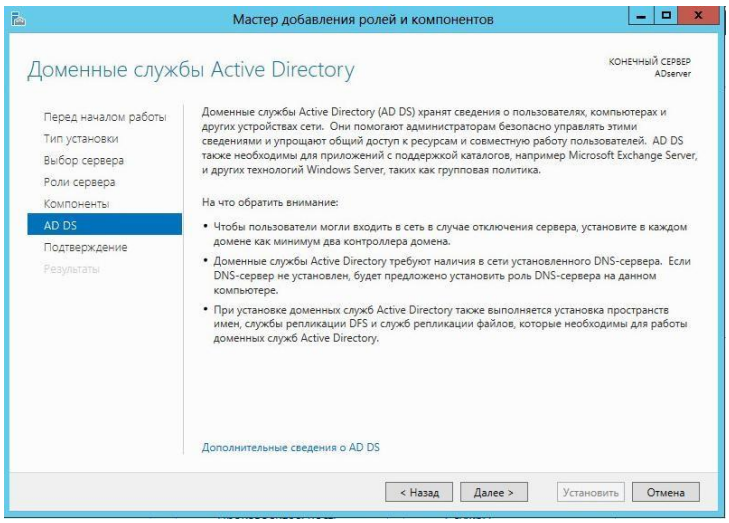
3.4 Теперь нужно выбрать какую роль мы хотим установить, выбираем «Доменные службы Active Directory» и нам предложат установить необходимые компоненты и службы ролей для роли AD соглашаемся нажав «Добавить компоненты» и опять «Далее«.



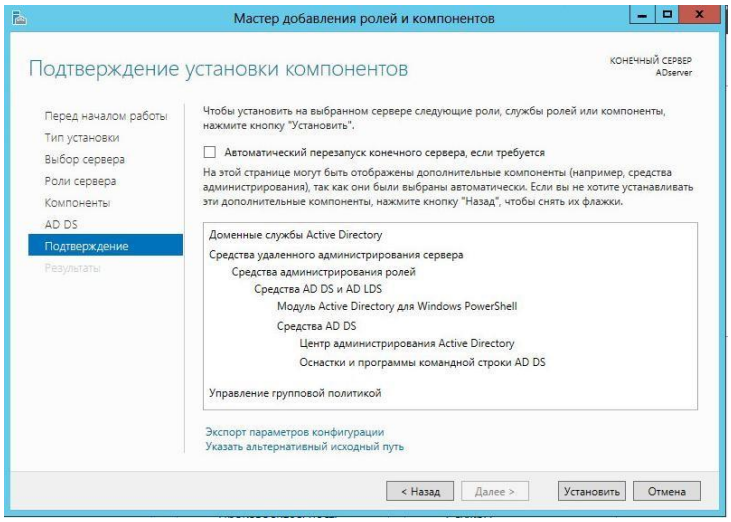
3.5 Тут предложат установить компоненты, но нам они пока не нужны, так что просто жмем «Далее«.



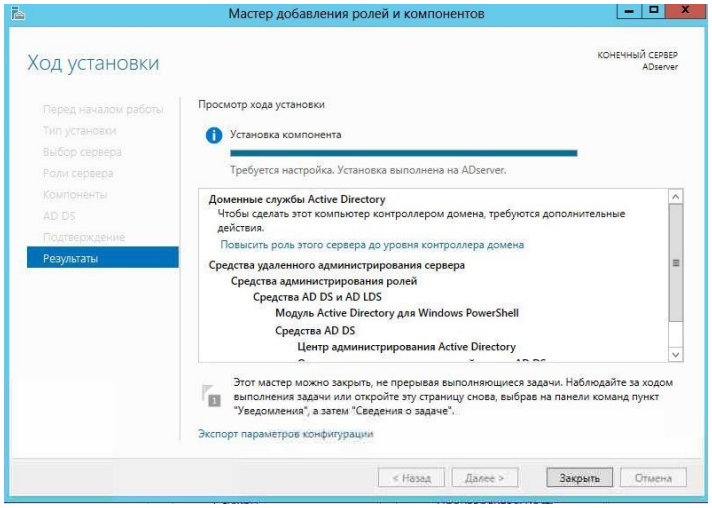
3.6 Теперь нам выведут описание роли «Доменных служб Active Directory«. Прочитаем внимательно и жмем «Далее«.



3.7 Мы увидим, что же именно мы будем ставить на сервер, если все хорошо, то жмем «Установить«.



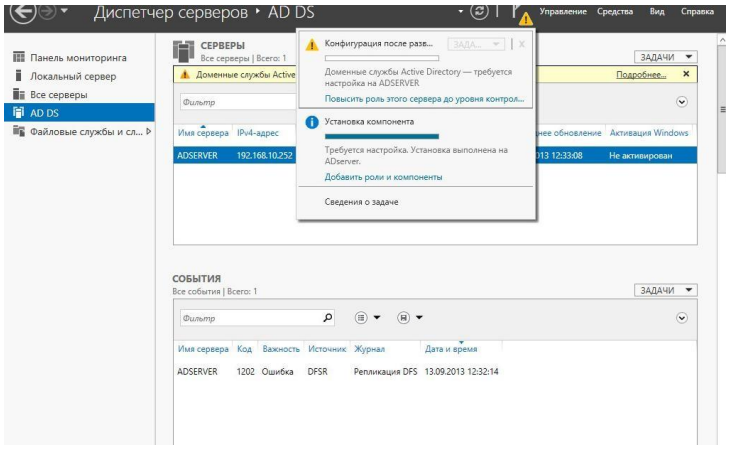
3.8 После установки просто жмем «Закрыть«.



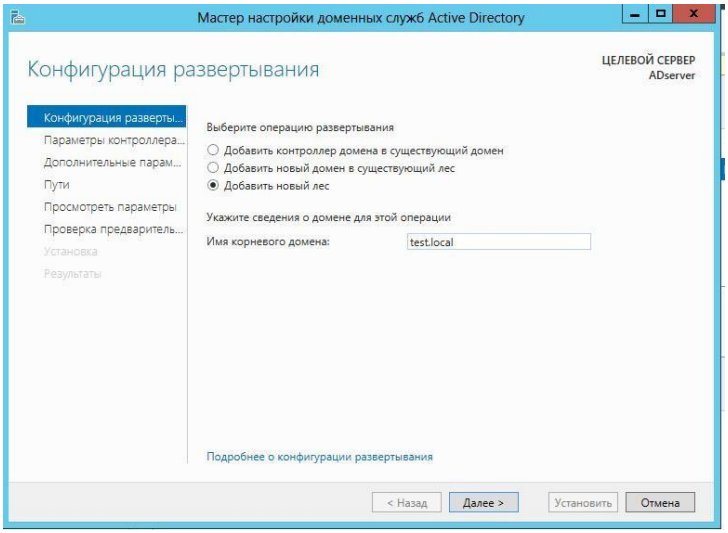
4. Настройка доменных служб Active Directory

Теперь настроим доменную службу запустив «Мастер настройки доменных служб Active Directory» (жмем на иконку «Уведомления» (флажок) в «Диспетчере сер-

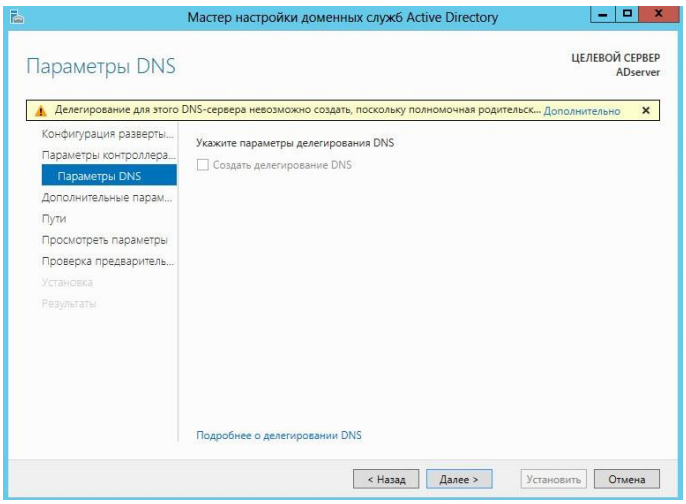
вера» и после этого выбираем «Повысить роль этого сервера до уровня контроллера домена«).



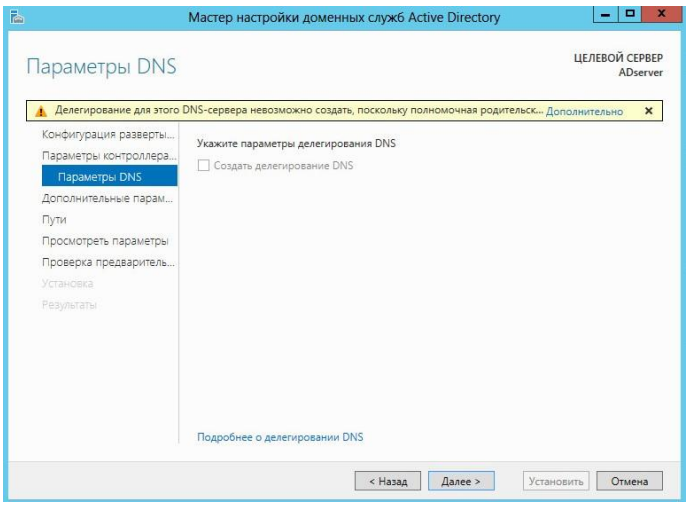
4.1 Выбираем «Добавить новый лес» и вписываем наш домен в поле «Имя корневого домена» (я решил взять стандартный домен для таких случаев test.local) и жмем «Далее«.



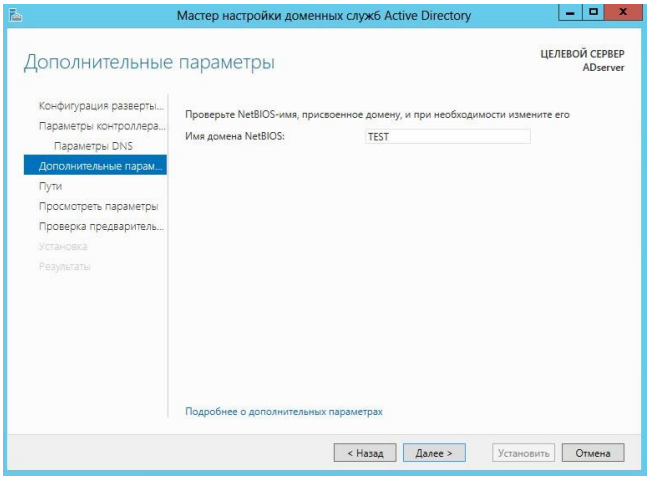
4.2 В данном меню можно задать совместимость режима работы леса и корневого домена. Так как у меня все с нуля я оставлю по умолчанию (в режиме работы «Windows Server 2012«). А еще можно отключить DNS-сервер, но я решил оставить это, так как хочу иметь свой локальный DNS-сервер. И еще необходимо задать пароль DSRM(Directory Service Restore Mode — режим восстановления службы каталога), задаем пароль и тыкаем «Далее«.



4.3 На данном этапе мастер настройки предупреждает нас, что домен test.local нам не делегирован, ну это и логично, нам ни кто его не давал, он будет существовать только в нашей сети, так, что жмем просто «Далее«.

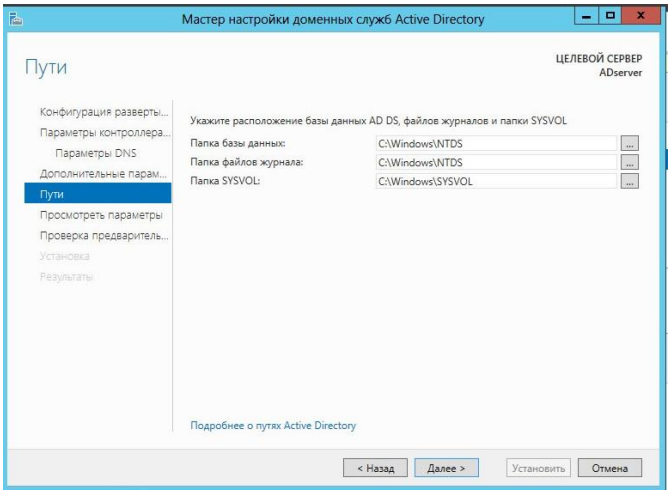


4.4 Можно изменить NetBIOS имя, которое было автоматически присвоено, я не буду этого делать, так, что жмем «Далее«.

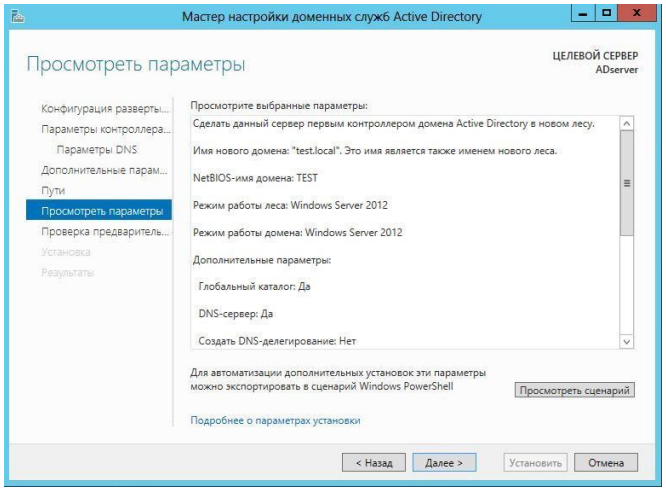


4.5 Тут можем изменить пути к каталогам базы данных AD DS (Active Directory Domain Services — доменная служба AD), файлам журнала, а так же каталогу SYSVOL.

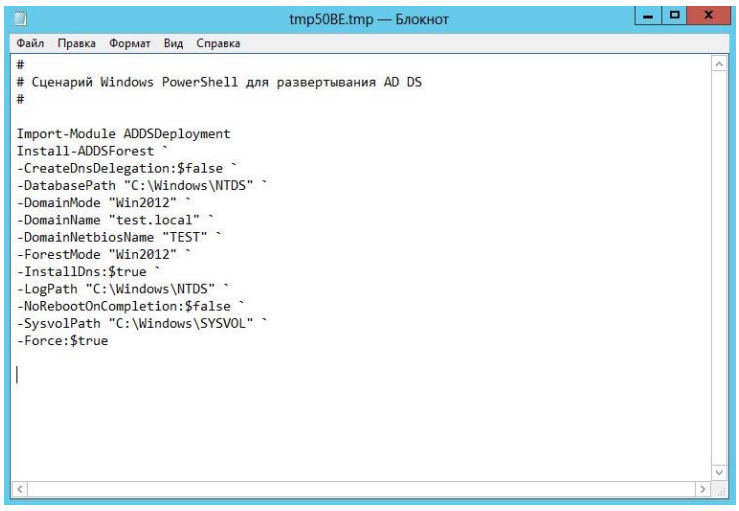
Не вижу смысла в изменении, так что просто жмем «Далее«.



4.6 Теперь мы видим небольшой итог, какие настройки мы выбрали.

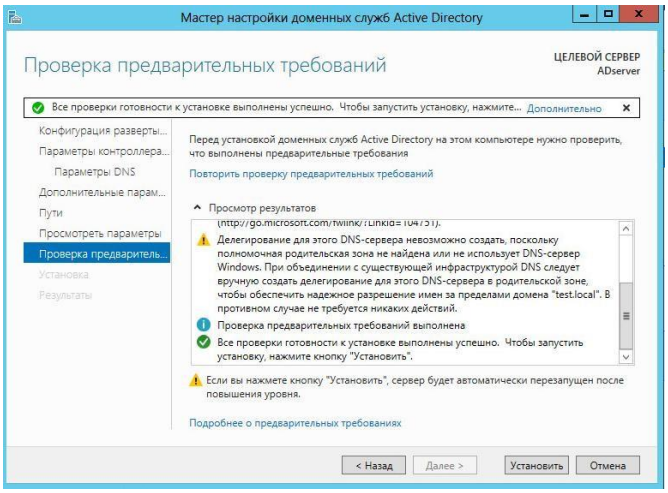


Тут же, нажав на кнопку «Просмотреть сценарий» мы можем увидеть PowerShell сценарий для развертывания AD DS выглядит он примерно так:



Жмем «Далее«.

4.7 Мастер проверит соблюдены ли предварительные требования, видим несколько замечаний, но они для нас не критичны, так что жмем кнопку «Установить«.

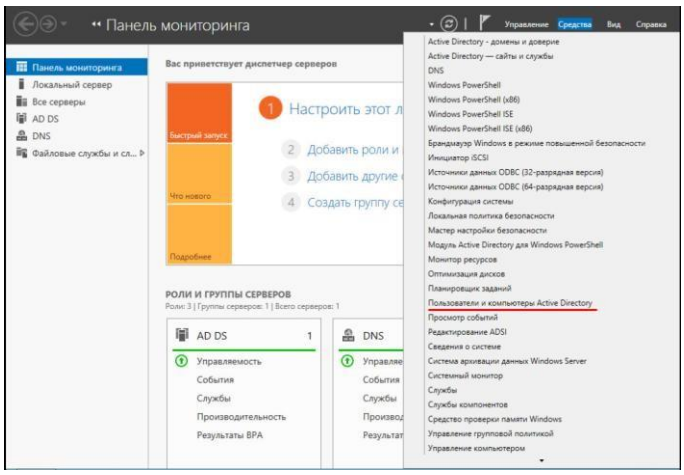


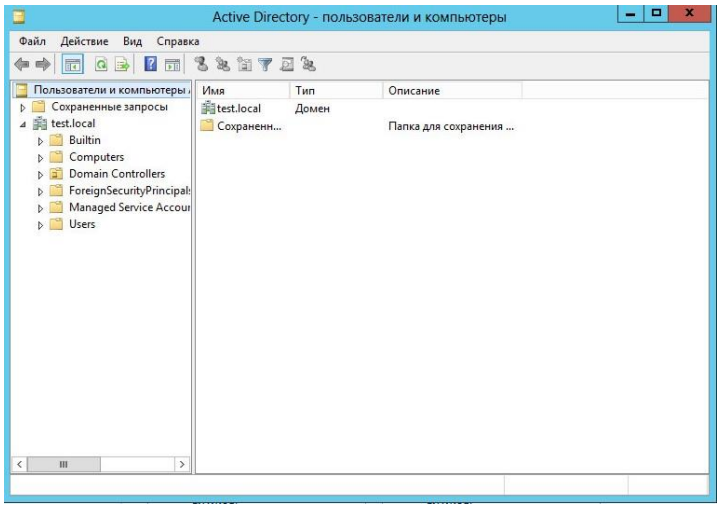
4.8 После завершения установки, компьютер перезагрузится.

5. Добавление нового пользователя

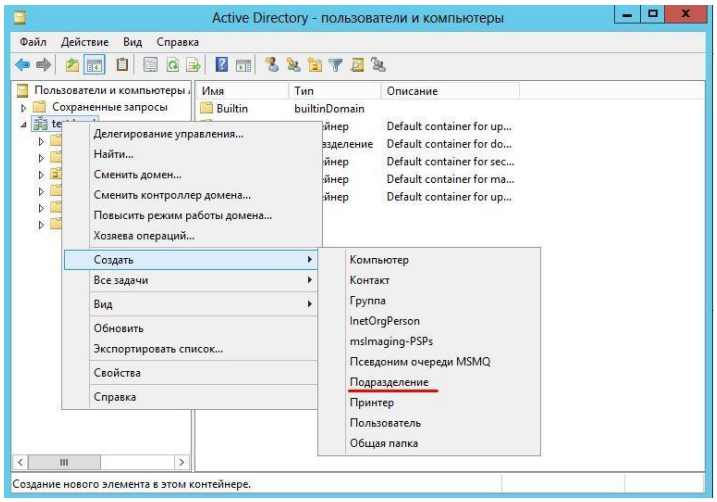
5.1 Запустим Пуск -> Панель управления -> Администрирование -> Пользователи и

компьютеры Active Directory. Или через панель управления сервером:

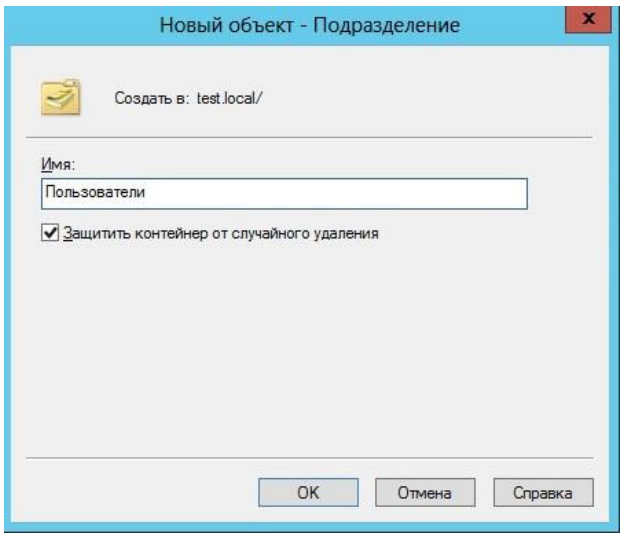




5.2 Выделяем название домена (test.local), нажимаем правой кнопкой и выбираем «Создать» -> «Подразделение«.



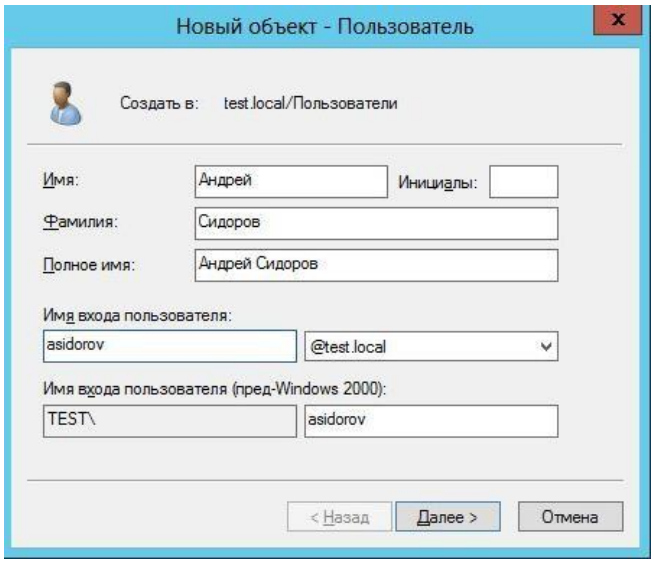
После чего вводим имя подразделения, а так же можем снять защиту контейнера от случайного удаления. Нажимаем «ОК«.



Подразделения служат для того, что бы удобно управлять группами компьютеров, пользователей и т.д. Например: можно разбить пользователей по группам с именами подразделений соответствующих именам отделов компаний, в которой они работают (Бухгалтерия, ИТ, отдел кадров, менеджеры и т.д.)

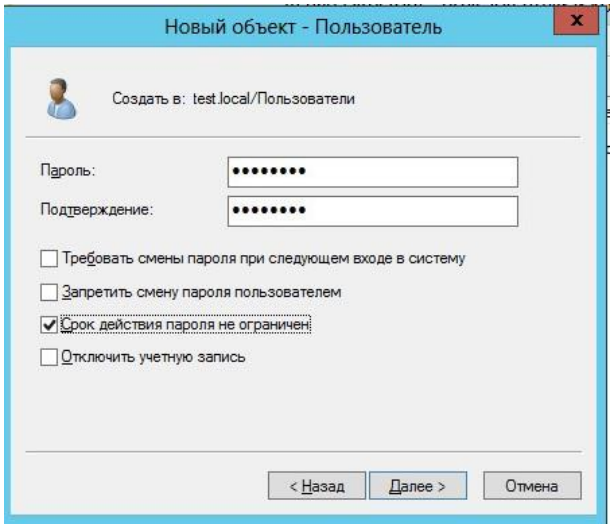
5.3 Теперь создадим пользователя в подразделении «Пользователи«. Правой кнопкой на подразделение и выбираем в нем «Создать» -> «Пользователь«. И заполняем основные данные: Имя, Фамилия, логин.

Подразделения служат для того, что бы удобно управлять группами компьютеров, пользователей и т.д. Например: можно разбить пользователей по группам с именами подразделений соответствующих именам отделов компаний, в которой они работают (Бухгалтерия, ИТ, отдел кадров, менеджеры и т.д.)

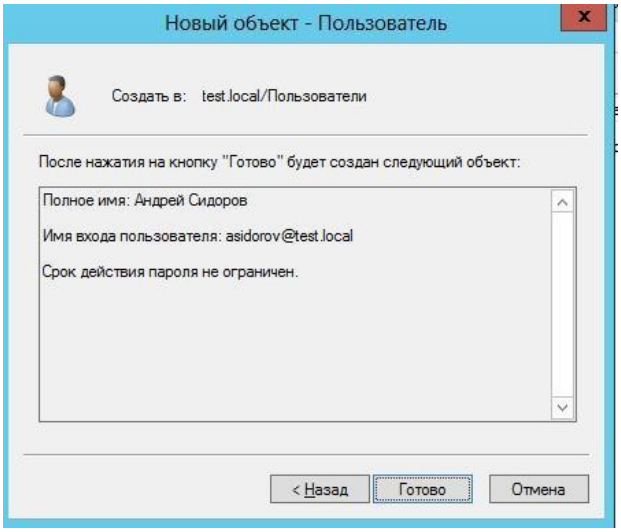


Жмем «Далее«. Теперь зададим пароль, для пользователя. Так же тут можно задать такие вещи как: — Требовать смены пароля пользователя при следующем входе в систему — при входе

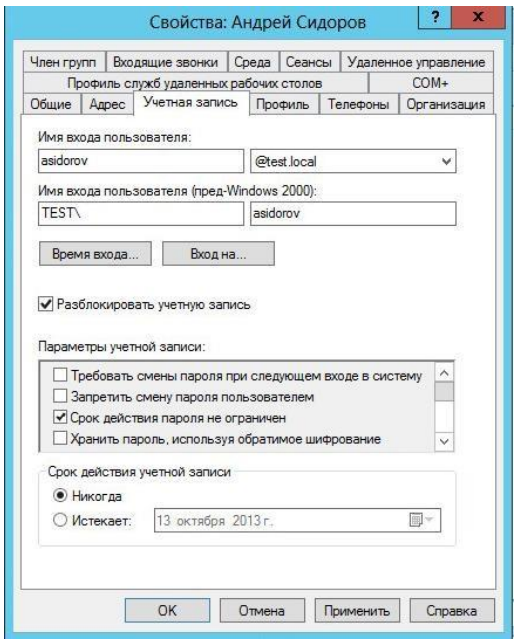
пользователя в наш домен, ему будет предложено сменить пароль. — Запретить смену пароля пользователем — отключает возможность смены пароля пользователем.
— Срок действия пароля не ограничен — пароль можно не менять сколько угодно. — Отключить учетную запись — делает учетную запись пользователя не активной.
Жмем «Далее«.



И теперь «Готово«.



5.4 Выделим созданного пользователя и в контекстном меню выберем «Свойства«. На вкладке «Учетная запись» ставим галочку напротив «Разблокировать учетную запись«, после чего нажимаем «Применить«, затем «ОК«.



6. Ввод компьютера в домен

6.1 Для начала, создадим новую виртуальную машину с Windows 7 на борту.

Зададим ему настройки сети, где:

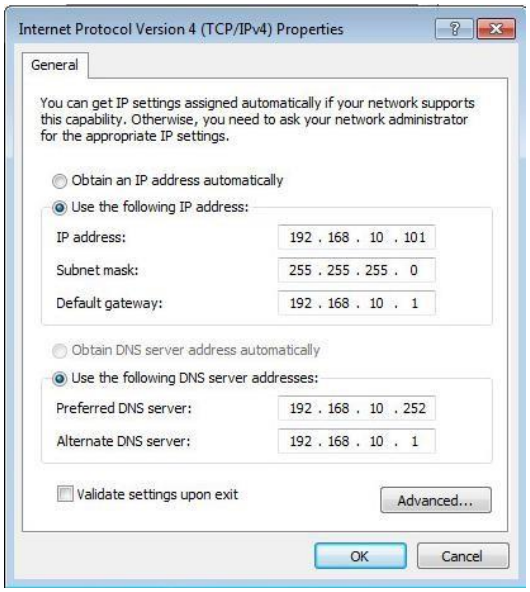
IP-address: 192.168.10.101

Subnet mask: 255.255.255.0

Default gateway: 192.168.10.1 (vyatta, где настроен NAT из мой прошлой заметки)

Preferred DNS server: 192.168.10.252 (AD сервер, который мы настраивали выше)

Alternate DNS server: 192.168.10.1 (опять vyatta, так как он проксирует DNS запросы на Google DNS сервер 8.8.8.8)

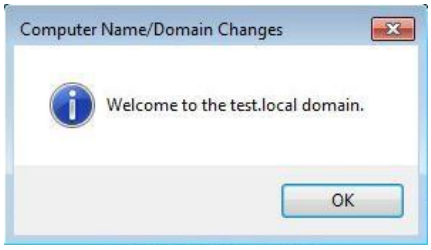


6.2 Переходим в Start -> правой кнопкой на Computer -> Properties -> Change settings. Жмем кнопку Change напротив The rename this com-

puter or change its domain or workgrup, click Change. Зададим имя компьютера и введем имя домена: test.local и жмем «ОК«.

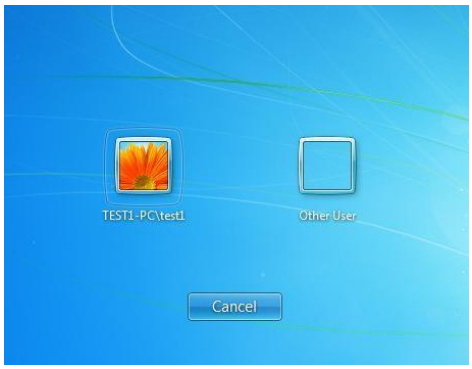
Введем логин и пароль заново

После успешного добавления в домен увидим сообщение:



6.3 После перезагрузки компьютера увидим сообщение о логине в систему. Жмем Switch User.

Нажмем на Other User.



И введем логин и пароль.

Мы залогинились как пользователь домена.

2.17 Практическая работа№ 17
Проектирование и реализация файловых служб

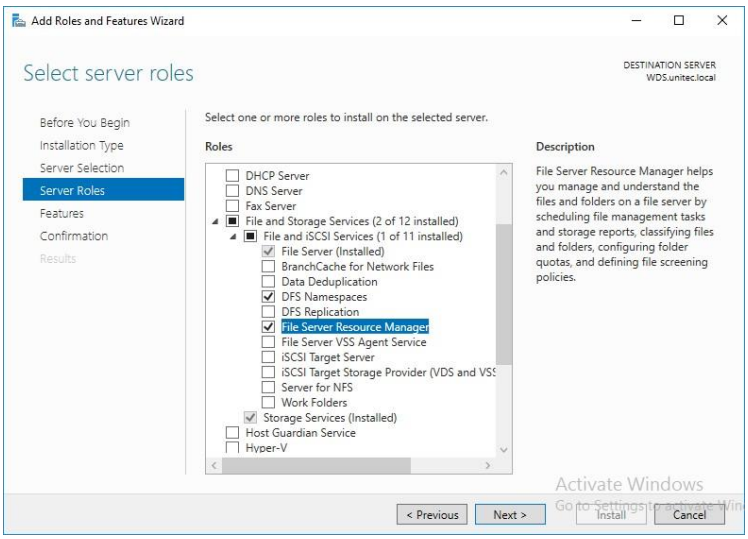
Задание:

1 . Открываем панель управления Server Manager, справа, вверху, находим Manage, выбираем «Add roles and features» (Добавить роли и компоненты)

2 . Тип установки указываем «Role-based or feature-based installation» (Установка ролей и компонентов)

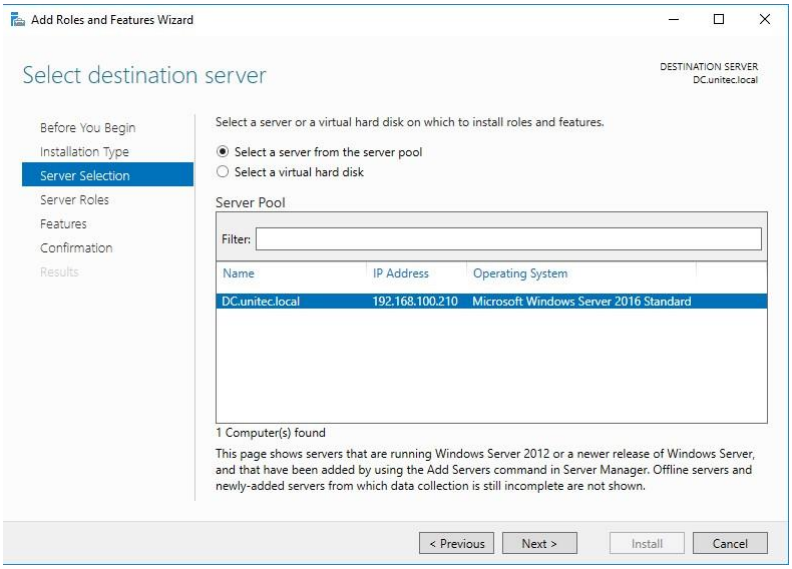
3 . Выбираем необходимый нам сервер из пула (списка) серверов

4 . Выбираем компоненты

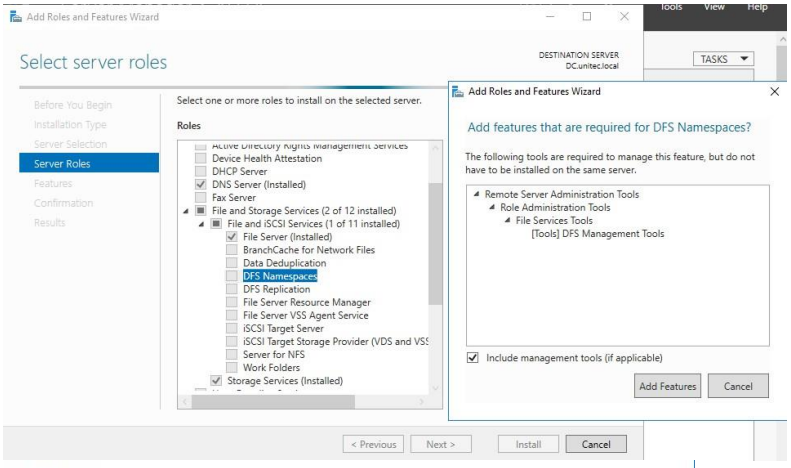


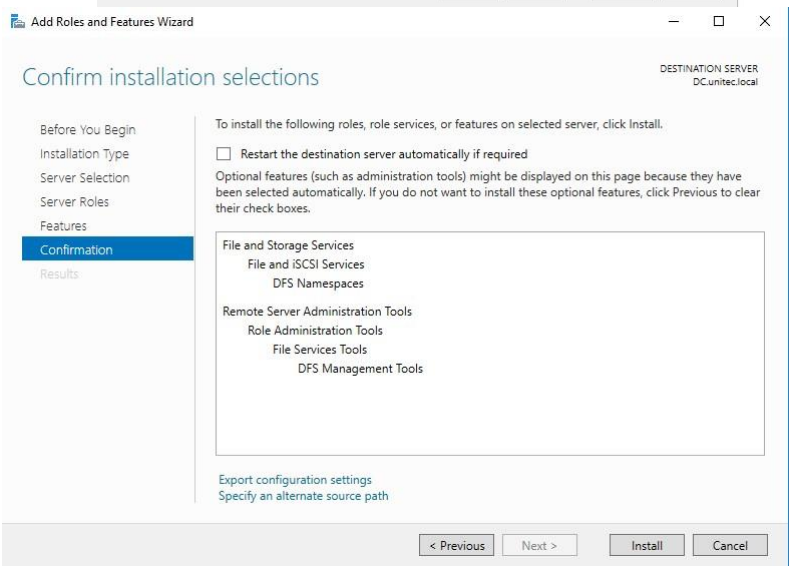
Установка DFS-namespace

Выбираем нужный сервер из пула серверов.

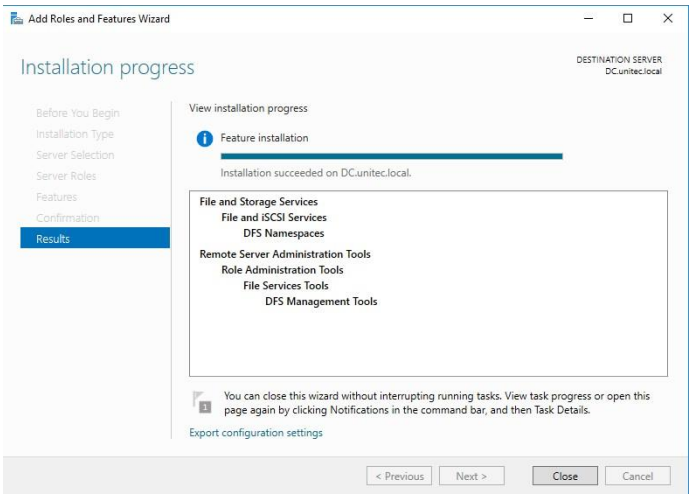


В следующем окне отмечаем DFS Namespaces и DFS Replication, если нужно.





После удачной инсталляции переходим к настройке DFS



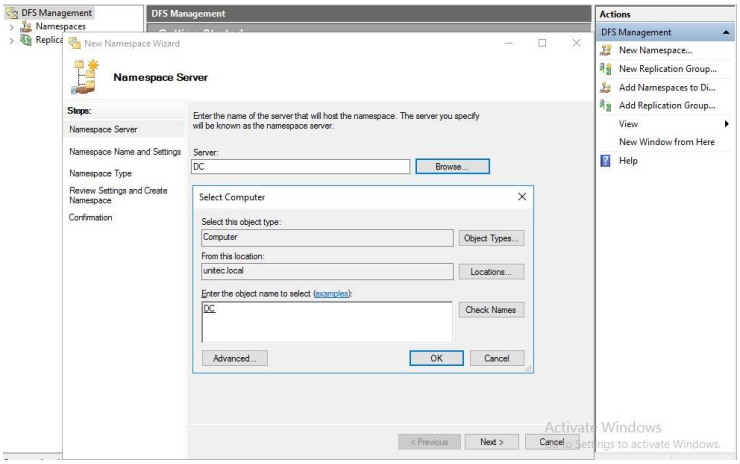
Настройка DFS

В Server Manager\Dashboard выберете > Tools > DFS Managment.

Или в поиске введите команду dfsmgmt.msc.

Для создания нового пространства имен выберете в правой части экрана New Namespace.

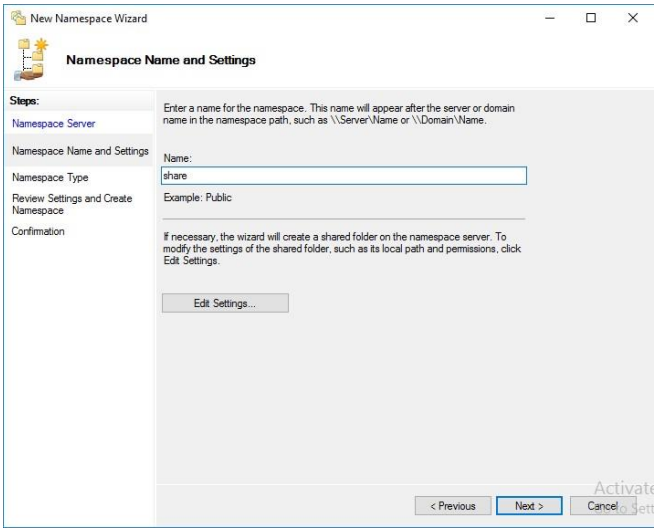
Введите название сервера и выберите его местоположение.



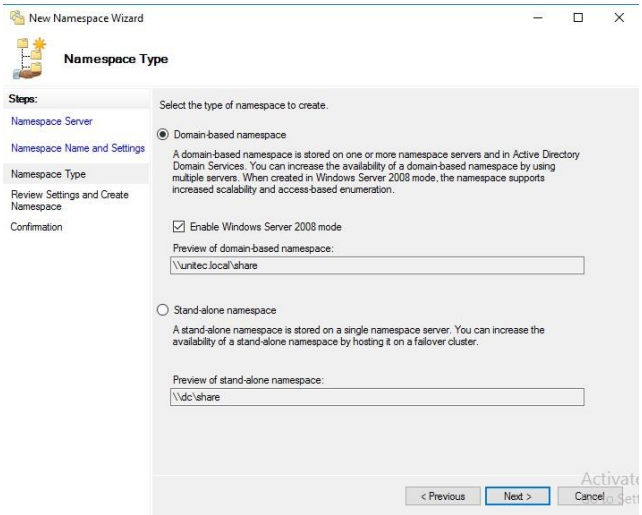
На следующем этапе задаем имя пространства имен DFS. Хочу обратить внимание, что заданное здесь имя будет использоваться при подключении общей сетевой папки.

Например:

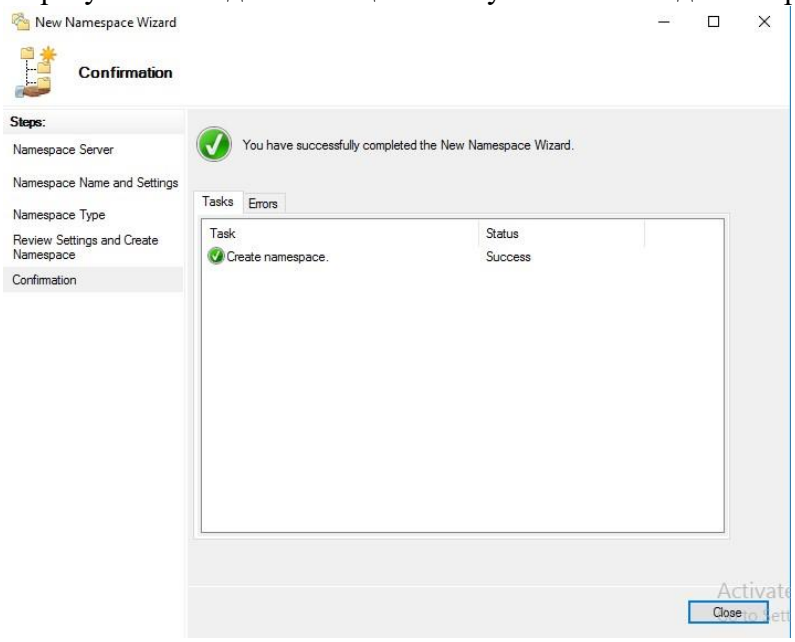
\\companyname.local\share



На следующем шаге выбираем Domain-based namespace, так как используются доменные службы Active Directory.



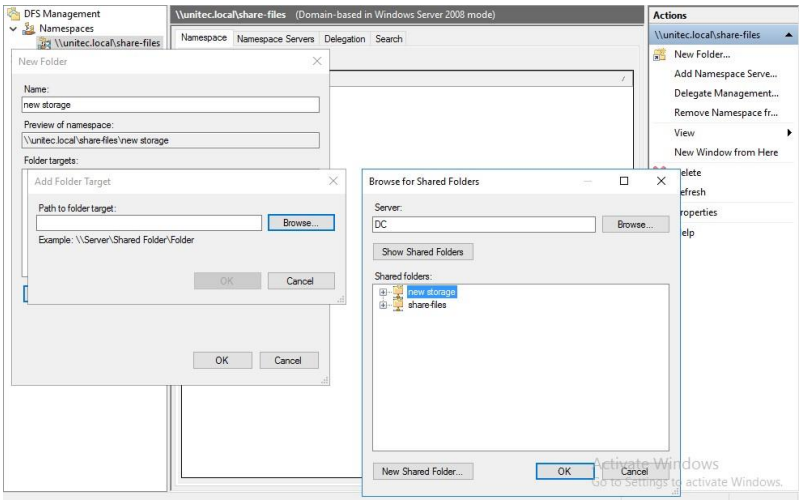
В результате видим сообщение об успешном создании пространства имен.



Теперь подключаем к нашему созданному Namespace сетевые папки.

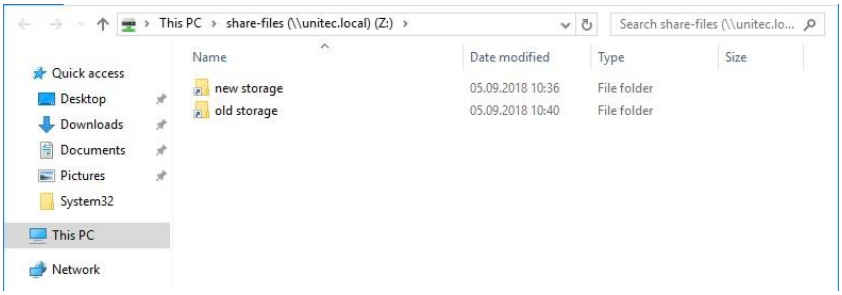
Настройку прав доступа для папок смотрите здесь >>>

Для создания новой папки выберете в правой части экрана New Folder. Задайте имя папки и путь к ней.



В моем случае у меня 2 разных сетевых папки на разных дисках. Но для пользователей отдела один сетевой ресурс:

\\companyname.local\share-files



Если в будущем мне понадобится добавить какие-либо сетевые папки для отделов, но при этом не подключать несколько сетевых ресурсов, то достаточно будет создать новый Namespace и подключить к нему нужные папки.

Если после удаления Namespace появилась ошибка и перестали отображаться другие, то нажмите на него и выберите Remove DFS Namespaces from the display. Ошибка исчезнет и все остальные Namespace появятся на экране.

Replication DFS (Репликация DFS) мною не настраивалась. Наличие свободных ресурсов всегда болезненный вопрос.

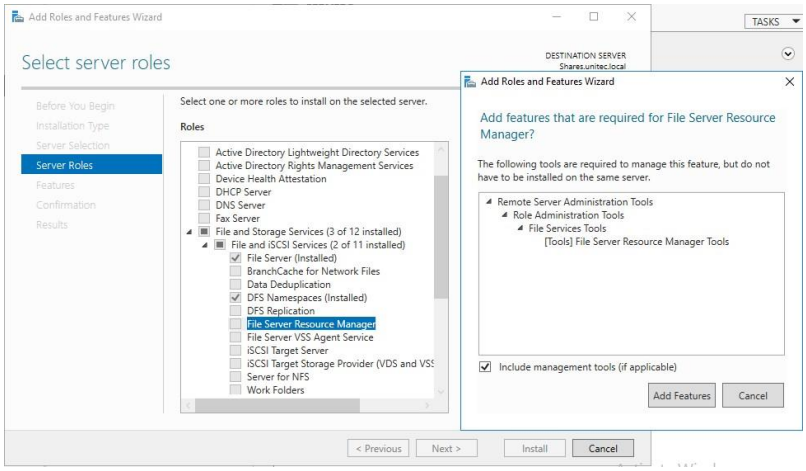
Для второго отдела был создана обычная сетевая папка с правами доступа.

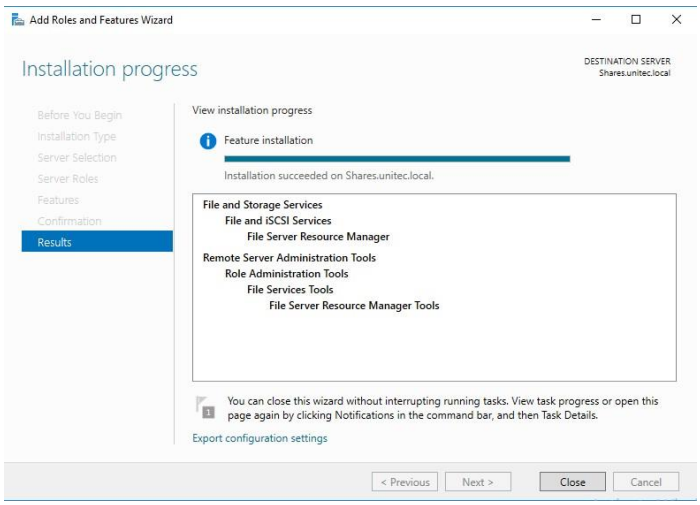
\\share\name-files

Настройка квот для сетевых папок в Windows Server 2016

Причины для установки квот на сетевые папки могут быть самые разные. Для меня было целью разделить место на логическом диске D: моего файлового сервера на 2 отдела.

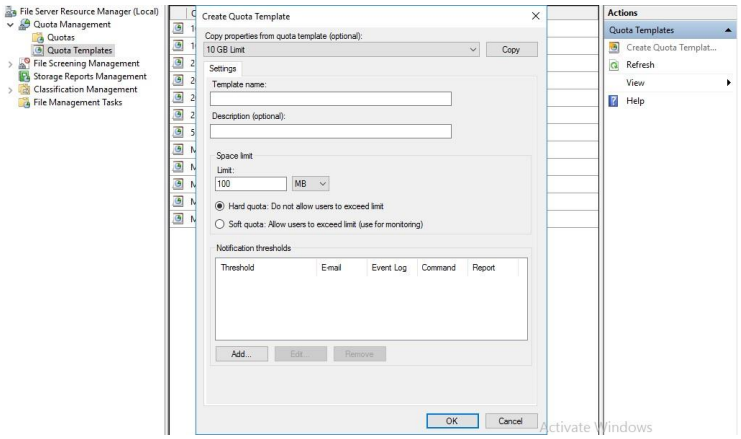
Для установки квот на сетевые папки необходимо установить File Server Resource Manager.





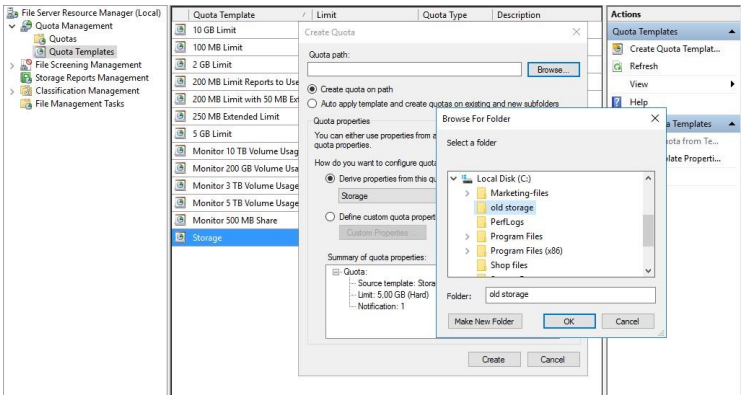
В Server Manager\Dashboard выберете > Tools > File Server Resource Manager. Откроется окно управления File Server Resource Manager. Если у вас в компании есть настроенный SMTP server с 25 портом, то вы можете настроить отправку уведомлений о квотах на e-mail администратора. Для этого выберите: File Server Resource Manager > Configure Options…

Для создания своей квоты выберите Quota Management > Quota Templates > Create Quota Templates

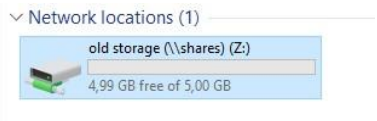


Задаем имя для нашей новой квоты, описание, если нужно, и устанавливаем лимит. Нажимаем OK. Квота создана. Если нажать кнопку ADD, то открывается окно с доп. настройками, в котором можно создать уведомления о действиях с папкой, к которой применена квота, запись уведомлений в журнал и отправки на e-mail администратора.

Создадим квоту Storage и применим ее к папке old storage.



Подключим эту папку на компьютере пользователя, видим результат.



2.18 Практическая работа№ 18
Реализация Client Endpoint Protection Настройка точки Endpoint Protection

Задание:

Загрузите установочный компакт-диск и запустите процедуру установки.

На панели установки выберите вариант Установить Symantec Endpoint Protection Manager.

В окне приветствия нажмите кнопку Далее.

В окне "Лицензионное соглашение" выберите Я согласен с условиями лицензионного соглашения. Нажмите кнопку Далее.

В окне "Целевая папка" измените или оставьте значение по умолчанию для папки установки.

Выполните одно из следующих действий:

Для настройки веб-сервера Symantec Endpoint Protection Manager IIS (Internet Information Service) в качестве единственного веб-сервера на этом компьютере выберите вариант Создать отдельный веб-сайт и нажмите кнопку Далее.

Для настройки веб-сервера Symantec Endpoint Protection Manager IIS для работы с другими веб-серверами на этом компьютере выберите Использовать веб-сайт по умолчанию и нажмите кнопку Далее.

Если установка производится на сервер под управлением Windows 2003 SB, то для настройки web-сервера необходимо выбирать вариант Использовать веб-сайт по умолчанию.

В окне, подтверждающем готовность к установке, нажмите кнопку Установить.

По завершении установки откроется окно "Работа мастера установки завершена". Нажмите Готово. Мастер настройки сервера управления запустится спустя примерно 15 секунд.

Как настроить Symantec Endpoint Protection Manager

На панели "Мастер настройки сервера управления" выберите тип конфигурации.

Примечание: Если выбрана Простая конфигурация, то пароль администратора SEPM применяется в качестве пароля шифрования. Если впоследствии пароль администратора изменяется, пароль шифрования остается без изменения.

Нажмите кнопку Далее.

В окне "Тип сайта" выберите Установить первый сайт и нажмите Далее.

В окне "Сведения о сервере" измените или оставьте значения по умолчанию для следующих полей и нажмите Далее:

Имя сервера

Порт сервера

Папка данных сервера

В поле "Имя сайта" измените или оставьте имя по умолчанию и нажмите Далее.

В окне "Пароль шифрования" укажите пароль в обоих полях и нажмите Далее.

Сохраните этот пароль во время установки Symantec Endpoint Protection в рабочей среде. Он указывается при восстановлении после аварии и добавлении аппаратных компонентов Enforcer.

В окне "Выбор сервера базы данных" выберите Встроенная база данных и нажмите Далее.

На панели настройки пользователя укажите пароль, который должен вводиться при входе на консоль от имени пользователя "Admin". Нажмите кнопку Далее. Или создайте пользователя который является администратором домена.

Как настроить клиент

В окне "Работа мастера настройки сервера управления завершена" выберите Да и нажмите Готово.

В окне "Вас приветствует мастер переноса и развертывания" нажмите кнопку Далее.

В окне "Выберите нужное действие" выберите Развернуть клиент и нажмите кнопку Далее.

В следующем окне выберите пункт Укажите имя новой группы, в которую следует добавить клиенты, введите имя группы и нажмите кнопку Далее.

В следующем окне отмените выбор программ клиента, которые не следует устанавливать, и нажмите Далее.

В следующем окне укажите параметры для пакетов, файлов и взаимодействия с пользователем.

Нажмите кнопку "Обзор", выберите папку для установочных файлов и нажмите кнопку Открыть.

Нажмите кнопку Далее.

В следующем окне выберите Да и нажмите Готово.

Не включайте параметр запуска консоли администратора. Создание и экспорт пакета установки для группы может занять до 5 минут. Потом откроется мастер развертывания методом рассылки.

Как развернуть клиент с помощью мастера развертывания методом рассылки

В окне мастера развертывания методом рассылки в списке "Доступные компьютеры" выберите компьютеры, на которых следует установить клиент, и нажмите кнопку Добавить.

Если клиент разворачивается на локальном компьютере, и брандмауэр Windows не настроен для обработки Java, то он может блокировать эту функцию, показав сообщение о необходимости ее настройки. Это окно может быть показано под окном мастера развертывания методом рассылки, то есть не будет видно пользователю. Если мастер развертывания методом рассылки перестал отвечать, переместите его окно вбок и проверьте, не скрыто ли под ним окно с сообщением брандмауэра Windows.

В окне "Идентификация удаленного клиента" введите имя пользователя и пароль для входа в домен или рабочую группу Windows этих компьютеров и нажмите кнопку OK. После того как все компьютеры будут выбраны и показаны на правой панели, нажмите кнопку Готово.

После завершения установки нажмите кнопку Готово.

Как активировать Symantec Network Access Control

Закройте консоль Symantec Endpoint Protection Manager, если она открыта.

Вставьте компакт-диск продукта Symantec Network Access Control.

На панели установки выберите пункт Установить Symantec Network Access Control. Нажмите Установить Symantec Endpoint Protection Manager.

В окне "Обновление сервера управления" нажмите кнопку Далее.

Нажмите Продолжить.

Когда в окне "Состояние обновления сервера" будет показано сообщение об успешном завершении обновления, нажмите кнопку Далее.

Нажмите кнопку Готово.

Войдите на консоль Symantec Endpoint Protection Manager.

На вкладке "Политики" выберите Целостность хоста.

На правой панели выберите Политика целостности хоста.

В разделе "Задачи" выберите Присвоить политику.

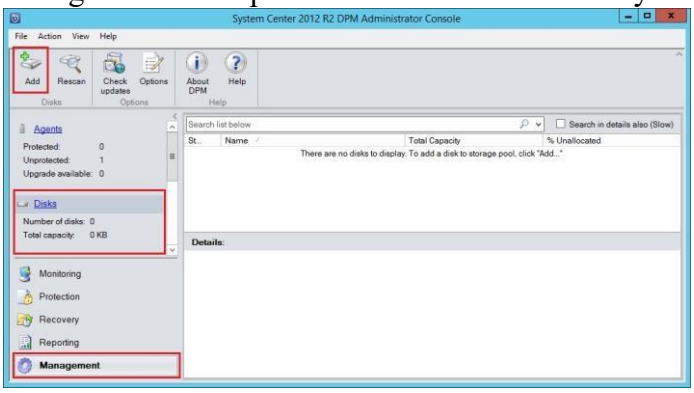
В окне "Присвоить политику целостности хоста" выберите группу, которой следует присвоить политику.

Нажмите кнопку Присвоить, а затем нажмите Да, чтобы подтвердить изменение.

2.19 Практическая работа№ 19
Настройка Data Protection для данных клиентского компьютера

Задание:

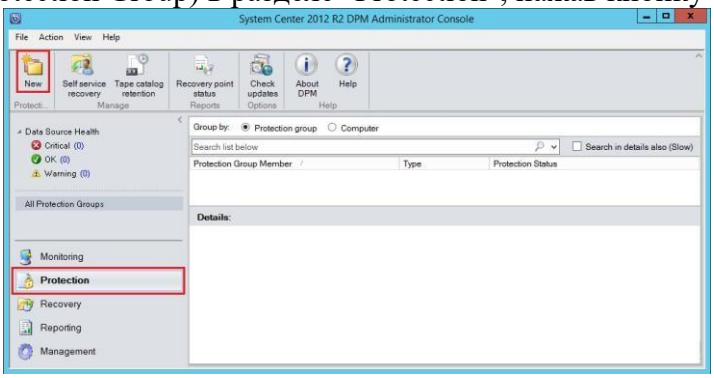
Подключение локального диска в SC DPM 2012 осуществляется в консоли DPM, в разделе "Management". В верхнем меню нажмите кнопку кнопку "Add".



Из предложенных дисков выберите тот диск или диски, которые будут использоваться для хранения резервных копий данных. Если подключены более одного диска, тогда дисковое пространство суммируется и представляется как один большой диск.
Примечание. С подключенного диска будут удалены все данные и он не будет доступен через Explorer в операционной системе.

Настройка резервного копирования на подключенный диск

Для настройки резервного копирования на локальный диск нужно создать группу защиты (Protection Group) в разделе "Protection", нажав кнопку "New"

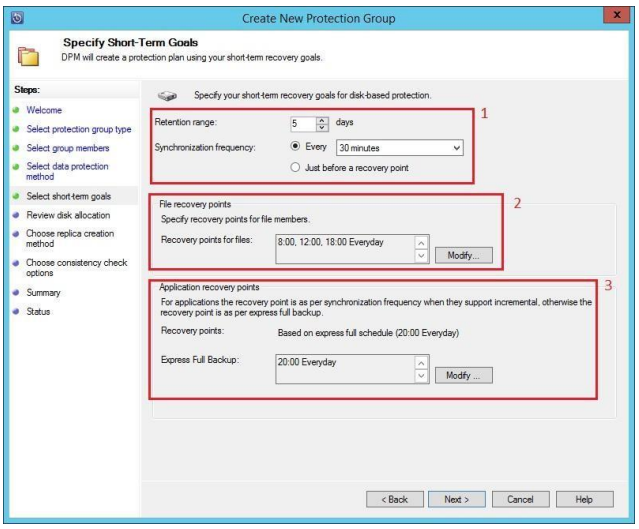


В разделе выбора метода защиты (Protection method) выберите "Disk"

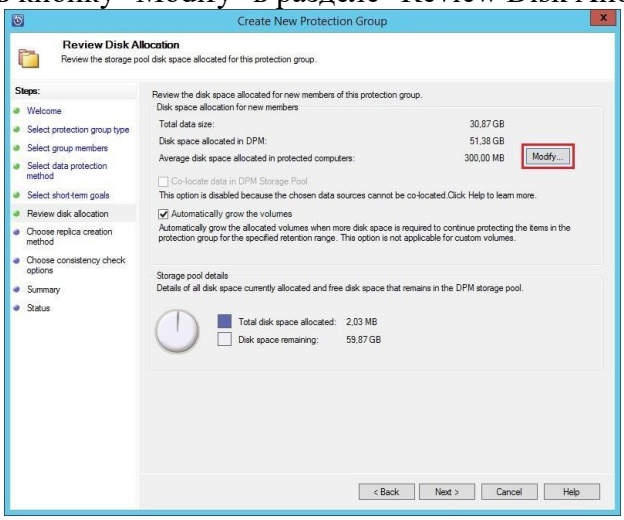
Объем данных резервного копирования регулируется настройкой копирования данных:
Глубиной архивации (в примере показано, что данные будут храниться за последние 5 дней)

Частотой создания точек восстановления файлов

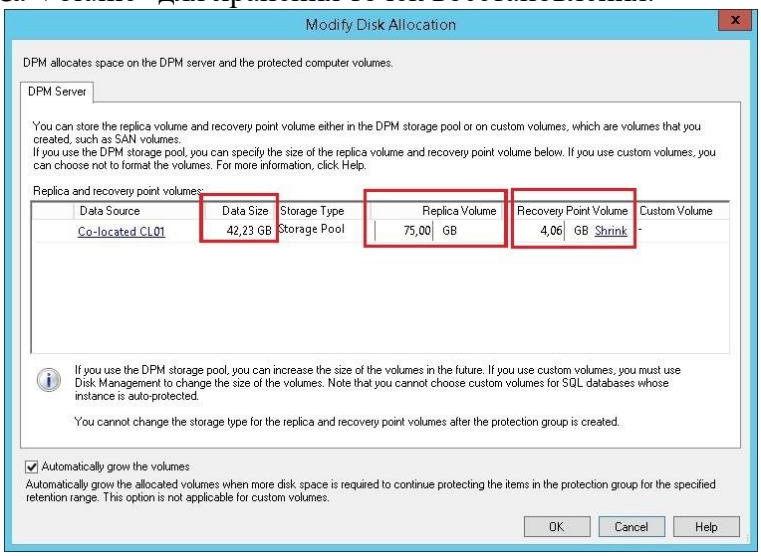
Частотой создания точек восстановления приложений



Дисковое пространство, выделяемое под резервное копирование данных, задается как автоматически, так и вручную. Чтобы выделить дисковое пространство вручную, нужно нажать кнопку "Modify" в разделе "Review Disk Allocation"

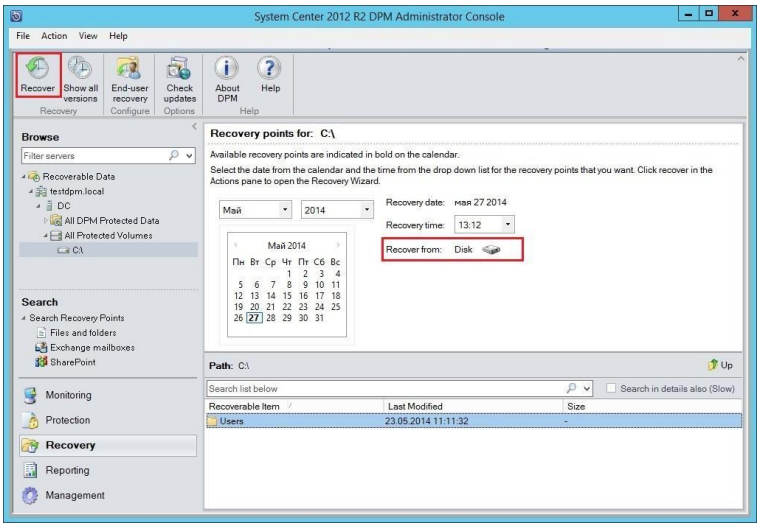


В поле "Data Size" отображается размер уже использованного дискового пространства под данные, в поле "Replica Volume" - общий размер выделенного дискового пространства под данные, в поле "Recovery Point Volume" - выделенное дисковое пространство из "Replica Volume" для хранения точек восстановления.

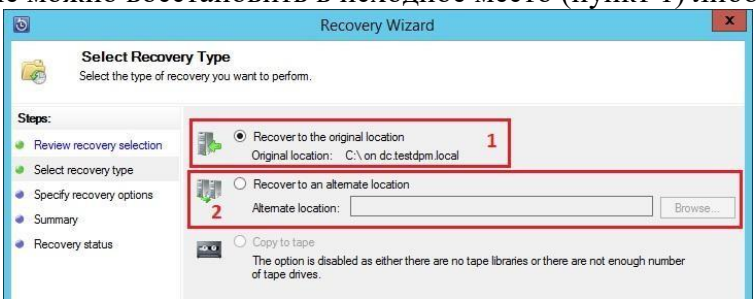


Восстановление данных из резервной копии на локальном диске

Для восстановления данных из резервной копии на локальном диске, нужно перейти в раздел "Recovery", выбрать точку восстановления данных и нажать кнопку "Recover"



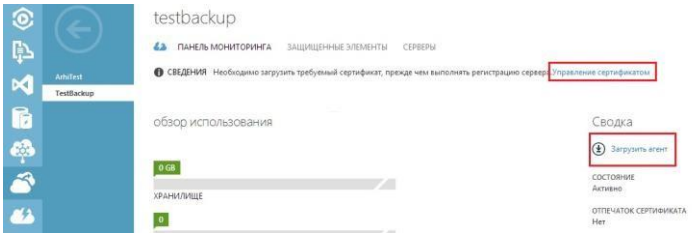
Данные можно восстановить в исходное место (пункт 1) либо в любое другое (пункт 2)



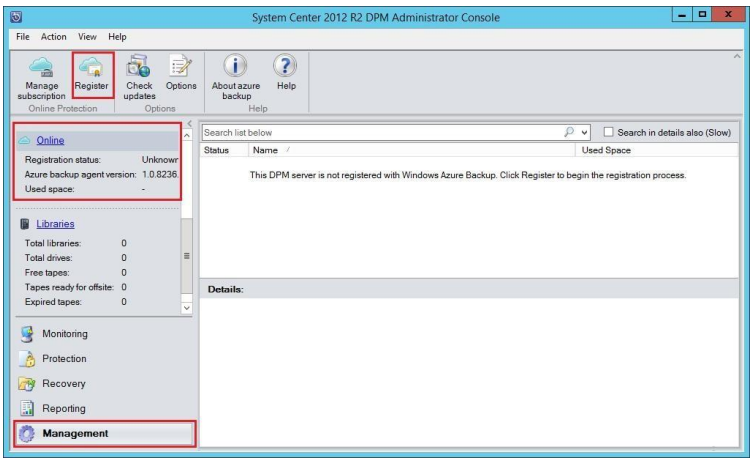
Подключение Azure Backup

Для подключения Azure Backup в SC DPM предварительно необходимо установить приложение-агент Azure Backup и установить сертификат.

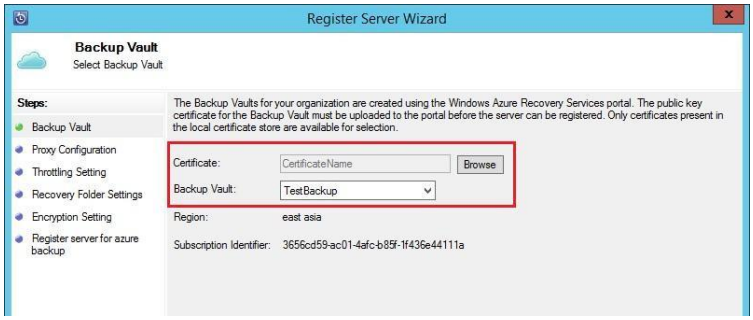
Приложение-агент скачайте с портала Azure Backup и установите сертификат.



Далее в SC DPM зарегистрируйте Ваш Azure Backup. Для этого в разделе "Management" нажмите "Online" и затем нажмите кнопку "Register".



При регистрации сервера Azure Backup в SC DPM нужно указать тот же сертификат, что и загружали в портале, после чего выбрать хранилище.

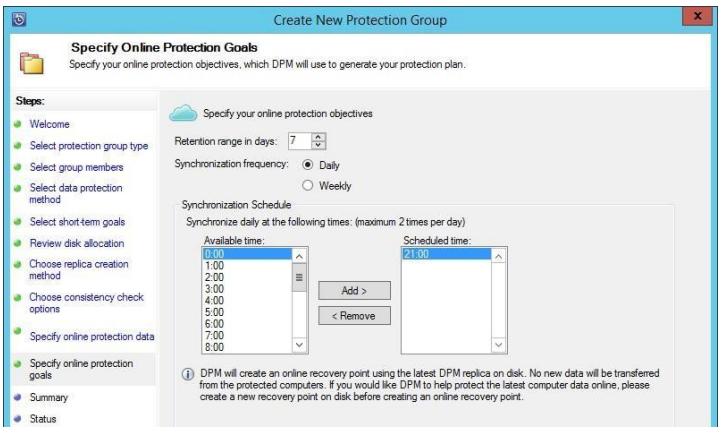


Настройка резервного копирования в Azure Backup

Настройка резервного копирования в Azure Backup выполняется аналогично копированию на диск. Отличием является то, что в Azure Backup можно копировать только файлы.

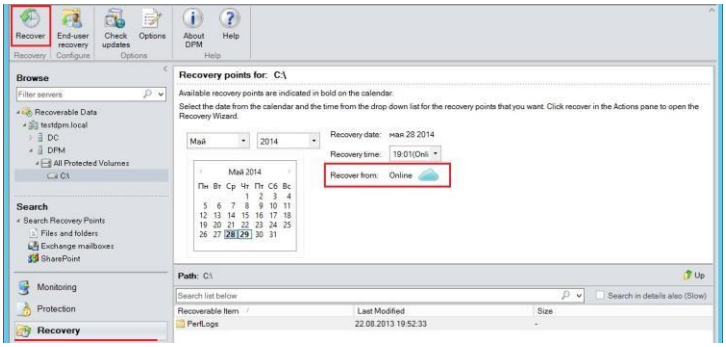
При выборе метода защиты нужно указать "Online protection". Следует заметить, что возможно одновременное использование и онлайн копирования, и копирования данных на локальный диск.

Также для онлайн копирования можно настроить глубину архивации (за какой промежуток времени будут хранится данные) и расписание синхронизации

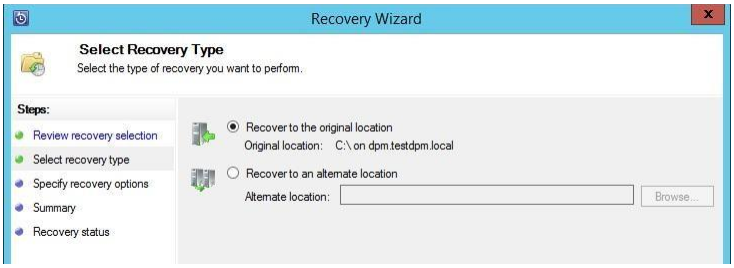


Восстановление данных с Azure Backup

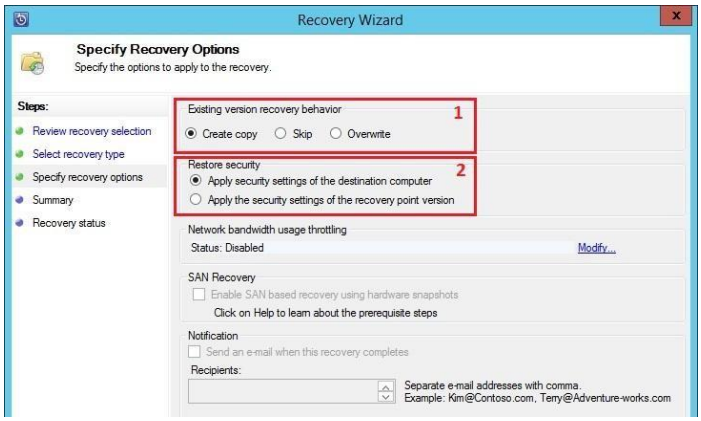
Процедура восстановления с Azure Backup аналогична восстановлению с диска. Для выполнения восстановления данных перейдите в раздел "Recovery", найдите нужную Вам запись и нажмите кнопку "Recover". Данные, хранящиеся в Azure Backup, будут отмечены как "Online"



Выберите метод восстановления: в исходное расположение данных или в любое другое место



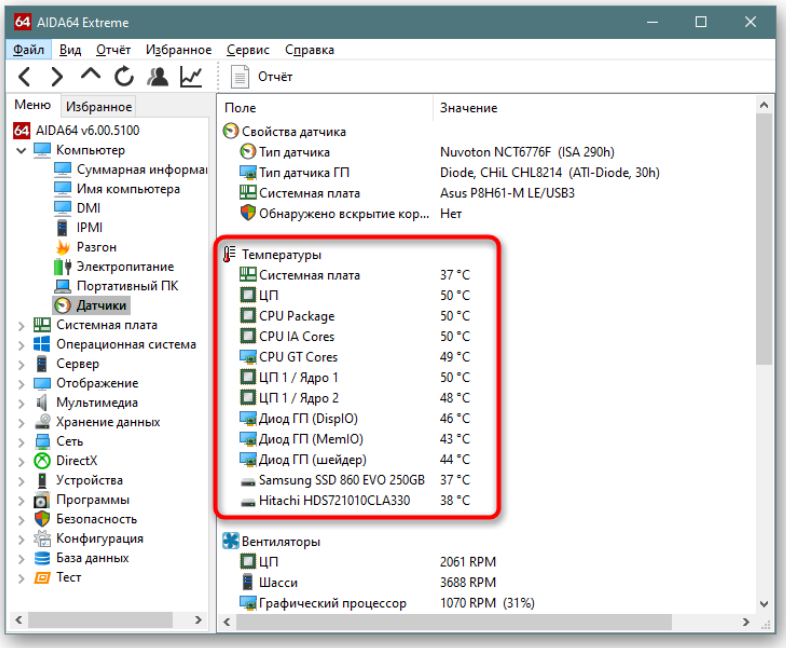
Укажите что делать с данными, если обнаружатся файлы с такими же именами (пункт 1) и какие настройки безопасности для данных использовать (пункт 2)



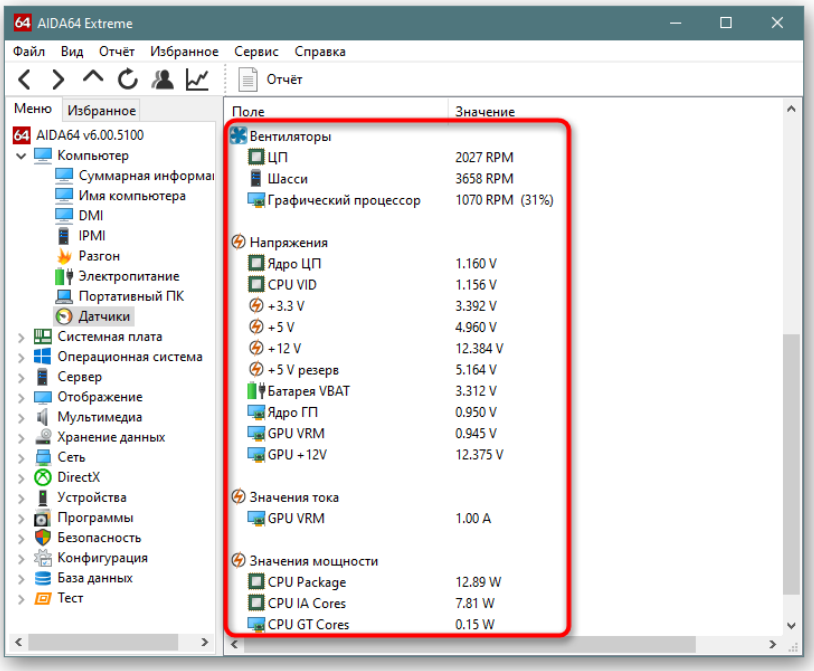
2.20 Практическая работа№ 20
Мониторинг производительности и работоспособности инфраструктуры клиентских ОС Настройка

Задание:

Вся информация отображается в режиме реального времени и позволяет отслеживать и вовремя выявлять перегрев каких-либо частей. Осуществляется это через «Компьютер» > «Датчики».

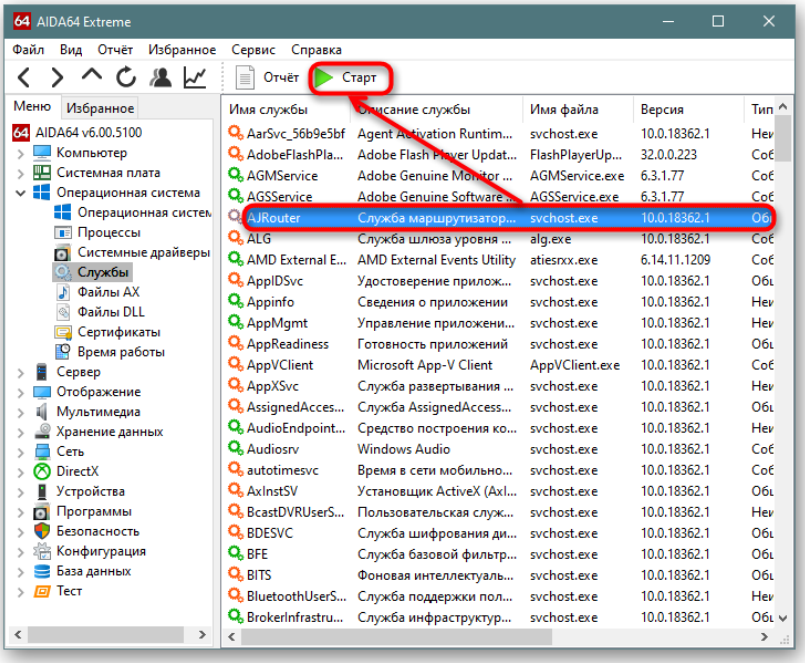


Здесь же можно посмотреть, с какой скоростью крутятся все установленные вентиляторы, под каким напряжением находятся компоненты компьютера, значение тока и мощности. Эти данные нужны уже для более продвинутых пользователей, которые занимаются разгоном и следят за тем, как ведут себя разогнанные устройства.



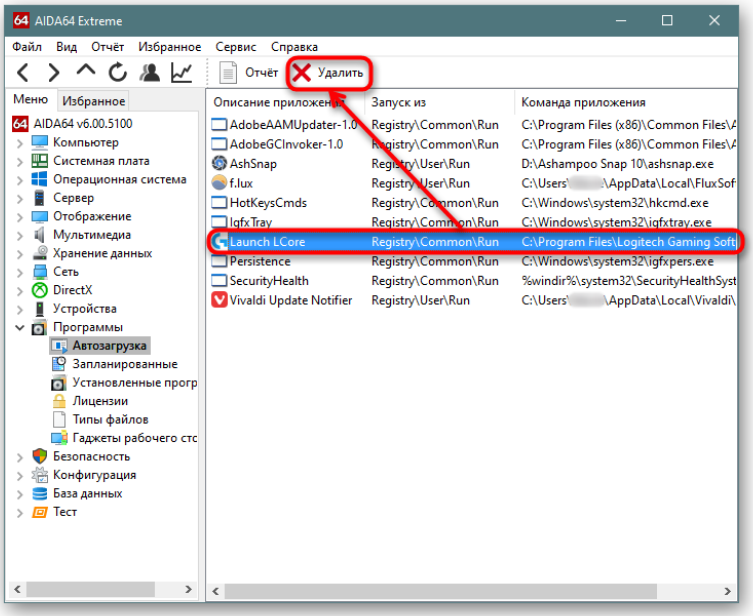
Запуск и остановка служб

При параллельном использовании других возможностей AIDA64 может стать альтернативой стандартному системному приложению «Службы». Зайдя в «Операционная система» > «Службы», вы будете с удобством просматривать отключенные и включенные службы, какие EXE-файлы отвечают за работу каждой службы, запускать остановленные и отключать запущенные службы.



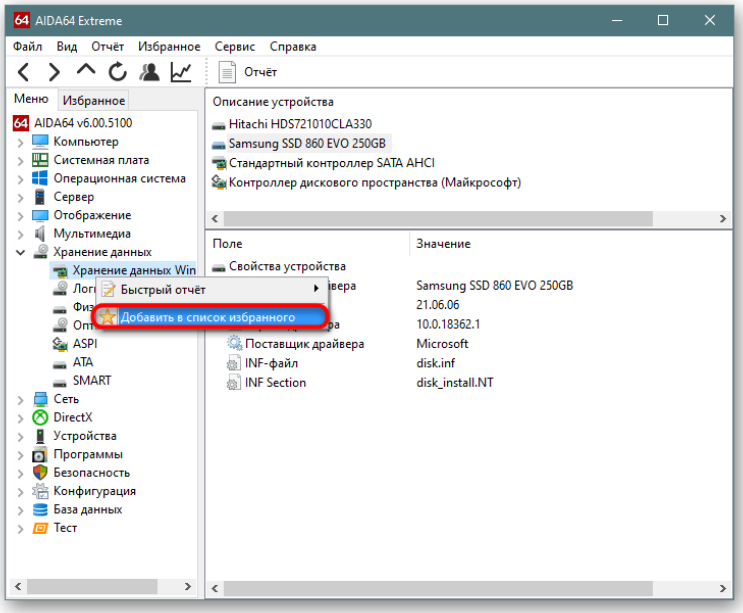
Управление автозагрузкой

Аналогично службам, позволяется управлять добавленными в автозагрузку программами («Программы» > «Автозагрузка»). На самом деле, это не очень удобно, поскольку ровно ту же функциональность предоставляет обычный «Диспетчер задач» в Windows 10, но определенным пользователям это все же будет полезно.

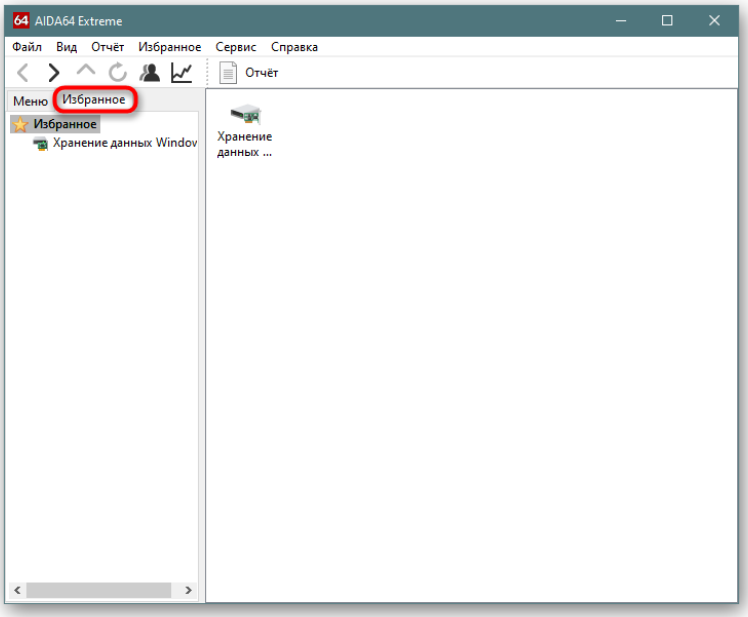


Добавление разделов в избранное

Поскольку в программе довольно много вкладок, которые дополнительно разворачиваются, при необходимости получения информации из разных разделов, удобнее всего добавить их все в «Избранное». Для этого достаточно кликнуть правой кнопкой мыши по подразделу и выбрать пункт «Добавить в список избранного».

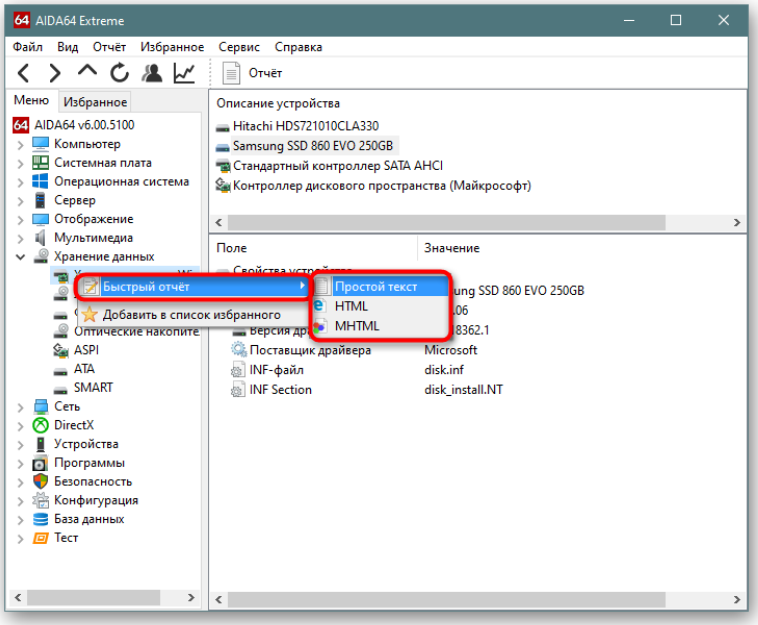


Теперь для просмотра всех избранных подразделов переключитесь на соответствующую вкладку.

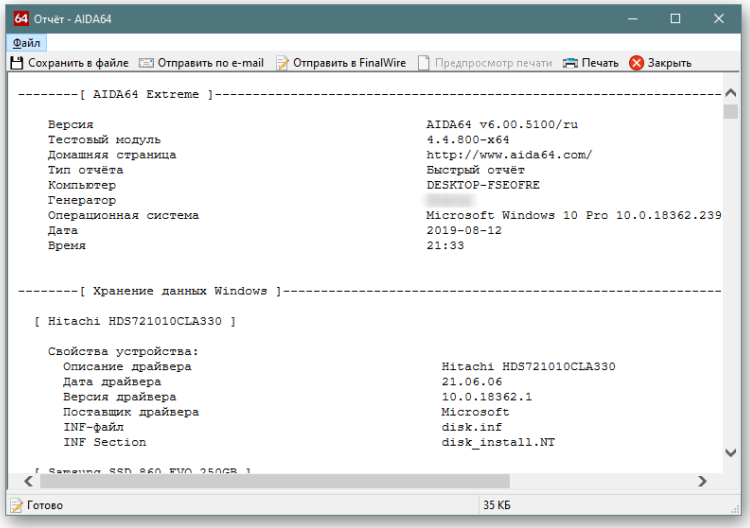


Создание отчетов

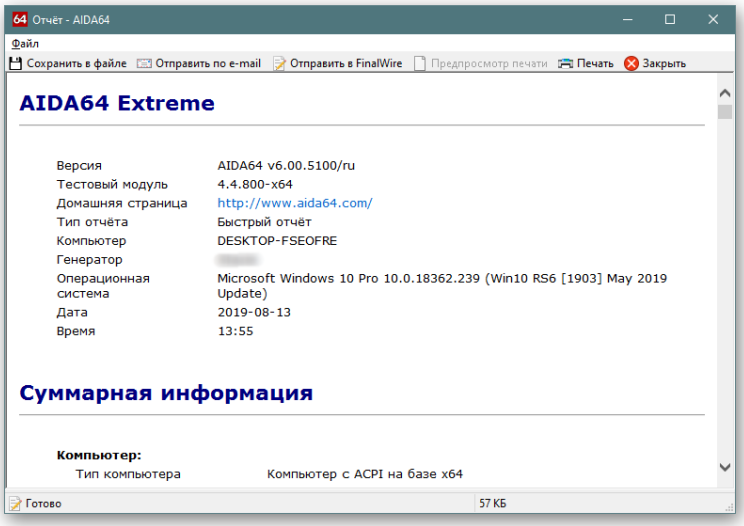
Функциональность AIDA64 была бы неполной без функции создания отчетов. Программа умеет создавать разные виды тестов, которые пригодятся пользователям в статистических целях, для отправки специалистам при возникшей проблеме с ПК или для сравнения при разгоне. Есть два варианта — быстрый отчет и «Мастер отчетов». Для получения быстрого отчета щелкните по подразделу правой кнопкой мыши и выберите «Быстрый отчет», где укажите формат, который хотите получить.



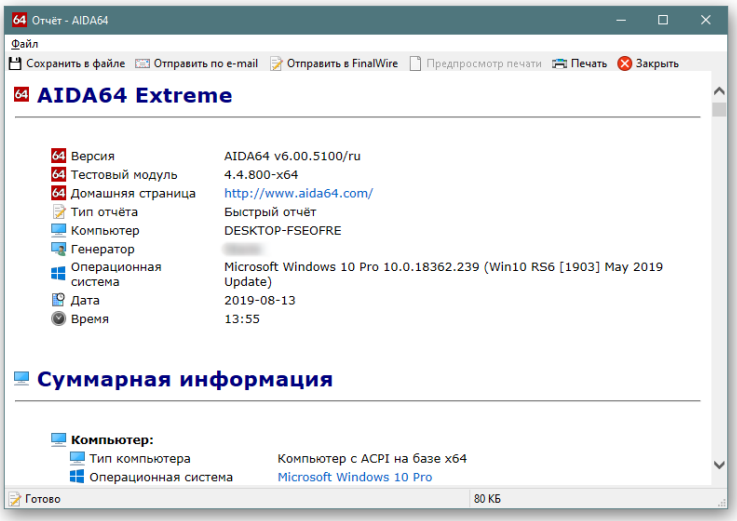
Вот пример «Простого отчета», который доступен для сохранения, отправки в печать или на E-mail.



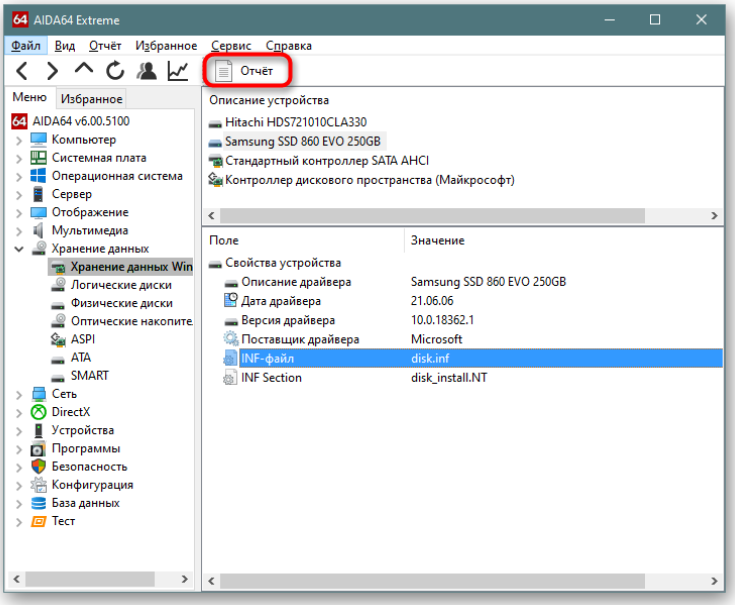
HTML-вариант просто добавляет разметку и сохраняет файл в соответствующем форме.



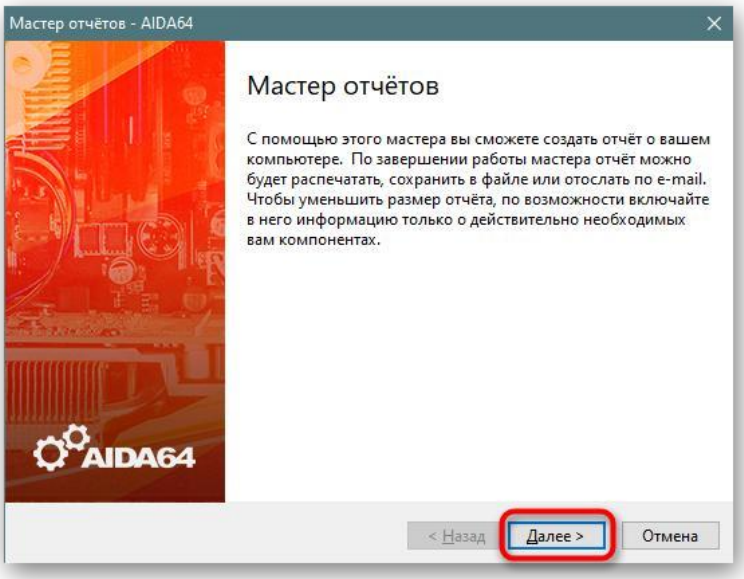
MHTML дополнительно оснащен иконками и сохраняется с расширением HTM, как и предыдущий вариант.



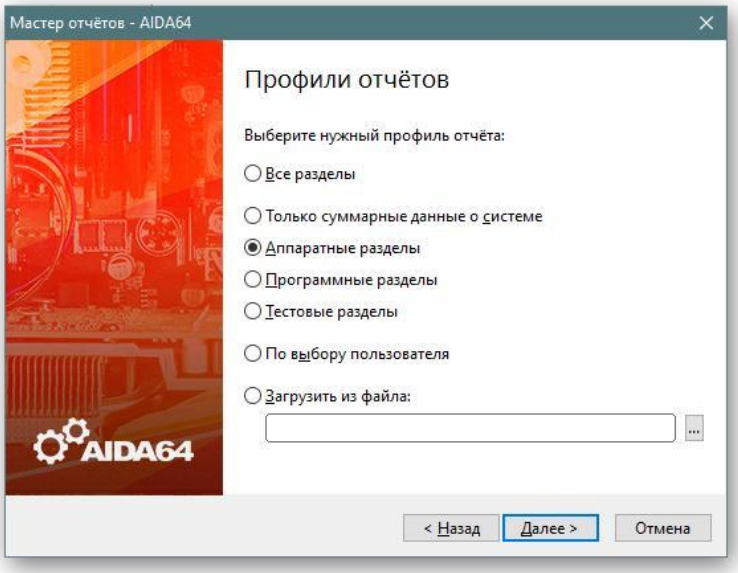
Однако таким образом можно получить отчет только одного подраздела. Когда появляется надобность сохранить текстом сразу несколько вариантов, поможет кнопка вызова «Мастера отчетов», что находится на верхней панели.



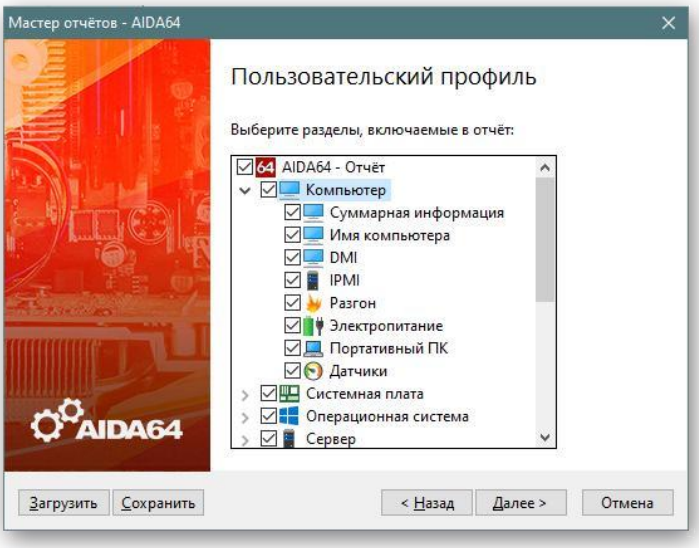
После нажатия на нее вам просто понадобится следовать подсказкам.



А именно — выбрать тип отчета и формат, в котором он будет сохранен (он будет экспортирован в те же TXT, HTM, показанные выше).

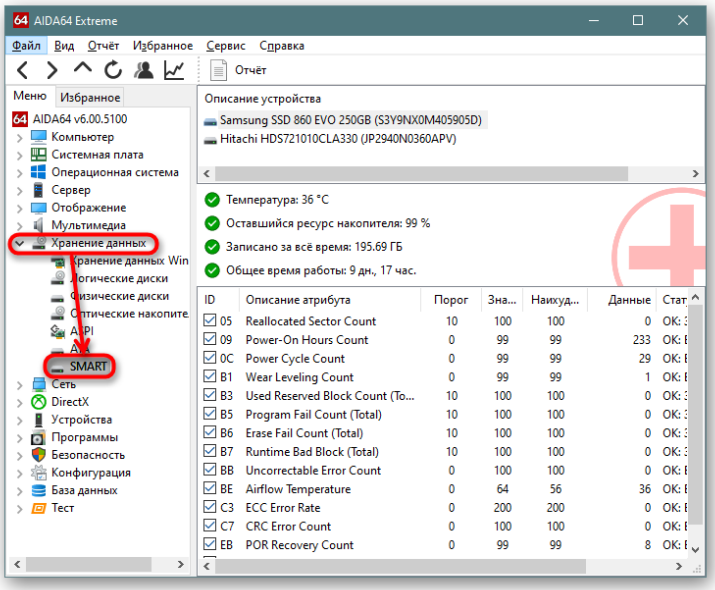


Например, если указать тип отчета «По выбору пользователя», можно быстро выделить несколько разделов и подразделов, указать расширение и получить текстовый файл с данными.



SMART-показатели

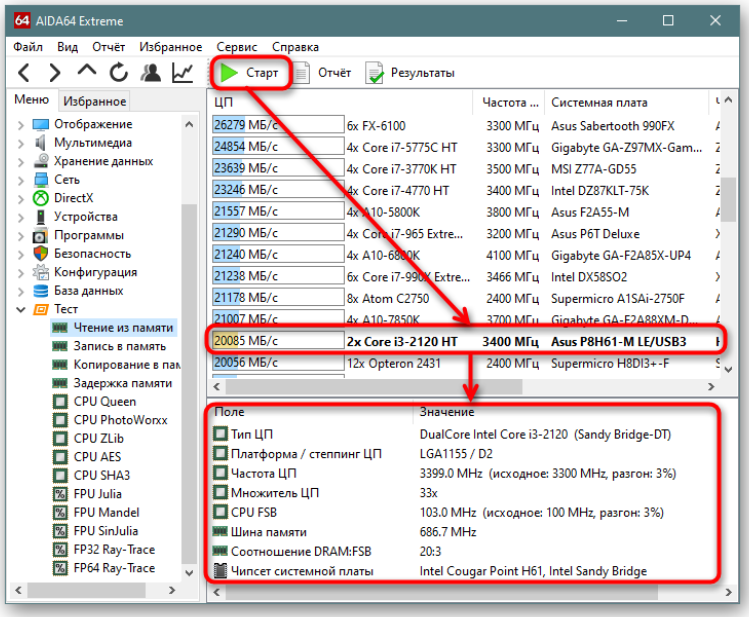
Для того чтобы узнавать подробные данные о состоянии жесткого диска, вовсе не обязательно скачивать отдельные программы типа HDD Life или SSD Life — эту же информацию тоже легко получить через AIDA64, перейдя в «Хранение данных» > «SMART». Тут надо выбрать устройство, которое будет проверяться, после чего в окне появится температура, оставшийся ресурс, количество записанных гигабайт и общее время работы.



Еще ниже вы увидите классическую таблицу с атрибутами SMART. Помимо стандартных колонок с порогом и значениями для удобства был добавлен столбец «Статус», который просто уведомляет о здоровье каждого составляющего устройства.

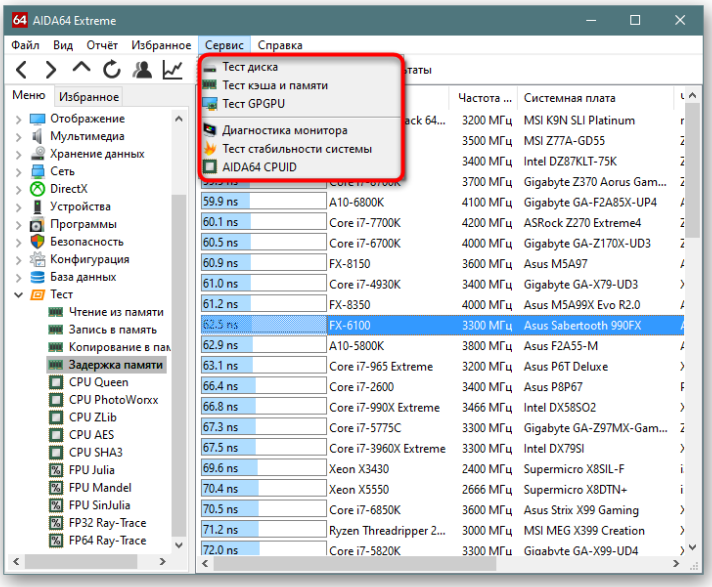
Прохождение тестов

В разделе «Тест» вы можете запустить тесты определенных параметров оперативной памяти и процессора. Это особенно полезно для тех юзеров, кто желает заняться грамотным разгоном компьютера. После нажатия на кнопку «Старт» начнется непродолжительная проверка, по результатам которой проверенный компонент попадет на определенную позицию сравнительной лестницы, а чуть ниже отображаются все сопутствующие значения.



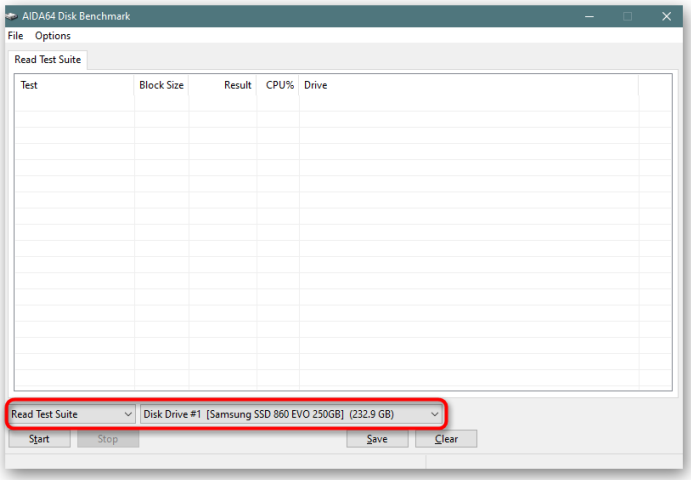
Бенчмарки

В программе есть также отдельный раздел, куда вынесено 6 тестов и бенчмарков, проверяющих разные составляющие компьютера. Они находятся в выпадающем меню «Сервис». Их существенный минус — отсутствие русификации, что вызовет затруднение в использовании у начинающих юзеров. Не забывайте, что результаты каждых тестов доступны к сохранению в виде файла, путем нажатия на кнопку «Save».

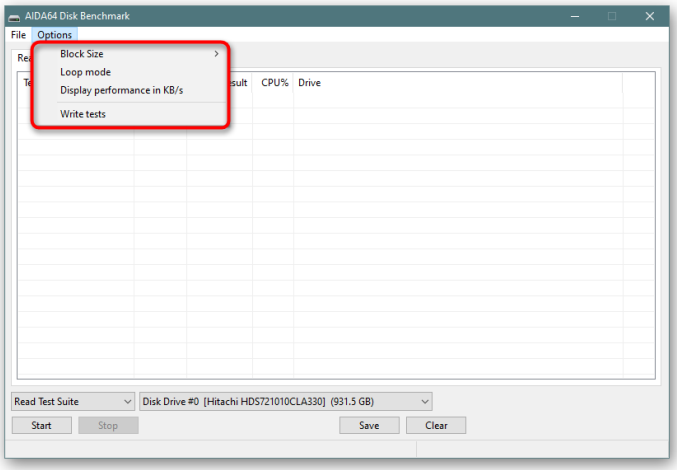


Тест диска

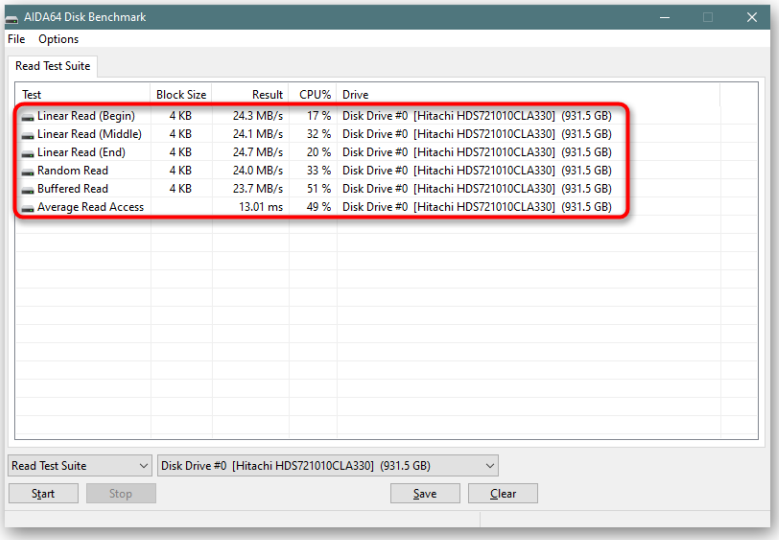
Тест позволяет проверить производительность устройств хранения данных: HDD (ATA, SCSI, RAID-массивы), SSD, CD/DVD, USB-Flash, карты памяти. В первую очередь это необходимо для поиска ошибок или обнаружения поддельных накопителей. Внизу окна выбирается операция чтения, которая будет производиться, а также диск, который будет проверяться.



Дополнительно рекомендуем настроить опции: размер блока, от которого зависит продолжительность проведения теста, режим петли (зацикленный запуск текста после его завершения до момента, пока он не будет остановлен вручную), отображение производительности в KB/s (по желанию).

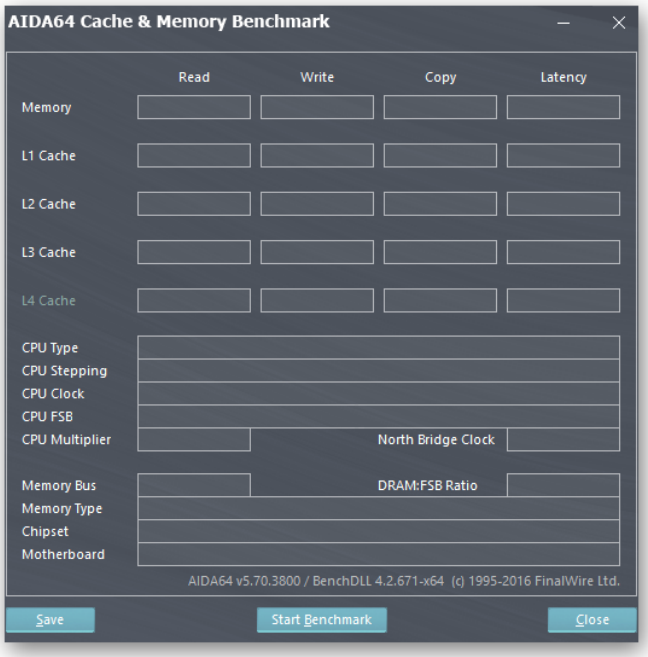


Если вы захотите провести тесты записи («Write tests»), учтите, что их использование сотрет все с накопителя. По этой причине имеет смысл их использовать только на новых устройствах для проверки на подлинность или если накопитель впоследствии все равно будет отформатирован.
Результат теста покажет, насколько производительно происходит выполнение той или иной операции с конкретным размером блока. Полученные скорости и процент загрузки процессора в этот момент имеет смысл сравнить с другими результатами (например, с отчетами других пользователей или при чтении обзора с тестированием какой-либо модели HDD/SSD) чтобы понять, насколько хороши или плохи полученные показатели.



Тест кэша и памяти

Благодаря этому тесту можно узнать пропускную способность и задержку кэшей процессора L1-L4 и его памяти. Не обязательно запускать проверку целиком, достаточно кликнуть дважды мышкой в каждый блок, чтобы получить конкретную информацию.
Если вместо этого нажать на «Start Benchmark», тоже можно указать, что будет проверено — память или кэш.



По большей части эти показатели нужны для разгона и сравнений «До» и «После».

Тест GPGPU и Тест стабильности системы

Мы объединили два эти теста потому, что для них у нас отведены отдельные статьи на сайте с инструкциями по использованию. Они позволяют проверить разные параметры процессора, и более подробно об этом предлагаем прочитать по ссылкам ниже. Тест стабильности системы в АИДА64 является самым популярным, поэтому советуем отвести изучению и пониманию тем, как им пользоваться, больше времени. Он будет очень полезным не только при разгоне, но и для проверки стабильности работы ПК, выявлению ошибок для дальнейшего их исправления.

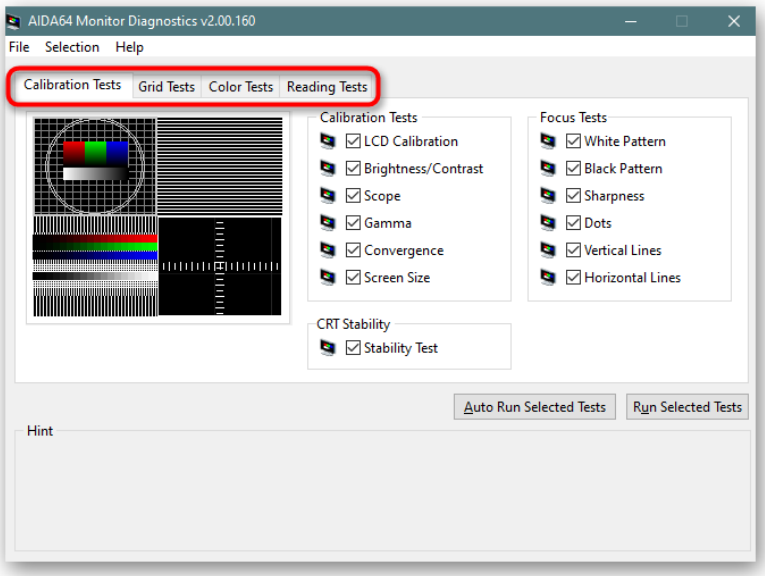
Подробнее:

Проводим тест на стабильность в AIDA64

Проводим тестирование процессора

Диагностика монитора

Узнать о возможностях и наличии проблем с монитором поможет этот бенчмарк. Здесь есть 4 вкладки: калибровка, сетчатые тесты, цветовые тесты, тесты с чтением текста.



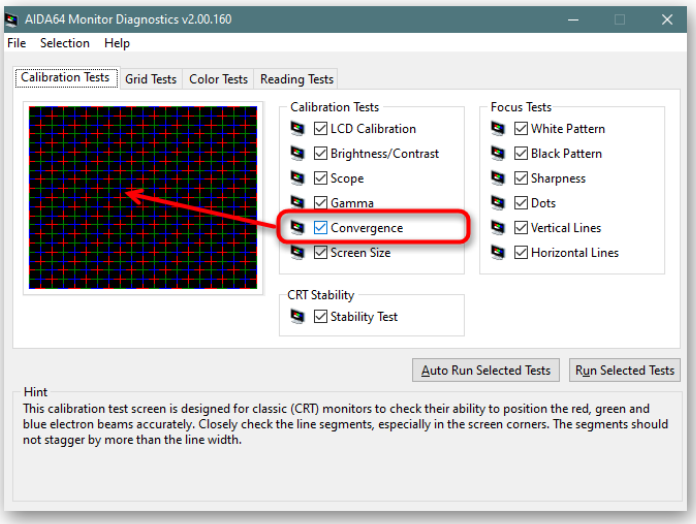
Calibration Tests. Эти тесты помогут настроить правильную передачу цветов, приблизить их отображение к натуральным на CRT и LCD-мониторах.

Grid Tests. Тесты для проверки и настройки геометрии и сближения монитора.

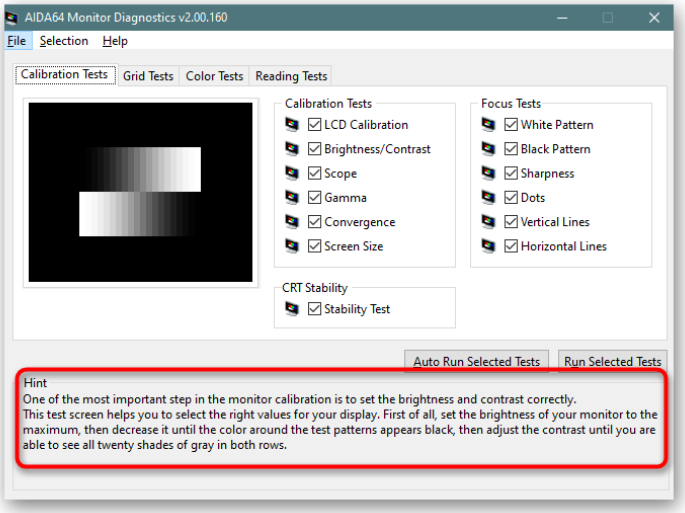
Color Tests. Тесты для проверки качества отображения цветов монитором, поиска битых пикселей на LCD-дисплеях.

Reading Tests. Проверка чтения шрифтов разных цветов на разных фонах.

Запускайте тесты и калибруйте дисплей, используя настройки вашего монитора при помощи кнопок на панели, обычно расположенной снизу.
Все тесты поделены на разделы, и вы можете снимать галочки с тех, которые не желаете проводить. Наводя на каждый из тестов, его превью будет видно слева, что упростит отключение всего ненужного.

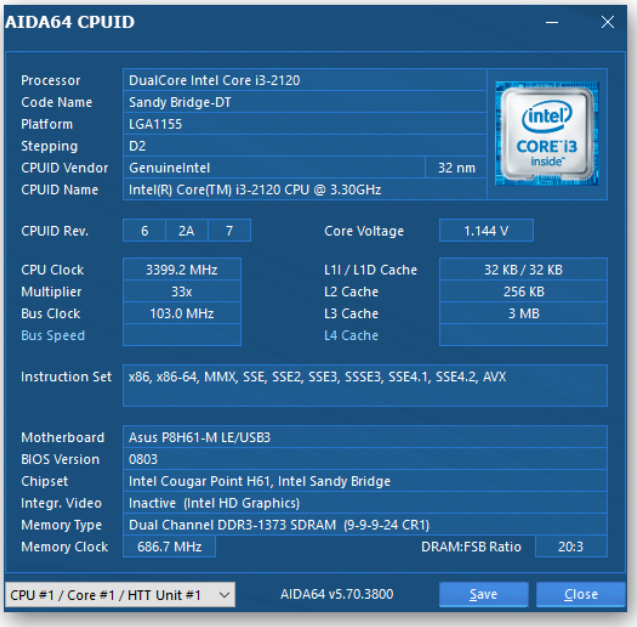


Кроме того, наводя на каждый тест, есть возможность узнать о нем подробнее, прочитав подсказку внизу. К сожалению, формат статьи не позволяет рассмотреть каждый из них, поэтому при необходимости воспользуйтесь онлайн-переводчиками или задайте вопрос в комментариях касательно любого из тестов.



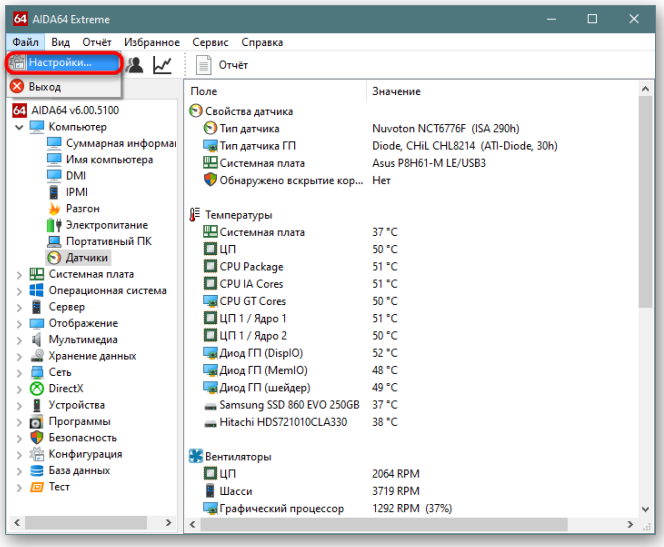
AIDA64 CPUID

Общая и расширенная информация о процессоре, отображающая герцовку и вольтаж в режиме реального времени. По сути, эти же сведения получаются и через одноименный раздел в главном меню AIDA64, с той лишь разницей, что визуальное восприятие более удобно, а также осуществляется выбор ядер и переключение между процессорами (если их в конфигурации ПК больше одного) при помощи специального выпадающего меню внизу.



Настройки

Активным пользователям АИДА64 часто требуется ее донастройка под себя и свои потребности. Для этого через меню «Файл» нужно перейти в «Настройки».



Помимо изменения стандартных параметров типа поведения AIDA64, обновлений и прочего тут можно найти и нечто более полезное. Например, настроить отправку отчетов на E-mail, изменить параметры создаваемых отчетов, добавить пользовательские устройства (кулер системы, источник питания и др.) вручную, изменить частоту обновления показателей температур, задать триггер для тревоги (например, максимальная загрузка ЦП, оперативной памяти, использования виртуального или физического диска, критическая температура, напряжение одного из компонентов ПК и так далее) и действие, которое будет происходить при возникновении опасности (уведомление, отключение ПК, запуск какой-либо программы, отправка уведомления на электронную почту).