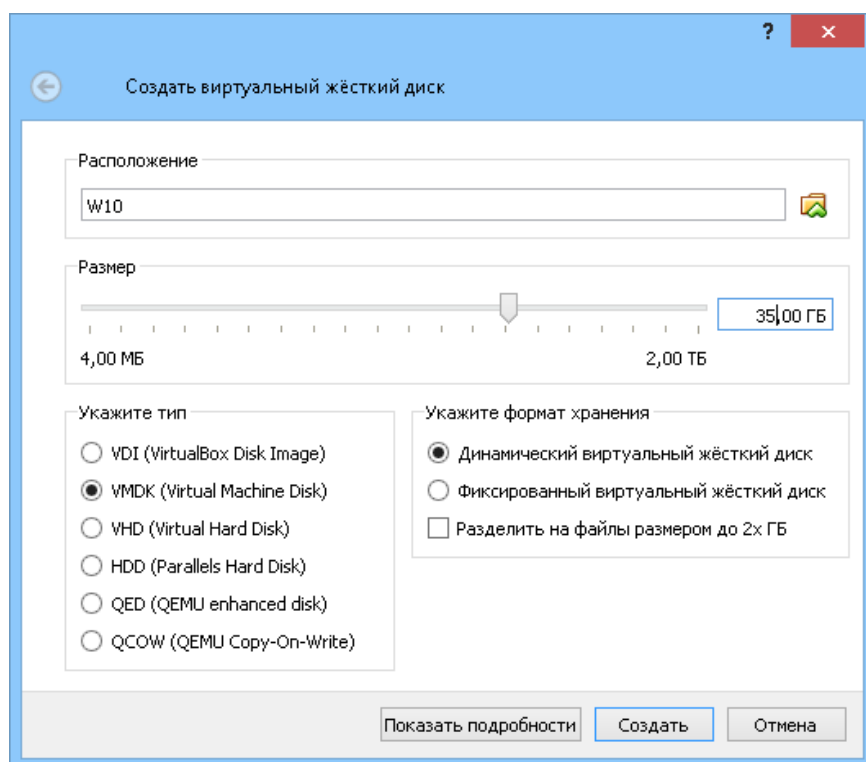
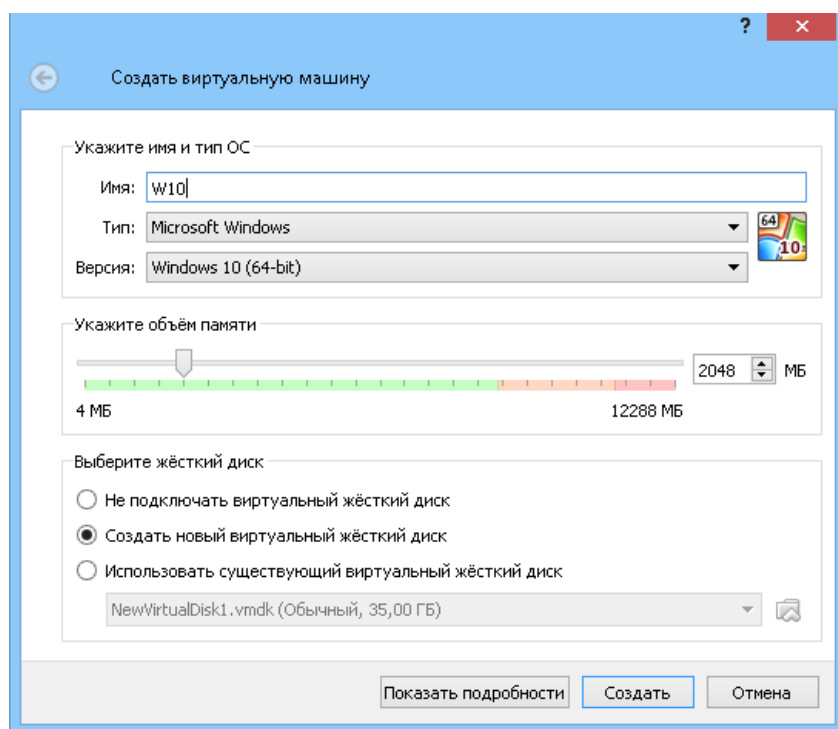
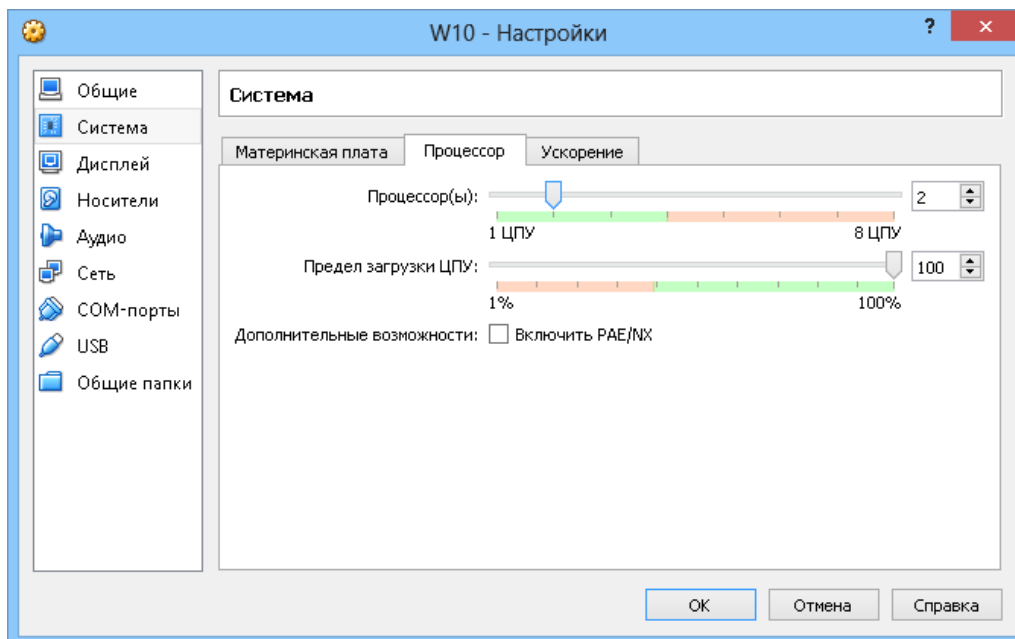
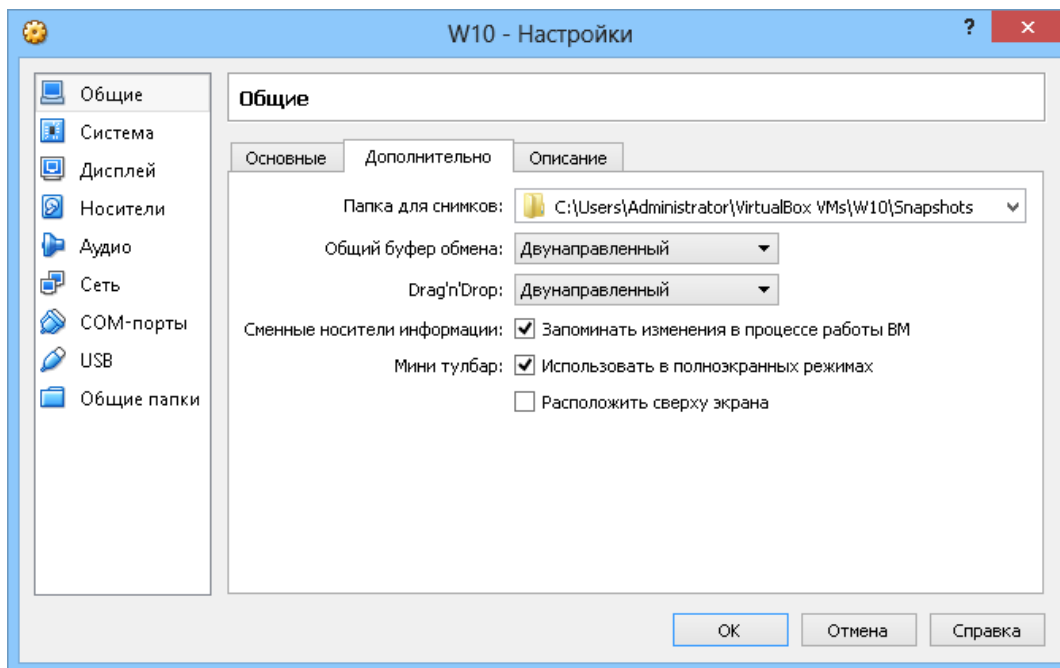
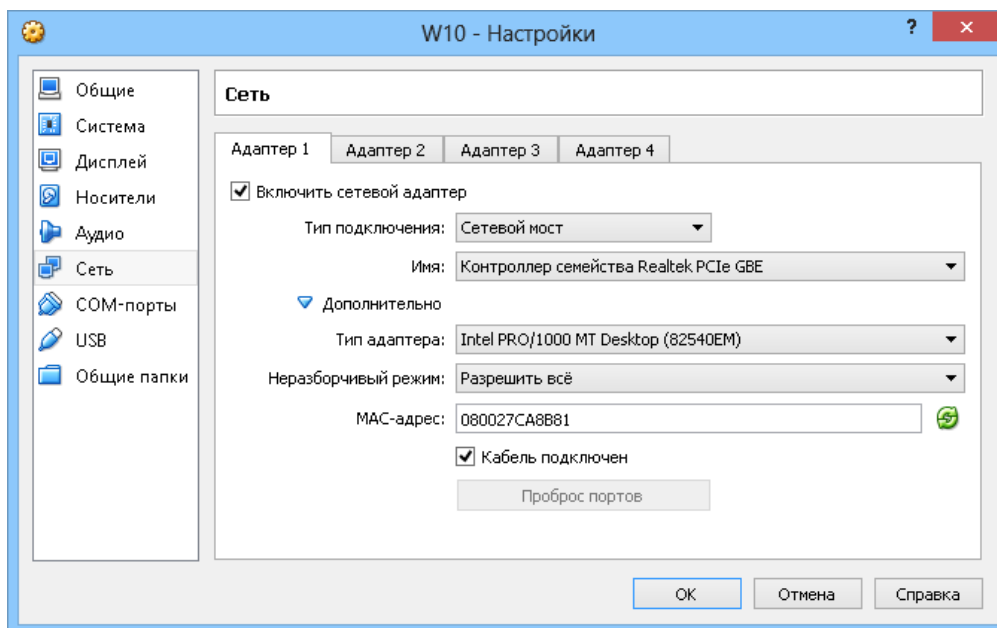
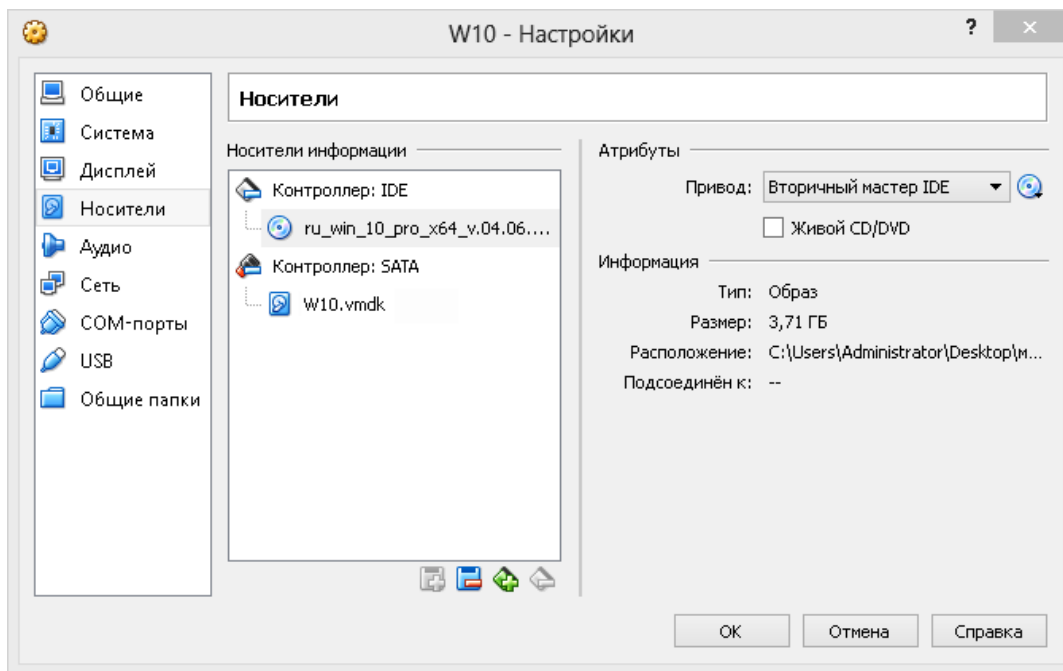


Шаг 1: Создание виртуальной машины Windows 10 в VirtualBox

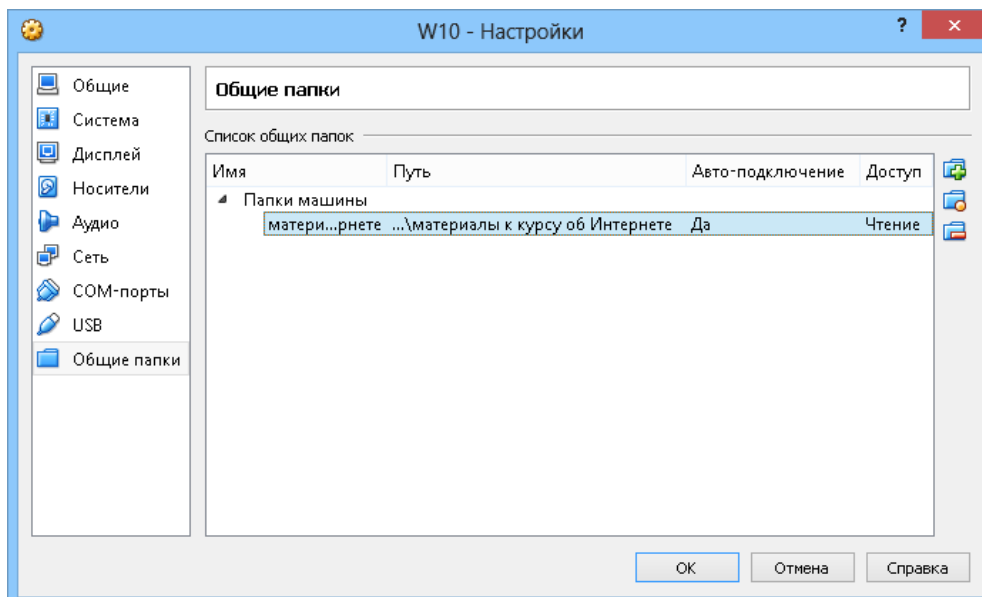
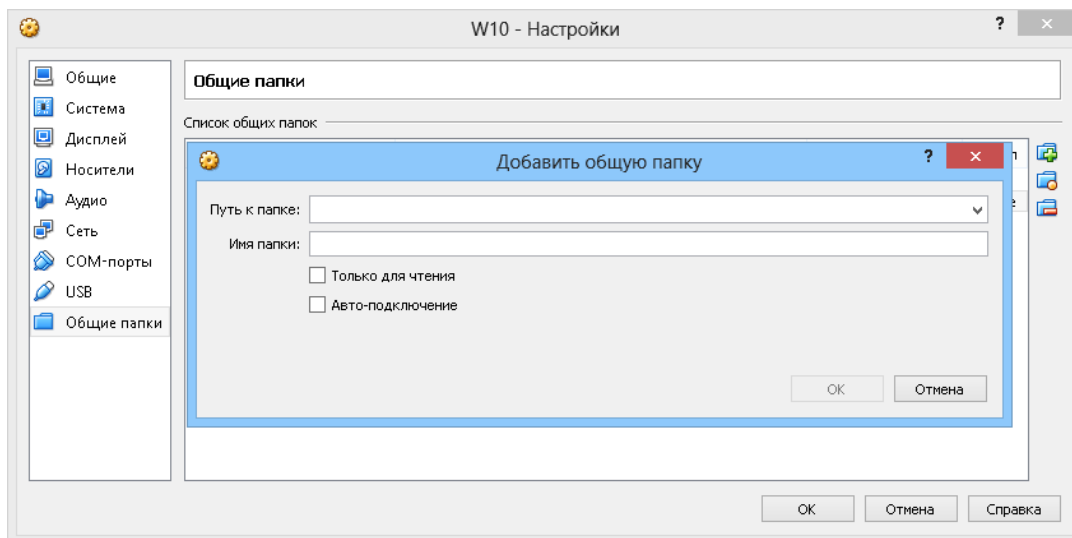
Запускаем среду виртуализации VirtualBox и создаем там виртуальную машину Windows 10 в VirtualBox по следующим характеристикам:





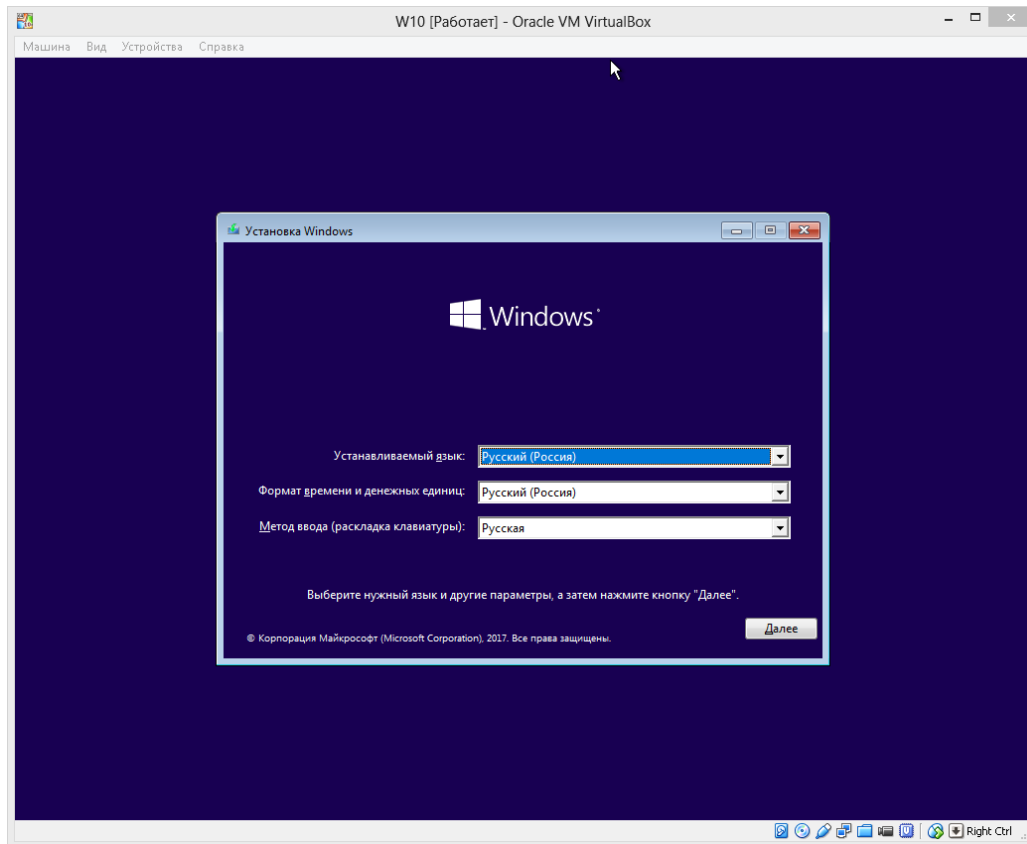


Также добавляем общую папку с рабочего стола реальной машины.

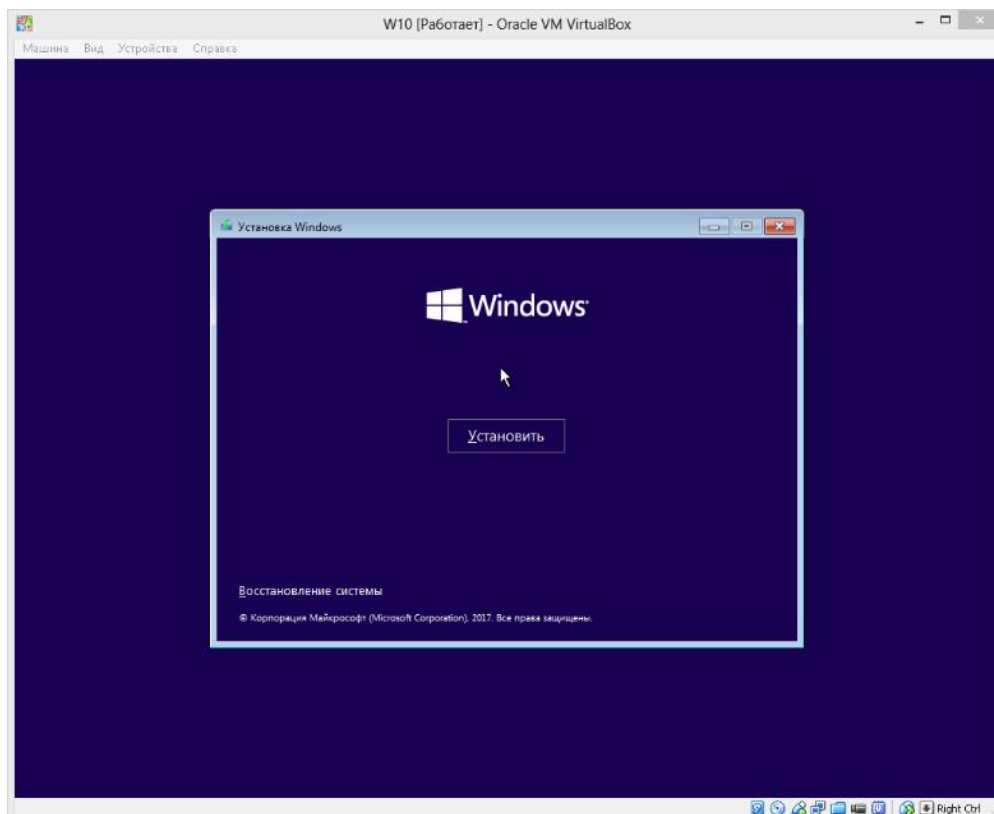


Шаг 2: Установка Windows 10 в VirtualBox

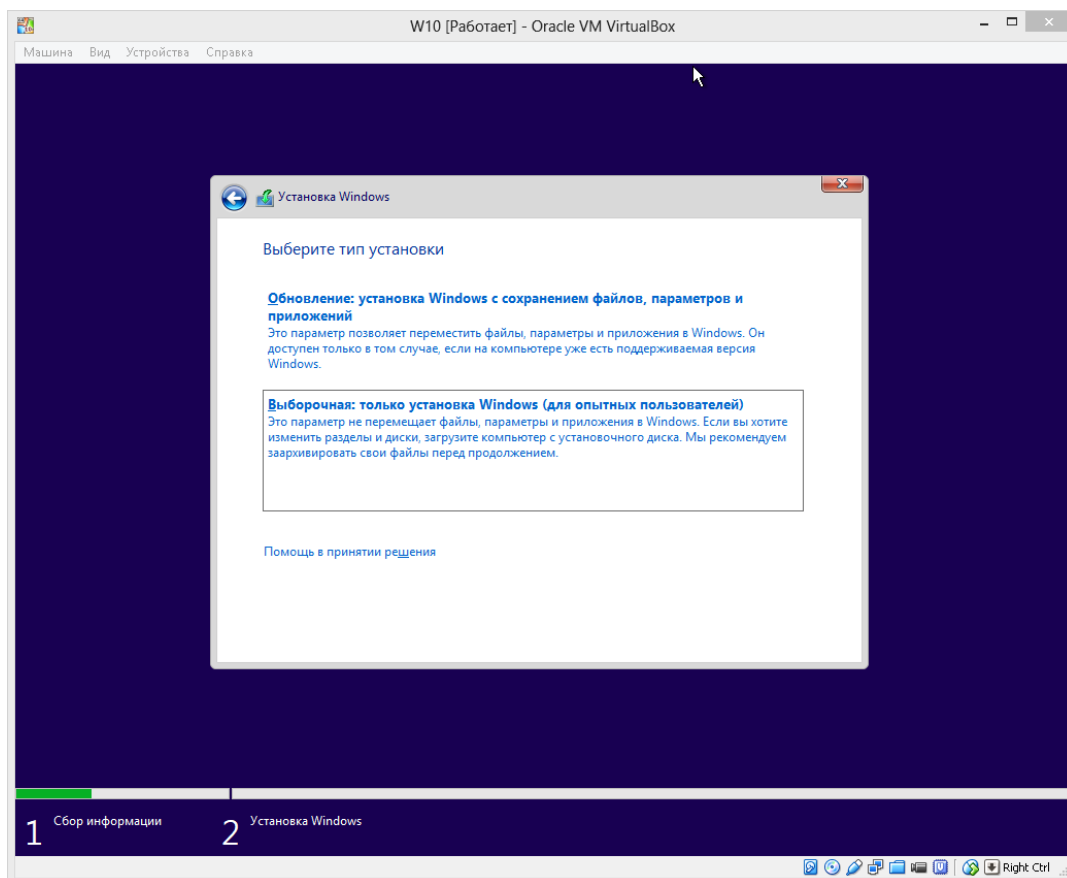
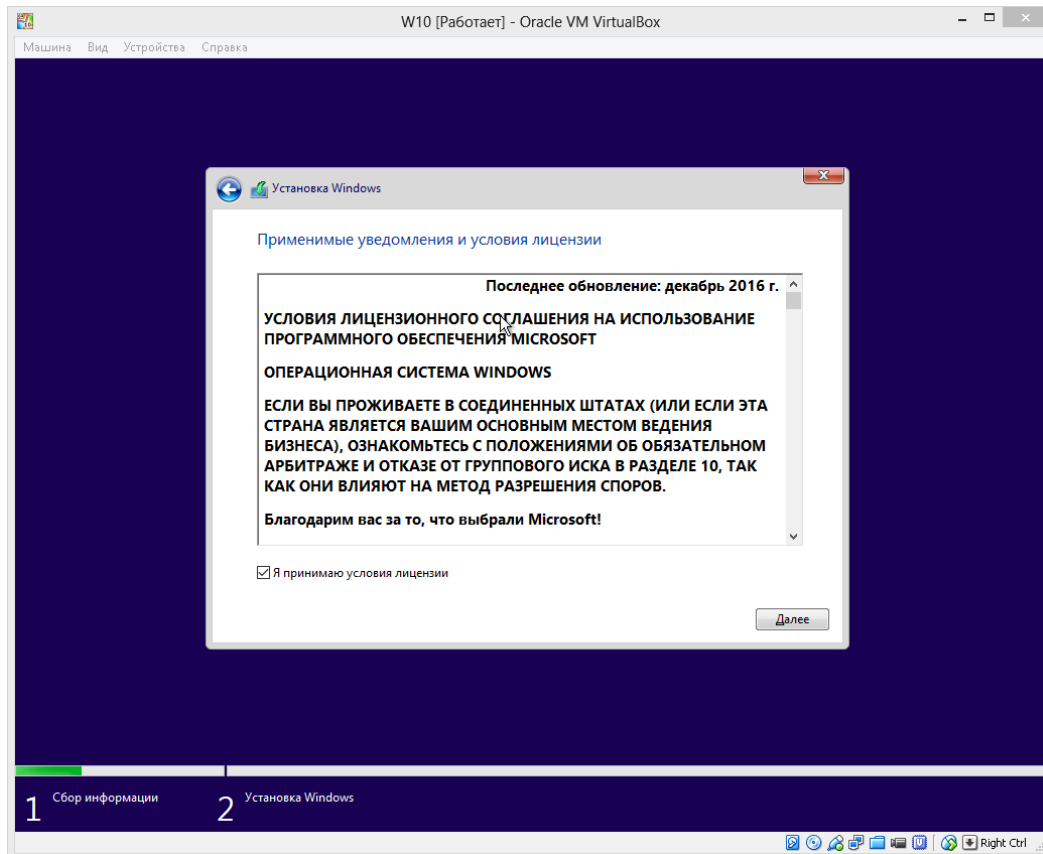
Первым делом установка ОС Windows начинается с выбора языка. Язык в первом появившемся окне оставляем как есть.



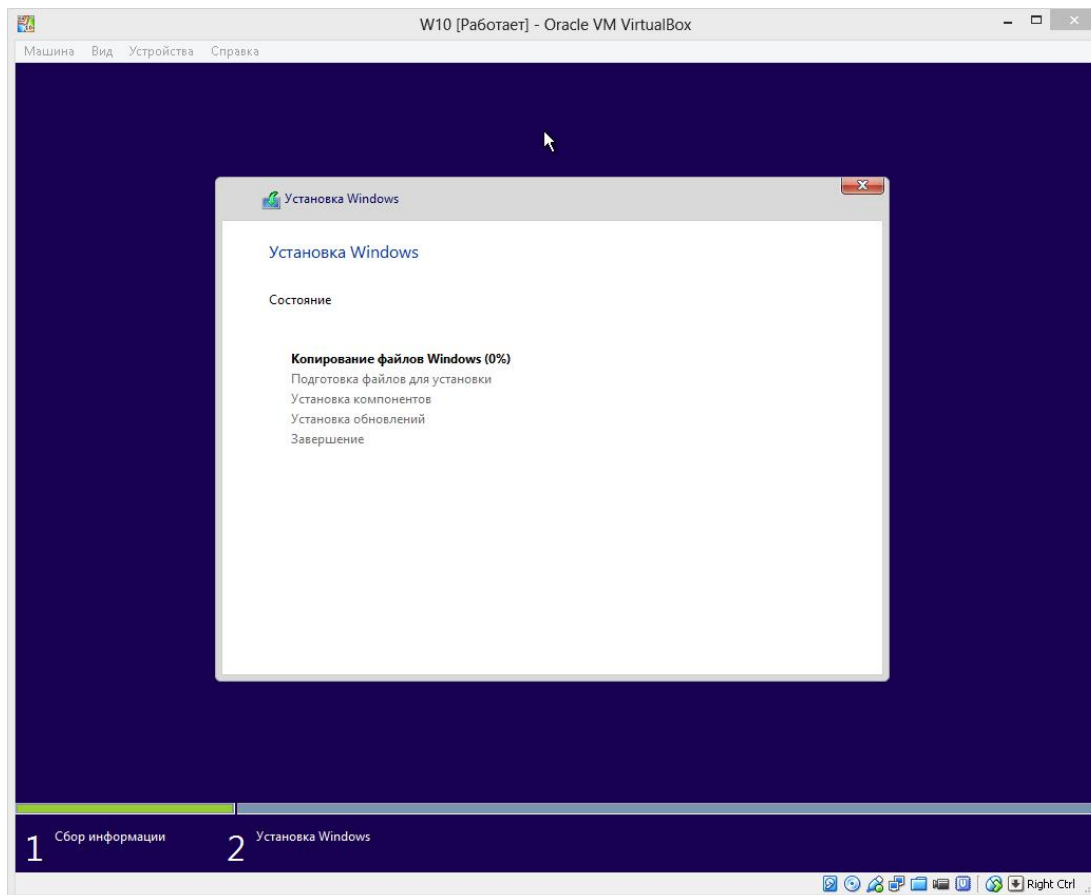
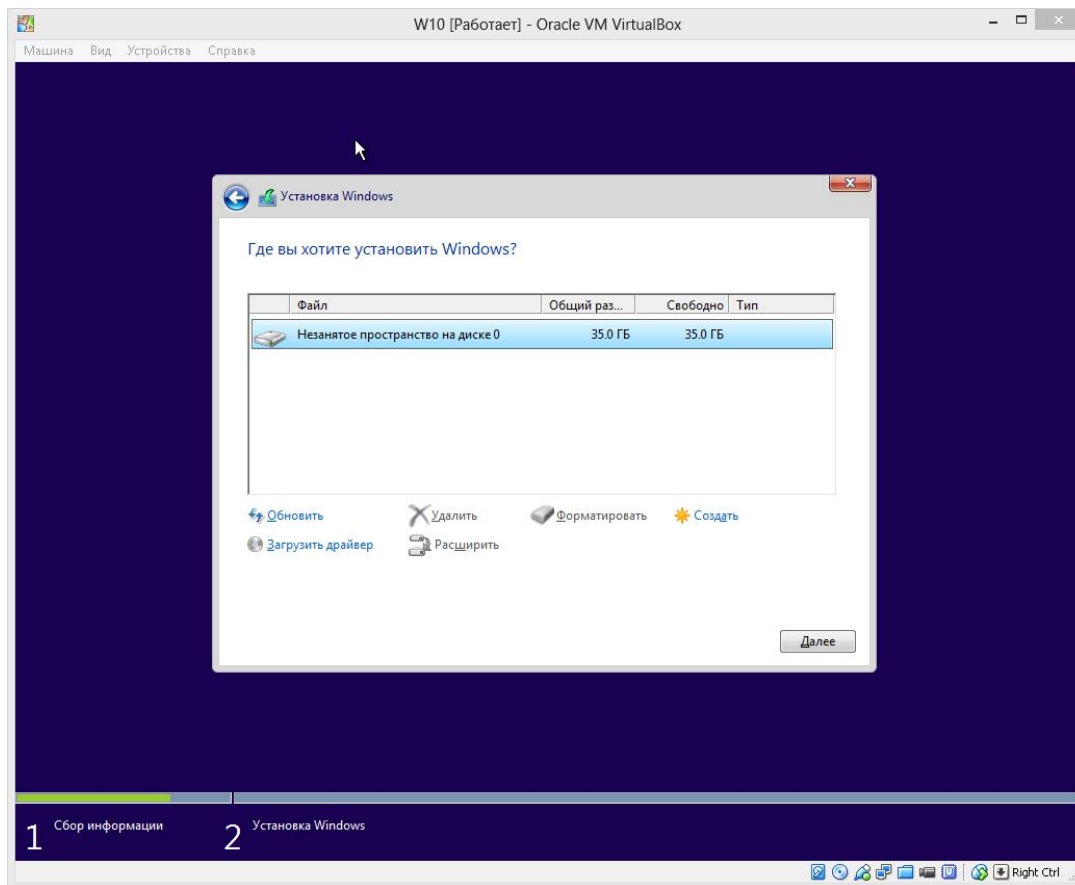
Далее жмем кнопку «Установить».



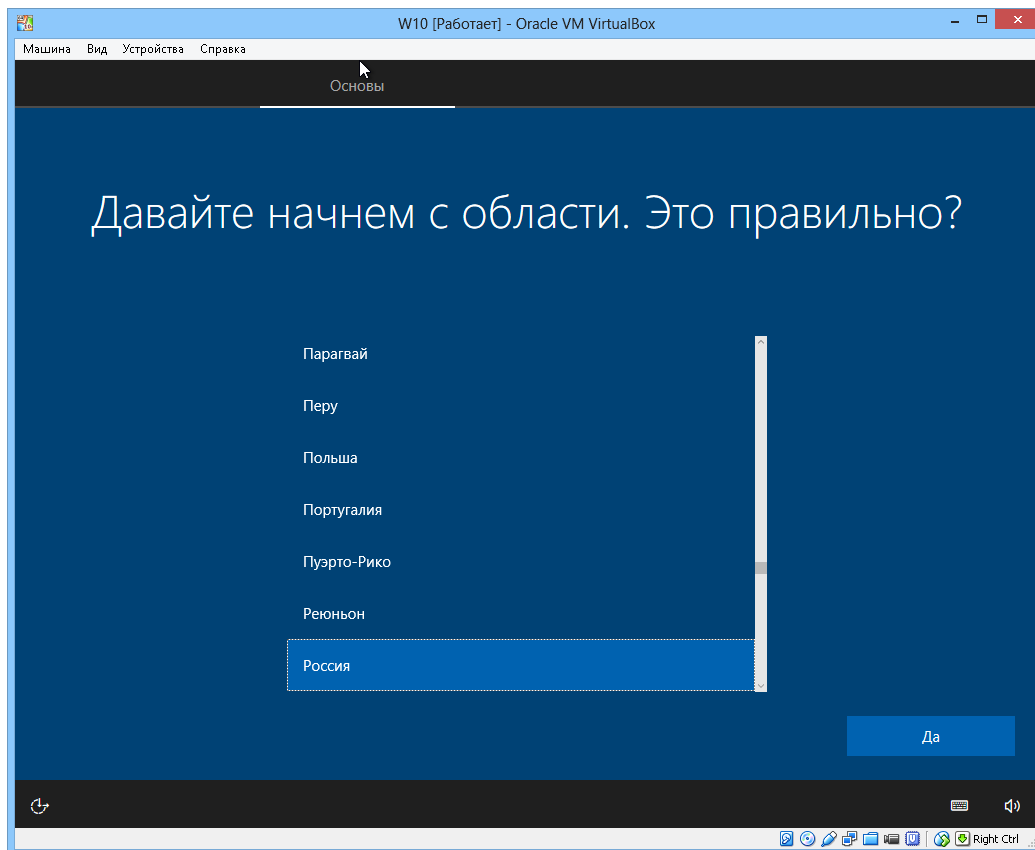
Жмем галочку принятия лицензионного соглашения и далее выбираем выборочную установку.



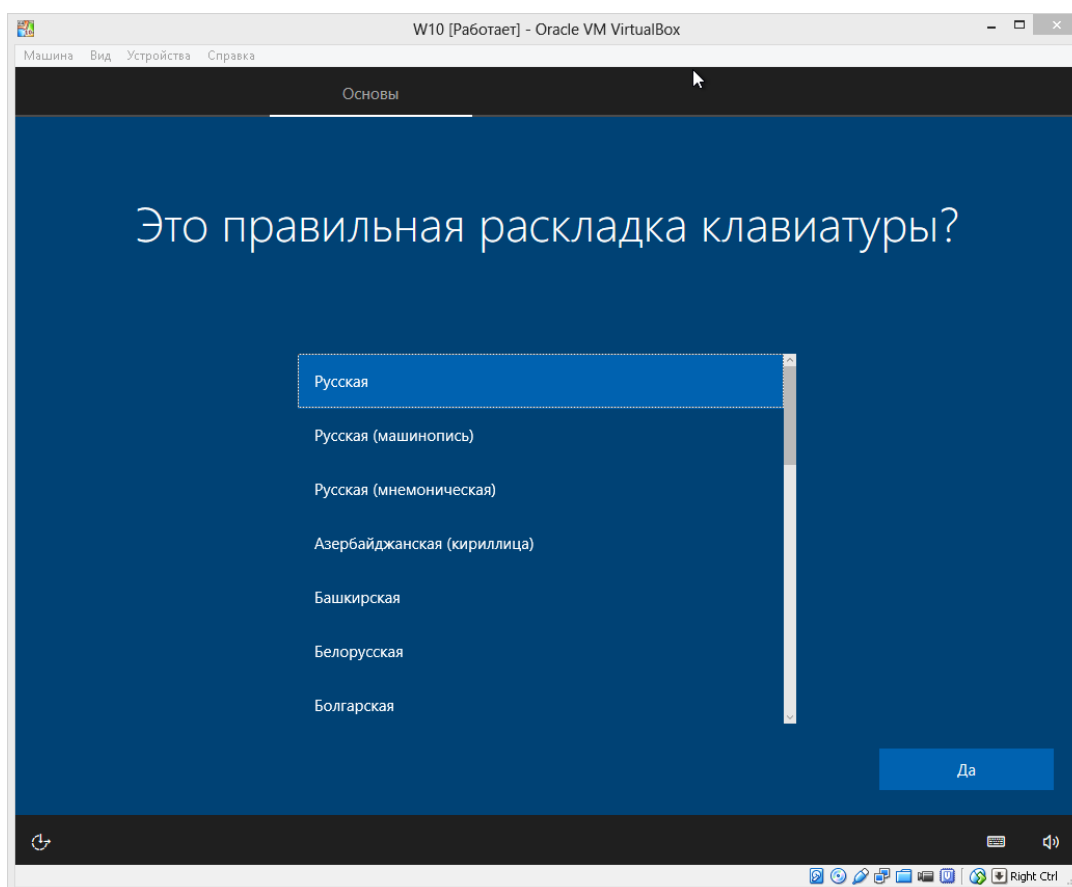
Выбираем незанятое пространство подключенного к машине диска и после подтверждения ждем установки файлов ОС.



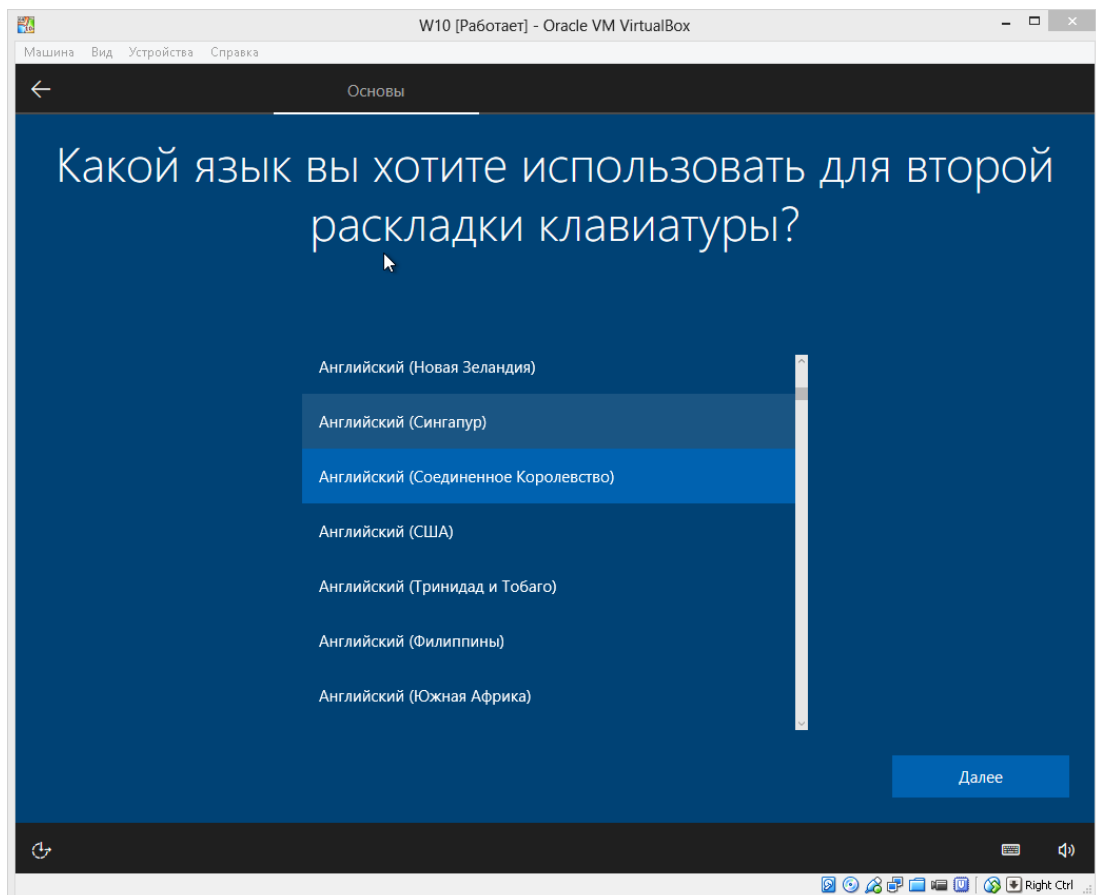
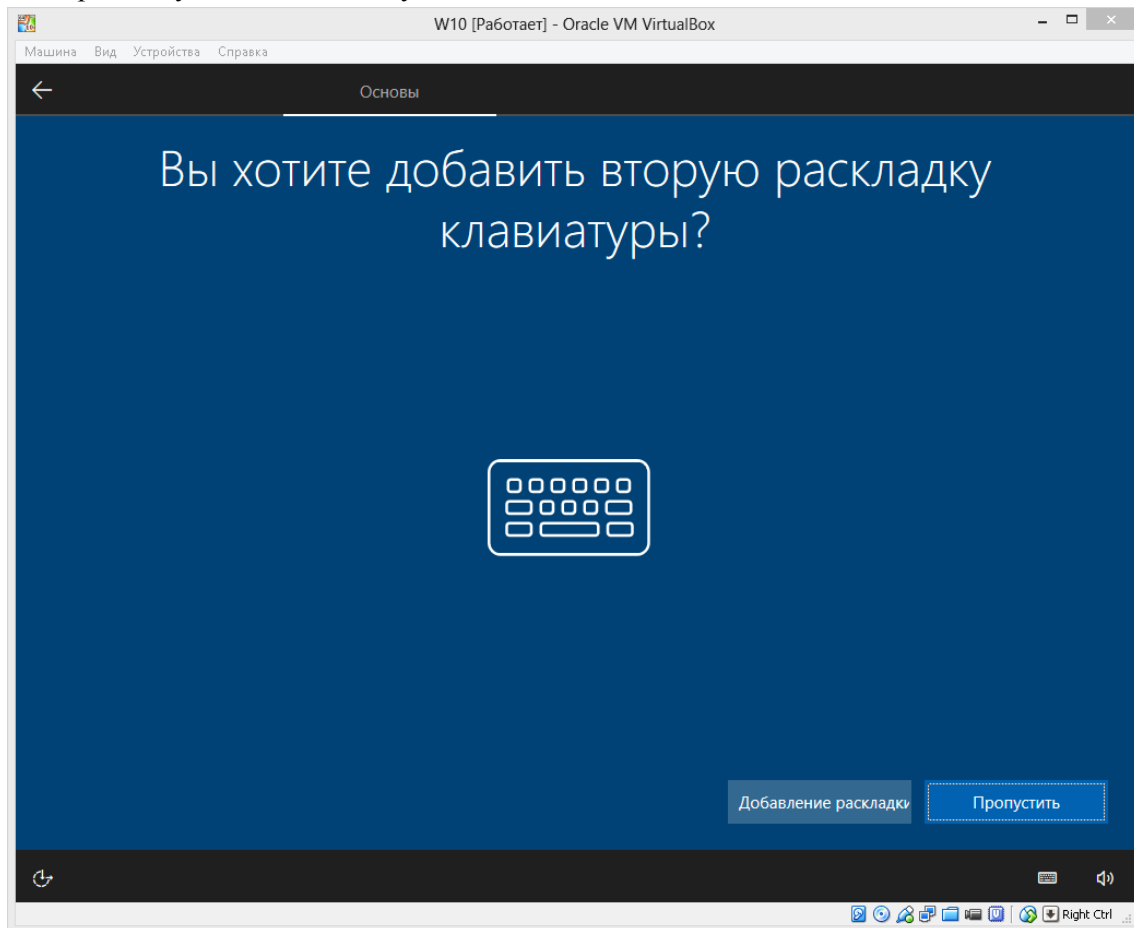
После процедуры установки файлов ОС выбираем регион.

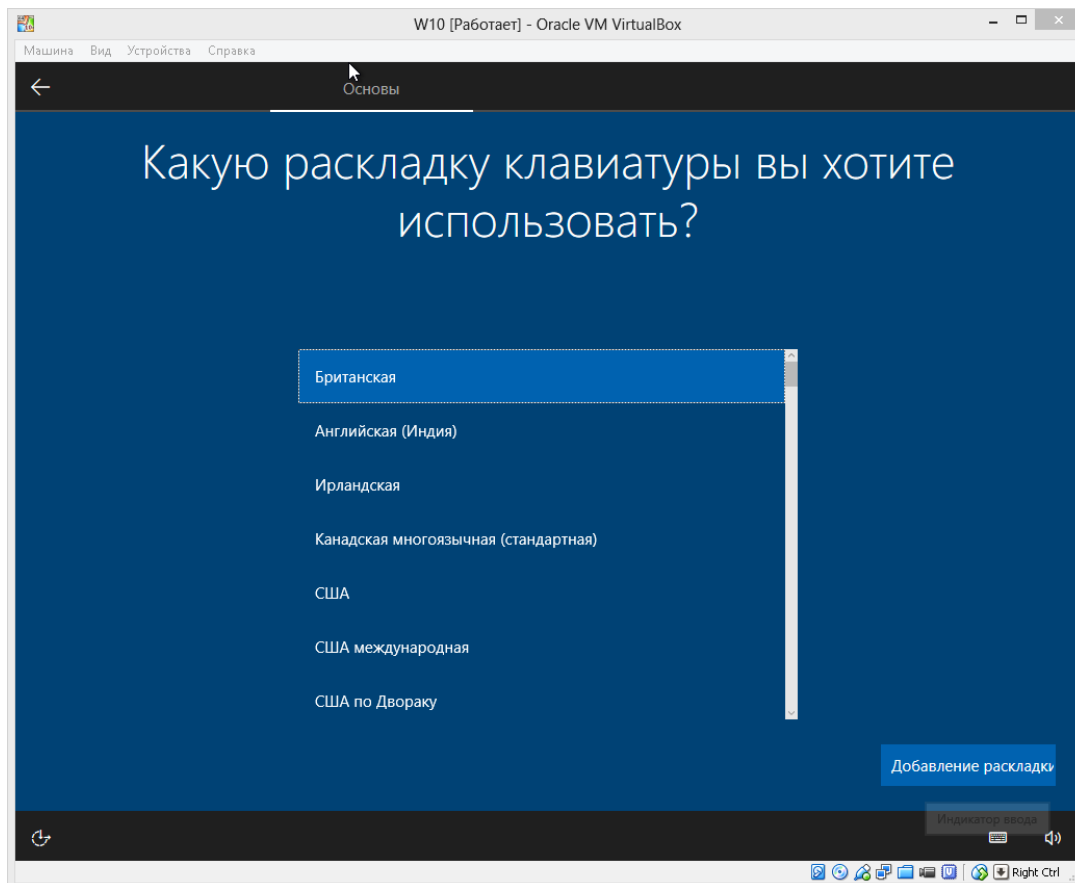


И нам дают возможность выбрать базовую раскладку клавиатуры.

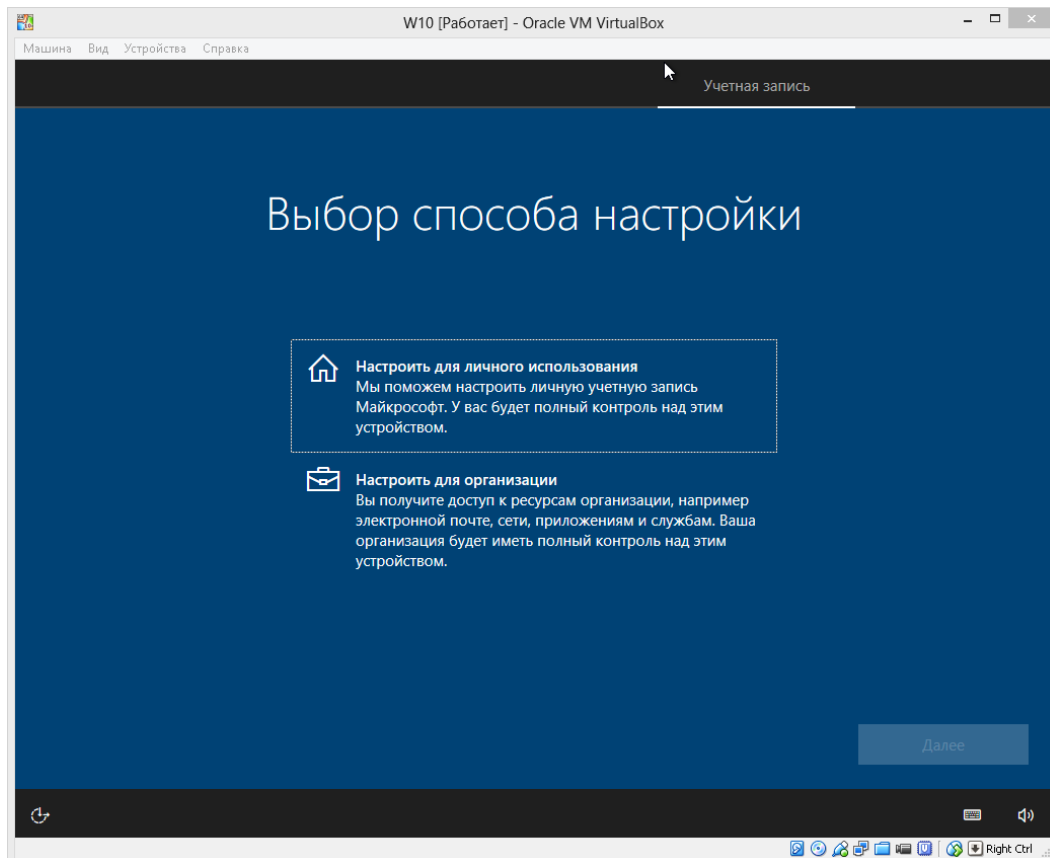


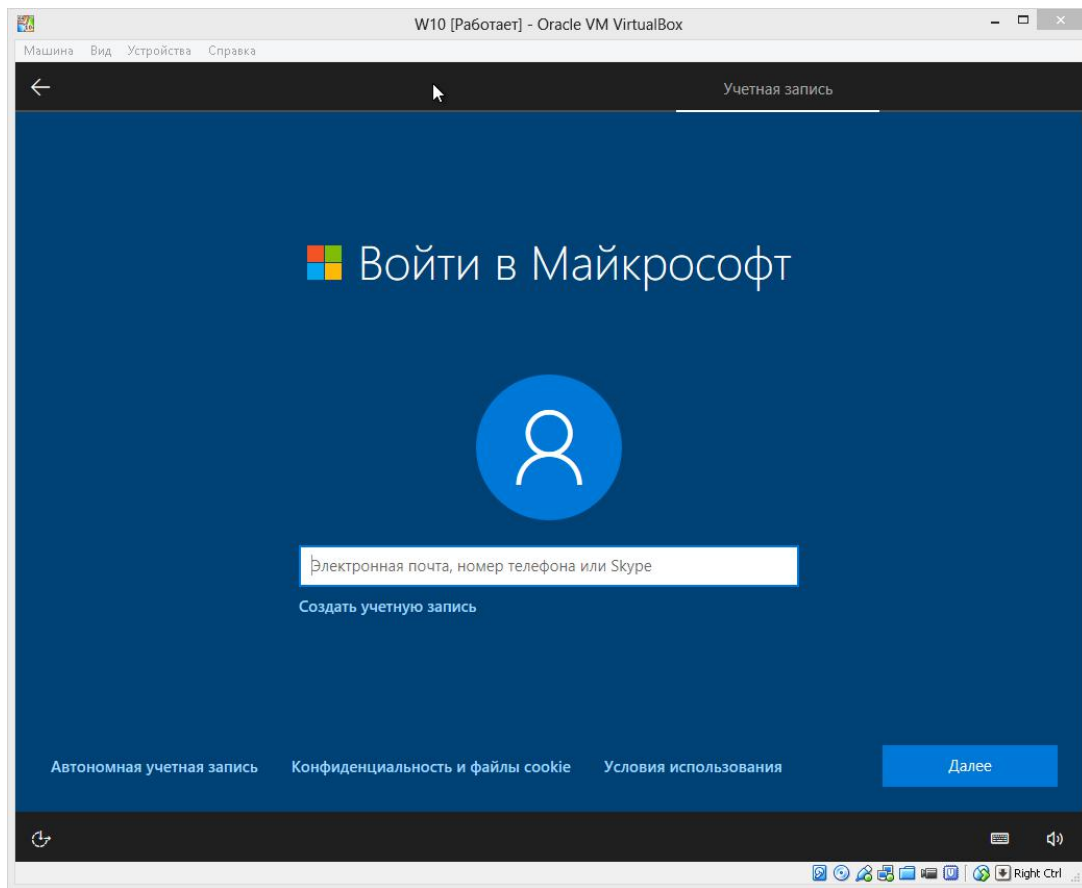
Выбираем «Русский» как базовую и в качестве дополнительной «Английский».



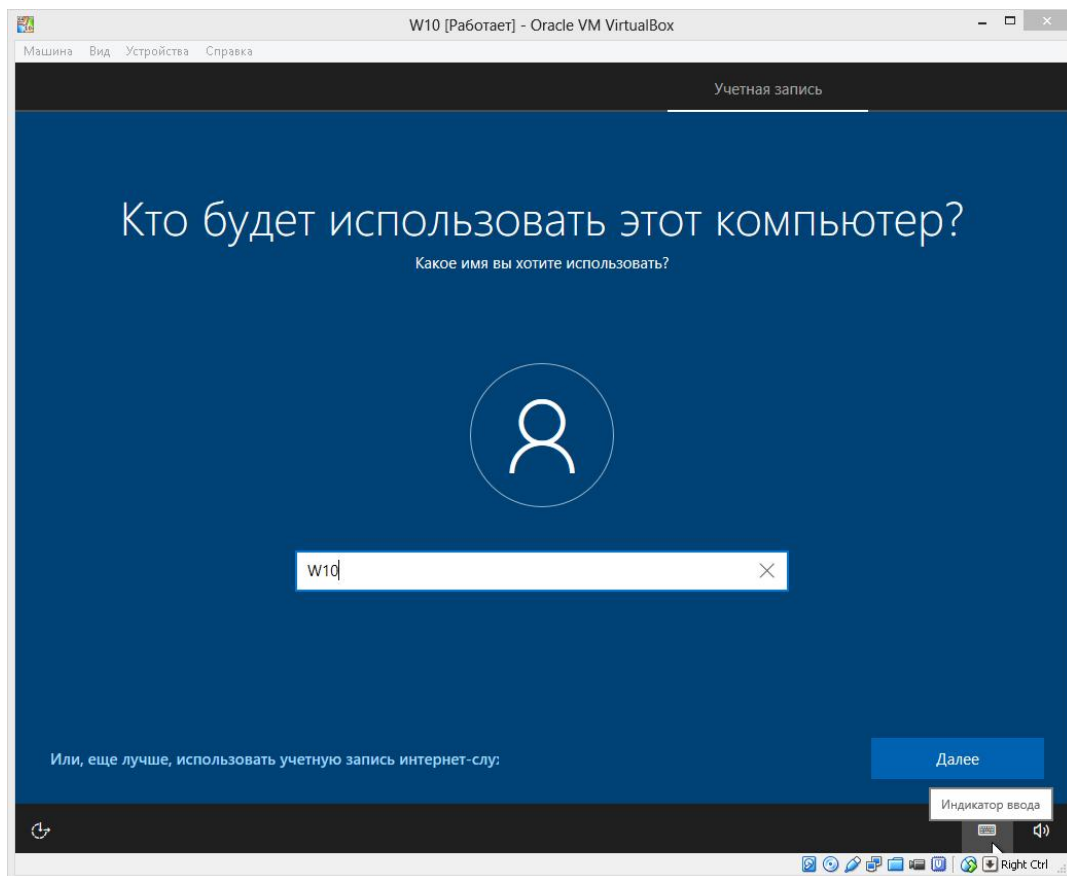


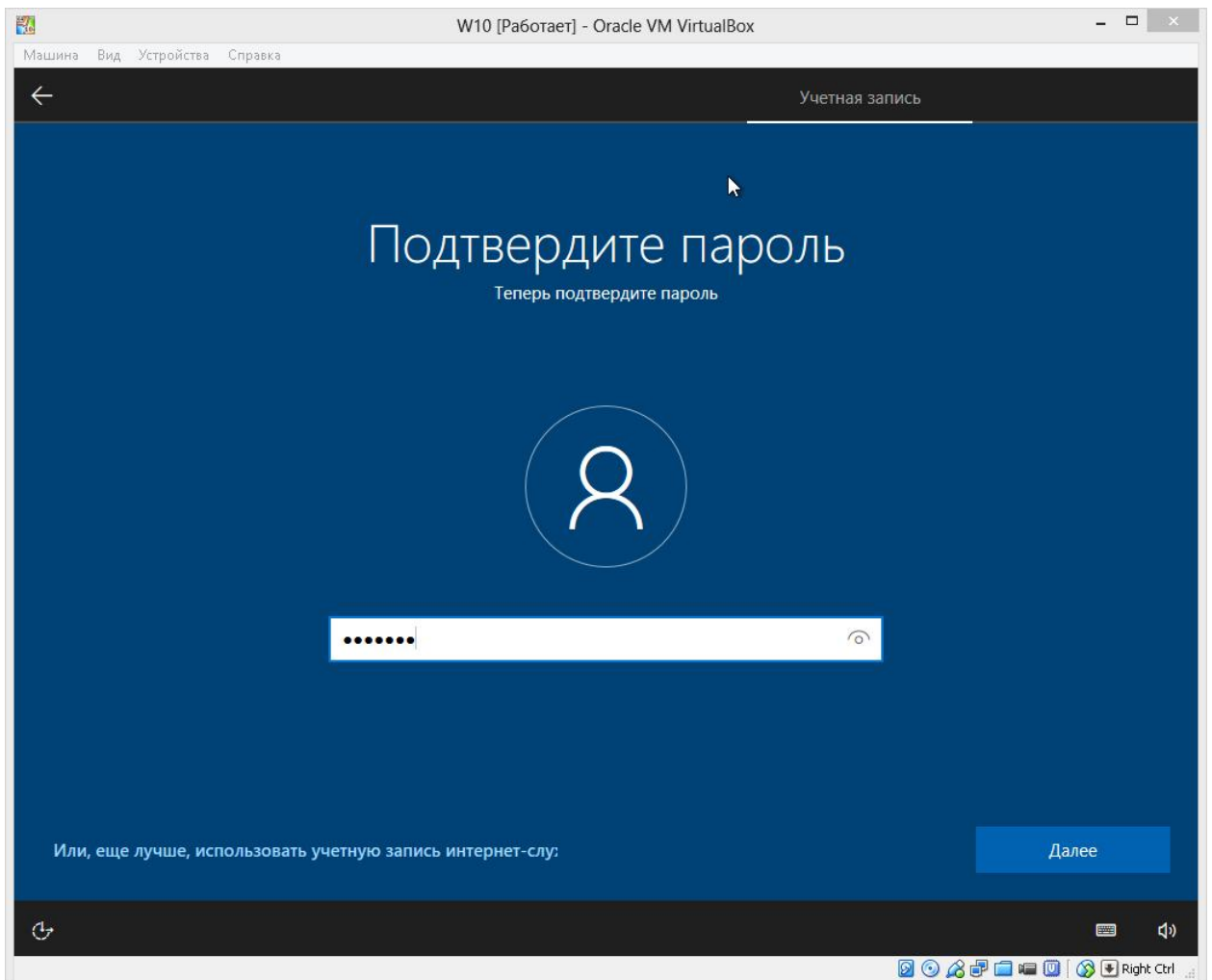
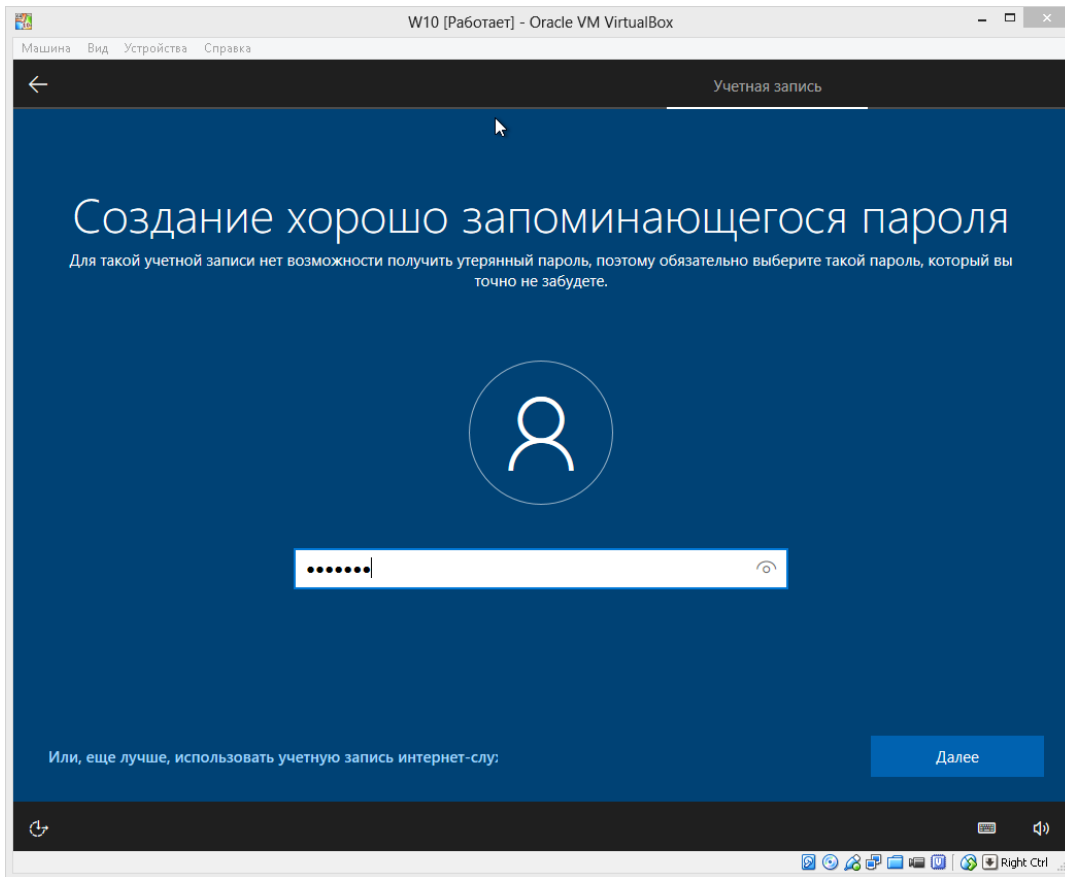
Способ настройки берем «личный» с выбором автономной учетной записи.



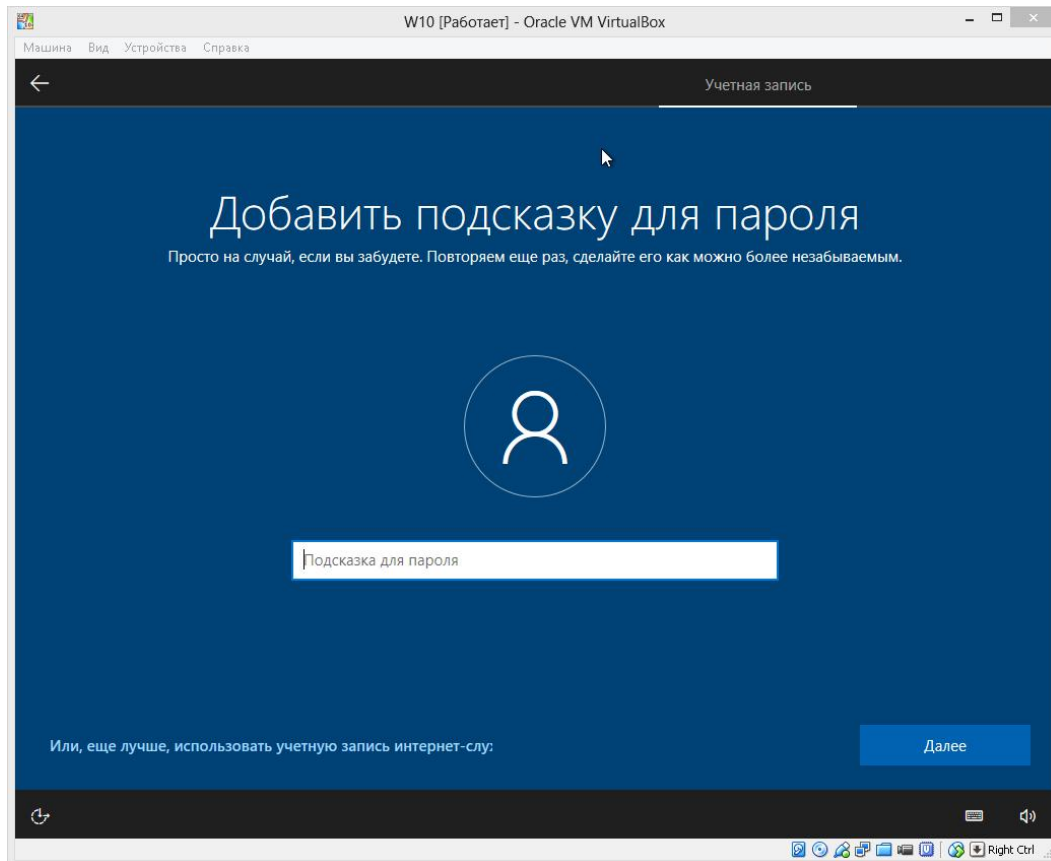


Далее задаем имя компьютера и запоминающийся пароль входа в ОС.

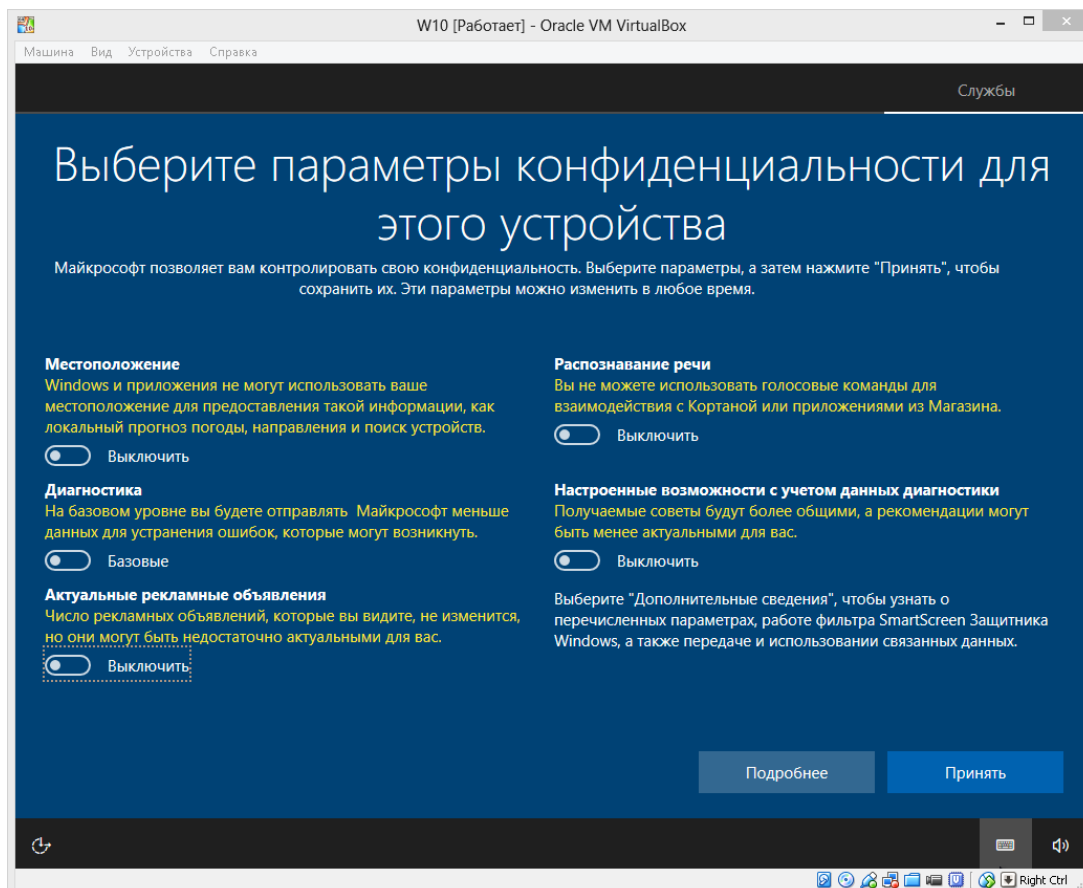




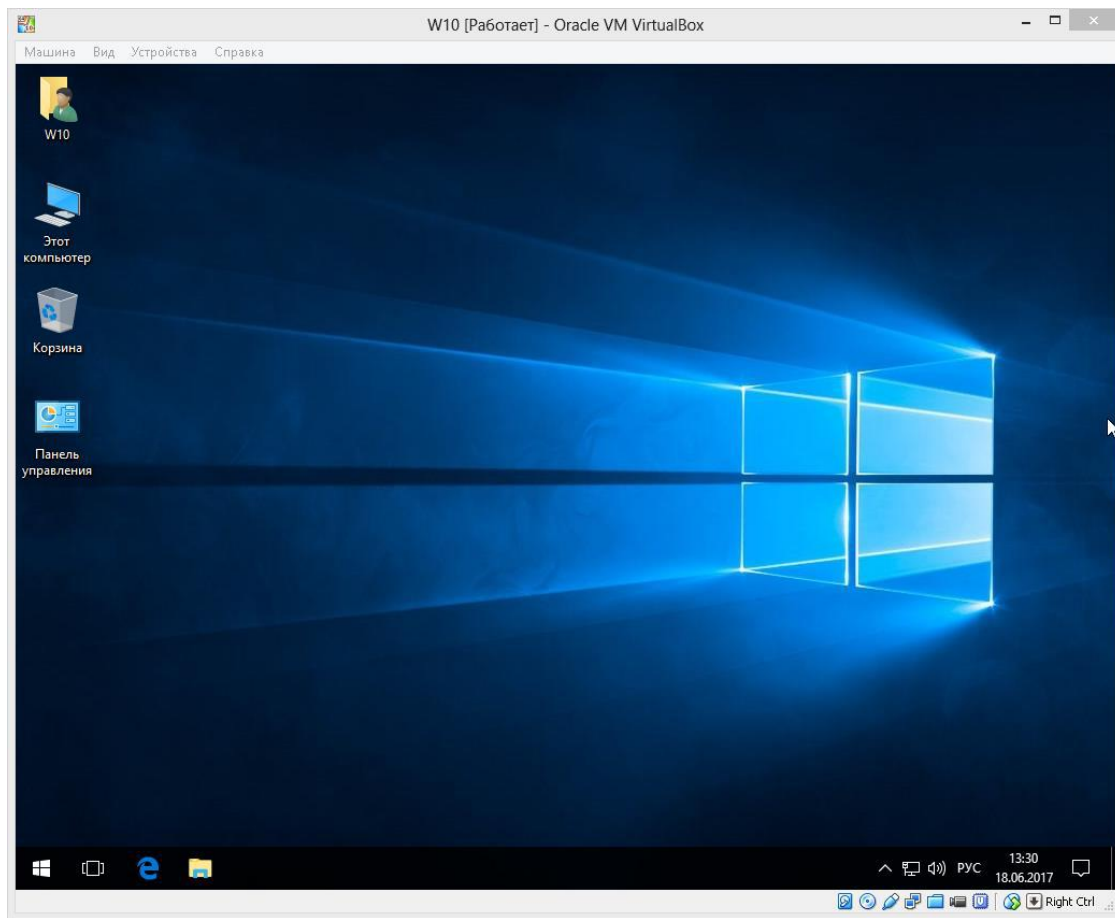
На всякий случай даем подсказку для того, чтобы вспомнить пароль.



Ставим параметры конфиденциальности Windows 10 такими и принимаем их.

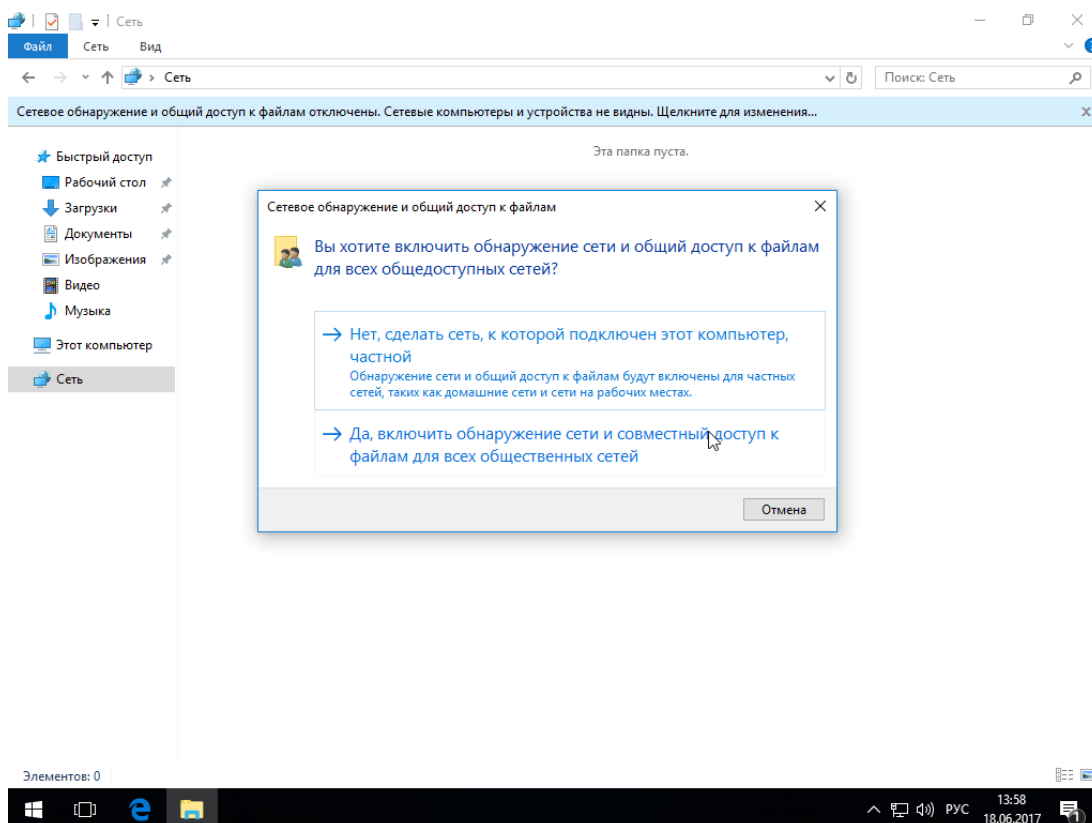
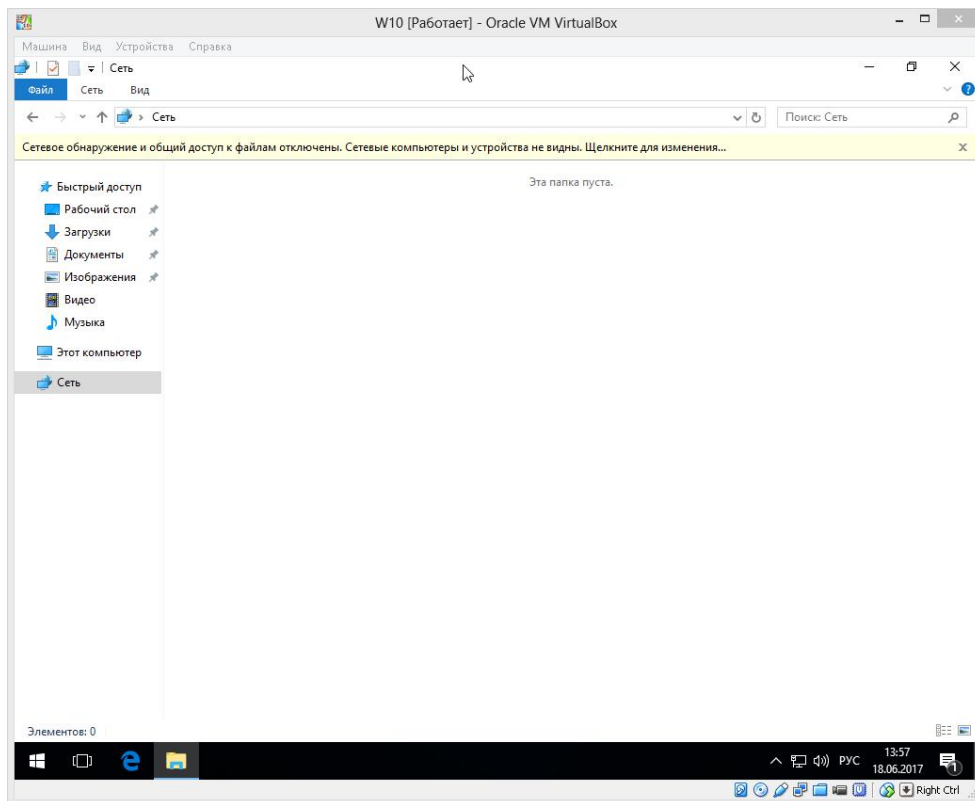


После этого ОС запускается, предварительно обрабатывая выбор пользовательских настроек.

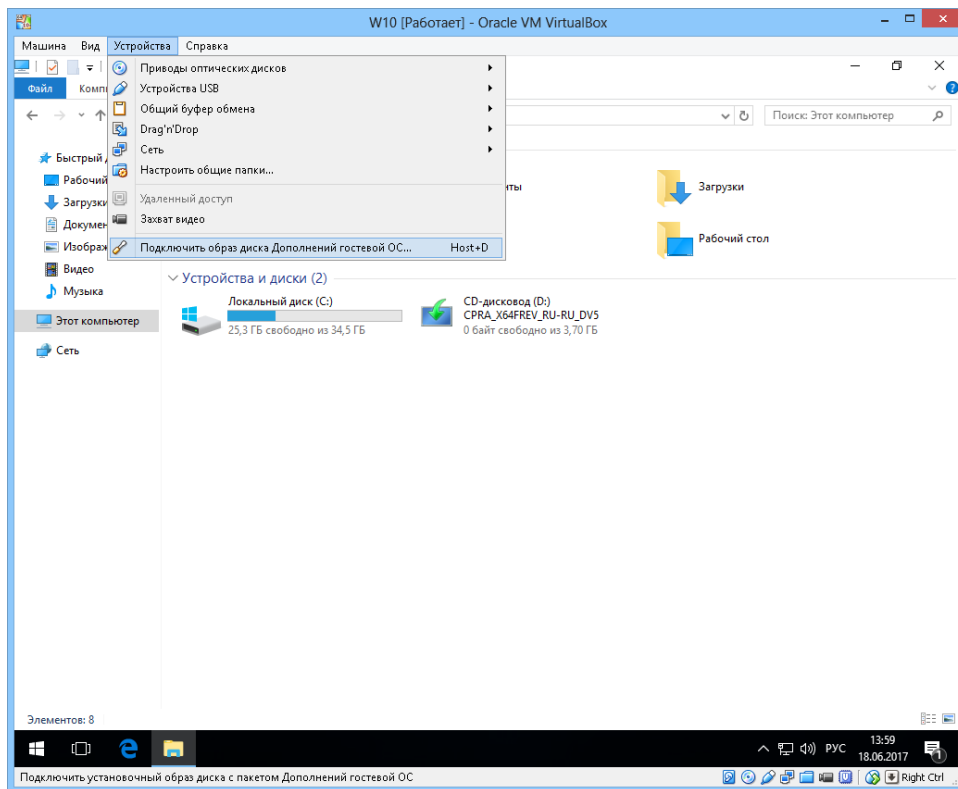


Шаг 3: Настройка сетевого соединения и установка папки общего доступа

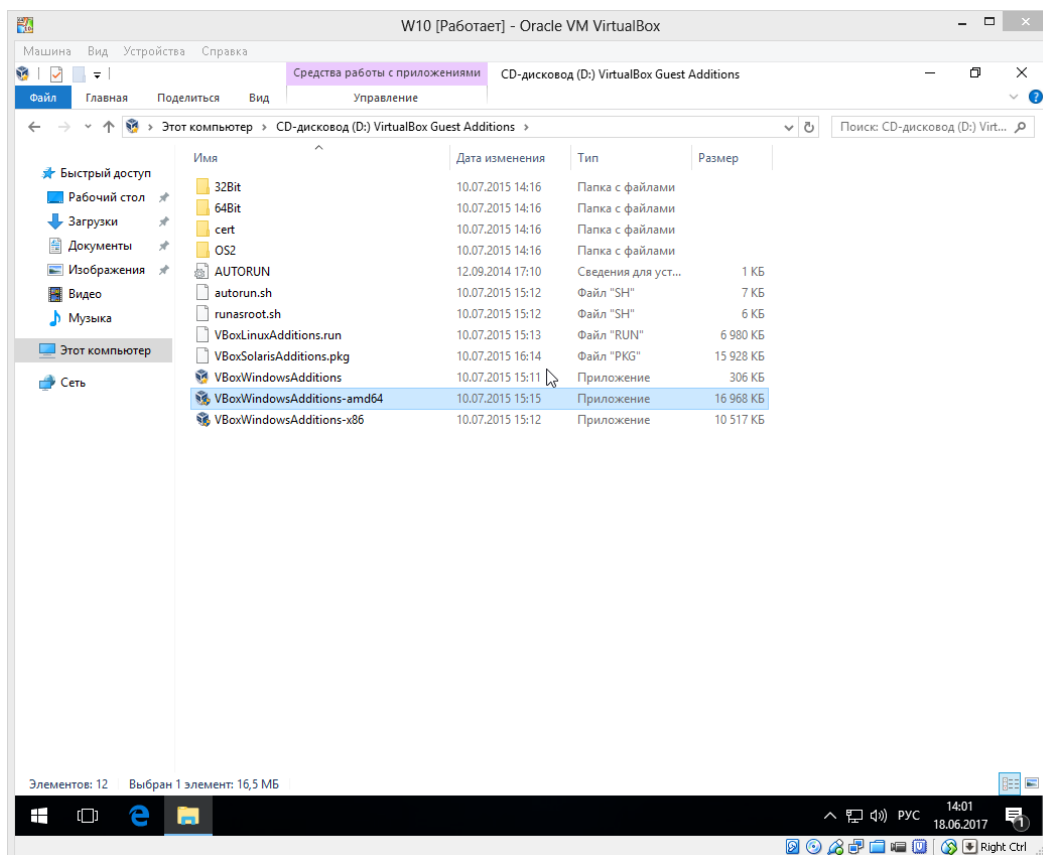
Заходим в «Проводник» и с левой стороны заходим в «Сеть», где расположены сетевые папки компьютера. Включаем обнаружение сети, щелкнув на всплывающую панель сообщения сверху.



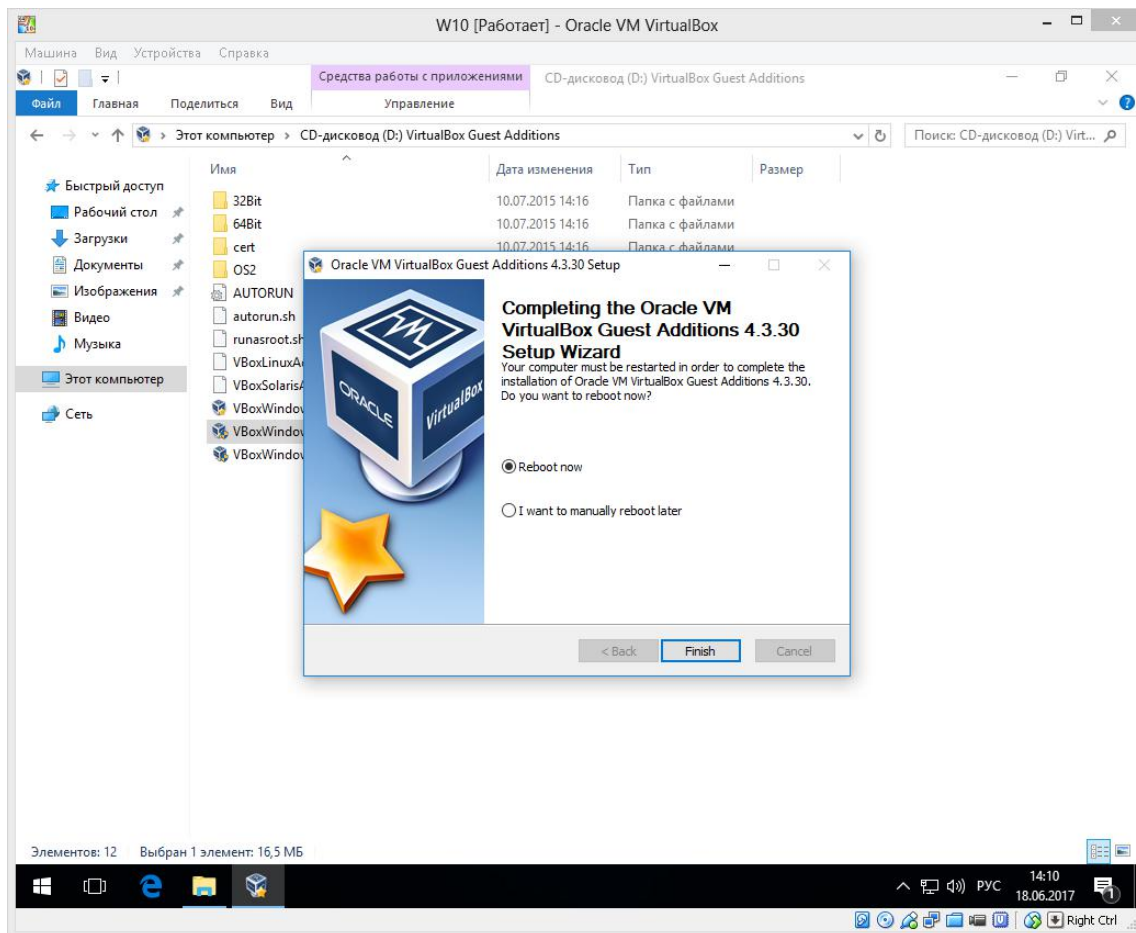
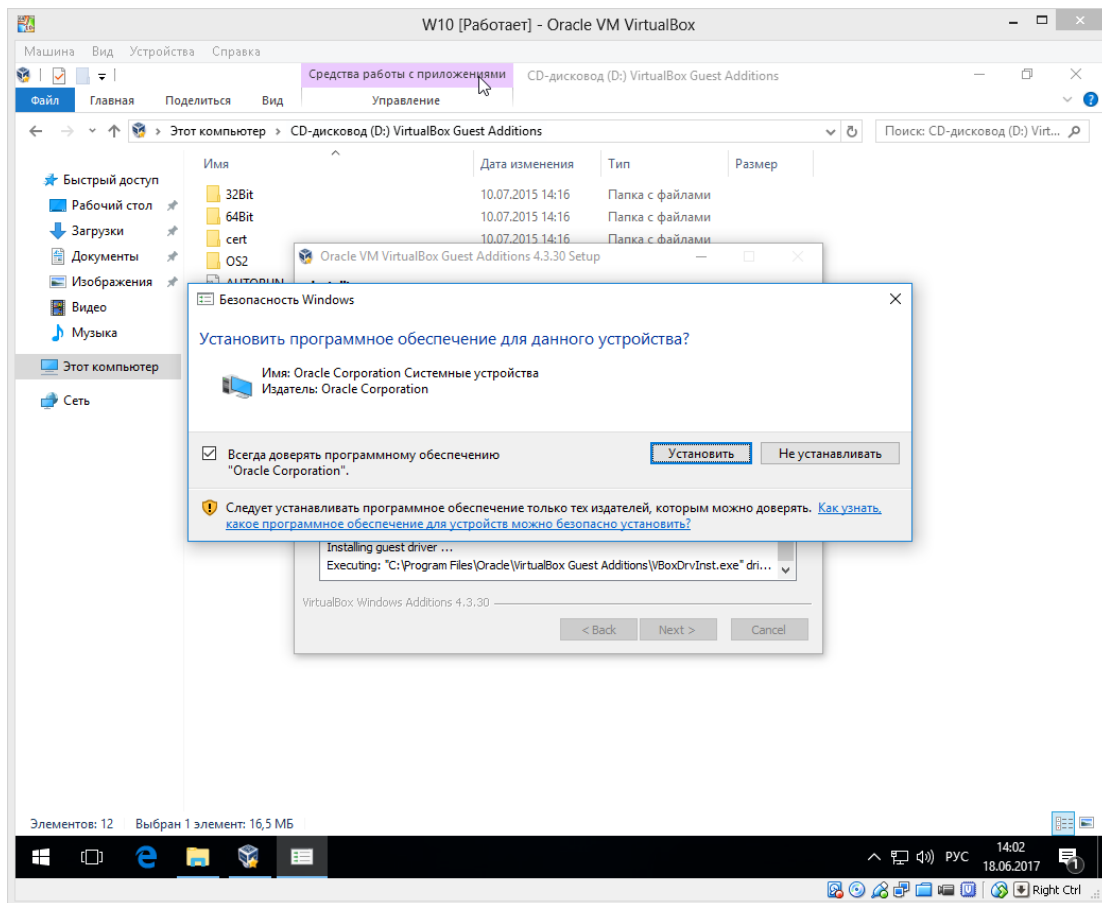
Далее монтируем образ диска дополнений гостевой ОС, чтобы установить общий доступ к папке из параметров виртуальной машины с помощью пункта меню «Устройства» «Подключить образ диска...».



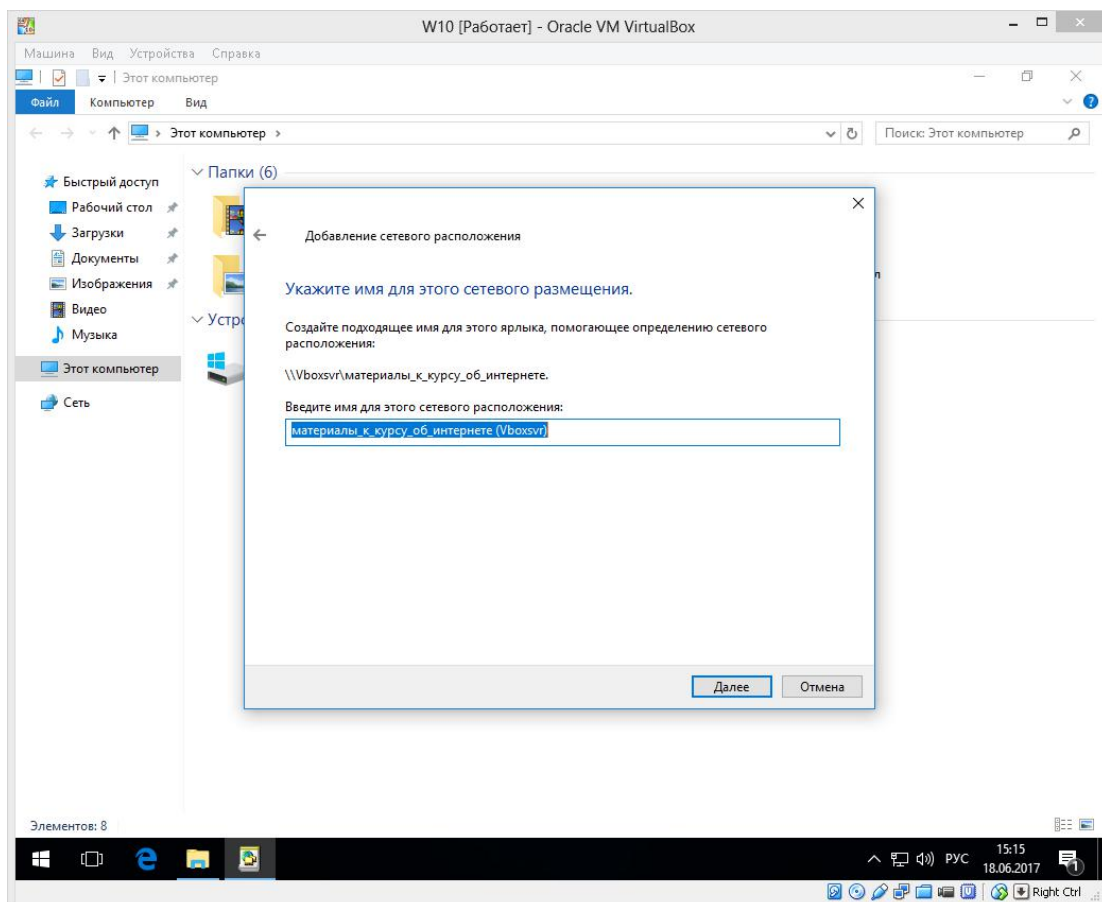
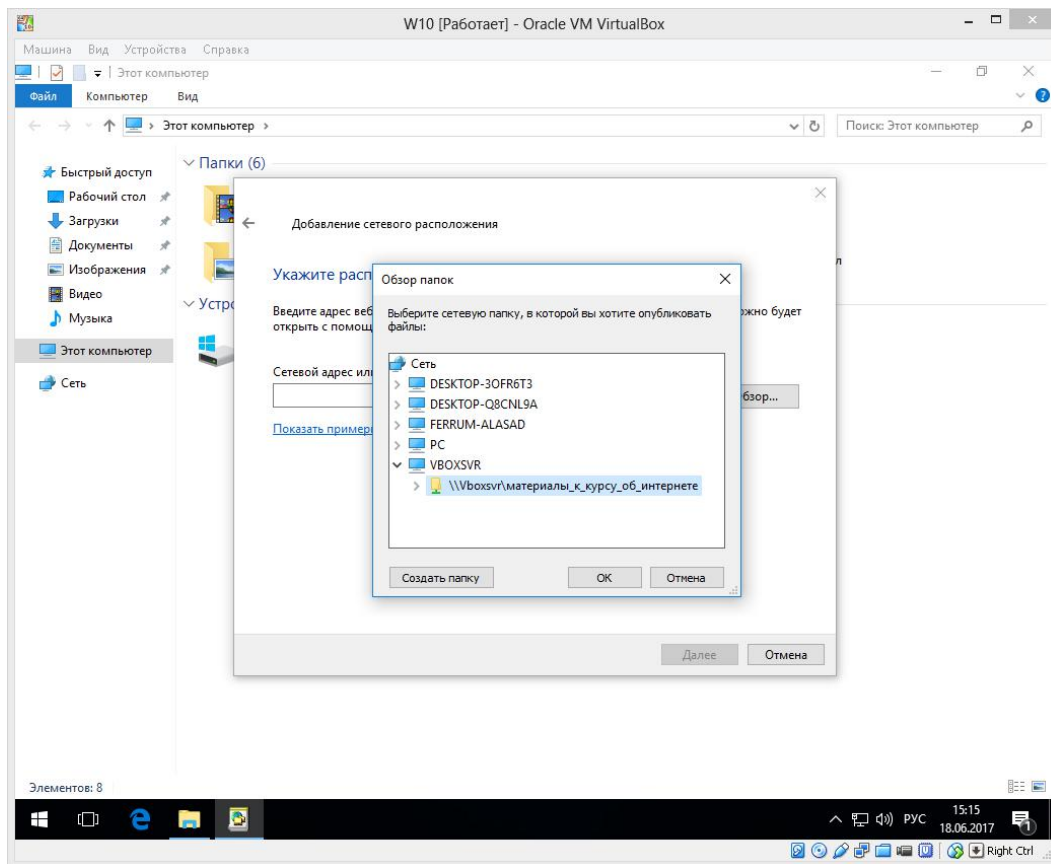
Открываем содержимое диска и запускаем исполняемый файл «VBoxWindowsAdditions-amd64».

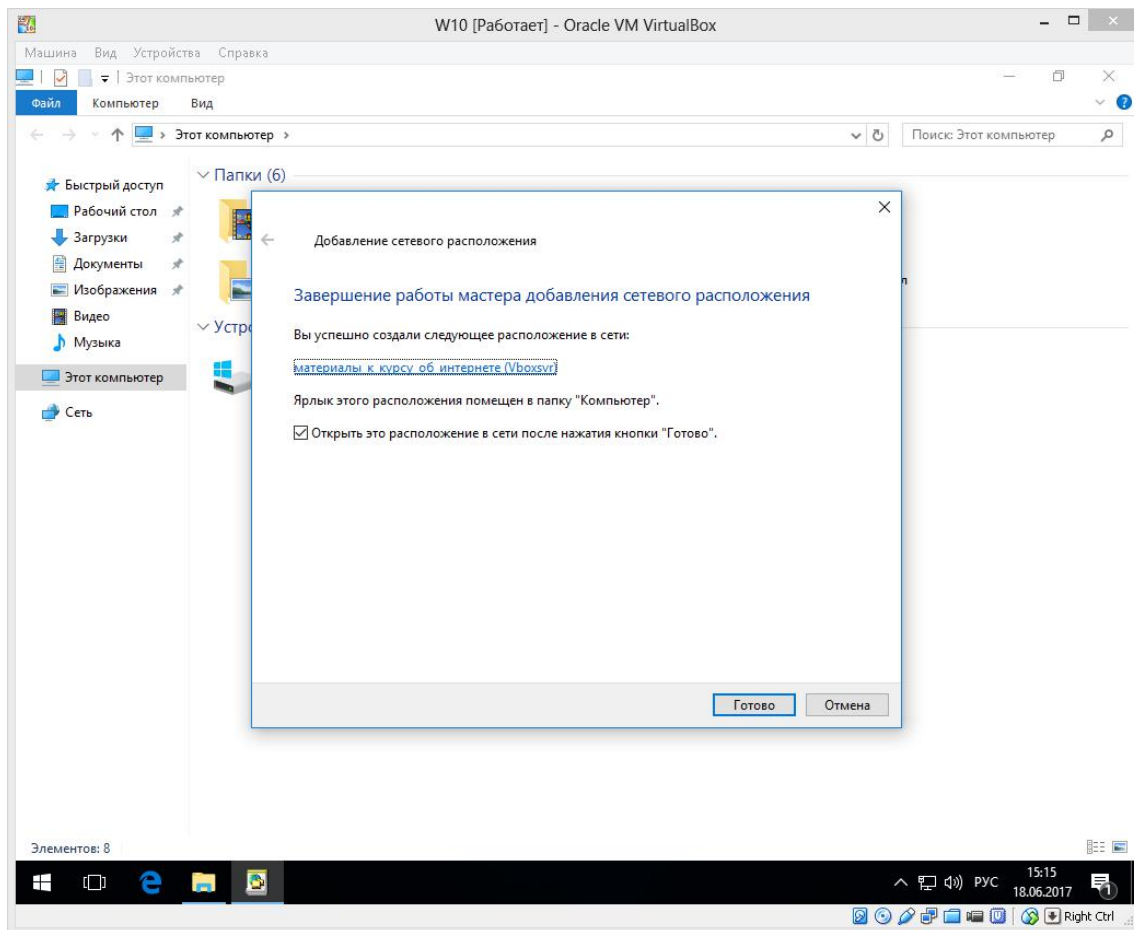


Устанавливаем дополнение к ОС и перезагружаем её.



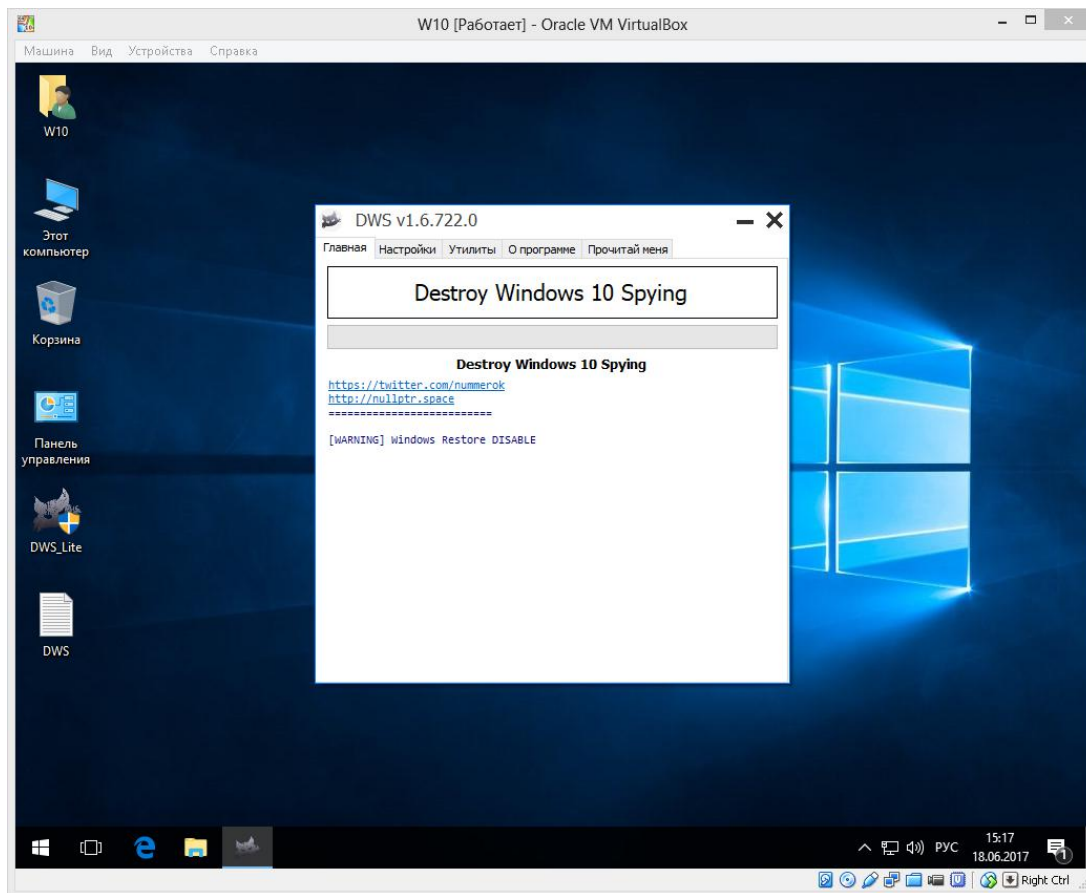
После перезапуска заходим в ОС, кликаем правым кликом на белый фон окна «Этот компьютер» и выбираем пункт «Добавить новый элемент в сетевое окружение...», после чего ищем в обзоре сетевых папок VBOXSVR и добавляем нашу сетевую папку.

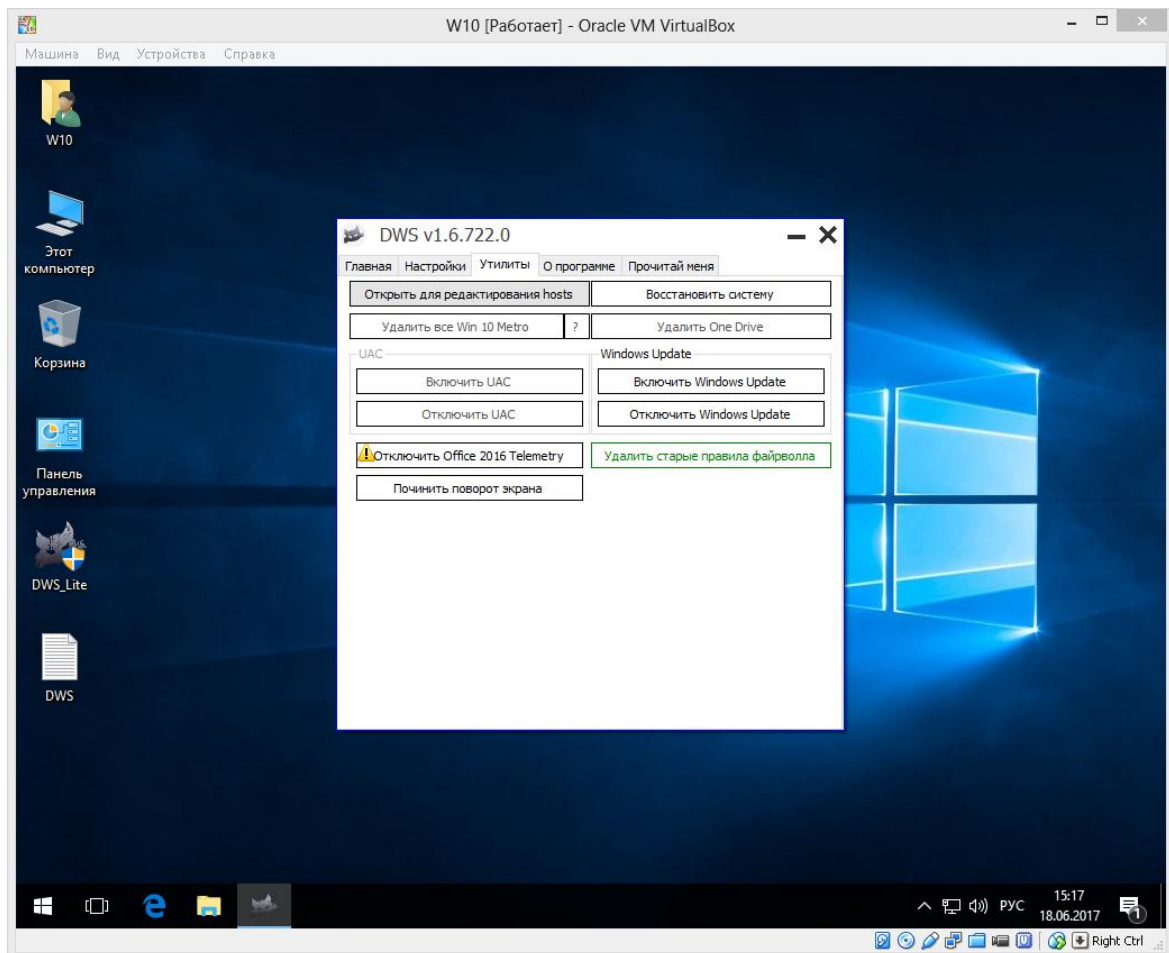
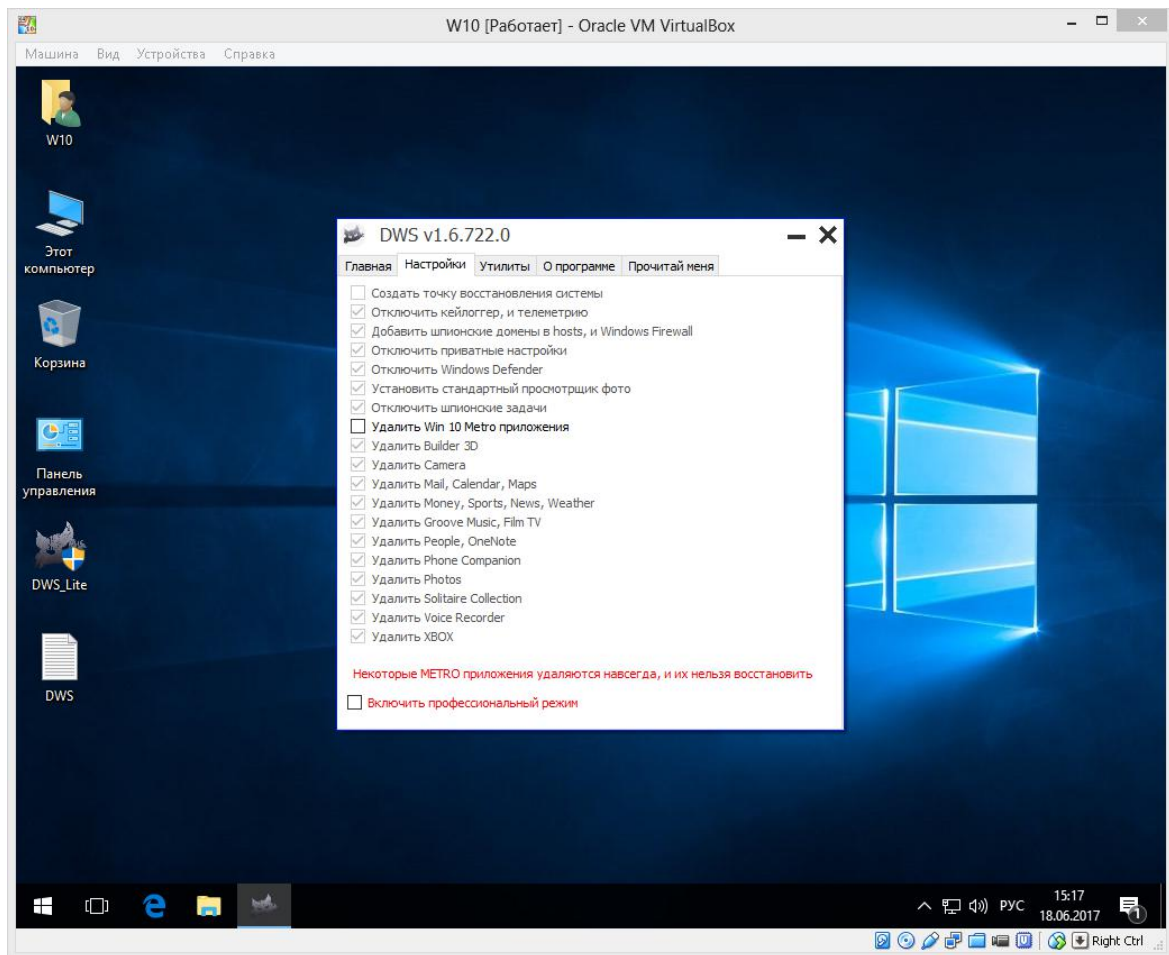


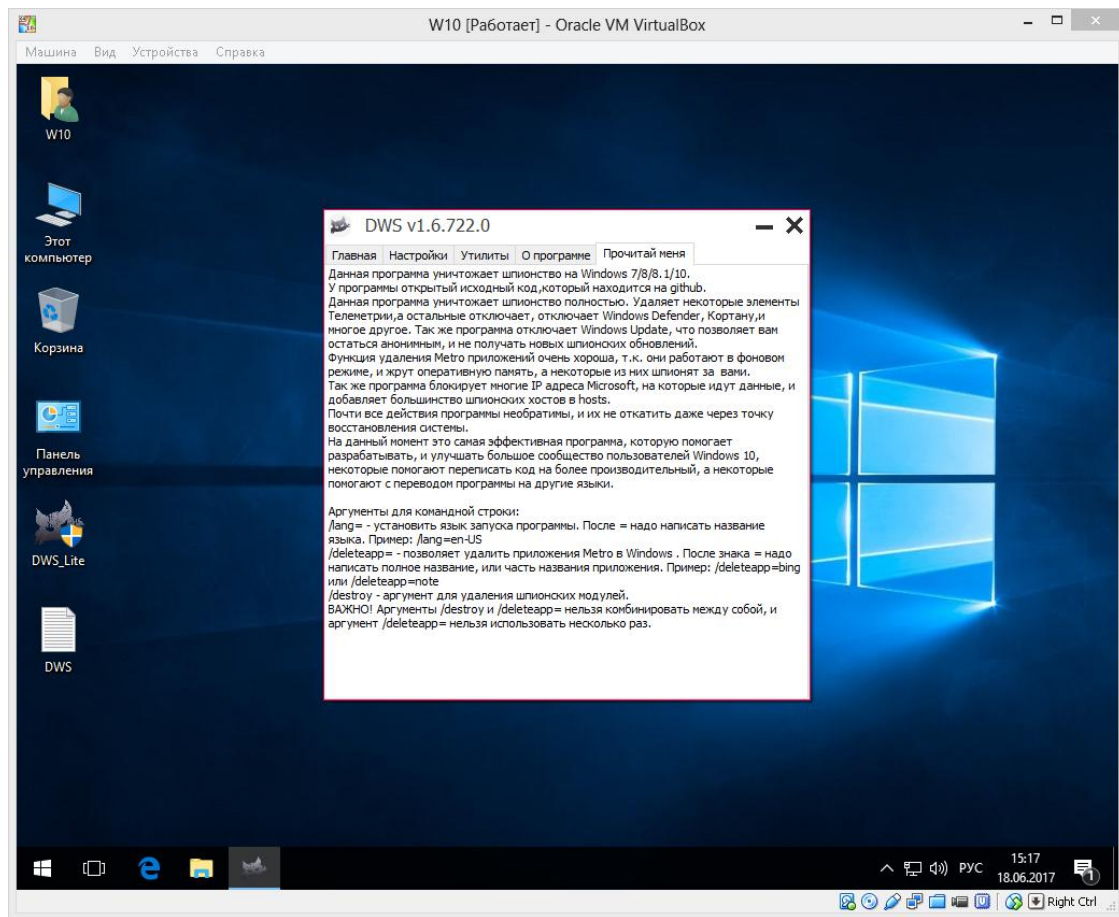


Шаг 4: Удаление шпионского функционала Windows 10

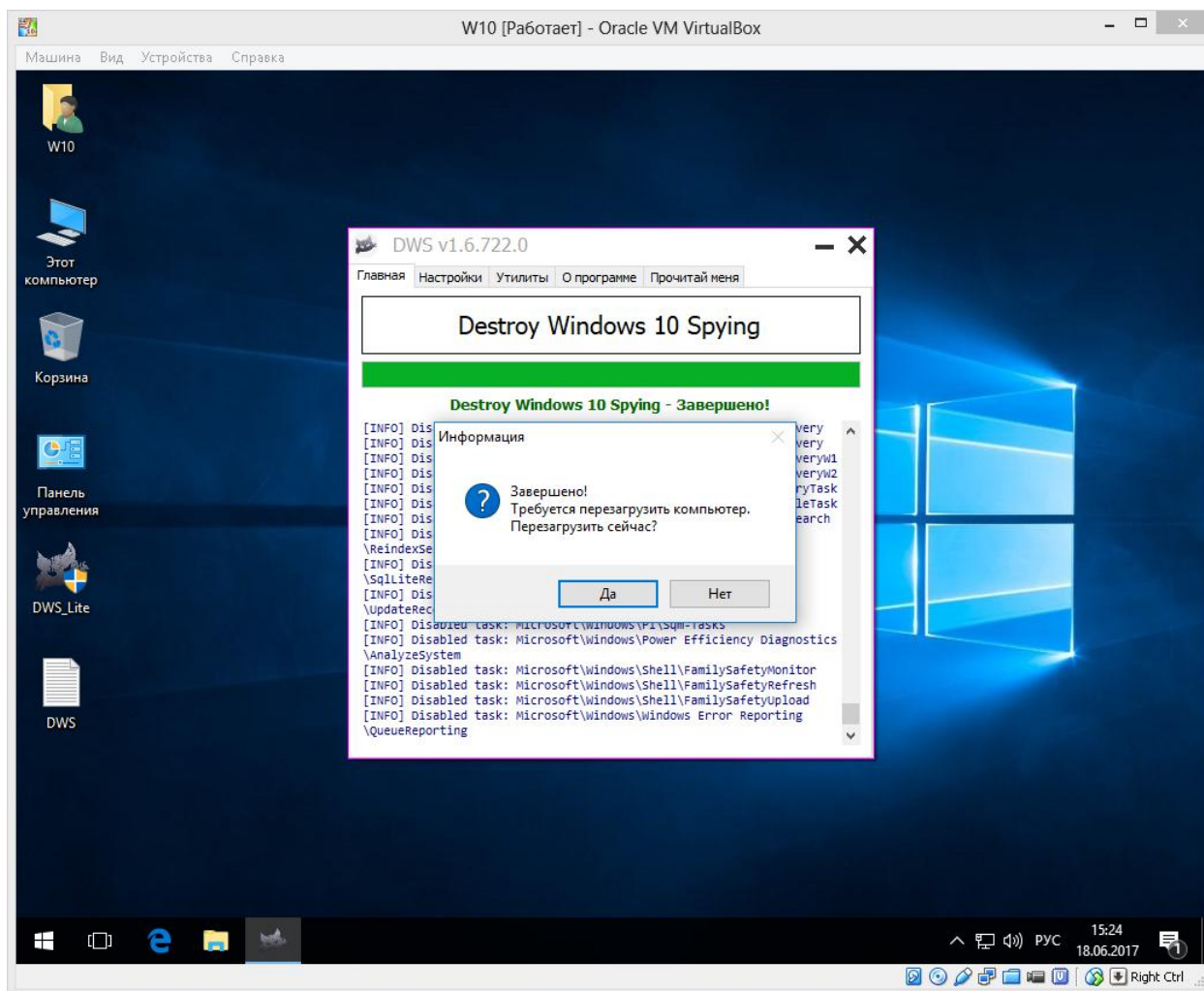
Заходим в Microsoft Edge и по ссылке https://github.com/Nummer/Destroy-Windows-10-Spying/releases/download/1.6.722/DWS_Lite.exe скачиваем утилиту удаления шпионского функционала Windows 10. Ставим настройки по умолчанию как есть. Опционально можно удалить стандартные Metro-приложения Microsoft.







После выбора настроек нажимаем кнопку «Destroy Windows 10 Spy» и перезагружаем машину.



Приложение: шпионские особенности функционала Windows 10

В описании к утилите [Destroy Windows 10 Spying](#) значится:

«После выхода Windows 10 пользователи стали изучать лицензионное соглашение, и заметили там пункты о том, что Microsoft следит за ними, и пользователи сами на это подписываются. Все ваши данные отсылаются на сервера Microsoft и остаются там. Получается что при любом взломе Microsoft (а это реально, вспомните как взломали Google, и слили все почты) все ваши данные утекут в сеть. Даже если не будет взлома Microsoft, то из-за слежки могут возникнуть проблемы. Уже были случаи с блокировкой Microsoft аккаунта, который привязан к операционной системе. Причина блока только одна — нарушение лицензионного соглашения. Чтобы ничего, из выше перечисленного не случилось, стоит позаботиться о своей анонимности, и отключить все шпионские модули, и записи в Windows 10. Можете это сделать руками, а можете воспользоваться автоматической утилитой Destroy Windows 10 Spying, и удалить через неё за два клика. Данная утилита обладает гибкими настройками для удаления шпионских модулей».

Поэтому вы можете использовать эти программные сервисы для предотвращения слежения за пользователем со стороны Windows 10 или же просто начать пользоваться другой ОС.

Дополнительный [материал](#) от NoNameClub:

Что именно крадет у пользователя Windows 10

Microsoft берет с вашего компьютера:

1. Весь печатаемый текст. Не важно, каким приложением вы пользуетесь. Нажатия клавиш перехватываются на уровне операционной системы, данные собираются в пакеты и отправляются с периодичностью 1 раз в 30 минут на сервера корпорации.

Например, пользователь пишет письмо с помощью сервиса Gmail, работающего в Chrome или Firefox. Но текст письма всё равно будет перехвачен на низком уровне ОС и отправлен на сервера Microsoft. Зачем? Для того, чтобы работал этот сервис. Формальное объяснение от Microsoft: нужно для улучшения работы системы предиктивного ввода (ускоренный набор текста).

2. Геолокационные данные. И названия сетей Wi-Fi поблизости. Накапливаются и передаются раз в 30 минут. Позволяют отслеживать физические перемещения пользователя с точностью до нескольких метров. Объяснение от Microsoft: данные нужны для поисковой системы Bing, чтобы она могла выдавать более релевантные ответы. Что это значит для пользователя: Microsoft знает ваш домашний адрес (зачем он нужен см. п. 5). Если у вас мобильное устройство с Windows 10, в Microsoft знают о всех местах, где вы бываете.

3. Запись с микрофона. Микрофон в Windows 10 включен постоянно (см. статью «Windows 10 тайно включает микрофон»). Сначала высказывались предположения, что это необходимо для работы сервиса Cortana (голосовой помощник), но чуть позже стало известно, что отключение Cortana не решает проблему. Записи голоса пользователя могут накапливаться, какая-то часть из них отправляется на сервера Microsoft. Эксперты по компьютерной безопасности предупреждают: если вы пользуетесь зашифрованными средствами связи (например, используете SIP-телефонию с шифрованием трафика), такая несанкционированная запись звуков с микрофона может поставить вашу безопасность под удар. Использовать надежный канал VoIP одновременно с Windows 10 — совершенно бессмысленное занятие. Лучше сразу выйти на улицу и прокричать.

4. Телеметрия. Фантастическая по своей потенциальной небезопасности функция, которая даже не скрывается компанией-разработчиком. Телеметрия — это передача данных в Microsoft о состоянии вашего компьютера и вашей активности. Собирается буквально всё: какие программы установлены, какие запущены, объем занятой памяти, журналы приложений, фрагменты оперативной памяти и так далее. Учитывая, что в оперативной памяти может оказаться что угодно — от данных для служебного пользования до номеров кредиток — такая передача на чужие сервера является потенциальной уязвимостью. Хотя в Microsoft уверяют, что данные надежно шифруются, кто может гарантировать, что шифр не будет тайком взломан злоумышленниками? Ведь всем известно, что у Microsoft всегда были большие проблемы с безопасностью. Точнее, с устойчивой неспособностью эту безопасность обеспечить¹.

5. Борьба с пиратством. Windows 10 просматривает названия пользовательских файлов и сверяет с постоянно обновляемым списком пиратских новинок. Если находятся

¹ См. историю распространения вируса-шифрователя WannaCry, эксплуатировавшего некоторые уязвимости Windows всех версий.

соответствия, листинги пользовательских директорий отправляются в Microsoft. Фактически, компьютер доносит на своего же владельца.

Напомним, данные об антипиратской активности Windows 10 были известны давно. Но предполагалось, что акцент будет сделан на борьбе с контрафактными играми. Сейчас становится понятно, что главная цель — лишить пользователей возможности скачивать с торрентов пиратские копии американских фильмов и сериалов.

Особо следует отметить, что сопоставление данных о наличии нелегального видео на компьютере пользователя с собранными геолокационными данными открывает отличную возможность для МРАА (Американская ассоциация кино) и RIAA (Американская ассоциация звукозаписи) отсудить у какой-нибудь американской домохозяйки очередную пару миллионов долларов. Российским пользователям, похоже, пока бояться нечего: система срабатывала только при обнаружении американских фильмов.

6. Портрет на память. Некоторые пользователи заметили, что после первой активации Windows 10 на короткий период включается web-камера. Исследования это подтверждают — в Microsoft передается 35 Мб данных сразу после активации и включения встроенной камеры. Предположительно, данные привязываются к пользовательскому аккаунту Microsoft.