

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

ФАКУЛЬТЕТ ПРОГРАММНОЙ ИНЖЕНЕРИИ И КОМПЬЮТЕРНОЙ ТЕХНИКИ

НАПРАВЛЕНИЕ ПРОГРАММНАЯ ИНЖЕНЕРИЯ

ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА СИСТЕМНОЕ И ПРИКЛАДНОЕ

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

СПЕЦИАЛИЗАЦИЯ СИСТЕМНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 1 (Windows)

курса «Информационная безопасность»

по теме: «Учетные записи и авторизация в ОС MS Windows»

Вариант № 4

Выполнил студент:

Тюрин Иван Николаевич

группа: Р33102

Преподаватель:

Маркина Т.А.,

Рыбаков С.Д.

Санкт-Петербург, 2025 г.

Содержание

Лабораторная работа № 1 (Windows). Учетные записи и авторизация в ОС MS Windows	2
1. Описание	2
2. Выполнение задания	2
1. Создание пользователя и администратора	2
2. Параметры контроля учетных записей пользователей (UAC)	8
3. Настройка контроллера домена (AD – Active Directory) .	9
3. Заключение	21

Лабораторная работа № 1

(Windows)

Учетные записи и авторизация в ОС MS Windows

1. Описание

Цель работы: Изучить типы учетных записей пользователей, ознакомиться с основными принципами управления учетными записями. Изучить основные способы авторизации пользователей.

2. Выполнение задания

2. 1. Создание пользователя и администратора

Создание пользователя можно выполнить различными способами, 2 основных подхода: с помощью графических приложений и с помощью командной строки (CMD или PowerShell). Ниже приводятся скриншоты демонстрирующие различные подходы к созданию пользователей; для графических приложений не выделяются отдельно создание администратора и рядового пользователя, т.к. вся разница лишь в выборе нужного пункта меню: обычный пользователь или администратор, который влияет на наличие пользователя в группе Administrators.

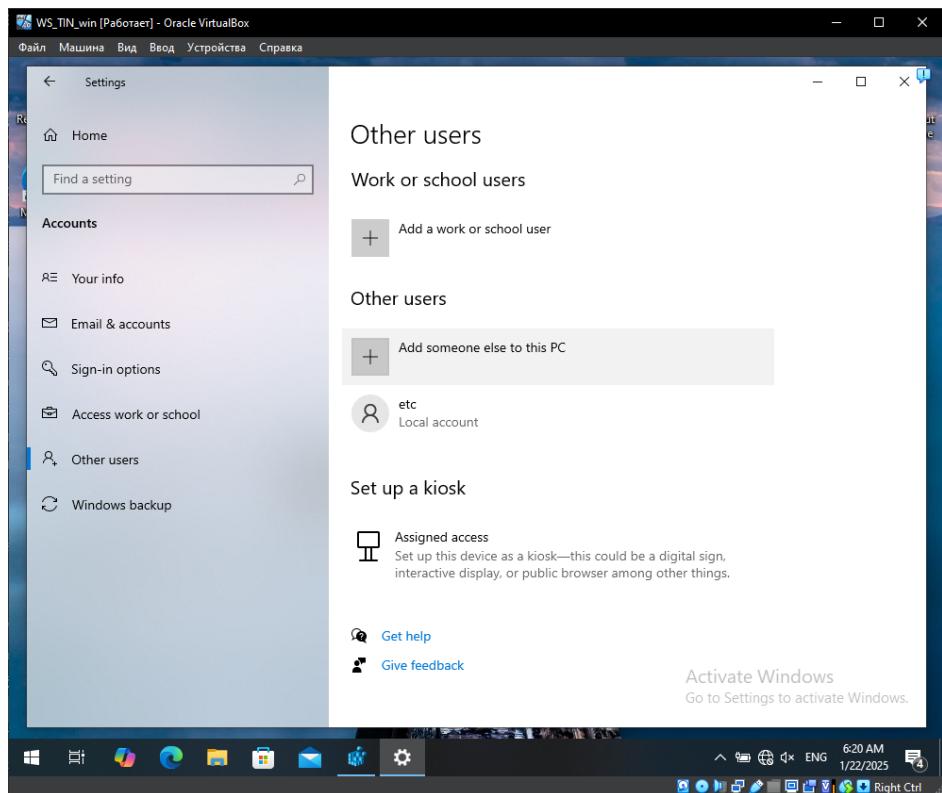


Рис. 1.1: Создание пользователя в приложении настроек системы.

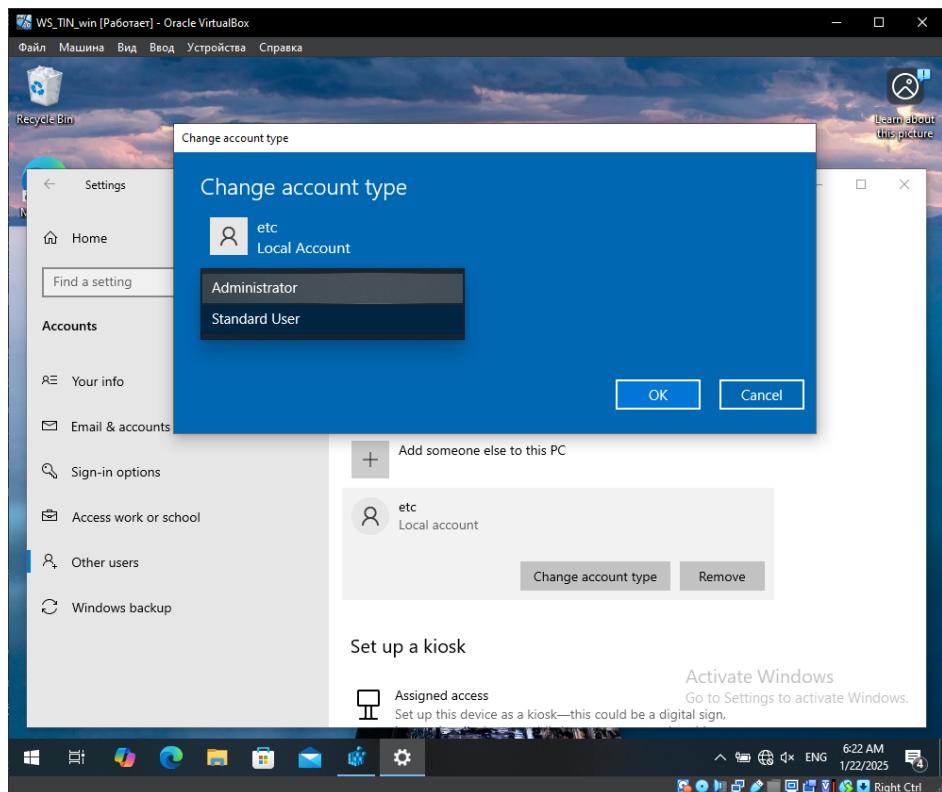


Рис. 1.2: Создание администратора из приложения настроек системы.

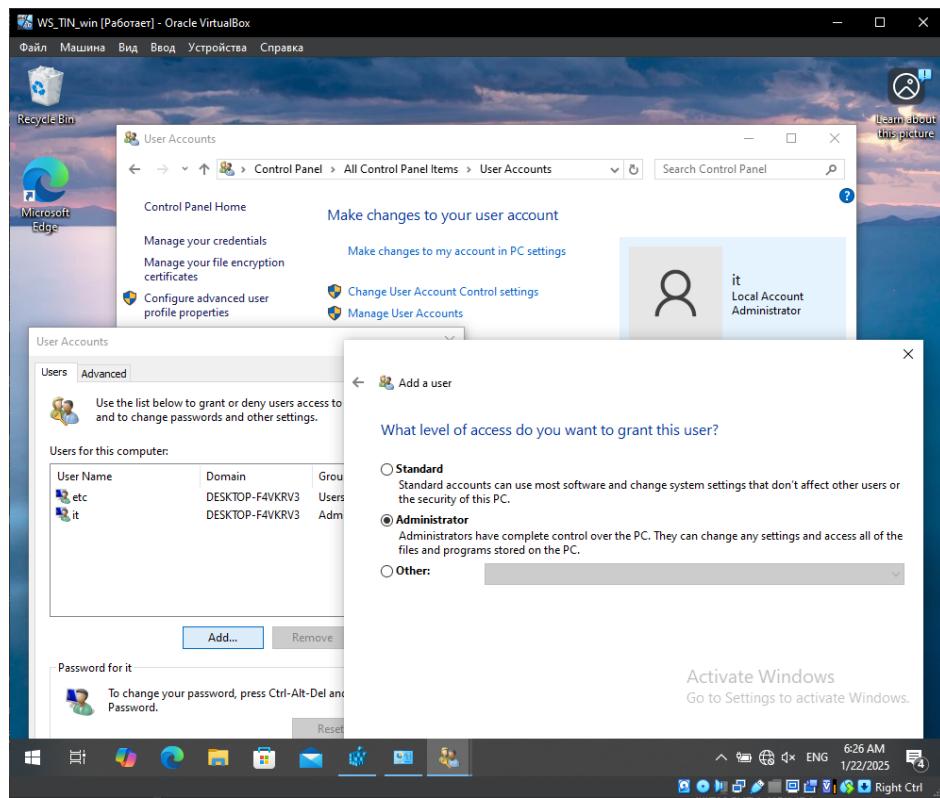


Рис. 1.3: Создание администратора из Панели управления.

Можно использовать утилиту lusrmgr (Win+R > lusrmgr.msc).

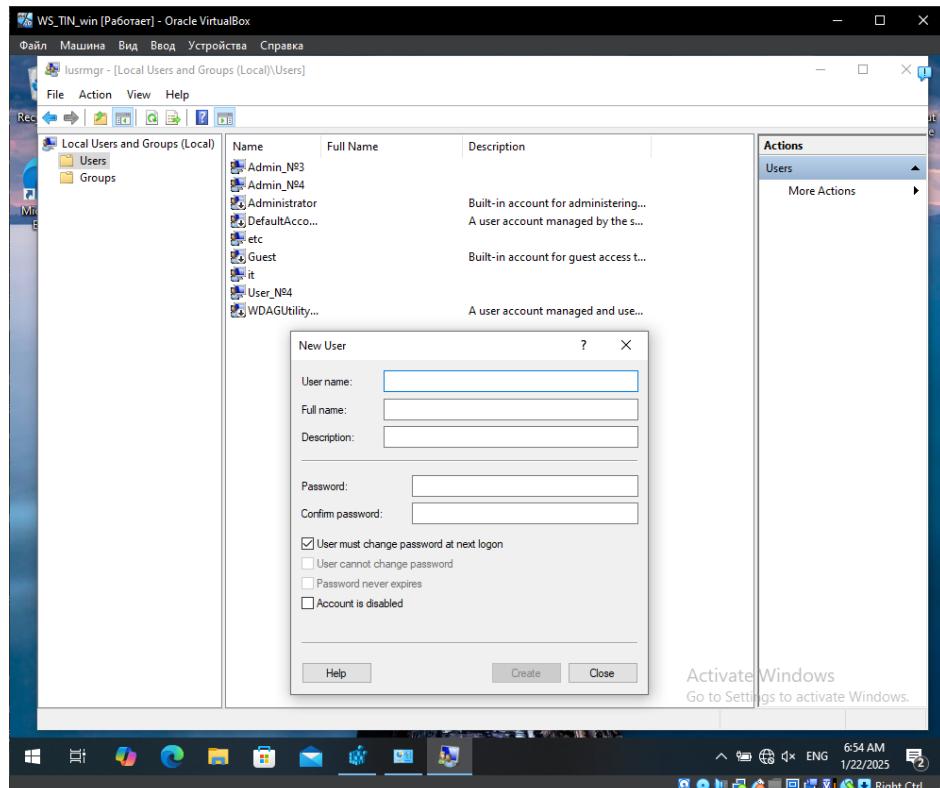


Рис. 1.4: Создание пользователя с помощью приложения lusrmgr.msc - [Local Users and Groups (Local)].

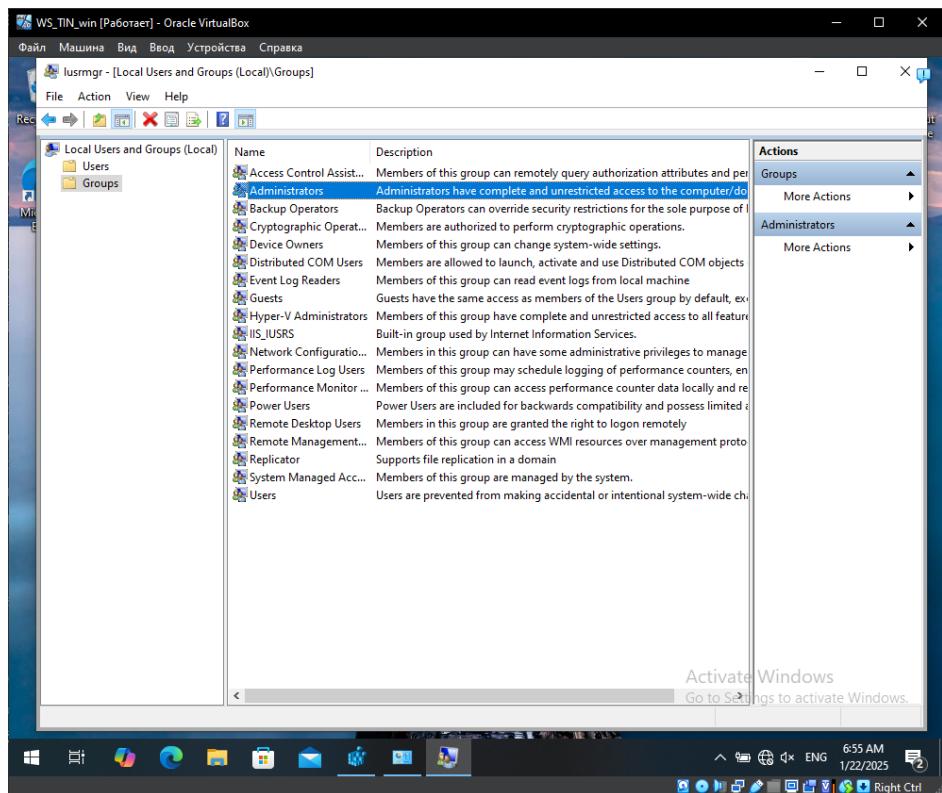


Рис. 1.6: Список имеющихся групп видимых в lusrmgr.msc.

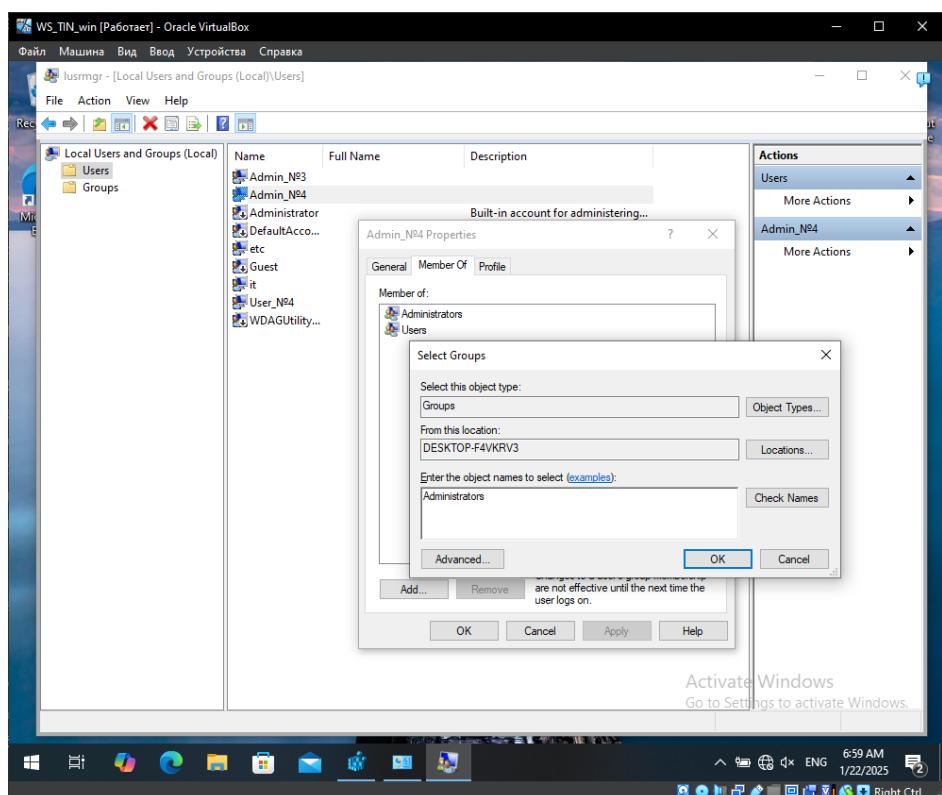


Рис. 1.5: Создание администратора с помощью приложения lusrmgr.msc (добавление в группу Administrators).

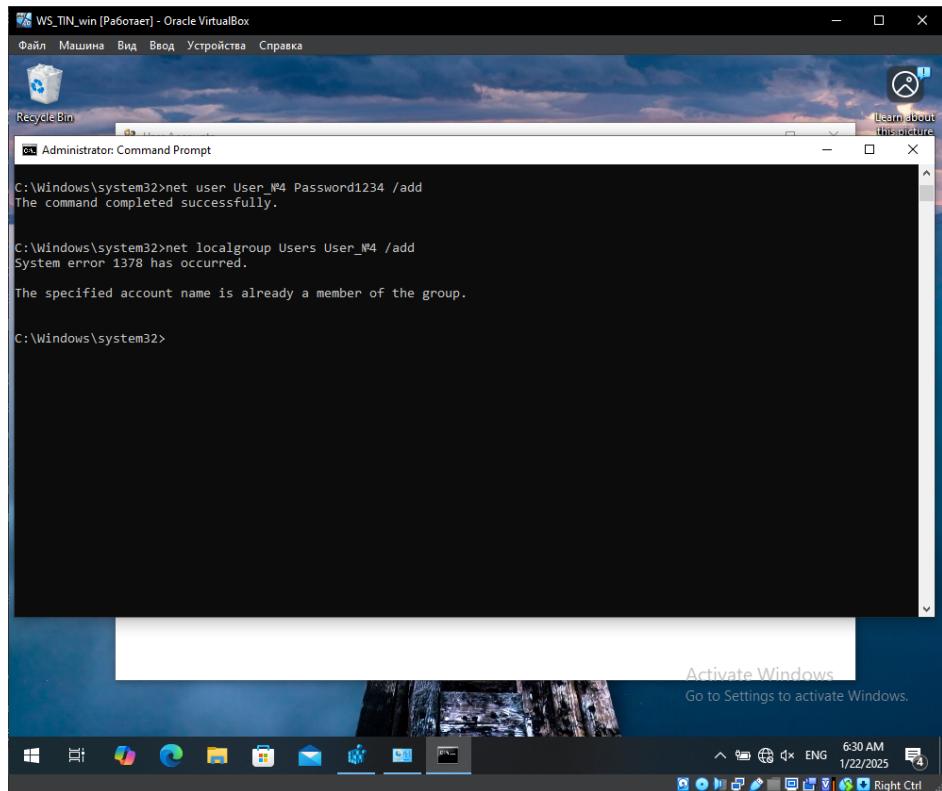


Рис. 1.7: Создание пользователя из командной оболочки.

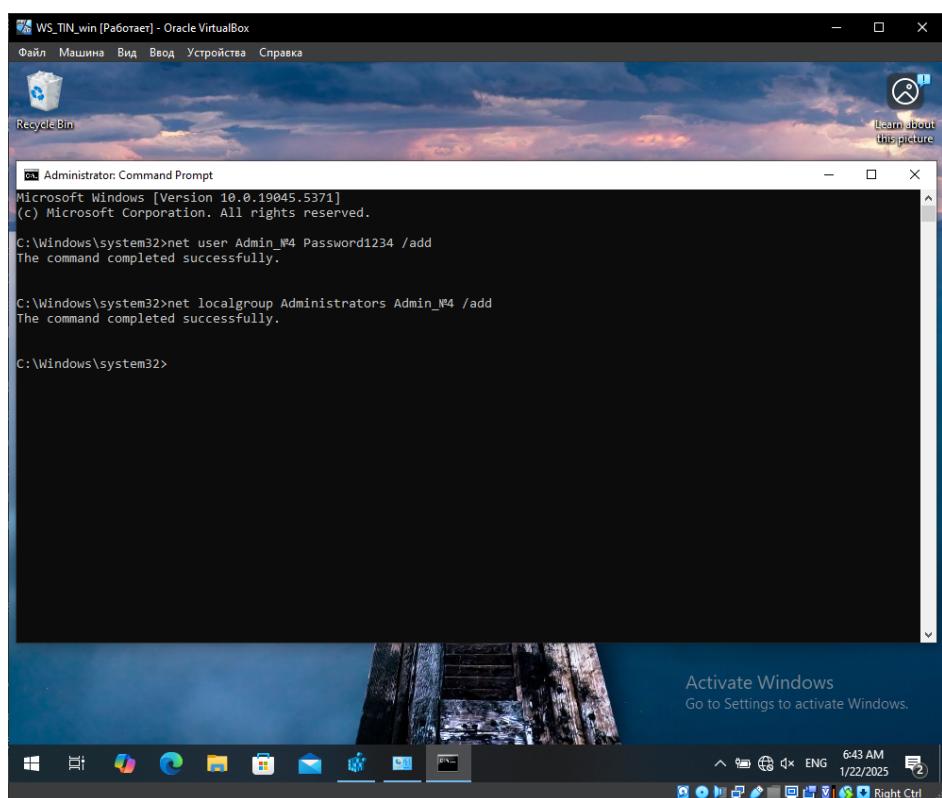


Рис. 1.8: Создание администратора (добавление пользователя в группу администраторов) из командной оболочки.

Важно, что для создания администратора локально необходимо выйти из домена, если ранее контроллер домена был настроен.

Соответственно, еще один способ создать пользователя – с помощью контроллера домена (AD DC), скриншоты здесь не приводятся, но будут далее.

У пользователя, входящего в группу "Пользователи есть **ограниченные возможности** по изменению конфигурации системы:

1. Пользователь может изменять настройки рабочего стола:

Например, изменить фоновый рисунок, экранную заставку, разрешение экрана. Также доступна настройка звуковых схем и пр.

2. Установка и настройка программ для текущего пользователя:

Пользователь может устанавливать программы, не требующие права администратора, которые размещаются в профиле пользователя (%AppData%).

Также возможно изменять параметры приложений, например, настроить параметры браузера, изменить настройки автозагрузки программ (в пределах своих прав).

3. Изменение временной зоны:

Пользователь может изменить часовой пояс.

Ограничения. Пользователь не может:

1. Изменять параметры системы, затрагивающие других пользователей (например, управление службами или системными реестрами).
2. Устанавливать драйверы или программы, требующие административных прав.
3. Управлять пользователями и группами.

Ограничения администратора. Несмотря на широкие права, учётная запись администратора всё же имеет ограничения:

1. Ограничения политики безопасности (UAC):

Даже с правами администратора, пользователь может столкнуться с запросами на подтверждение действий, изменяющих системные файлы. Например, запуск программы, требующей привилегий администратора (например, редактора реестра), сопровождается запросом UAC.

2. Ограничения на доступ к защищённым системным файлам:

Некоторые системные файлы (например, содержимое папки System Volume Information) недоступны даже для администратора без изменения настроек прав доступа.

3. Ограничения в доменной среде:

Если компьютер находится в домене, администратор локального компьютера не имеет полномочий изменять доменные политики. Например, нельзя отключить групповые политики, установленные сервером домена.

2. 2. Параметры контроля учетных записей пользователей (UAC)

Контроль учетных записей пользователей (UAC, User Account Control) — это механизм безопасности в Windows, который помогает предотвращать несанкционированные изменения системы, требуя подтверждения действий, связанных с повышением привилегий.

Ползунок UAC позволяет выбрать один из четырех уровней уведомления.

- Всегда уведомлять:

- Уведомляет, когда программы пытаются установить программное обеспечение или внести изменения на компьютере.
- Уведомляет, когда вы вносите изменения в параметры Windows.
- Замораживает выполнение других задач, пока вы не ответите.

Рекомендуется, если вы часто устанавливаете новое программное обеспечение или посещаете незнакомые веб-сайты.

- Уведомлять только при попытках приложений внести изменения в компьютер:

- Уведомляет, когда программы пытаются установить программное обеспечение или внести изменения на компьютере.
- Не уведомляет, когда вы вносите изменения в параметры Windows. Замораживает выполнение других задач, пока вы не ответите.

Рекомендуется, если вы не часто устанавливаете приложения или посещаете незнакомые веб-сайты.

- Уведомлять только при попытках приложений внести изменения в компьютер (не затемнять рабочий стол):

- Уведомляет, когда программы пытаются установить программное обеспечение или внести изменения на компьютере.

- Не уведомляет, когда вы вносите изменения в параметры Windows.
- Не замораживает выполнение других задач, пока вы не ответите.

Не рекомендуется. Выбирайте этот вариант, только если затемнение рабочего стола компьютера занимает много времени.

- Никогда не уведомлять (отключить запросы UAC):
 - Не уведомляет, когда программы пытаются установить программное обеспечение или внести изменения на компьютере.
 - Не уведомляет, когда вы вносите изменения в параметры Windows.
 - Не замораживает выполнение других задач, пока вы не ответите.

Не рекомендуется по соображениям безопасности.

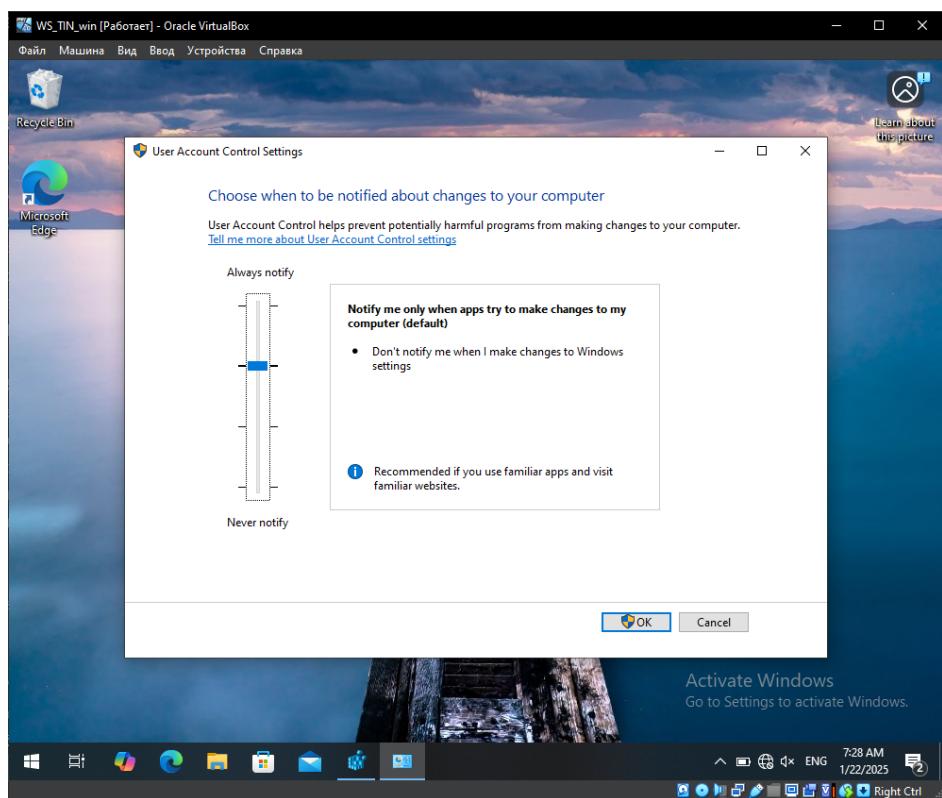


Рис. 1.9: Панель управления UAC с «ползунком».

2. 3. Настройка контроллера домена (AD — Active Directory)

Установка и настройка сервиса контроллера домена (AD) происходила с использованием инструкций из статьи <https://www.ibm.com/docs/en/storage-scale-bda?topic=support-install-configure-active-directory>.

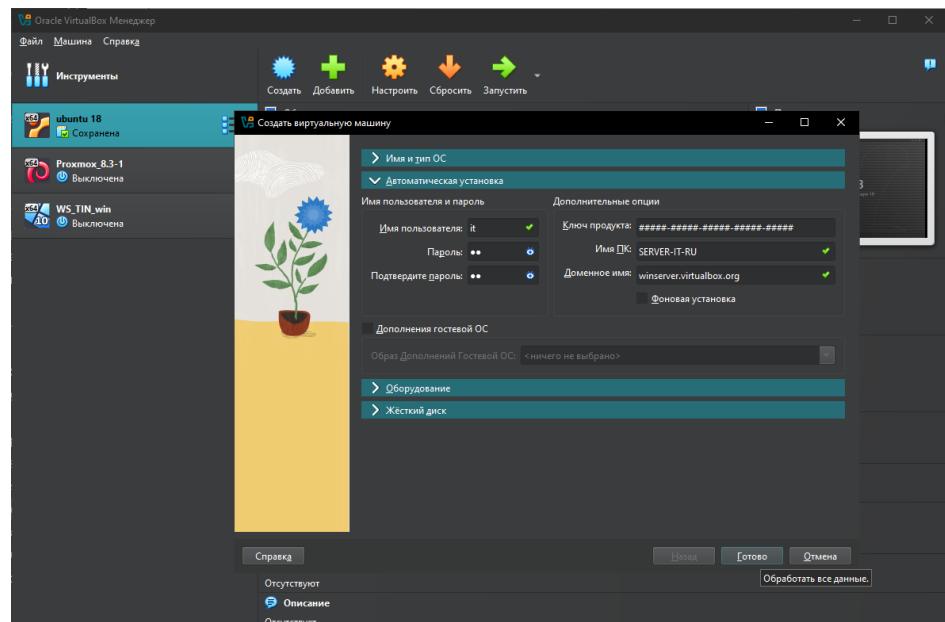


Рис. 1.10: Настройка виртуальной машины с Windows Server.

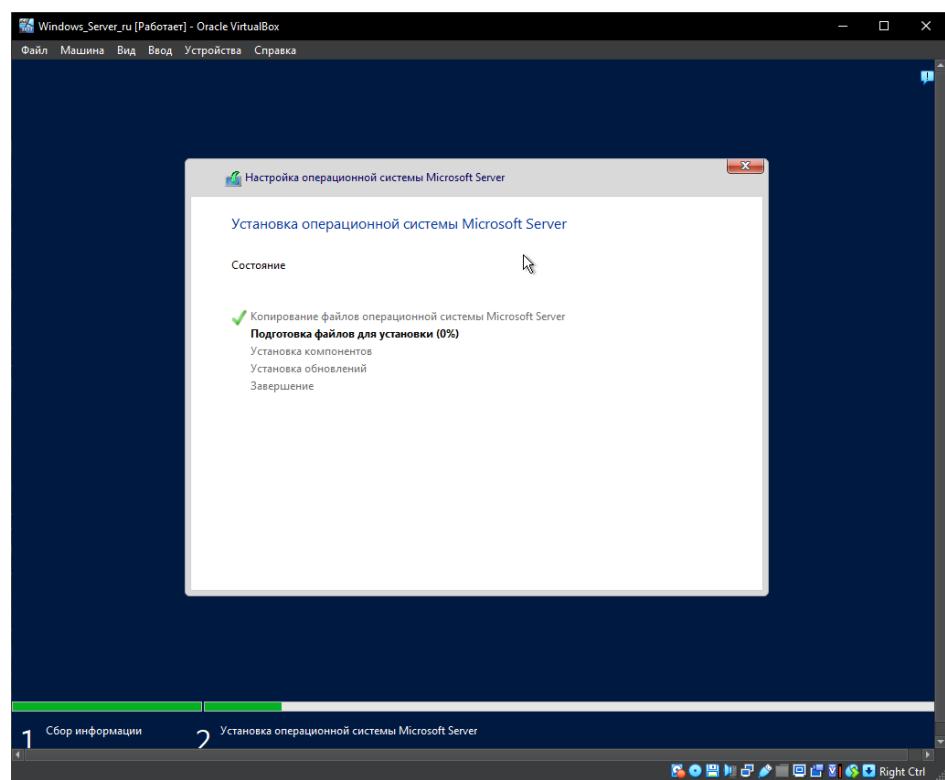


Рис. 1.11: Установка Windows Server в виртуальной машине.

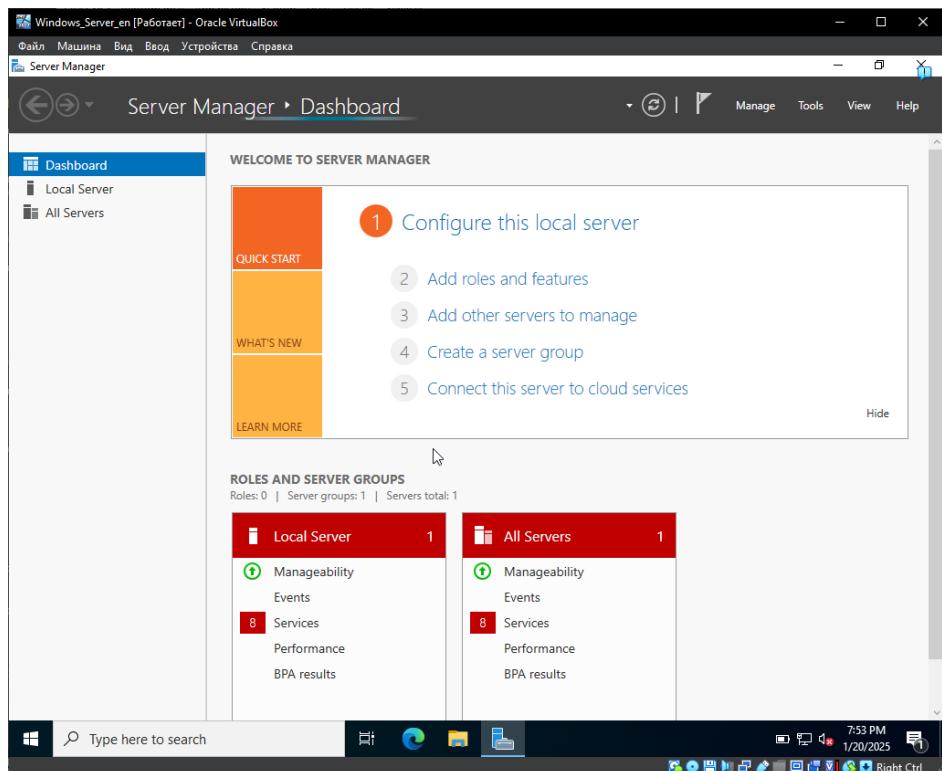


Рис. 1.12: Панель настройки Windows Server.

Для установки сервиса использовался выдуманное название домена `root.vbox.org`, через которое будет происходить аутентификация и авторизация пользователей. Позже придется настроить статический DNS на управляемых компьютерах, чтобы этот домен был доступен в сети управляемых компьютеров

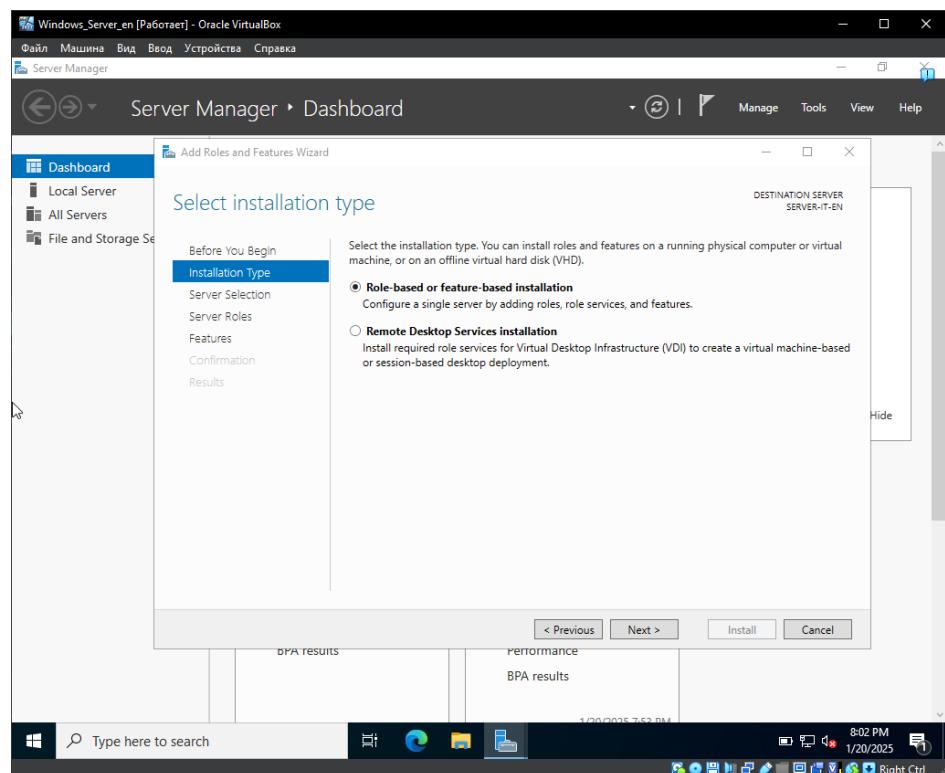


Рис. 1.13: Выбор типа сервиса для установки.

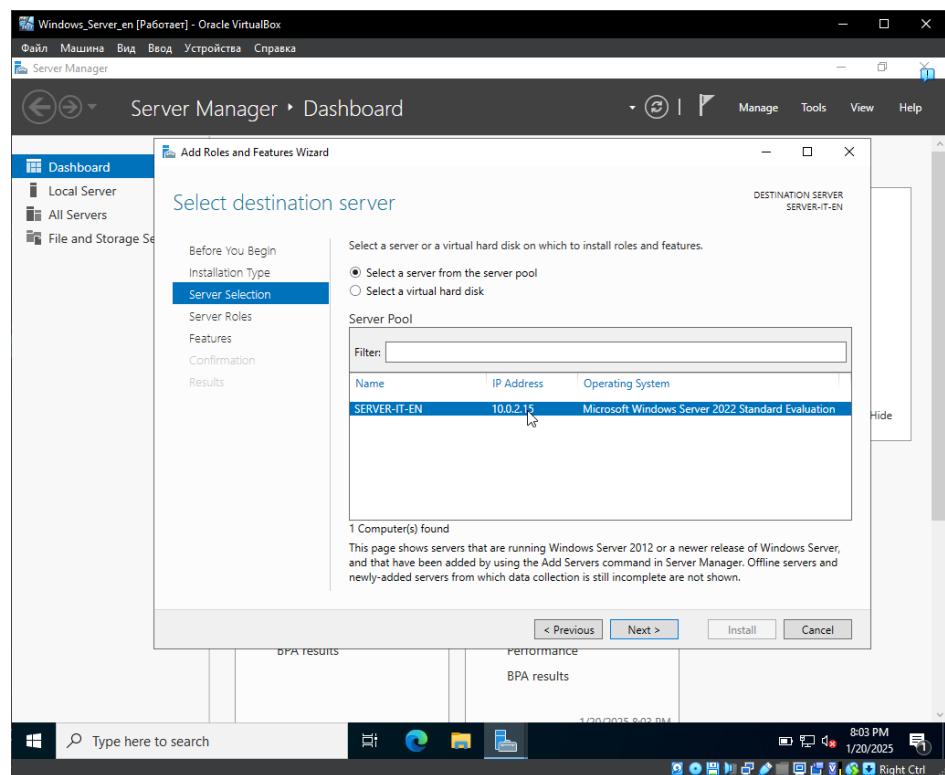


Рис. 1.14: Выбор компьютера для установки сервиса контроллера домена.

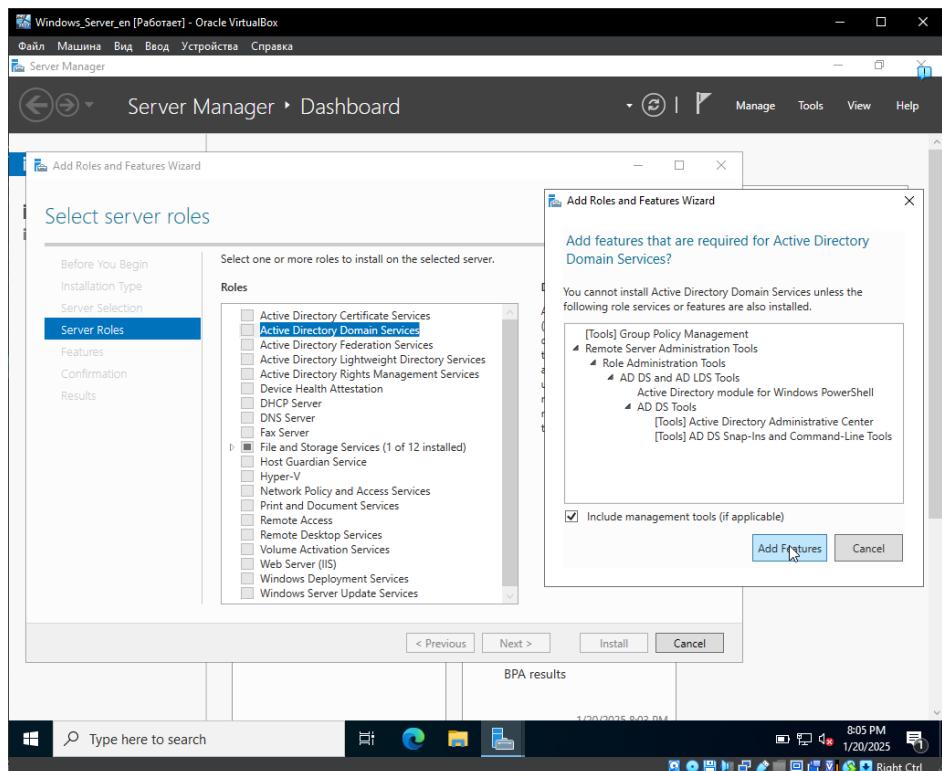


Рис. 1.15: Добавление сервиса контроллера домена.

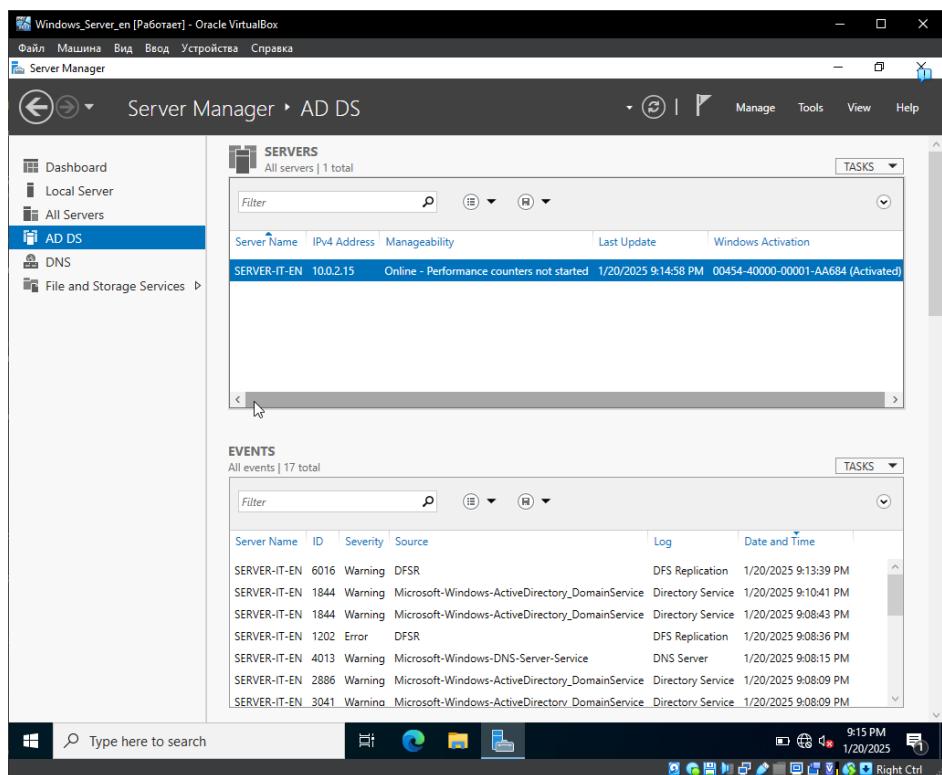


Рис. 1.16: Успешное установление сервиса контроллера домена на Window Server.

Для дальнейшей настройки использовались инструкции из статьи: realmeghamishra.medium.com/how-join-a-client-machine-with-domain-

controller-machine-and-login-with-ad-domain-user-as-c113ebcdeb3b.

В домене были созданы 2 новых пользователя: «kek lol» и «idk omg». Они нужны для проверки аутентификации без соединения с контроллером домена.

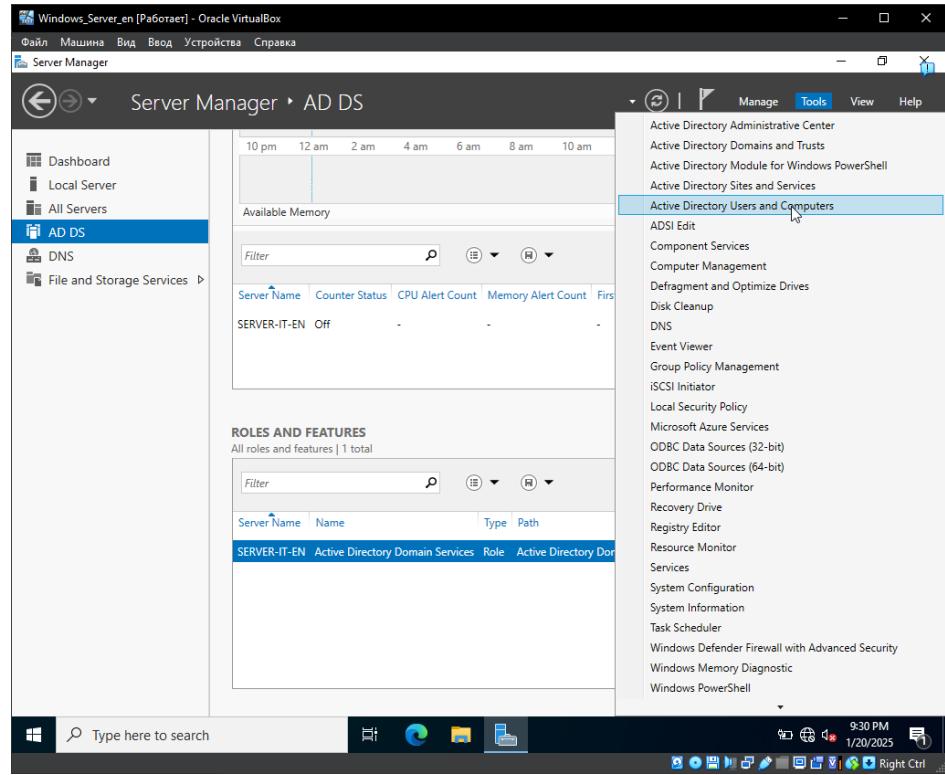


Рис. 1.17: Панель управления доменом, меню управления пользователями и компьютерами.

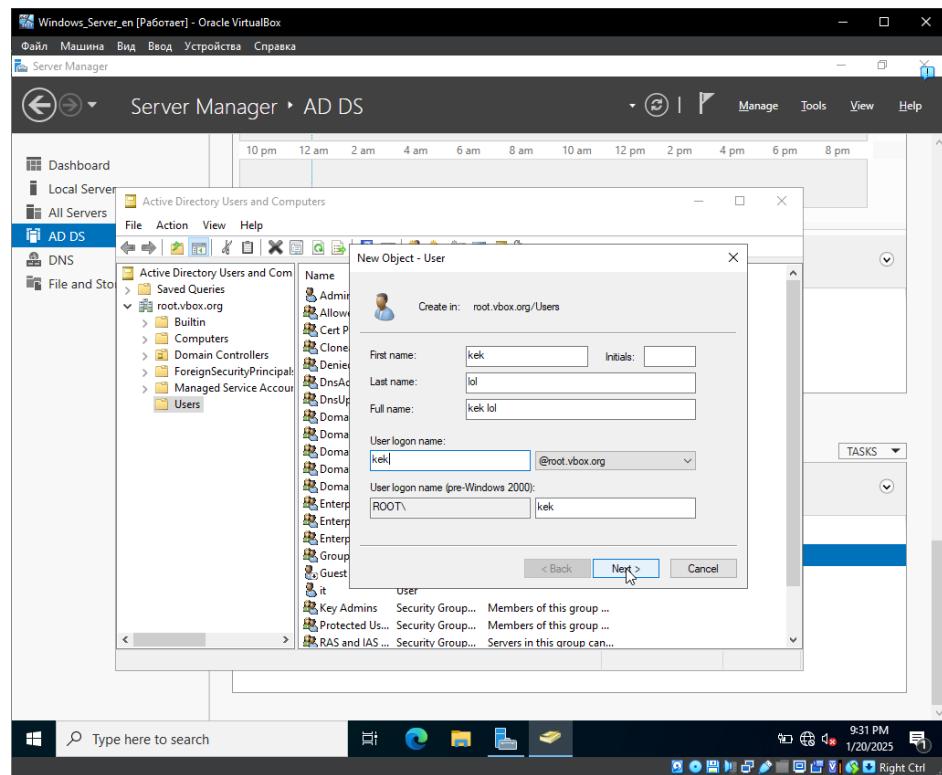


Рис. 1.18: Панель добавления пользователя в домен.

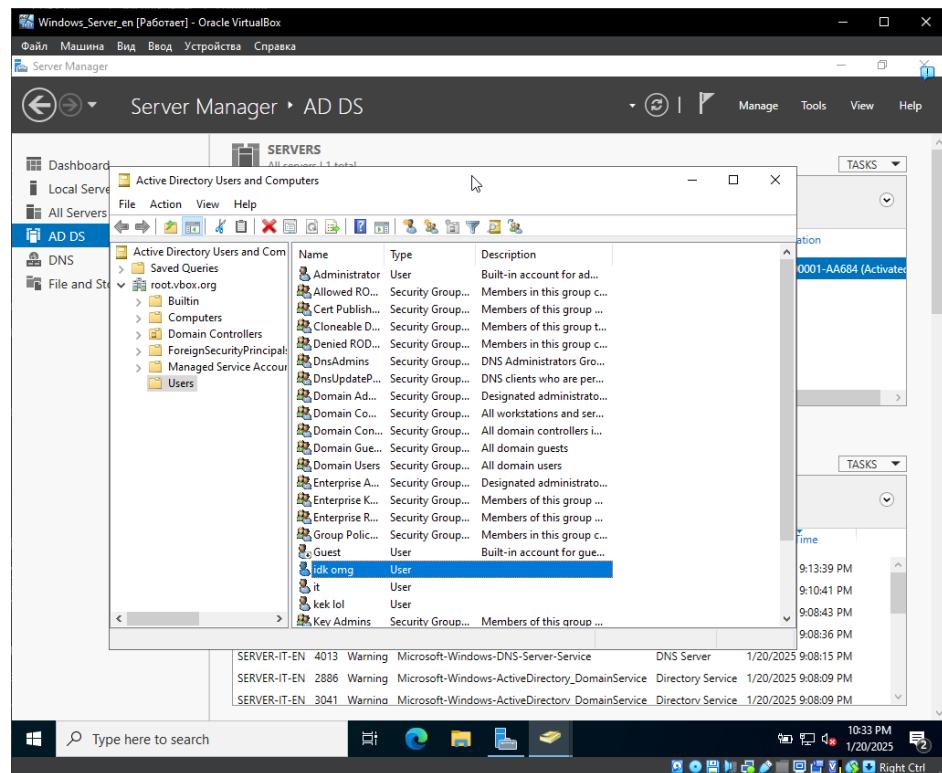


Рис. 1.19: Добавление пользователей в домене.

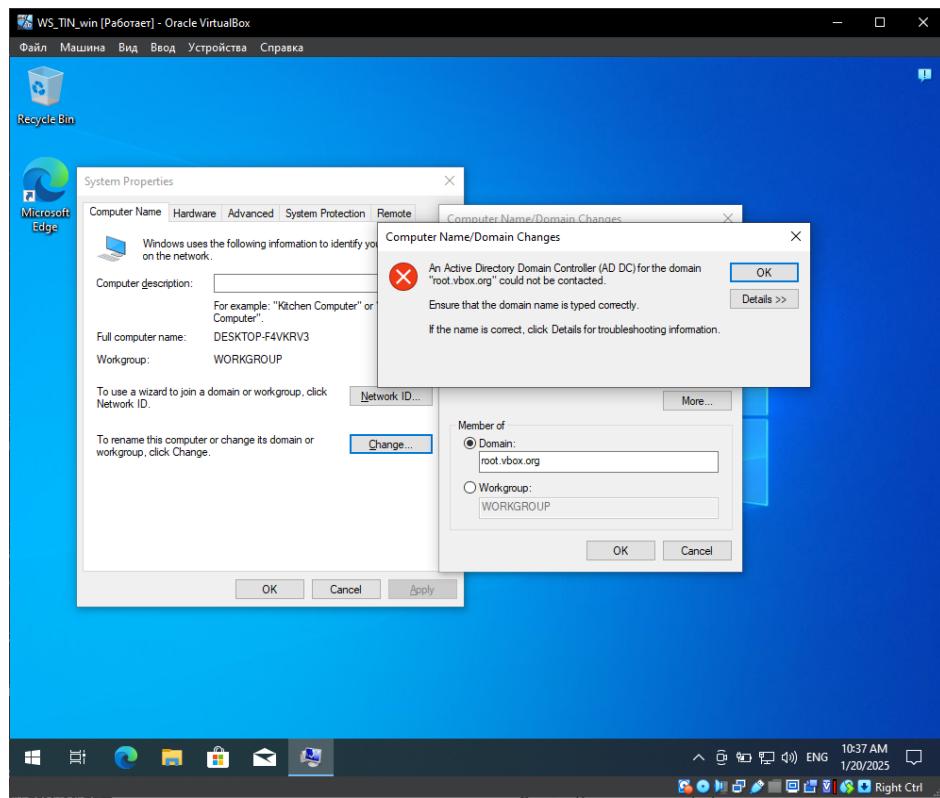


Рис. 1.20: Ошибка при подключении к домену из-за отсутствия соединения между компьютерами

Для устранения проблем с соединением в настройках виртуальных машин установим тип адаптера – сетевой мост, тем самым получим, что все компьютеры (в том числе хост) находятся в одной локальной сети. Теперь можно настроить подключение к домену.

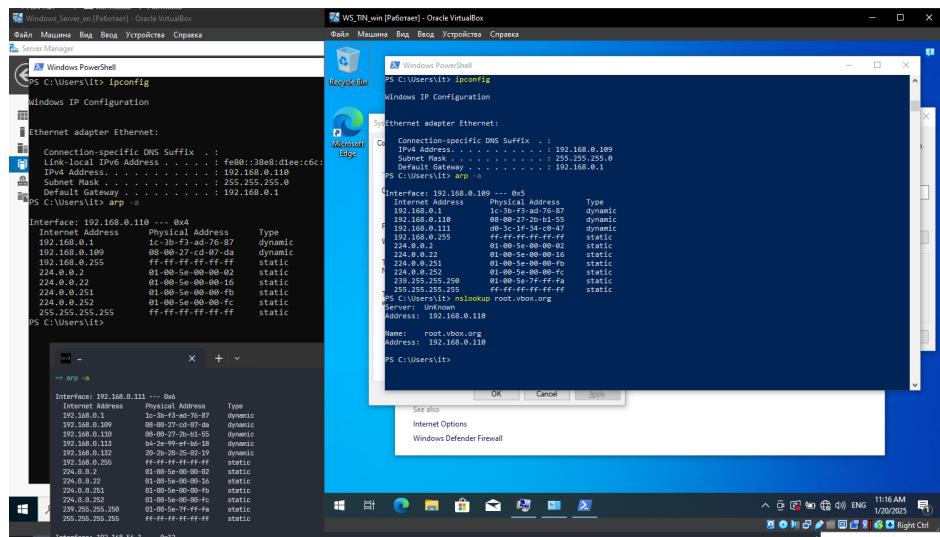


Рис. 1.21: Компьютеры размещены в одной сети.

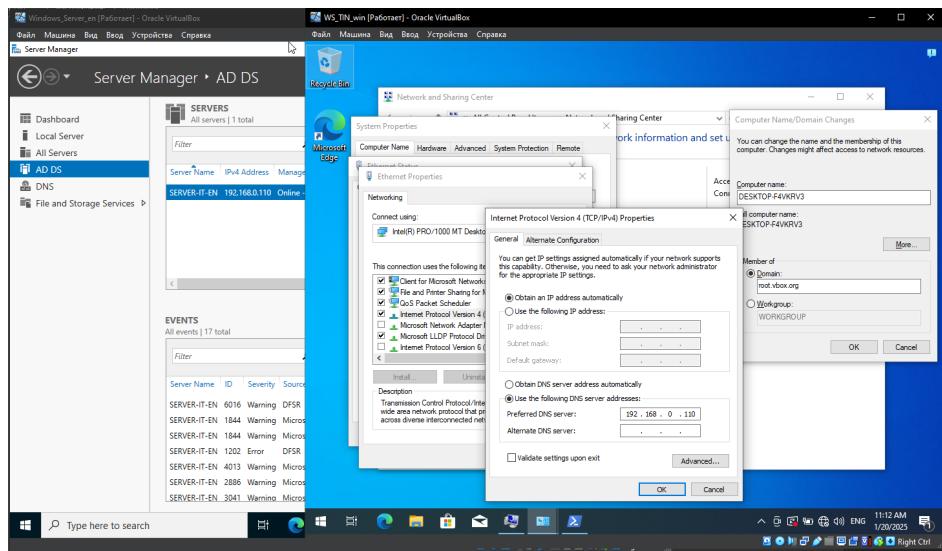


Рис. 1.22: Настройка соединения с контроллером домена.

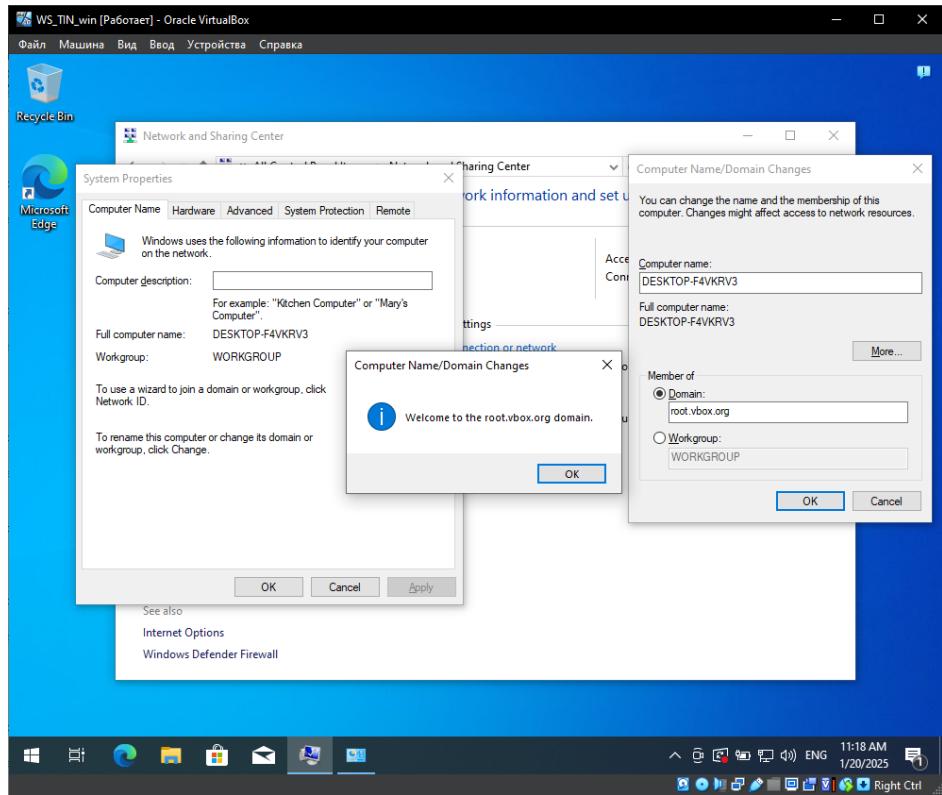


Рис. 1.23: Успешное подключение к контроллеру домена.

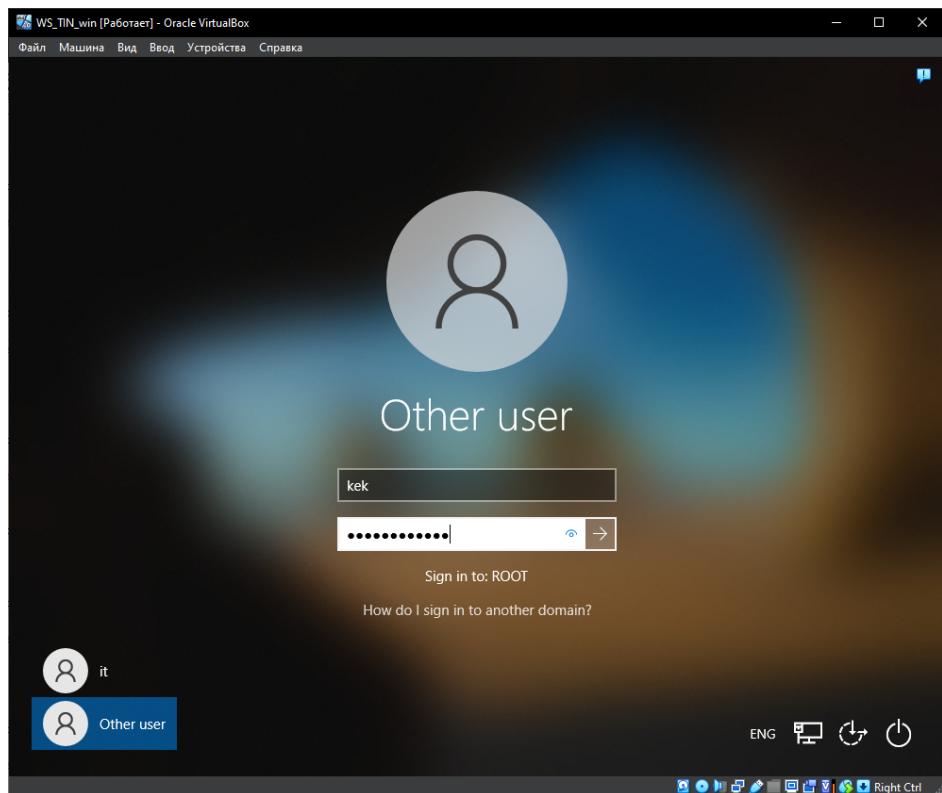


Рис. 1.24: Вход в систему под учетной записью пользователя в домене ROOT (root.vbox.org).

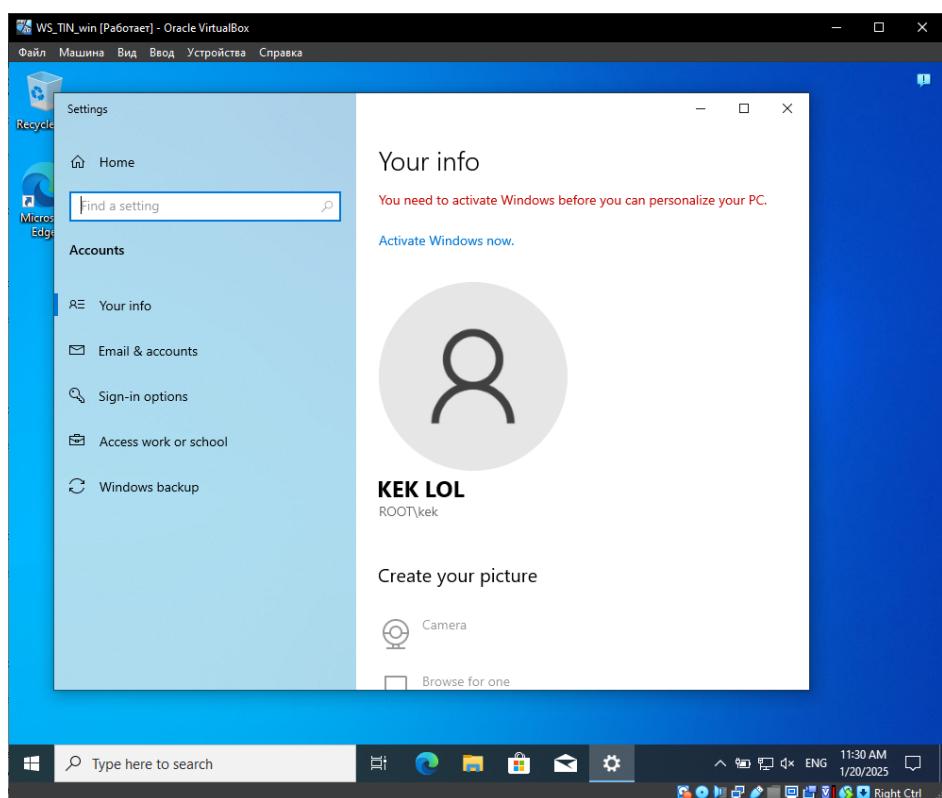


Рис. 1.25: Профиль пользователя в домене

Далее для проверки возможности аутентификации в домене без соединения с контроллером отключили адаптер виртуальной машины.

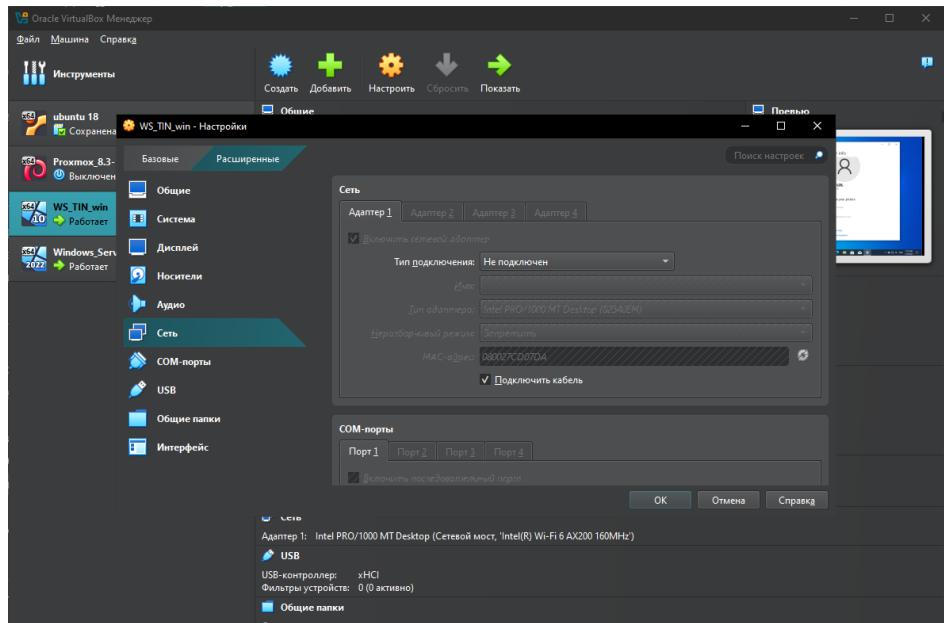


Рис. 1.26: Отключение от сети компьютера в домене.

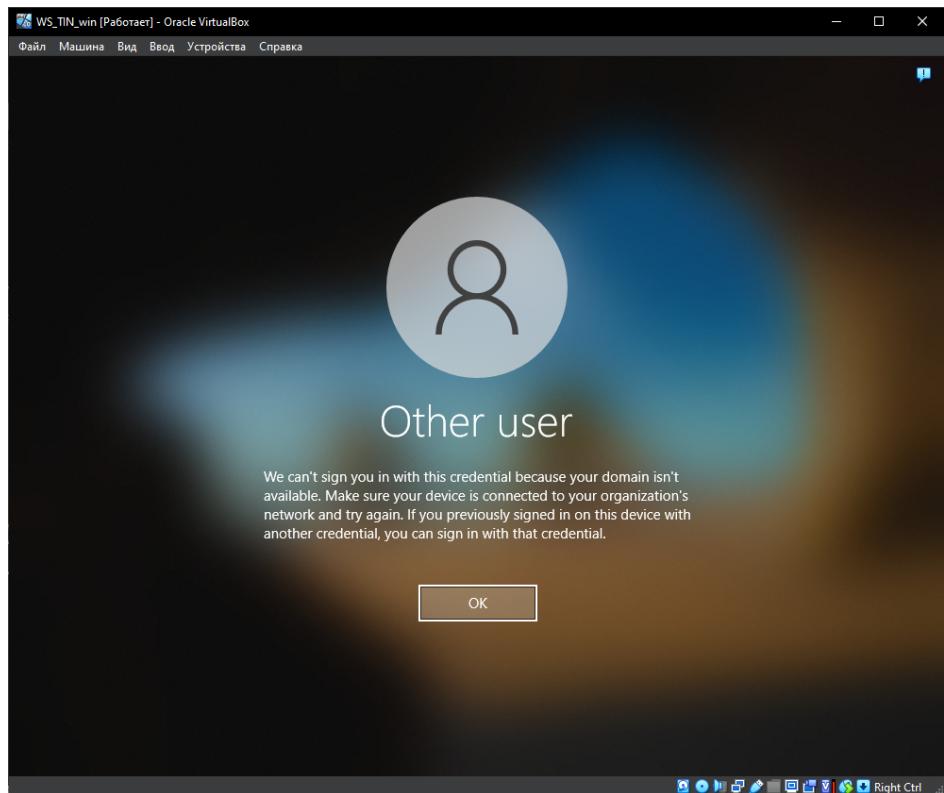


Рис. 1.27: Проблемы с аутентификацией пользователя в домене ранее не вошедшего в систему в отсутствии соединения с контроллером домена.

В системе сохраняется хеш пароля для единожды аутентифицировавшихся пользователей, поэтому при отсутствии соединения с сетью тоже можно аутентифицироваться.

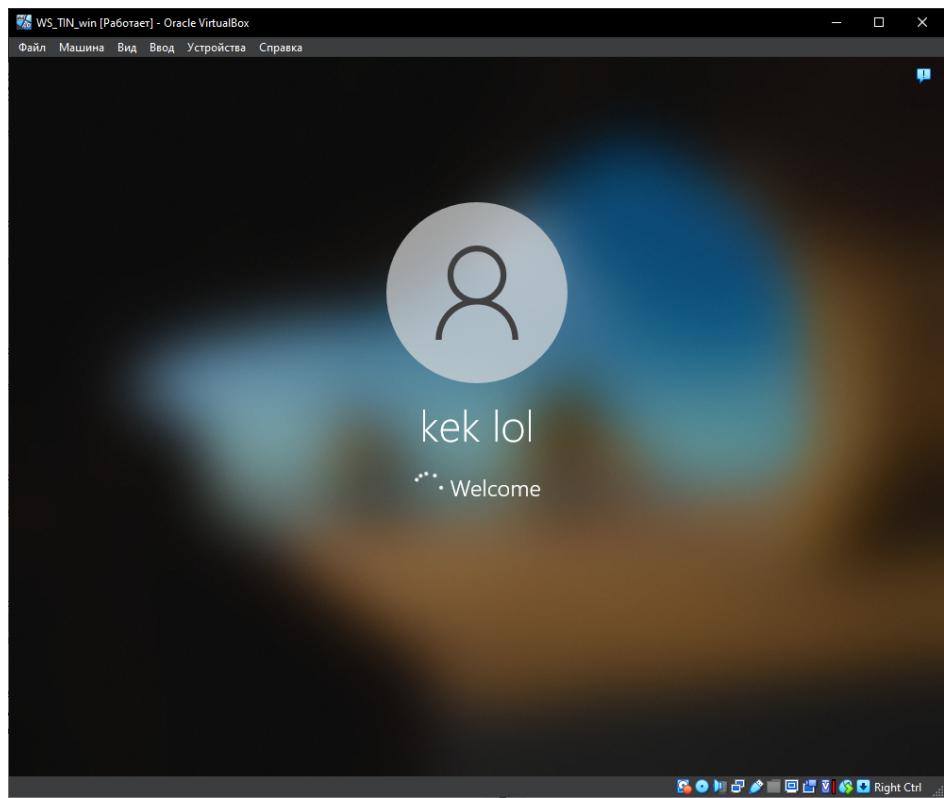


Рис. 1.28: Успешный вход в систему через ранее аутентифицировавшегося пользователя при отсутствии подключения к сети.

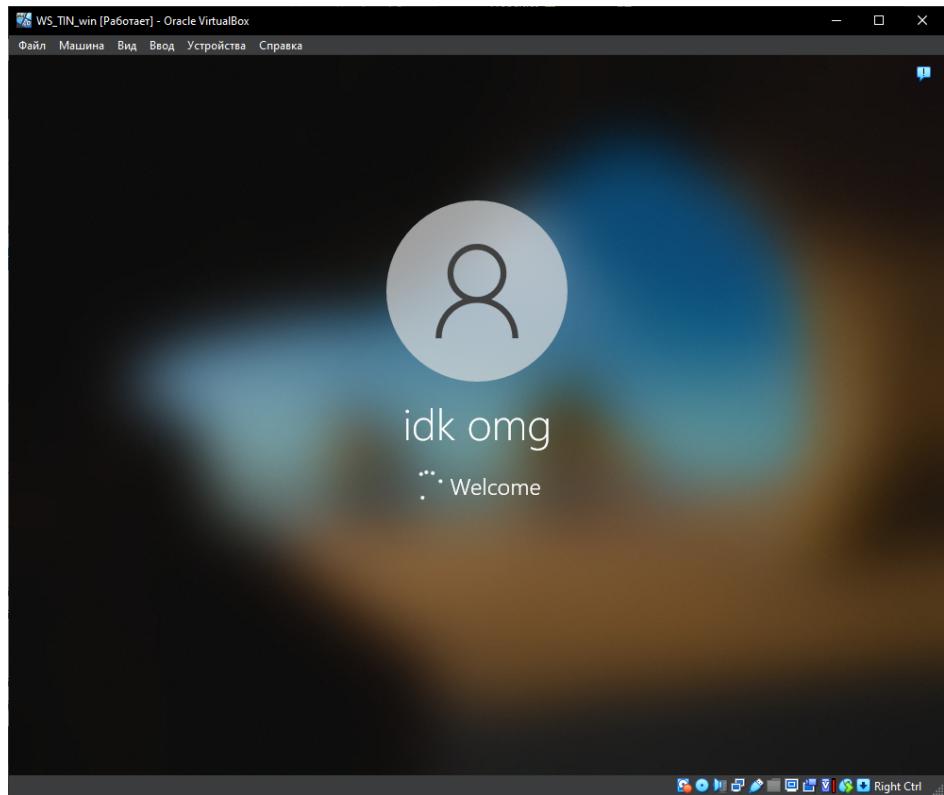


Рис. 1.29: Успешный вход в систему через ранее не авторизованного пользователя из домена с появлением интернет соединения с контроллером домена.

3. Заключение

Изучили типы учетных записей пользователей, ознакомились с основными принципами управления учетными записями. Изучили основные способы авторизации пользователей.

Так же научились настраивать контроллер домена и использовать его для разграничения доступа в подконтрольных операционных системах домена.

К сильным сторонам Active Directory (AD) в ОС Windows можно отнести централизованное управление, групповые политики, аудит и мониторинг, шифрование и резервное копирование.

В то же время к недостаткам можно отнести: единый центр отказа (в случае такой настройки), большая нагрузка на сеть LDAP трафиком, обширные возможности администратора домена.