|  |  |  |
| --- | --- | --- |
|  |  |  |
| МИНОБРНАУКИ РОССИИ | | |
| Федеральное государственное бюджетное образовательное учреждение  высшего образования  **«МИРЭА – Российскийтехнологическийуниверситет»**  **РТУ МИРЭА** | | |
| **Институт комплексной безопасности и специального приборостроения** | | |
|  |  |  |

Кафедра КБ-3 «Управление и моделирование систем»

**Отчет**

по дисципилне «Основы Информационной Безопасности»

Выполнил:

Студент 2 курса

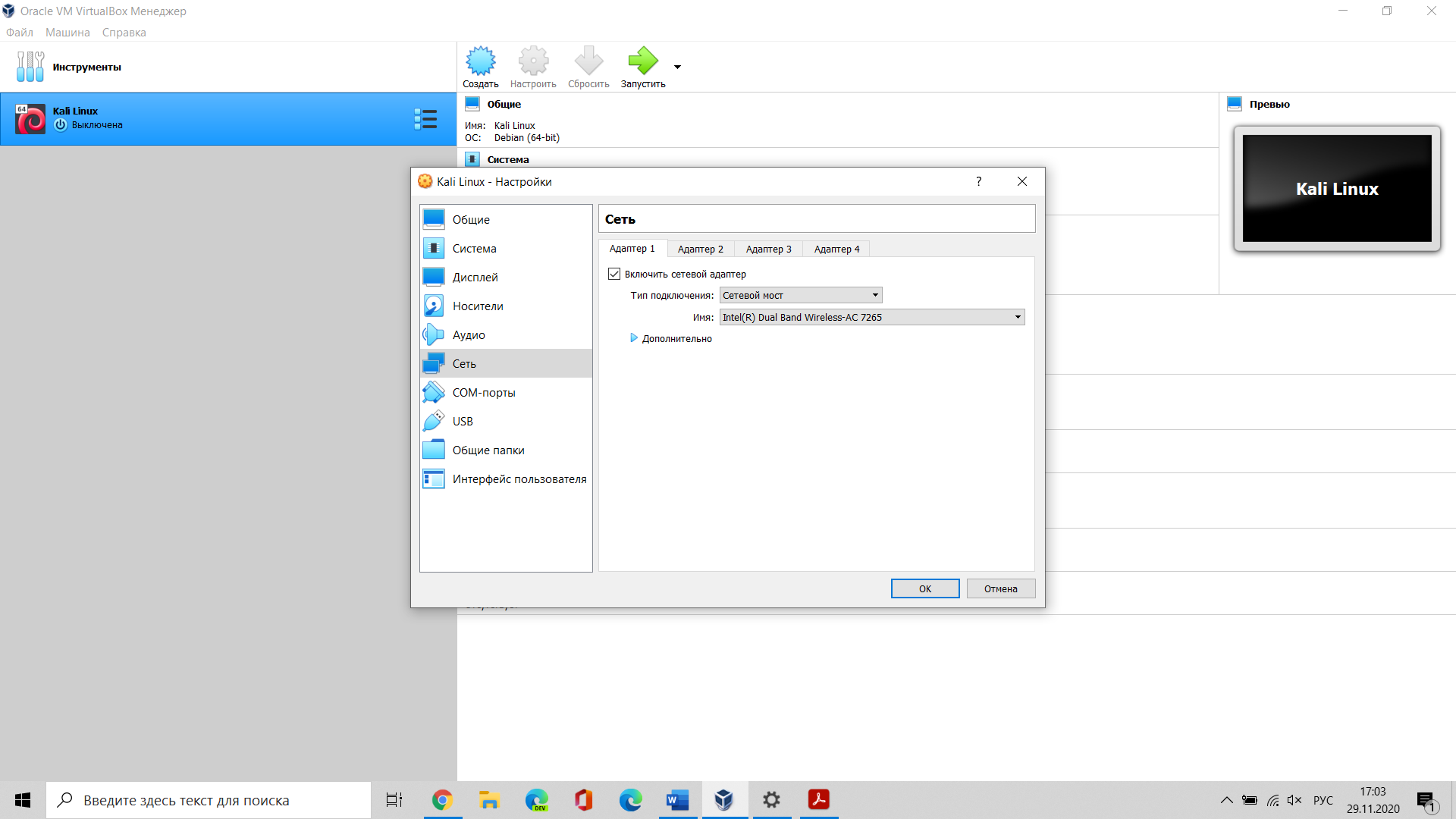
Группа БИСО-03-19

Шифр 19Б1391

Ветохин Станислав Кириллович

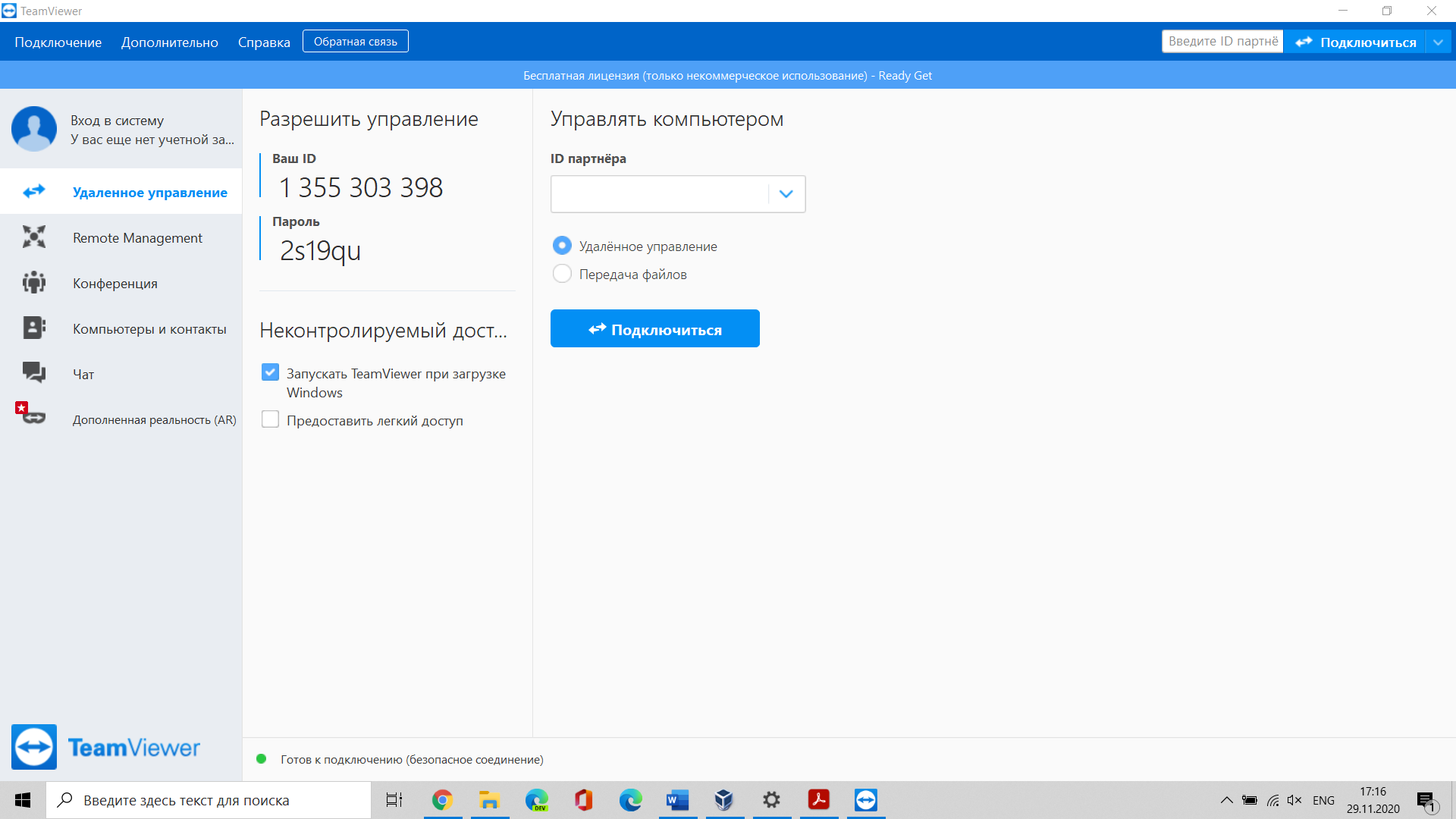
Москва, 2020

**Переведём сетевые адаптеры у виртуальных ОС в режим «Мост/Bridge»**



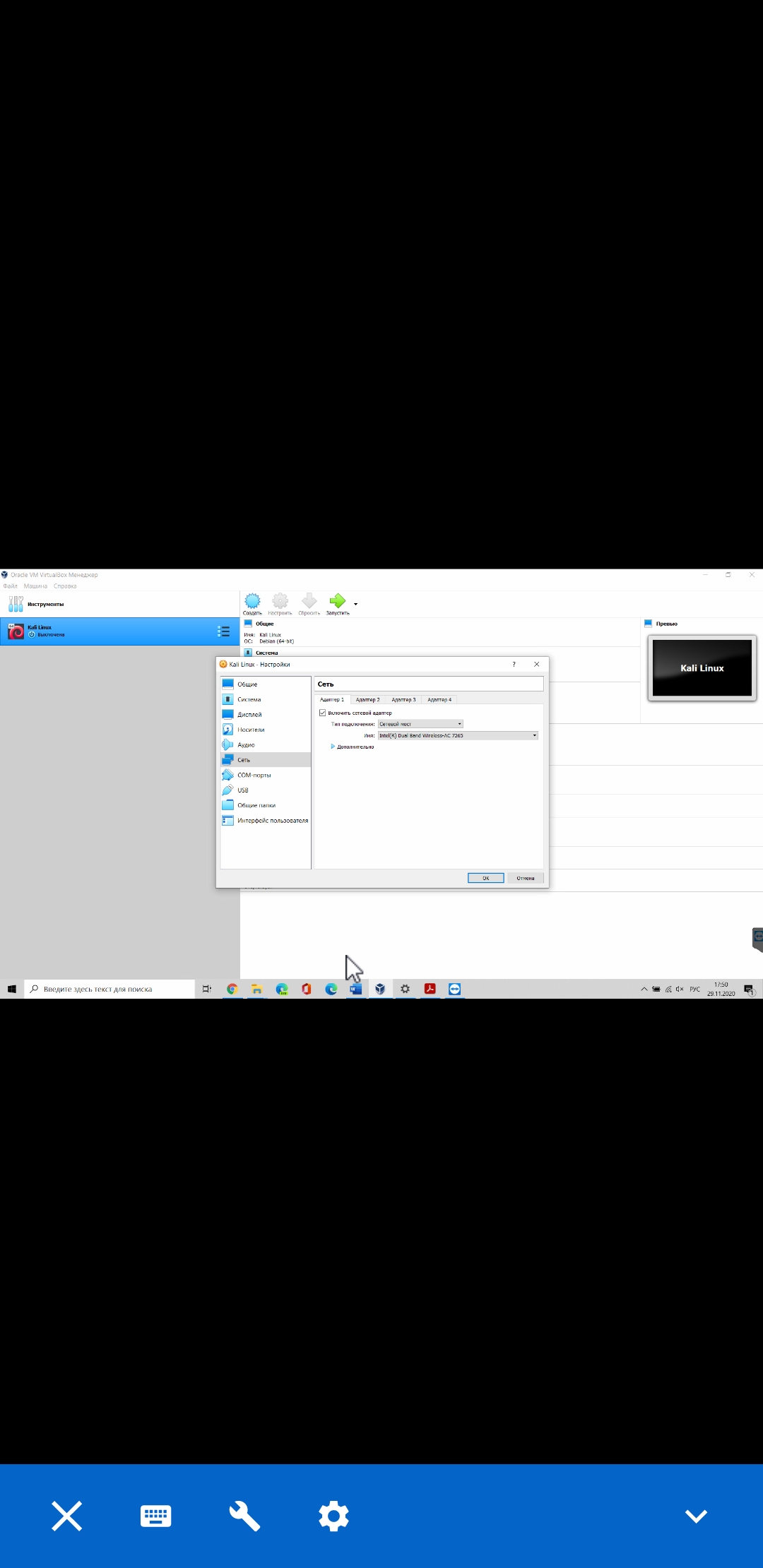
**TeamViewer**

Установим автозапуск программы:



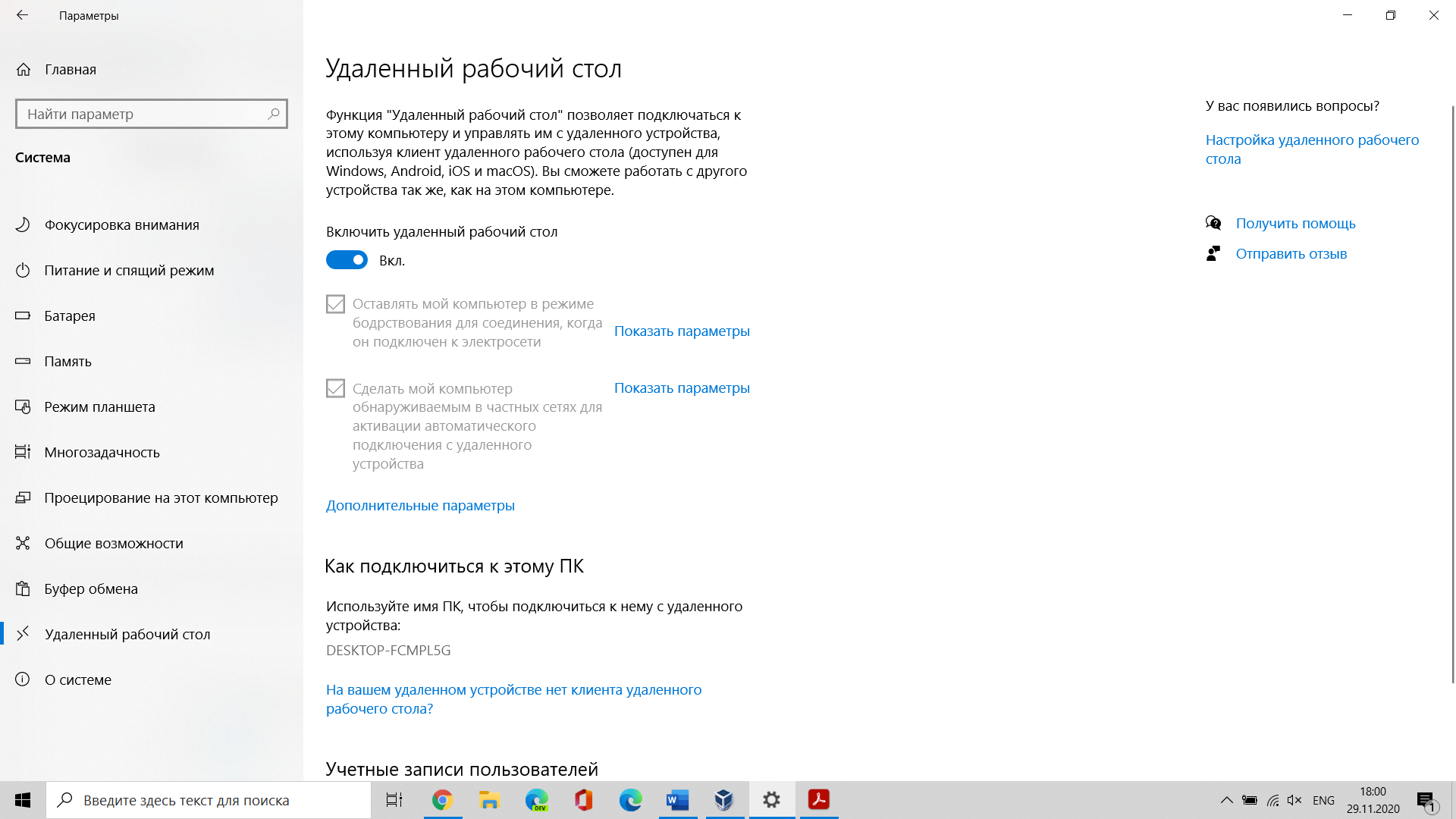
Зарегистрируемся, авторизуемся через мобильное устройство и подключимся

к компьютеру:

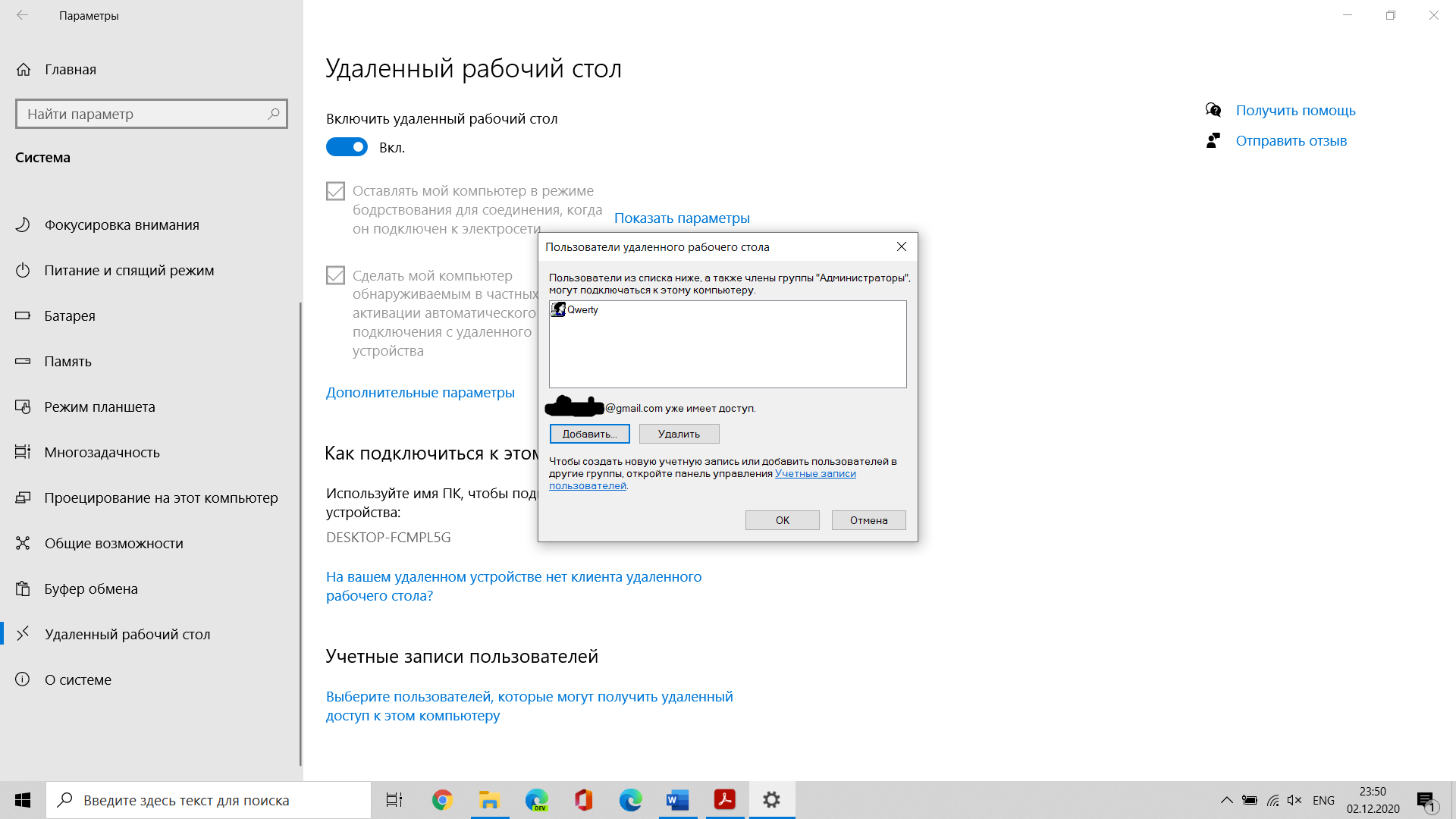


**RDP**

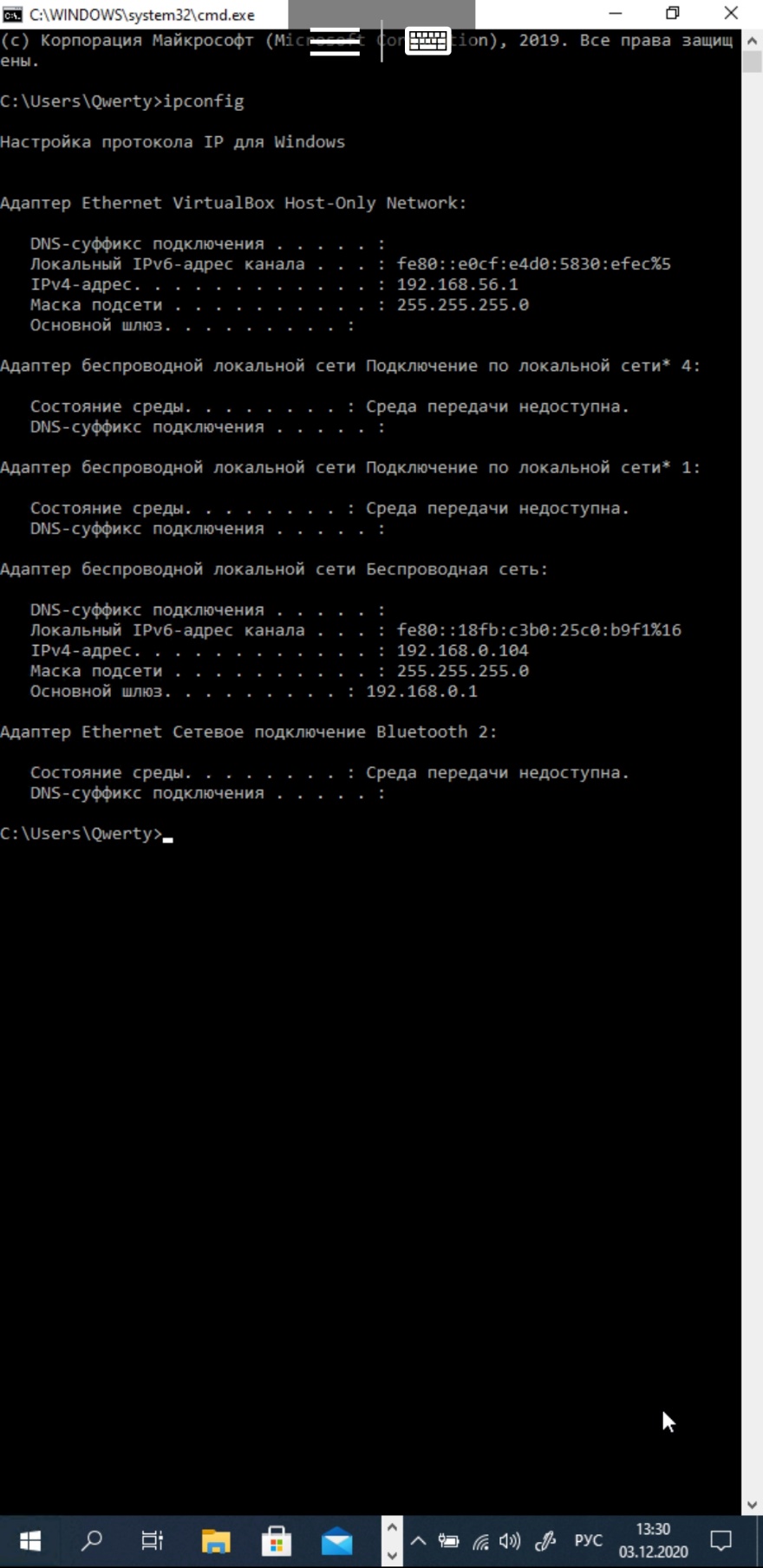
Включим удалённый рабочий стол:



Создадим пользователя и добавим его в меню «Удалённый доступ»:

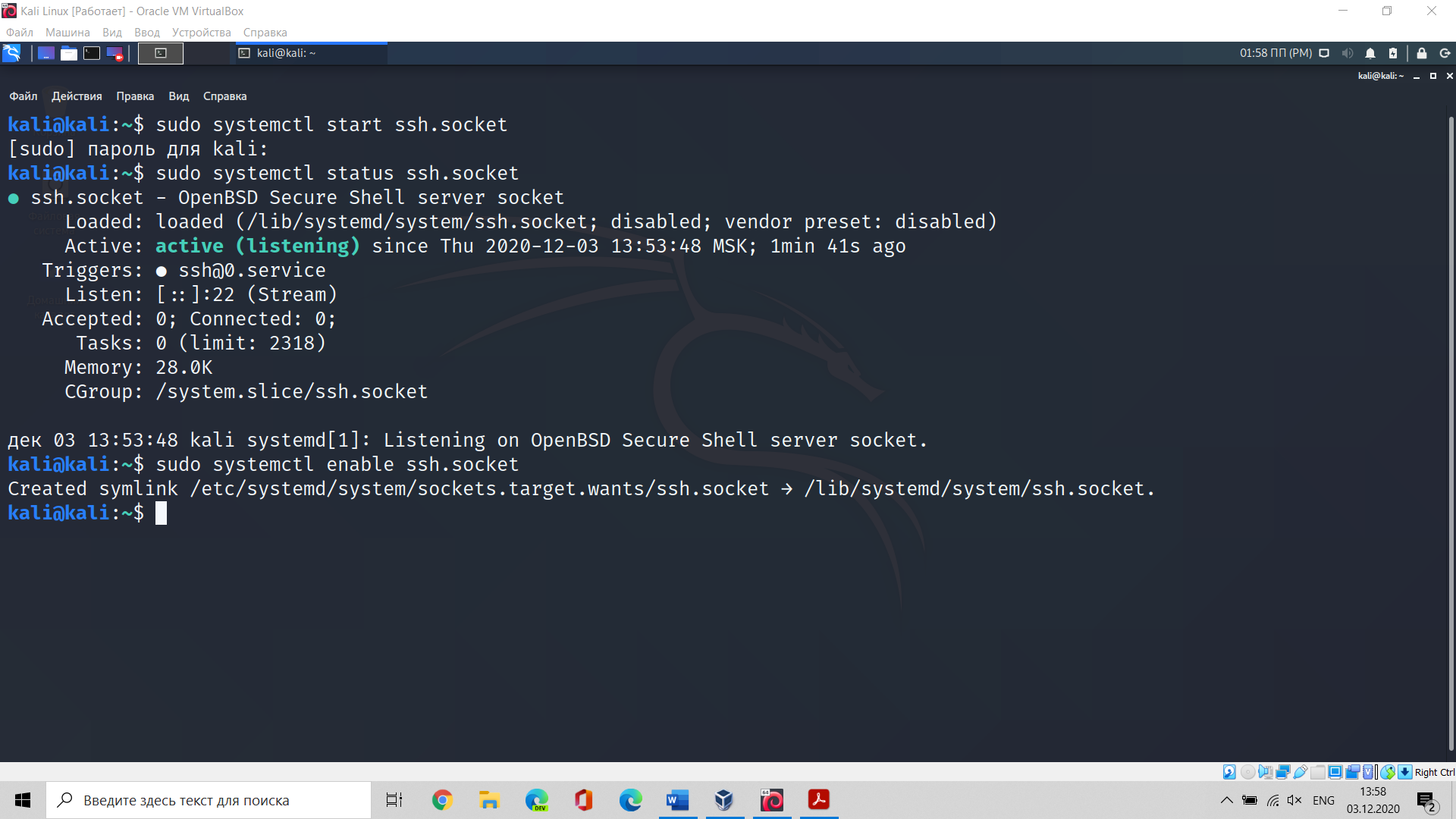


Подключимся через мобильное приложение Microsoft Remote Desktop:

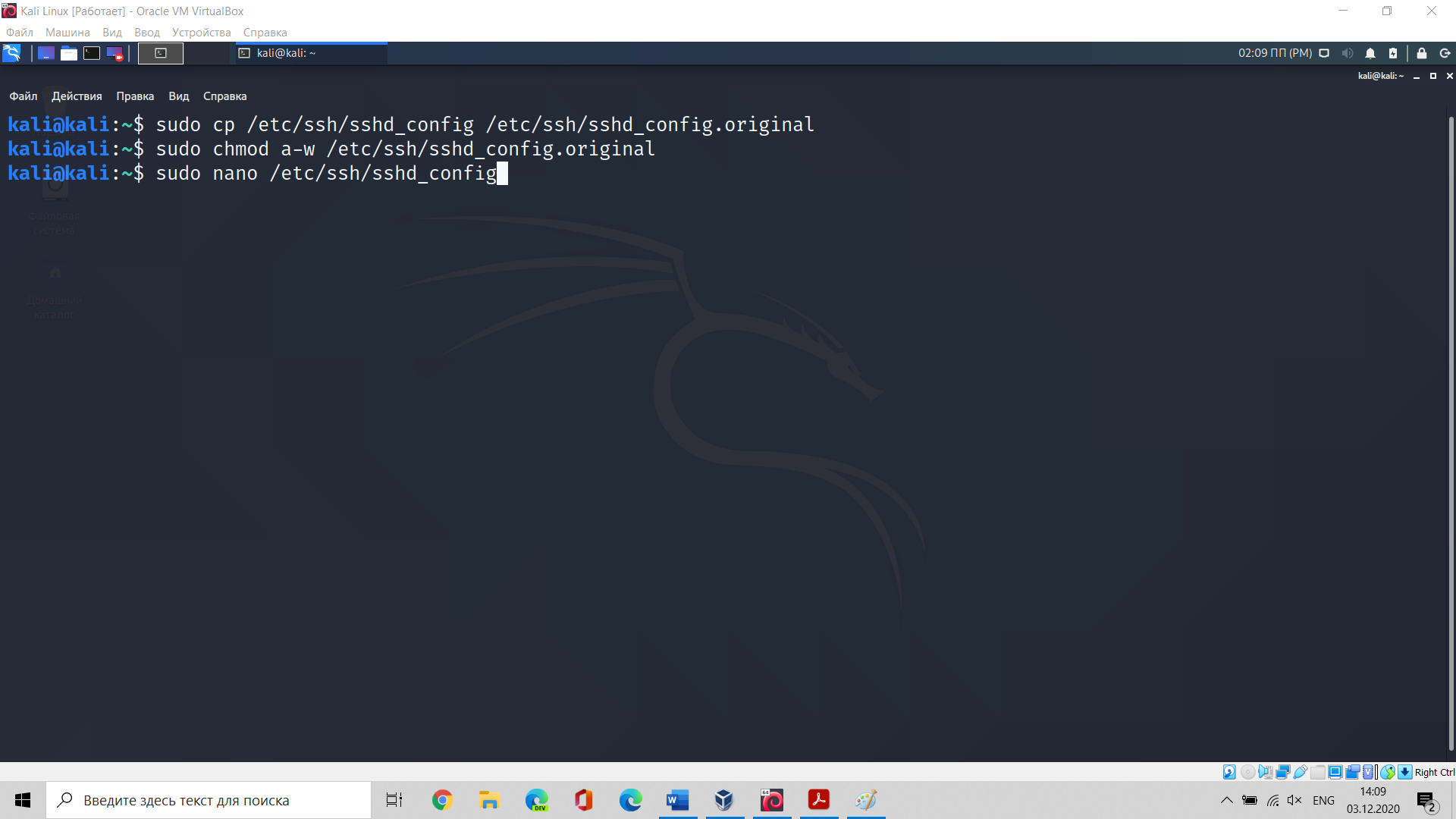


**SSH**

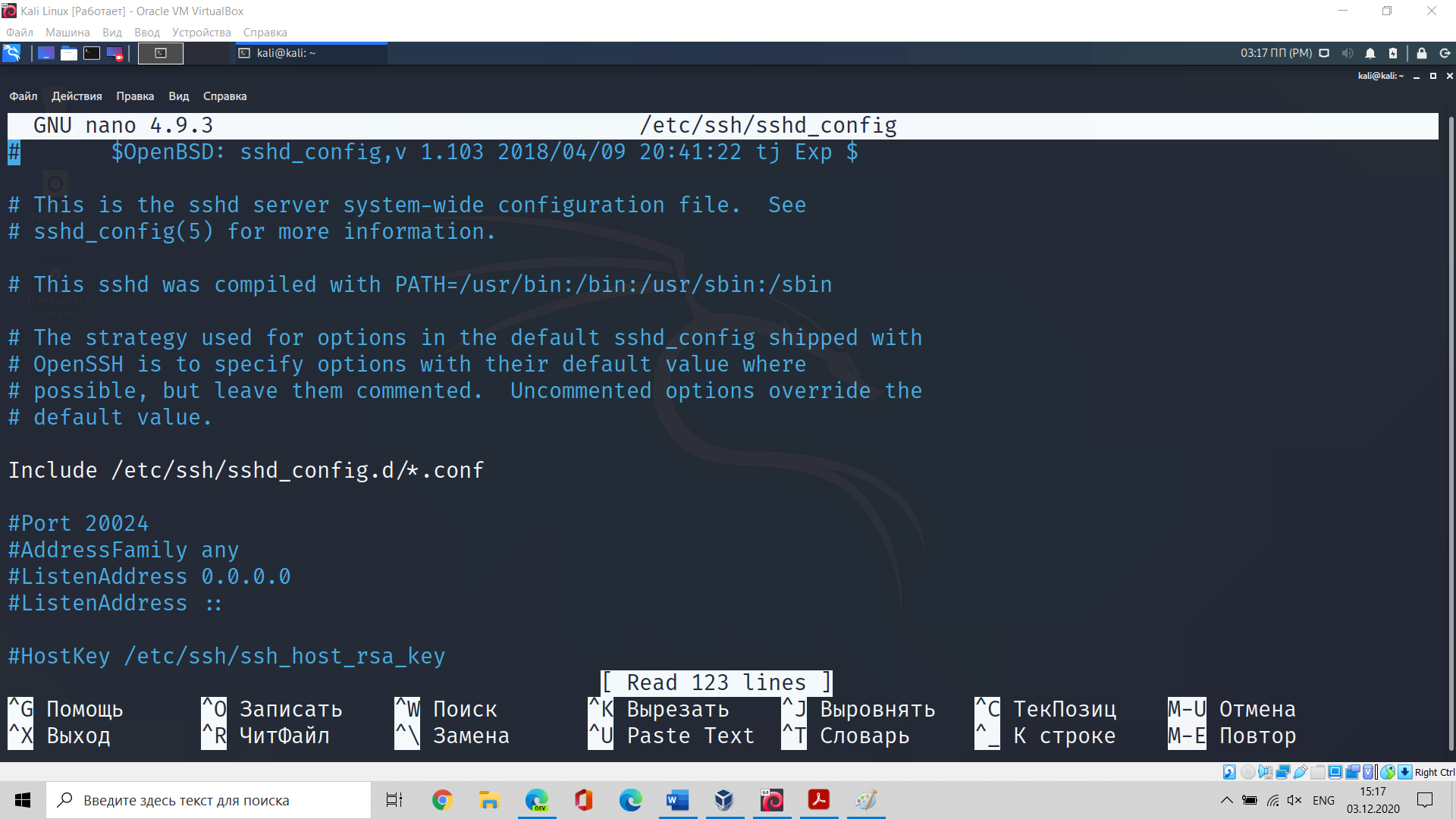
Запустим и проверим SSH, а после сделаем автоматический запуск:



Сделаем копию файла и поставим защиту от записи:

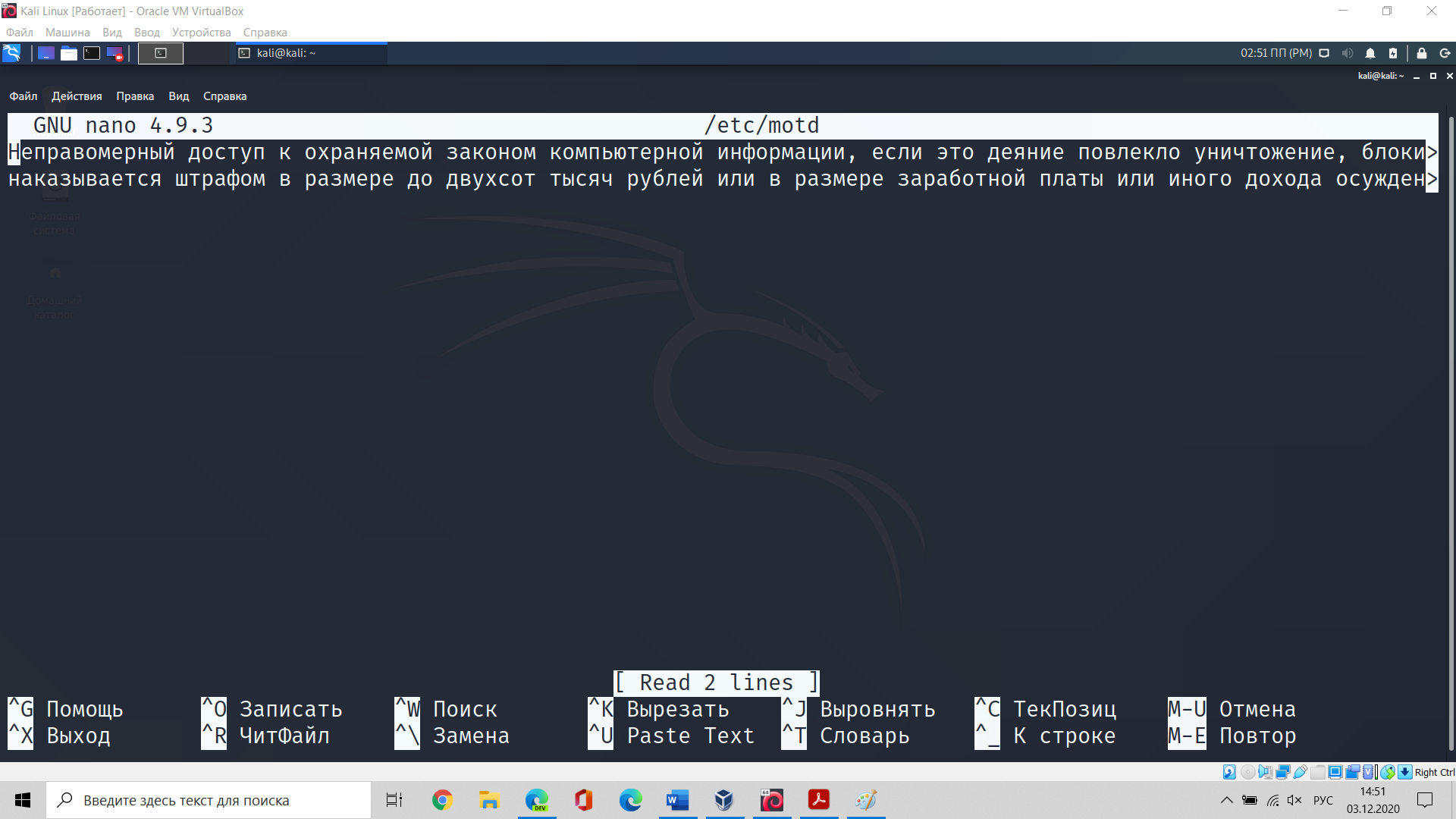


Изменим файл sshd\_config:

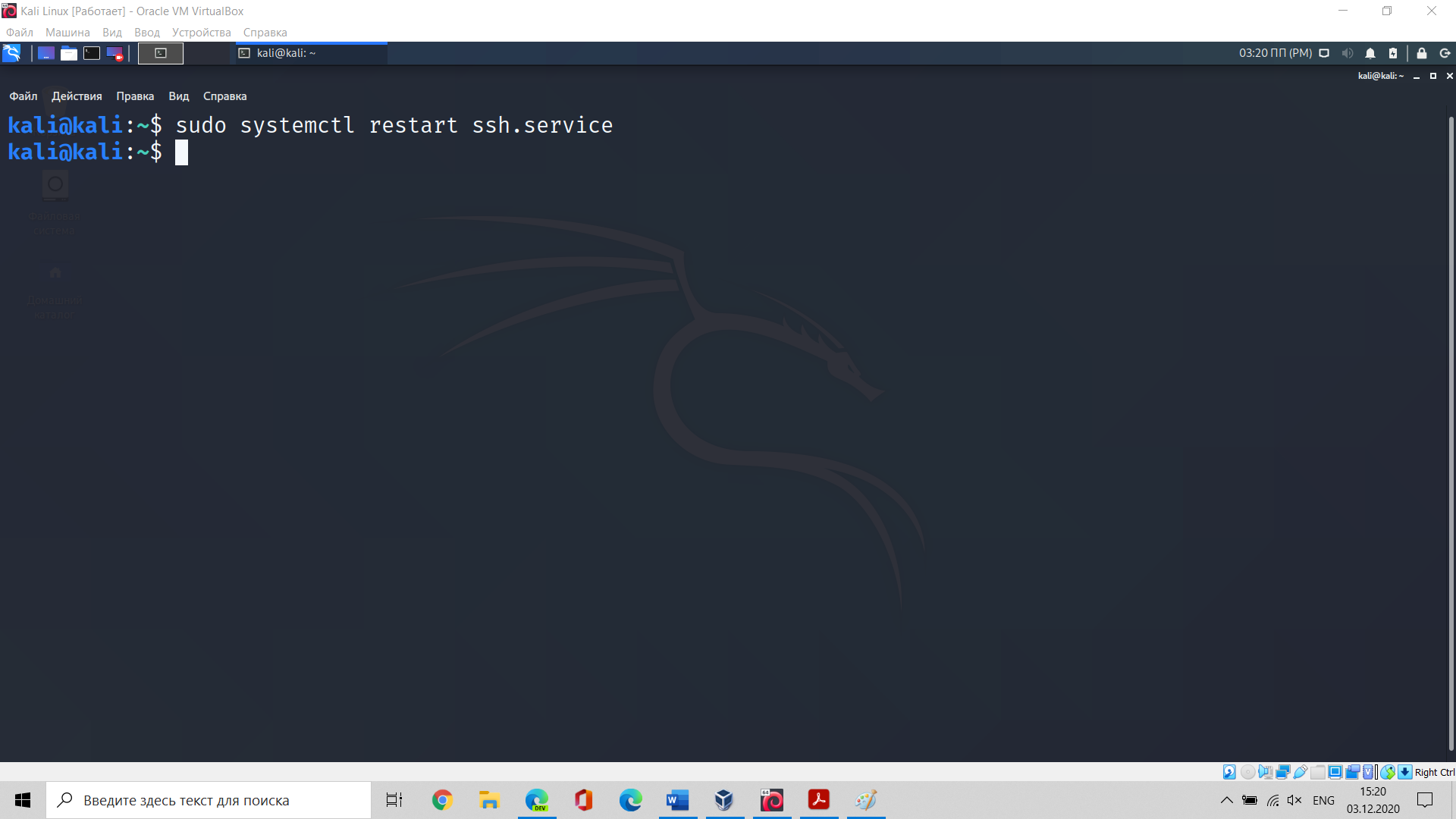


В файле issue.net изменим баннер:

В файле motd изменим приветственное сообщение:



Перезапустим сервис ssh.service:



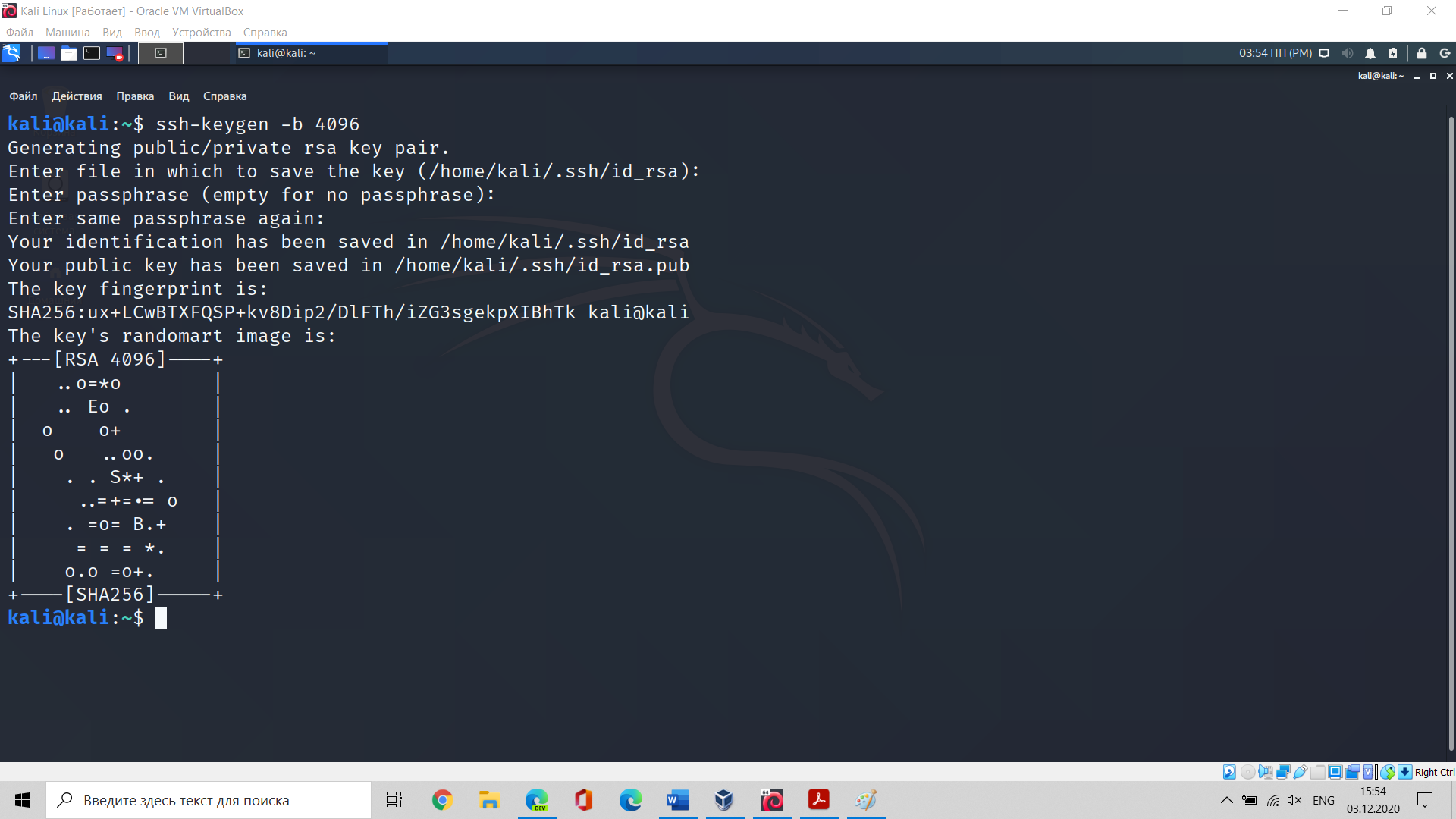
Проверим функционирование данного сервиса:



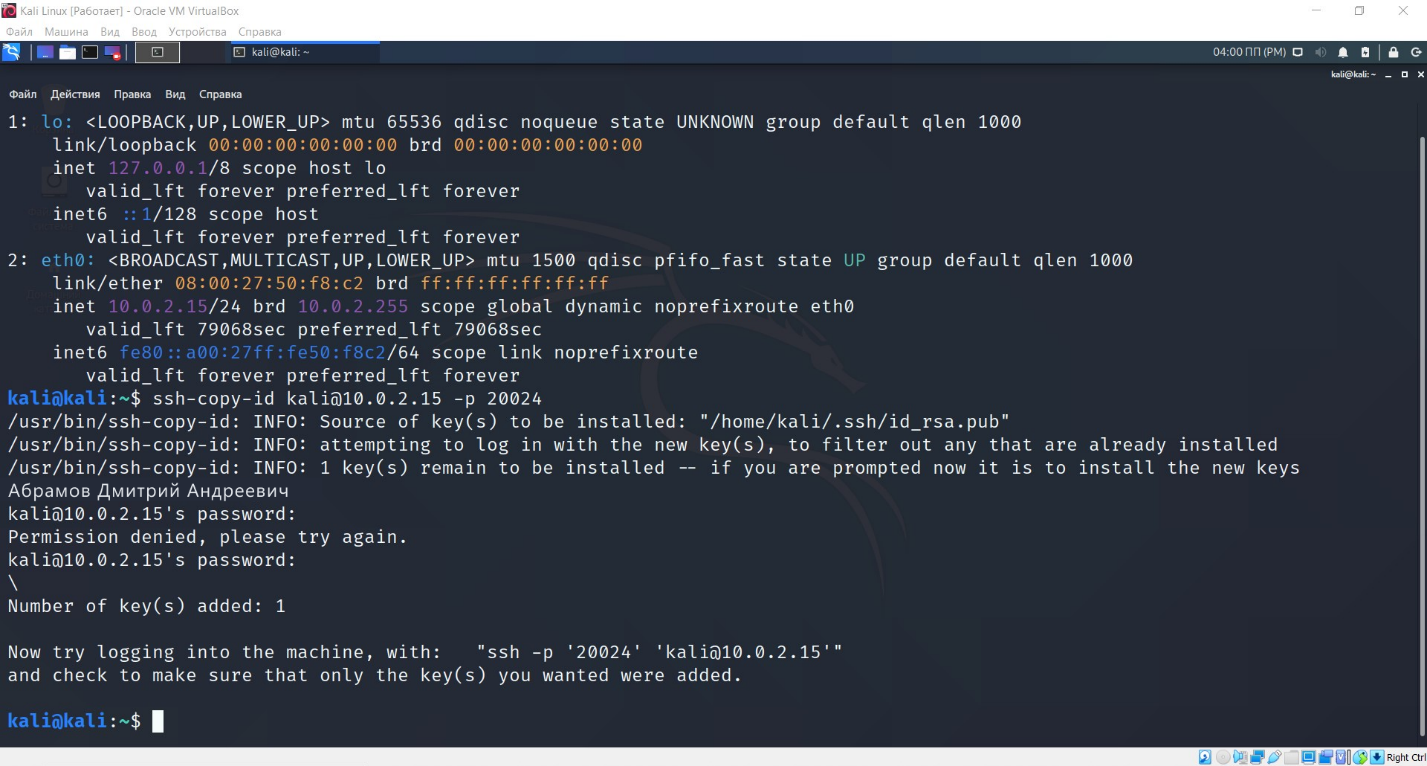
Подключимся к удалённому серверу:



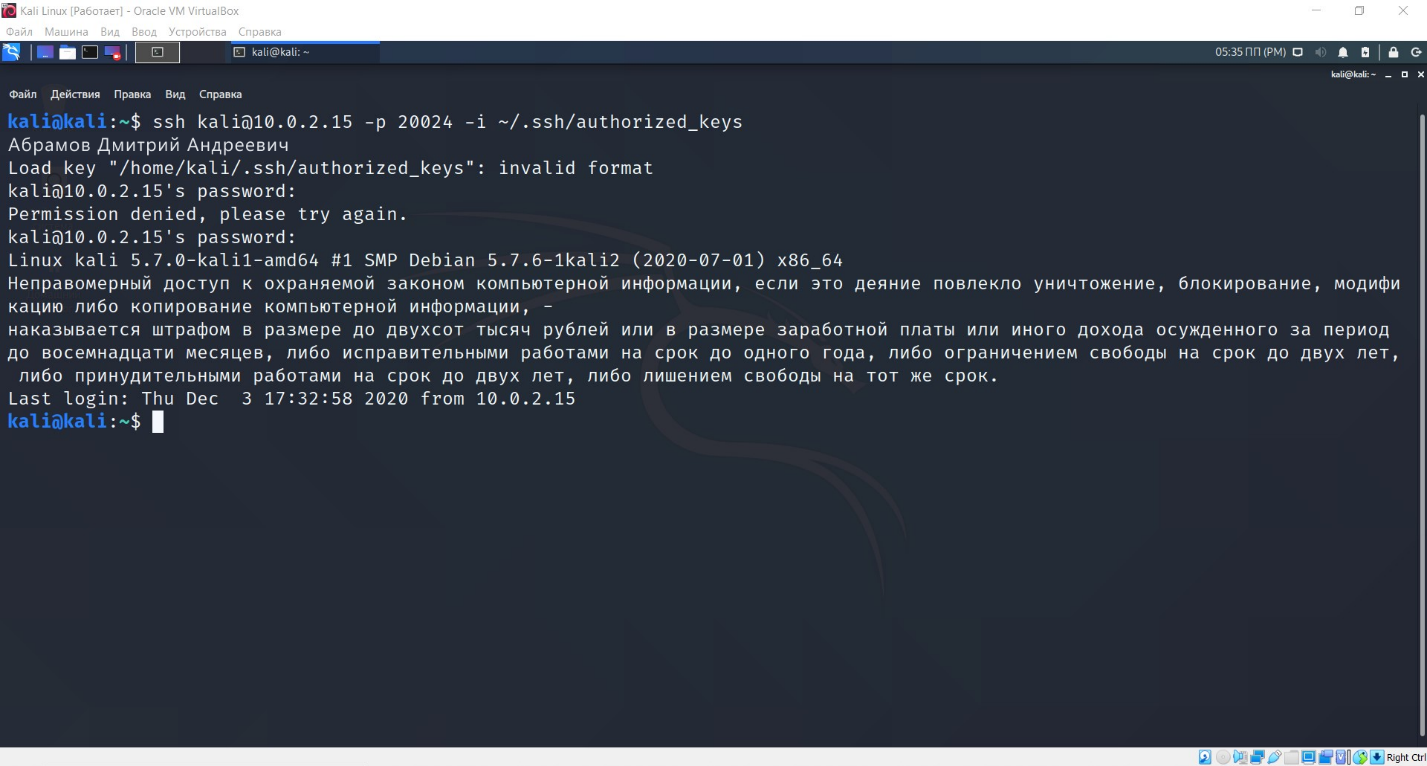
Сгенерируем 4096 битный ключи:



Скопируем публичный ключ:



Авторизация:



Отключим возможность входа на сервер по паролю:

