Цель практической работы

Вы научитесь анализировать логи внешнего сервиса.

Анализ лог-файлов — важное умение для сетевого администратора. При устранении любых инцидентов правильно проведённый анализ поможет точно определить причину сбоя. После этого вы сможете подобрать варианты решения.

За периметром сети анализ логов помогает выявлять и своевременно пресекать попытки компрометации внешних сервисов.

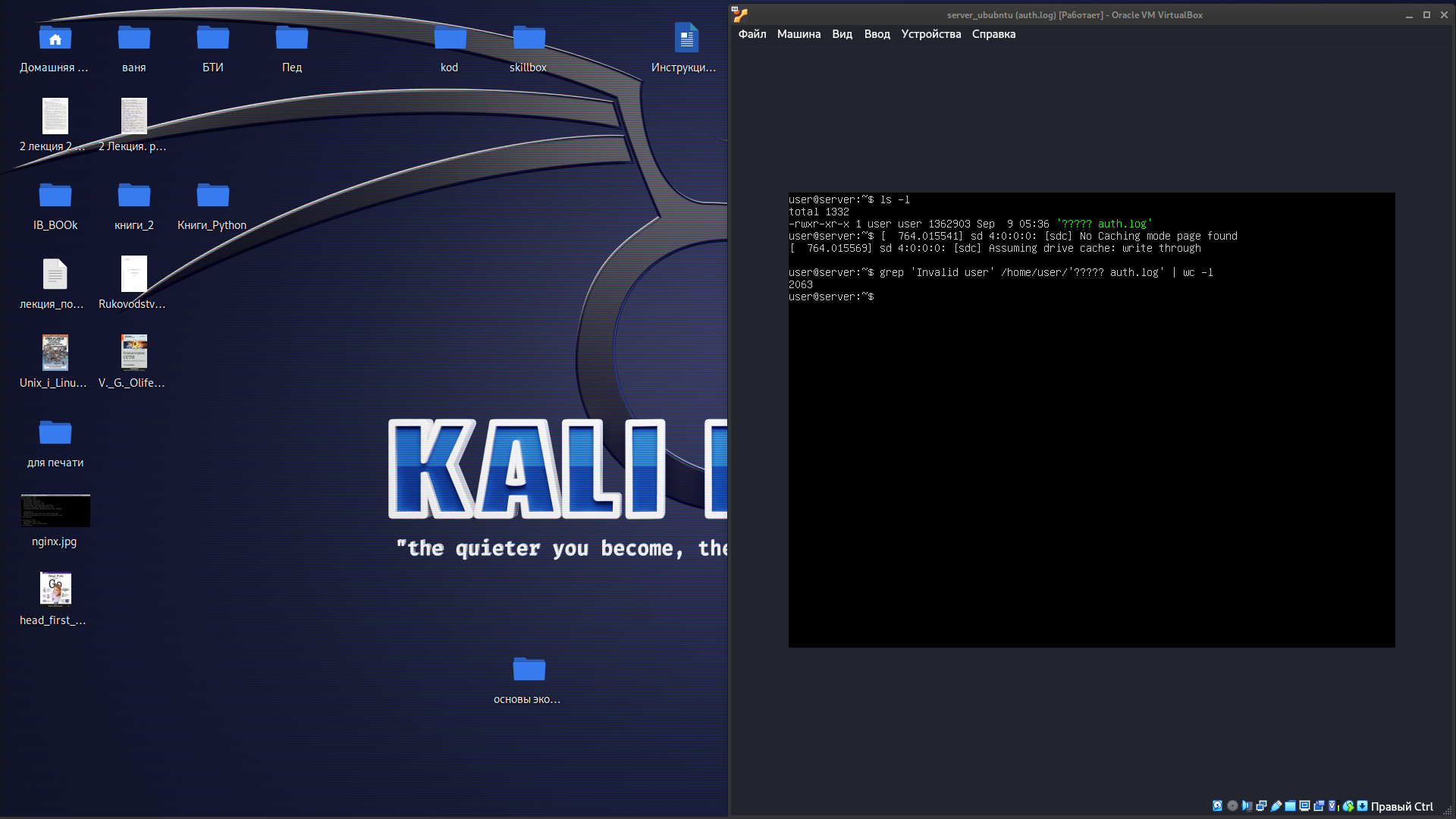
**Задание 1. Попытки компрометации внешнего SSH-сервера**

Скопировал [предоставленный лог-файл](https://drive.google.com/file/d/1p20nfrsGeKhUcRD58muYGI-F5jGMvPzO/view?usp=sharing) в свой Linux-сервер.

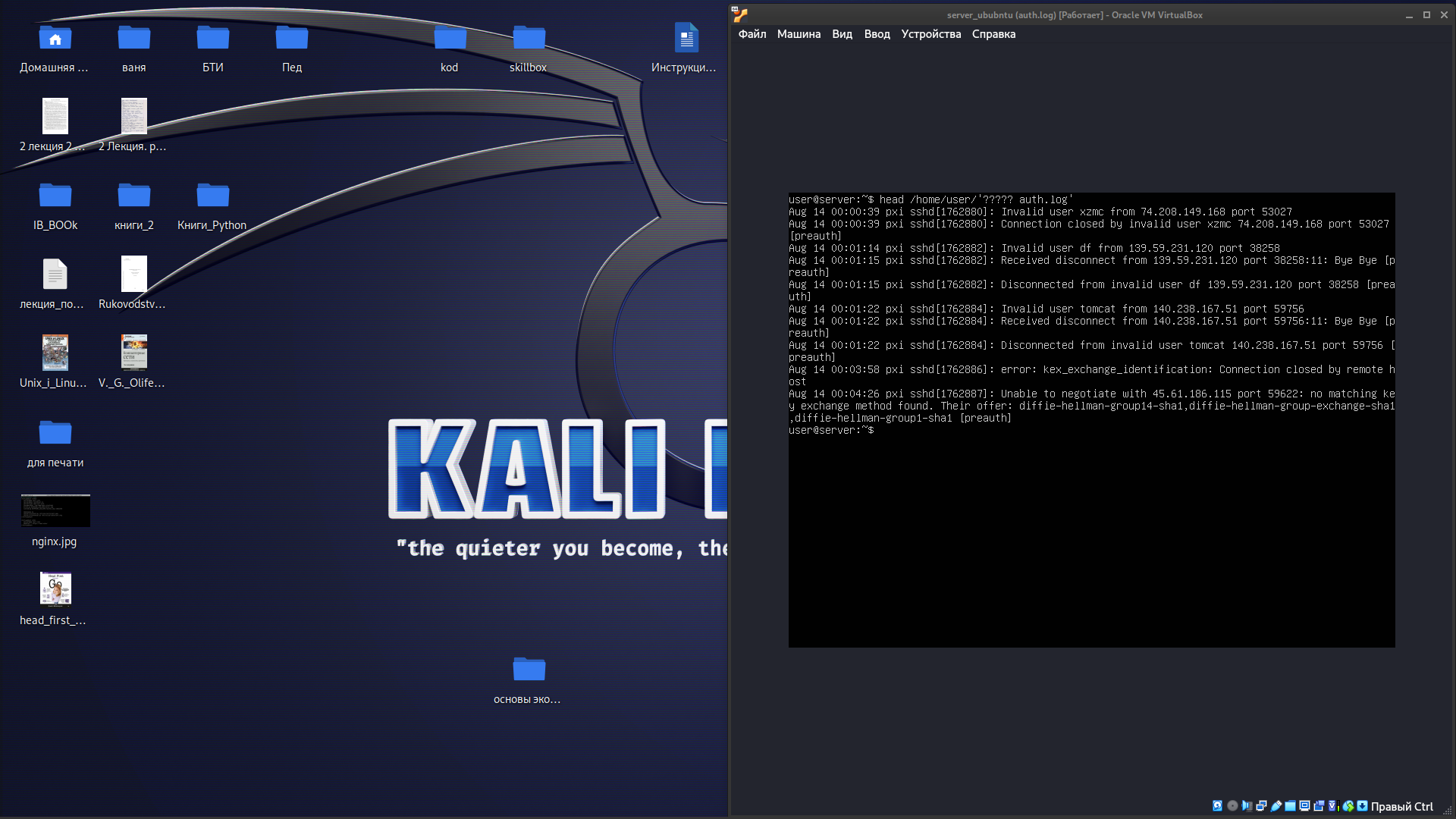


Выполнил анализ этого файла с помощью текстовых утилит grep, wc, head и tail-анализ файла, чтобы получить следующие значения:

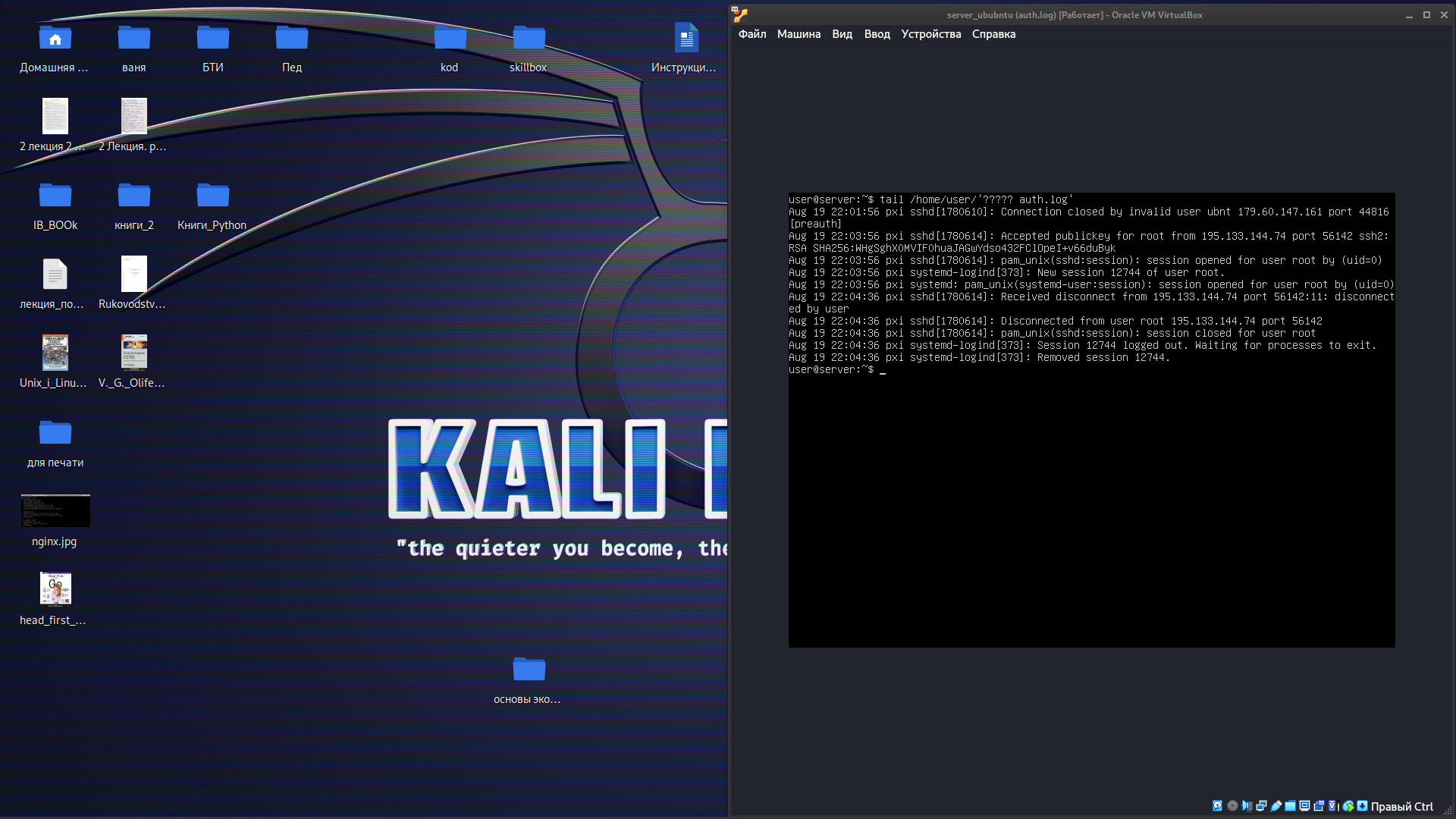
Число строк, содержащих паттерн Invalid user.



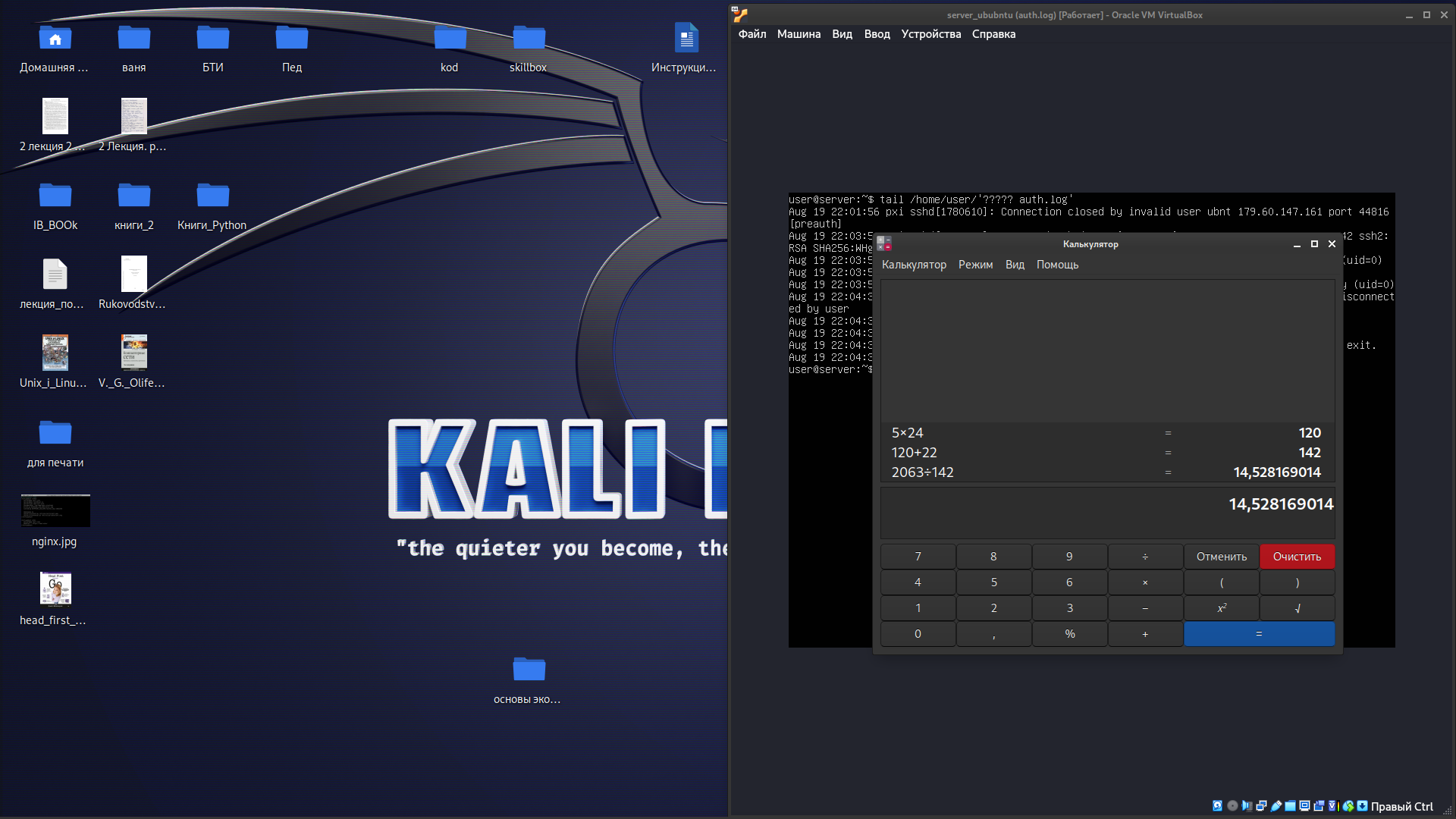
Дата и время первой записи в файле.



Дата и время последней записи в файле.

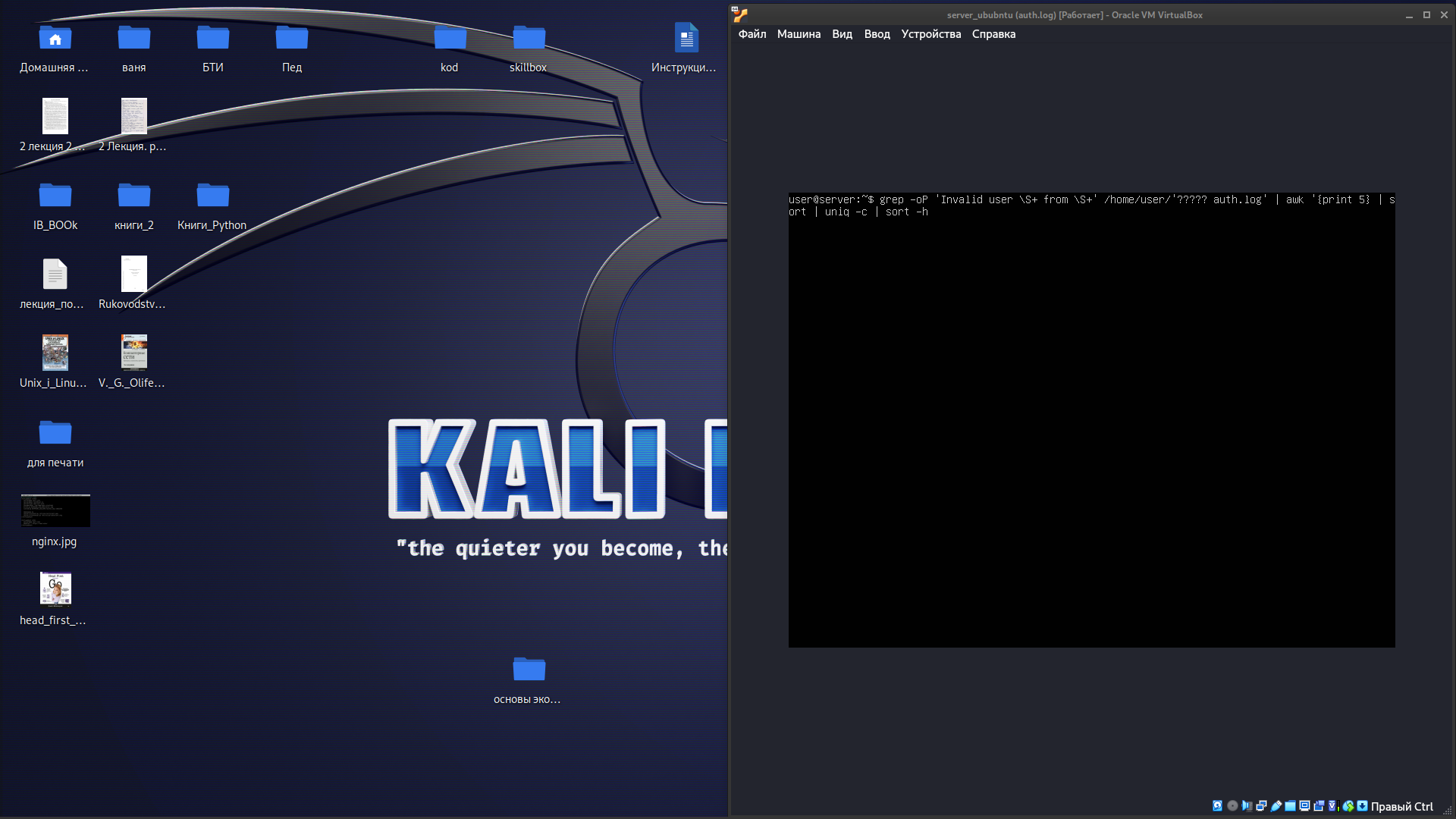


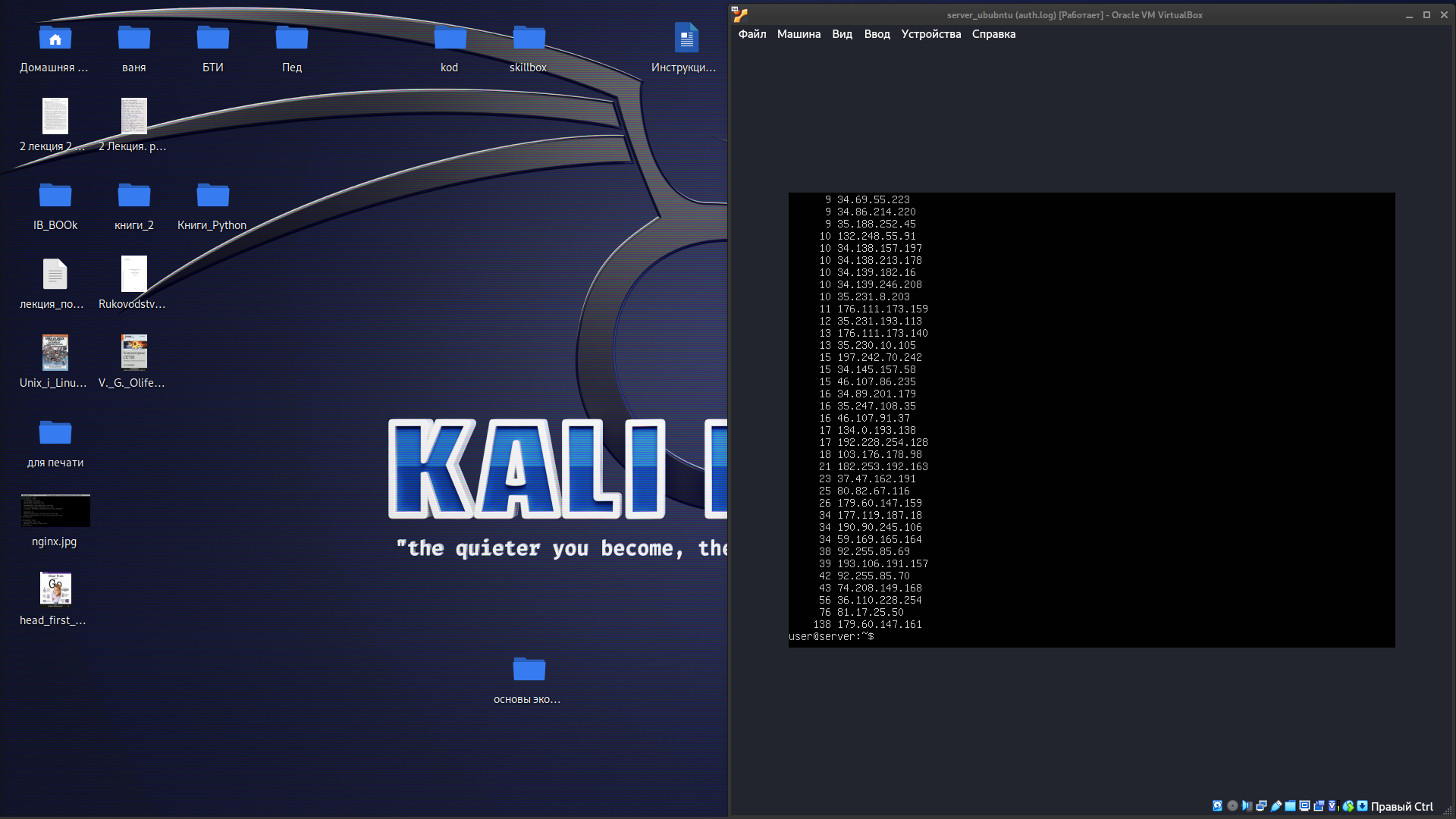
Вычислите из полученных значений среднее число атак в час.



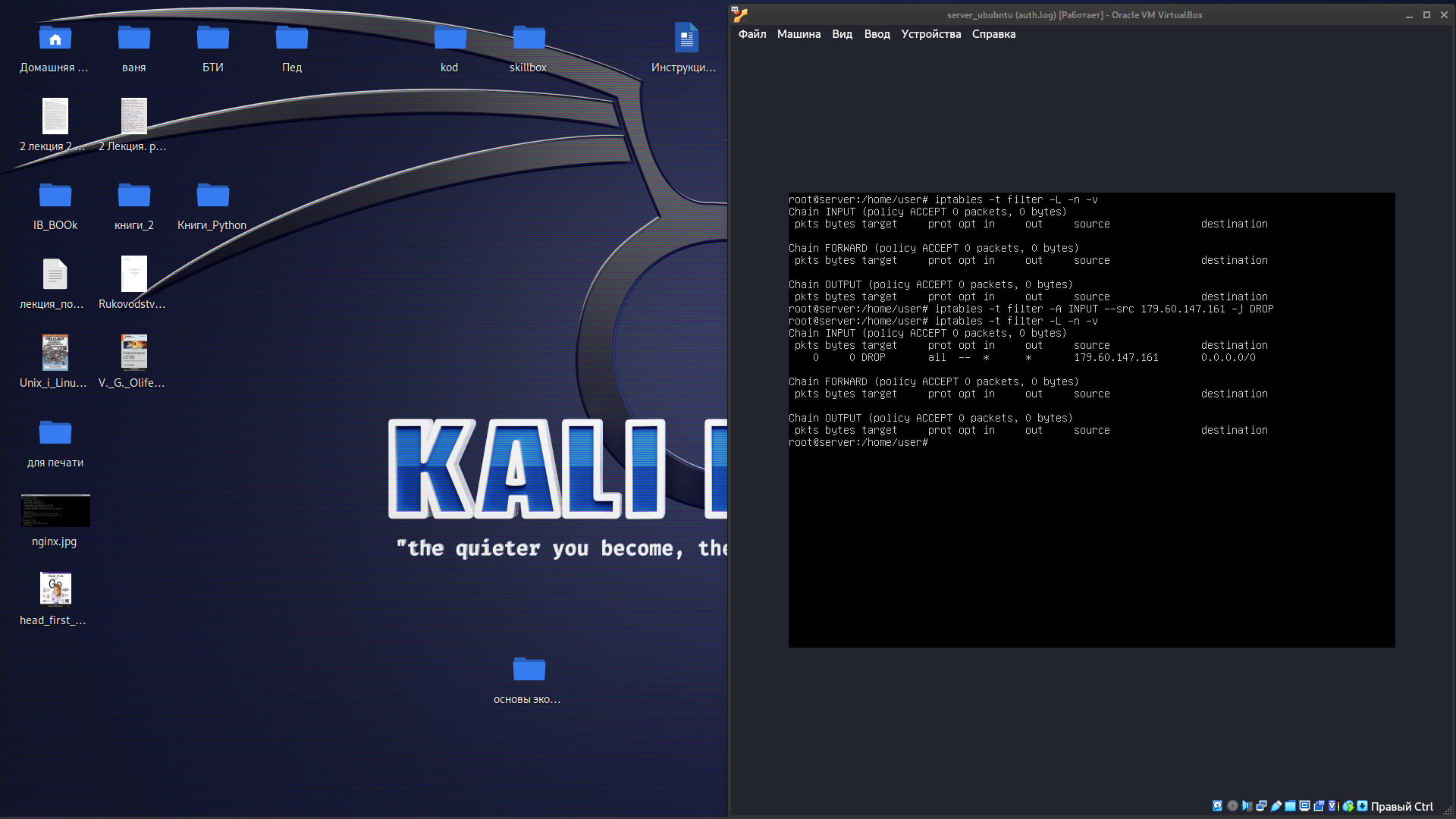
**Задание 2. Определение IP-адреса**

С помощью текстовых утилит grep, awk, sort и uniq получил из файла [auth.log](https://drive.google.com/file/d/1p20nfrsGeKhUcRD58muYGI-F5jGMvPzO/view?usp=sharing) IP-адреса атакующих и число попыток в табличном виде.Зафиксировал текст всей строки команды, которая выводит такие данные.





Сделал скриншот нижней части таблицы.Зафиксировал IP-адрес, с которого было больше всего атак.



IP-адрес, с которого было больше всего атак: 179.60.147.161