

**МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МИРЭА – Российский технологический университет»**

|  |
| --- |
| **РТУ МИРЭА** |
|  |
| **Институт кибербезопасности и цифровых технологий (ИКБ)** |
|  |
| КБ-2 «Информационно-аналитические системы кибербезопасности» |

**ОТЧЕТ О ВЫПОЛНЕНИИ ИНДИВИДУАЛЬНОГО ЗАДАНИЯ №4**

# **В РАМКАХ ДИСЦИПЛИНЫ «ТЕХНОЛОГИИ ХРАНЕНИЯ В СИСТЕМАХ КИБЕРБЕЗОПАСНОСТИ»**

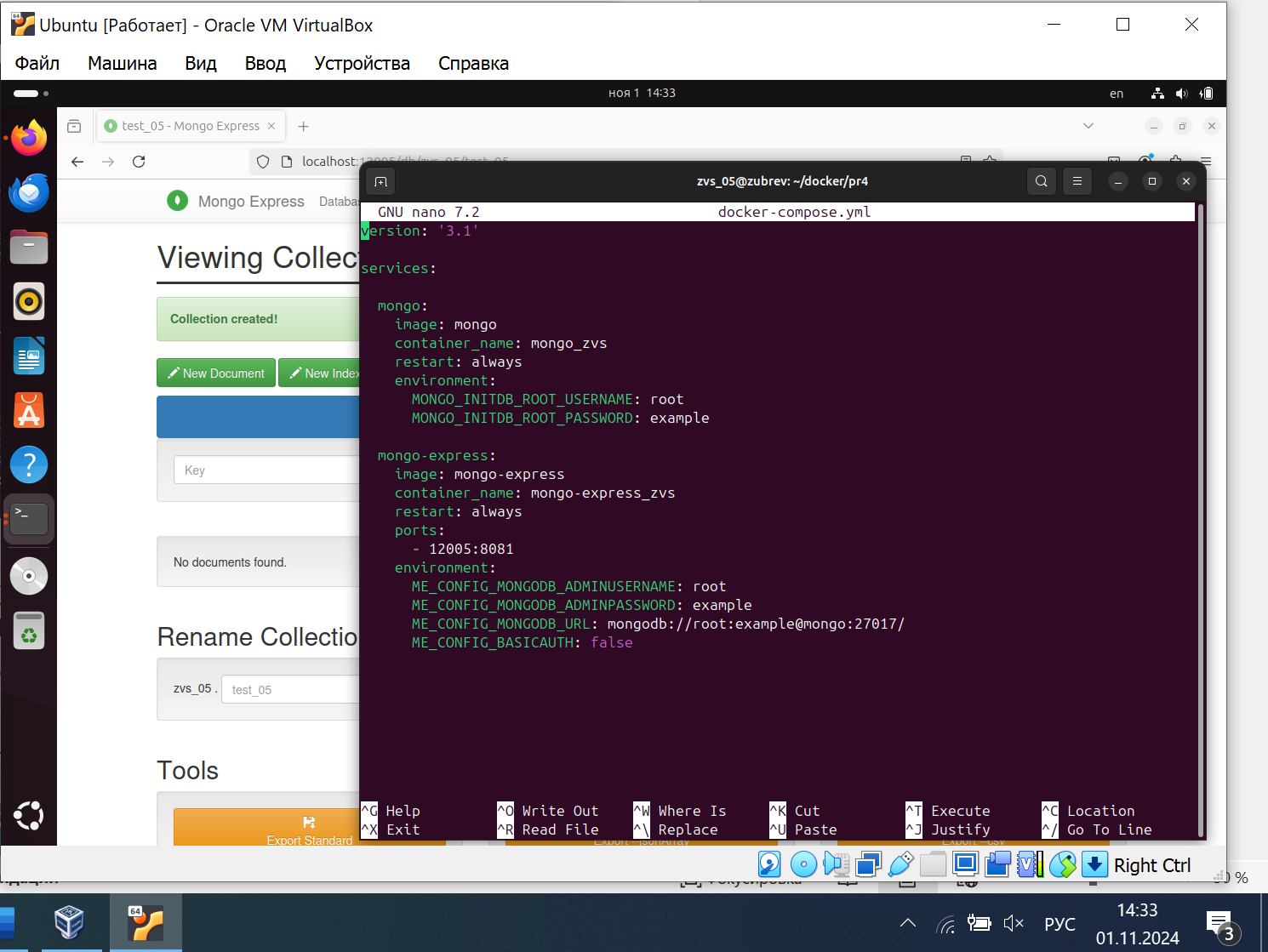
Выполнил:

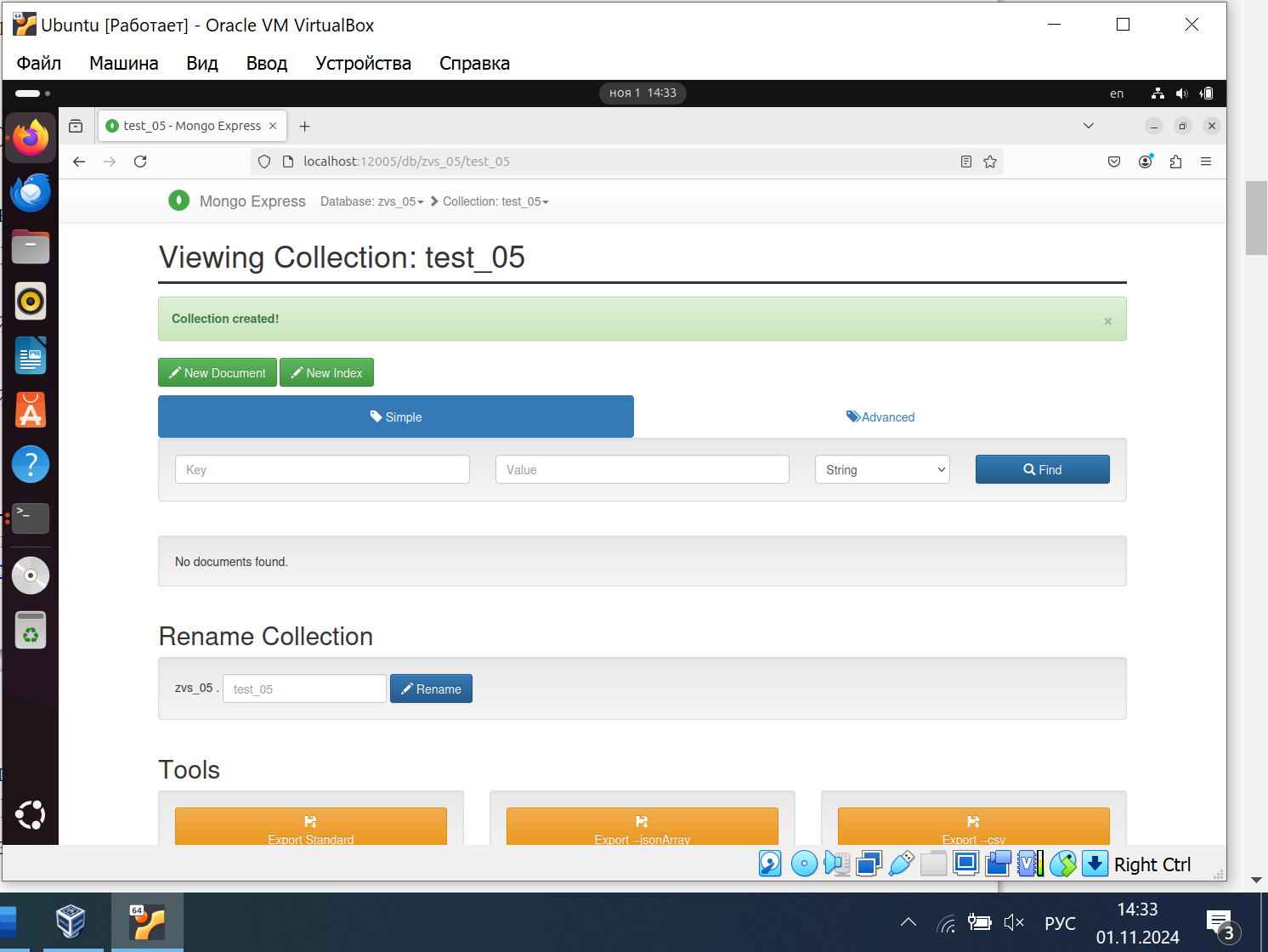
Студент 3-ого курса

Учебной группы БИСО-02-22

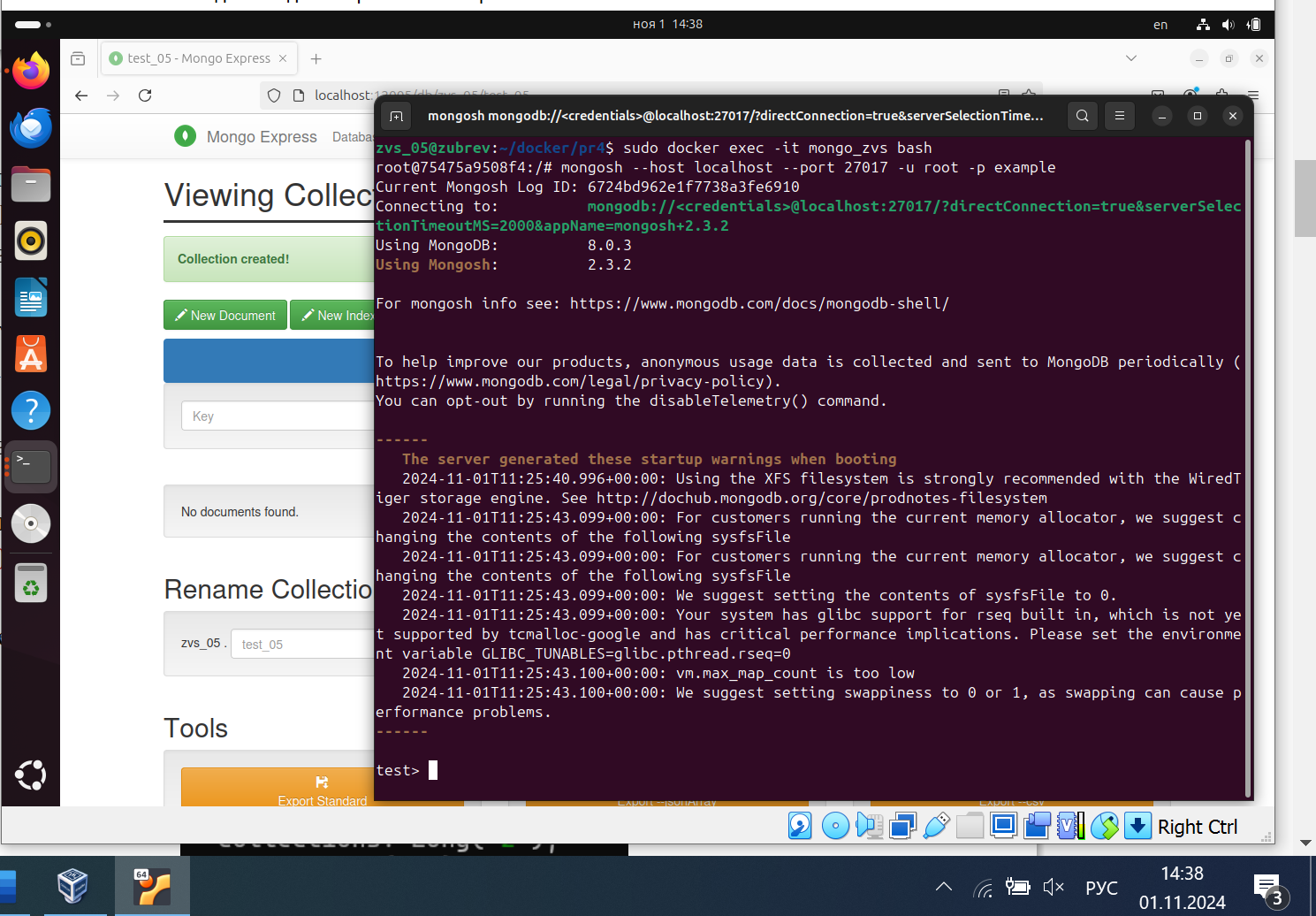
Зубарев В.С.

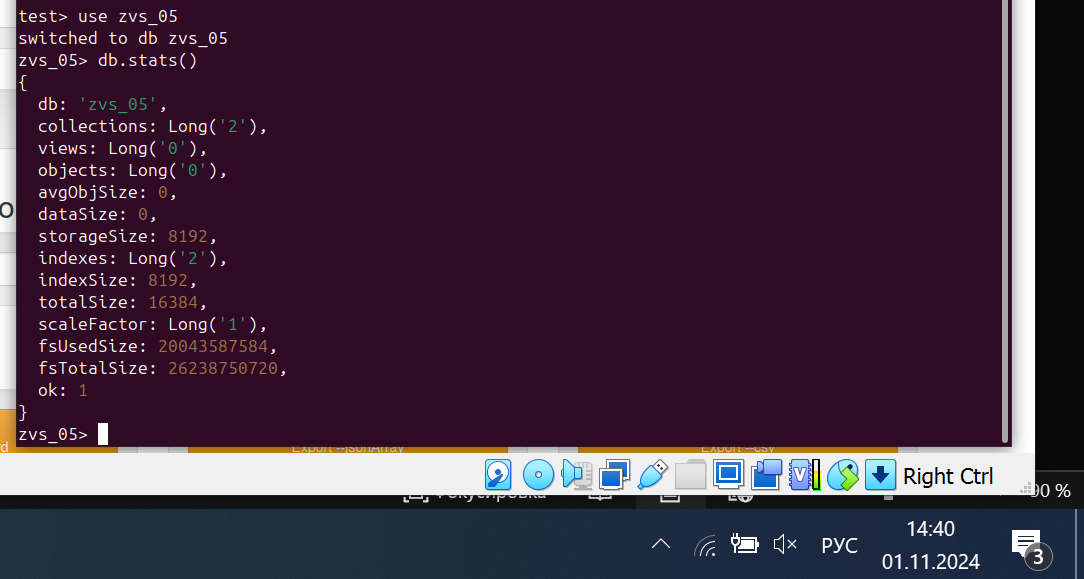
Разверните MongoDB и Mongo Express с помощью Docker Compose.



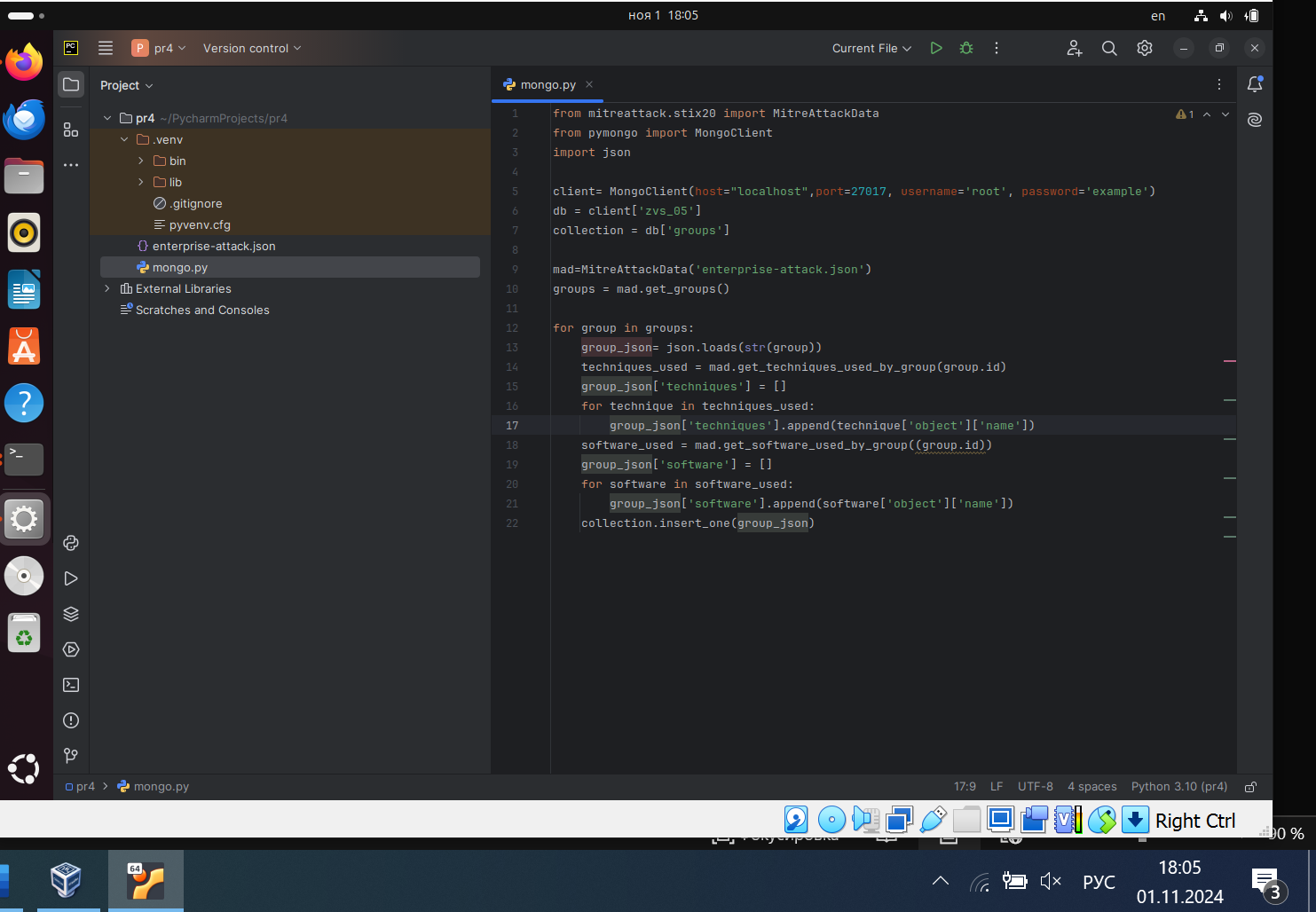


Зайдите в контейнер MongoDB с помощью команды docker execВыйти из контейнера можно с помощью команды exit.

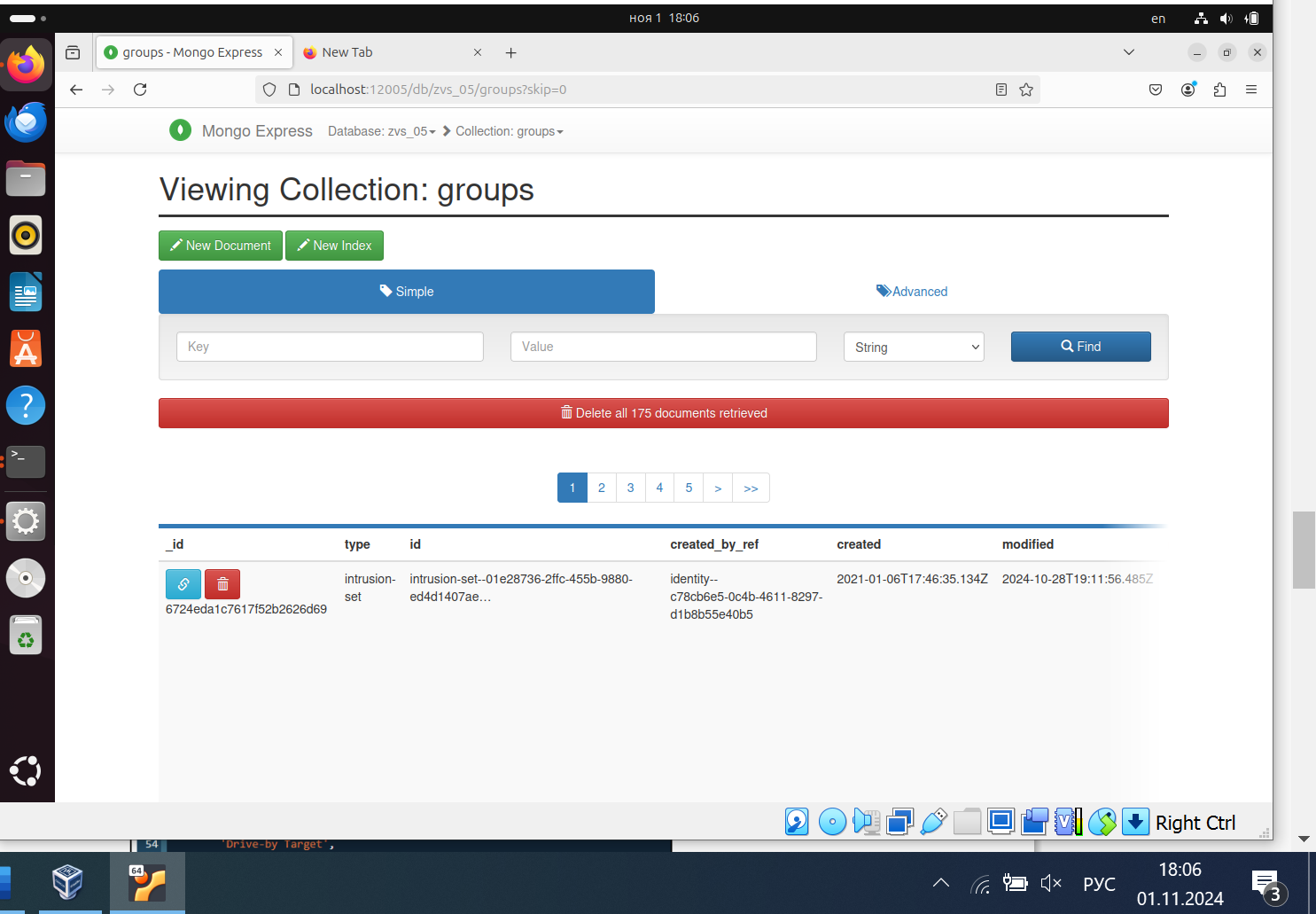


Подключитесь к ранее созданной БД. Пример: use ipd\_07. Проверьте, что все корректно работает. Например, командой db.stats():

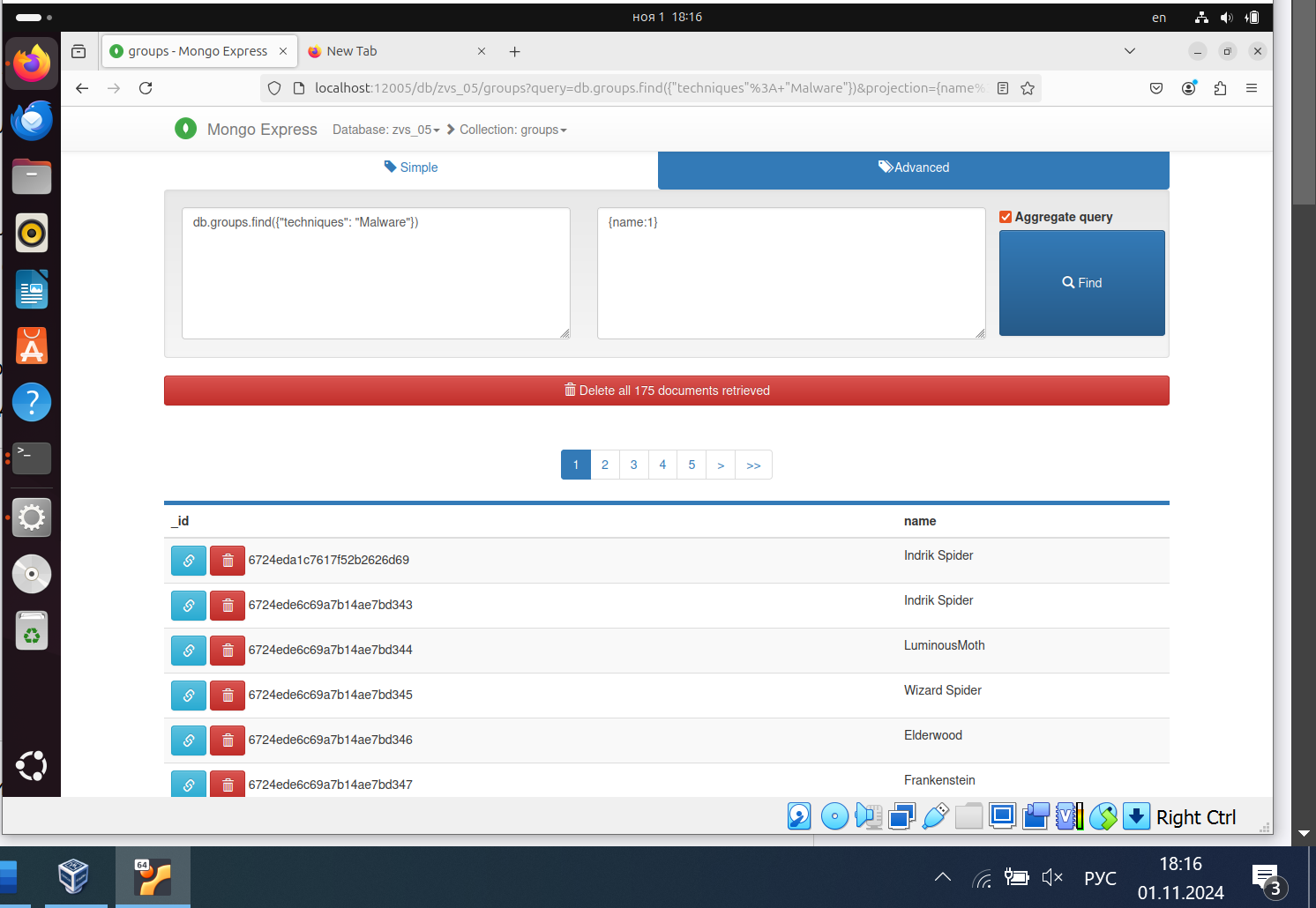
Напишите скрипт



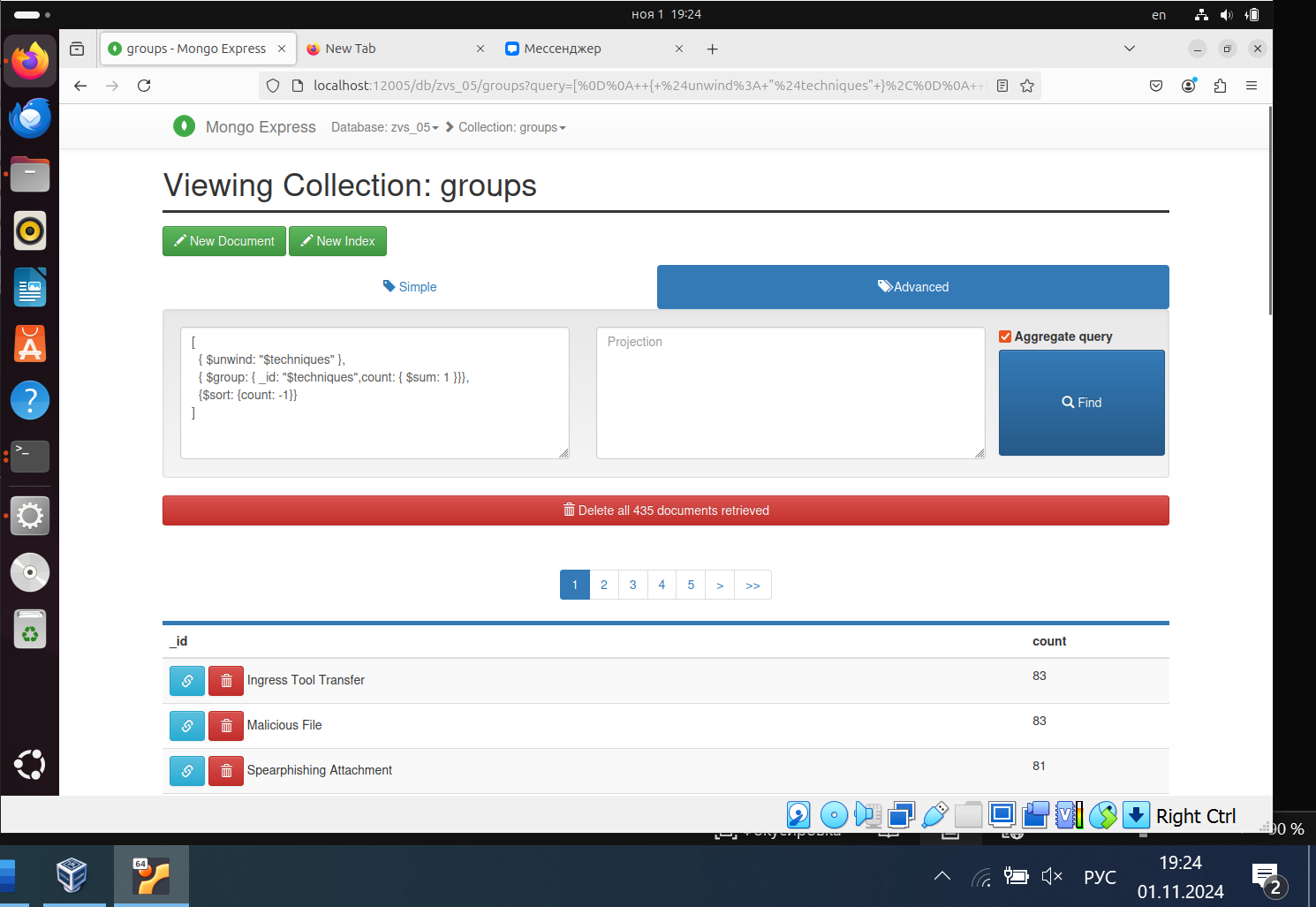
Загрузите с помощью программы/скрипта данные в MongoDB.

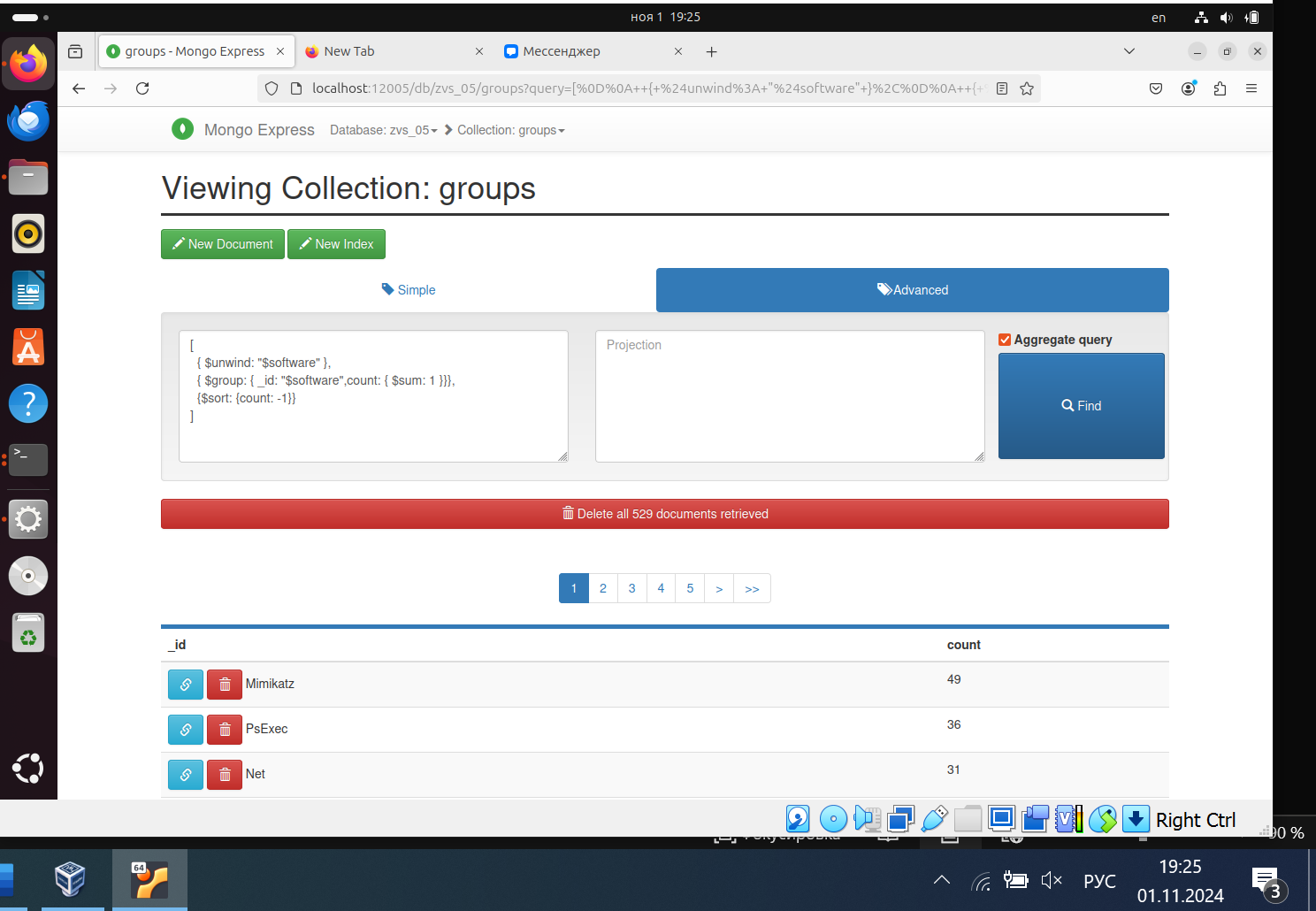


Выполните несколько поисковых запросов в данной коллекции. Например: поиск групп, которые используют определенную технику или ПО; поиск группы по названию.



С помощью запроса в MongoDB выведите списки техник и ПО, используемых группировками по убыванию частоты использования (название техники – сколько групп использует; название ПО – сколько групп использует).





Выберите две техники и две программы, используемых APT-группами, из выборки.

Техники: WindowsCommandShell, PowerShell

ПО – Cobalt Strike, Empire

Опишите две выбранные техники (название, описание техники; ссылка на страницу техники на любом из двух ресурсов из п. 12).

WindowsCommandShell

Злоумышленники могут использовать командную оболочку Windows для выполнения команд. Командная оболочка Windows ([cmd](https://attack.mitre.org/software/S0106)) является основным командным интерфейсом в системах Windows. Командный интерфейс Windows можно использовать для управления практически любым аспектом системы, при этом для разных наборов команд требуются разные уровни разрешений. Командный интерфейс можно вызывать удалённо с помощью [удалённых служб](https://attack.mitre.org/techniques/T1021), таких как [SSH](https://attack.mitre.org/techniques/T1021/004).

<https://attack.mitre.org/techniques/T1059/003/>

PowerShell

Злоумышленники могут использовать команды и скрипты PowerShell для выполнения действий. PowerShell — это мощный интерактивный интерфейс командной строки и среда разработки сценариев, включенная в операционную систему Windows.

<https://attack.mitre.org/techniques/T1059/001/>

Опишите две выбранных программы (название ПО; для чего и как используется; ссылка на ПО, если есть в открытом доступе – часто размещены на GitHub)

Cobalt Strike

Cobalt Strike — это программное обеспечение для моделирования угроз, которое используется красными командами и тестировщиками проникновения для симуляции продвинутых угроз и выполнения целевых атак.

Оно сочетает различные инструменты и техники, такие как социальная инженерия, обфускация сети и выполнение вредоносного кода, для оценки защиты организации.

<https://www.cobaltstrike.com/>

Empire

Empire — это **фреймворк для пост-эксплуатации**, который сочетает в себе возможности Powershell и Python и позволяет развертывать модули пост-эксплуатации, такие как кейлоггеры или Mimikatz, в целевых системах.

https://github.com/EmpireProject/Empire