

#### МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

## «МИРЭА – Российский технологический университет» РТУ МИРЭА

## МАТЕРИАЛЫ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

## Технологии хранения в системах кибербезопасности

	(наименование дисциплины (модуля) в соответствии с учебным планом)	
Уровень	специалитет	
•	(бакалавриат, магистратура, специалитет)	
Форма обучения	очная	
•	(очная, очно-заочная, заочная)	
Направление(-я) подготовки	10.05.04 Информационно-ана	алитические системы безопасности
	(код(-ы) и наименование(-я))	
Институт	Кибербезопасности и цифровых технологий (ИКБ)	
•	(полное и краткое наименование)	
Кафедра	КБ-2 «Прикладные информационные технологии»	
•	(полное и краткое наименование кафедры, реализующей дисциплину (модуль))	
Лектор	к.т.н., Селин Андрей Александрович, Бугаев Александр Александрович	
•	(сокращенно – ученая степень, ученое звание; полностью – ФИО)	
Используются в данной редакции с учебного года		2024/2025
		(учебный год цифрами)
Проверено и согласовано «»2024 г.		А.А. Бакаев
		(подпись директора Института/Филиала
		с расшифровкой)

#### ПРАКТИЧЕСКАЯ РАБОТА № 4

# «Знакомство с инструментами для работы с частично структурированными данными на примере документо-ориентированной СУБД MongoDB»

**Цель работы** – получение практических навыков работы с MongoDB.

#### Задание:

- 1. Запустите Unix-подобную систему (например, Debian 12.6.0 64-bit<sup>1</sup>).
- 2. Создайте пользователя с именем формата **fio\_nn**,

где f – первая буква фамилии на латинице;

- і первая буква имени на латинице;
- о первая буква отчества на латинице (при наличии),
- nn двузначный номер по списку в группе.

Добавьте его в группу sudo. Все дальнейшие действия необходимо выполнять от имени созданного пользователя.

- 3. Запустите терминал и установите Docker и Docker Compose.
- 4. Разверните MongoDB и Mongo Express с помощью Docker Compose.

## Требования к запускаемым сервисам:

- последние 2 цифры номера порта, на котором будет развернут сервис, должны соответствовать номеру по списку в группе (например, для 3-12303, 8003, 9903 и т.п.);
- имя контейнера должно заканчиваться на символ подчеркивания и инициалы ФИО (например, для Иванова Петра Дмитриевича mongo\_ipd, mongo-express\_ipd).
- 5. Создайте в MongoDB базу данных с именем в формате **fio\_nn** (см. п. 2).
- 6. Создайте коллекцию с именем **test\_nn**, где nn номер по списку.

<sup>&</sup>lt;sup>1</sup> Можно скачать готовый образ виртуальной машины по ссылке <a href="https://sourceforge.net/projects/osboxes/files/v/vb/14-D-b/12.6.0/64bit.7z/download">https://sourceforge.net/projects/osboxes/files/v/vb/14-D-b/12.6.0/64bit.7z/download</a>

- 7. Зайдите в контейнер MongoDB с помощью команды docker exec: sudo docker exec -it mongo\_ipd bash
  Выйти из контейнера можно с помощью команды exit.
- 8. Запустите консоль MongoDB (/bin/mongosh) со своими параметрами: mongosh --host localhost --port 27017 -u root -p password

Выйти из консоли можно с помощью команды exit.

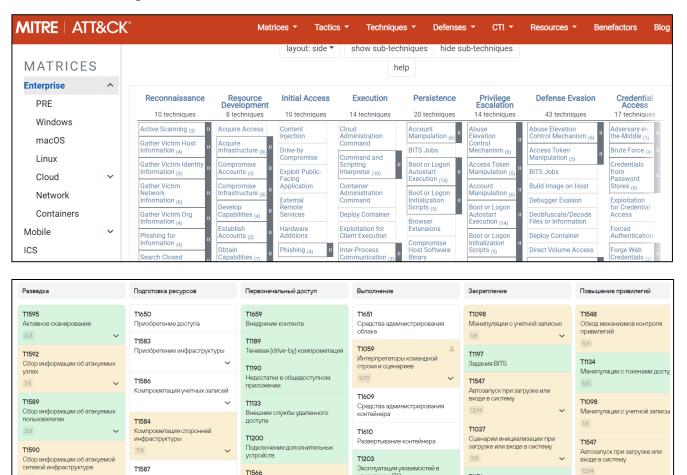
- 9. Подключитесь к ранее созданной БД. Пример: use ipd\_07
- 10. Проверьте, что все корректно работает. Например, командой **db.stats**():

```
test> use ipd_07
switched to db ipd_07
ipd_07> db.stats()
  db: 'ipd_07',
  collections: Long('2'),
  views: Long('0'),
  objects: Long('0'),
  avgObjSize: 0,
  dataSize: 0,
  storageSize: 8192
  indexes: Long('2'),
  indexSize: 8192,
  totalSize: 16384,
  scaleFactor: Long('1'),
  fsUsedSize: 62231244800,
 fsTotalSize: 1081101176832,
  ok: 1
ipd_07>
```

- 11. Изучите основные команды и потренируйтесь в их выполнении:
  - добавление одного документа;
  - добавление нескольких документов;
  - удаление и обновление документов;
  - поиск по документам;
  - пагинация и сортировка документов;
  - получение количества документов и другие.

Примеры можно посмотреть по ссылке: <a href="https://metanit.com/nosql/mongodb">https://metanit.com/nosql/mongodb</a>.

- 12. Изучите матрицу MITRE ATT&CK (описывает тактики и техники, которыми злоумышленники пользуются в своих атаках на корпоративную инфраструктуру):
  - <a href="https://attack.mitre.org">https://attack.mitre.org</a> (официальный адрес);
- <a href="https://mitre.ptsecurity.com/ru-RU">https://mitre.ptsecurity.com/ru-RU</a> (версия на русском языке от компании Positive Tehnologies).



13. Скачайте данные матрицы в формате JSON: <a href="https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack/enterprise-attack.json">https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack/enterprise-attack.json</a>

- 14. Напишите программу/скрипт для загрузки данных матрицы из скачанного файла в БД. Ниже приведен пример на языке Python.
- 14.1. Установите библиотеки mitreattack-python и pymongo: pip install mitreattack-python pip install pymongo

Документация по библиотеке mitreattack-python: https://mitreattack-python.readthedocs.io/en/latest/index.html

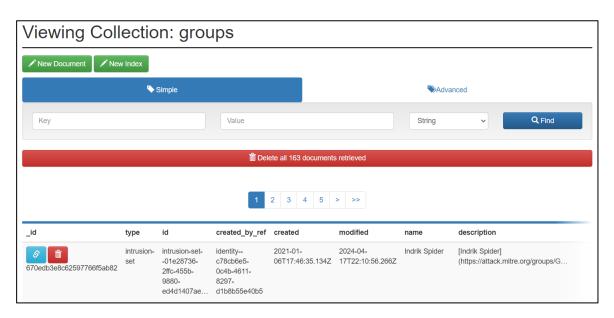
#### Документация по библиотеке pymongo:

https://pymongo.readthedocs.io/en/stable

### 14.2. Напишите скрипт:

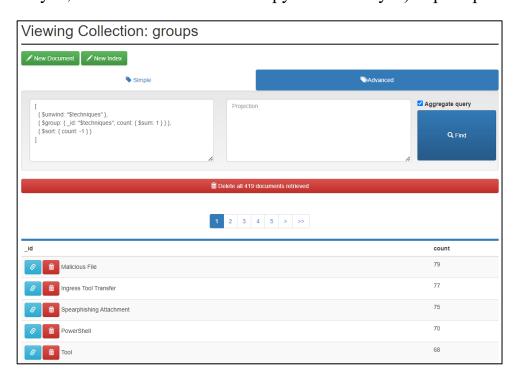
```
from mitreattack.stix20 import MitreAttackData
      from pymongo import MongoClient
 3
      import json
 4
      # Подключение к MongoDB (root:example - ваши логин и пароль)
      client = MongoClient('mongodb://root:example@localhost:27017/')
      db = client['ipd 07']
 8
      collection = db['groups']
 9
      # Создание объекта MitreAttackData
      mitre attack data = MitreAttackData("enterprise-attack.json")
11
12
13
      # Получение данных об АРТ-группах
14
      groups = mitre attack data.get groups()
15
16
      # Цикл по каждой группе
17
    for group in groups:
18
        group json = json.loads(str(group))
19
20
        # Получение информации о техниках, используемых группой
21
        techniques used by group = mitre attack data.get techniques used by group (group.id)
        group json['techniques'] = []
23
        for technique in techniques used by group:
24
          # Наполнение списка используемых группой техник
25
          group_json['techniques'].append(technique['object']['name'])
26
27
        # Получение информации о ПО, используемом группой
28
        software used by group = mitre attack data.get software used by group (group.id)
        group json['software'] = []
29
        for s in software used by group:
31
          # Наполнение списка используемого группой ПО
          group json['software'].append(s['object']['name'])
33
34
        # Загрузка информации о группе в БД
        collection.insert one (group json)
```

## 15. Загрузите с помощью программы/скрипта данные в MongoDB.



```
x_mitre_modified_by_ref: 'identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40
          x_mitre_version: '1.0',
         techniques: [
               'Exfiltration to Cloud Storage',
               'Malware',
               'Data Transfer Size Limits',
49
50
               'Hidden Files and Directories',
               'Upload Malware',
              'Replication Through Removable Media',
'Exfiltration Over C2 Channel',
58
              'Tool',
'Data from Local System',
               'DLL Side-Loading',
              'Registry Run Keys / Startup Folder', 'File and Directory Discovery',
               'Match Legitimate Name or Location',
               'Modify Registry',
'Scheduled Task',
               'Code Signing'
73
74
75
         software: [
               'PlugX',
'Cobalt Strike'
```

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



Разберитесь с синтаксисом операторов **\$unwind**, **\$group**.

- 18. Выберите две техники и две программы, используемых АРТ-группами, из выборки, полученной по следующему правилу:
- в списках, полученных в п. 16, найдите технику/ПО по вашему номеру в списке;
- ваша выборка будет состоять из найденной техники/ $\Pi$ O и +/-2 от нее (выборка из 5 элементов).
- 19. Опишите две выбранные техники (название, описание техники; ссылка на страницу техники на любом из двух ресурсов из п. 12).
- 20. Опишите две выбранных программы (название ПО; для чего и как используется; ссылка на ПО, если есть в открытом доступе часто размещены на GitHub).