

### Задание 3.

В этом задании вам необходимо поработать с резервной копией базы данных. Прочтите «легенду» и само задание ниже.

#### **Легенда:**

**10 октября 2024 года в 17:25** SIEM система компании «Must Do It» обнаружила **угрозу межсайтового скриптинга (УБИ.041)** на одном из компьютеров пользователей. Известно, что злоумышленник пользовался в это время сомнительным браузером **Mozilla Firefox**. После чего в здании было вырублено электричество, и нарушитель успел скрыться. Из-за перебоев с электричеством записи с камер и часть журнала безопасности были повреждены и заменены на символы «###».

Вам необходимо восстановить резервную копию базы данных на своем компьютере при помощи инструмента. При помощи SQL-запросов определите **имя и ip-адрес преступника**, используя всю доступную вам информацию в базе данных. И помните, время не на вашей стороне. Советуем начать с таблицы **security\_journal** и общей схемы БД.

#### **Пояснения:**

- Резервная копия базы данных «**TaskSQL.backup**» расположена в том же локальном репозитории, где и файл с этим заданием.
- Ответ на это задание необходимо записать в файл с расширением «.txt» или «.sql».
- В файле необходимо указать имя и ip\_адрес преступника, а также SQL-запросы, которые подтверждают причастность данного сотрудника к произошедшему инциденту, т.е. с помощью которых вы нашли злоумышленника.
- Оценивается правильность вашего ответа, а также количество и структура SQL-запросов с помощью которых вы выполнили задание.

В базе данных расположены следующие таблицы:

1. *security\_journal* – таблица с произошедшими угрозами ИБ в компании
2. *vlan* – таблица с номерами виртуальных сетей компании
3. *pc* – таблица с информацией об устройствах в сети организации
4. *employees* – таблица с данными о сотрудниках организации
5. *statuses* – таблица с данными о рабочем статусе сотрудника
6. *employee\_report* – таблица с отчетами сотрудников и их алиби в день происшествия
7. *applications* – таблица с сессиями браузеров и временем их запуска на устройствах