Федеральное государственное автономное образовательное
учреждение высшего образования
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

Московский институт электроники и математики им. Тихонова
Департамент электронной инженерии

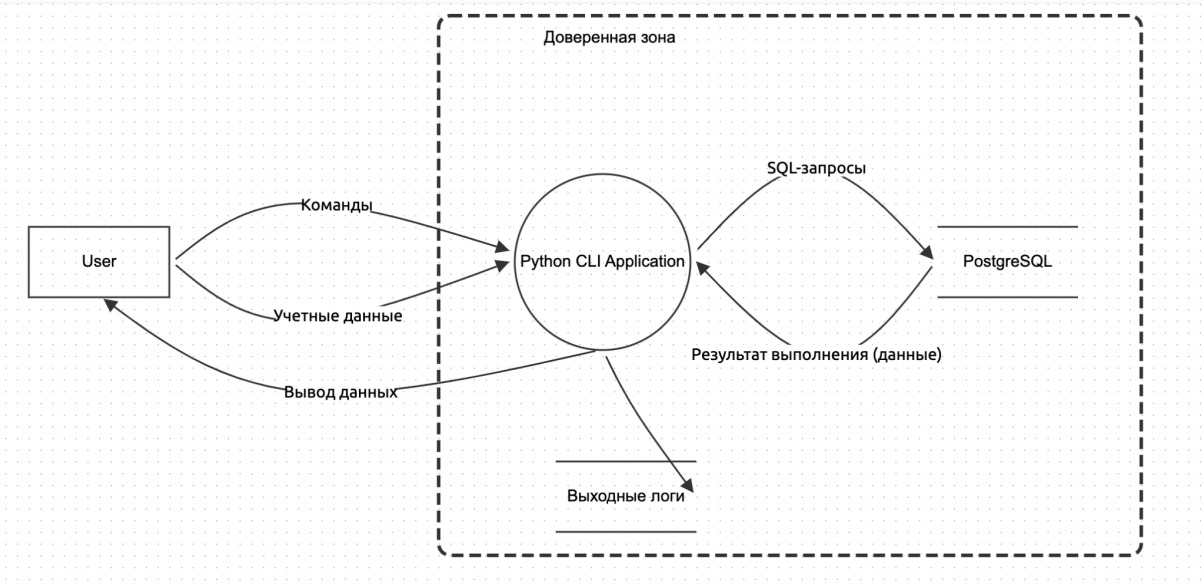
Практическая работа №4

по курсу «Разработка защищенных программных систем»

Выполнила:
Студентка группы МИБИ251
Балясникова Екатерина Сергеевна

Москва, 2025

1. Диаграмма потоков данных для приложения



2. STRIDE-угрозы

A. Опасности для канала: Пользователь → CLI-приложение

STRIDE	Угроза	Локализация
T	Манипуляция вводимыми данными (SQL хотя бы частично может быть подвержена).	Поля ввода пользователя.
I	Подсмотр логина/пароля через shoulder surfing.	Интерфейс ввода.
R	Отсутствие доказательств, кто ввёл вредоносный запрос.	Нет аутентификации внутри приложения.

B. Опасности: CLI-приложение (процесс)

STRIDE	Угроза	Локализация
S	Ввод неверных пользовательских учётных данных, подбор пароля.	Функция connect_db().
T	Модификация SQL-запросов (подмена table/column).	Формирование запросов.

R	Нет аудит-лога действий.	Отсутствует журнал транзакций приложения.
I	Вывод ошибок, содержащих конфиденциальные данные.	Блок except.
D	Падение программы при некорректном вводе.	Весь ввод пользователя.
E	Пользователь может подключиться под учёткой с избыточными правами.	Параметр user.

C. Опасности: PostgreSQL-сервер

STRIDE	Угроза	Локализация
S	Подбор учетных данных.	Аутентификация.
T	Изменение данных через приложение.	INSERT / UPDATE.
I	Утечка данных при SELECT без ограничений.	view_table().
D	Интенсивные запросы вызывают нагрузку.	filter_table, view_table.

D. Опасности: Переменные окружения

STRIDE	Угроза	Локализация
I	Утечка DB_HOST, DB_NAME, DB_PORT.	os.getenv().
T	Изменение окружения злоумышленником.	Environment.

E. Опасности: Логи

STRIDE	Угроза	Локализация

I	Утечка информации о пользователях.	logging.info(f"user…").
T	Подмена логов.	log file.
R	Отсутствие неизменяемости.	Формат логирования.

3. Оценка рисков по методике DREAD

Основные критерии методики DREAD:

- Damage (ущерб): Насколько серьезен потенциальный ущерб от реализации угрозы?
- Reproducibility (воспроизводимость): Насколько легко повторить эту угрозу?
- Exploitability (эксплуатируемость): Насколько легко злоумышленнику воспользоваться этой уязвимостью?
- Affected users (затронутые пользователи): Сколько пользователей или систем пострадает от угрозы?
- Discoverability (обнаруживаемость): Насколько легко злоумышленнику найти эту уязвимость?

Шкала: 1 (низко) – 10 (очень высоко).

Риск = (D + R + E + A + D)/5.

Ниже таблица для 9 наиболее типичных угроз

№	Угроза	D	R	E	A	D	Риск
1	Подбор пароля PostgreSQL	8	7	8	8	8	7.8
2	Раскрытие конфиденциальных данных из-за ошибок	8	6	7	9	8	7.6
3	Подмена переменных окружения	7	6	7	5	6	6.2
4	SQL-иньекции через ввод пользователя	9	8	7	9	8	8.2
5	Использование УЗ с избыточными правами	7	5	7	7	6	6.4

6	Отсутствие аудита действий	5	9	9	3	7	6.6
7	Утечка логов	6	7	6	7	5	6.2
8	Некорректный ввод вызывает DoS	5	8	9	5	8	7.0
9	Перехват учетных данных	7	6	6	7	8	6.8

4. Отсортированная таблица угроз по убыванию риска

Ранг	Угроза	Риск
1	SQL-иньекции через ввод пользователя	8.2
2	Подбор пароля PostgreSQL	7.8
3	Раскрытие конфиденциальных данных из-за ошибок	7.6
4	Некорректный ввод вызывает DoS	7.0
5	Перехват учетных данных	6.8
6	Отсутствие аудита действий	6.6
7	Использование УЗ с избыточными правами	6.4
8	Подмена переменных окружения	6.2
9	Утечка логов	6.2

5. Подбор 5 соответствующих угроз из БДУ ФСТЭК России

Угроза	БДУ ФСТЭК
SQL-иньекции через ввод пользователя	УБИ.006 Угроза внедрения кода или данных
Подбор пароля PostgreSQL	УБИ.074 Угроза несанкционированного доступа к аутентификационной информации УБИ.090 Угроза несанкционированного создания учётной записи пользователя

Раскрытие конфиденциальных данных из-за ошибок	УБИ.037 Угроза исследования приложения через отчёты об ошибках
Некорректный ввод вызывает DoS	УБИ.140 Угроза приведения системы в состояние «отказ в обслуживании»
Перехват учетных данных	УБИ.074 Угроза несанкционированного доступа к аутентификационной информации