ТЕХНИЧЕСКОЕ ЗАДАНИЕ

И критерии для отбора на конкурс

По безопасной разработке ИИ-помощника
по кредитам для АКБ “Микрокредитбанк»

1. Общее положение

АКБ “Микрокредитбанк” объявляет лот на разработку умного помощника на основе Искусственного Интеллекта и существующих LLM моделей для консультации по кредитованию и другим продуктам банка. Бот необходимо разработать с современными и принципами “AI Security” и профессиональной кибербезопасности с целью недопустимости утечки конфиденциальных и персональных данных пользователей помощника.

2. Требования к реализации

Исполнитель обязуется разработать умного бота на основе Искусственного Интеллекта, как отдельной системы в виде трех компонентов:

1. **Back-End сервис**, с помощью которого клиентская часть (чат в мобильном приложении, телеграм-бот и другие) смогут обращаться к умному помощнику как пользователи банка к отдельной системе;
2. **LLM агент** – ядро проекта, разработанного в виде отдельного программного модуля;
3. **Сервис базы данных (СУБД)**, который будет хранить и обрабатывать данные, необходимые для функционирования LLM агента и данные о пользователях приложения;
4. **Интерфейс чата** – разработка или интеграция в клиентский компонент помощника. По предпочтению заказчика, интеграция в один из интерфейсов обработки клиентов:
    - — Интеграция в телеграм-чате;
    - — Интеграция в чате на веб-сайте банка;
    - — Интеграция в чате в мобильном приложении.

2.1 Требования к реализации Back-End сервиса

Back-End сервис необходимо разработать с использованием современных технологий для разработки Restful API. Сервис будет представлять собой небольшой Restful API с монолитной архитектурой, главная задача которого будет создание обертки для использования LLM агента потенциальных или существующих клиентов банка. Общее количество API endpoints не будет превышать 20 штук.

2.2 Требования к реализации LLM агента

Умного помощника необходимо разработать в виде LLM агента, с “fine-tuning” или другим механизмом загрузки данных о возможностях кредитования в АКБ “Микрокредитбанк” и других данных, на существующей Large Language Model (OpenAI GPTs, llama, и так прочее). Разработка LLM агента должна строго следовать принципам безопасности, описанным в данном техническом задании, для исключения утечки конфиденциальной информации пользователей.

Разработка LLM агента должна в себя включать комплексные техники для построения умных помощников на основе Искусственного Интеллекта, так как помощник должен понимать сложные запросы пользователей и производить комплексную аналитику по

кредитованию и давать ценные советы, а не просто предоставлять информацию из базы данных; LLM агенту необходимо будет рассуждать над запросами пользователей.

2.3 Требования к реализации СУБД

Использование PostgreSQL для хранения любых данных, связанных с системой. PostgreSQL будет использоваться в том числе для:

- Хранения истории чатов пользователей.
- Сохранения и управления индексами данных (FAQ и информация о кредитах).
- Логирования действий и аналитики по использованию системы.

2.4 Требования к реализации клиентской части

Будут сформированы в процессе выбора одной из трех видов систем. Однако, интеграция в клиентскую часть не является более комплексным процессом, чем получение, отправка на Back-End сервис и презентация данных в рамках среды интерфейса чата.

3. Требования к безопасности

Разработанному ПО в виде всех компонентов (back-end сервиса, LLM агент и клиентской части) необходимо пройти комплексный анализ защищенности и быть устойчивым к следующим атакам/уязвимостям:

— Prompt Injection атак;
— Sensitive Information Disclosure;
— LLM Supply Chain Attacks;
— LLM Data and Model Poisoning;
— LLM Improper Output Handling;
— LLM Excessive Agency;
— System Prompt Leakage;
— Vector and Embedding Weakness атак;
— Unbounded Consumption и перегрузке системы.

Пользователям бота не должна быть доступна история использования других пользователей или и данные. LLM агент не должен допускать утечки конфиденциальных и персональных данных пользователей помощника.

4. Требования к кандидатам отбора

1. Право на осуществление данных видов деятельности в РУз (как обычно, во всех тендерах);
2. Официальный опыт разработки умных консультантов-помощников на основе Искусственного Интеллекта/LLM. Предоставить кейс конкретного реализованного продукта
3. Официальный опыт реализации проектов по Кибербезопасности.
4. Иметь в штате специалистов по разработке ИИ.
5. Иметь в штате специалистов по ИБ.

6. Сотрудники по кибербезопасности должны быть сертифицированы международными сертификатами, такими как OSCP, Hack The Box CPTS, BSCP, OSEP и иметь подтвержденный опыт по кибербезопасности