Отзыв научного руководителя о прохождении практики

Вид практики:	*Учебная практика*
Обучающий(ая)ся:	*Хокимзода Муборакшои Иноятулло*
Тема практики:	*Разработка адаптивной системы защиты ML-моделей на основе мультиагентного подхода с гомоморфным шифрованием.*

Хокимзода Муборакшои Иноятулло в ходе прохождения практики своевременно и качественно выполнил следующие задачи:

- провёл обзор современных методов обеспечения безопасности ML-моделей, сделав акцент на использовании полностью гомоморфного шифрования (FHE);
- изучил особенности схем FHE и их применимость в задачах машинного обучения, рассмотрев подробно схему CKKS и её поддержку в библиотеке TenSEAL;
- разработал архитектуру мультиагентной системы, обеспечивающей процесс защищённого обучения модели логистической регрессии на зашифрованных данных;
- реализовал прототип системы с четырьмя специализированными агентами: мониторинга, шифрования, передачи и анализа;
- провёл тестирование на реальном наборе данных, сравнил точность моделей, обученных на зашифрованных и незашифрованных данных, а также проанализировал влияние FHE на производительность.

В ходе работы *Хокимзода Муборакшои Иноятулло активно* взаимодействовал с руководителем *и консультантом*, *своевременно* выполнял поставленные задачи, *проявлял разумную* самостоятельность, *оперативно и вовремя учитывал* замечания к работе. В то же время к работе остался ряд замечаний:`

1. Используемые параметры шифрования и конкретные ограничения FHE по времени/памяти следовало бы описать более подробно;
2. Возможны улучшения отдельных участков кода с точки зрения применения паттернов проектирования и принципов SOLID/KISS/DRY, а также автоматизация этапов тестирования;
3. Интерпретация влияния аппроксимации сигмоиды на точность модели требует уточнений.

Рекомендую аттестовать положительно, прохождение практики по шкале ETCS оценить на «C» при условии успешной презентации доклада.

Дата: 19.06.2025

Научный руководитель, *к.ф. м.н.,*
доцент кафедры системного программирования
Луцив Д. В.