

Уважаемые коллеги!

Приглашаем Вас принять участие в онлайн-мероприятии, посвящённом самой актуальной теме в области информационной безопасности – **защита LLM-моделей**.

Поговорим про защиту ИИ-моделей и их безопасное использование, обсудим лучшие практики и кейсы.

ИИ и машинное обучение всё чаще используются в бизнесе, но с этим приходят и новые риски. Важно понимать как эффективно защищать модели от атак и манипуляций, а также обеспечить их безопасную эксплуатацию на каждом этапе их жизненного цикла.

По мере роста внедрения искусственного интеллекта классической защиты инфраструктуры становится недостаточно. Заказчикам требуется системный контроль безопасности самих моделей, данных для обучения и процессов эксплуатации AI-сервисов.

INFERA AI.Firewall позволяет выстраивать безопасность ИИ как часть архитектуры цифровых продуктов – от контроля доступа и защиты данных до активного тестирования устойчивости моделей к современным типам атак. Это особенно важно для компаний, использующих ИИ в критически значимых бизнес-процессах и работающих с конфиденциальной информацией.

ML Red Teaming позволяет моделировать реальные сценарии атак на системы машинного обучения и выявлять критические риски, связанные с эксплуатацией ИИ в корпоративной среде.

Не упустите шанс узнать о самых передовых решениях в этой области и обсудить актуальные вызовы с ведущими ИБ-экспертами!

ПРОГРАММА ОНЛАЙН-МЕРОПРИЯТИЯ

Защита ИИ-моделей и их безопасное использование

- **Эволюция угроз: как ИИ меняет ландшафт кибербезопасности.**
- **Вызовы и проблемы. Как их решать?**
- **INFERA AI.Firewall. Как защитить конфиденциальные данные при использовании LLM-моделей**
- **Сканер безопасности ML Red Teaming**
- **Кейсы и ответы на вопросы**

Ссылку на подключение пришлем за час до мероприятия