Онлайн-мероприятие

Приглашаем Вас принять участие в онлайн-мероприятии, посвящённом самой актуальной теме в области информационной безопасности – безопасное использование искусственного интеллекта и контроль работы ИИ-агентов.

Сквозная видимость ИИ: как защитить модель, агентов и инфраструктуру на всём жизненном цикле

ИИ расширяет поверхность атаки. Готова ли ваша защита? ИИ работает с конфиденциальными данными, пишет код и выполняет задачи автономно. Как контролировать эти процессы и снижать риск киберинцидентов?

10 декабря, 12:00GMT+3

Регистрация доступна на сайте www.inferasecurity.ru или по ссылке

На мероприятии мы расскажем и разберём:

- Законодательные требования по использованию ИИ в корпоративной среде
- Сценарии комплексной защиты ИИ – от модели до автономных агентов
- Защищённый контур ИИ: кибербезопасность как основа инфраструктуры
- Сквозная видимость всего жизненного цикла использования ИИ: от первого запроса до вывода решения из эксплуатации
- Новый ландшафт угроз с появлением LLM и автономных агентов
- Защита данных при работе с моделями – практические подходы
- Agent Runtime Security: переход от защиты модели к контролю действий и намерений ИИ-агентов
- Shadow AI под контролем: учёт использования токенов и безопасная эксплуатация ИИ-агентов
- Vibe Coding и AI-генерируемый код: как выстроить единый контур контроля – от запроса к модели до готового кода в процессах разработки.

Спикеры



Антон Голубков
Исполнительный директор
ICL Системные Технологии



Бирюков Игорь
Генеральный директор
INFERA Security

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