КРОНШТАДТ

Обеспечение безопасности с использованием технологий искусственного интеллекта. Реагирование и снижение риска угроз

XVII Международная конференция
«ЗАБАБАХИНСКИЕ НАУЧНЫЕ ЧТЕНИЯ»
г. Снежинск, Челябинская область
19 мая 2025г.

Федулин Андрей Михайлович
Директор Центра разработки ПО
Группа Компаний «Кронштадт»

Международные тренды внедрения ИИ в системы обеспечения безопасности

- Автономные РТК СН для работы в условиях противодействия
- Совместное применение разносредных средств
- Прогнозирование возникновения ЧС и оценка его развития
- Безакцептные средства оповещения (в т.ч. на основе языковых моделей)
- Оценка состояния пострадавших при ЧС
- Тактические VR-тренажеры

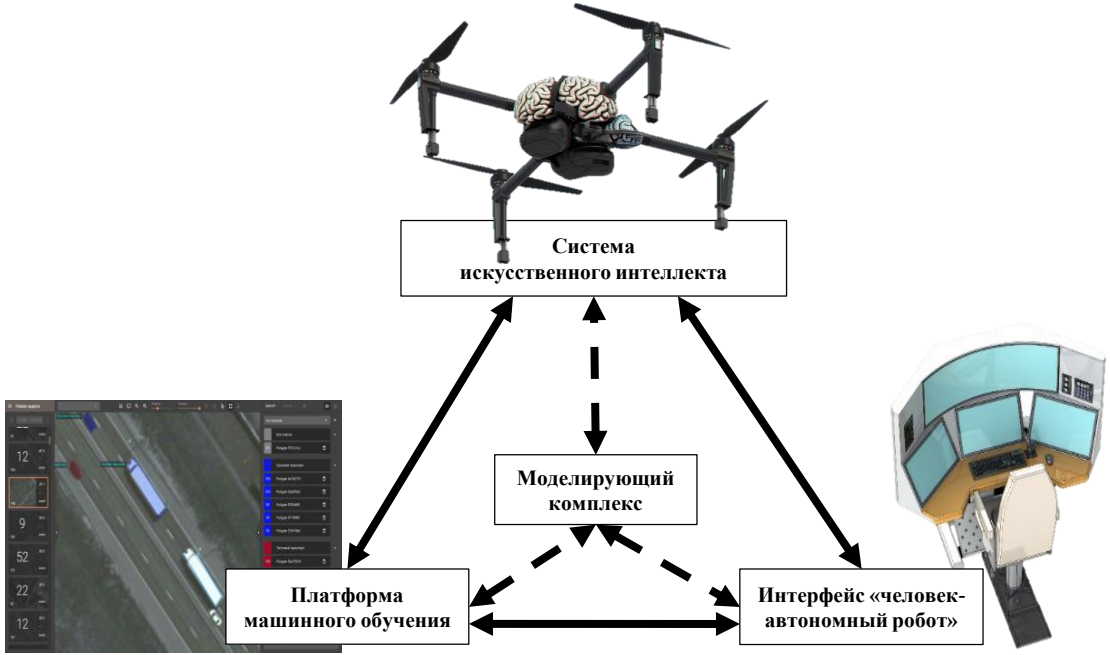
Проблематика внедрения ИИ в системы безопасности

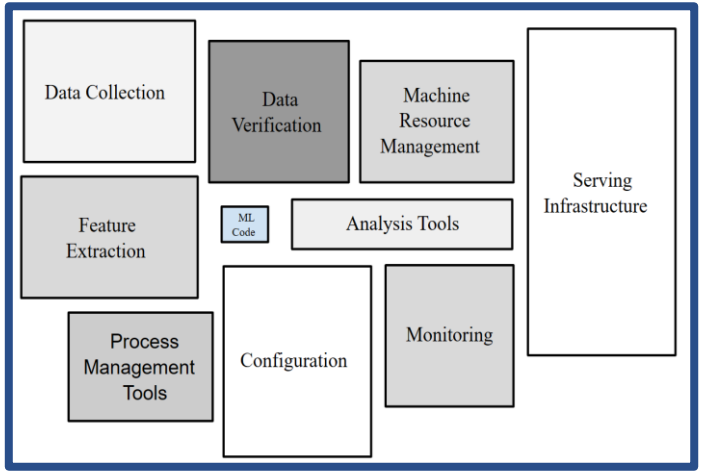
- Кто будет нести ответственность за происшествие?
- Что делать, если ИИ перестанет работать?
- Проблема перехвата управления
- Необходимость дообучения и связанные риски
- Как контролировать «dark AI»?
- Международные соглашения и ограничения

УБИ	Описание (ФСТЭК)
№218	Угроза раскрытия информации о применяемой технологии ИИ
№219	Угроза хищения данных
№220	Угроза «обхода» средств, реализующих технологии ИИ
№221	Угроза модификации ИИ путем искажения данных
№222	Угроза подмены элементов ИИ

Пример маскировки («обхода» ГНС) за счет покрытия самолета покрышками, спутниковые снимки а/б Энгельс-2, сделанные Maxar Technologies, из статьи «Russia Covering Aircraft With Tires Is About Confusing Image-Matching Missile Seekers U.S. Military Confirms»

Скрытые затраты на внедрение ИИ





Экспертная оценка Google затрат на создание технологий ИИ и их внедрение в конечное изделие, из доклада «Sculley, D., Holt, G., Golovin, D., Davydov, E. и др. Hidden technical debt in ML-systems» на NIPS-2015

Продукты компании по тематике безопасности

- Воздушный мониторинг пространственных объектов
- Воздушный мониторинг ледовой обстановки
- Формирование банка доверенных данных для машинного обучения