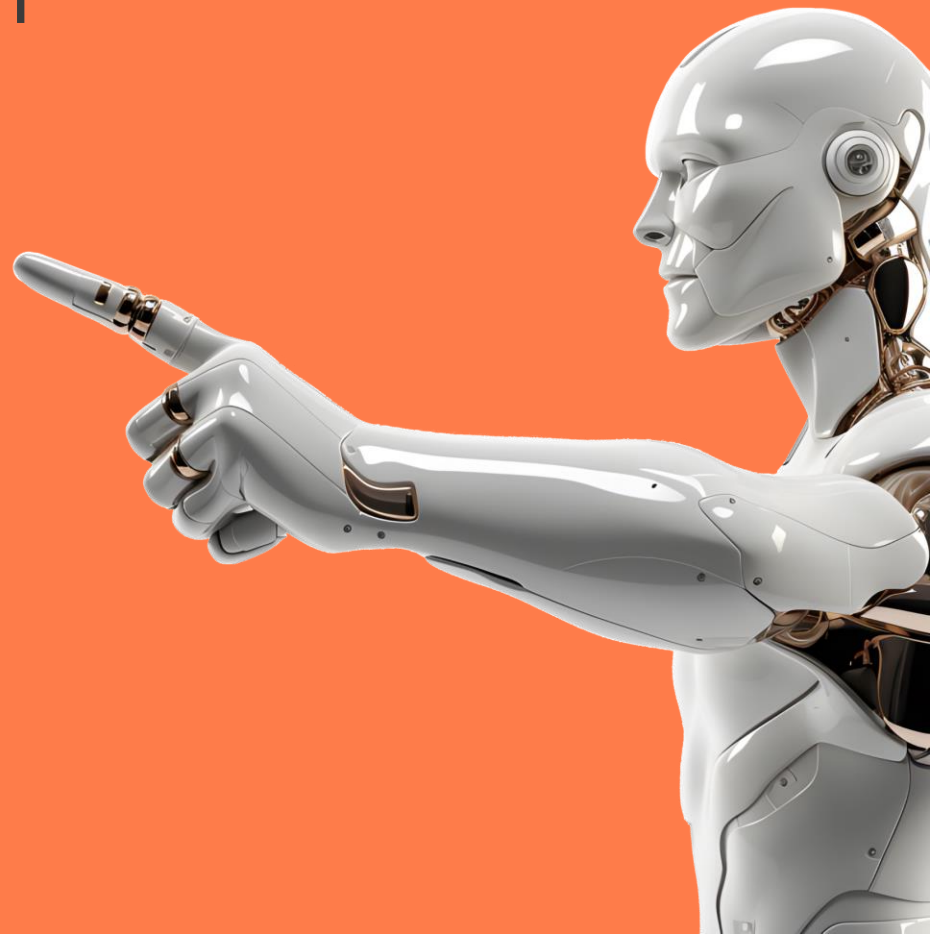
СОЛАР

ПРОБЛЕМАТИКА ДОВЕРЕННОГО ИИ В РАЗРАОБОТКЕ ИБ ПРОДУКТОВ

Руководитель R&D лаборатории
Центра технологий кибербезопасности ГК «Солар»



ПРИМЕНЕНИЕ КЛАССИЧЕСКИХ ML-ТЕХНОЛОГИИ

- Speech Recognition ASR

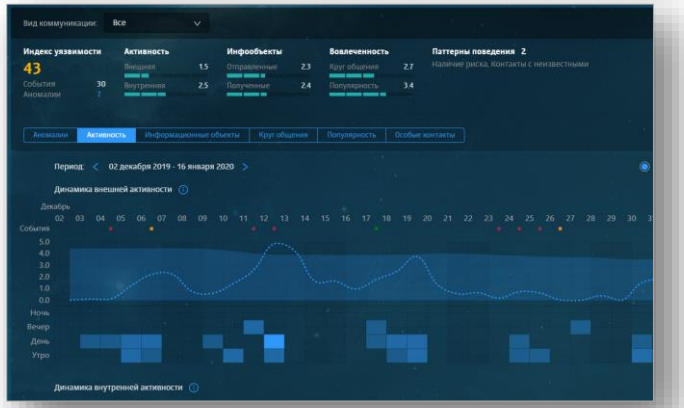
- Computer Vision

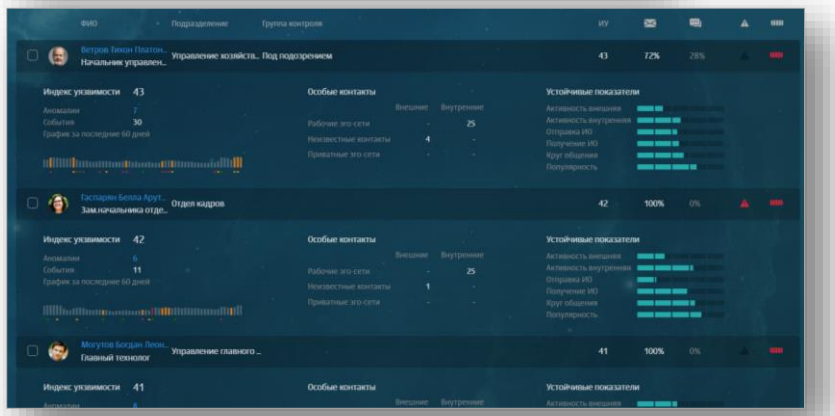
ПРОБЛЕМАТИКА ДОВЕРЕННОГО ИИ

- Дата-сеты с чувствительными данными
- Быстроустаревающие модели
- Зависимость от open-source решений и проектов
- Работа на большом потоке данных
- Недостаточный уровень знаний ОИБ о технологиях ИИ
- Удорожание GPU-решений
- Дороговизна оборудования сертифицированного Минпромторгом

АНАЛИЗ ПОВЕДЕНИЯ И ПРОФИЛИРОВАНИЕ

UBA / UEBA / MSS





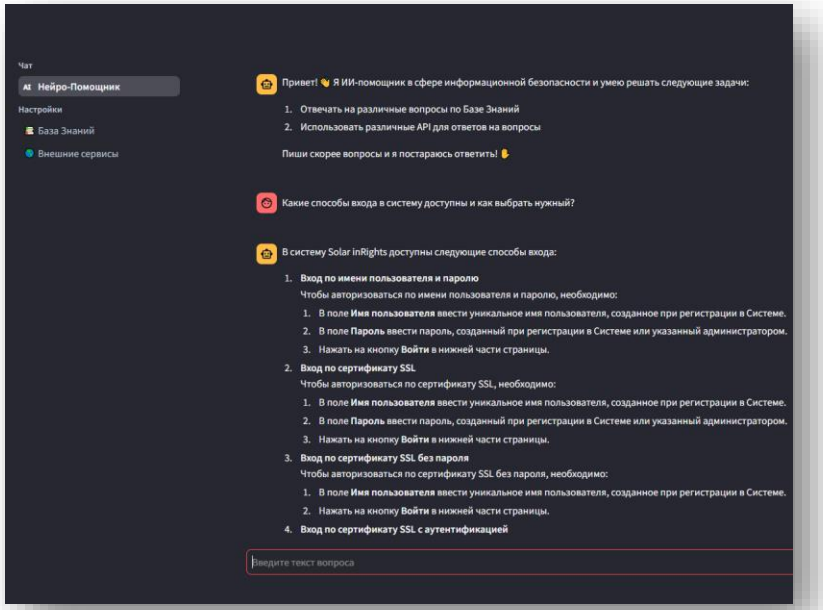
ПРОБЛЕМАТИКА ДОВЕРЕННОГО ИИ

- Почти все данные чувствительные
- White Box ИЛИ Black Box
- Этика VS эффективность расследования
- Специфика и кастомизация для заказчиков
- Красные линии профилирования человека
- Сила рекомендаций ИИ

ПОМОЩЬ СОТРУДНИКАМ ИБ И АВТОМАТИЗАЦИЯ ИБ-ПРОЦЕССОВ

НЕЙРОПОМОЩНИКИ ПО БАЗЕ ЗНАНИЙ

ИИ-помощники и ассистенты

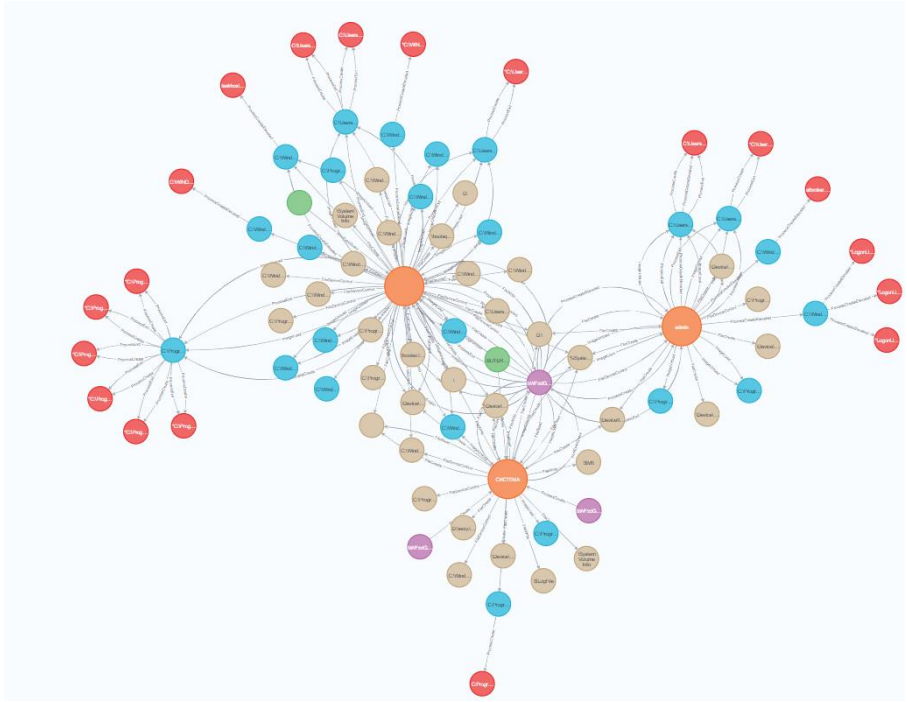


ПРОБЛЕМАТИКА ДОВЕРЕННОГО ИИ

- Зависимость от интернета
- Качество базы знаний и ее непротиворечивость
- Галлюцинации модели
- Юридические последствия рекомендаций
- Ответственность за ошибки

ДЕТЕКТИРОВАНИЕ АНОМАЛИЙ И СЛОЖНЫХ АТАК

EDR 4Rays



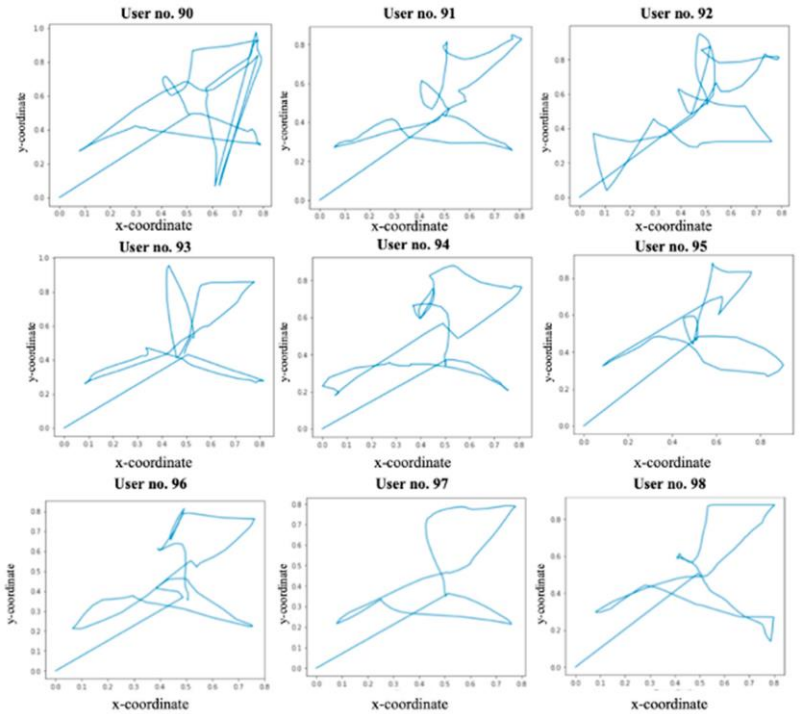
ПРОБЛЕМАТИКА ДОВЕРЕННОГО ИИ

- Устаревшие инструменты правил корреляций
- Скудность информации о реальных сложных атаках
- Сложность разметки данных
- Проблема черного ящика
- Адаптируемость в реальном времени

ЗАЩИТА ОТ КОМПРОМЕТАЦИИ ПОЛЬЗОВАТЕЛЕЙ

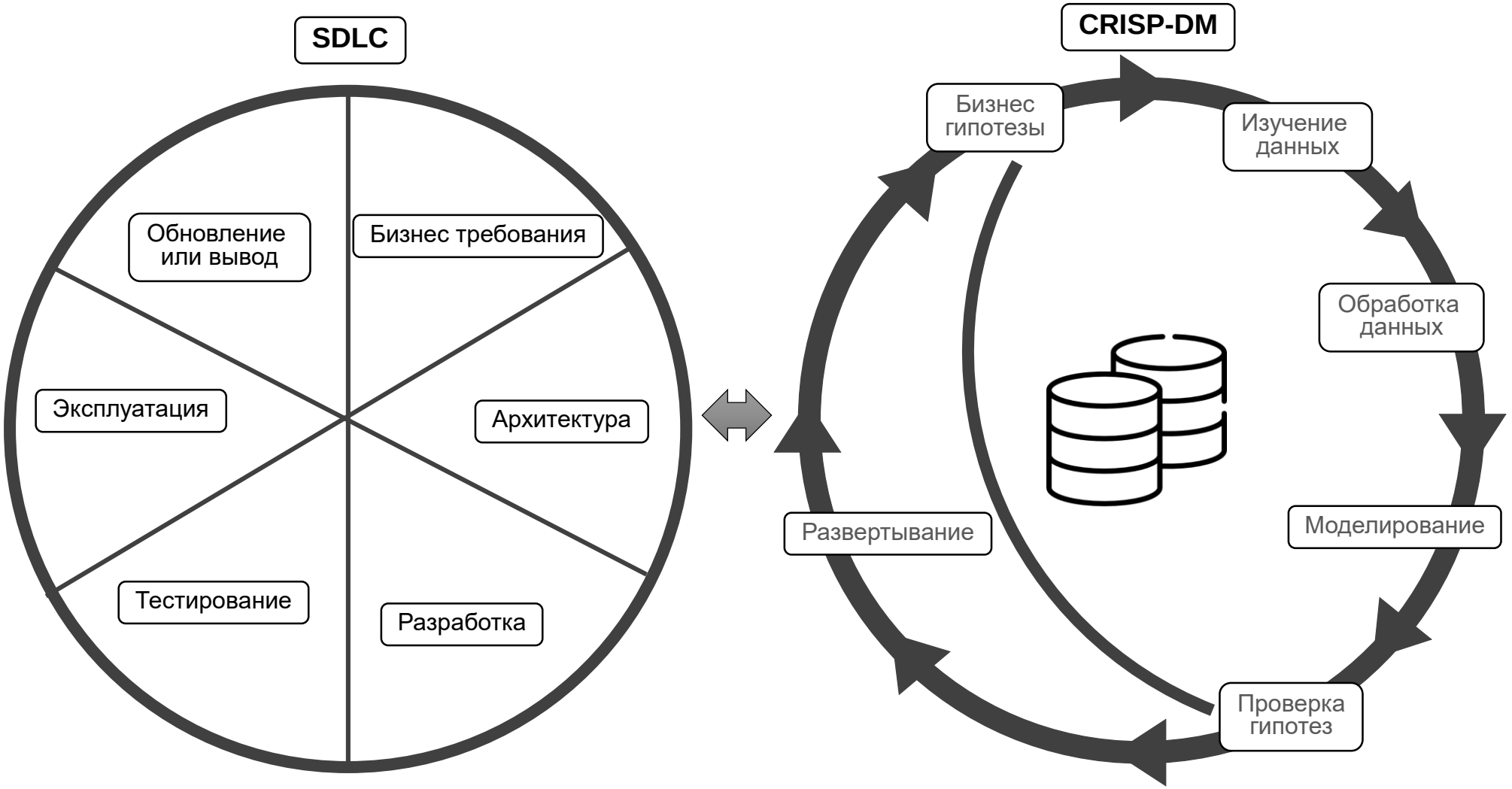
РАСПОЗНАВАНИЕ БИОМЕТРИИ И ДЕТЕКТИРОВАНИЕ РОБОТИЗИРОВАННЫХ ДЕЙСТВИЙ

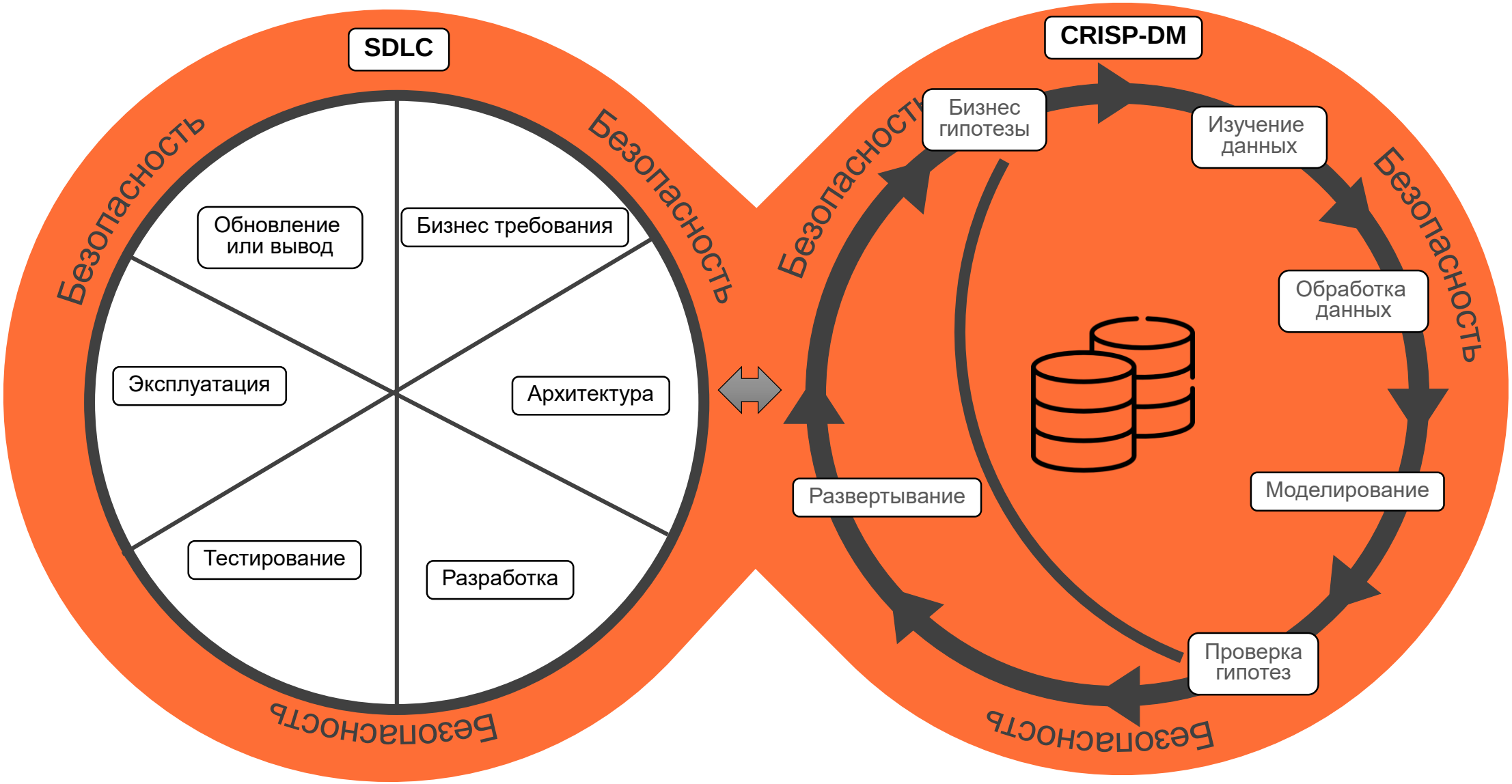
- Face ID Voice ID Key ID Deep Fake



ПРОБЛЕМАТИКА ДОВЕРЕННОГО ИИ

- Персональные данные
- Ложные срабатывания
- Разнообразие цифрового медиаконтента
- Технические требования


SDLC
Обновление или вывод
Бизнес требования
Эксплуатация
Архитектура
Тестирование
Разработка
CRISP-DM
Бизнес гипотезы
Изучение данных
Обработка данных
Моделирование
Проверка гипотез
Развертывание


SDLC
Безопасность
Безопасность
Безопасность
Обновление или вывод
Бизнес требования
Эксплуатация
Архитектура
Тестирование
Разработка
CRISP-DM
Безопасность
Безопасность
Безопасность
Бизнес гипотезы
Изучение данных
Обработка данных
Моделирование
Проверка гипотез
Развертывание

SOLAR

Доверенный ИИ

ХАРАКТЕРИСТИКИ ДОВЕРЕННОГО ИИ

Безопасность

Надежность и отказоустойчивость

Объяснимость и интерпретируемость

Повышенная конфиденциальность

Управляемая предвзятость

Подотчетность и прозрачность

Валидность и надежность

СОЛАР

Спасибо