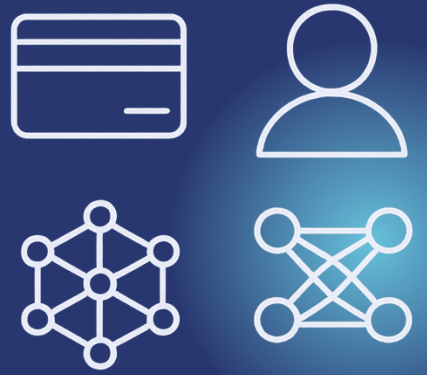
СПР: транзакционный антифрод нового поколения

Графовые сети
ML и скоринговые модели



КБ ТехноСкор

sales@technoscore.ru

PCI Certified
Level 1 Service Provider

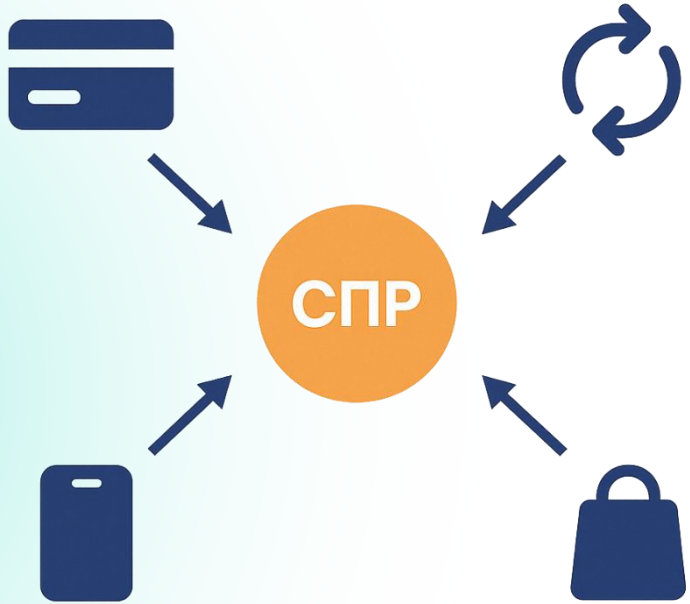
Московский акселератор

Sk Участник

Реализуется при грантовой поддержке Фонда «Сколково»

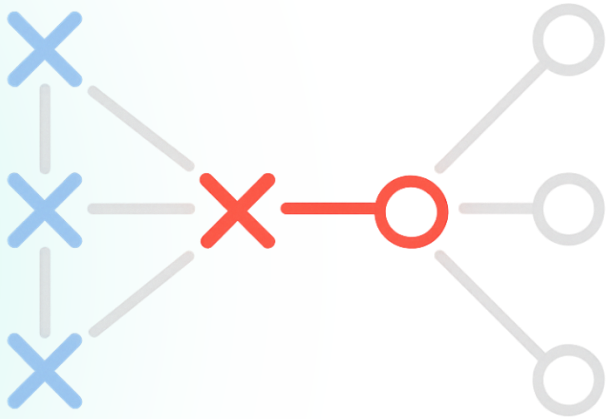
Разнородные данные

- **Каналы:** карты, P2P, интернет-банк, e-commerce – множество разных источников транзакций.
- Проблема: данные из разных каналов имеют разные форматы и стандарты.
- **СПР создаёт единую онтологию** и выполняет **кросс-канальный анализ** событий.



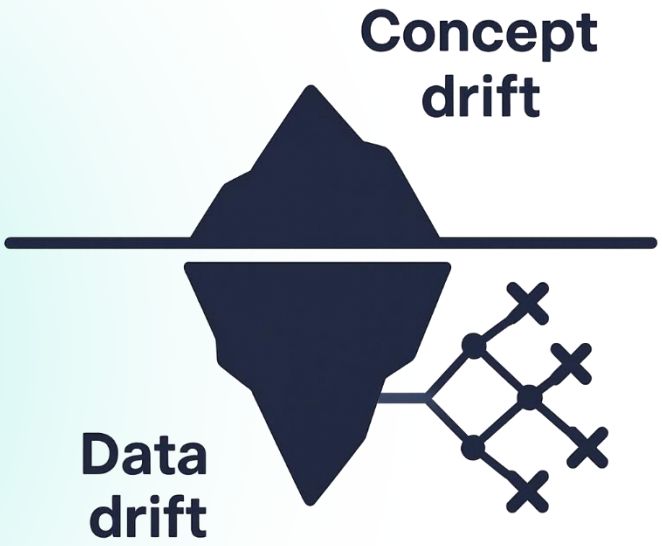
Кросс-канальные угрозы

- **Аномальные комбинации** действий в разных каналах:
- перевод P2P + подозрительная покупка e-commerce,
- новая регистрация + возврат средств в другом канале.
- **СПР выявляет комбинированный фрод**, учитывая связи между событиями разных типов.



Дрейф и адаптивность

- **Data drift:** постепенно смещаются распределения данных (например, география транзакций, популярные MCC-коды).
- **Concept drift:** мошенники меняют сами схемы атак (появляются новые модели мошенничества).
- **Решение:** онлайн-обучение моделей, постоянное авто-обновление профилей + обратная связь (feedback loop).



Методы: Isolation Forest

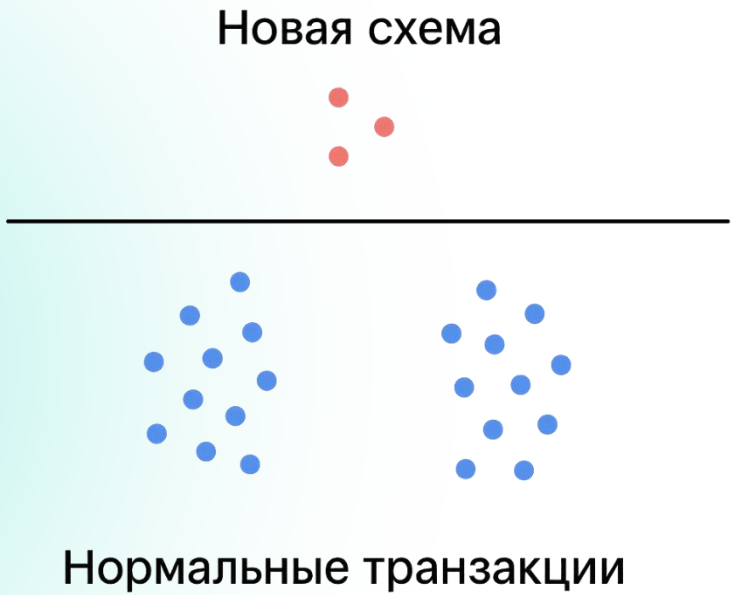
- Модель Isolation Forest строит множество случайных **деревьев** для данных.
- Аномальные точки «изолируются» быстрее (в меньшем количестве разбиений), чем нормальные.
- Простая и **быстрая модель** для онлайн-анализа потоков транзакций, эффективно выявляет выбросы.

Методы: Автоэнкодер

- **Сжатие → восстановление:** модель-автоэнкодер сжимает данные в узкое представление, затем пытается восстановить исходные.
- **Высокая ошибка восстановления = аномалия:** если модель сильно ошибается при реконструкции объекта, значит этот объект не похож на те, что она видела (он подозрителен).

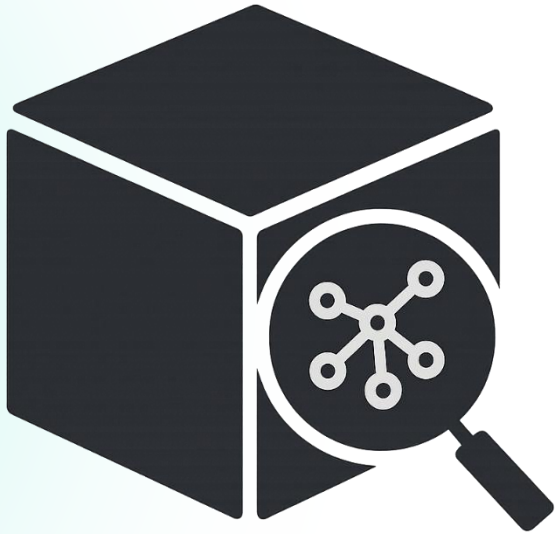
Кластеризация в реальном времени

- Похожие транзакции **автоматически группируются** в кластеры по признакам.
- Появление **новой схемы** фрода проявляется как **отдельный «новый» кластер** данных.
- **Время выявления** атаки сокращается до 2–3 часов (тренды видны почти сразу).



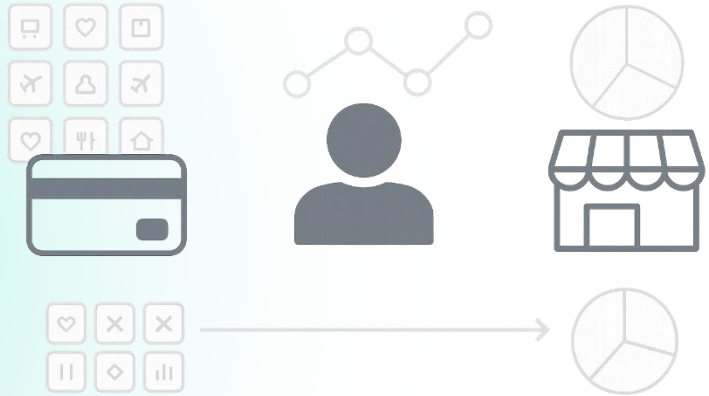
Explainable AI

- «**Чёрный ящик**» ML-модели – серьёзная проблема (непрозрачность решений).
- Методики Explainable AI помогают **понять причины решения** модели.
- Но пояснение сложных моделей остаётся **нетривиальным вызовом** (особенно для нейросетей).



Поведенческие профили

- **Карта** – имеет свой “отпечаток”: любимые магазины, средний чек, география, время активностей.
- **Клиент** – индивидуальный паттерн платежей и действий (поведение пользователя).
- **Мерчант** – характеристика аудитории, сезонность продаж, рисковые индикаторы.
- Графовые эмбеддинги формируют **цифровой «поведенческий отпечаток»** для каждого объекта.



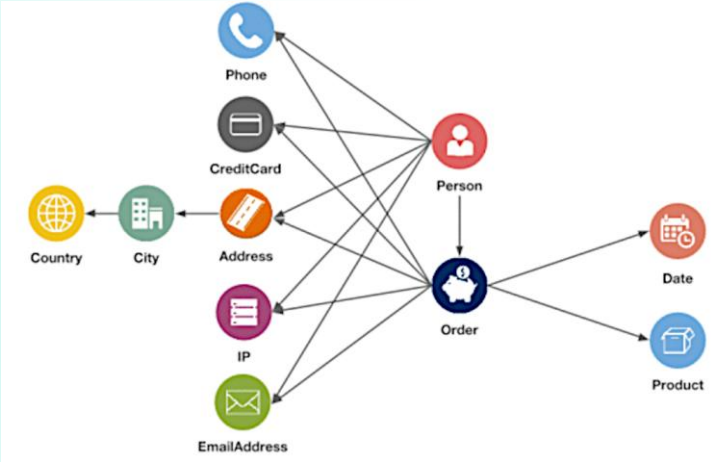
Почему нужен уровень графов и как он применяется в антифроде

- Одна сессия = кусочек картины.
- Нужно связать:

пользователи,
устройства, IP, сессии,
карты, аккаунты и т.д.

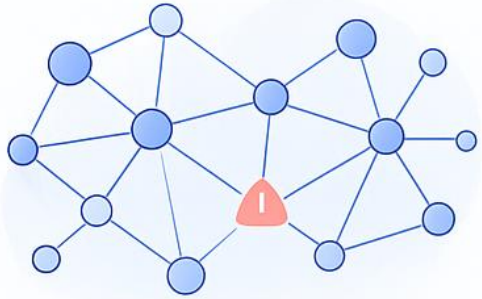
- Видимые угрозы:

мультиаккаунтинг,
бонусхантеры,
распределённые боты.



Графовый антифрод и графовые нейронные сети

На графе применяем label propagation и графовые нейросети (GAT – graph attention network), чтобы узлы обменивались контекстом, а Graph Transformer — чтобы видеть дальние связи и учитывать структурные признаки (расстояния, центральность, кратчайшие пути).



Такой подход выявляет мультиаккаунтинг, сетки ботов, бонусхантеров и сложные отмывочные схемы, ломая kill chain ещё на разведке и тестировании, до транзакции.

ТехноСкор СПР

ТехноСкор СПР —
Система Принятия Решений
для кросс-канального
мониторинга платежей
и защиты учетных записей
от рисков мошенничества
для банков, финтеха,
e-comm, кредитных организаций.

7 лет опыта (ex Cybertonica)

Сертификация PCI DSS Level 1 с 2017

Лицензия ФСБ с 2024

Лицензия ФСТЭК с 2024

Выгоды:

- Защита платежей, учётных записей и репутации от кибермошенников.
- Выполнение требований регуляторов: ЦБ РФ, НСПК ОПКЦ СБП, ПОД ФТ (167-ФЗ, 115-ФЗ, 382-П), 16МР, Стандарт Банка России СТО БР БФБО-1.7-2023 и др.
- Импортозамещение и отсутствие санкционных рисков — только отечественные компоненты. Система внесена в РосРеестр.
- Адаптивность и масштабируемость — защищаем сервисы с миллионной аудиторией. Готовая методика и правила мониторинга.
- Возможность совместной работы с сессионным мониторингом ИРИС и системой конфиденциального инфообмена КРАБ. Возможность мониторинга вебсайтов мерчантов для защиты от мискодинга.
- Быстрая интеграция в виде облачного сервиса за 1 месяц или развертывывание внутри периметра.

О КОМПАНИИ КБ ТЕХНОСКОР

Мы помогаем банкам, финтеху, e-comm защищаться от угроз и управлять рискам за счет анализа данных и криптографии.

1. Технологическая компания, основанная в 2015 году выходцами из МГТУ им. Н.Э. Баумана. Штаб квартира в Москве, офис в ОАЭ. Резидент Сколково.
2. Мониторинг более 150 млн платежей в месяц и более 2 млн устройств в режиме 24x7.
3. Росреестр, Сертификация PCI DSS Level 1 (2017 – н.в.), лицензия ФСБ от 10.09.2024, лицензия ФСТЭК от 26.08.2024.

Сергей Вельц

Технический директор и сооснователь

svelts@technoscore.ru

Андрей Шишов

Руководитель отдела продаж

ashishov@technoscore.ru

Дмитрий Камагин

Руководитель технического прейсейла и ИБ

dkamagin@technoscore.ru