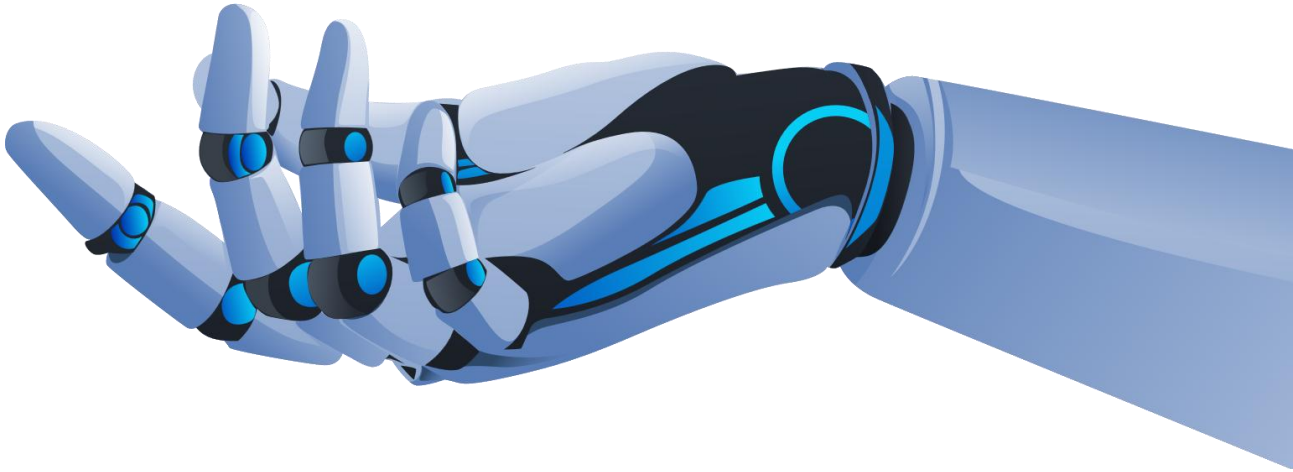
СОВРЕМЕННЫЕ АНТИФРОД-СИСТЕМЫ

КОРПОРАТИВНАЯ БОРЬБА С МОШЕННИЧЕСТВОМ

Эффективное решение антифрод проблем с помощью централизованных кросс-канальных решений



ACFE
Association of Certified Fraud Examiners
KAZAKHSTAN CHAPTER

SYMTECH

Вебинар, 20.03.2025, 13:00 – 14:15

Цель вебинара

Помочь участникам в понимании и получении базовых знаний:

- ✓ **Ключевые проблемы корпоративной борьбы с фродом с точки зрения организации данных и их обработки.**
- ✓ **Решение проблем с помощью автоматизированных систем, релевантные best-practice.**
- ✓ **Дополнительные вызовы внедрению антифрод-систем.**
- ✓ **Будущее развития антифрод-систем.**

10 общих ключевых проблем корпоративной борьбы с фродом

01 **Большое количество и разнородность**

участников, систем, приложений, данных, их взаимодействий

02 **Неэффективная организация операций**

ручной труд, слабая автоматизация плюс неупорядоченность

03 **Недостаточность покрытия данных**

их отсутствие и плохое качество данных

04 **Разрозненность и несогласованность данных**

по фактическому и потенциальному мошенничеству

05 **Слабая аналитика**

и моделирование

Последствия

- Финансовые и репутационные потери из-за невыявленных или допущенных кейсов.
- Повышенные затраты на борьбу с мошенничеством.
- Повышенные временные издержки.

10 общих ключевых проблем корпоративной борьбы с фродом

06 **Быстрое развитие схем и методов мошенничества**
и низкая адаптивность компании

07 **Неготовность к проверкам онлайн или их отсутствие**
в т.ч. по большим потокам транзакций

08 **Конфликт интересов**
при борьбе с фродом или управлении риском фрода

09 **Отсутствие единой картины**
в части состояния противодействию фроду, в части рисков фрода, эффективности их управления

10 **Сложность управления**
включая планирование, формирование отчетности и мониторинг

Последствия

- Финансовые и репутационные потери из-за невыявленных или допущенных кейсов.
- Повышенные затраты на борьбу с мошенничеством.
- Повышенные временные издержки.

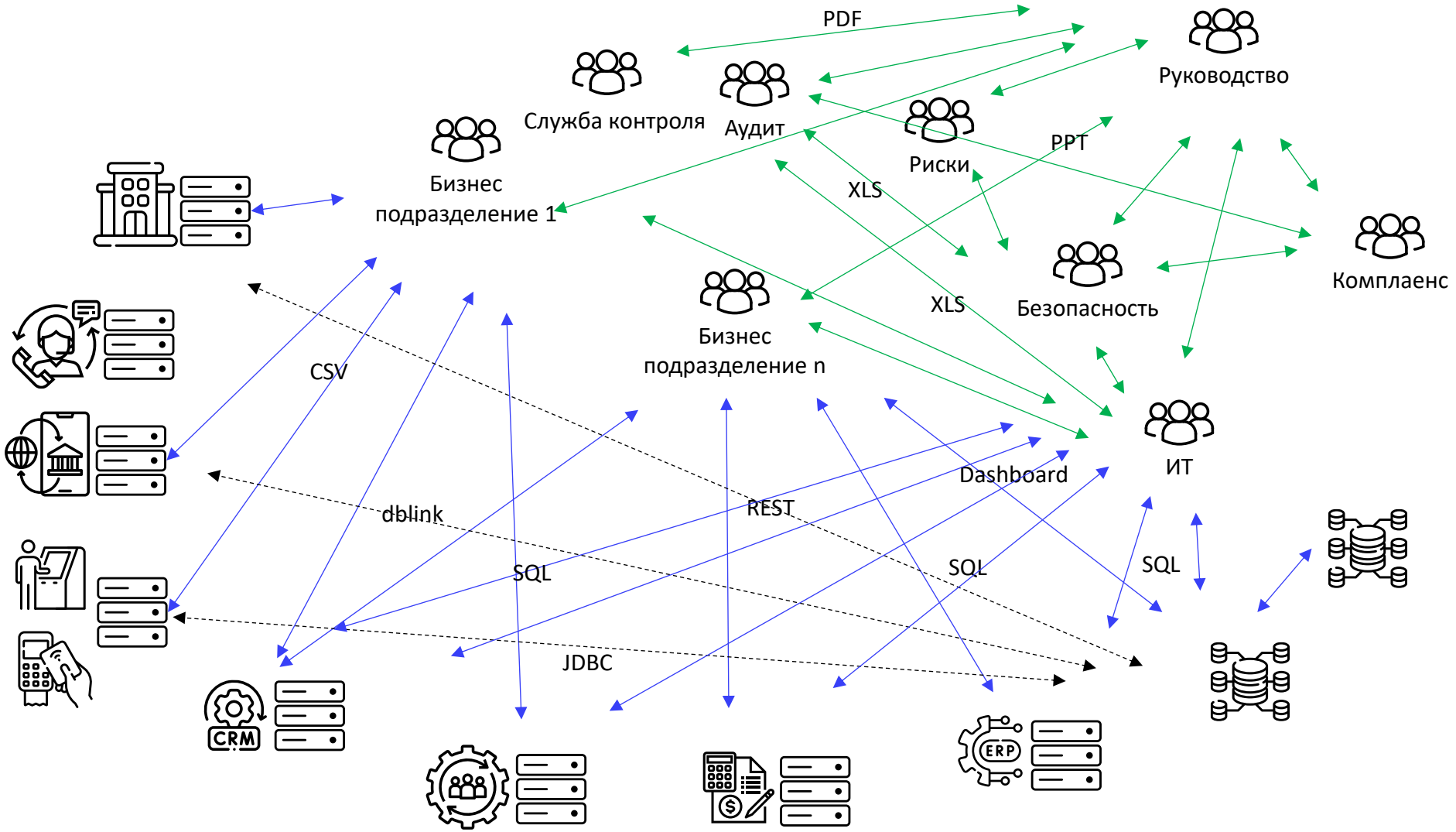
01

Большое количество и разнородность

участников, систем-источников, приложений, данных, их взаимодействий в части задач противодействия мошенничеству

Последствия:

- дублирование задач и ресурсов разными подходами и способами
- высокая сложность операций и управления
- повышенная продолжительность разработок и внедрений
- дороговизна
- разрозненность данных
- недостаточность данных ввиду отказа от задач или отсутствия доступа, а также разработок и внедрений
- невыявленные кейсы и риски
- сложность получения единой картины в масштабах всей организации
- прочие



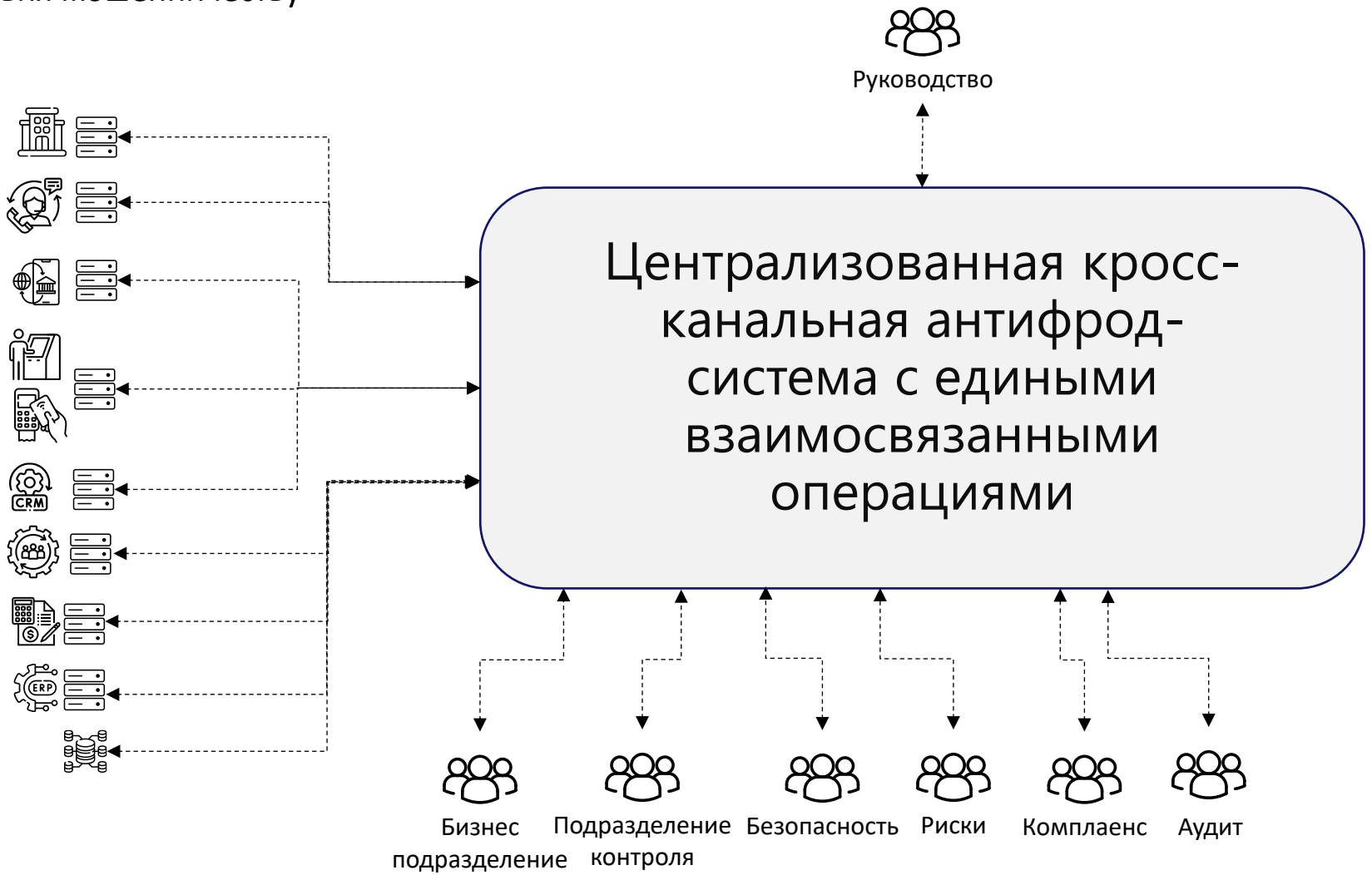
01

Большое количество и разнородность

участников, систем-источников, приложений, данных, их взаимодействий в части задач противодействия мошенничеству

Решение проблемы технически начинается с...

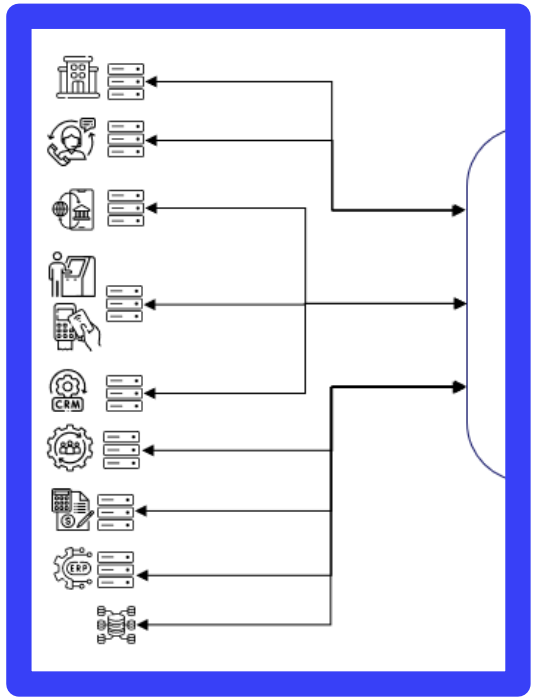
- Объединение всех необходимых каналов данных в одну центральную систему.
- Единые подходы и методы типичных операций по борьбе с фродом, например, анализ, подготовка к выявлению, выявление, реагирование.



01

Большое количество и разнородность

участников, систем-источников, приложений, данных, их взаимодействий в части задач противодействия мошенничеству



- Текстовые данные
  - Структурированные
  - Неструктурированные
- Картинки
- Видео
- Аудио

- Финансовые и транзакционные данные
- Поведенческие
- Социальные и репутационные
- Биометрические
- Геолокационные
- Технические, системные, сетевые

Системный подход к интеграции

- Запросы/ответ (синх./асинх.)
- Потоки
- Потоки запрос/ответ
- Пакетная обработка
- Пользовательская загрузка файлов

- Коннектор на получение
  - Ожидающий получение
  - С запросом на получение
- Коннектор для отправки

- Разрабатываемые и настраиваемые ИТ
- Конструируемые пользователем

Топ наиболее популярных протоколов, механизмов или архитектурных подходов:

- **REST API** – самый распространенный и универсальный.
- **gRPC** – для высоконагруженных систем с низкими задержками.
- **Kafka / RabbitMQ / прочие (Message Brokers)** – для асинхронных событий и обработки потоковых данных.
- **WebSockets / Webhooks** – для событий в реальном времени.
- **SFTP / Batch Processing** – для работы с большими объемами данных.

- ✓ Гибкость в аспектах интеграции
- ✓ Упрощение работы по созданию коннекторов – снижение зависимости от ИТ-специалистов

02

Неэффективная организация операций

ручной труд, слабая автоматизация плюс неупорядоченность

Последствия:

1. Низкая скорость реагирования

- Пока сотрудники вручную проверяют транзакции, мошенники успевают вывести деньги или скрыть следы.
- Медленное расследование инцидентов приводит к накоплению нерешенных случаев.

2. Высокие операционные затраты

- Нужен большой штат аналитиков для обработки потока подозрительных операций.
- Затраты на ручной труд растут быстрее, чем эффективность работы.

3. Ошибки и пропущенные случаи мошенничества

- Человеческий фактор: усталость, невнимательность, перегрузка → пропуск критических угроз.
- Нет стандартизированной обработки, каждый аналитик может работать по-разному.

4. Низкое качество клиентского сервиса

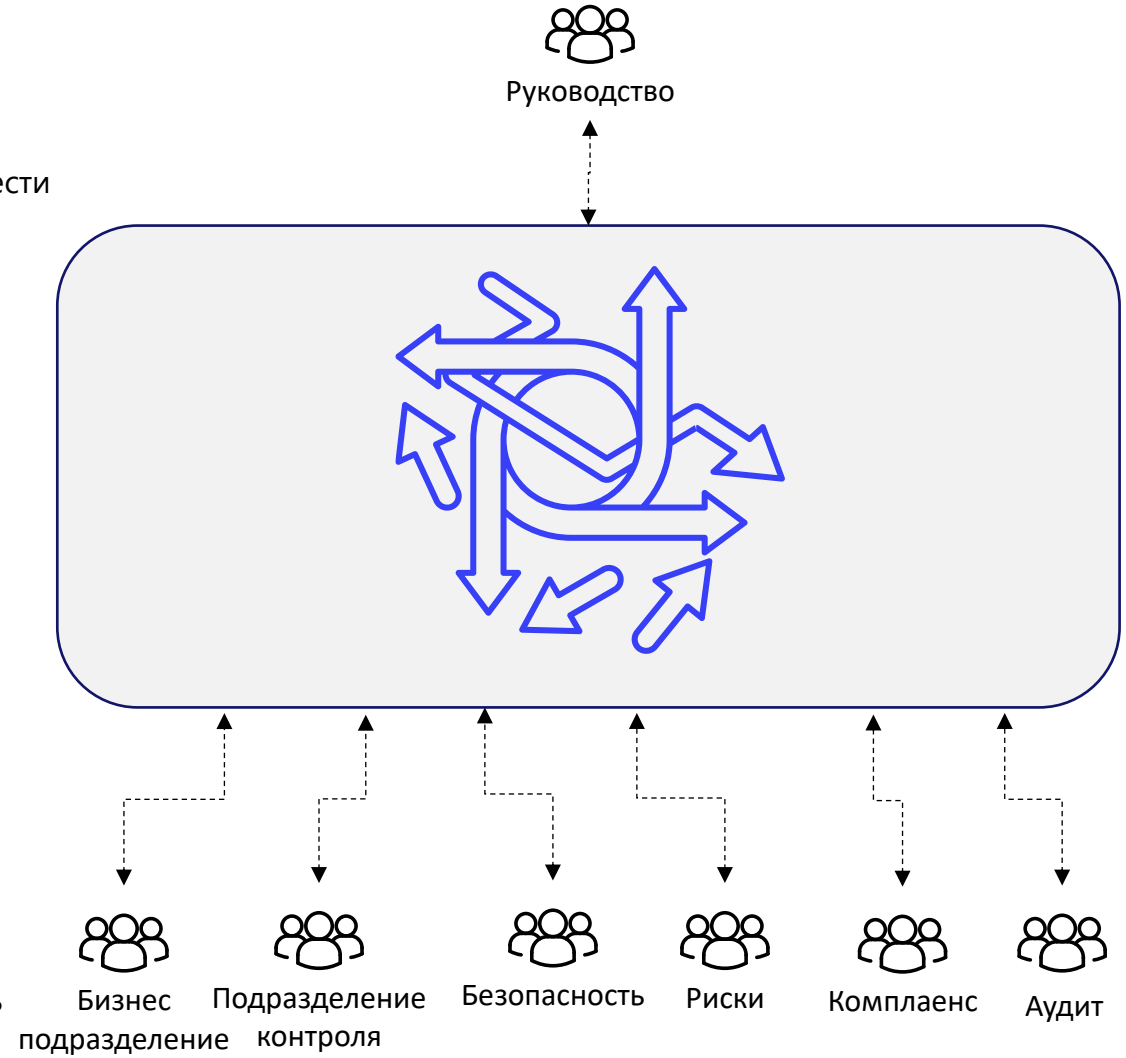
- Долгие проверки могут замораживать счета добросовестных клиентов.
- Негативный пользовательский опыт снижает доверие к компании.

5. Рост репутационных и юридических рисков

- Если мошенничество не выявляется вовремя, могут пострадать клиенты → судебные иски.
- Регуляторы могут наложить штрафы за несоблюдение требований по противодействию фроду.

6. Моральное выгорание сотрудников

- Перегруженность, рутина, стресс → снижение мотивации и высокая текучесть кадров.



02

Неэффективная организация операций

ручной труд, слабая автоматизация плюс неупорядоченность

Решение проблемы

- Упорядоченные автоматизированные и автоматические процессы
- Единые общие и интегрированные процессы
- Единые политики, процедуры и регламенты

03

Недостаточность покрытия данных

их отсутствие и плохое качество данных

- **Недостаточное покрытие данных** — система не получает данные из всех возможных источников.
- **Отсутствие данных** — критически важные данные отсутствуют вовсе, поступают с задержкой, либо их нет ввиду запрета доступа.
- **Плохое качество данных** — ошибки, пропуски, дубликаты и устаревшие данные затрудняют анализ.
- **Данные есть, но в организации не знают**, что они есть, или не знают, где они точно находятся.

03

Недостаточность покрытия данных

их отсутствие и плохое качество данных

Решение проблемы

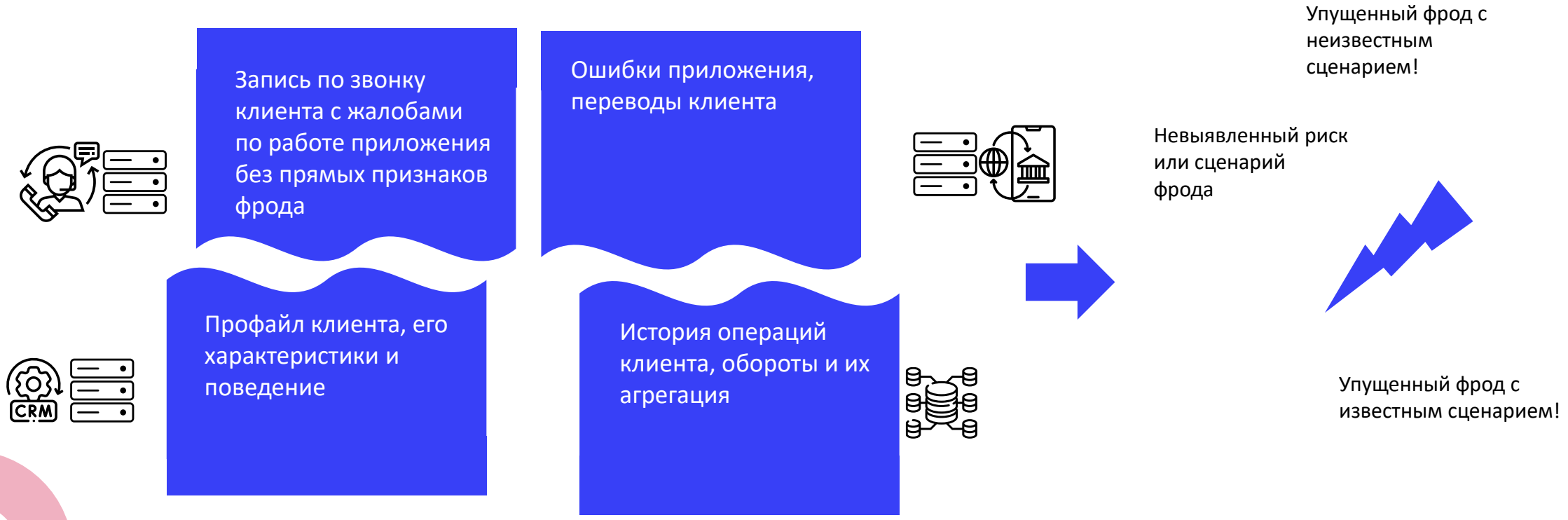
Недостаточное покрытие данных	Отсутствие данных	Плохое качество данных	Данные есть, но в организации не знают
• Рассмотрение других систем организации • Системы смежных отраслей • Экосистемы партнерств • Онлайн-сервисы • Государственные БД • Частные БД или сервисы	• Использование компенсационных прокси-метрик • Генерация синтетически данных на основе поведенческих паттернов • Использование алгоритмов для восстановления данных (например, метод ближайших соседей, интерполяция) • Анализ аномалий в имеющихся данных и выявление косвенных индикаторов мошенничества • Запросы в режиме реального времени (например, при динамической среде)	• Очистка • Нормализация • Стандартизация • Форматирование • Дедупликация • Контроль консистентности и кросс-валидация • Разрешение конфликтности • Обогащение • Дополнение данных • Data Governance • Контроли приложений • Мониторинг качества • Каталогизация и классификация • DWH, Data Lake	• Анализ и исследование существующих систем • Каталог данных • Управление знаниями • Data Governance • Автоматизация поиск данных • DWH, Data Lake • Обучение и коммуникации

04

Разрозненность и несогласованность данных

по фактическому и потенциальному мошенничеству

- Разрозненные источники и структуры данных
- Отсутствие или сложность сопоставления, корреляции, кросс-проверок и неактуальные данные для сопоставления
- В рамках разных или одних и тех же систем или каналов



04

Разрозненность и несогласованность данных

по фактическому и потенциальному мошенничеству

Решение проблемы

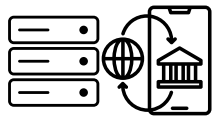
- Связывание разных данных в рамках разных или одних и тех же систем или каналов (SQL (Select, Join, etc.), SPL, специальные приложения)
- Корреляция событий
- Комплексное правило по анализу и выявлению по данным из разных коннекторов, систем, или каналов
- Заранее соединенные и согласованные данные из DWH, Data Lake

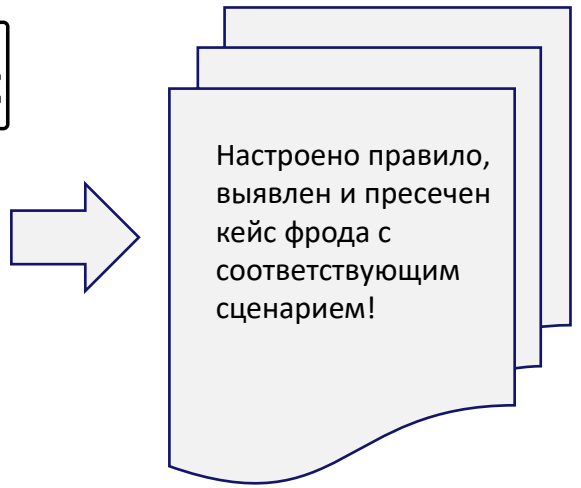
Запись по звонку клиента с жалобами по работе приложения без прямых признаков фрода

Ошибки приложения, переводы клиента

Профайл клиента, его характеристики и поведение

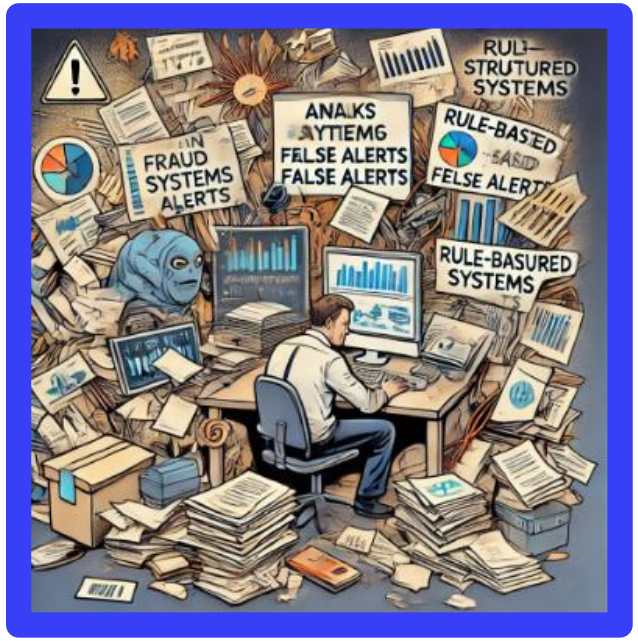
История операций клиента, обороты и их агрегация





05

Слабая аналитика
и моделирование



- **Отсутствующий анализ**
- Доминирование **rule-based** подхода (правила на основе известных шаблонов или сценариев с простой логикой)
- **Недостаточная глубина** анализа – поверхностная обработка данных, слабый анализ поведенческих паттернов.
- **Неприменимость к неструктурированным данным** (неструктурированный текст, изображения, видео, звук)
- **Слабая интерпретируемость** результатов:
  - Антифрод-система дает высокую долю ложноположительных срабатываний.
  - Бизнес не понимает, почему система блокирует транзакции или клиентов.
  - Аналитика не дает четких рекомендаций по корректировке правил.
- **Невозможность или ограниченность детекции новых схем**, в том числе ввиду человеческого фактора и недостаточной развитости управления рисками фрода
- **Невозможность или проблемы подачи данных** разного вида
- **Невозможность или проблемы применения одновременно нескольких разных аналитик**, особенно разного вида
- **Плохая системность** управления аналитикой

05

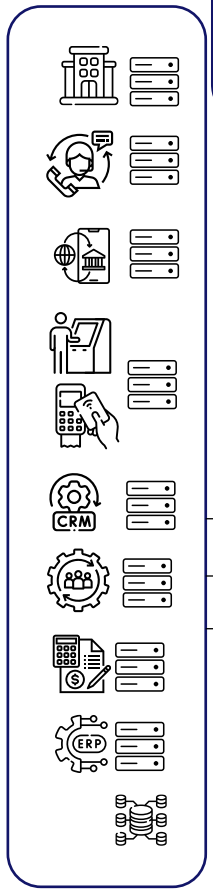
Слабая аналитика
и моделирование

- Запросы/ответ (синх./асинх.)
- Потоки
- Потоки запрос/ответ
- Пакетная обработка
- Файлы

Текстовые данные
- Структурированные
- Неструктурированные

Изображения
Видео
Аудио

Обычные — быстрые, но легко обходятся.
ML (регрессия, деревья решений) — объясним, но не всегда точен.
Глубокие нейросети (Deep Learning) — мощные, но требуют много данных и сложно интерпретируются.
Графовые модели — хорошо выявляют сложные схемы фрода, но работают медленно



Получение данных
- Список связей – CRM-система
- Список дропперов (Антифрод-центр)
- Платежи клиента – Канал обслуживания 3
- Действия пользователя – Система мобильного приложения
- Видео файл двухфакторной аутентификации – Система мобильного приложения
- Запись (последние разговоры) – Система колл-центра
- Изображение лица с удостоверения – Гос. система

Анализ, расчеты /скоринг/ выявление
- Правило проверки наличия необычных получателей с аномально высокой суммой платежа
- Провило проверки на наличие в списках дропперов
- ML, изучающий связи, при наличии нового получателя
- Нейросеть по выявлению аномалий, обученная на данных платежей всего банка, в том числе анализируя логи
- Нейросеть по сопоставлению изображения лица: видео-файл и удостоверение, проверяющая аудио-записи на наличие подозрительных моментов

Функционирование модели антифрод-системы в части получения и анализа данных.
Пример проверки платежа.

Решение проблемы

06

Быстрое развитие схем и методов мошенничества

и низкая адаптивность компании

- **Отсутствие механизмов быстрой настройки правил** и алгоритмов под новые схемы.
- **Слабая или отсутствующая предикция или прогнозирование:** схемы и кейсы.
- **Отсутствие технической стратегии проактивной защиты.**
- **Статичная антифрод-система** (вендор).
- **Запаздывающая реакция и низкая скорость принятия решений –** бюрократия и медленные внутренние процессы мешают оперативному реагированию.
- Низкая адаптивность **по другим факторам**: персонал, культура, прочее.

Решение проблемы: развитие и внедрения по исправлению соответствующего недостатка

07

Неготовность к проверкам онлайн или их отсутствие

в т.ч. по большим потокам транзакций

- **Отсутствие или недостаточная онлайн-проверка транзакций** – операции в реальном времени не анализируются.
- **Неготовность к высоконагруженным проверкам** – система не справляется с анализом больших объемов транзакций.
- **Запаздывающая реакция на мошенничество** – угрозы выявляются постфактум, а не на этапе совершения операции.
- **Ручной или выборочный** контроль – проверки осуществляются случайным образом, без комплексного охвата.
- **Ограниченные вычислительные мощности** – недостаточные ресурсы для обработки потока транзакций в режиме онлайн.
- **Отсутствие масштабируемости** – рост нагрузки приводит к сбоям или отключению антифрод-функционала.
- **Высокий риск упущенных инцидентов** – мошеннические операции проходят незамеченными из-за низкой скорости анализа.

07

Неготовность к проверкам онлайн или их отсутствие

в т.ч. по большим потокам транзакций

Специальные ИТ-технологии, используемые в антифрод-системах для решения проблемы

- **In-Memory DBMS** – системы управления базами данных, которые хранят все данные в оперативной памяти (RAM) вместо традиционных дисков.
- **Потоковая обработка данных (Stream Processing)** – если необходимо анализировать и реагировать на данные в реальном времени (например, обнаружение аномалий).
- **Очереди сообщений (Message Brokers)** – если нужно эффективно передавать потоки транзакций между различными компонентами системы.
- **NoSQL базы данных** – если нужен быстрый доступ к данным без строгой схемы хранения.
- **Аналитические базы данных (OLAP)** – если требуется быстрая аналитика и сложные SQL-запросы в режиме реального времени.
- **Гибридные базы данных (HTAP - Hybrid Transactional/Analytical Processing)** – если нужно одновременно быстро обрабатывать транзакции и делать real-time аналитику.
- **Графовые базы данных** – если необходимо анализировать связи между транзакциями и пользователями (например, для выявления мошеннических схем).
- **Кэширование и ускорение обработки** – если необходимо ускорить обработку за счет кэширования данных.
- **Машинное обучение в реальном времени**– если требуется анализ транзакций с применением ML-моделей.
- **High-Performance Event Processing (CEP - Complex Event Processing** – если требуется обнаруживать аномалии или мошенничество на основе сложных событийных паттернов.
- **Аппаратные ускорители для транзакционной обработки** – если требуется минимальная задержка в high-load транзакционных системах.

08

Конфликт интересов

при борьбе с фродом или управлении риском фрода

Бизнес подразделение

- Против проверок и воздействия на клиентов: качество обслуживания.
- Против дополнительных расходов и/или временных издержек.
- Боязнь потери собственной репутации ввиду упущений по мошенничеству, сокрытие, уклонение.
- Сотрудники бизнес-подразделения могут быть сами внутренними фродерами.

Безопасность/ИБ

- Чрезмерно строгие или жесткие меры или подходы, что усложняет работу, создает проблемы организации и клиентам.
- Превышение полномочий.
- Использование слабой или отсутствующей доказательной базы, опора на субъективные суждения.
- Недостаточная оценка влияния на бизнес.
- Отказываются отвечать за борьбу с фродом в масштабах всей организации.

Риски

- Могут не углубляться в вопросах рисков фрода либо применяют подход верхнего уровня, при этом, в организации никто так и не делает такое углубление.
- Могут требовать дорогостоящие меры.
- Требования рисков могут замедлять внедрение новых технологий и увеличивать сложность систем.
- Иногда наделение ответственностью за 1-ю линию защиты СВК.

Комплаенс

- Требование строгого KYC и AML, что усложняет привлечение клиентов.
- Требование соблюдения регуляторных антифрод требований может увеличивать затраты и снижать рентабельность.
- Требование внедрения сложных процессов проверок, что замедляет разработку новых продуктов.
- Требование блокировки или заморозки подозрительных аккаунтов, что приводит к жалобам клиентов.
- Требование строгих формальных процедур, что может замедлять оперативную борьбу с мошенниками.

Аудит

- Часто, одновременно проверяет, внедряет и расследует антифрод-контроль, что создаёт риск необъективности
- Разные цели аудита и антифрода
- Просьбы не «выносить сор из избы»
- Давление и ограничения со стороны менеджмента

09

Отсутствие единой картины

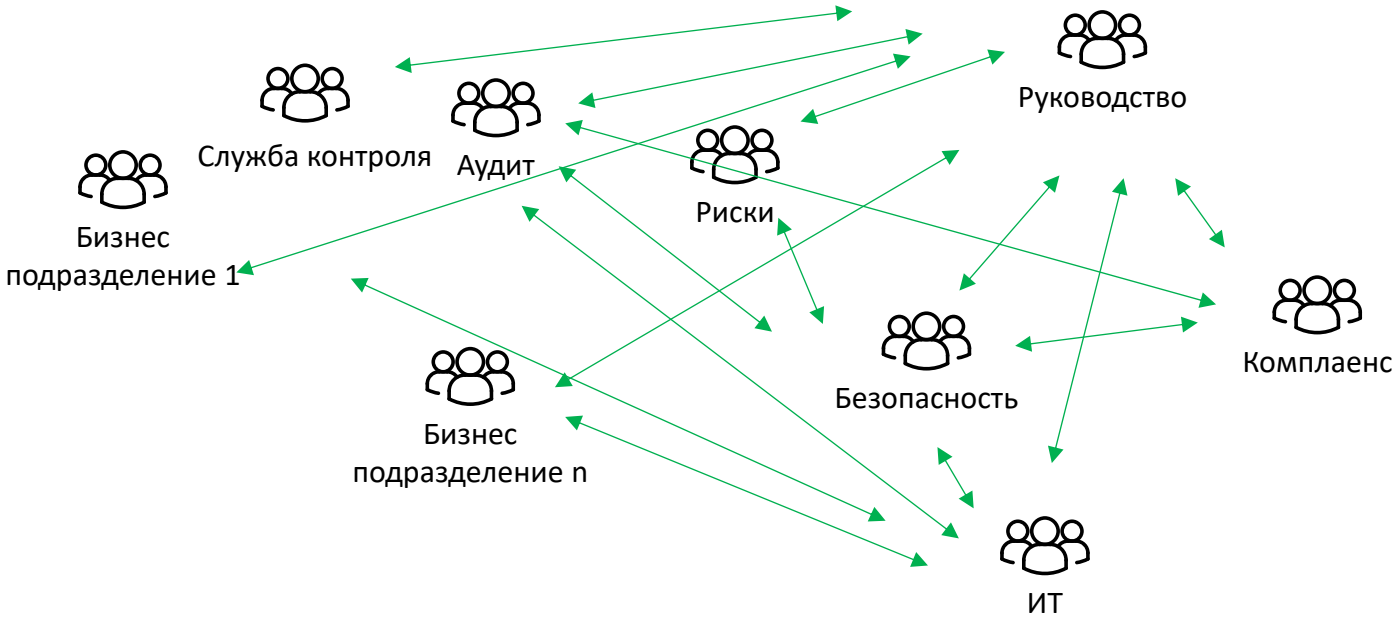
в части состояния противодействию фроду, в части рисков фрода, эффективности их управления

	Бизнес подразделение	Подразделение контроля	Безопасность	Руководство	Риски	Комплаенс	Аудит
Выявление и анализ случаев фрода	• Обозначение того, что «всплыло». • Фиксация и предоставление «удобных» кейсов. • Информирование руководства. • Обычно систематического учета и аналитики кейсов нет.	• Обычно специальной цели выявления именно кейсов фрода нет – только действия в рамках прописанных процедур • Фиксация скорее нарушений, отклонений, ошибок, нежели кейсов. • Предоставляют всю информацию по кейсам, если политически корректно.	• Выявление, регистрация и анализ с точки зрения действующих и виновных лиц. • Обычно большинство кейсов засекречено и недоступно другим подразделениям. • Предоставляют важную информацию руководству и ключевым партнерам должностным лицам.		• Сбор и регистрация кейсов по подразделениям • Отдельные проверки и расследования.	• AML кейсы, часто, не больше, не меньше. • «Горячие» линии. • Могут делиться информацией с подразделениями 2 и 3линии защиты СВК. • Аналитика для руководства в части AML	• Кейсы, выявленные на плановых и внеплановых проверках. • «Горячие» линии. • Кейсы, «спущенные» руководством, в т.ч. для расследования • Аналитика в рамках отдельной проверки и годовой отчетности, часто фрагментарная.
Идентификация, анализ и оценка фрод рисков	• При бизнес-планировании риски либо рассматривается поверхностно, либо не рассматриваются вовсе. • Аналитика от случая к случаю.	• Идентификация, анализ и оценка рисков скорее комплаенс (внутренний), нежели фрода.	• При бизнес-планировании риски либо рассматривается поверхностно, либо не рассматриваются вовсе.		• Реестр рисков на основе кейсов и проверок. • Идентификация и оценка по классам и субклассам, в том числе с использованием best-practice классификаторов, например, ACFE Fraud Tree, но, часто, не более (классов).	• Идентификация, анализ и оценка в рамках обработки инцидентов AML. • Реестр рисков AML на основе сценариев от регулятора.	• При действительно риск-ориентированных подходах. • Аналитика в рамках отдельной проверки и годовой отчетности.

10

Сложность управления

включая планирование, формирование отчетности и мониторинг



08

Конфликт интересов

при борьбе с фродом или управлении риском фрода

09

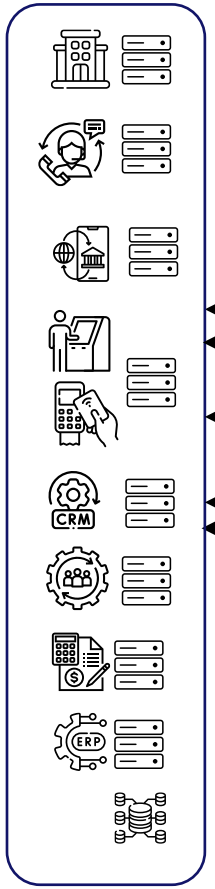
Отсутствие единой картины

в части состояния противодействию фроду, в части рисков фрода, эффективности их управления

10

Сложность управления

включая планирование, формирование отчетности и мониторинг



Комплексное решение проблемы:

единая централизованная антифрод-система + антифрод-подразделение, в т.ч. как оркестратор борьбы с фродом

Руководство

Антифрод-подразделение

Антифрод аналитики и методологи

ИТ

Колл-центр по борьбе с фродом

Создание, настройка, управление антифрод-моделями

Управление рисками фрода: идентификация, анализ, оценка, обработка, мониторинг, реестр риско, риск-профиль

Планирование

«Управленческая» отчетность по фроду

Функционирование созданной и настроенной антифрод-модели

Получение данных
- Коннектор 1
- Коннектор …
- Коннектор n

Анализ, расчеты /скоринг/ выявление
- Правило 1
- Правило …
- Правило n

Обработка / реагирование
- Пропуск
- Блокировка
- Приостановка для пров.

Отправка данных
- Коннектор 1
- Коннектор …
- Коннектор n

Хранилище данных на проверку

Ручные проверки и аналитика

История проверок

Управл. списками

KYC

Визуализ. связей

Управление инцидентами фрода

«Оперативная» отчетность и аналитика

Бизнес подразделение

Подразделение контроля

Безопасность

Риски

Комплаенс

Аудит

08

Конфликт интересов

при борьбе с фродом или управлении риском фрода

09

Отсутствие единой картины

в части состояния противодействи ю фроду, в части рисков фрода, эффективности их управления

10

Сложность управления

включая планирование, формирование отчетности и мониторинг

Примеры показателей для планирования и отчетности

- **уровень мошенничества** – отношение пропущенных мошеннических транзакций к общему количеству транзакций;
- **«давление» мошенничества** – отношение количества попыток мошеннических транзакций к общему количеству транзакций;
- **уровень одобрения** – отношение количества одобренных транзакций к общему количеству транзакций;
- **точность антифрод системы** – отношение мошеннических транзакций к общему количеству отклоненных транзакций;
- **уровень отклонений** - отношение количества отклоненных транзакций к общему количеству транзакций;
- **качество одобрения** - отношение одобренных транзакций, которые действительно оказались не мошенническими, к общему числу одобренных транзакций;
- **«индекс антифрод системы»** - отношение остановленного антифрод системой мошенничества к пропущенным случаям;
- **«коэффициент обнаружения»** - процент мошеннических транзакций, которые обнаруживаются из всех мошеннических транзакций;
- **среднее время реагирования** команды по расследованиям на инцидент мошенничества;
- **коэффициент чарджбэков** – процент транзакций, которые приводят к возвратным платежам клиентам и прочим сторонам;
- **уровень ручной проверки** – измеряет процент транзакций, которые требуют ручной проверки командой антифрода.

Дополнительные вызовы проектам внедрению антифрод-систем

- Сильное сопротивление изменениям
- Недостаточная развитость процессов бизнеса и ИТ
- Сложность интеграции

✓ Компетентность команды и ее демонстрация, принося реальную пользу

✓ Высокая клиентоориентированность

✓ Финансово-экономическое обоснование

✓ Хорошая техническая документация

✓ Активные прямые коммуникации с исполнителями ИТ и бизнес-подразделений

РЕШЕНИЯ

Будущее развития антифрод-систем

Будущее антифрод-систем — это умные, автономные и самонастраивающиеся решения, использующие ИИ, блокчейн и биометрию. Всё движется к сверхбыстрому выявлению мошенников и их действий в реальном времени.

✓ Гибридные ИИ модели:

- Классический ML (объяснимость + интерпретируемость)
- + Глубокие нейросети (высокая точность + адаптивность)
- + Графовый анализ (поиск скрытых мошеннических связей)
- + Генеративный ИИ (построение симуляций атак)

✓ Самообучение в реальном времени на новых данных

✓ Автоматическое развернутое описание принятых решений

✓ Автономность в выявлении и блокировании, авто адаптация

✓ Алгоритмы квантовой эры: аналитика и меры

Вопросы-ответы

СПАСИБО

З А В Н И М А Н И Е

ACFE
Association of Certified Fraud Examiners
KAZAKHSTAN CHAPTER

SYMTECH

WhatsApp: +7 708 535 69 61, E-mail: a.daltaev@symtech.kz