ООО «ИКС ЛАБЗ»
г. Москва, вн.тер.г. муниципальный округ Тверской,
ул. Новослободская, д. 24а, стр. 2, кв. 26

ОГРН 1237700394480
ИНН/КПП 9707001238/770701001
Тел. +7 985 923-09-90, email: info@x-labs.ru

XLCORE

Техническое описание

Версия 2

24.02.2025

Оглавление

1. Основные виды мошенничества в телекоммуникационной отрасли

Мошенничество в области телекоммуникаций представляет собой серьезную угрозу для операторов связи, поскольку оно может существенно повлиять на их прибыльность, репутацию и финансовую стабильность. Существуют различные типы мошенничества, которые могут варьироваться от простых случаев использования услуг без оплаты до более сложных схем, включающих высокотехнологичные методы взлома и манипуляции с данными.

Основные виды мошенничества в телекоммуникационной сфере для борьбы с которыми применяется XLCORE:

1. Мошенничество с международным разделением доходов (IRSF)

Мошенники арендуют премиальные телефонные номера и взламывают телефонные системы компаний, чтобы автоматически совершать звонки на эти номера. В результате организация получает огромные счета, а злоумышленники получают процент от тарифа на вызовы. Чаще всего такие звонки совершаются в нерабочее время, что затрудняет своевременное обнаружение атаки. В отличие от банковской сферы, механизмов защиты, аналогичных чарджбэкам, в телекоммуникациях нет.

2. Wangiri-мошенничество

Название происходит от японского выражения «один звонок и сброс». Мошенники совершают короткие звонки с незнакомых номеров, провоцируя жертву на обратный вызов, который соединяет её с премиальным платным номером. Существует и SMS-вариант атаки, когда абоненту приходит сообщение с просьбой срочно перезвонить или ответить на SMS. Основным индикатором атаки является всплеск трафика на номера с повышенными тарифами, что можно отслеживать с помощью систем мониторинга.

3. Обход межсетевого соединения (SIM-box fraud)

Мошенники используют SIM-боксы для нелегальной маршрутизации международных звонков через дешёвые местные каналы связи, вместо того чтобы пропускать вызовы по официальным межоператорским маршрутам. Это снижает их затраты, но конечный пользователь продолжает платить стандартную цену. В результате операторы теряют доходы, а качество связи ухудшается.

4. Телеком-арбитраж

Мошенники используют разницу в тарифах на международные звонки между странами. Они заявляют, что соединяют вызовы напрямую между странами, но фактически перенаправляют их через третью страну с более низкими тарифами, извлекая выгоду из разницы. Это приводит к финансовым потерям операторов и нарушению их тарифных моделей.

5. Взлом корпоративных АТС

Злоумышленники получают несанкционированный доступ к IP-АТС организаций, используя слабые пароли, уязвимости в ПО или неправильно настроенные системы. После этого они совершают мошеннические звонки, чаще всего в рамках IRSF, перенаправляя вызовы на премиальные номера. Компании обнаруживают атаку только при получении счетов за связь. Защита включает строгие меры контроля доступа, мониторинг активности и своевременное обновление ПО.

6. Манипуляция трафиком

Некоторые региональные операторы искусственно увеличивают количество вызовов в свои сети, чтобы получать повышенные компенсационные выплаты. Это достигается путём привлечения мошеннического или нежелательного трафика через массовые автоматические вызовы. В результате крупные операторы несут убытки, а клиенты могут столкнуться с ростом тарифов.

7. Депозитное мошенничество

Мошенники используют украденные данные кредитных карт для покупки SIM-карт и мобильных устройств через онлайн-магазины операторов. Впоследствии владелец карты инициирует чарджбэк, а оператор несёт финансовые потери. Основные меры защиты включают использование решений для предотвращения чарджбэков, мониторинг подозрительных покупок и двухфакторную аутентификацию клиентов.

8. Мошенничество с подписками

Преступники оформляют контракты на мобильные устройства, используя поддельные документы и украденные данные. После получения смартфонов они взламывают защиту устройств и продают их на вторичном рынке. В результате оператор остаётся с неоплаченными счетами. Чаще всего мошенники используют краденные личные данные, купленные в даркнете. Повышенный риск связан с покупками в розничных точках, так как там легче использовать фальшивые документы.

9. Перехват учётных записей

Злоумышленники получают доступ к личным аккаунтам пользователей операторов, используя украденные логины и пароли. Это позволяет им изменять настройки, оформлять подписки или приобретать устройства от имени жертвы. Операторы должны внедрять многофакторную аутентификацию и системы мониторинга подозрительной активности.

10. Фишинг через SMS

Этот вид мошенничества основан на массовой рассылке SMS с фальшивыми ссылками, ведущими на сайты для кражи персональных данных. Мошенники используют специализированные сервисы для проверки номеров на мобильность (чтобы избежать

блокировок), а также создают собственные платформы для перепродажи украденных данных. Несмотря на рост числа атак, уровень осведомлённости пользователей о таких угрозах остаётся низким.

11. Замена SIM-карты

Злоумышленники переносят номер жертвы на новую SIM-карту, получая контроль над SMS и звонками, включая одноразовые пароли и двухфакторную аутентификацию. Это позволяет им взламывать банковские счета, соцсети и криптовалютные кошельки жертвы. Операторы внедряют дополнительные уровни защиты, требуя подтверждения личности перед сменой SIM-карты.

В таблице 1 указаны характеристики упомянутых выше видов мошенничества в телекоммуникационной отрасли.

Таблица 1. Характеристики видов мошенничества в коммуникационной отрасли

	Мошенничество с голосовой связью и SMS	**Высокие счета**	**Отток клиентов**	**Нарушение конфиденциальности**	**Убытки от доходов**	**Ущерб репутации**
Мошенничество с международным разделением доходов (IRSF)	✓	✗	✗	✗	✓	✓
Обход межсетевого соединения (SIM-box fraud)	✓	✓	✓	✗	✓	✓
Телеком-арбитраж	✓	✗	✗	✗	✓	✗
Взлом корпоративных АТС	✓	✗	✗	✓	✓	✓
Манипуляция трафиком	✓	✗	✗	✗	✓	✗
Депозитное мошенничество	✓	✓	✗	✗	✓	✗
Мошенничество с подписками	✓	✓	✗	✗	✓	✗
Перехват учётных записей	✓	✓	✗	✓	✓	✓
Фишинг через SMS	✓	✓	✓	✓	✓	✓
Wangiri-мошенничество	✓	✓	✓	✗	✓	✓
Замена SIM-карты	✓	✗	✗	✓	✓	✓

Платформа XLCORE относится к классу FMS (система управления мошенничеством) и разработана компанией X-Labs для эффективного выявления, расследования и предотвращения мошеннических действий.

2. Функциональные возможности системы XLCORE

XLCORE — это система управления мошенничеством, обеспечивающая комплексный мониторинг, анализ и предотвращение фрода в телекоммуникационной отрасли. Система интегрируется с любыми источниками данных, использует передовые алгоритмы машинного обучения, автоматизирует управление кейсами и предоставляет гибкую отчетность.

Функциональные возможности XLCORE:

1. **Интеграция с любыми типами данных**

XLCORE позволяет операторам связи агрегировать данные из различных источников, обеспечивая полный охват возможных мошеннических схем. Ключевые возможности:

- Гибкая интеграция с любыми системами сбора данных: поддержка Kafka, Pub/Sub, API, потоковых данных и файловых хранилищ.
- Обработка широкого спектра событий: голосовые вызовы, SMS/MMS, IP-трафик, VoIP, роуминговые записи, GPRS/3G/4G/5G сессии, транзакции мобильной коммерции (m-commerce).
- Поддержка мультиформатных данных: CDR, IPDR, данные биллинга и CRM.
- Интеллектуальная ETL-обработка: автоматическая нормализация, дедупликация, обогащение данных и настройка бизнес-логики.
- Гибкость системы позволяет быстро адаптироваться к новым требованиям бизнеса и изменениям в ландшафте угроз.

2. **Интеллектуальная обработка данных**

XLCORE использует передовые алгоритмы машинного обучения (ML) и искусственного интеллекта (AI), обеспечивая:

- Автоматическое выявление мошеннических схем с высокой точностью и минимальными ложными срабатываниями.
- Гибкую настройку детекционных правил: поддержка пороговых, географических, поведенческих, ML- и паттерн-ориентированных правил.
- Обнаружение скрытых угроз с помощью моделей, анализирующих данные в режиме реального времени.

3. Кейс-менеджмент

XLCORE интегрируется с существующими системами управления расследованиями и предлагает широкий набор инструментов для эффективного управления кейсами:

- Централизованное управление расследованиями: сбор информации о мошеннических действиях, хранение доказательной базы.
- Автоматическое назначение задач: перераспределение кейсов на основе предопределенных правил и нагрузки аналитиков.
- Механизмы эскалации и совместной работы: обмен информацией между аналитическими, техническими и бизнес-командами.

Эти возможности позволяют значительно сократить время на обработку кейсов и повысить эффективность аналитиков.

4. Отчетность и аналитика

XLCORE интегрируется с BI-системами и аналитическими платформами клиента, предоставляя мощные инструменты отчетности и анализа:

- Гибкий конструктор отчетов: возможность создания кастомизированных отчетов в табличном и графическом виде.
- Визуализация сложных мошеннических схем: инструмент Link Analysis помогает выявлять связи между подозрительными субъектами.
- Интерактивные дашборды: отображение ключевых показателей эффективности (KPI), динамики фрода и статистики расследований.
- Автоматизированная генерация отчетов: поддержка различных форматов (PDF, Excel, JSON, API-выгрузки).

3. Конвейер обработки данных для выявления и предотвращения мошенничества в XLCORE

В общем виде процесс обработки данных и выявления мошеннических схем реализованный в XLCORE выглядит следующим образом:

1. **Сбор данных:** XLCORE интегрируется с различными источниками данных — от голосовых вызовов и SMS до IP-трафика и транзакций мобильной коммерции. Она поддерживает гибкие форматы данных, такие как CDR, IPDR, данные биллинга и CRM, а также может работать с потоковыми данными (например, Kafka или Pub/Sub). Все эти данные агрегируются и передаются в систему для дальнейшего анализа.

2. **Обработка данных:** программа автоматически выполняет ETL-обработку (извлечение, преобразование и загрузка данных). Она нормализует, дедуплицирует и обогащает данные, чтобы привести их к единому стандарту. Эти данные затем проходят через интеллектуальные алгоритмы, которые готовят их для анализа на более глубоком уровне.

3. **Настройка правил детекции:** система позволяет настроить различные типы детекционных правил. Это могут быть:

    - Пороговые правила, которые реагируют на определенные значения или изменения в данных (например, слишком высокая активность в сети за короткий промежуток времени).
    - Географические правила, которые отслеживают необычные паттерны активности в определенных регионах.
    - Поведенческие правила, анализирующие привычки пользователей и выявляющие отклонения от нормальных паттернов.
    - ML- и паттерн-ориентированные правила, которые основаны на машинном обучении и анализе предыдущих случаев мошенничества для выявления новых угроз.

4. **Обнаружение мошенничества:** на основе настроенных правил система автоматически анализирует данные в реальном времени, выявляя аномалии или подозрительные действия, которые могут указывать на мошенничество. Для этого XLCORE использует передовые алгоритмы машинного обучения и искусственного интеллекта, которые позволяют не только находить известные схемы мошенничества, но и выявлять новые, ранее неизвестные угрозы.

5. **Анализ скрытых угроз:** система использует самообучающиеся модели, которые могут обнаруживать скрытые угрозы, даже если они не были заранее прописаны в правилах. Эти модели анализируют данные в реальном времени, сравнивая их с историческими данными и выявляя потенциальные аномалии, которые могут быть признаком мошенничества.

6. **Сигнализация и уведомления:** как только система обнаруживает подозрительные действия, она генерирует сигнал или уведомление для аналитиков. В случае обнаружения угроз, таких как атаки на уровне SS7 или VoIP, XLCORE может оперативно отреагировать, предотвращая их до того, как они причинят серьезный ущерб.

7. **Управление кейсами и расследованиями:** все обнаруженные случаи фрода автоматически создаются как кейсы, которые поступают в систему управления расследованиями. XLCORE предоставляет аналитикам инструменты для эффективного

управления расследованиями: автоматическое распределение задач, механизм эскалации и совместной работы между различными командами (анализ, технические специалисты, бизнес-отделы).

8. **Отчетность и визуализация:** вся информация о фроде собирается в централизованных отчетах и дашбордах, которые наглядно показывают динамику мошенничества, связи между подозрительными субъектами и ключевые показатели эффективности. Эти отчеты можно кастомизировать под потребности бизнеса, чтобы аналитики могли принимать информированные решения.

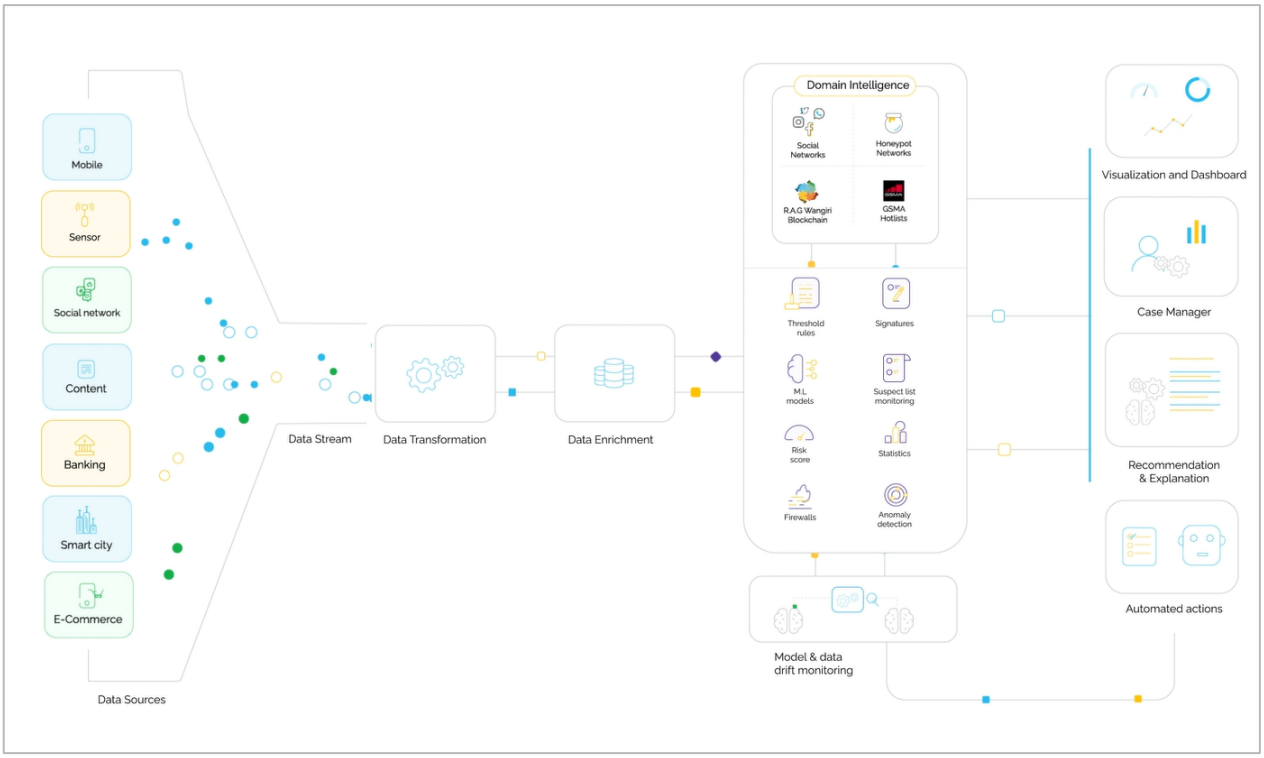

Рисунок 1. Конвейер обработки данных для выявления и предотвращения мошенничества в XLCORE

Таким образом, XLCORE обеспечивает непрерывный мониторинг, анализ и предотвращение мошенничества, позволяя своевременно выявлять угрозы, минимизировать убытки и повышать общую безопасность в телекоммуникационной сети.

Заключение

XLCORE — это современное, высокотехнологичное решение для операторов связи, обеспечивающее надежную защиту от фрода в режиме реального времени. Благодаря мощным возможностям интеграции, интеллектуальному анализу данных, автоматизации кейс-менеджмента и гибкой отчетности, система позволяет не только выявлять мошеннические схемы, но и проактивно предотвращать новые угрозы, минимизируя финансовые потери и повышая эффективность бизнес-процессов.