



FDS:
СИСТЕМА
ПРЕДОТВРАЩЕНИЯ
МОШЕННИЧЕСКИХ
ОПЕРАЦИЙ

КЕЙС: ФРОД В БАНКЕ

ЧТО ПРОИЗОШЛО:

Мошенники купили на даркнет-рынке пустые банковские карты и данные держателей карт и сделали с их помощью «белый пластик» (дубликаты реальных карт). Поддельные карты выдали группе людей, которые одновременно начали снимать деньги в банкоматах и расплачиваться в интернет-магазинах.

Значительное число настоящих владельцев карт не успевает заблокировать карту, особенно если у них не было подключено смс-информирование об операциях.

УЩЕРБ ДЛЯ БАНКА:

до **2-4 млн руб.**
в течение нескольких
часов



** Фрод – (от англ. fraud «мошенничество») — вид мошенничества в области информационных технологий, в частности, несанкционированные действия и неправомерное пользование ресурсами и услугами в различных отраслях бизнеса: от ритейла до банковского сектора.*

КЕЙС: ФРОД В ОНЛАЙН-ИГРЕ

ЧТО ПРОИЗОШЛО:

Пользователь скупил на игровом рынке некий дешевый артефакт, а затем приобрел его сам у себя по огромной цене. Система автоматически подняла среднюю рыночную стоимость артефакта до небес, и находчивый игрок стал виртуальным мультимиллионером. Далее он предложил свои услуги другим пользователям за вознаграждение. Они уничтожали объекты, нагруженные артефактом, и получали за это большое количество очков лояльности. А согласно последнему обновлению игры за эти очки можно было купить по-настоящему ценные артефакты. Так наш игрок заработал приличную сумму реальных денег, а его клиенты обогатились виртуально в обход игровой экономики.

УЩЕРБ ДЛЯ РАЗРАБОТЧИКА ОНЛАЙН-ИГРЫ:

Игровая экономика на грани краха



КЕЙС: ФРОД В СЕТИ АЗС

ЧТО ПРОИЗОШЛО:

Оператор одной из бензоколонок проводила платежи клиентов через свою личную карту, выданную по программе лояльности. Кешбэк поступал в полное распоряжение мошенницы. Схему раскрыли, просмотрев список транзакций по картам за день: получалось, что владелец этой карты заправил бензином целую цистерну.

УЩЕРБ ДЛЯ СЕТИ АЗС:

126 000 руб.
в день



FDS INFOSECURITY

Fraud Detection System — система автоматизированного выявления мошеннических операций в информационных системах



полностью своя
разработка

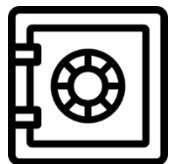


успешно работает более 6
лет
в крупных банках



обновляется при
появлении новых
мошеннических схем

СФЕРА ПРИМЕНЕНИЯ РЕШЕНИЯ



Финансы



E-commerce



Ритейл



Онлайн-игры

ЦЕЛИ АТАК



Платежные
шлюзы



АРМ
КБР



Автоматизированные
системы

ВИДЫ АТАК:

подмена платежей в канале связи

подмена / внедрение платежей в самой системе

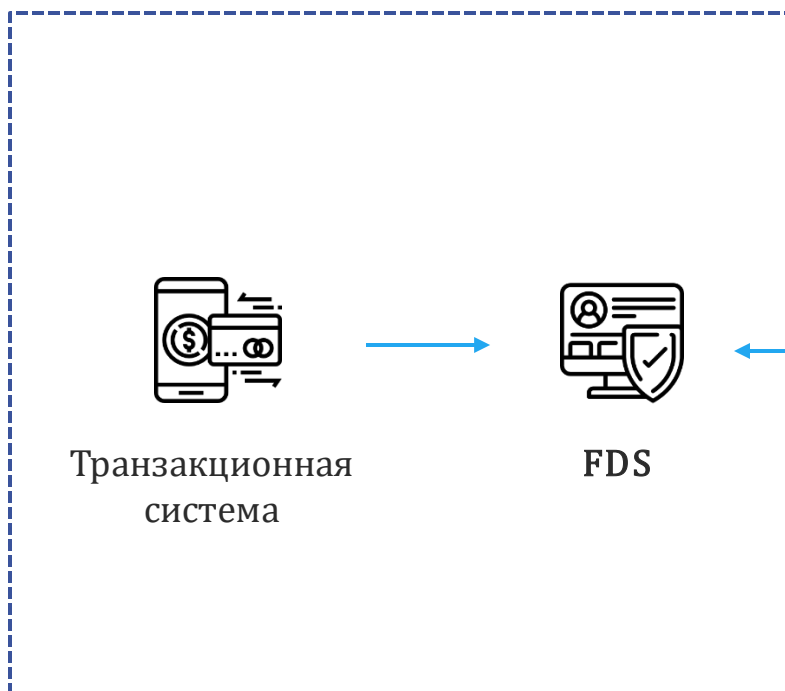
СРАВНЕНИЕ С ДРУГИМИ РЕШЕНИЯМИ

	Вендор 1	Вендор 2	Вендор 3	INFOSECURITY	Вендор 5
Поиск фрода по предоставленным данным	3	5	4	5	4
Непрерывность деятельности	5	4	5	5	5
Ролевая модель	5	5	5	5	4
Эксплуатация системы	5	4	4	5	4
Внутренняя безопасность	4	4	3	4	4
Аналитика	5	4	4	5	4
Контроль	5	5	4	5	3
Кредитование	5	5	4	5	3
Скорость внедрения решения	4	3	3	4	2
Итог	41	39	36	43	33

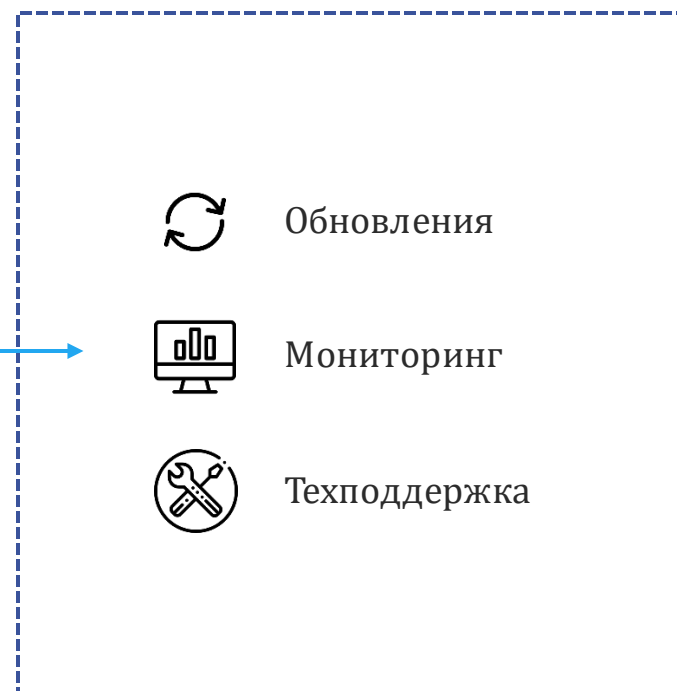
Сравнение проводилось заказчиком по внутренней методике.

СХЕМА FDS

ИНФРАСТРУКТУРА КЛИЕНТА

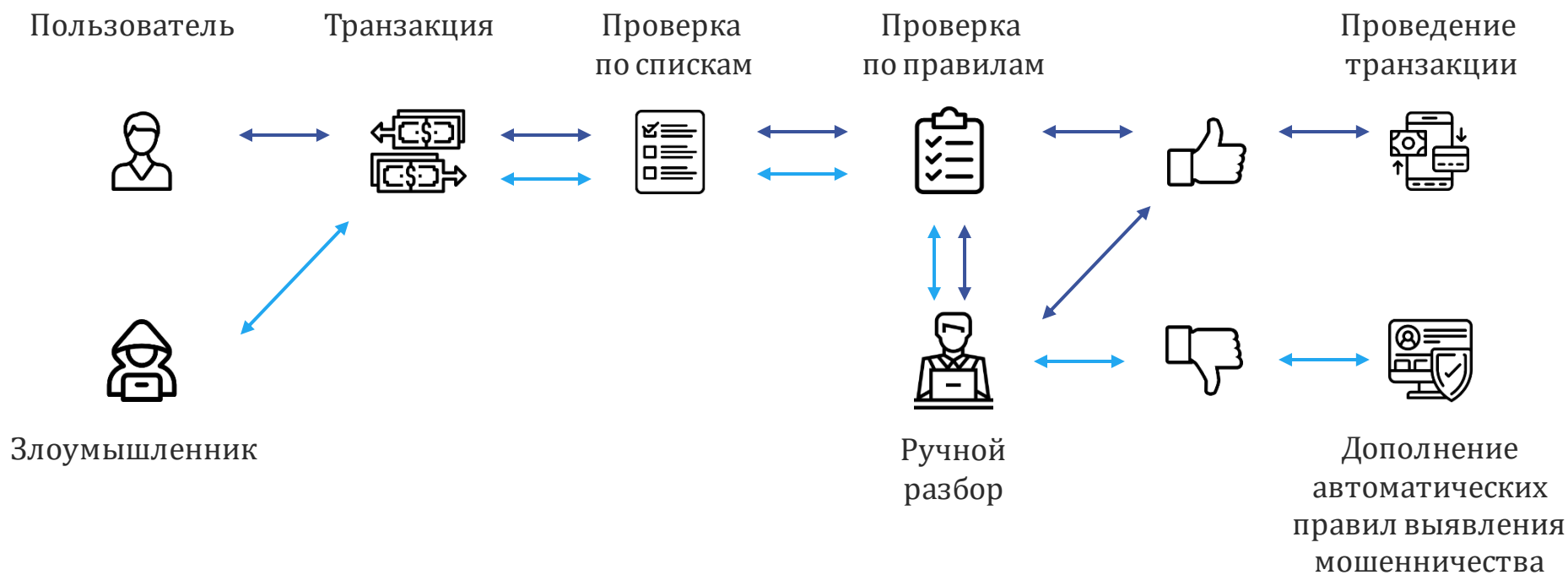


ИНФРАСТРУКТУРА ИСС



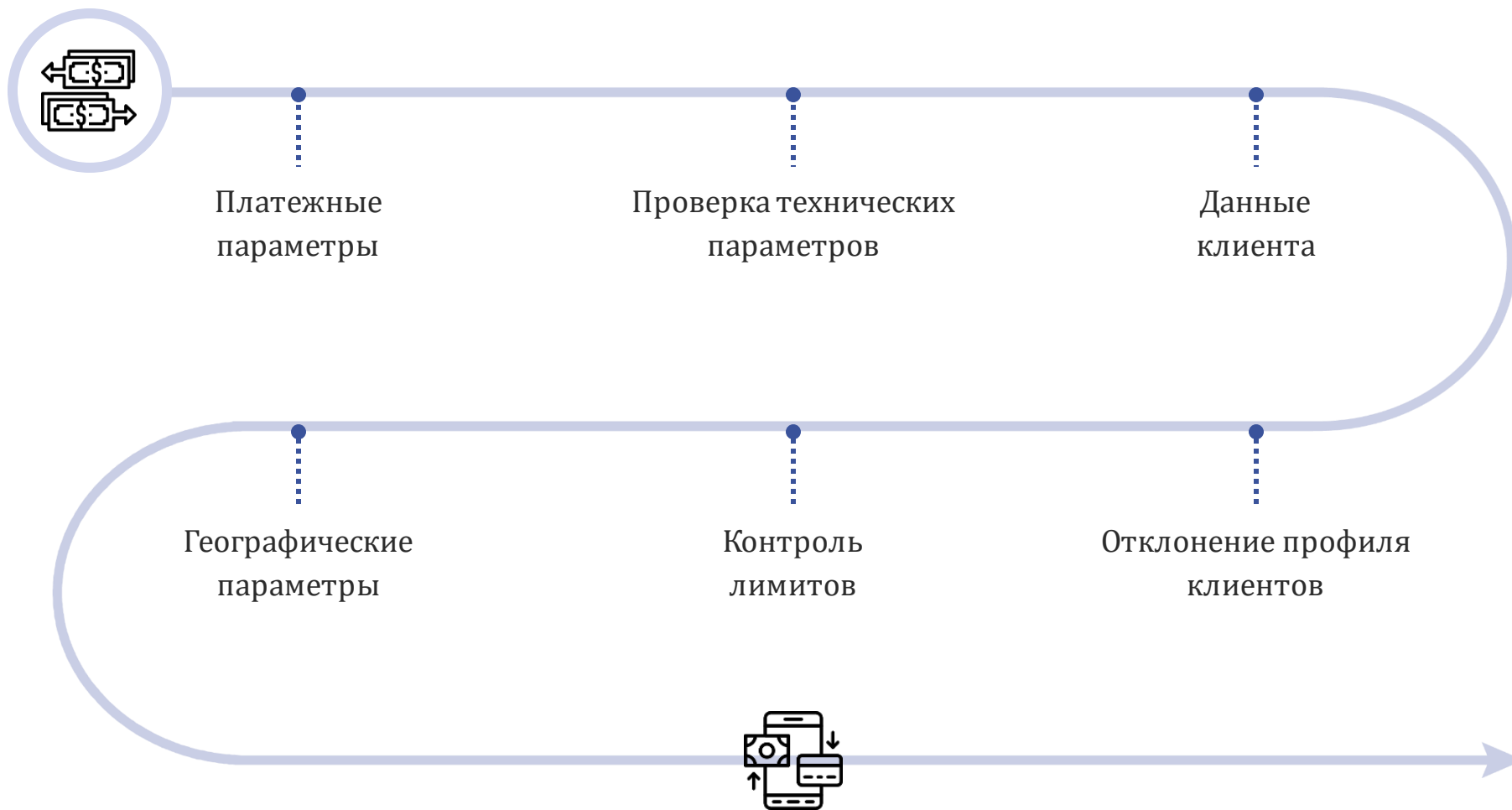
Канал
связи

КАК РАБОТАЕТ FDS



КАК РАБОТАЮТ ПРАВИЛА

Транзакция



РЕЖИМЫ РАБОТЫ FDS

В ЧАСТИ ВЗАИМОДЕЙСТВИЯ С ТРАНЗАКЦИОННЫМИ СИСТЕМАМИ:



Ведущий
FDS самостоятельно
выгружает и загружает
транзакции в системы



Ведомый
загрузка транзакций в
FDS выполняется
системами

В ЧАСТИ ВЛИЯНИЯ НА РАБОТУ ТРАНЗАКЦИОННЫХ СИСТЕМ:



Активный
FDS блокирует обработку
транзакций
в системах до вынесения
решения по транзакции



Пассивный
FDS не блокирует
обработку транзакций в
системах

КЛЮЧЕВЫЕ ПОКАЗАТЕЛИ



Большой набор коннекторов к источникам информации о транзакциях (MS|Postgres|MySQL Server, Oracle, DB2, MQ, REST API)



Возможность предварительного обучения системы на имеющихся данных заказчика

70

предустановленных правил выявления мошенничества

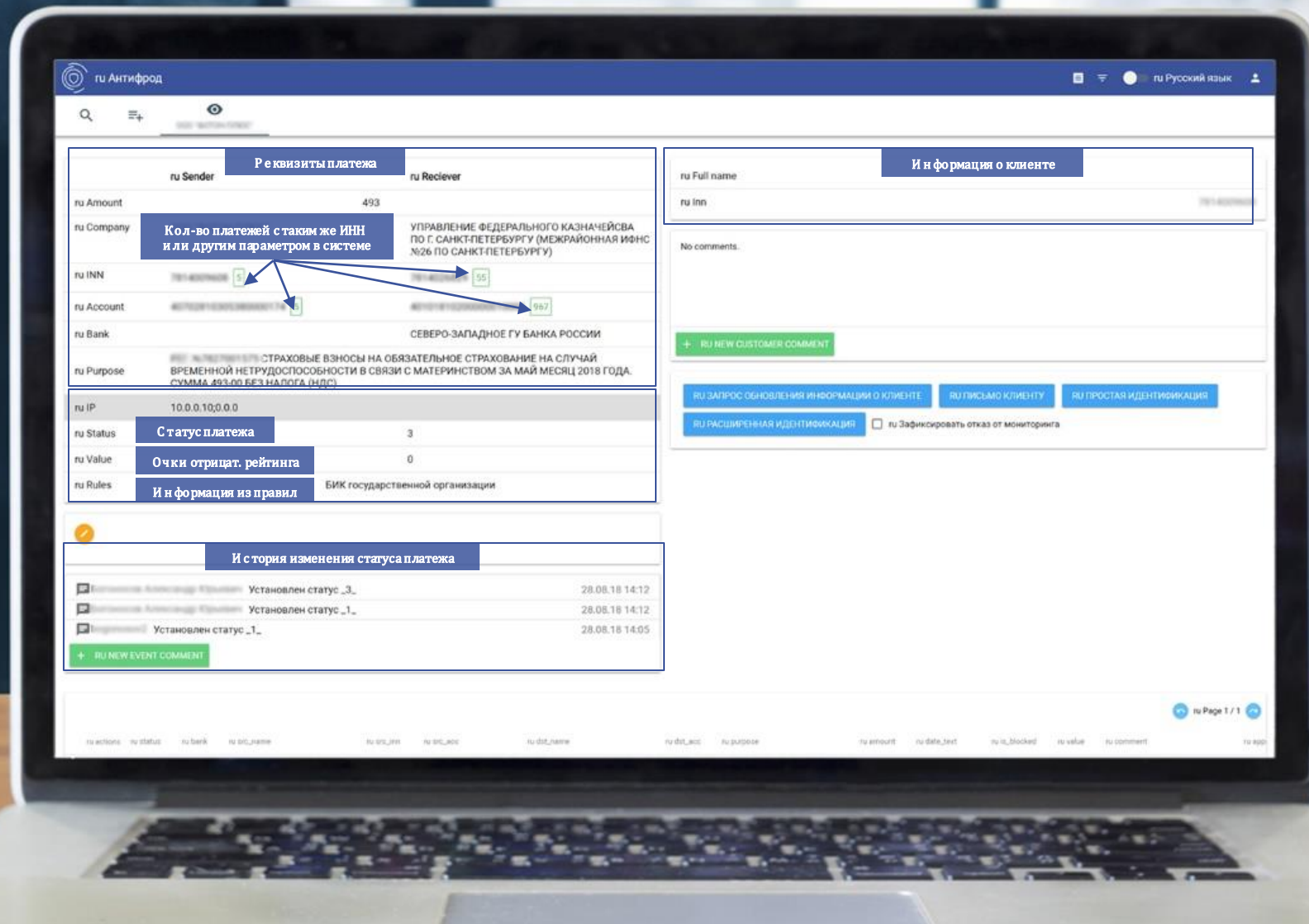
23 000

транзакции обрабатывается в минуту

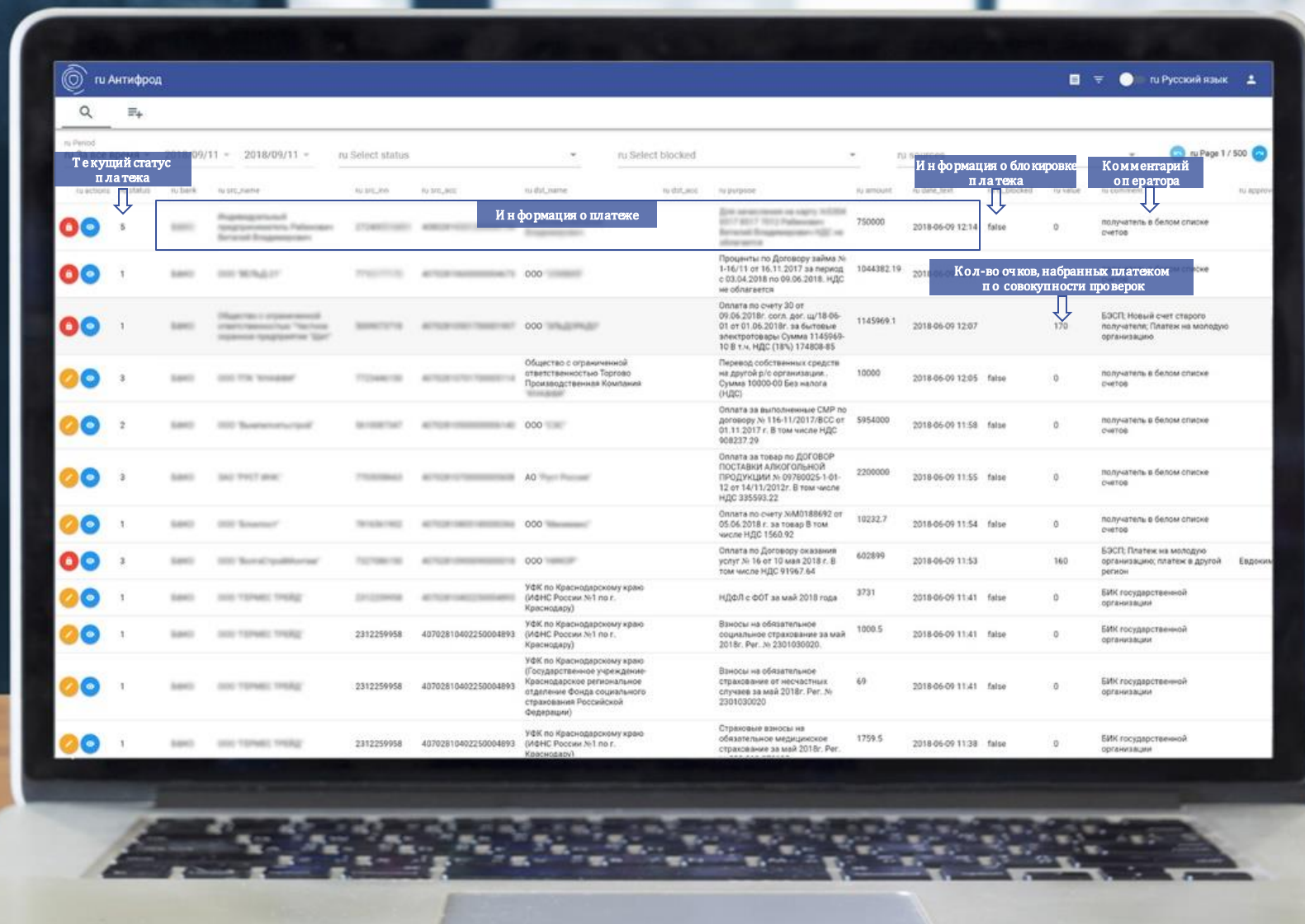
13

только транзакций из 1000 попадает на ручной контроль

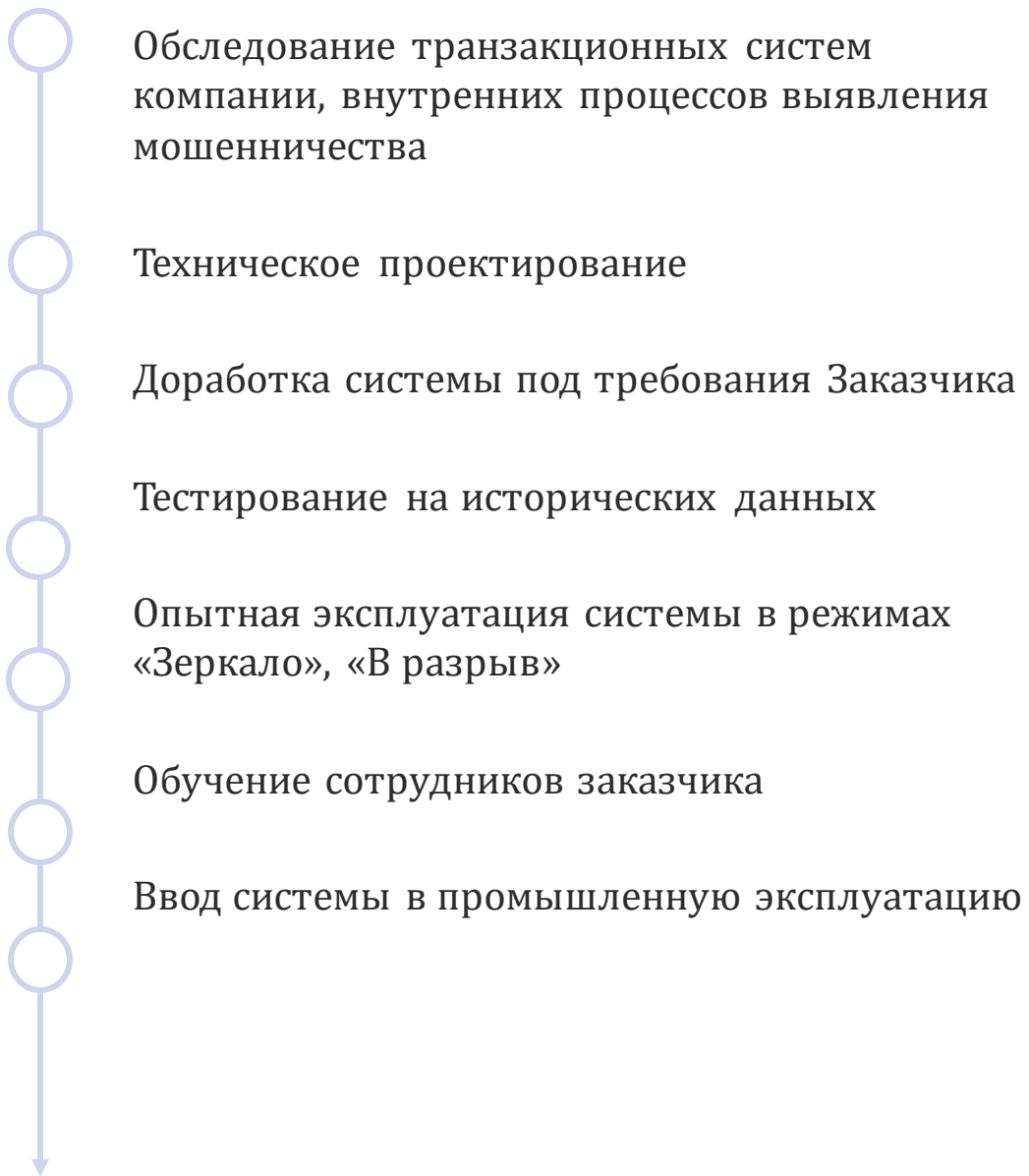
ИНТЕРФЕЙС FDS



ИНТЕРФЕЙС FDS



ЭТАПЫ ВНЕДРЕНИЯ



ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

	Bronze	Silver	Gold
Мониторинг работы ядра системы	24/7	24/7	24/7
Мониторинг коннекторов	—	24/7	24/7
Техническая поддержка (2я линия)	8/5	24/7	24/7
Подписка на обновления базы правил	✓	✓	✓
Типовая отчетность	✓	✓	✓
Доработка правил по требованию заказчика	—	5 правил в месяц	10 правил в месяц
Детализированная отчетность	—	—	✓
Рекомендации по оптимизации работы системы	—	—	✓

ИНТЕГРАЦИЯ С ВНЕШНИМИ СИСТЕМАМИ

methodix

|GROUP|IB|

mfms[•]



ЦФТ ЦЕНТР
ФИНАНСОВЫХ
ТЕХНОЛОГИЙ





gk-is.ru