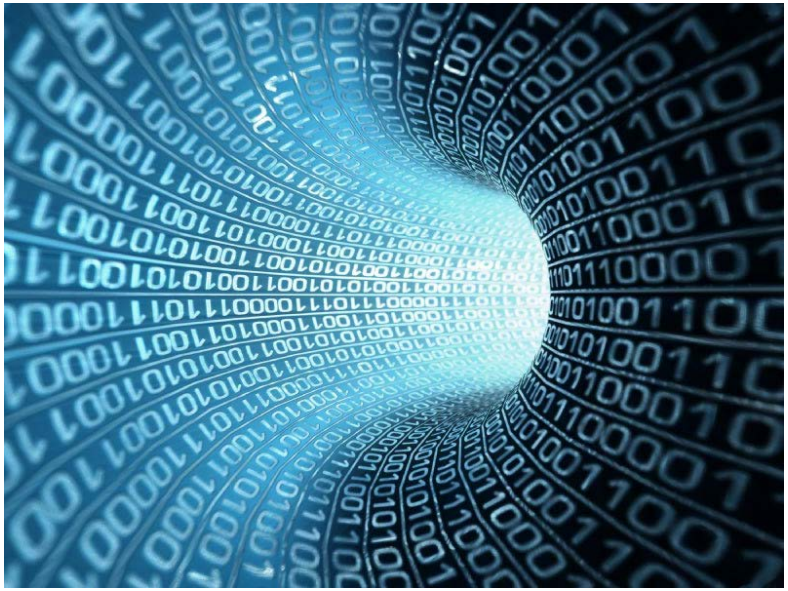
XI Уральский форум
Информационная безопасность финансовой сферы

Практика построения комплексной системы антифрода в банке «Восточный»



СЕРГЕЙ ЕГОРОВ
начальник управления мониторинга
и предотвращения мошенничества
банка «Восточный»

АНДРЕЙ ЛУЦКОВИЧ
ДИРЕКТОР
КОМПАНИИ ФРОДЕКС
e-mail: ceo@frodex.ru

ВОСТОЧНЫЙ БАНК

ФРОДЕКС | эффективные технологии противодействия мошенничеству

Компания ФРОДЕКС, основана в 2011 году

Сотрудники компании являются экспертами в сфере разработки программного обеспечения, сопровождения систем защиты информации, глубокого анализа данных, расследования инцидентов информационной безопасности.

- ✓ **разработка и эксплуатации систем обнаружения мошеннических платежей**
- ✓ **выполнение консультирования, помощь в расследовании и анализе инцидентов**

ВОСТОЧНЫЙ БАНК

ФРОДЕКС | эффективные технологии противодействия мошенничеству

Миссия компании: разработка эффективных технологий противодействия мошенничеству

Базовые принципы работы:

1. Узкая специализация – разработка систем аналитики
2. Создание центра компетенции по проблемам мошенничества
3. Тест драйв разрабатываемых продуктов

Более 40 банков РФ – действующие клиенты компании "Фродекс"

организации разного уровня:

- 5 банков из TOP-50
- 6 банков из TOP-100
- 19 банков из TOP-300

и в другие кредитно-финансовых организации РФ

Свыше 30 банков тестируют наши решения в пилотном режиме

ВОСТОЧНЫЙ БАНК

ФРОДЕКС | эффективные технологии противодействия мошенничеству

НАШИ ПАРТНЕРЫ

информационные системы

GROUP IB

ЦРТ

Simple Lab

KASPERSKY lab

Аладдин РД

Trusteer
an IBM Company

ICL
СИСТЕМНЫЕ ТЕХНОЛОГИИ

КАФЕДРА
ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ
И ЗАЩИТЫ ИНФОРМАЦИИ

ВОСТОЧНЫЙ БАНК

ФРОДЕКС | эффективные технологии противодействия мошенничеству

Комплексный подход

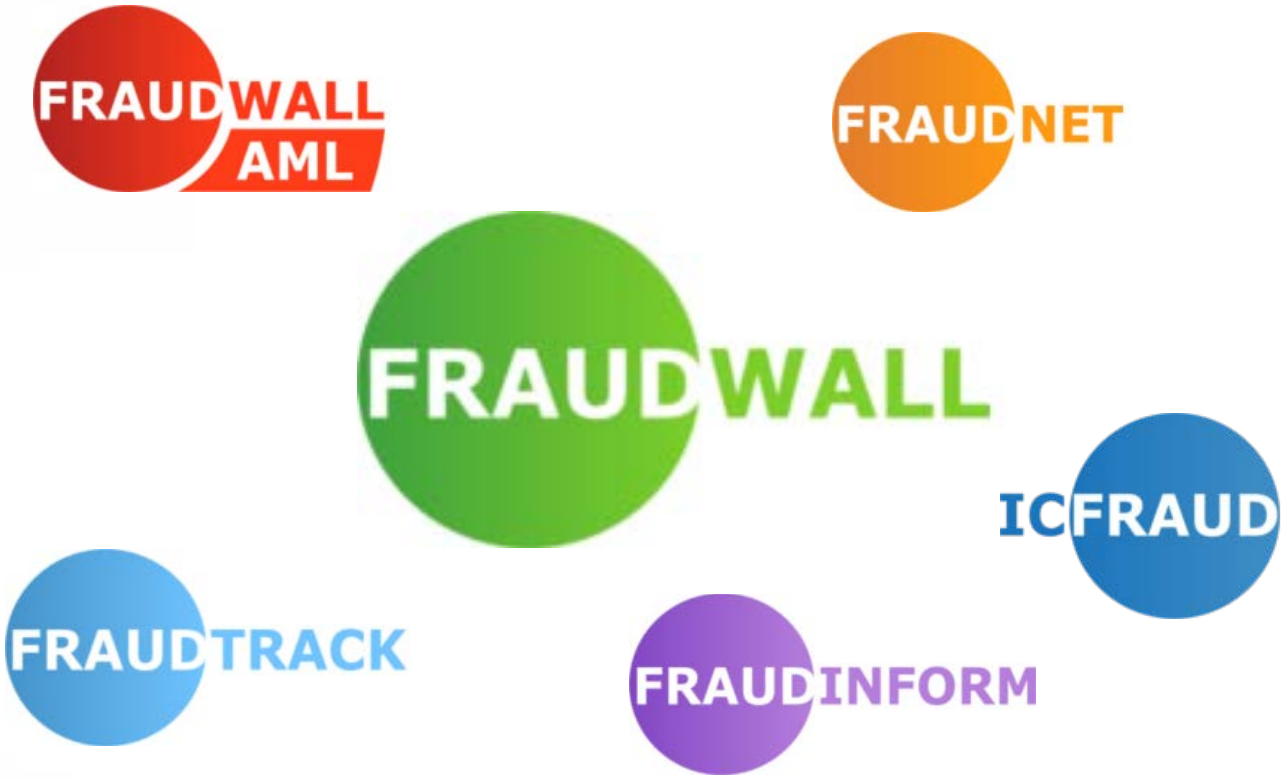
Предотвращение кражи средств в системах ДБО

ПОД/ФТ

Борьба с внутренним мошенничеством (платежи в АБС)

Предотвращение кражи средств через АРМ КБР

РЕШЕНИЯ КОМПАНИИ



ВОСТОЧНЫЙ БАНК

ФРОДЕКС | эффективные технологии противодействия мошенничеству

Проблемы при реализации антифрода

1. Данные (что смотреть?)
2. Логика обнаружения (что искать?)
3. Организация реагирования (что делать?)

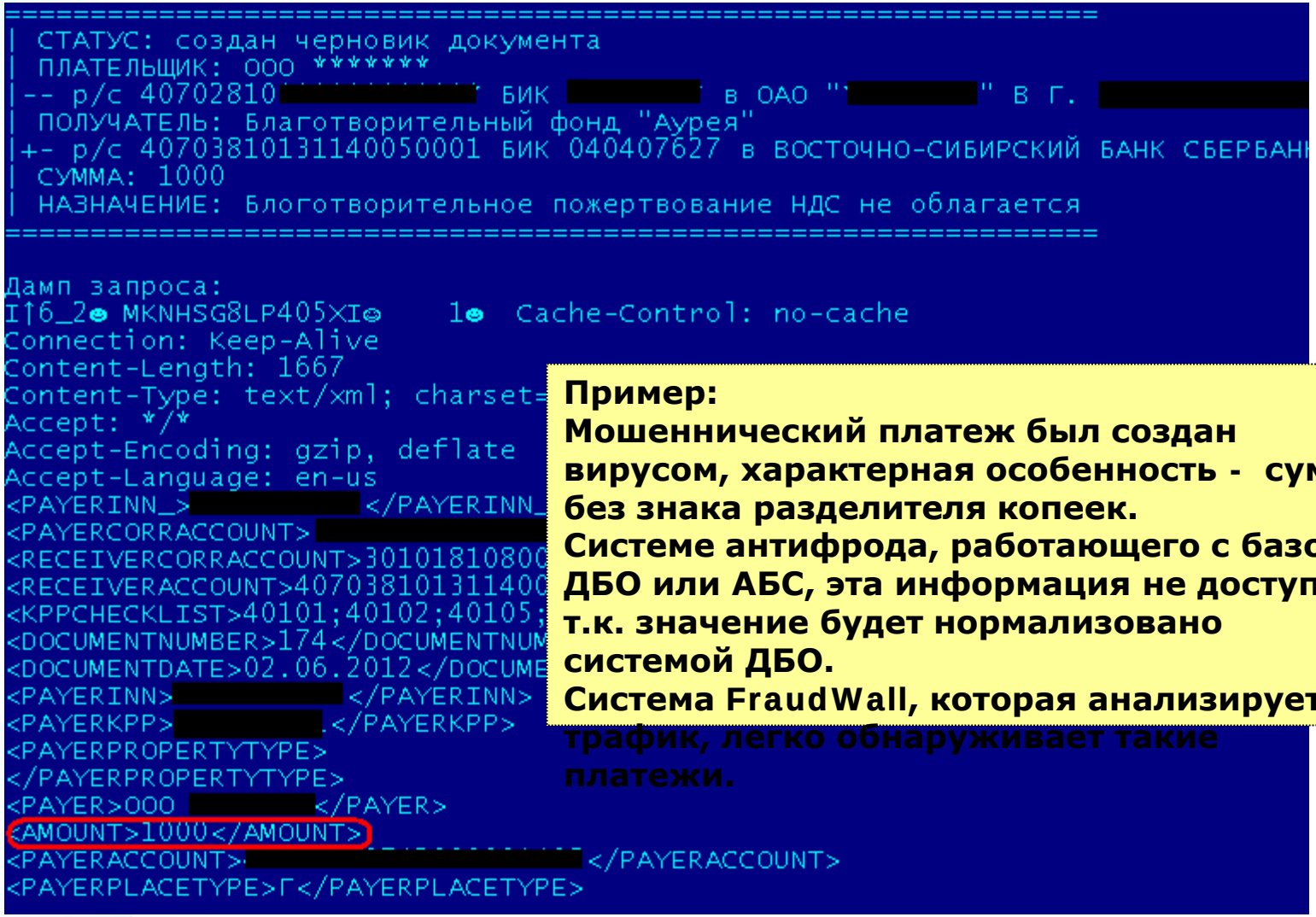
Ключевые принципы системы FRAUDWALL

1. Многоканальность
2. Глобальность анализа
3. Простота интеграции
4. Наличие сервисов обогащения данных
5. Гибкость механизмов организации реагирования
6. Постоянное и непрерывное обновление логики обнаружения

Пару слов о простоте интеграции

ВОСТОЧНЫЙ БАНК

ФРОДЕКС | эффективные технологии противодействия мошенничеству

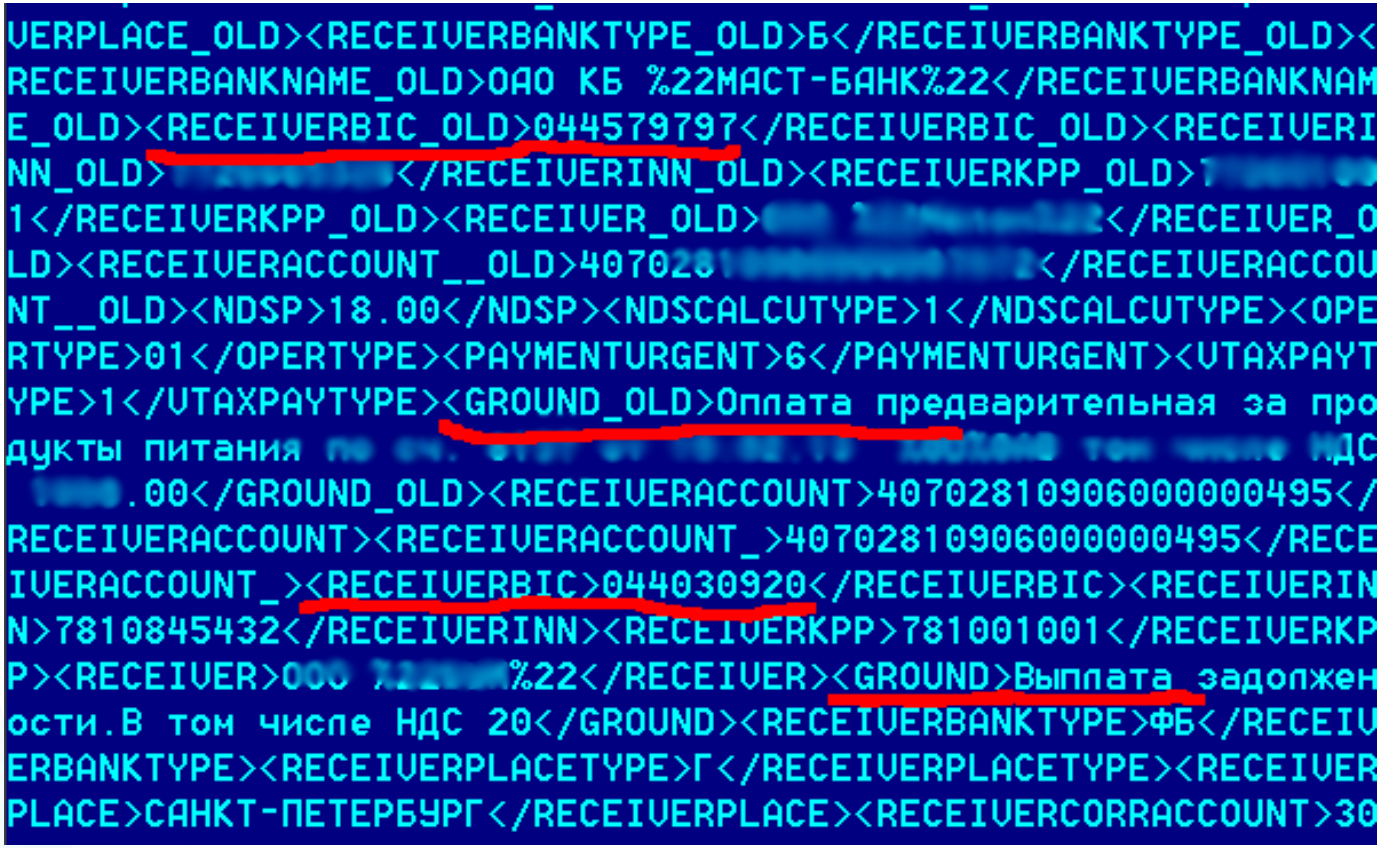


Пример:
Мошеннический платеж был создан вирусом, характерная особенность - сумма без знака разделителя копеек.
Системе антифрода, работающего с базой ДБО или АБС, эта информация не доступна, т.к. значение будет нормализовано системой ДБО.
Система FraudWall, которая анализирует трафик, легко обнаруживает такие платежи.

ВОСТОЧНЫЙ БАНК

ФРОДЕКС | эффективные технологии противодействия мошенничеству

Вирус, подменяющий реквизиты получателя «на лету», любезно оставлял реквизиты реального получателя платежей в тегах, заканчивающихся на _OLD



ВОСТОЧНЫЙ БАНК

ФРОДЕКС | эффективные технологии противодействия мошенничеству

клиент банка

Сервер приложений ДБО

база данных ДБО

периодическое чтение из VIEW реквизитов новых платежек

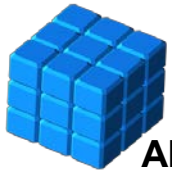
Антифрод – анализатор

подозрительная платежка

Модуль управления

информирование по e-mail

информирование в АБС



АБС

ВОСТОЧНЫЙ БАНК

ФРОДЕКС

эффективные технологии противодействия мошенничеству

Ключевые факторы успеха проекта

1. Быстрота разворачивания
2. Простота интеграции = сроки запуска
3. Организация процесса реагирования (подтверждения подозрительных платежей)
4. Контроль эффективности работы системы
5. Соответствие требованиям законодательства

Задачи для решения в банке Восточный

1. Внутреннее мошенничество (№1 по потенциальным масштабам ущерба), которое может усиливаться за счет уязвимостей ПО и нарушений внутренних регламентов и порядков.
2. Целевые атаки с использованием вредоносного ПО

3. Уязвимости ПО и ошибки в настройках (АБС, карточный процессинг, платежные шлюзы и т.п.)

4. Внешние угрозы:

4.1 Социальная инженерия (СИ, 90% всего внешнего фрода на текущий момент в Банке)

4.2 Фишинг как разновидность СИ

4.3 СИ с использованием социальных сетей и сайта Банки.Ру

4.4 Вредоносное ПО на устройстве клиента

5. Подделка документов, удостоверяющих личность для получения доступа к счетам, картам и личным кабинетам МБ и ИБ

Требования к системе антифрода

1. Широкая функциональность
2. Простой и удобный интерфейс
3. Гибкость настройки правил
4. Обучение системы в процессе работы
5. Широкий спектр black-листов

Результаты

В результате поэтапной интеграции FW в различные каналы получили защиту платежей ДБО ЮЛ, ДБО ФЛ и АБС

Используемые инструменты для предотвращения мошенничества.

ВОСТОЧНЫЙ БАНК

ВОСТОЧНЫЙ ЭКСПРЕСС БАНК

Что сейчас может FraudWall?

- проверка платежей одновременно в разных системах (АБС, ДБО юр.лиц, ДБО физ.лиц)
- в комплекте уже идут проверки, полностью соответствующие требованиям ЦБ РФ
- автоматизированная обработка фидов с черными списками получателей от ЦБ
- автоматизированная подготовка отчета в ФинЦЕРТ об инцидентах (в т.ч. с изменениями в формате JSON-файла от 8.02.2019 г.)

ПОД/ФТ.

КЛЮЧЕВЫЕ ИЗМЕНЕНИЯ, О КОТОРЫХ МАЛО ГОВОРЯТ

ВОСТОЧНЫЙ БАНК

ФРОДЕКС | эффективные технологии противодействия мошенничеству

БЫЛО:

- подразделения фин.мониторинга банка делали проверку клиентов после того, как платеж был исполнен в АБС (offline-проверка)

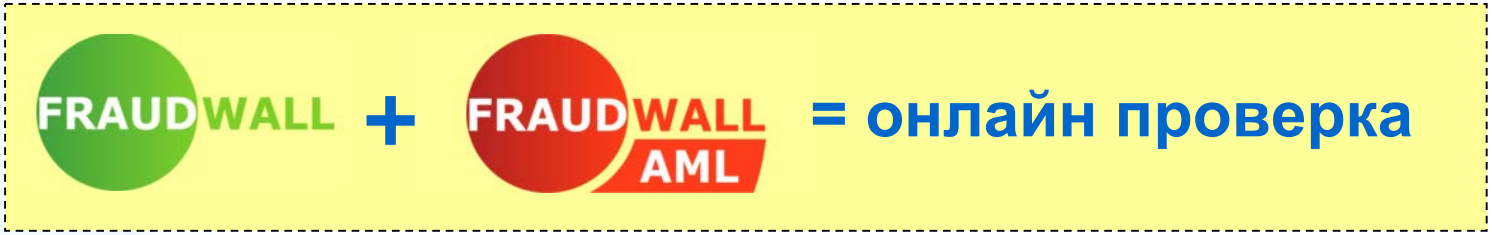
СТАЛО:

- в начале октября 2018 г. ЦБ разослал банкам письмо, в котором обязал банки проводить высокорисковые операции клиентов только после анализа сотрудником фин.мониторинга
- если платеж вызвал подозрение – он останавливается на срок до 1 рабочего дня

FraudWall + FraudWall AML

- **Нововведение ЦБ РФ заставило нас по-другому посмотреть на архитектуру системы проверки ПОД/ФТ FraudWall AML – если это раньше был отдельный продукт, то сейчас он должен быть тесно интегрирован с антифрод-системой FraudWall**

- **реализовано в версии 5.5.1**



СПАСИБО ЗА ВНИМАНИЕ!

СЕРГЕЙ ЕГОРОВ
начальник управления мониторинга
и предотвращения мошенничества
банка «Восточный»

АНДРЕЙ ЛУЦКОВИЧ
ДИРЕКТОР
КОМПАНИИ ФРОДЕКС
e-mail: ceo@frodex.ru

ВОСТОЧНЫЙ БАНК

ФРОДЕКС | эффективные технологии противодействия мошенничеству