Развитие современных платежных инструментов и банковских приложений как элемент устойчивого и эффективного функционирования НПС России

Fraud-мониторинг в ДБО – проактивная защита от хищений

Принципы работы, практика применения, перспективы развития

Компания «БИФИТ»

МОСКВА, 2013

Способы защиты от хищений ДБО

1. Построение защиты на стороне клиента:
   - аппаратные решения;
   - антивирусные решения.
2. Построение защиты на стороне банка (Fraud-мониторинг)

Ключевая проблема современных аппаратных решений – необходимость подтверждения практически каждого платежа

Результат – уязвимость к социальной инженерии

Fraud-мониторинг для ДБО

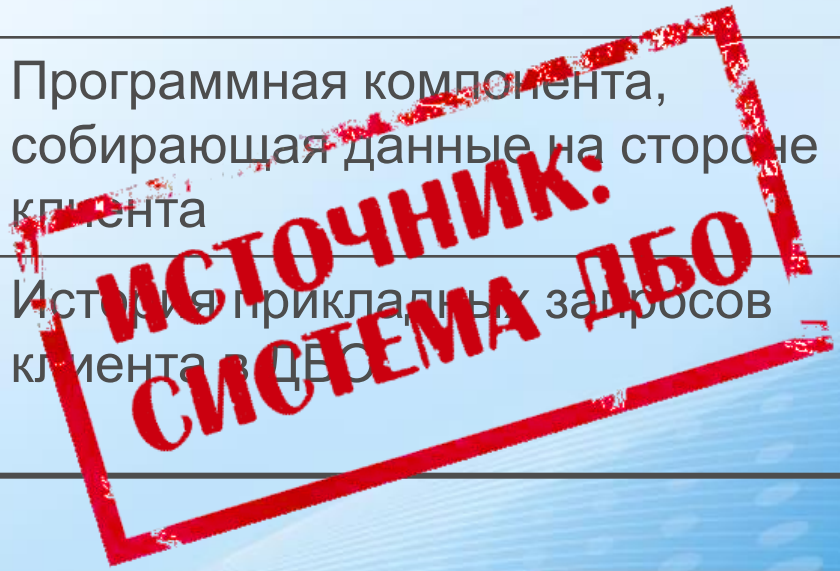
Критерии эффективности Антифрод решений

1. Высокая доля выявленных мошеннических операций
2. Низкая доля ложных срабатываний
3. Управление показателями работы

Fraud-мониторинг для ДБО

Способы выявления мошеннических платежей:

Анализируемые данные	Источник данных
Реквизиты платежа	Непосредственно платеж История платежей клиента
Признаки рабочей среды (оборудование, системное и прикладное ПО)	Программная компонента, собирающая данные на стороне клиента
Модель поведения клиента	История прикладных запросов клиента в ДБО



BIFIT

Fraud-мониторинг для ДБО

Вывод:

Только плотная интеграция Fraud-мониторинга с системой ДБО способна обеспечить высокие показатели как по числу выявленных мошенничеств, так и по доле ложных срабатываний

Fraud-мониторинг для ДБО: наш опыт

Проект: интеграция с системой RSA Transaction Monitoring в банке Топ-10 в 2013 году

О системе RSA Transaction Monitoring:

- более 8 000 внедрений в мире

- в основе – самообучающийся Risk Engine

- в 2012 году адаптирована под реалии РФ

Fraud-мониторинг для ДБО: наш опыт

Проект: интеграция с системой RSA Transaction Monitoring в банке Топ-10 в 2013 году

Ход проекта:

1. **Написание и согласование постановки задачи – 3 мес.**
2. **Интеграция RSA TM с ДБО iBank 2. Встраивание механизмов RSA для анализа среды клиента – 3 мес.**
3. **Обучение RSA TM на реальных данных – 3 мес.**

Fraud-мониторинг для ДБО: наш опыт

Компания «БИФИТ» с 2008 года содействует банкам в борьбе с хищениями

На базе накопленной компетенции в конце 2011 г. было принято решение разработать собственную систему Fraud-мониторинга

Система Fraud-мониторинга для ДБО

Состав решения от компании «БИФИТ»

- Детектор Угроз
- Мониторинг транзакций
- Анализатор активности

Fraud-мониторинг. Детектор Угроз

Объект анализа: **клиентское устройство** (компьютер)

Цель анализа: **выявление зловредного ПО**

Результат анализа: **«отчет», передаваемый на банковский сервер**

Архитектура: **встроен в клиентское приложение**

Выявляет угрозы до попытки хищения

NB!!! Может использоваться как отдельный модуль (например, со сторонними антифрод-системами)

BIFIT

Fraud-мониторинг. Мониторинг транзакций

Объект анализа: платежи

Цель анализа: выявление мошеннических операций

Результат анализа:
- уведомление
- перевод документа в спец. статус
- запрос подтверждения платежа
- материалы для расследования

Обучаемость

Настраиваемость

Анализирует более 50 параметров

Fraud-мониторинг. Мониторинг транзакций

Дополнительно

Анализирует более 50 параметров

Предопределенные индикаторы:

- Получатели незаконных платежей и их счета
- Устройства и IP-адреса, ранее использованные злоумышленниками
- Страны и регионы, связанные с повышенным риском
- Сумма платежа
- Тип получателя
- Недавнее изменение профиля и т. д.

Профиль пользователя:

- Суммы платежей
- Количество платежей
- Получатели
- Параметры устройства
- Параметры подключения
- Временной режим и т.д.

BIFIT

Fraud-мониторинг. Анализатор активности

Анализируемые события – прикладные запросы клиентского приложения к банковскому Серверу

Модели анализа:

1. **Выявление «невозможных» событий**
2. **Выявление маловероятных, нехарактерных для типичного пользователя событий**

Fraud-мониторинг. Анализатор активности

Анализируются

1. Параметры запросов
2. Последовательность запросов
3. Шаблоны последовательностей
4. Нетипичные действия,
   количество таких действий в сессии

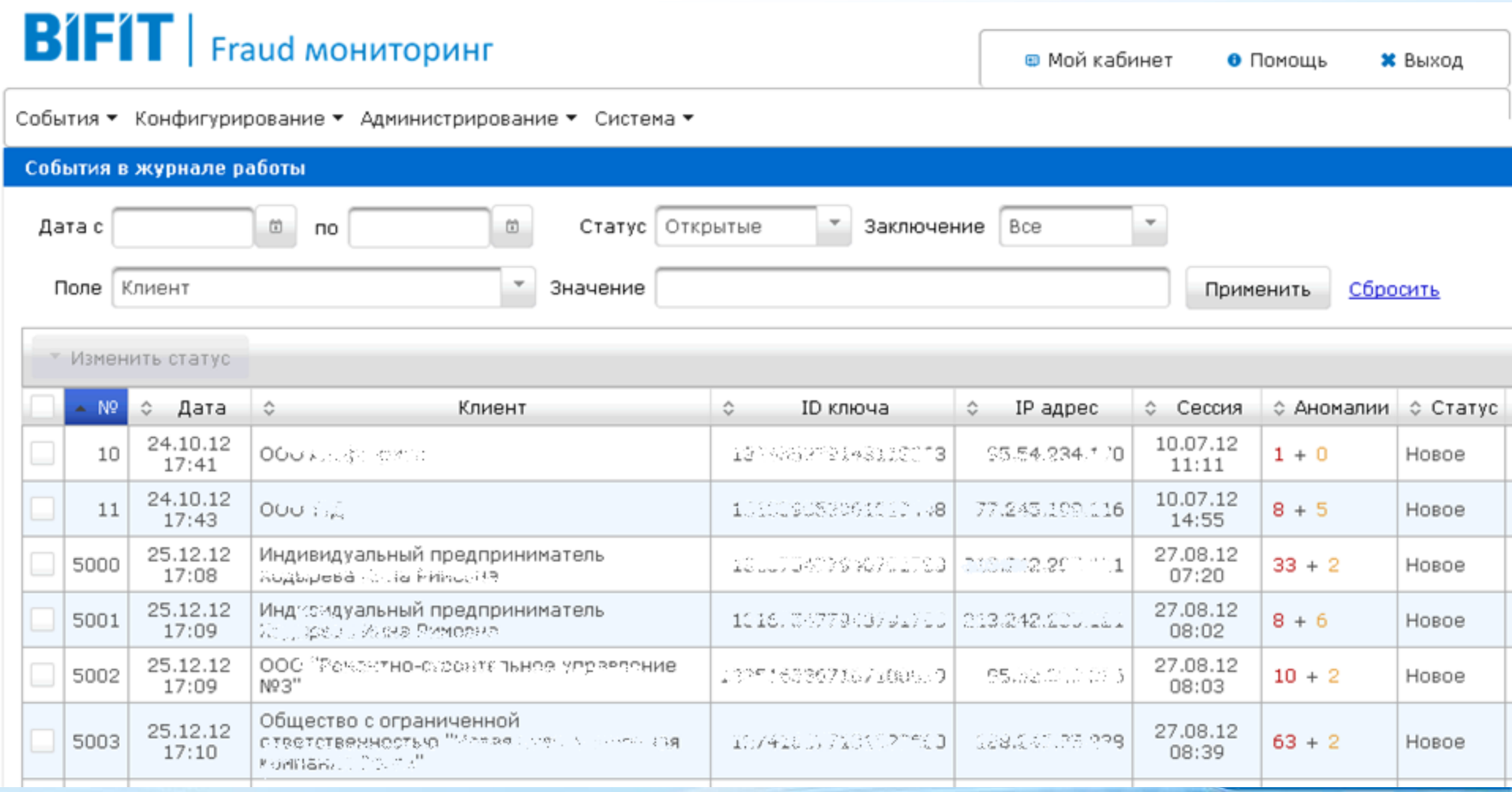
Fraud-мониторинг. Анализатор активности

Результаты работы – уведомления:

1. **О вирусной активности на компьютере клиента**
2. **О фродовой операции**
3. **О подозрительной, аномальной активности в действиях пользователя**

Fraud-мониторинг. Анализатор активности

Результаты работы – уведомления



BIFIT | Fraud-мониторинг

Мой кабинет | Помощь | Выход

События | Конфигурирование | Система

Информация о событии в журнале работы

Изменить статус | Предыдущий | К списку | Следующий

Номер события: 1
Дата события: 27.12.2011 7:10

Наименование клиента: ООО "[illegible]"
ID ключа: [illegible]
IP адрес: [illegible]

Сотрудник:
Статус:
Заключение:

Сводка | Детали сессии | История

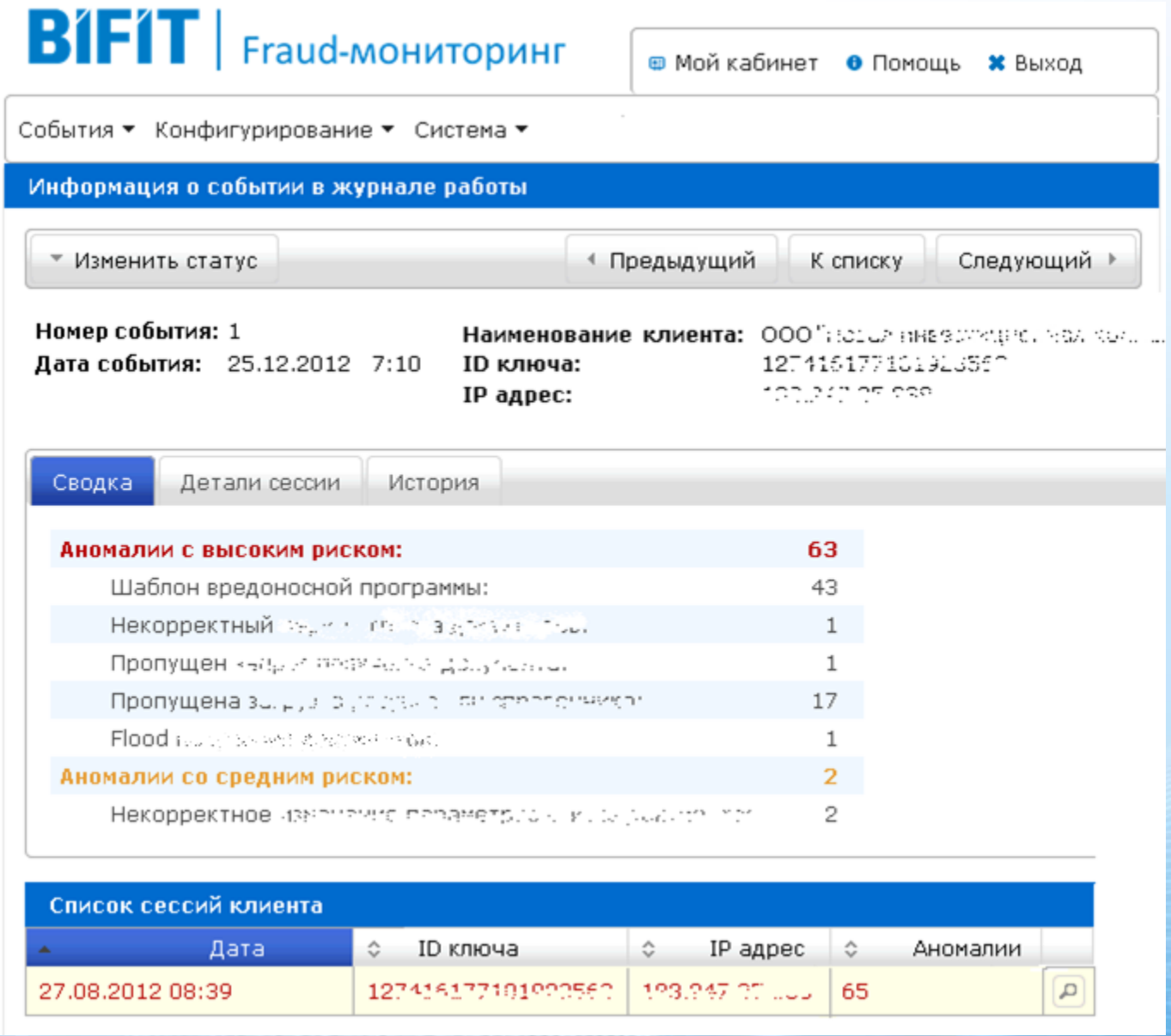
11 - 20 / 129 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9

	Начало	Завершение	IP-адрес	Тип запроса	Детали запроса
	27.08.2012 08:39:49,600	27.08.2012 08:39:49,600	188.247.[illegible]	[illegible]	[illegible]
	27.08.2012 08:39:50,053	27.08.2012 08:39:50,115	188.247.[illegible]	[illegible]	[illegible] filterItem, идентификаторы_документов=null
	Пропущена [illegible]				
	27.08.2012 08:39:50,490	27.08.2012 08:39:54,584	188.247.[illegible]	[illegible]	тип_документов=doc/payment, статусы_документов=[illegible] идентификаторы_документов=null
	27.08.2012 08:39:57,584	27.08.2012 08:39:57,600	188.247.[illegible]	[illegible]	
	27.08.2012 08:39:57,959	27.08.2012 08:39:58,037	188.247.33.238	[illegible]	тип_документов=doc/[illegible]

Список сессий клиента

Дата	ID ключа	IP адрес
27.08.2012 08:39	[illegible]	188.247.33.239

Анализатор активности. Результаты работы. Сводка



Fraud-мониторинг. Анализатор активности

Актуальная статистика

75% мошеннических транзакций «оформляются» вредоносным ПО на компьютере клиента

Статистика результатов испытаний Анализатора активности

1. **Выявление вирусной активности – 100% случаев**
2. **Выявление аномальной активности – 50% случаев**

Fraud-мониторинг. Анализатор активности

Важно

Не требует обучения

Работает в режиме онлайн

Позволяет заблаговременно выявить «проблемного» клиента и принять меры до возникновения «проблемных» платежей

Система Fraud-мониторинга для ДБО

Ключевые преимущества нашего решения для системы электронного банкинга «iBank 2»

1. Плотная интеграция с iBank 2 (Детектор Угроз, Анализатор активности) – снижает количество ложных срабатываний при сохранении доли обнаруженных фродовых операций
2. Быстрота внедрения за счет наличия интеграции с iBank 2, предустановленным правилам и возможности обучения на исторических данных. Срок внедрения – менее 1 месяца
3. Доступная цена – лицензируется по количеству клиентов с ежеквартальной оплатой срочной лицензии. Нет высокой «цены входа», для банков Топ-100 ТСО в 2-4 раза ниже, чем у зарубежных решений
4. Постоянное развитие

BIFIT

Развитие современных платежных инструментов и банковских приложений как элемент устойчивого и эффективного функционирования НПС России

Fraud-мониторинг в ДБО – проактивная защита от хищений

Принципы работы, практика применения, перспективы развития

Шилов Станислав
shilov@bifit.com

BIFIT