Где проходит граница доверенной среды? Стратегия эшелонированной обороны ДБО

Доверенная среда. История вопроса

2007 г.

Первая волна технологичных хищений в ДБО

Суть

- **Заражение компьютера**
- **Хищение ключа подписи (из файла, реестра, памяти)**
- **Использование ключа от имени клиента**

Доверенная среда. Стадия 1

Доверенная среда – там, где нет злонамеренного ПО.

Способ: защита компьютера клиента

- **Антивирус**
- **Сетевые экраны**
- **Контроль среды исполнения**
- **Регламенты работы, «электронная гигиена»**

Минусы и ограниченность очевидна

Доверенная среда. Стадия 2

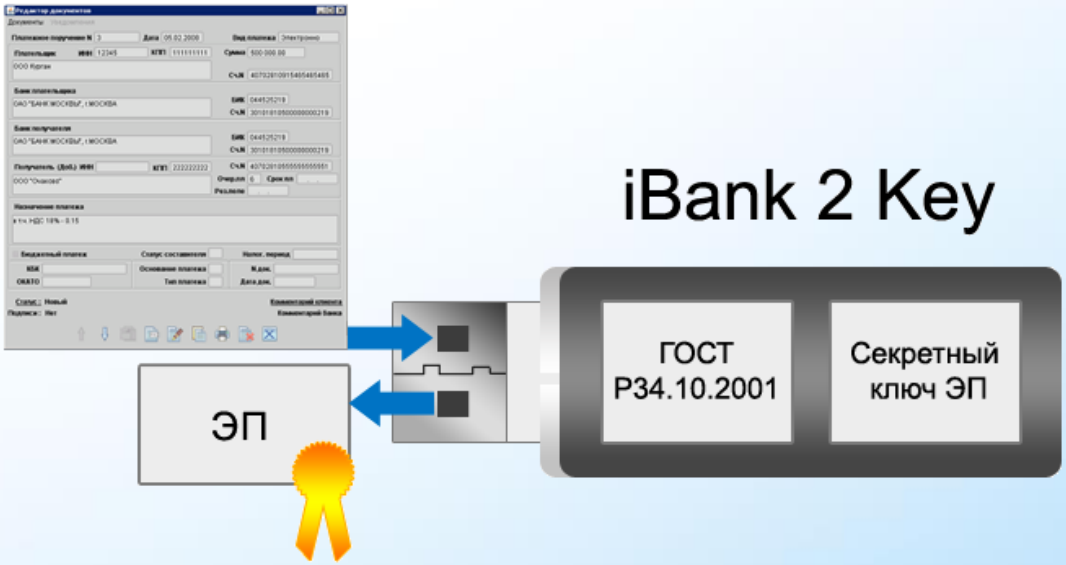
Доверенная среда – там, где нет и не может быть злонамеренного ПО.

Трудно, дорого, без гарантий, если стремиться реализовать на компьютере клиента.

Выход: доверенная среда для самой ответственной процедуры – подписи документа.

Доверенная среда. Стадия 2

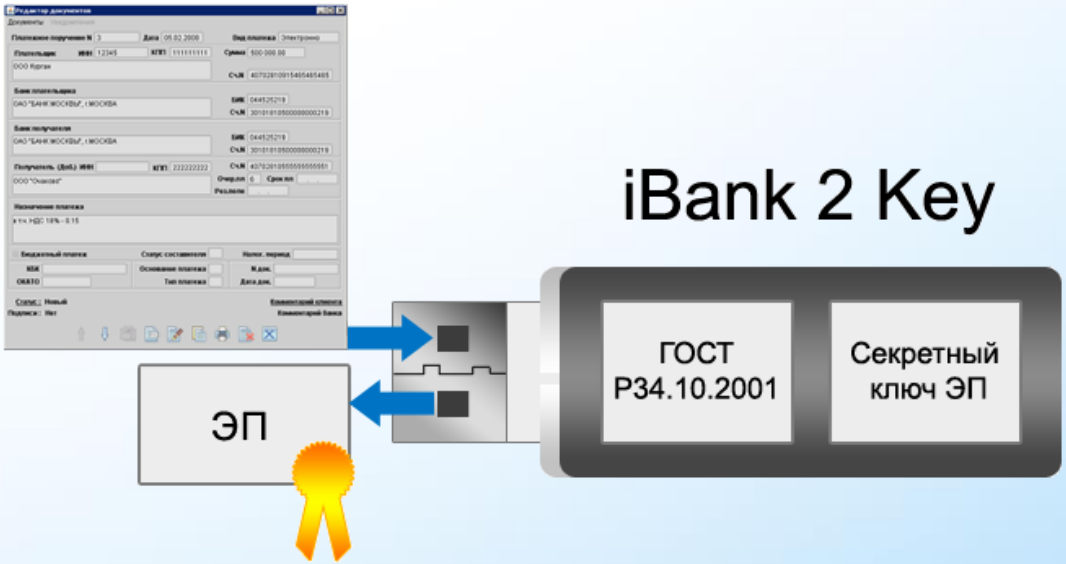
Доверенная среда – там, где нет и не может быть злонамеренного ПО.



2008 г. Токены и смарткарты с неизвлекаемым хранением ключей подписи

Доверенная среда. Стадия 2

Доверенная среда – там, где нет и не может быть злонамеренного ПО.



Результат: процесс подписи защищен, атаковать сложнее

Следствие: мнение о приоритетности атак на извлекаемые ключи...

Не оправдалось (выводы IV кв. 2009).

Доверенная среда. Стадия 3

2010 г. Исходные данные:

Комплексная защита компьютера по-прежнему сложна.

Атаки на использование неизвлекамых ключей стали реальностью.

Оперативное решение: дополнительный эшелон обороны – одноразовые пароли (OTP)

Доверенная среда. Стадия 3

2010 г. Дополнительные одноразовые пароли (OTP)

Источники OTP

OTP применяются для аутентификации пользователей и дополнительного подтверждения документов.

Доверенная среда. Стадия 3

2010 г. Дополнительные одноразовые пароли (OTP)

Плюсы

- **Быстро, просто, понятно**
- **Недорого (доступнее смарткарт) или «совсем недорого» (SMS)**

Минусы

- **Дополнительные операции**
- **Очевидна направленность новых векторов атак**

BIFIT

Доверенная среда. Стадия 4

2011 г. MAC-токены

БИК
Счет
Сумма

➔ *Код подтверждения*

Плюсы

- Код подтверждения зависит от ключевых реквизитов
- Нет ожидания SMS, нет передачи информации через сторонние каналы

Минусы

- Много дополнительных операций для пользователя

BIFIT

Доверенная среда. Стадия 4а

2012 г. MAC-токены + «Доверенные получатели»

БИК
Счет
Сумма

➔ *Код подтверждения*

Реквизиты постоянного контрагента заверяются только один раз и запоминаются системой.

Результат:

- **Устройство то же, но работать проще**
- **Нет рутины – выше бдительность пользователей**

Доверенная среда. Стадия 5

Устройства с визуализацией подписываемого документа, ключевых реквизитов платежа

BIFIT

Доверенная среда. Стадия 5

Устройства с визуализацией

Плюсы

- Видим, что подписываем в доверенной среде

Минусы

- Дополнительные операции пользователя
- Стоимость владения
- Нужна доработка «схемы подписи» ДБО

BIFIT

Доверенная среда

Стадия 6 или эпоха «Б»?

Fraud-мониторинг для ДБО – эффективный эшелон обороны на стороне Банка

Fraud-мониторинг для ДБО

Состав решения для iBank 2

- Детектор угроз
- Анализатор активности
- Мониторинг транзакций

Fraud-мониторинг. Детектор угроз

Объект анализа:	**среда исполнения клиентского приложения** (компьютер клиента)
Цель анализа:	**выявление зловредного ПО**
Результат анализа:	**«сигнал» передаваемый на банковский сервер**
Архитектура:	**встроен в клиентское приложение**
Особенность:	**Выявляет потенциальные угрозы до попытки хищения**

Fraud-мониторинг. Анализатор активности

Объект анализа:	**прикладные запросы клиентского приложения**
Цель анализа:	**выявление аномалий, связанных с деятельностью мошенников**
Результат анализа:	**отчеты для службы информационной безопасности, учет аномалий при скоринговой оценке транзакции**

BIFIT

Fraud-мониторинг. Мониторинг транзакций

Объект анализа:	**платежи (транзакции), операции типа «вход в систему»**
Цель анализа:	**выявление подозрительных транзакций**
Результат анализа:	**- уведомление - перевод документа в спец. статус - запрос подтверждения платежа - материалы для расследования**

Fraud-мониторинг

Детектор угроз

BIFIT

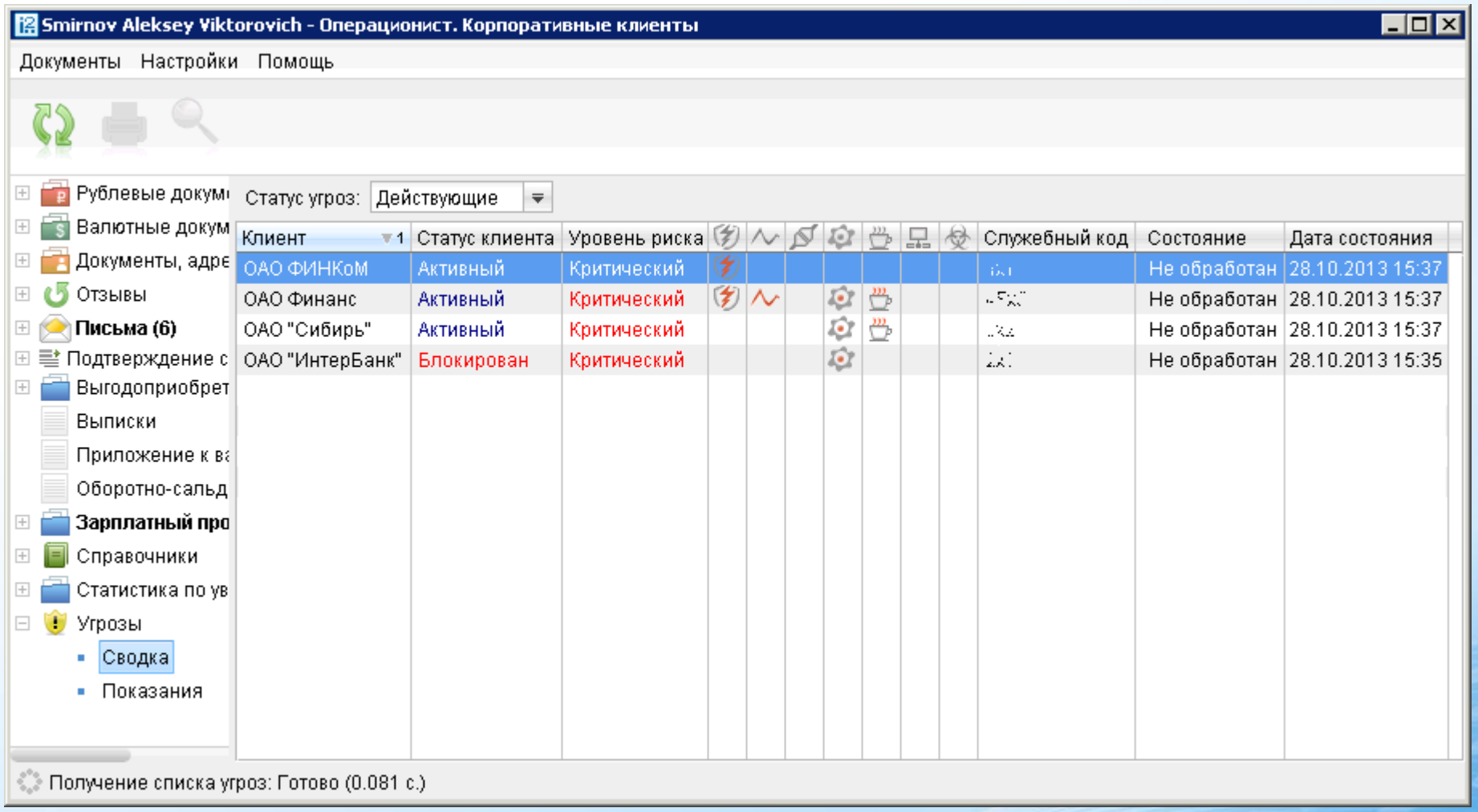
Fraud-мониторинг. Детектор угроз

Встроен в стандартные клиентские модули

Выявляет признаки присутствия злонамеренного ПО в среде исполнения клиентского приложения

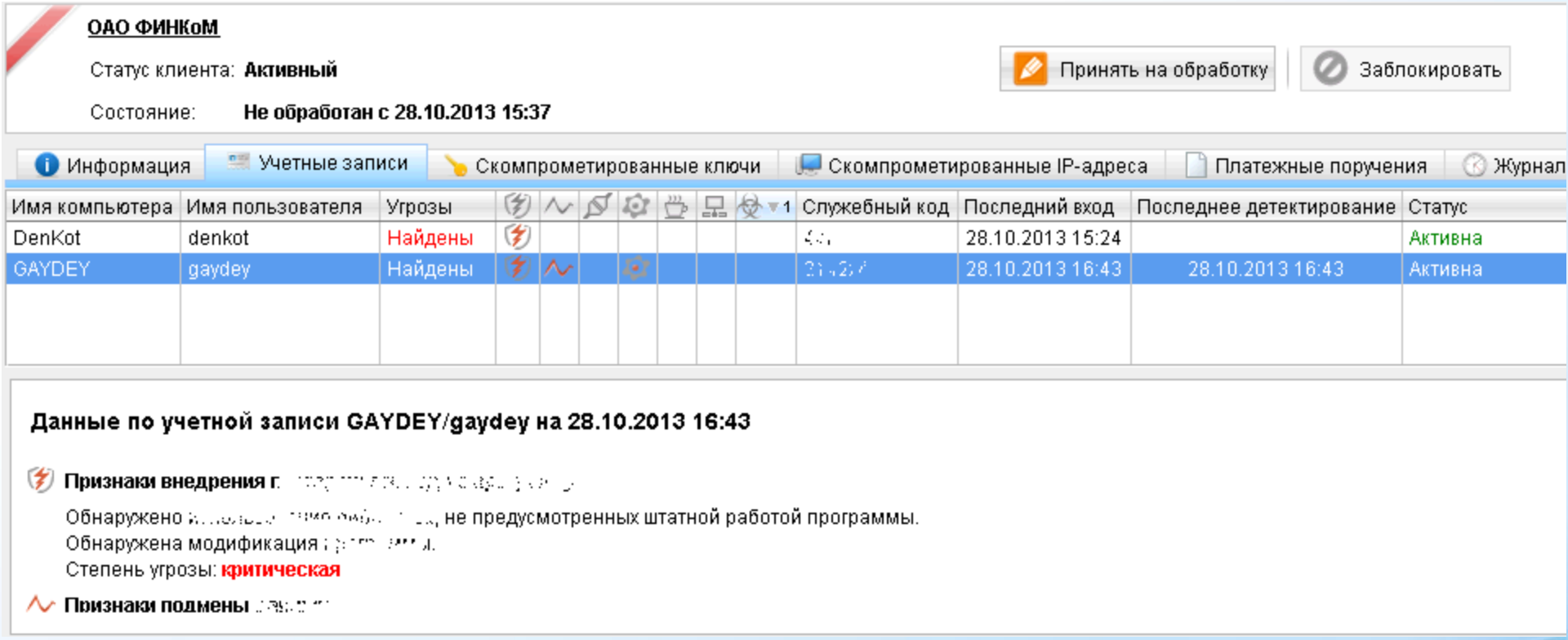
Не «борется» с вирусами, а сигнализирует о проблеме на банковский сервер

Fraud-мониторинг. Детектор угроз



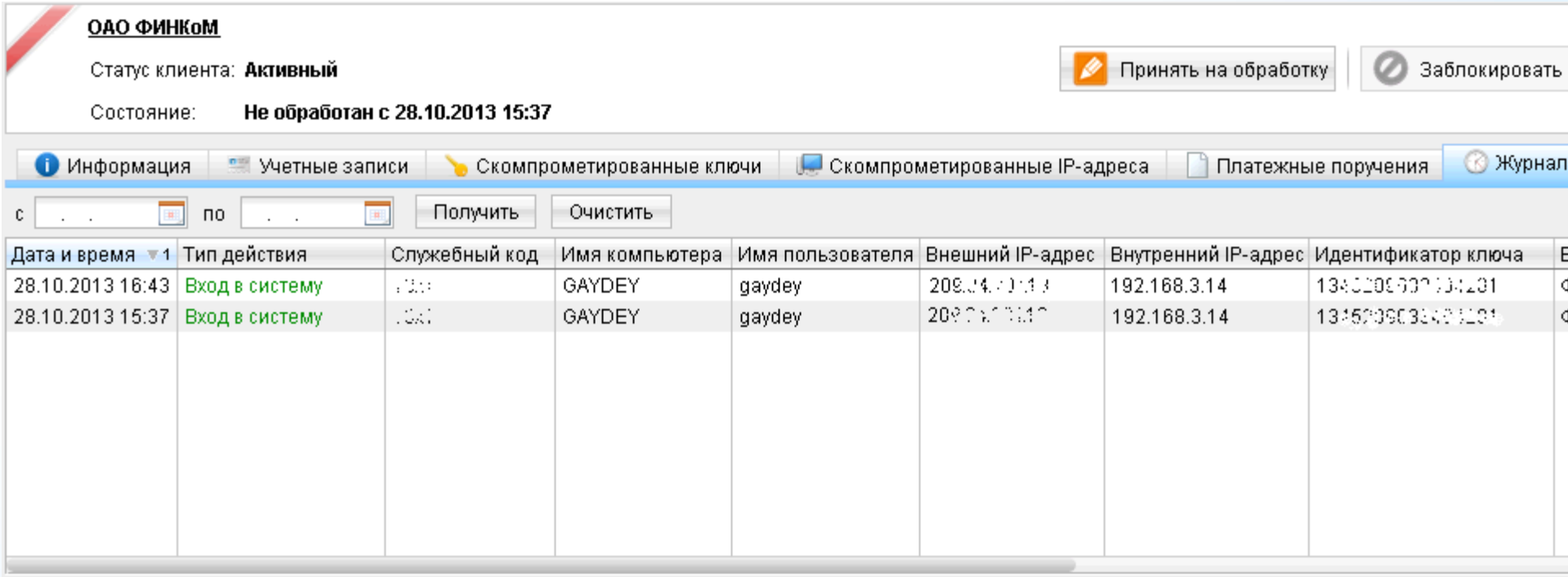
«Сигналы» группируются в «сводки» по клиентам

Fraud-мониторинг. Детектор угроз



Показания по отдельному клиенту.
Информация группируется по учетным записям, ключам ЭП, IP-адресам рабочих мест и т. д.

Fraud-мониторинг. Детектор угроз



Показания. Детальный журнал

Детектор угроз может использоваться как самостоятельное решение и в составе системы Fraud-мониторинга

BIFIT

Fraud-мониторинг

Анализатор активности

Fraud-мониторинг. Анализатор активности

Анализирует прикладные запросы, поступающие клиентского приложения к банковскому Серверу

Модели анализа

1. **Техническая: выявление невозможных действий**
2. **Поведенческая: выявление маловероятных, нехарактерных для пользователя действий**

Fraud-мониторинг. Анализатор активности

Результаты работы

BIFIT | Fraud-мониторинг

Мой кабинет | Помощь | Выход

События | Исследование | Конфигурирование | Справочники | Администрирование | Система

События в журнале работы

Дата с | по | Статус: Открытые | Заключение: Все

Поле: Клиент | Значение: Customer | Применить | Сбросить

Изменить статус

№	Дата	Клиент	Аномалии	ID ключа	IP адрес	Положение	Сессия
10	13.02.13 20:09	Customer224	28 + 2		1	RU, Unknown, Unknown	27.08.12 07:20
11	13.02.13 20:09	Customer224	8 + 6			RU, Unknown, Unknown	27.08.12 08:02
12	13.02.13 20:09	Customer348	10 + 2			RU, Komi, Syktyvkar	27.08.12 08:03
13	13.02.13 20:11	Customer622	63			known, Unknown	27.08.12 08:39
14	13.02.13 20:12	Customer869	19			azan', Ryazan	27.08.12 09:01

Аномалии с высоким риском:	**63**
Шаблон вредоносной программы:	43
Некорректный период	1
Пропущен запрос	1
Пропущена загрузка	17
Flood получения	1
Аномалии со средним риском:	**2**
Некорректное изменение параметров	2

Просмотр сессий клиента

Время начала сессии: 27.08.2012 08:39
IP адрес:
Наименование клиента: Customer622
ID ключа:

Сводка | Детали сессии

11 - 20 / 129 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 10

	Начало	Завершение	IP адрес	Тип запроса	Детали запроса
	27.08.2012 08:39:49,600	27.08.2012 08:39:49,600		Получение ресурса	ресурс=entity/doc_list
▶	27.08.2012 08:39:50,053	27.08.2012 08:39:50,115		Получение списка документов	тип_документов=doc/payment,
▼	27.08.2012 08:39:50,490	27.08.2012 08:39:54,584		Получение списка документов	тип_документов=doc/payment,
	Пропущена Шаблон вредоносной программы Некорректный				
	27.08.2012 08:39:57,584	27.08.2012 08:39:57,600		Уведомление о состояниях документов	
	27.08.2012 08:39:57,959	27.08.2012 08:39:58,037		Получение документа	тип_документа=doc/payment, id_документа=
	27.08.2012 08:39:58,381	27.08.2012 08:39:58,709		Получение ресурса	ресурс=entity/vip
	27.08.2012 08:39:59,193	27.08.2012 08:39:59,209		Получение документа	тип_документа=doc/payment, id_документа=
	27.08.2012 08:39:59,522	27.08.2012 08:39:59,522		Получение справочника	справочник=default_accounts
	27.08.2012 08:39:59,865	27.08.2012 08:39:59,865		Получение документа	тип_документа=doc/payment, id_документа=

Предыдущая сессия | Следующая сессия

Детали сессии

Fraud-мониторинг. Анализатор активности

Ключевые свойства

1. Работает в режиме онлайн

2. Не требует обучения

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

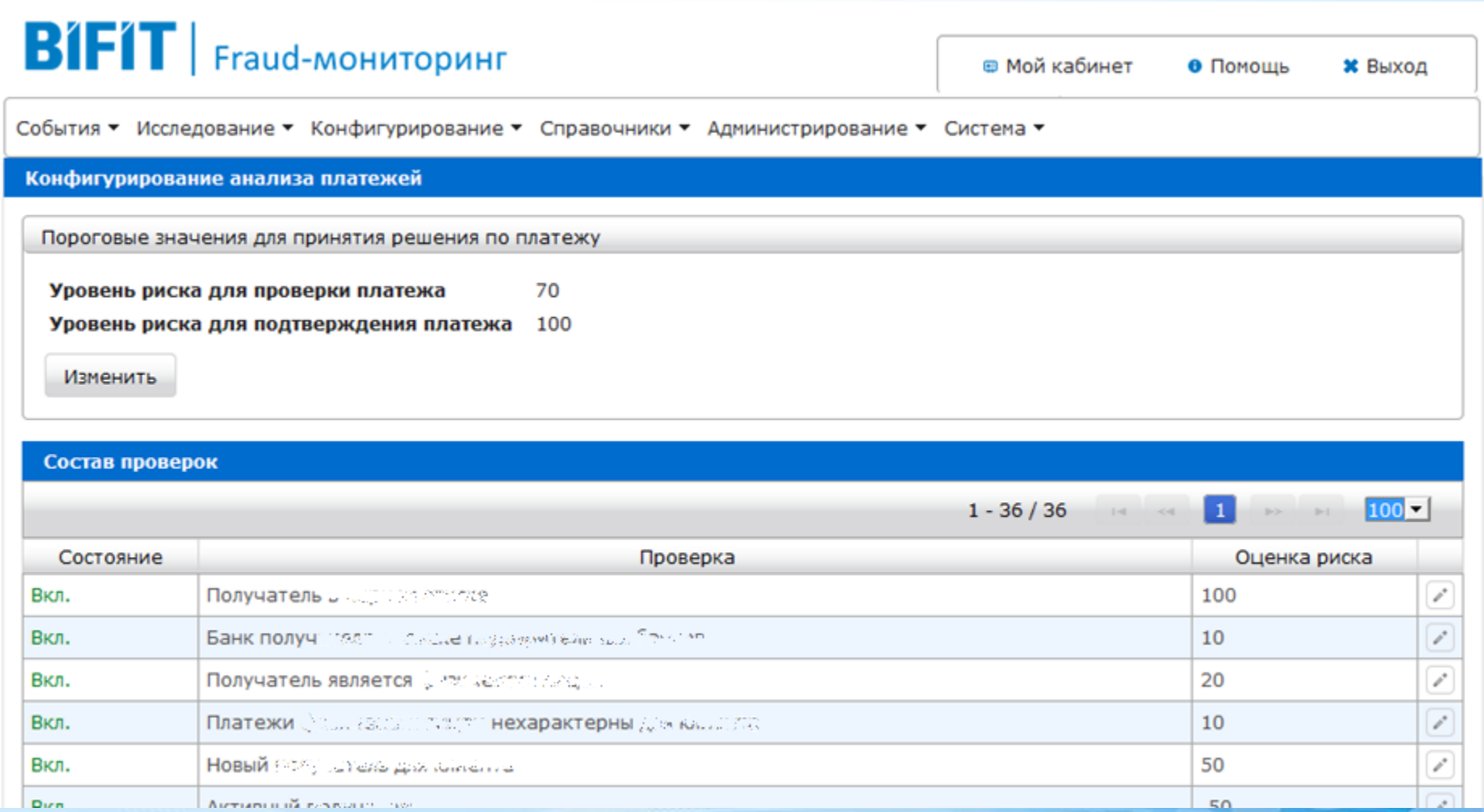
Fraud-мониторинг

Мониторинг транзакций

iBank 2. Fraud-мониторинг. Структурная схема

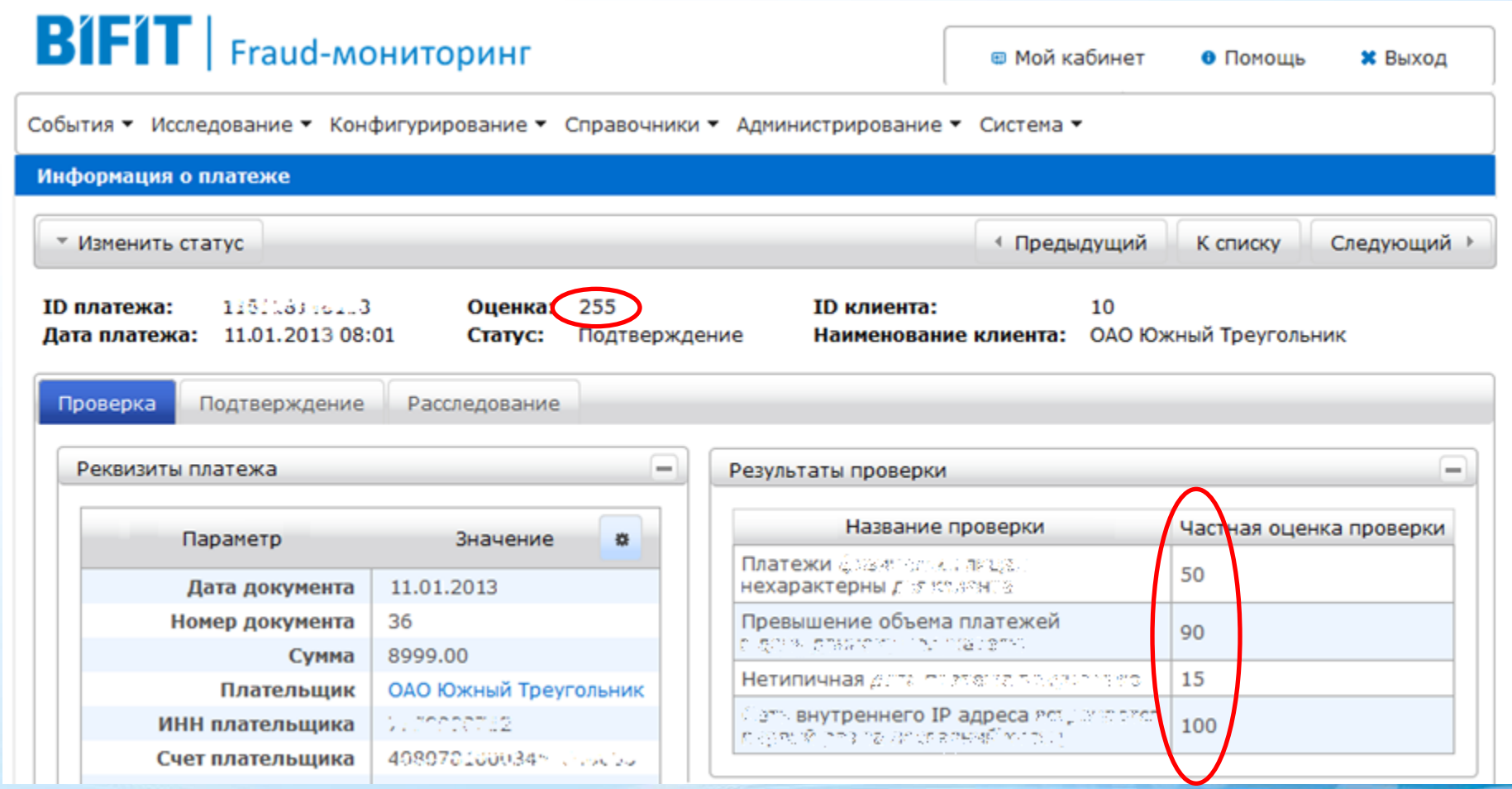
Fraud-мониторинг. Мониторинг транзакций

Конфигурирование проверок



Fraud-мониторинг. Мониторинг транзакций

Пример оценки транзакции



Fraud-мониторинг для ДБО

Вместо выводов

Плотная интеграция Fraud-мониторинга с ДБО обеспечивает высокий уровень выявления попыток мошенничества.

Управляемость критериев проверок помогает оптимизировать долю ложных срабатываний, снизить нагрузку на исполнителей.

BIFIT

Стратегия эшелонированной обороны ДБО

1. Одним «эшелоном» сегодня не обойтись
2. В противостоянии «брони и снаряда» вчерашние подходы не обеспечивают нужный уровень защиты
3. Предотвратить создание условий для хищения проще, чем перехватить попытку в режиме онлайн
4. Универсальных сценариев для всех клиентов нет. Возможность выбора – живучесть бизнеса
5. Эшелоны обороны на стороне банка более управляемые, контролируемые, охватывают сразу всех клиентов
6. «Любительский подход» в обороне неэффективен против профессиональных «нападающих»

BIFIT

Где проходит граница доверенной среды? Стратегия эшелонированной обороны ДБО

Мустафаев Рустам
mustafaev@bifit.com

BIFIT