

**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

BIFIT

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

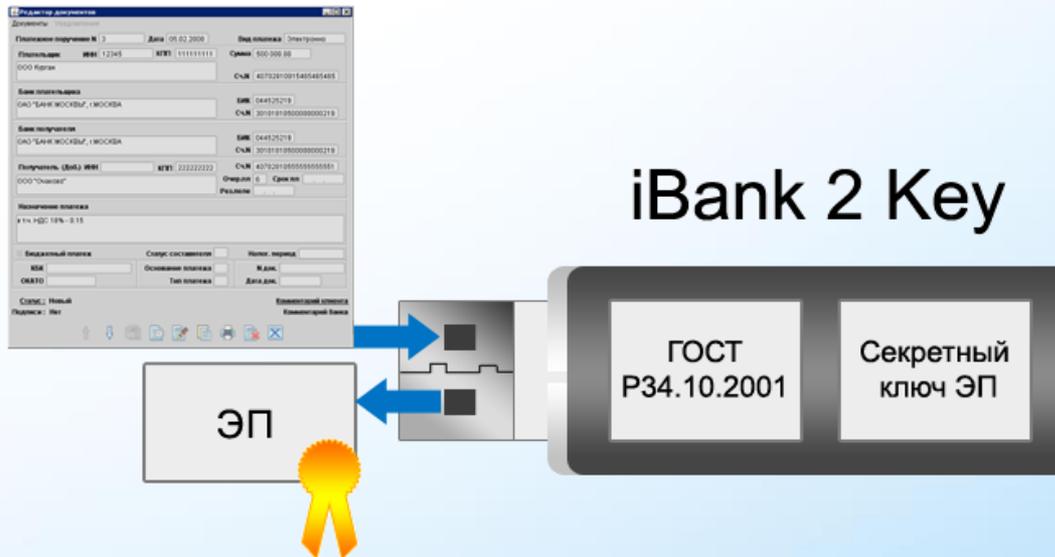
Доверенная среда – там, где нет и не может быть злонамеренного ПО.

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.

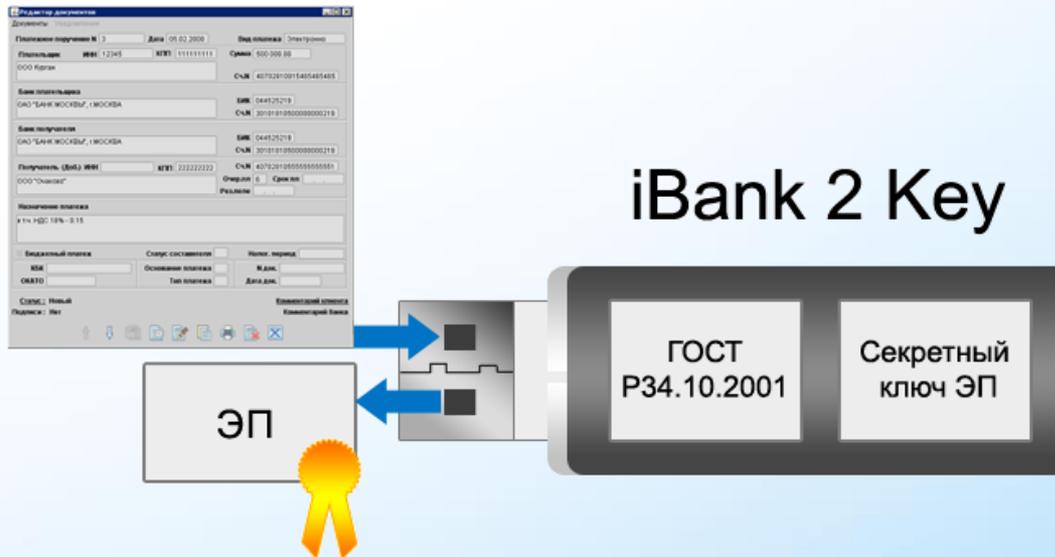


2008 г. Токены и смарткарты с неизвлекаемым хранением ключей подписи

BIFIT

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).

BIFIT

Доверенная среда. Стадия 3

2010 г. Исходные данные:

Комплексная защита компьютера по-прежнему сложна.

Атаки на использование неизвлекаемых ключей стали реальностью.

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

Доверенная среда. Стадия 3

2010 г. Дополнительные одноразовые пароли (ОТР)

Источники ОТР



ОТР 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

Доверенная среда. Стадия 4

2011 г. МАС-токены



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. МАС-токены + «Доверенные получатели»



Реквизиты постоянного контрагента заверяются только один раз и запоминаются системой.

Результат:

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

BIFIT

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**

BIFIT

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

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

Smirnov Aleksey Viktorovich - Операционист. Корпоративные клиенты

Документы Настройки Помощь

Статус угроз: Действующие

Клиент	Статус клиента	Уровень риска							Служебный код	Состояние	Дата состояния
ОАО ФИНКoM	Активный	Критический	⚡						001	Не обработан	28.10.2013 15:37
ОАО Финанс	Активный	Критический	⚡	~		⚙	☕		002	Не обработан	28.10.2013 15:37
ОАО "Сибирь"	Активный	Критический				⚙	☕		003	Не обработан	28.10.2013 15:37
ОАО "ИнтерБанк"	Блокирован	Критический				⚙			004	Не обработан	28.10.2013 15:35

Получение списка угроз: Готово (0.081 с.)

«Сигналы» группируются в «сводки» по клиентам

BIFIT

Fraud-мониторинг. Детектор угроз

ОАО ФИНКОМ

Статус клиента: **Активный**

Состояние: **Не обработан с 28.10.2013 15:37**

 Принять на обработку

 Заблокировать

 Информация

 Учетные записи

 Скомпрометированные ключи

 Скомпрометированные IP-адреса

 Платежные поручения

 Журнал

Имя компьютера	Имя пользователя	Угрозы								Служебный код	Последний вход	Последнее детектирование	Статус
DenKot	denkot	Найдены								44	28.10.2013 15:24		Активна
GAYDEY	gaydey	Найдены								21427	28.10.2013 16:43	28.10.2013 16:43	Активна

Данные по учетной записи GAYDEY/gaydey на 28.10.2013 16:43

Признаки внедрения г...

Обнаружено использование функций, не предусмотренных штатной работой программы.

Обнаружена модификация программы.

Степень угрозы: **критическая**

Признаки подмены

Показания по отдельному клиенту.

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

BIFIT

Fraud-мониторинг. Детектор угроз

ОАО ФИНКoM

Статус клиента: **Активный**

Состояние: **Не обработан с 28.10.2013 15:37**

 Принять на обработку

 Заблокировать

 Информация

 Учетные записи

 Скомпрометированные ключи

 Скомпрометированные IP-адреса

 Платежные поручения

 Журнал

с по

Дата и время	Тип действия	Служебный код	Имя компьютера	Имя пользователя	Внешний IP-адрес	Внутренний IP-адрес	Идентификатор ключа	Б
28.10.2013 16:43	Вход в систему	...	GAYDEY	gaydey	209.24.10.13	192.168.3.14	13:520990733491201	Ф
28.10.2013 15:37	Вход в систему	...	GAYDEY	gaydey	209.24.10.13	192.168.3.14	13:520990733491201	Ф

Показания. Детальный журнал

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

BIFIT

Fraud-мониторинг

Анализатор активности

BIFIT

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

События ▾ Исследование ▾ Конфигурирование ▾ Справочники ▾ Администрирование ▾ Система ▾

События в журнале работы

Дата с по Статус Заключение

Поле Значение [Сбросить](#)

Изменить статус

№	Дата	Клиент	Аномалии	ID ключа	IP адрес	Положение	Сессия
10	13.02.13 20:09	Customer224	28 + 2	01070477946761780	0107241120111	RU, Unknown, Unknown	27.08.12 07:20
11	13.02.13 20:09	Customer224	8 + 6	010675171048791100	2103069260111	RU, Unknown, Unknown	27.08.12 08:02
12	13.02.13 20:09	Customer348	10 + 2	0100100787117100120	0106702131100	RU, Komi, Syktyvkar	27.08.12 08:03
13	13.02.13 20:11	Customer622	63			Unknown, 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 времени для запроса:	1
Пропущен запрос получения документа:	1
Пропущена загрузка ресурса для получения документа:	17
Flood получения документа:	1
Аномалии со средним риском:	2
Некорректное изменение параметров времени для запроса:	2

Время начала сессии: 27.08.2012 08:39
 IP адрес: 193.147.251.100

Наименование клиента: Customer622
 ID ключа: 027401177101030000

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	193.147.251.100	Получение ресурса	ресурс=entity/doc_list
▶	27.08.2012 08:39:50,053	27.08.2012 08:39:50,115	193.147.251.100	Получение списка документов	тип_документов=doc/payment, id_документа=9775159710, id_документа=9775159710, id_документа=9775159710, id_документа=9775159710
◀	27.08.2012 08:39:50,490	27.08.2012 08:39:54,584	193.147.251.100	Получение списка документов	тип_документов=doc/payment, id_документа=9775159710, id_документа=9775159710, id_документа=9775159710, id_документа=9775159710
<p>Пропущена запись, так как она не соответствует шаблону вредоносной программы Некорректный шаблон вредоносной программы</p>					
	27.08.2012 08:39:57,584	27.08.2012 08:39:57,600	193.147.251.100	Уведомление о состояниях документов	
	27.08.2012 08:39:57,959	27.08.2012 08:39:58,037	193.147.251.100	Получение документа	тип_документа=doc/payment, id_документа=9775159710
	27.08.2012 08:39:58,381	27.08.2012 08:39:58,709	193.147.251.100	Получение ресурса	ресурс=entity/vip
	27.08.2012 08:39:59,193	27.08.2012 08:39:59,209	193.147.251.100	Получение документа	тип_документа=doc/payment, id_документа=9775159710
	27.08.2012 08:39:59,522	27.08.2012 08:39:59,522	193.147.251.100	Получение справочника	справочник=default_accounts
	27.08.2012 08:39:59,865	27.08.2012 08:39:59,865	193.147.251.100	Получение документа	тип_документа=doc/payment, id_документа=9775159710

← 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

BIFIT

iBank 2. Fraud-мониторинг. Структурная схема



Fraud-мониторинг. Мониторинг транзакций

Конфигурирование проверок

Конфигурирование анализа платежей

Пороговые значения для принятия решения по платежу

Уровень риска для проверки платежа 70
Уровень риска для подтверждения платежа 100

Изменить

Состав проверок

1 - 36 / 36

1

100

Состояние	Проверка	Оценка риска	
Вкл.	Получатель находится в списке	100	
Вкл.	Банк получателя находится в списке	10	
Вкл.	Получатель является физическим лицом	20	
Вкл.	Платежи получателя нехарактерны для клиента	10	
Вкл.	Новый получатель для клиента	50	
Вкл.	Активный получатель	50	

Fraud-мониторинг. Мониторинг транзакций

Пример оценки транзакции

BIFIT | Fraud-мониторинг

Мой кабинет Помощь Выход

События ▾ Исследование ▾ Конфигурирование ▾ Справочники ▾ Администрирование ▾ Система ▾

Информация о платеже

Изменить статус ← Предыдущий К списку Следующий →

ID платежа: 118118118113 **Оценка:** 255 **ID клиента:** 10
Дата платежа: 11.01.2013 08:01 **Статус:** Подтверждение **Наименование клиента:** ОАО Южный Треугольник

Проверка Подтверждение Расследование

Реквизиты платежа

Параметр	Значение	#
Дата документа	11.01.2013	
Номер документа	36	
Сумма	8999.00	
Плательщик	ОАО Южный Треугольник	
ИНН плательщика	7709000712	
Счет плательщика	40807010003401000000	

Результаты проверки

Название проверки	Частная оценка проверки
Платежи физическим лицам нехарактерны для клиента	50
Превышение объема платежей в день платежа над планом	90
Нетипичная дата платежа по договору	15
Использование внутреннего IP адреса при доступе к сервису для не доверенных клиентов	100

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»

Где проходит граница доверенной среды?

Стратегия эшелонированной обороны ДБО