



Решение некоторых актуальных вопросов информационной безопасности для банков

А.Г.Сабанов, к.т.н.,
зам.ген.директора ЗАО «Аладдин Р.Д.»
Эксперт по информационной безопасности АРЕС Electronic
Commerce Steering Group

*2-я Международная конференция
«Инфофорум–Болгария»*

13-17 сентября 2010г.

Служба ИБ в банке

Удостоверяющий Центр Корпоративной Информационной Системы

Отдел внедрения и сопровождения систем обеспечения информационной безопасности

Отдел криптографической защиты информации

Отдел администраторов безопасности

Отдел информационной безопасности автоматизированных банковских систем

Отдел безопасности платежных систем

Отдел аудита и аттестации информационных систем



Функционал системы ИБ банка

- Управление запросами СКП и ключами
- Управление ключевыми носителями
- Система защищенного доступа
- Учет дистрибутивов ПО
- Управление лицензиями СКЗИ
- Интеграция с АБС
- Система управления паролями и SSO
- Система VPN на сертифицированном СКЗИ
- Система учета внутренних АРМ
- Система учета носителей информации
- Система контроля действий пользователей
- Автоматизация обновления ПО и смены СКП

ТОП-5 наиболее актуальных задач ИБ

- Противодействие атакам на системы дистанционного банковского обслуживания (ДБО);
- Защита от инсайдерских атак;
- Фильтрация Web-трафика от вирусов, троянов и т.д.;
- Защита от распределенных сетевых DDoS-атак на сайты банков;
- Атаки на платежные карты, банкоматы и платежные терминалы.

По материалам 2-ой Международной межбанковской конференции по информационной безопасности ДЦ «Юбилейный» г.Магнитогорск 15-20 февраля 2010г.

Атаки на ДБО - появление новых «бизнесов»

1. Атаки на клиентов банков стали массовыми и адресными
2. «Разделение труда»
 - Сбор информации о клиентах, их счетах и суммах с целью перепродажи
 - Кража денег с выбранных счетов – проведение адресных атак

Причины

- Кризис (обострение проблем)
- Доступность инструментария для подготовки и проведения адресных атак
 - Используются уязвимости ПО и бот-сети
 - Стоимость менее \$100
- Перекладывание ответственности за безопасность на клиента (хотя он не может себя нормально защитить)

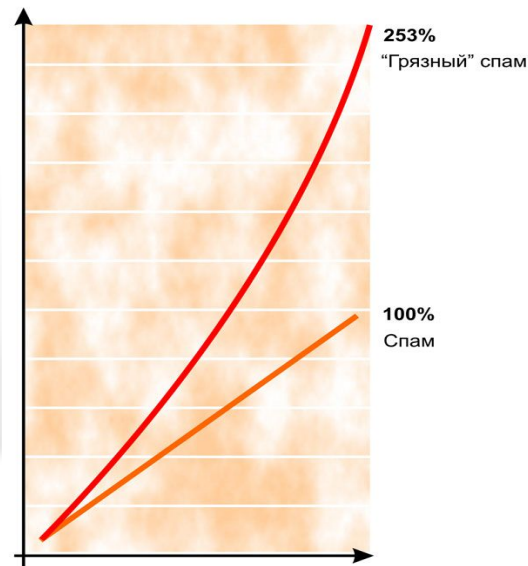
Что происходит и почему?

Масштаб бедствия

Из 600 млн. компьютеров, подключенных к Интернет, 100-150 млн. уже являются частью бот-сетей.

Давос, январь 2007
Из доклада Виртона Серта

25%



Главные источники угроз

- Уязвимости Web-приложений – «заряженные» сайты – эксплойты
 - 63% сайтов РФ имеют критические уязвимости*
- Специализированные эксплойты и трояны - антивирусы против них не эффективны

Как мы получаем spyware

- Переходя по ссылкам в спамерских письмах («грязный» спам)
- Через поисковики (подозрительные сайты)
- Фишинг (письма «от банка»)

Инструментарий

Конструктор для подготовки и организации адресных атак

- Создание эксплойта для сайта, скрытно устанавливающего исполняемые программы на компьютере клиента

Web Attacker
Toolkit

inet-lux | - Microsoft Internet Explorer provided by Finjan

File Edit View Favorites Tools Help

Address <http://inet-lux.com/index.php?go=PageSid=3>

Google Search 7 blocked Check AutoLink AutoFill Options

« Не пытайся избежать своих врагов, а просто контролируй их. Знай где они, что думают и кому верят! »

| =INET-LUX.COM= |

Здравствуйте, Гость | Авторизация | Регистрация

Навигация

- На главную
- О нас
- Новости
- Наши продукты
- Вопрос-ответ
- Оставить отзыв
- Мой офис
- Пресс-центр
- Контакты

Авторизация

Логин:

Пароль:

Запомнить меня

Войти...

Регистрация
Напомнить пароль

Ваше мнение

Сколько вы готовы платить за эксплойт?
© 100-300\$

Мульти-компонентный эксплойт **Web-Attacker IE0604** (Март 2006г.)


Уважаемые друзья! Мы рады предложить Вам мультикомпонентный эксплойт **Web-Attacker IE0604**, реализующий уязвимости в популярных Интернет-браузерах Internet Explorer и Mozilla Firefox. При помощи данного эксплойта Вы можете устанавливать любые исполняемые программы на локальных дисках посетителей Ваших сайтов. В основе работы эксплойта **Web-Attacker IE0604** лежат семь обнаруженных ранее уязвимостей в Интернет-браузерах:

Назначение эксплойта: скрытая загрузка EXE-программы с удаленного ресурса с последующим запуском этой программы на локальном диске посетителя.

В основе работы эксплойта лежат 7 уязвимостей:

1. Last Stage of Delirium Research Group, "Java and Java Virtual Machine Security Vulnerabilities and their Exploitation Techniques", <http://ltd-pl.net/>. По классификации Microsoft - MS03-11. Цель: машины с Windows 98-XP, браузером Internet Explorer, с установленной Microsoft Virtual Machine версии 5.0.3805.0 или младше.
2. Roozbeh Afrasiabi, "IE ms-its: and mk:@MSITStore: vulnerability", Insecure.org mail archive <http://www.insecure.org/>, Mar 27 2004 По классификации Microsoft - MS04-013

Отзывы клиентов:



"Знакомого купил связку - говорит она просто [redacted]. Он все секреты не выдает, но мою тачку и тестовую и настоящую пробило как за не*** делать".

JagUarc

Оставить отзыв

Done Internet

Конструктор spyware

- специализированных троянов

Downloader - RootLauncher v2.5

Downloader предназначен для скрытой загрузки произвольного WIN32 EXE-файла с удаленного ресурса с последующим запуском этого файла на локальном диске.

Продукты - RootLauncher	[Цена]	[Документация]
"Professional Edition" [PE]	150\$ обновления: 20\$	готовится готовится
"Econom Edition" [EE]	100\$ обновления: 15\$	Онлайн Офлайн
"Light Edition" [LE]	50\$ обновления: 10\$	готовится готовится

Даунлоадеры - RootLauncher v2.5 не обнаруживается следующими антивирусами:

HTMLProtector interface showing various protection options:

- Disable right mouse button
- Show warning: This page has been protected. Preview only.
- Disable text select
- Disable off-line page viewing
- Don't display links in status bar
- Disable page printing
- Disable clipboard and printscreen
- Disable drag and drop
- Disable adobe acrobat web capture
- Disable opera user
- Kill frame
- Location lock: Domain/URL address: http://www.yourhost.com
- Referrer lock: Domain/URL address: http://www.your-referrer-domain.com

Pinch II PRO Builder interface showing configuration options:

- Protocol: HTTP
- HTTP Properties: URL: [empty], Allow to resolve IP, Add CID, Status check str: _ret_ok_1
- Run: PWD, Run, Spy, NET, BD, etc, Kill
- Location folder: C:\
- Values: KEY: MStask, DLL: p2sys.dll, EXE: svchost.exe, SVC: ServiceName, DIS: ServiceDiscript
- Act after: date, time (12:12)
- Act after stop svc and kill process: Bypass Windows Firewall (SP2)
- Packing: FSG, UPX, MEW
- COMPILE button

Web-Attacker (IE0604) config editor dialog box:

- Enter here an URL path for CGI-script on your server: http://www.yourhost.com/cgi-bin/ie0604.cgi
- Enter here the folder name for placing an output exploit components: c:\Ie0604\Output
- Web-Panel password: admin
- Encrypt HTML files: [unchecked]
- (c) by Inet-Lux Team (http://www.inet-lux.com), 2006
- Registered to ID 1234ABCD

От защиты объекта к защите взаимодействия

Основные векторы угроз

- Кража регистрационных данных клиентов (account'ов)
- Кража / перехват ключей ЭЦП / кодов авторизации / одноразовых паролей (SMS)

Противодействие

- Усиление аутентификации
 - Использование автономных устройств
 - OTP (One Time Password)- генераторов
 - Токенов для защищенного хранения криптографических ключей ЭЦП
 - Токенов с аппаратной ЭЦП (неизвлекаемый ключ ЭЦП)
- Для «толстого клиента» основной проблемой остается вопрос доверенной среды
- Большой интерес и новые разработки связаны с «тонким клиентом» (Web) □ **основные вопросы обеспечения безопасной работы**

Даже Токен с аппаратным ЭЦП проблем не снимает – требуется прорабатывать всю security-архитектуру решения

Смарт-карты (2000 – н.в.)

- + Разработаны для задач ИБ (secure by design)
- + Встроенная защищённая память
- + Общепринятые стандарты безопасности, аппаратно реализованы криптоалгоритмы
- Сложность расширения функционала, длительный цикл разработки и тестирования

2

Микроконтроллеры для Java-карт (2007 – н.в.)

- + Быстрая периферия (USB-контроллер), драйвера в ОС

4

3

Java-карты (2002 – н.в.)

- + Расширение функционала за счёт загрузки Java-апплетов
- Медленное взаимодействие с периферией

1

Микроконтроллеры общего назначения (1998 – н.в.)

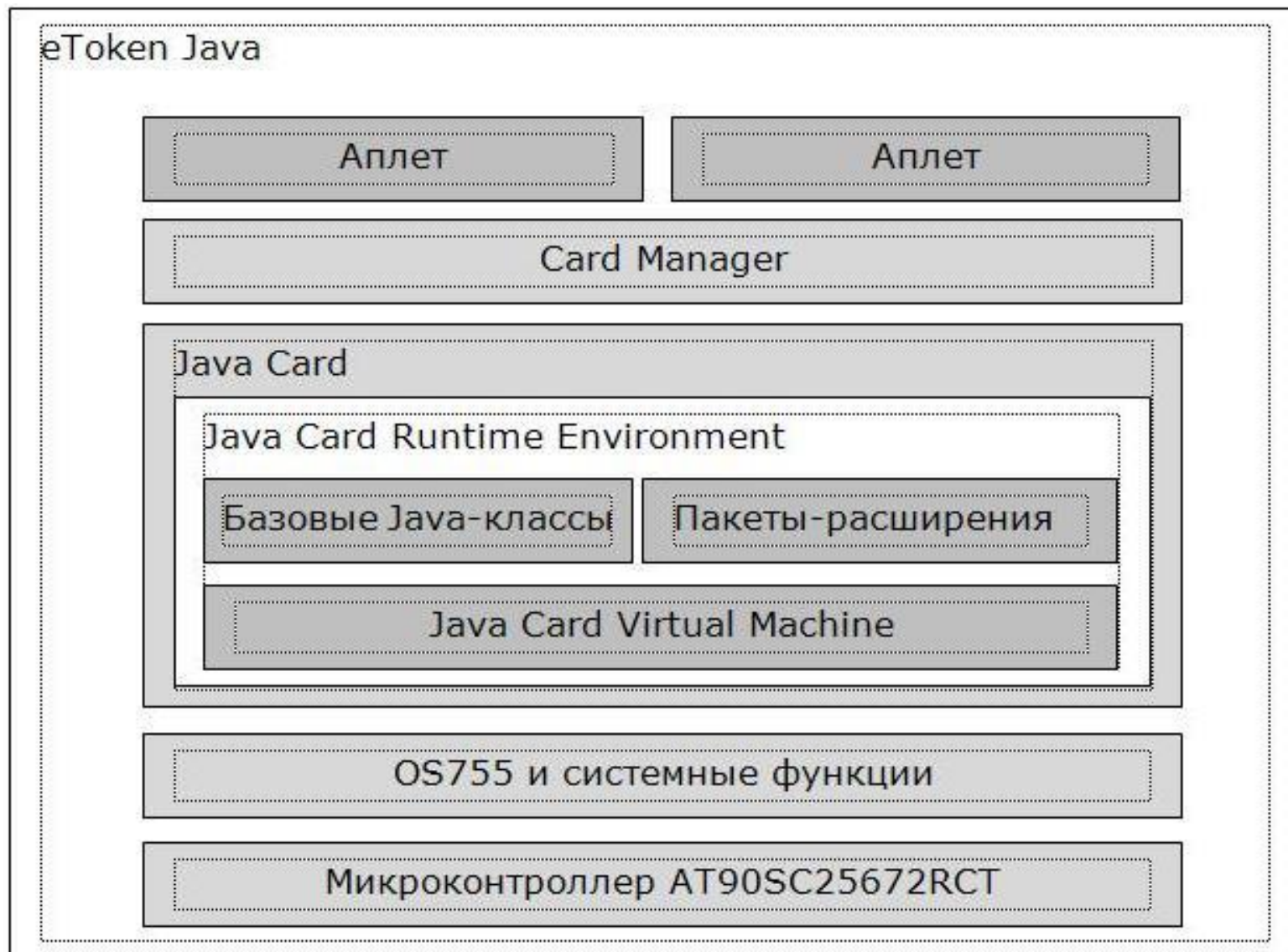
- Не предназначены для задач ИБ (unsecure by design)
- Данные хранятся во внешней памяти, невозможность форм-фактора смарт-карты
- Программная реализация функций безопасности, алгоритмов шифрования
- Проприетарная архитектура, нет стандартов

Примеры: iKey 1000, eToken R2, ruToken, Шипка

ВАЖНО: Есть факты взлома ключей, построенных на данной архитектуре (iKey1000)



Общая архитектура eToken Java



Электронные ключи eToken Java

- Содержат Java-карту, полностью соответствующую стандартной спецификации Java Card компании SUN (ныне Oracle) и спецификации Global Platform
 - [Java Card Platform Specification](#) Java Card Platform Specification 2.2 Java Card Platform Specification 2.2.1 (<http://java.sun.com/products/javacard/>)
 - Global Platform 2.2 (<http://www.globalplatform.org>)
- В карту загружен Java-апплет, реализующий функционал eToken PRO
- Есть возможность загрузки дополнительных апплетов, созданных независимыми разработчиками



Электронные ключи eToken

- Модели eToken
 - USB-ключ/смарт-карта eToken PRO (Java)
 - MobilePASS – программный OTP
 - Генератор одноразовых паролей eToken PASS
 - Комбинированный USB-ключ с генератором одноразовых паролей eToken NG-OTP (Java)
 - Комбинированный USB-ключ с дополнительным модулем flash-памяти eToken NG-FLASH (Java)
 - USB-ключ/смарт-карта eToken ГОСТ

Финансово-экономическое обоснование проекта.

«Стоимость» риска

1. Прямые потери клиентов

- При атаке на одного клиента обычно похищается от 500,000 до 25,000,000 руб. При этом, в большинстве случаев одновременно атакуются несколько клиентов.

**Известны прецеденты, когда клиентам удавалось через суд взыскать с банка похищенные средства.*

2. Репутационные потери Банка

- «Продвинутые» пострадавшие публикуют информацию о хищениях на банковских ресурсах (www.banki.ru) «Продвинутые» пострадавшие публикуют информацию о хищениях на банковских ресурсах (www.banki.ru, www.bankir.ru и т.д.), что вызывает отток клиентов и формирование негативного имиджа банка.

3. Затраченные ресурсы

- *Необходимо принимать во внимание расход на отвлеченный от работы департамент ИТ и Информационной безопасности*

Финансово-экономическое обоснование проекта «Стоимость» риска (2)

Кроме того, после хищения обычно организуется DDoS-атака на сервис системы ДБО, в результате чего он временно прекращает функционирование.

Можно посчитать убытки банка при атаке длительностью в 8 часов:

- Недополученная прибыль:

Количество операций в ДБО. Цена одной операции в среднем 16 рублей.

16 руб. – 5000 клиентов – 15 операций в день. = 1 200 000 руб.

- Расходы на защиту от DDoS.

оперативная защита 100 000 - 200 000 руб.

Если у ISP (провайдер) тарифицируется входящий трафик, то умножаем трафик в Гб на цену 1 Гб: 5 – 100 Гб.

перерасход трафика. 5000 – 100 000 руб.

Итого:

Не считая расследование (не входит в ущерб): **от 1 305 000 до 1 500 000 руб.**

** Расходы злоумышленника - 300 Евро.*

Финансово-экономическое обоснование проекта (3)

Как сделать информационную безопасность прибыльной?

- Клиенты готовы платить за свою безопасность
- При правильной организации процесса, Банк имеет возможность дополнительно зарабатывать на услугах по обеспечению безопасности в своей системе ДБО.

Предоставление ключей:	
на защищенном носителе	1650 руб.
на бюджетном носителе	375 руб.

Обслуживание и поддержка безопасности Системы «Альфа-Клиент On-line»

2 200 руб. в месяц (комиссия взимается с одного счета Клиента, независимо от количества счетов в валюте РФ/иностранной валюте, открытых в банке)

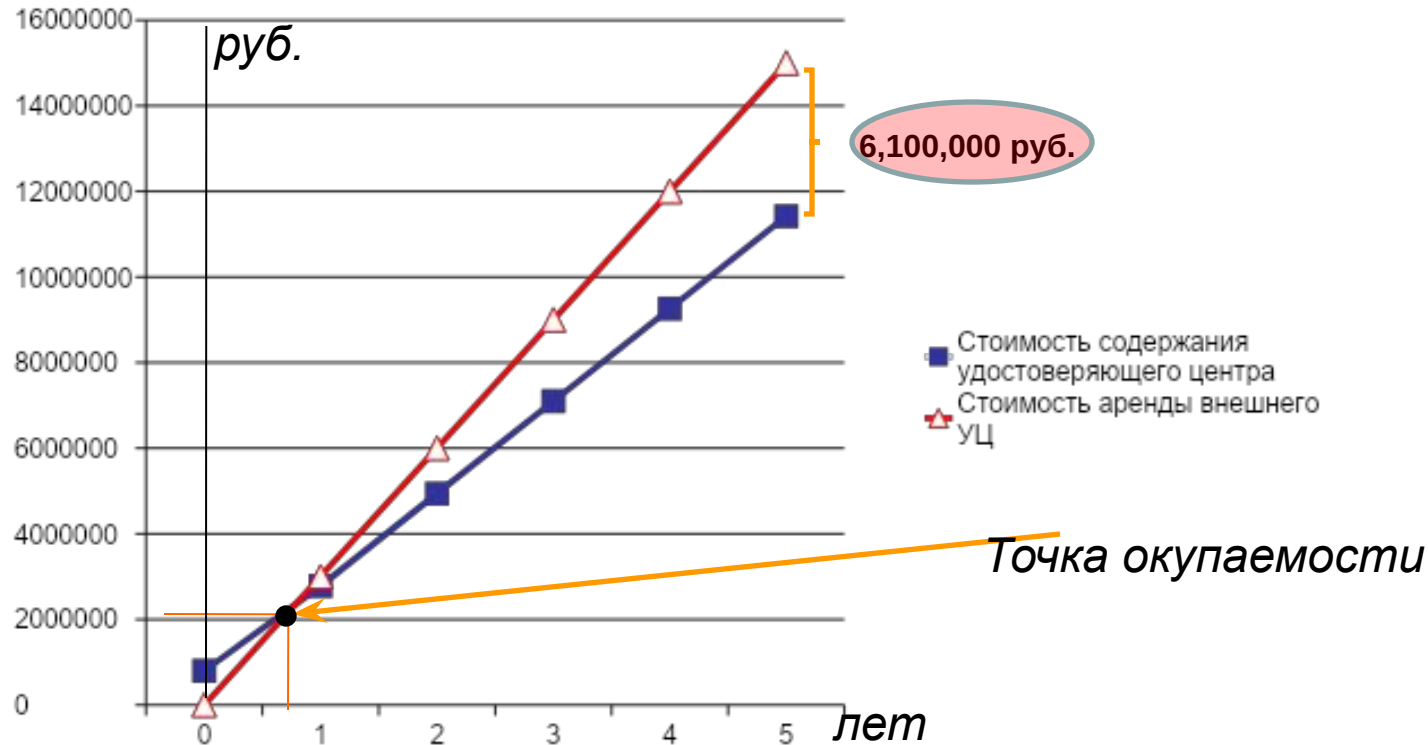
1.4	Ключевые носители ¹ для системы Corporate Online	
1.4.1	Ключевой носитель eToken PRO	<p>Стоимость 2 (двух) ключевых носителей eToken PRO входит в стоимость подключения системы Corporate Online, указанную в п.п. 1.3.1 и 1.3.2.</p> <p>1 000 RUB</p> <p>Комиссия взимается при приобретении 3-го (третьего) и каждого последующего ключевого носителя eToken PRO.</p>

7.	Предоставление электронного USB-ключа «E-Token»	1500 RUB за ключ
----	---	------------------

Предоставление Банком ключевого носителя USB eToken PRO/64K	2200	в случае предоставления взамен поломанных или утерянных по вине клиента носителей, предоставленных в составе комплекта системы «Клиент-Банк» или «Интернет-Клиент»
---	------	--

Финансово-экономическое обоснование проекта (4)

Содержание собственного Удостоверяющего центра



Исходные данные для расчёта:

- Стоимость ПО для УЦ на 5000 лицензий – 600,000 руб.
- Стоимость оборудования – 200,000 руб.
- Зарплата сотрудников в год (всего 3 человека) – 2,160,000 руб.
- Стоимость одного цифрового сертификата (коммерческий УЦ) – 600 руб.

Старт проекта.

Оценка рисков и выбор технологии защиты

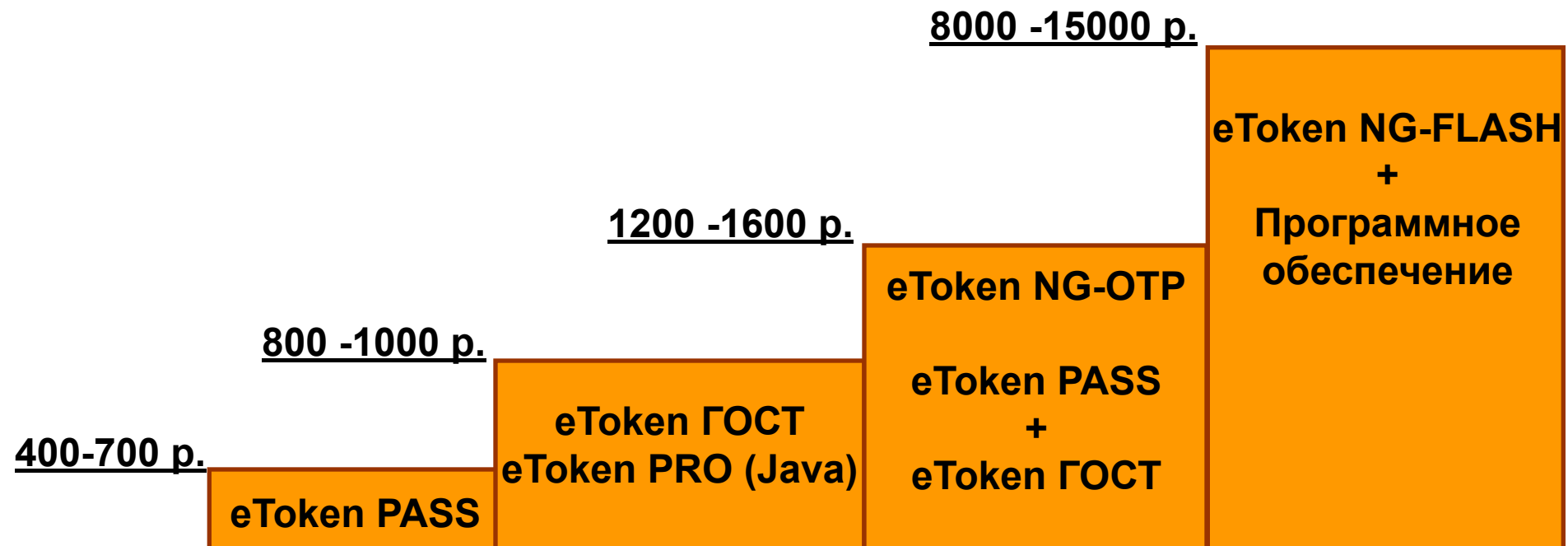
Угроза	Риск	Актуальность риска*	Решение
Цель: закрытый ключ ЭЦП пользователя			
Несанкционированное копирование закрытого ключа ЭЦП пользователя с последующим использованием	Хищение закрытого ключа из незащищенного хранилища	70%	Использование токенов, выполняющих операции с закрытым ключом пользователя внутри физического устройства. Закрытый ключ не может быть скомпрометирован.
	Хищение закрытого ключа из оперативной памяти РС	5%	
Цель: криптографические возможности токена			
Несанкционированное использование ключевого контейнера, либо токена, непосредственно на рабочей станции клиента системы ДБО	Хищение СКЗИ, инсайд	10%	Для работы с токеном требуется аутентификация в устройстве на основе PIN-кода пользователя.
	Удаленное управление машиной с подключенным токеном	14%	Наряду с использованием ЭЦП, вырабатываемой токеном, можно требовать подтверждения транзакций одноразовым паролем (OTP), который вырабатывается (eToken NG-OTP/eToken PASS).
Цель: документ, для которого вырабатывается ЭЦП, или его HASH			
Подмена документа или хеш-значения в процессе его передачи в СКЗИ	Активность вирусного ПО	1%	Предоставление клиентам Токена в комплекте с антивирусным пакетом, который существенно снижает уровень угроз, связанных с вирусами.

* По данным **Group IB** для систем дистанционного банковского обслуживания

«Лесенка» решений для клиентов

Предоставление клиентам средств защиты должно быть приведено в соответствие с их потребностями и уровнем риска

- Физические лица - ОТР-токены
- Юр. лица (SMB) - Защищенные ключевые носители
- Корпоративные клиенты - ОТР + Защищенные ключевые носители
- VIP-клиенты – защищенная мобильная ОС на носителе





«Подводные камни»

На что стоит обратить внимание:

1. Организация работы подразделений, участвующих в процессе

- Обучение персонала, который непосредственно общается с клиентами
 - операционисты должны уметь правильно объяснить клиенту, зачем ему нужны средства защиты
- Должен существовать регламент реагирования службы безопасности на инциденты (хищения средств, DDoS и т.д.)

*возможна передача данных задач на аутсорсинг специализированным компаниям

2. Юридические вопросы

- Корректность клиентских договоров на обслуживание по системе ДБО, актов, доверенностей на генерации и т.д.

*при судебном разбирательстве любое упущение в договоре может привести к тому, что банку придется возмещать ущерб

- Наличие лицензий на распространение СКЗИ, в соответствии с требованиями регулирующих органов

*претензии проверяющих на наличие лицензий ФСБ могут привести к приостановке деятельности организации

Best practice (1)

1. Повышение уровня безопасности должно сопровождаться улучшением пользовательских характеристик системы

МОСКОВСКИЙ
ИНДУСТРИАЛЬНЫЙ
БАНК

Aladdin
SECURITY SOLUTIONS

Персональное средство защиты пользователей электронной системы ПТК «Интернет-Банк»

- ▶ Установить ПТК «Интернет-Банк»
- ▶ Установить программное обеспечение для eToken PRO (Java)
- ▶ Прочитать инструкцию по установке ПТК «Интернет-Банк»
- ▶ Прочитать инструкцию по работе с ПТК «Интернет-Банк»
- ▶ Установить Adobe Acrobat Reader
- ▶ Выход

© 2005-2010, ОАО «МИНБ»

А

Альфа-Банк

Электронный ключ для системы
«Альфа-Клиент On-line» ОАО «АЛЬФА-БАНК»

- ▶ Инструкция по установке
- ▶ Запустить Мастер установки

Aladdin
SECURITY SOLUTIONS

Информация ОАО «АЛЬФА-БАНК» - Зарплатный Проект

Решения Aladdin по защите информации

Выход



2. Для бизнеса: дополнительные возможности для коммуникации с клиентами и донесения рекламной информации

Best practice (2)

3. «Схема одного визита». В Банке:



Best practice (3)

3. «Схема одного визита». Удаленно:





Итоги реализованных проектов

1. Повышение лояльности клиентов за счет увеличения защищенности сервиса ДБО.
2. Снижение репутационных рисков, связанных с распространением в СМИ публикаций о краже средств со счетов клиентов.
3. Повышение удобства подключения и работы клиента в системе ДБО
4. Дополнительные доходы для Банка. Департамент информационной безопасности перестает быть затратным подразделением.

eToken в системах ДБО:

В России:

- Альфа-банк
- Банк Возрождение
- Газпромбанк
- КМБ-Банк
- Коммерцбанк-Евразия
- Метробанк
- Уралпромбанк
- Интерпрогрессбанк
и многие другие ...



В мире:

- Bankernes EDB Central (BEC)
- Banco Central do Brasil
- Bank Hapoalim
- Postbank
- Commerzbank International S.A.
- Israel Securities Authority
- Hypovereinsbank (HVB)
- Deutscher Ring
- Israel Discount Bank Ltd.
- NH-Bank
и многие другие...





Спасибо за внимание!

asabanov@aladdin.ru

www.aladdin.ru

«Аладдин Р.Д.» – визитная карточка

- 15 лет на рынке
- Более 90 чел. (Московский офис)
- Офисы:
 - Казахстан
 - Украина
- Лицензии:
 - ФСБ (включая лицензии на гос.тайну и разработку шифросредств)
 - ФСТЭК России
 - Минэкономразвития (на экспорт/импорт шифросредств)

Основные направления:

- Обеспечение безопасного доступа к информационным ресурсам (аутентификация)
 - ✓ eToken
- Content Security для крупных корпоративных сетей и интернет-провайдеров
 - ✓ eSafe
- Шифрование дисков, защита БД и перс. Данных
 - ✓ Кripto БД
 - ✓ Secret Disk
- Защита ПО
 - ✓ HASP

Сертифицированные по требованиям ФСТЭК решения

- eToken Pro 32K
- eToken PRO SmartCard
- Secret Disk NG 3.1
- eToken Windows Logon
- eToken PRO 64K
- eToken NG-OTP
- Secret Disk Server NG 3.2
- eToken Java
- eSafe 6
- TMS