Защита систем дистанционного банковского обслуживания от мошенничества

Окулесский Василий Андреевич,
кандидат технических наук

Урал, 2014

О чем будем говорить

0. Очень краткий обзор проблемы
1. Современные системы ДБО
   - Функции современного Интернет-банкинга
   - Штрихи о виртуальных платежных системах
2. Организация работы Интернет-банкинга
3. Модель угроз
4. Краткая историческая справка по способам мошенничеств в ДБО
5. Краткая история механизмов безопасности в ДБО
6. Источники и составные части причин возможности мошенничеств в ДБО
7. Особенности наиболее распространенных схем мошенничеств
8. Стратегия защиты систем
9. Примеры отдельных технических решений

0. Состояние дел с мошенничествами в «паутине»

МВД подсчитало количество жертв от киберпреступлений в мире
30.01.2014 14:23
Каждую секунду жертвами киберпреступников в мире становятся 12 человек, и эта цифра растет, сообщил в четверг начальник Бюро специальных технических мероприятий МВД России Алексей Мошков.

"Согласно оценкам экспертов, каждую секунду жертвами киберпреступности в мире становятся 12 человек, и это количество с каждым годом растет. Основной мотив киберпреступников - привлечение материальной выгоды. Количество преступлений, совершаемых из хулиганских и иных побуждений, крайне незначительно", - сказал он, выступая с докладом на форуме информационной безопасности.
По его словам, в прошлом году сотрудниками Управления "К" было предотвращено хищение около 1 миллиарда рублей с банковских счетов граждан.
"В истекшем году нами установлены лица, причастные к созданию и использованию вредоносных программ. Злоумышленники успели получить персональные данные нескольких десятков тысяч клиентов российских банков. Сотрудниками Управления "К" было предотвращен хищение на сумму около 1 миллиарда рублей с банковских счетов граждан", - отметил Мошков

0. Состояние дел с мошенничествами в «паутине»

Управление «К» МВД России и Центр информационной безопасности ФСБ России задержали в Москве организаторов хакерской банды, которая за полгода при помощи троянских вирусов похитила с банковских счетов около 60 млн рублей, сообщила во вторник 20 марта 2012 руководитель пресс-службы Управления «К» Лариса Жукова.

Подозреваемые занимались массовым распространением специализированных «банковских» троянских программ типа Carberp и RDP-door, с помощью которых получали полный доступ к персональным компьютерам большого количества организаций, использовавшихся для работы с системами «Банк-Клиент».

По данному факту возбуждено уголовное дело по ст. 272 УК РФ (Неправомерный доступ к компьютерной информации), ст. 273 УК РФ (Создание, использование и распространение вредоносных программ для ЭВМ) и ст. 158 УК РФ (Кража).

0. Состояние дел с мошенничествами в «паутине»

- **Российский рынок киберпреступности растет на 80-100% каждый год и в 2011 г. составил 2,3 млрд. долларов. Большая часть этих денег заработана на взломах систем ДБО.***
- **В 2011 г. качественно изменился состав хакерских преступных группировок, что привело к резкому росту процента успешных атак и обходу всех традиционных методов защиты ДБО (системы фрод-мониторинга, токены, одноразовые пароли и т.д.).**
- **В начале 2012 г. в межбанковской системе обмена информацией об инцидентах безопасности были опубликованы данные о новом классе атак (т.н. «автозалив»), которые позволяют незаметно для пользователя подменять реквизиты платежного документа при передаче его на подпись в токен.**
- **Максимальная зафиксированная сумма атаки - около 900 млн. руб.**
- **Средняя сумма атаки составляет от 400 тыс. руб. до 2 млн. руб**

** По данным компании Group IB*

1. Современные системы дистанционного банковского обслуживания

- Платежные карты платежных международных и национальных систем
- Системы дистанционного доступа к клиентским счетам с использованием специальных каналов доступа (Банк-клиент)
- **Системы дистанционного доступа к клиентским счетам с использованием сети Интернет (Интернет-Банкинг)**
- Системы дистанционного доступа к клиентским счетам с использованием мобильной связи (мобильный банкинг)
- Системы электронных платежей через специальные небанковские платежные системы (WEB-деньги)

1.1 Функции современного Интернет-банкинга

- Рублевые внутрибанковские и межбанковские переводы;
- Осуществление предопределённых платежей (таких как оплата ЖКУ, мобильного телефона, услуг коммерческого телевидения, услуг Интернет-провайдеров и пр.)
- Валютные межбанковские переводы
- Переводы между своими счетами/картами, в том числе с конвертацией из одной валюты в другую
- Различные заявления, в т.ч. об утере/краже карты
- Создание шаблонов и расписаний платежей и переводов
- Просмотр информации о начислении по жилищно-коммунальным услугам, выставленным ГУ ИС
- Просмотр информации и получение выписки по всем открытым в Банке счетам/вкладам/картам
- Получение информации о задолженности по кредитным продуктам

И т.д.

1.1 Функции современного Интернет-банкинга

Все это можно разбить на группы риска:

- **Информационные функции**
- **Переводы по своим счетам**
- **Предопределенные переводы**
- **Переводы в пользу третьих лиц**

1.2 Штрихи о виртуальных платежных системах

В России :

2009 год – 40 млрд рублей

- **2010 год – 70 млрд. рублей**

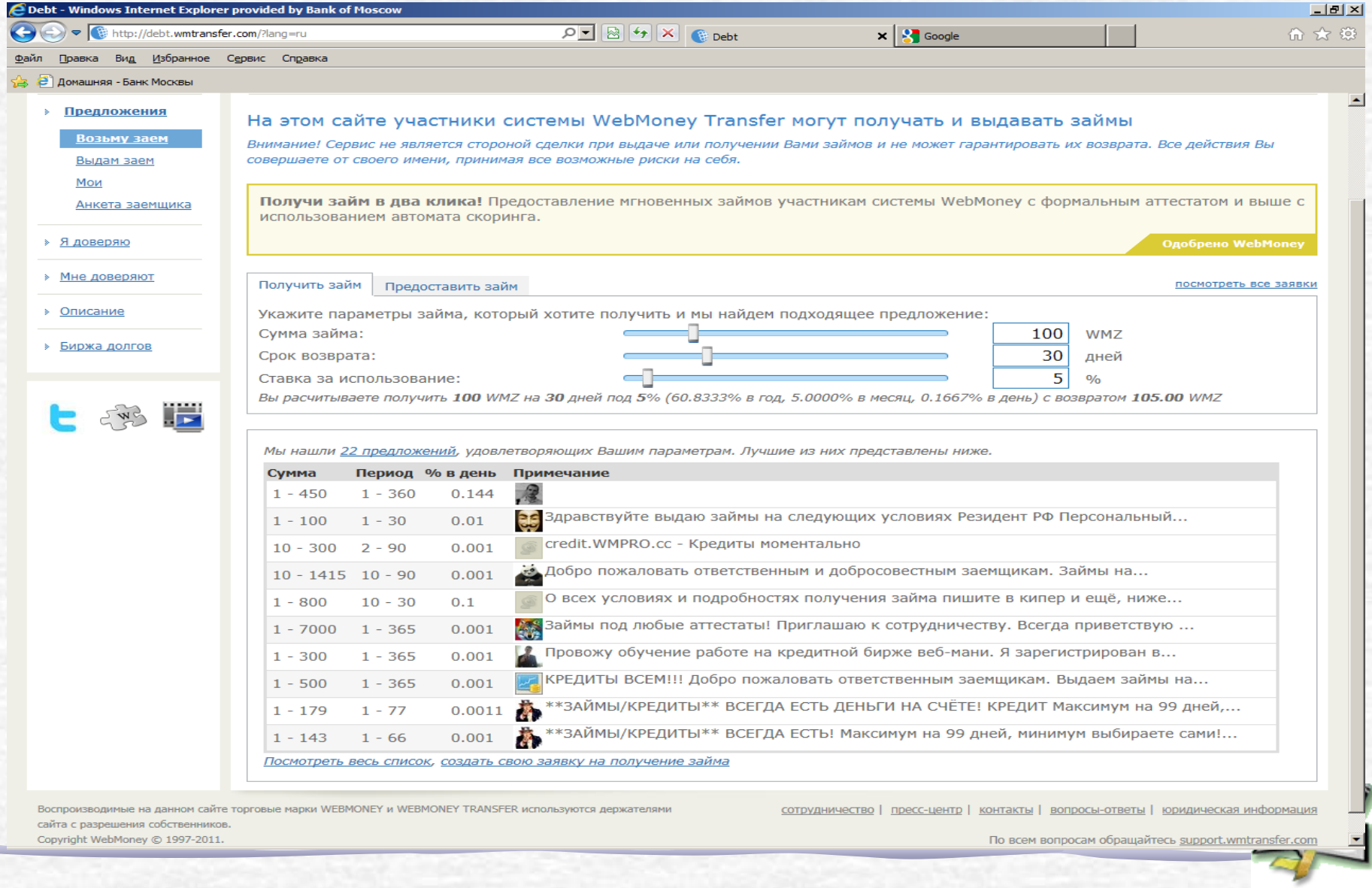
- **47% виртуальных сделок – Интернет**
- **36% виртуальный сделок – мобильные телефоны**
- **только 17% - платежные терминалы**

- **до 90% платежей + Яндекс.деньги + WebMoney**
- **Остальные - Qiwi + i-Free**

- **По планам развития этих сетей в 2011 году объем рынка должен составить более 140 млрд. рублей, а в 2012 – удвоиться по сравнению с 2011**

- **В мире – более 80 видов виртуальных валют**

1.2 Штрихи о виртуальных платежных системах



2. Организация работы Интенет-банкинга

Типовой состав участников:

- **Оборудование (серверное, пользовательское, сетевое, служебное);**
- **Каналы связи (основной, резервный);**
- **Программное обеспечение (системное, прикладное);**
- **Информация (платежная, сопутствующая);**
- **Используемые процессы, процедуры (разработка, внедрение, сопровождение);**
- **Люди (администраторы, пользователи);**
- **Помещения, используемые для работе в системах ИБК**

2. Организация работы Интенет-банкинга

Примерная схема взаимодействия

3. Модель угроз

Для примера - крупнейшая кредитная организация страны страдает от хакеров. По словам Натальи Старостиной в 2013 году мошенники через дистанционные каналы обслуживания (интернет-банк и мобильный банк) похитили со счетов клиентов более 362 млн руб. Правда, в 2012 году хакеры были более удачливыми: они опустошили счета клиентов Сбербанка, пользующихся мобильным и интернет-банкингом, на 648 млн руб.

3.1. Типы угроз Интернет-банкинга

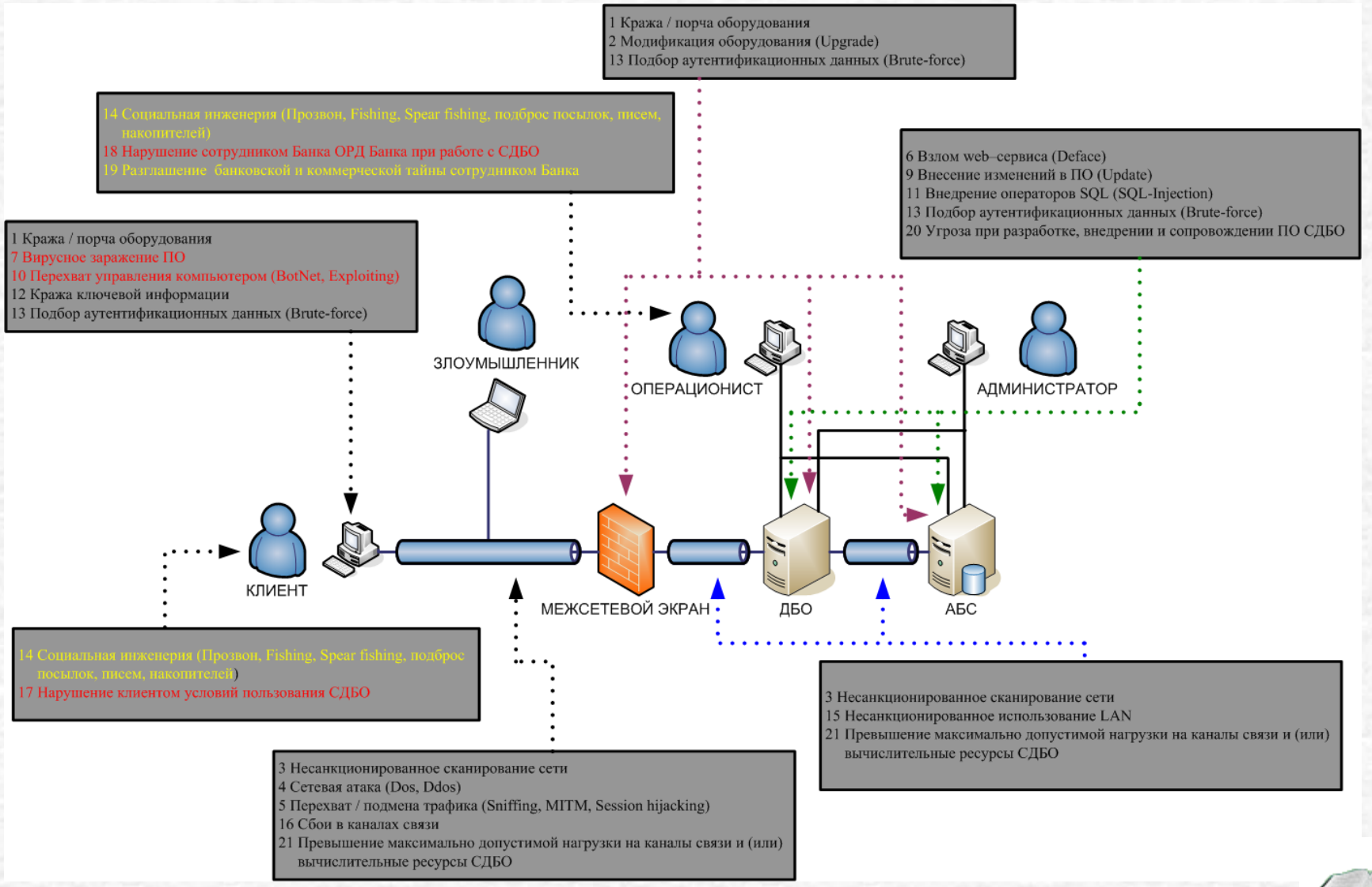
№	Наименование угрозы	Код угрозы	Актуальность угрозы	Уровень риска
1	Кража / порча оборудования	Д1	Актуальная	Риск = 4
2	Модификация оборудования (Upgrade)	Д1	Неактуальная	Риск = 2
3	Несанкционированное сканирование сети	Д2	Актуальная	Риск = 3
4	Сетевая атака (Dos, Ddos)	Д2	Актуальная	Риск = 3
5	Перехват / подмена трафика (Sniffing, MITM, Session hijacking)	Д2	Неактуальная	Риск = 2
6	Взлом web–сервиса (Deface)	Д3	Актуальная	Риск = 3
7	Вирусное заражение ПО	Д4	Актуальная	Риск = 5
8	Внедрение вирусного кода (BackDoors, LogicBomb)	Д4	Актуальная	Риск = 3
9	Внесение изменений в ПО (Update)	Д5	Актуальная	Риск = 3
10	Перехват управления компьютером (BotNet, Exploiting)	Д6	Актуальная	Риск = 5
11	Внедрение операторов SQL (SQL-Injection)	Д3	Актуальная	Риск = 4
12	Кража ключевой информации	Д7	Актуальная	Риск = 4
13	Подбор аутентификационных данных (Brute-force)	Д3	Актуальная	Риск = 4
14	Социальная инженерия (Прозвон, Fishing, Spear fishing, подброс посылок, писем, накопителей)	Д8	Актуальная	Риск = 4
15	Несанкционированное использование LAN	Д2	Актуальная	Риск = 3
16	Сбои в каналах связи	Д2	Актуальная	Риск = 4
17	Нарушение клиентом условий пользования СДБО	Д9	Актуальная	Риск = 5
18	Нарушение сотрудником Банка ОРД Банка при работе с СДБО	Д12	Актуальная	Риск = 5
19	Разглашение банковской и коммерческой тайны сотрудником Банка	Д12	Актуальная	Риск = 4
20	Угроза при разработке, внедрении и сопровождении ПО СДБО	Д10	Актуальная	Риск = 3
21	Превышение максимально допустимой нагрузки на каналы связи и (или) вычислительные ресурсы СДБО	Д11	Актуальная	Риск = 3

3.1. Источники угроз Интернет-банкинга

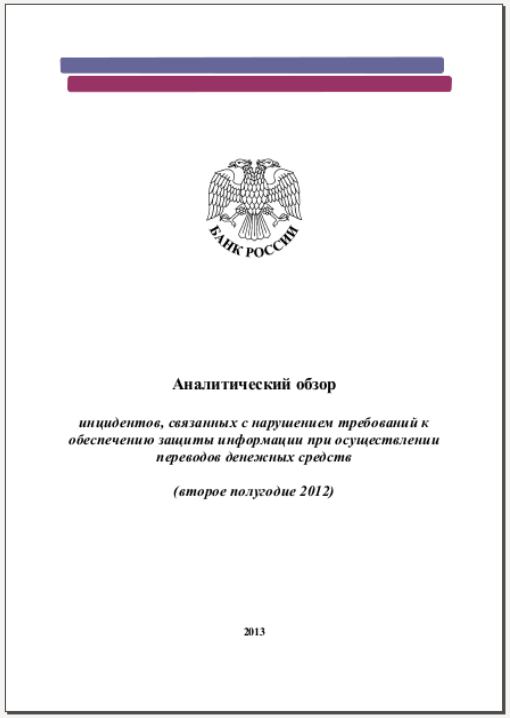
Источники угроз ИБ СДБО могут быт условно разделены на:

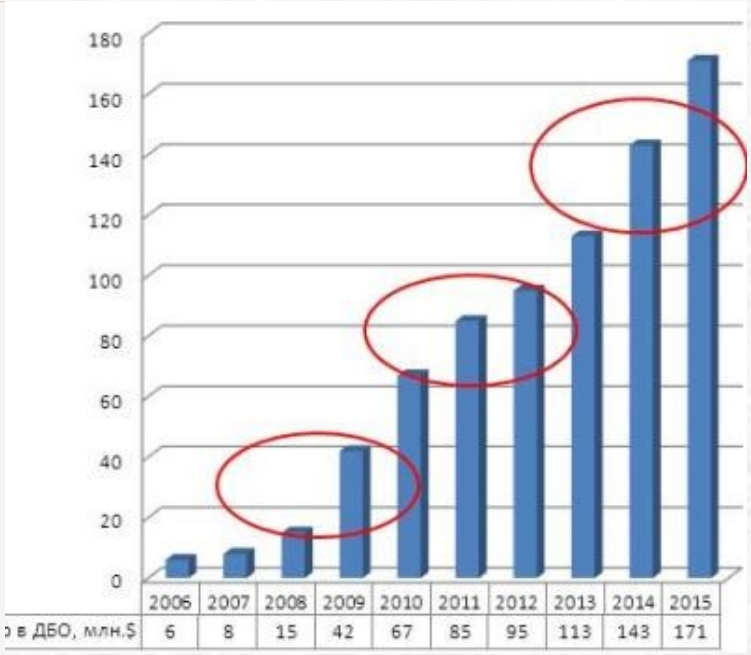
- **человеческие**, когда действия или бездействие физического лица несут прямую угрозу нанесения ущерба СДБО. Человеческие угрозы исходят от внешних и(или) внутренних нарушителей ИБ и подразделяются на:
  - преднамеренные (например, компьютерные атаки, взломы, несанкционированная модификация электронной информации и т.п.);
  - непреднамеренные (например, ошибки при проектировании и разработке ПО, ошибки при эксплуатации компьютерных (информационных) систем);
- **технические**, возникающие в результате самопроизвольного выхода из строя того или иного электронного оборудования. К ним относятся технические сбои и отказы оборудования СДБО (например, выход из строя серверов или компьютеров, каналов связи по причине заводского брака оборудования, несовместимости версий ПО и т.п.);
- **непредвиденные обстоятельства** (например, стихийные бедствия, аварии, пожары, наводнения, землетрясения, ураганы, массовые беспорядки и т.п.).

3.1. Распределение угроз Интернет-банкинга



3.2 Анализ модели угроз





Один инцидент на 250 тысяч платежей.
90% операторов не выявляют инцидентов.
8% операторов выявляют менее 10 инцидентов в месяц.
2% операторов выявляют более 10 инцидентов в месяц.
Средняя сумма одного инцидента может быть оценена в 250 т.руб.

Удельная величина риска в системах ДБО составляет 0.001 коп./руб.

3.2 Анализ классов угроз

4. Краткая историческая справка по способам мошенничеств в ДБО

4.1 Незаконный товар или услуга на "черном" рынке

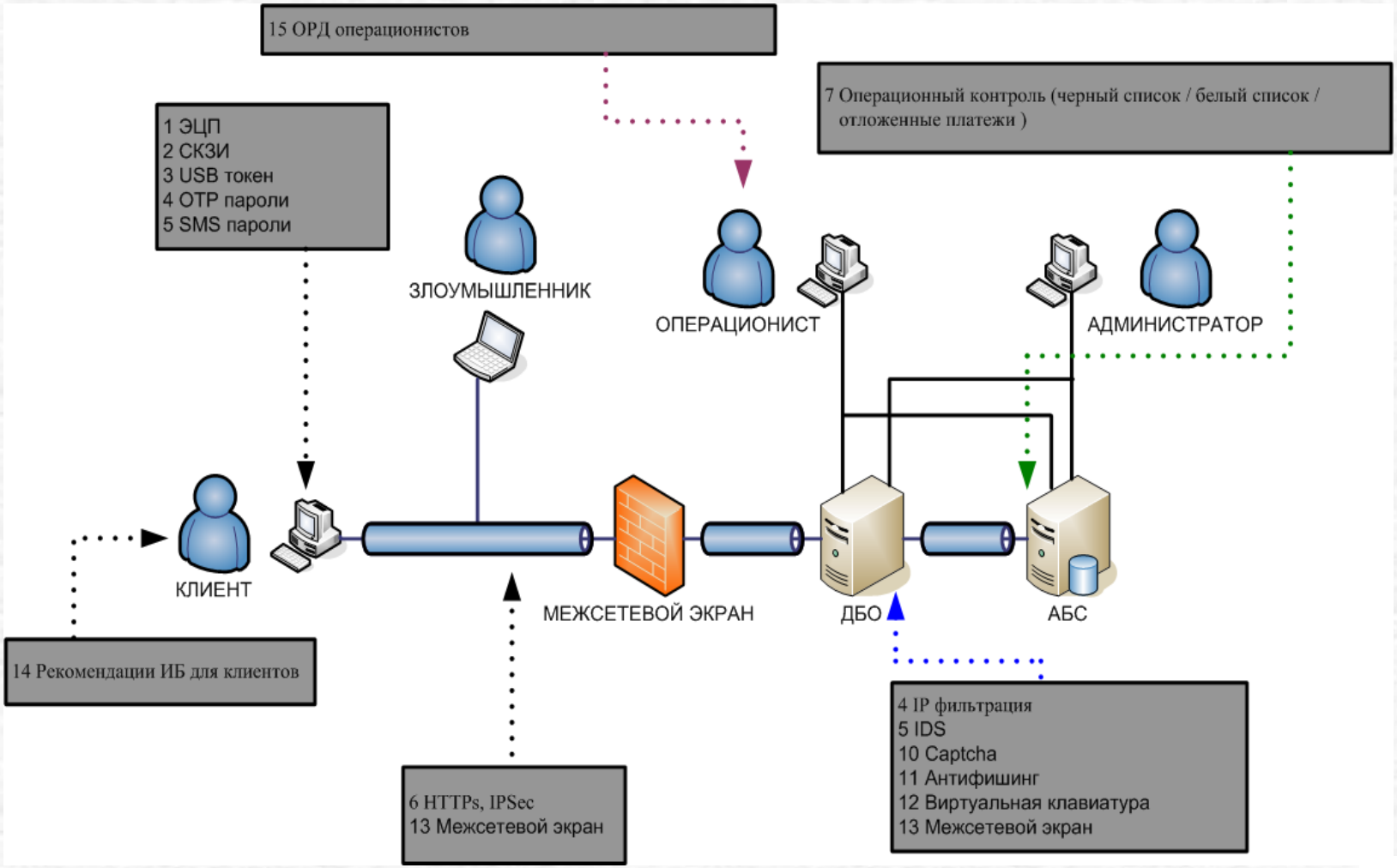
**по данным исследования состояния кибермошенничества в 2010 году "PandaLabs"*

• Данные кредитной карты	От $2-$90
• Поддельные кредитные карты	От $190 плюс стоимость данных счета
• Кард-клонеры (устройства, дающие возможность скопировать данные платежных карт)	От $200-$1000
• Поддельные банкоматы	До $35 000
• Подложные реквизиты и сертификаты Банка	От $80 до $700
• Платформы для онлайн-магазина и платежной системы	От $80 - до $1500
• Спамерские услуги	От $15
• Аренда SMTP	От $20 до $40
• Аренда VPN	$20 за 3 месяца

5. Краткая история механизмов защиты в ДБО

- Логин
- Долговременный пароль
- Одноразовый пароль (OTP-token, SMS, скретч-карты и т.д.)
- ЭЦП (на файловом носителе или на криптопровайдере)
- Виртуальная клавиатура
- Технология "каптча"
- Пользовательский индивидуальный интерфейс
- SMS – информирование
- Штатные средства WEB
- Антивирусные средства
- Системы on-line мониторинга и анализа транзакций

5. Краткая история механизмов защиты в ДБО. Итоги



6. Источники и составные части причин Интернет – мошенничества.

6.1 Субъективные причины

- Недостаточная осведомленность клиентов об опасности использования Интернет - среды для финансовых операциях
- Недостаточное внимание клиентов к обеспечению собственной безопасности в Интернете

6. Источники и составные части причин Интернет – мошенничества.

6.2 Объективные причины

Технические:

- Использование нелицензионного программного обеспечения
- Использование неадекватных уровней безопасности в системах ДБО
- Технологические ошибки в разработке систем ДБО
- Использование в системах ДБО не сертифицированных СКЗИ
- Широкая доступность в Интернете мошеннических услуг и программного инструментария для совершения компьютерных преступлений
- Отсутствие доверенной среды для работы систем ДБО

6. Источники и составные части причин Интернет – мошенничества.

6.2 Объективные причины

Организационные

- Сложности взаимодействия кредитных организаций в части, касающейся обмена информацией о мошенниках и о мошеннических платежах
- Отсутствие единого центра сбора, анализа и распространения информации о мошеннических действиях в ДБО, а также единой государственной системы противодействия таким действиям
- Затрудненность взаимодействия кредитных организаций в случае совершения мошеннических платежей из-за неучета установленными Центральным Банком правилами специфики таких платежей (возникают сложности с отзывом платежей, с блокировкой счетов мошенников и т.п.)

6. Источники и составные части причин Интернет – мошенничества.

6.2 Объективные причины

Правовые

- Несовершенство уголовного права в части, касающейся компьютерных преступлений, в частности, касающихся совершения мошеннических операций в ДБО,
- Несовершенство уголовно-процессуального права, отсутствие единых и утвержденных методик у правоохранительных органов по расследованию компьютерных преступлений в сфере ДБО,
- Отсутствие действующих международных соглашений и законодательства по противодействию мошенничеству в ДБО.
- Наличие элемента формализма, движение по пути наименьшего сопротивления при рассмотрении дел, связанных с мошенничествами в ДБО как правоохранительными органами, так и судами, что приводит либо к зацикливанию процесса (например, дело в принципе не возбуждается из-за разной трактовки понятия места совершения преступления и постоянной пересылки материалов заявления между разными территориями), либо к замещению целей – вместо поиска мошенников внимание концентрируется либо на клиенте, либо на банке. При этом задача наказания истинных виновных отходит на второй план.

6. Источники и составные части причин Интернет – мошенничества.

6.2 Объективные причины

Правовые (пример)

- местом преступления в таких преступлениях принимается место обналичивания (согласно Постановлению Пленума Верховного Суда РФ от 27.12.2007 № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате»).

6. Источники и составные части причин Интернет – мошенничества.

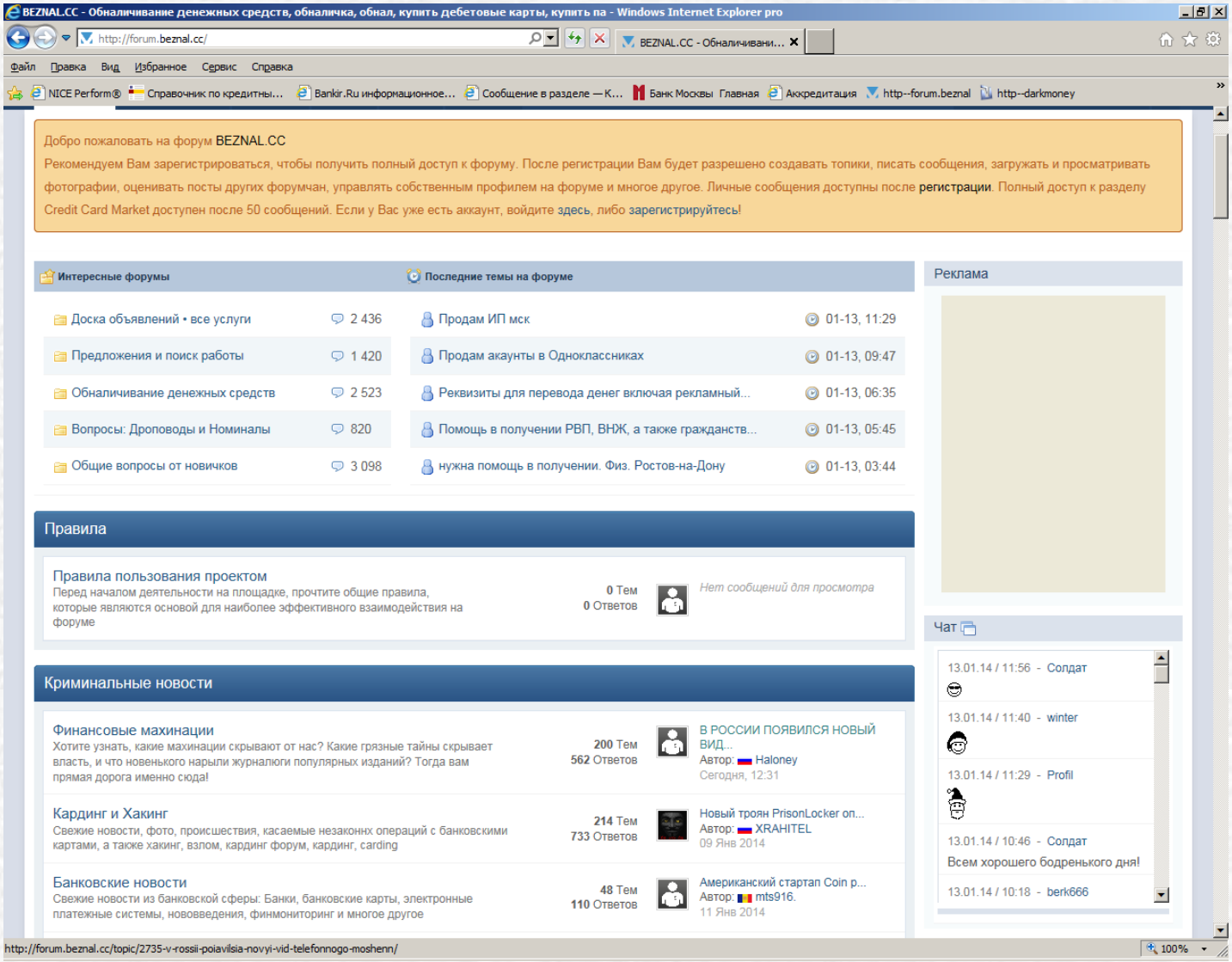
6.2 Объективные причины

Кадровые

Недостаточная кадровая обеспеченность правоохранительных органов сотрудниками, способными проводить экспертизу и расследовать компьютерные преступления в сфере ДБО

7.1 Особенности наиболее распространенных схем

7.1 Особенности наиболее распространенных схем



7.1 Особенности наиболее распространенных схем

7. Особенности наиболее распространенных схем

7.1 Организация работы ОПГ

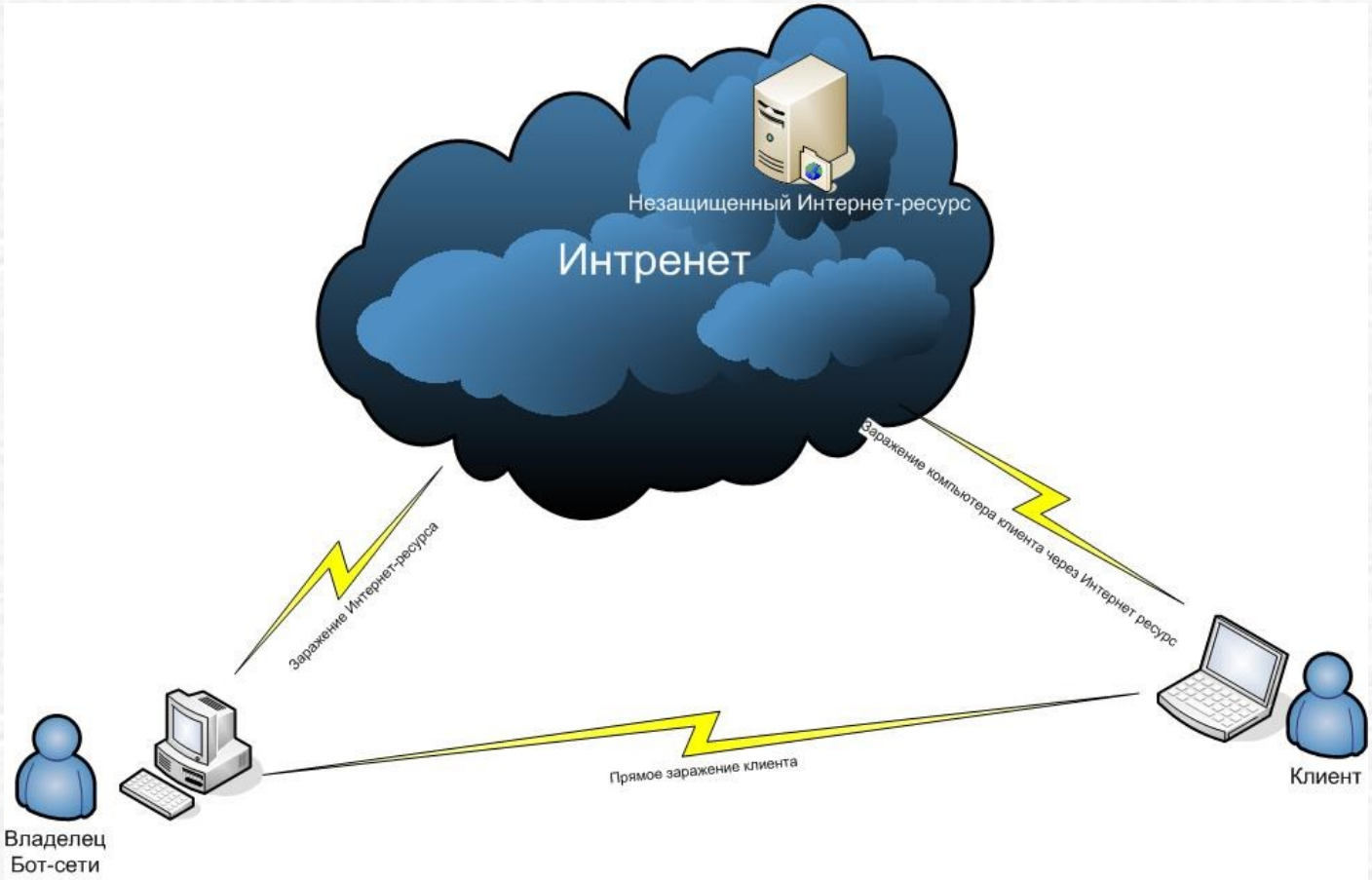
- **Мошеннические действия производятся организованными группами, распределёнными по регионам и ролям.**
- **Хищения тщательно подготавливаются технически: создаются средства для кражи данных, фишинговые сайты, bot-сети, программы для организации DDoS-атак, планирование и координация действий участников.**
- **Меняется "инструментарий" злоумышленников, растет доля технических сложных способов взлома, таких, как перехват управления.**
- **Вывод средств производится, как правило, сразу после хищения; чтобы замедлить обнаружение организовывают DDoS-атаку на Web-сайт банка или клиента.**
- **Для вывода похищенных средств используются банковские карты, системы «электронных денег», системы расчётов через Интернет, фиктивные компании с «зарплатными схемами» и т.п.**
- **После хищения «заметаются следы» - выводится из строя компьютер и т.п.**
- **Хищения происходят чаще всего в регионах (где вопросам безопасности уделяется меньше внимания), вывод средств – в Москве**

7.2 Этапы «операции» по атаке на системы ДБО

1	Разработка комплекса троянских программ	Организатор, программисты	При анализе образа диска определение автора по характерным признакам написания программ
2	Создание БОТ-сети	Владелец Бот-сети, программисты	При использовании большинства антивирусных программ определение факта заражения компьютера и с использованием специального ПО выявление адресов потенциальтного центра управления БОТ-сетью
3	Подготовка "Дропов"	Покупатель посредников, Дроповод, Дропы	Только оперативные мероприятия
4	Подготовка мошеннической операции покупка/аренда хостинга – внешних серверов, через которые будут организовываться атаки, где будут храниться промежуточные данные, украденные у клиентов	Организатор: закупка дропов, заказ заливщикам, подготовка центров управления	Только оперативные мероприятия
5	Заражение компьютера клиента специализированным трояном,	Заливщик	Возможно выявление факта заливки и адреса центра управления заливки только при использовании специализированного ПО
6	Обналичивание денежных средств	Посредник , дропы	Возможно выявление и задержание дропов и попытка установление посредника или организатора
7	Зачистка следов операции	Организатор	

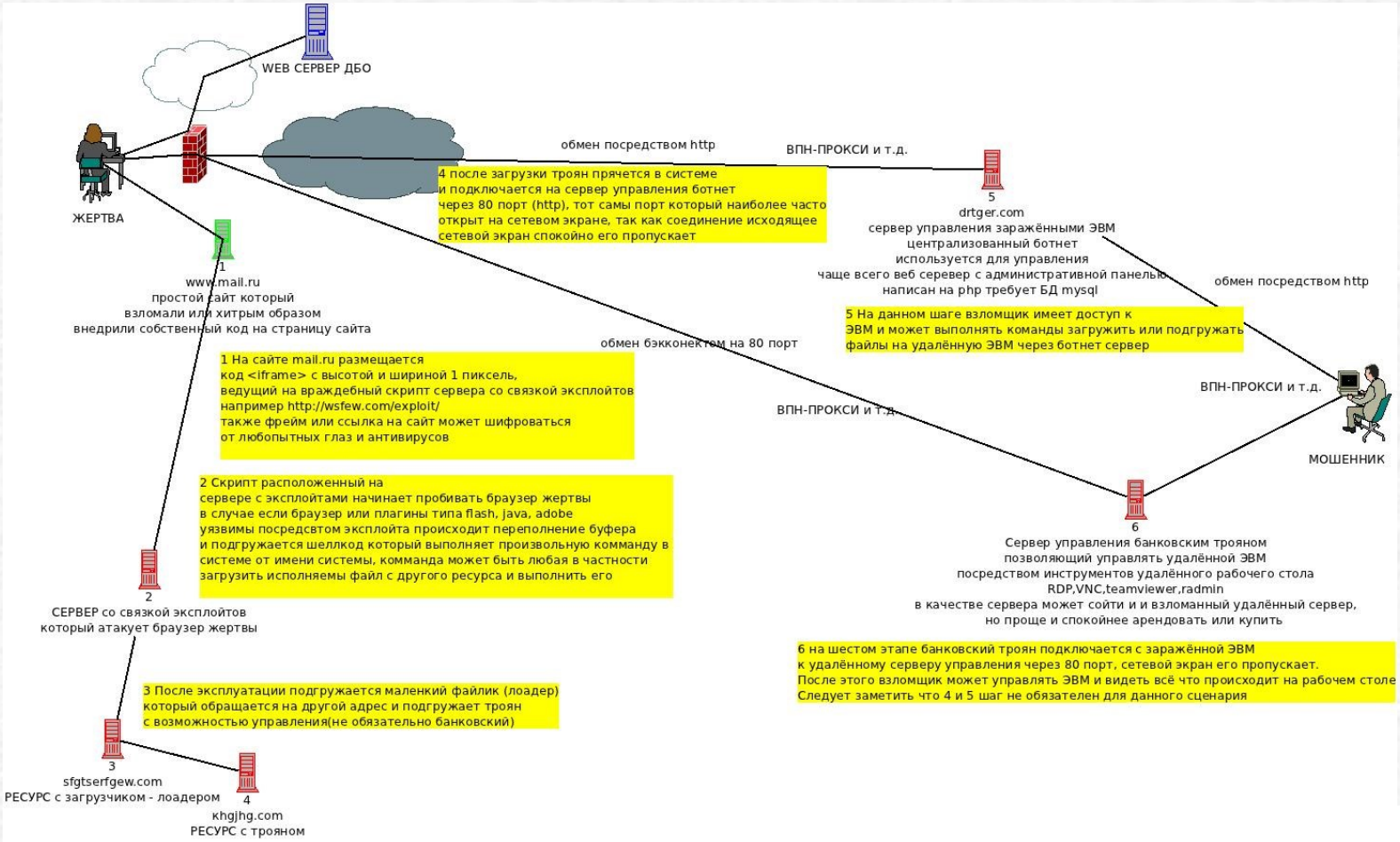
7. Особенности наиболее распространенных схем

7.2.1 Заражение клиента. Создание бот-сети



7. Особенности наиболее распространенных схем

7.2.2 Заражение клиента. Проведение операции



7. Особенности наиболее распространенных схем

7.3 Некоторые особенности троянов

Trojan-Spy.Win32.Lurk - Самая агрессивная и профессиональная группа, работает с т.н. «фантомными троянами», наиболее трудно идентифицируемыми, как правило автоматизированное формирование ПП на большие суммы, ориентирован на большую «десятку», в основном СБ и БМ

Carberg – так же профессиональная группа, но работает в полуавтоматизированном режиме, требует предварительного «ручного» анализа клиента, имеет наиболее универсальный механизм работы с системами ДБО – БИФИТ, BSS, R-Style и т.д.

Trojan.Win32.Antavmu.omf - низкопрофессиональный «продукт», требует практически непосредственного доступа RDP к клиенту, зато работает со всеми видами ДБО

8. Стратегия безопасности

- **Ни одна из технических мер в отдельности не обеспечивает достаточной защиты**
- **Ни одно из решений не является «быстрым» и «бесплатным»**
- **Слепая вера в технические средства – тоже источник угрозы!**
- **Подавляющее большинство клиентов не придаёт безопасности электронных платежей должной важности**
- **Любые дополнительные меры безопасности в силу своей природы неизбежно приводят к усложнению процесса работы с системой и удорожанию услуги**

- Придётся преодолевать недовольство клиентов
- Необходима большая разъяснительная работа

- Нужен баланс рисков и сложности / стоимости решений
- Клиент должен иметь возможность сам регулировать свои риски
- **Предупреждён – значит вооружён!**

- Совершенств. законов
- Взаимодействие с МВД

Необходим комплекс технических решений:

- общесистемные меры у клиентов;
- защищённые ключевые носители;
- дополнительная аутентификация и/или авторизация;
- средства Fraud-анализа в банке;
- система оповещения клиентов (SMS, e-mail)

Отказ от использования какого-либо компонента комплекса существенно повышает риски банка и клиентов

Основная цель всех мероприятий: себестоимость мошеннических операций (с учётом рисков) не должна окупаться. Мошенничество должно стать невыгодным!

8. Стратегия безопасности

Направление	Задачи
Увеличение трудозатрат совершение хищения	• Использование комплекса технических средств защиты на всех уязвимых направлениях • Повышение контроля за средствами защиты через обучение пользователей • Повышение ответственности клиентов за использование средств защиты • Большая защита для рискованных операций и операций на крупные суммы
Снижение ожидаемого дохода злоумышленника	• Снижения вероятности вывода похищенных средств за счет раннего обнаружения атаки и блокирования мошеннической транзакции
Увеличение риска злоумышленника	• Увеличение вероятности поимки злоумышленника при подготовке или проведении хищения или при выводе похищенных средств • Увеличение вероятности привлечения злоумышленника и тяжести наказания

- Использование комплекса технических средств защиты
- Информирование, подготовка и "дисциплинирование" клиентов
- Применение дифференцированных режимов защиты
- **Внедрения механизмов раннего обнаружения атак**
- Создание коллективной системы оперативного реагирования и блокирования мошеннических транзакций
- Развитие и эффективное использование юридических инструментов защиты

8. Стратегия безопасности

1. Определение политики безопасности СДБО

2. Организационные мероприятия

3. Технические мероприятия

4. Повышение осведомленности клиентов СДБО о мерах безопасности

8.1 Определение Политики безопасности

1. Разработка комплекса нормативных документов – модели угроз, оценка текущего состояния, методика оценки рисков, планы защиты
2. Разработка политик страхования и взаимодействия с клиентами в случаях возникновения инцидентов
3. Разработка требований к банковскому контуру СДБО и организация контроля их выполнения
4. Разработка и использование различных стратегий мониторинга транзакций

8.1 Определение Политики безопасности

Требования, которые д.б. учтены при разработке Политики:

- Аутентификация клиентов в операциях электронного банкинга
- Отсутствие отказов от проведения операций и возможность учета для транзакций, осуществляемых в рамках электронного банкинга
- Должные меры по обеспечению управления правами доступа
- Необходимые средства авторизации в системах электронного банкинга, базах данных и прикладных программах
- Целостность данных в транзакциях электронного банкинга, записях и информации
- Организация формирования точных аудиторских записей для транзакций, осуществляемых в рамках электронного банкинга
- Конфиденциальность важнейшей банковской информации

8.2 Организационные мероприятия

1. Формирование рабочей группы развития бизнеса ДБО в составе представителей бизнеса, IT, ИБ, рисков.
2. Разработка плана развития бизнеса ДБО с учетом оценки рисков
3. Установление видов контролей за реализацией плана, правил пересмотра, в том числе показателей оценки рисков
4. Разработка нормативных документов по реагированию на различные инциденты по нарушению безопасности

8.3 Технические мероприятия

1. Внедрение промышленных методов разработки программного обеспечения
2. Создание надежного периметра банковского контура систем ДБО
3. Внедрение систем IPS/IDS, систем активной защиты от DdoS-атак
4. Использование современных и сертифицированных механизмов защиты, обеспечивающих заданный Политикой уровень доступности, целостности, конфиденциальности и неотказуемости, создание дополнительных каналов управления и информирования

8.3 Технические мероприятия

5. Разработка и внедрение систем сбора и анализа информации об инцидентах в системах ДБО
6. Внедрение систем мониторинга и анализа транзакций на основе профилей клиентов, которые могут включать :
   - Среднее/максимальное число операций в день
   - Среднее/максимальное число операций в месяц
   - Средняя/максимальная операционная сумма
   - Среднее/максимальное число информационных запросов
   - Основные типы платежей
   - основные корреспонденты
   - Среднее/максимальное число сделок на одном самом счете и т.д.

8.3 Технические мероприятия

При разработке программных средств систем ДБО необходимо:

•*изучать* способы и практические примеры противоправной деятельности с помощью банковских информационных технологий
•создавать и *адаптировать* модели возможной противоправной деятельности с использованием банковских информационных технологий
• *тестировать* программно-информационное обеспечение финансового мониторинга на предмет его адекватности указанным моделям
•*актуализировать* и обновлять программно-информационное обеспечение финансового мониторинга

8.4. Традиционные меры безопасности

1. Разработка и внедрение алгоритмов он-лайн анализа проведенных транзакций
2. Использование чиповых карточных продуктов, использование «электронных кошельков» или «виртуальных» карт для интернет- платежей
3. Использование традиционных активных и пассивных механизмов безопасности ИБК
4. Разработка специальных инструкций службам ДБО по действиям в чрезвычайных обстоятельствах проведение тренингов
5. Повышение осознания клиентами необходимости соблюдения безопасности, в т.ч. повышение осведомленности клиентов через интернет-сервисы о мерах безопасности, настоятельная рекомендация клиентам, работающим в системах ДБО, применять антивирусное программное обеспечение с функциями анти-хакер и анти-шпион
6. Организация оперативного взаимодействия с правоохранительными органами

9. Примеры отдельных технических решений

Два направления повышения безопасности ДБО

Компенсация недостаточного уровня защищенности рабочих мест клиентов

Техническая защита Рабочих мест клиентов

Контроль и подтверждение транзакций

9.1 Техническая защита Рабочих мест клиентов

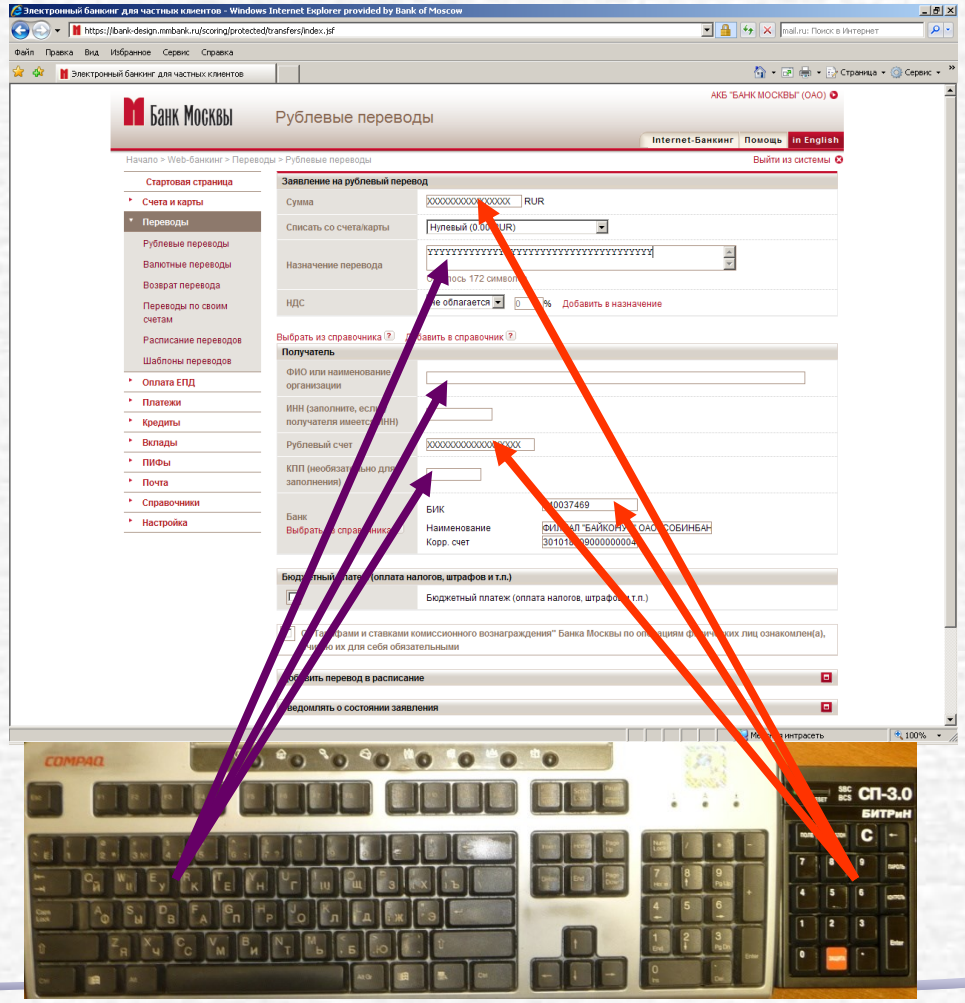
1. Создание дополнительных технических устройств ввода ключевых данных в доверенной среде
2. Создание временной доверенной среды на штатном компьютере с использованием различных методик «доверенной загрузки» операционной системы и среды исполнения
3. Создание специализированных банковских терминалов на базе мобильных компьютеров

9.1.1 Пример доверенного устройства ввода ключевых полей

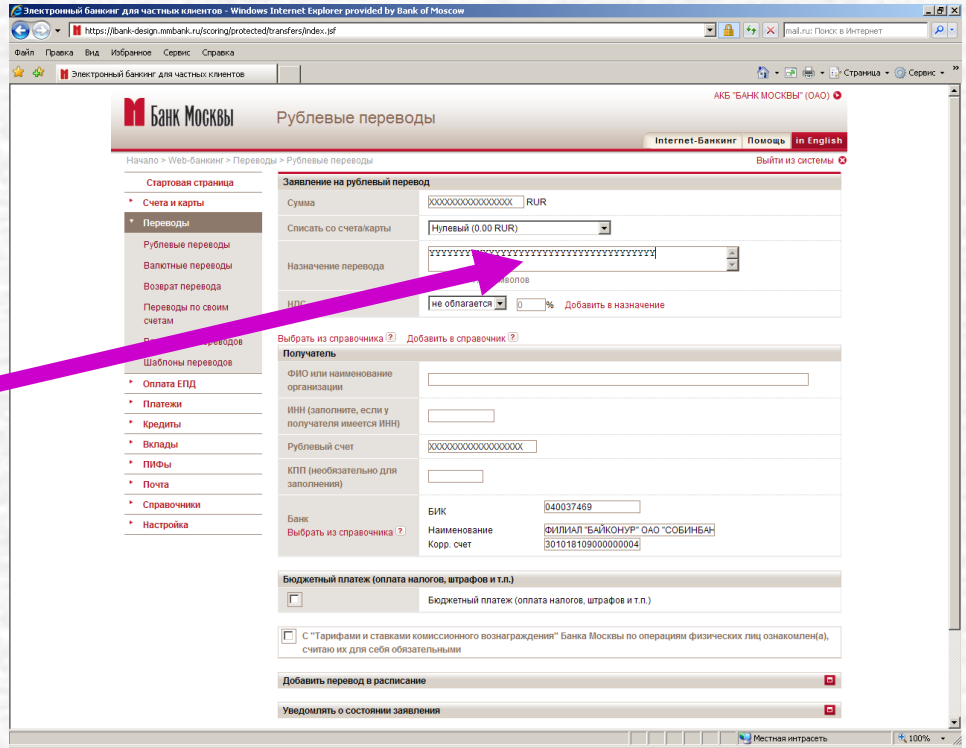
- Подключается к USB-порту
- Драйверов не требует
- Данные ключевых полей вводятся с клавиатуры «ИЗДЕЛИЯ»

9.1.2. Пример доверенного устройства

Пример доверенного устройства ввода ключевых полей



9.1.2. Пример доверенного устройства ввода ключевых полей



Вычисление контрольного параметра и его запись в текстовое поле

9.1.2. Пример доверенного устройства ввода ключевых полей

PAYER_NAME= ООО «XXXXXXXXXX»
PAYER_ACCOUNT=40702810200350000284
AMOUNT=395000.00
PAYER_BANK_NAME=ОАО "БАНК ", г.МОСКВА
PAYER_BANK_BIC=044525219
PAYER_BANK_ACC=30101810500000000219
RCPT_INN=778903218217
RCPT_NAME=Иванов Иван Иванович
RCPT_ACCOUNT=40817810308430008345
RCPT_BANK_NAME=ОАО "А-БАНК", г.МОСКВА
RCPT_BANK_BIC=044525593
RCPT_BANK_ACC=30101810200000000593
TYPE_OPER=01
QUEUE=6
PAYMENT_DETAILS= **«1234567890ABCDEF0987654321FEDCBA»**
Заработная плата за сентябрь 2010г, все налоги удержаны и в бюджет перечислены.
Сумма 395000-00 НДС не облагается.
[content end] Клиент: ООО «XXXXXXXXXX»
10-09-30 15:52:52,153 INFO : 95.31.7.246 - 12831592027442888893:Обработка события 'Смена статуса документа' для документа 'doc/payment' для клиента '234176'. Клиент: ООО «XXXXXXXXXX»
10-09-30 15:52:52,167 INFO : 95.31.7.246 - 12831592027442888893:Подпись документа, ***[новый статус=2]***. Клиент: ООО «XXXXXXXXXX»

Ключевые поля

Контрольный параметр

9.1.2. Пример доверенного устройства ввода ключевых полей

Существенно снизить риски, уменьшить требования к защите компьютера и ее стоимости можно, используя специализированное устройство **SafeTouch**, подключаемое к компьютеру через порт USB. Это устройство является считывателем смарт-карты (карт-ридером) с функцией визуализации значимых полей в подписываемом документе

9.2 Контроль и подтверждение транзакций

1. Создание специализированных систем он-лайн анализа транзакций на основе т.н. «профилей клиента»

2. Создание дополнительных, не зависимых от компьютера клиента, каналов и механизмов подтверждения клиентом платежа, принятого банком (сравнение того, что отправлял/не отправлял клиент, с тем, что получил Банк)

9.2.1. «Домашний» фрод-мониторинг

- Контролировать IP-адреса и изменения параметров компьютеров клиента
- Контролировать «черные» и «белые» списки по номерам счетов корреспондентов
- Контролировать пороговые значения сумм платежа
- Контролировать значимые параметры (ИНН, КПП, назначение, сумму и т.д.)
- Контролировать «новизну» параметров платежа

ЭТО ДАЕТ 80%-ВЕРОЯТНОСТЬ ВЫЯВЛЕНИЯ ФРОДА

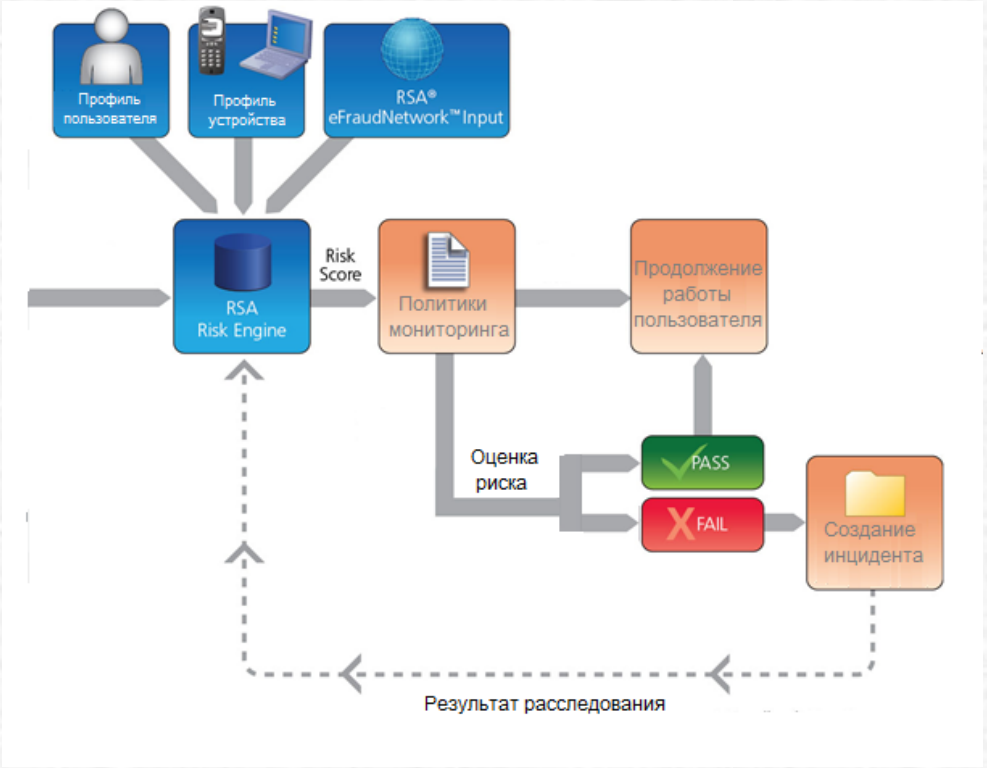
Недостатки:

- При большом числе (более 10 тыс платежей в день) очень велико число платежей, попадающих под дополнительный «ручной» контроль
- Велика доля «человеческого фактора» (ошибки) при ручном исполнении большого объема контрольных функций
- При полуручной обработке невозможно быстро и эффективно применять «тонкую» аналитику по «профилю клиента»
- В ручном режиме сложно проводить корреляционные оценки в он-лайн режимах контроля

9.2.1. Вариант промышленной системы мониторинга. Принцип функционирования

Этапы анализа в решении RSA:

- Получение событий от внешнего источника.
- Обработка модулем Risk Engine с учетом:
  - Профиля пользователя;
  - Профиля устройства;
  - Данных единого центра борьбы с мошенничеством.
- Формирование оценки риска.
- Анализ события правилами, создаваемыми в системе:
  - Использование лимитов;
  - Использование черных и белых списков;
  - Других типов правил.



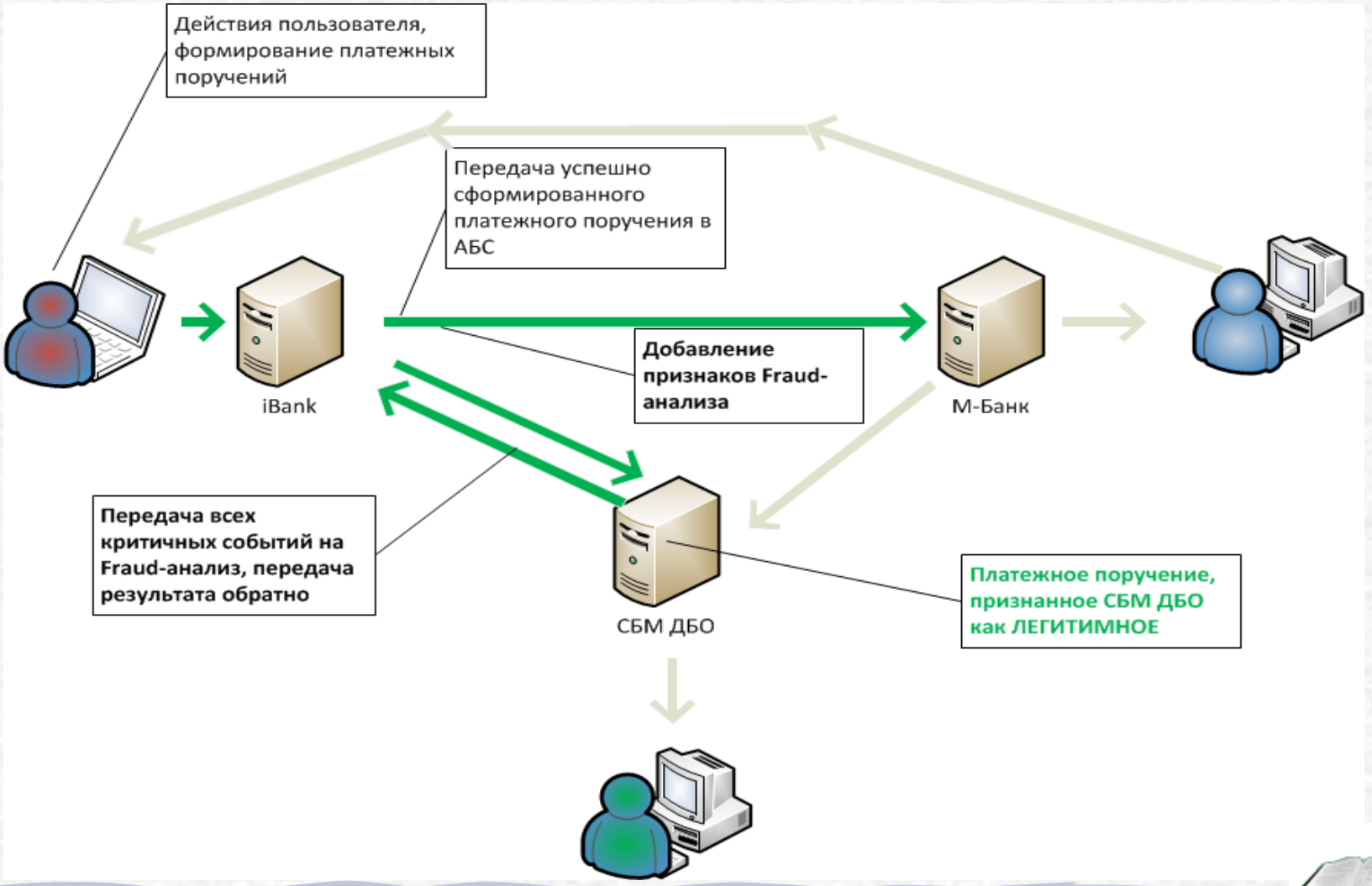
- Категорирование оценки риска и принятие решения о разрешении, приостановлении или блокировке операции.
- Создание инцидента по подозрительной или заблокированной операции.
- Передача результата расследования инцидента в самообучаемую модель.

9.2.1. Вариант промышленной системы. Принцип функционирования

Типовая схема «домашней системы»

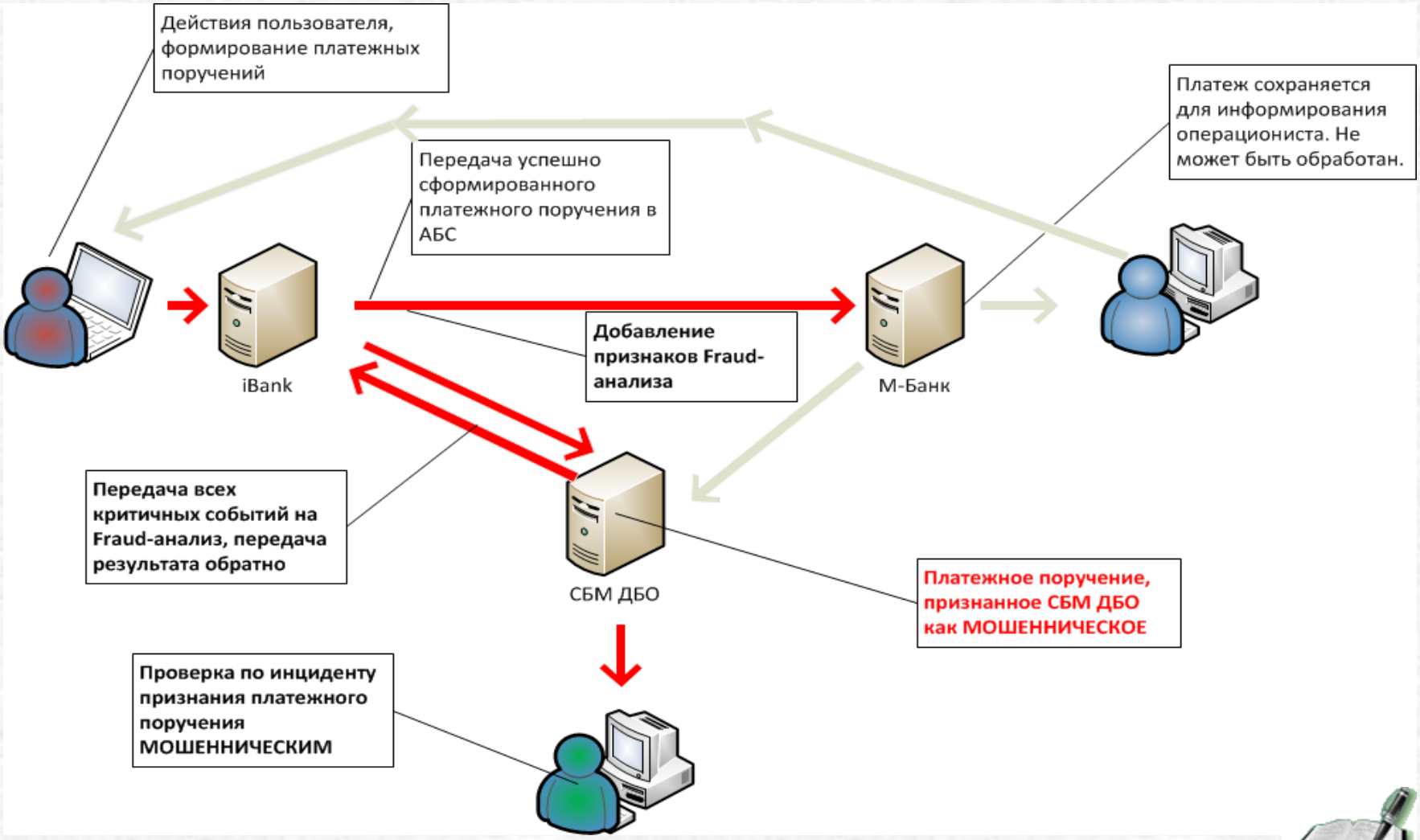
9.2.1. Вариант промышленной системы. Принцип функционирования

Легитимный платеж



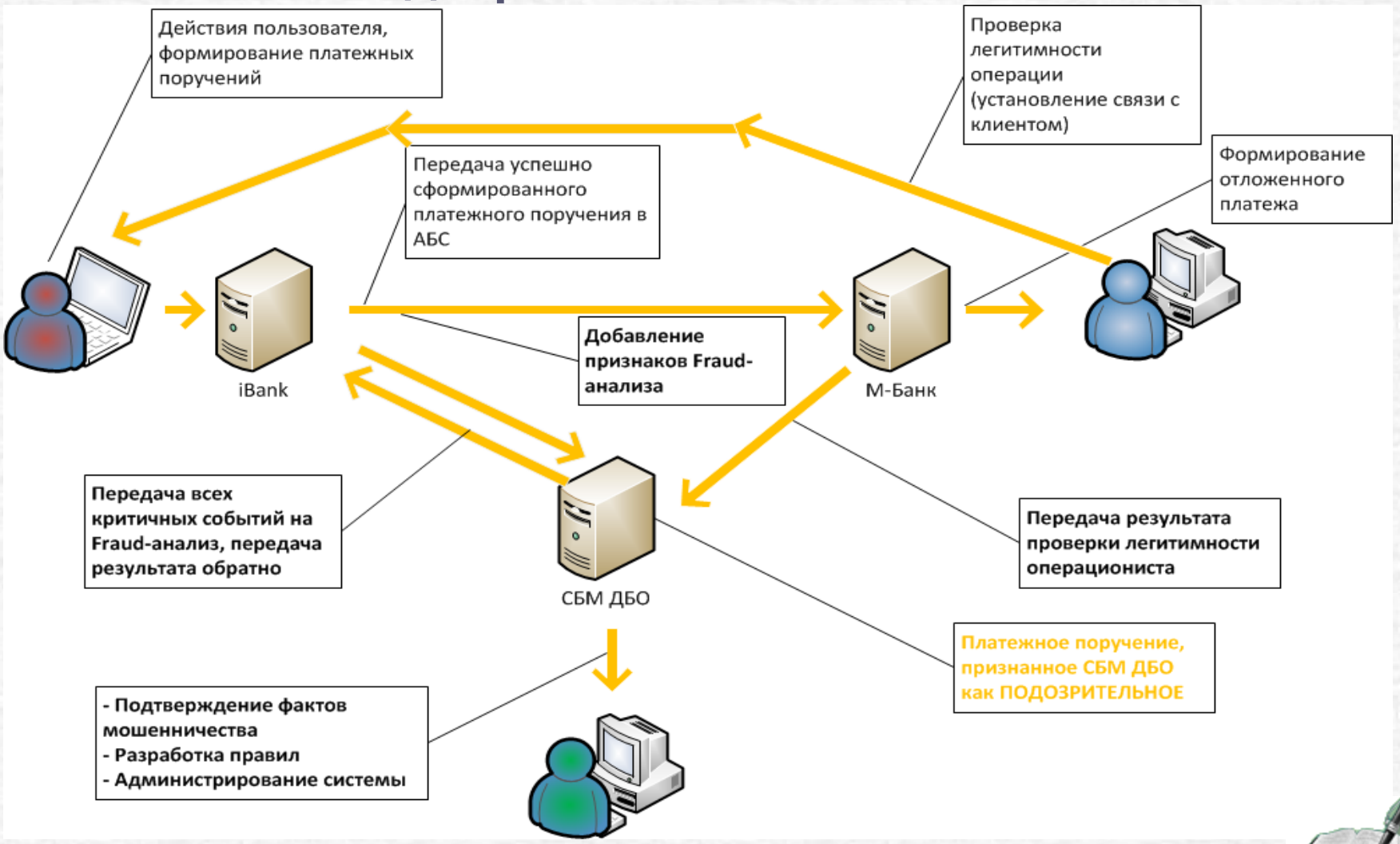
9.2.1. Вариант промышленной системы. Принцип функционирования

Мошеннический платеж



9.2.1. Вариант промышленной системы. Принцип функционирования

Подозрительный платеж



9.2.2. Независимые каналы подтверждения платежей

Одноразовый пароль
OTP One-Time-Password

OTP, независимый от контента

Временно – зависимый

Ивентно – зависимый

OTP, связанный с контентом

Hash

Содержащий текст

СПАСИБО !

Какие будут вопросы?

Контакты:

Окулесский Василий Андреевич, к.т.н.

Тел. (495) 925-8000 доб. 114-58
E-mail: Okulessky_VA@bm.ru