Практический опыт построения системы защиты СДБО от мошенничества

Окулесский Василий Андреевич,
кандидат технических наук

Урал, 2015

Вместо вступления

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.

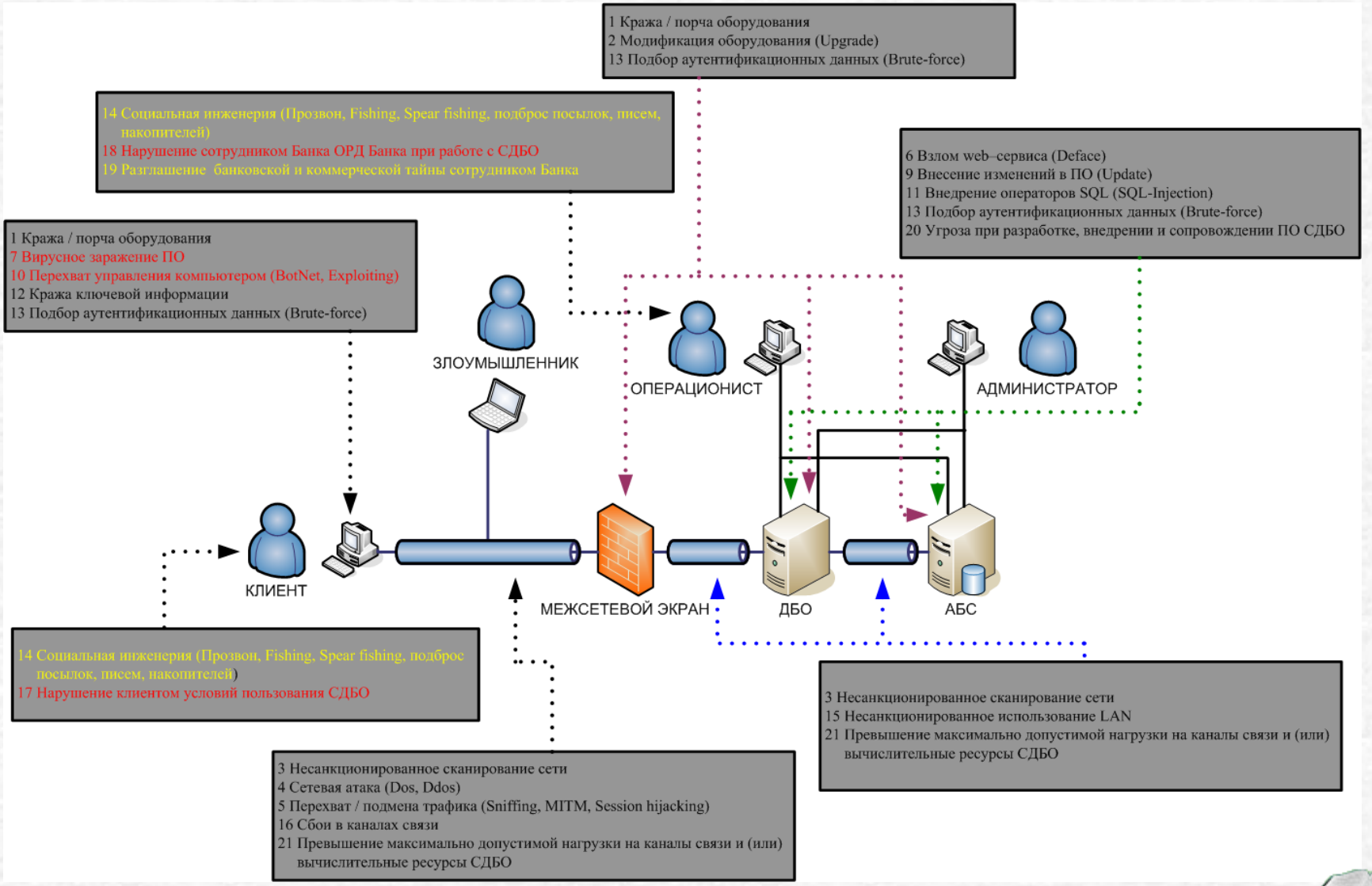
"Согласно оценкам экспертов, каждую секунду жертвами киберпреступности в мире становятся 12 человек, и это количество с каждым годом растет. Основной мотив киберпреступников - привлечение материальной выгоды. Количество преступлений, совершаемых из хулиганских и иных побуждений, крайне незначительно", - 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

Источники угроз Интернет-банкинга

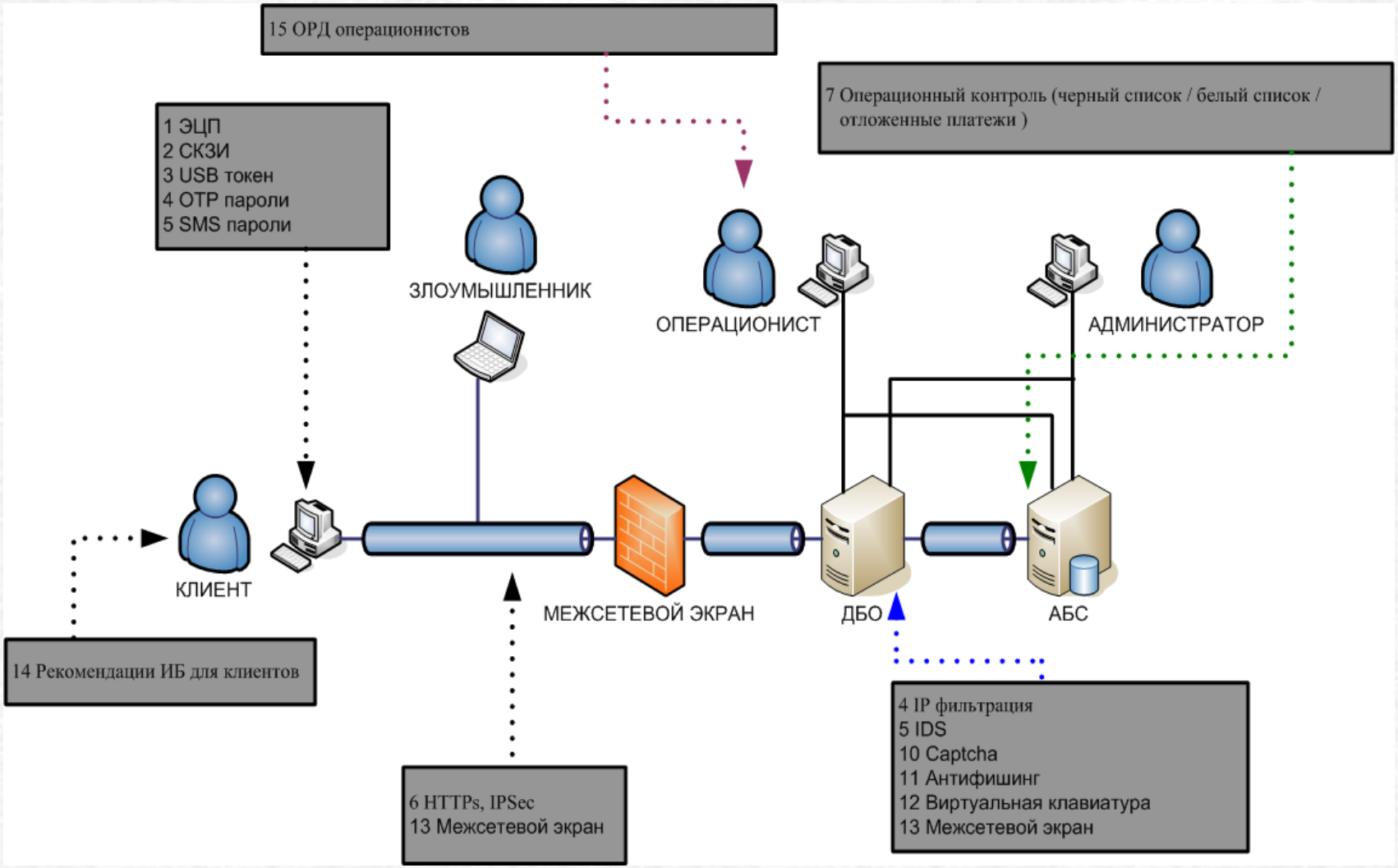
Источники угроз ИБ СДБО могут быт условно разделены на:

- **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.).

Распределение угроз Интернет-банкинга



Типовые механизмы защиты в СДБО



На «той» стороне

Как «там» организовано

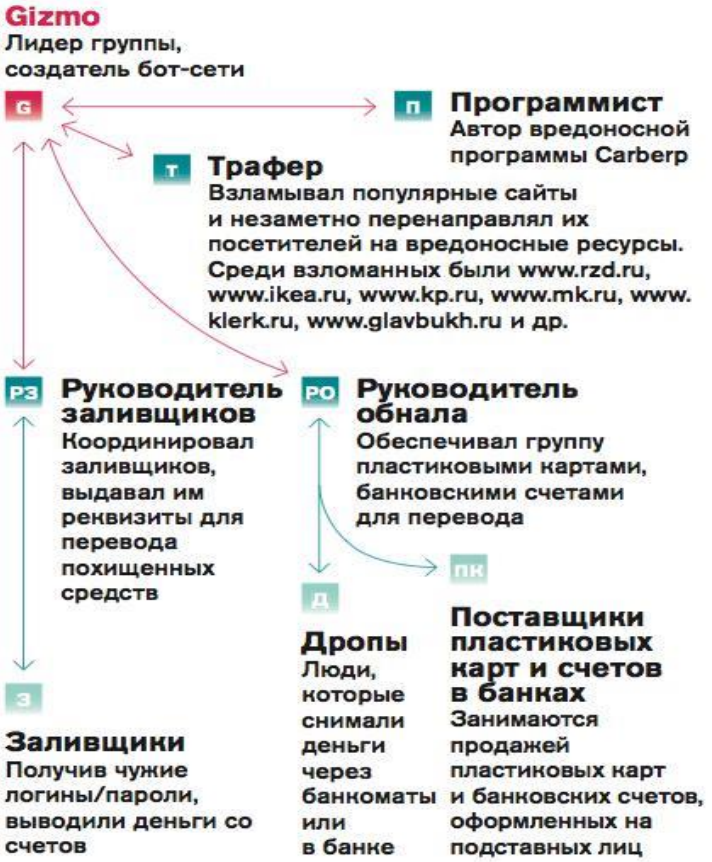
- Мошеннические действия производятся организованными группами, распределёнными по регионам и ролям.
- Хищения тщательно подготавливаются технически: создаются средства для кражи данных, фишинговые сайты, bot-сети, программы для организации DDoS-атак, планирование и координация действий участников.
- 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

«Живой» пример

Киберпреступная иерархия

Структура типичной мошеннической группы на примере группы Carberp, ликвидированной в марте 2012 года.

Весь доход делился пополам между организатором преступной группы и организатором обнала. При этом руководитель преступной группы из своих 50% оплачивал работу программиста, трафера, а также аренду серверов, доменов, шифрование, анонимизацию и пр. Руководитель обнала со своих 50% оплачивал работу заливщиков, их руководителя, дропов, поставщиков карт и банковских счетов.



Источник: Group-IB

Как увидеть

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	

Разработка стратегии безопасности СДБО

1. Определение политики безопасности СДБО

2. Организационные мероприятия

3. Технические мероприятия

4. Повышение осведомленности клиентов СДБО о мерах безопасности

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

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

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
5. Создание систем мониторинга

«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:

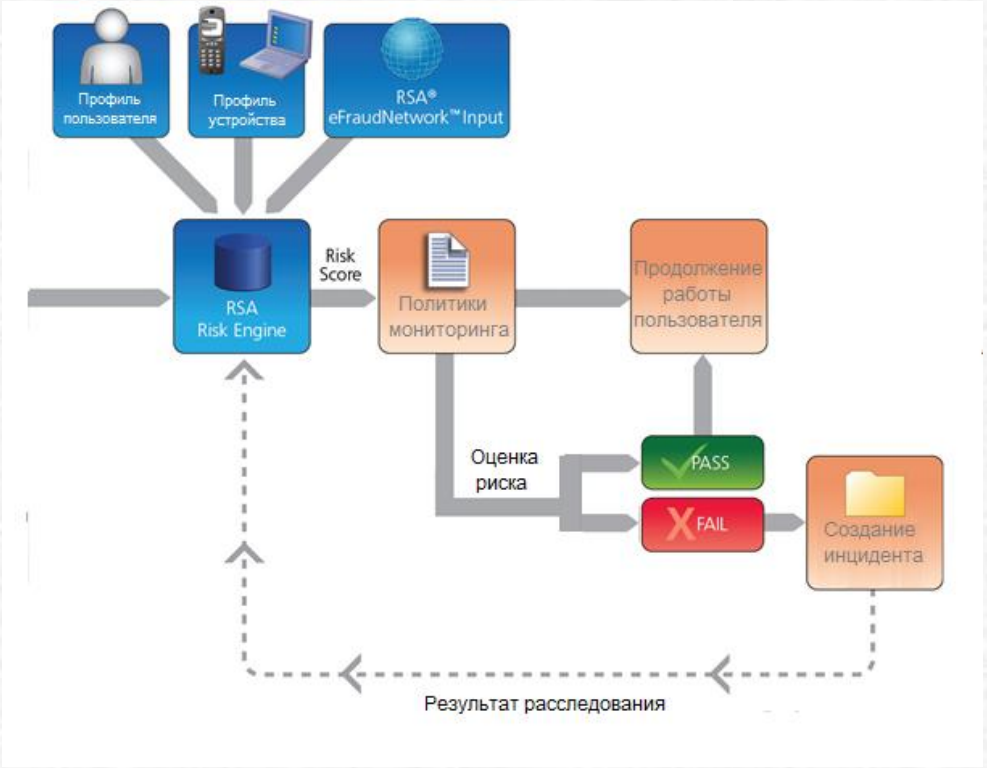
- При большом числе (более 10 тыс платежей в день) очень велико число платежей, попадающих под дополнительный «ручной» контроль
- Велика доля «человеческого фактора» (ошибки) при ручном исполнении большого объема контрольных функций
- При полуручной обработке невозможно быстро и эффективно применять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

Типовая схема «домашней системы»

Принцип функционирования промышленной системы мониторинга.

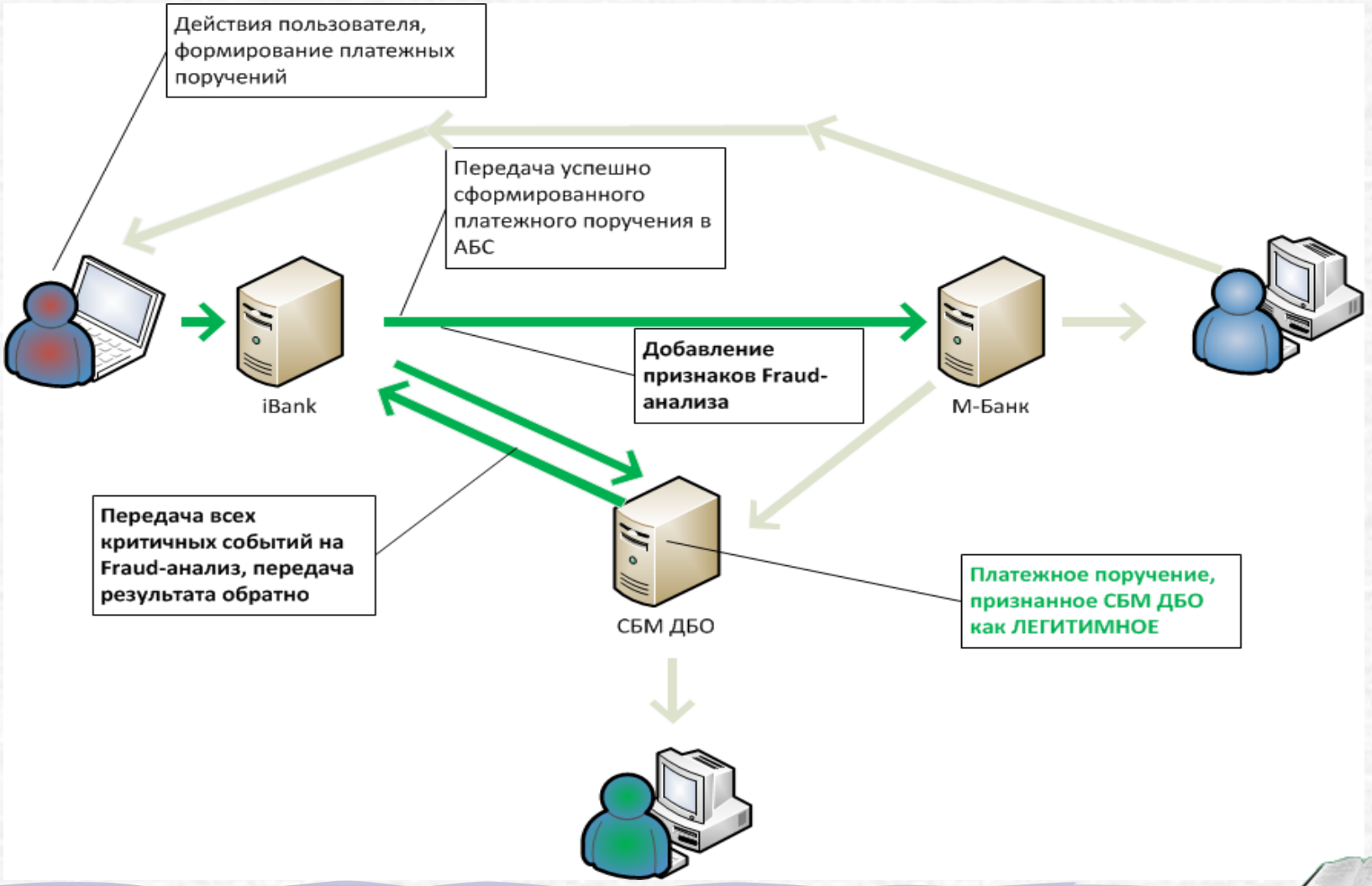
Этапы анализа в решении RSA:

- 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.

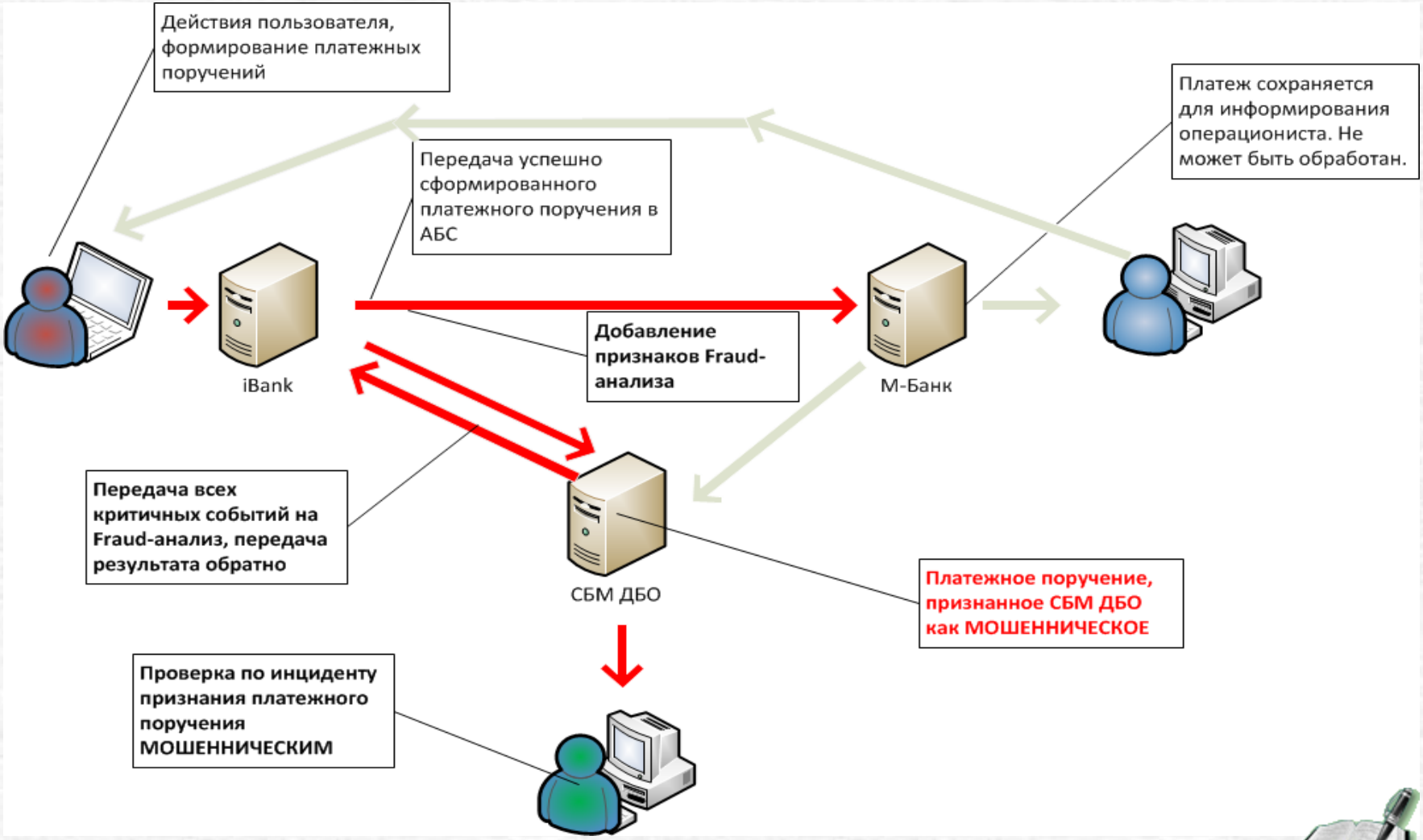


- Категорирование оценки риска и принятие решения о разрешении, приостановлении или блокировке операции.
- Создание инцидента по подозрительной или заблокированной операции.
- Передача результата расследования инцидента в самообучаемую модель.

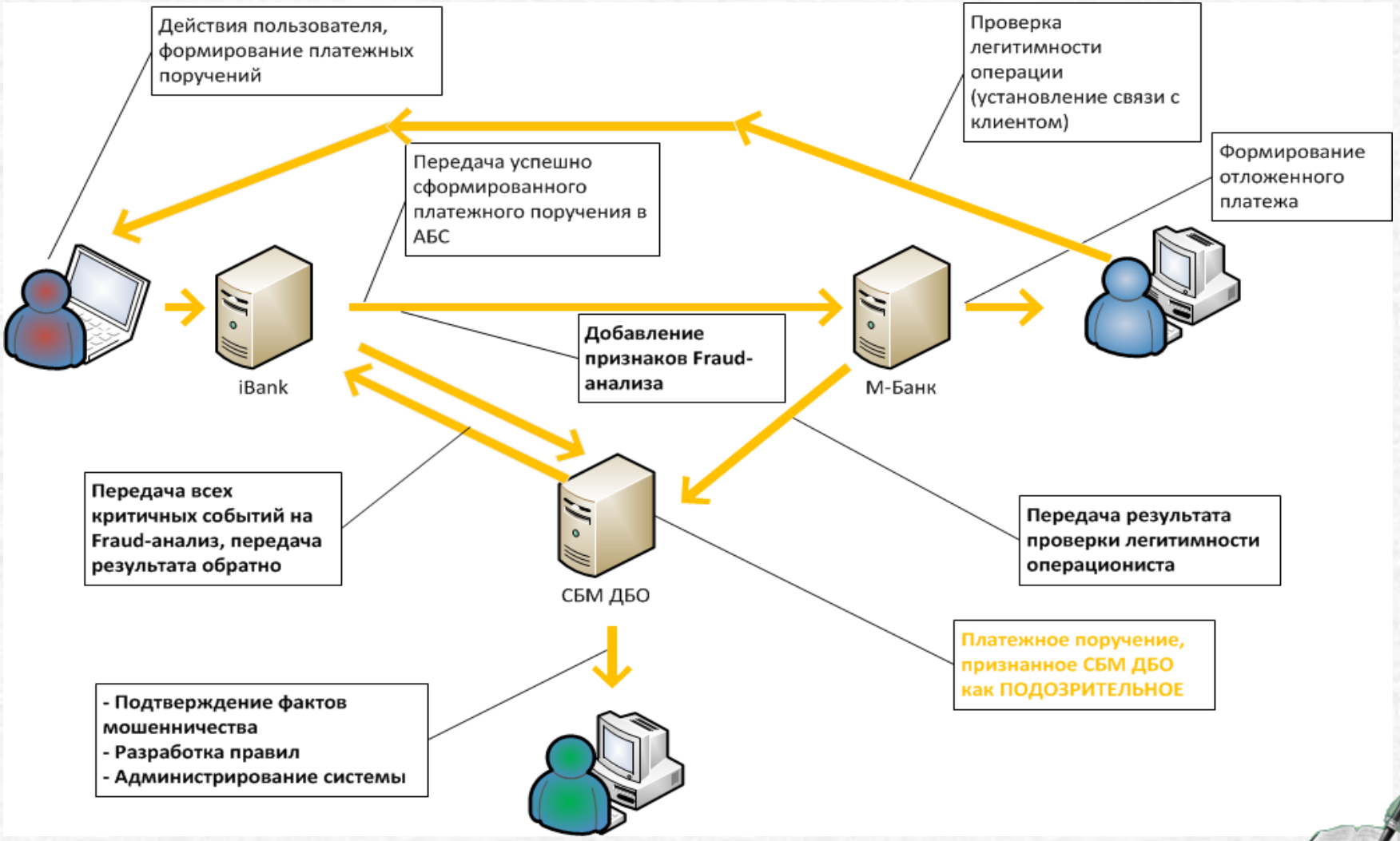
Легитимный платеж



Мошеннический платеж



Подозрительный платеж



Вместо заключения

Система за 2014 выявила 100% мошеннических платежей

Число контрольных звонков снижено практически в 10 раз, что позволило только за год окупить половину стоимости внедрения промышленной системы

Тем не менее, 5 мошеннических платежа за год прошло исключительно по вине человеческого фактора.

Из них – 3 возвращено благодаря взаимодействию с коллегами из других банков

СПАСИБО !

Какие будут вопросы?

Контакты:

Окулесский Василий Андреевич, к.т.н.

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