

Последние тренды фрода в ДБО и эффективное противодействие

Алексей Голенищев
Директор
Дирекция мониторинга электронного бизнеса
ОАО «АЛЬФА-БАНК»
Член MasterCard Europe Fraud Advisory Committee

ОСНОВНЫЕ УЯЗВИМОСТИ СЕГОДНЯ

- ✓ PC, сетевая инфраструктура, корп. сети
- ✓ Процессы & технологии
- ✓ Каналы & коммуникации
- ✓ Базы данных
- ✓ **!!! Персональное «ПО» головы клиента**



ЗНАКОМСТВА В ИНТЕРНЕТЕ

всегда приятный сюрприз



Угрозы 2016 - 2017



P2P переводы

От поддельных «торгово-сервисных» сайтов.... – к поддельным «банковским» сайтам денежных переводов

ДБО

Интернет банк

«Таргетированное» вирусное заражение компьютеров (в т.ч. инсайд, атаки на ПО, Приложения). Получение удалённого управления. Поддельные сайты Банков. «Комплексная» социальная инженерия (дублирование SIM, смена УЛ).

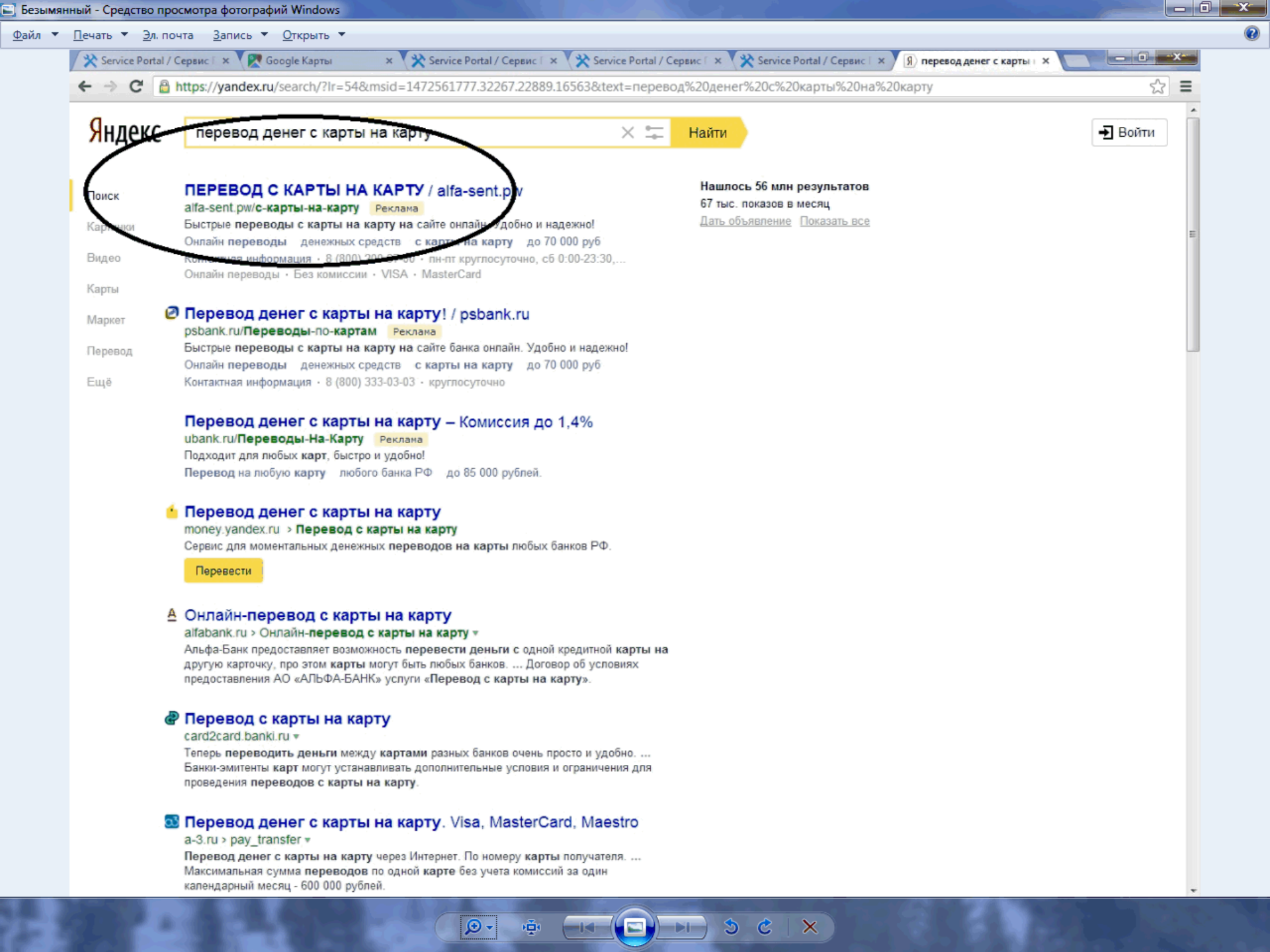
Мобильный банк

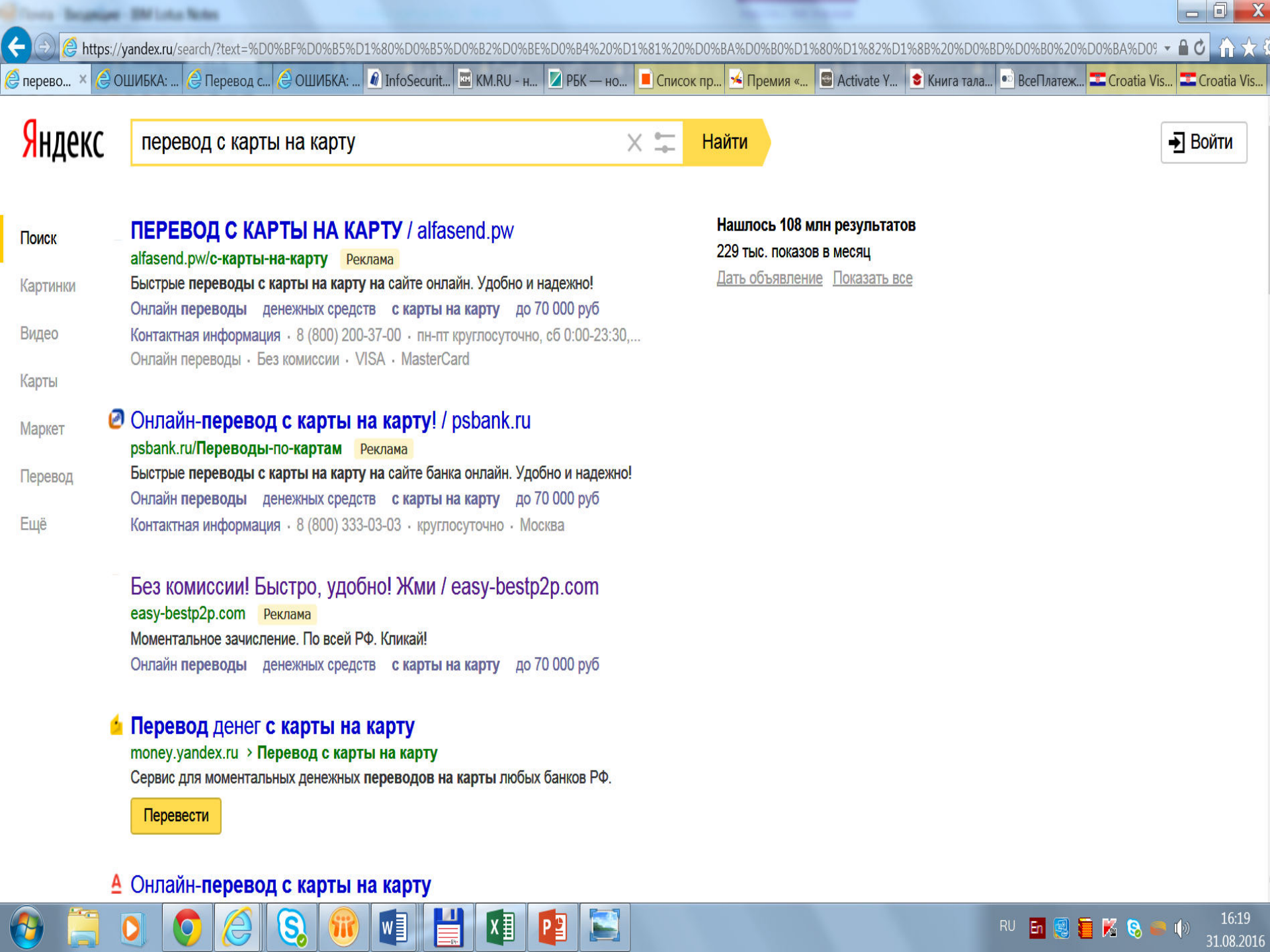
Атаки/заражение ПО моб. Телефонов (получение доступа к банковским app)

Корпоративные сети

Внешнее/внутреннее проникновение в корп. Сети.

Обнаружение/заражение/управление РС с доступом к корр. счетам и др.





← →

https://yandex.ru/search/?text=%D0%BF%D0%B5%D1%80%D0%B5%D0%B2%D0%B5%D1%81%D1%82%D0%B8%20%D0%B4%D0%B5%D0%BD%D1%8C%D0%B3%D0%B8%20%D1%81%20%D0%BA%9

Ошибка ве... InfoSecurity... Проезд и п... Ошибка ве... РБК — нов... KM.RU - но... Политика lemeridienni... перевест... x Le Meridien ... Le Méridien ... Booking.co... Перевод с ...

Яндекс

перевести деньги с карты на карту

Найти

Войти

Поиск

Картинки

Видео

Карты

Маркет

Перевод

Ещё

Перевести с карты на карту / send-skb.pw

send-skb.pw/с-карты-на-карту Реклама

Быстрые переводы с карты на карту на сайте онлайн. Удобно и надежно!

Онлайн переводы денежных средств с карты на карту до 70 000 руб

Перевести деньги с карты на карту – Комиссия до 1,4%

ubank.ru/Переводы-На-Карту Реклама

Подходит для любых карт и банков, быстро и удобно!

Перевод на любую карту любого банка РФ до 85 000 рублей

Перевод денег с карты на карту! / psbank.ru

psbank.ru/Переводы-по-картам Реклама

Быстрые переводы с карты на карту на сайте банка онлайн. Удобно и надежно!

Онлайн переводы денежных средств с карты на карту до 70 000 руб

Контактная информация · 8 (800) 333-03-03 · круглосуточно · Москва

Перевод денег с карты на карту

money.yandex.ru > Перевод с карты на карту

Сервис для моментальных денежных переводов на карты любых банков РФ.

Перевести

«Сбербанк» - Безналичный перевод по России с карты...

sberbank.ru > ...person/paymentsandremittances...beznal... ▾

Вы можете мгновенно перевести средства со своей карты на свою карту Сбербанка

Нашлось 24 млн результатов

235 тыс. показов в месяц

Дать объявление Показать все

RU En

13:50

21.09.2016

Перевод с карты на карту

Перевод с карты на карту – это просто и удобно!

- Сроки зачисления переводов на карту зависят от банка получателя и составляют от нескольких минут до трех рабочих дней.
- Переводы осуществляются в валюте Российской Федерации с/на счета карт, выпущенных банками, находящимися на территории Российской Федерации.
- Комиссия за перевод - фиксированная и составляет ровно 10 руб. в независимости от суммы платежа.
- Минимальная сумма перевода, без учета комиссии, не менее 100-00(сто) рублей.

ОТПРАВИТЕЛЬ  

НОМЕР КАРТЫ

СРОК ДЕЙСТВИЯ **CVC2/CVV2 ?**

Январь ▾

 /

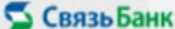
2016 ▾

ПОЛУЧАТЕЛЬ  

НОМЕР КАРТЫ

СУММА ДЛЯ ПЕРЕВОДА (В РУБЛЯХ)

RUR

Powered by 

Максимальная сумма перевода – 100 000 руб.

P2P переводы

[http:// www.ast-pays.ru/](http://www.ast-pays.ru/)
[http:// www.alfa-perevod.pw/](http://www.alfa-perevod.pw/)
[http:// www.paycard.pw/](http://www.paycard.pw/)
[http:// www.cardpay.pw/](http://www.cardpay.pw/)
[http:// www.card-pay.pw/](http://www.card-pay.pw/)
[http:// www.fastpays.pw/](http://www.fastpays.pw/)
[http:// www.cardpay.pw/](http://www.cardpay.pw/)
[http:// www.card-pays.pw/](http://www.card-pays.pw/)
[http:// www.card2card-alfa.pw/](http://www.card2card-alfa.pw/)
<http://www.easy-c2c.com/>
<http://www.client-2-card.com/>
<http://card-to-client.cc/>
<http://easy-bestp2p.com/>

Registrant Name: Pingvin Shirokokrilov

Registrant Organization: Private Person

Registrant Street: Pingvinovaya 34

Registrant City: Anantarktida

Registrant State/Province: Antarkticheskaya

Registrant Postal Code: 125000

Registrant Country: AQ

Registrant Phone: +7.9087742319

Registrant Phone Ext:

Registrant Fax:

Registrant Fax Ext:

Registrant Email: pingvin77887655677@gmail.com

Admin ID: C81386516-CNIC

Admin Name: Pingvin Shirokokrilov

Admin Organization: Private Person

Admin Street: Pingvinovaya 34

Admin City: Anantarktida

Admin State/Province: Antarkticheskaya

Admin Postal Code: 125000

Admin Country: AQ

Admin Phone: +7.9087742319

Admin Phone Ext:

Admin Fax:

Admin Fax Ext:

Admin Email: pingvin77887655677@gmail.com

Admin ID: C81386516-CNIC



[Как это работает?](#)

[Наши тарифы](#)

Моментальные переводы между картами любых банков РФ Комиссия - 0.1%



Отправитель

Введите номер карты

Срок действия карты

 /

CVV/CVC код ?

Сумма перевода

РУБ.

Получатель

Введите номер карты

Введите ваш e-mail (необязательно)

ПЕРЕВЕСТИ

Действительно простой способ
перевести деньги

Перевод с карты на карту

Мгновенно между любыми картами любых банков

Номер карты

Месяц

/

Год

CVC

Номер карты

Сумма перевода*

Комиссия будет рассчитана автоматически

☒ Я ознакомлен и согласен с [условиями публичной оферты](https://static.tinkoff.ru/documents/oferta/universal_c2c_payments.pdf)

Перевести



Перевод с карты на карту

Мгновенно между любыми картами любых банков

5521 75 CENSORED 6350

11 / 21 cvc 123

CENSORED

Задать вопрос >

**MasterCard**
SecureCode

На подтвержденный номер мобильного телефона было направлено SMS-сообщение с персональным одноразовым кодом для целей дополнительной аутентификации при совершении Операции в сети Интернет с использованием Карты.

Магазин	Card to card
Сумма операции	RUB 15000.00
Номер карты	XXXX XXXX XXXX 6350
Персональный одноразовый код	 введите кода

Для целей дополнительной аутентификации при совершении Операции в сети Интернет с использованием Карты нажмите кнопку «Подтвердить».



Часто задаваемые вопросы

Переводы между картами любых банков

Хочу перевести 85 000 рублей

Максимальная сумма перевода 85 000 рублей

Номер карты отправителя

4123 5678 9012 3456

Срок действия

02 / 23

CVC2/CVV2

096

?

Номер карты получателя

4987 6543 2109 8765

₽ Тарифы

Бесплатное пополнение карт
МДМ Банка.

Бесплатно между картами
МДМ Банка и Бинбанка.

1,40%, min 40 рублей – между
картами разных банков или с
карты МДМ Банка на карту
другого банка.

При переводе кредитных
средств с карт МДМ Банка
взимается дополнительная
комиссия – 4,9%,
min 400 рублей.

× Лимиты

Минимальная сумма одного
перевода – 10 рублей,
максимальная – 85 000
рублей.

Максимальная сумма
переводов с одной карты
в месяц – 599 000 рублей.

🕒 Сроки

Перевод денежных средств
происходит моментально.

В некоторых случаях срок
зачисления может быть
увеличен банком-эмитентом
карты получателя средств до
6 рабочих дней.



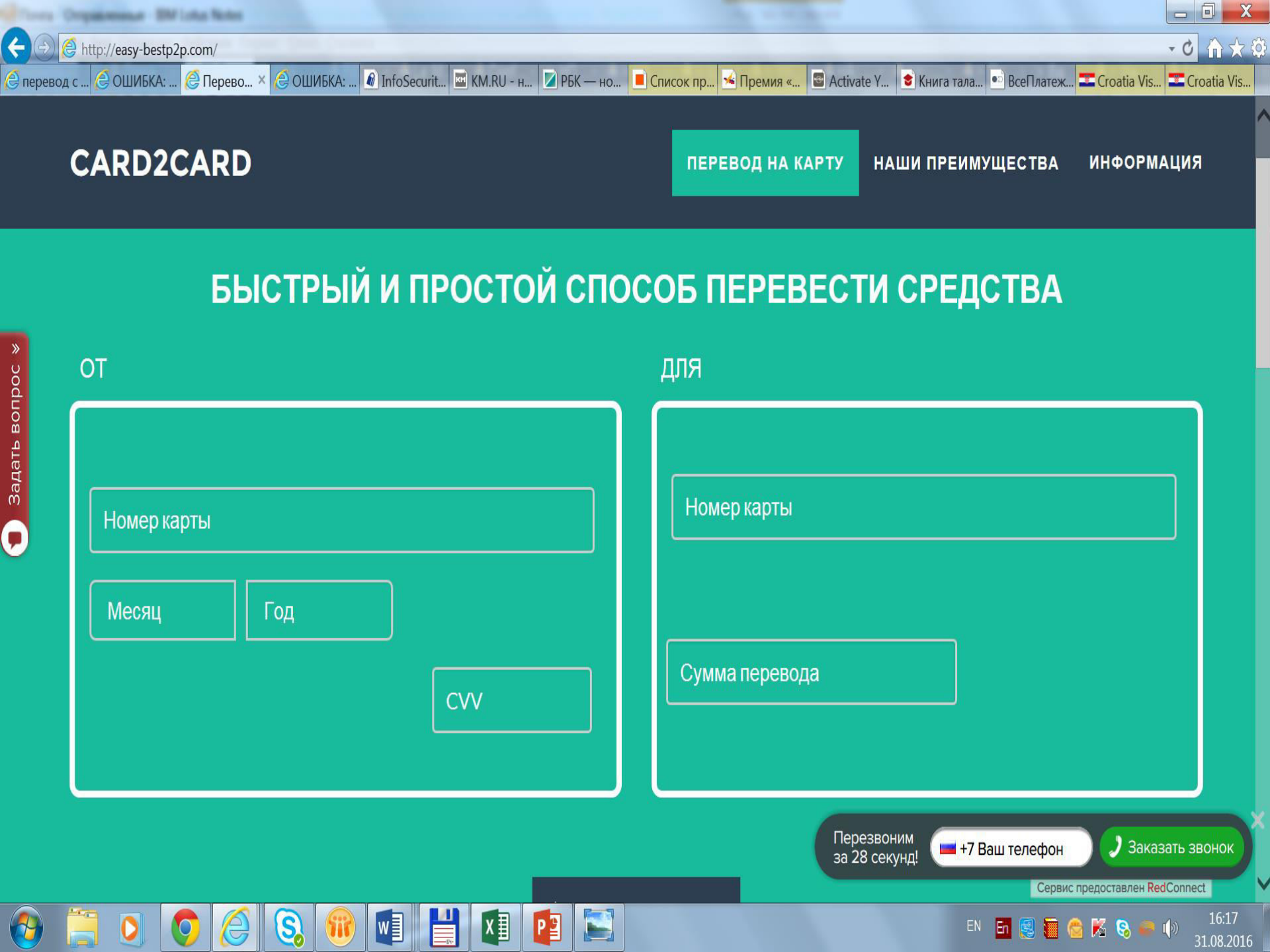
VISA

MasterCard
MoneySend™

Verified by
VISA

MasterCard.
SecureCode.

thawte™
It's a trust thing™



CARD2CARD

ПЕРЕВОД НА КАРТУ

НАШИ ПРЕИМУЩЕСТВА

ИНФОРМАЦИЯ

БЫСТРЫЙ И ПРОСТОЙ СПОСОБ ПЕРЕВЕСТИ СРЕДСТВА

ОТ

для

Номер карты

Номер карты

Месяц

Год

CVV

Сумма перевода

Перезвоним
за 28 секунд!

+7 Ваш телефон

Заказать звонок

Сервис предоставлен RedConnect

EN

En

16:17
31.08.2016



- 1) Новые способы атак на физических лиц (ПО, РС, моб. App).
Таргетизация атак
- 2) «Lurk» and Co по прежнему в бою
- 3) Конфликты интересов среди «мошенников» - угрозы банку?
- 4) Мониторинг - как один из основных способов эффективной защиты

ДБО (физ. лица)

- отсутствие грамотности и навыков по безопасному пользованию РС
- не достаточная финансовая грамотность при работе с системами ДБО
- доверчивость граждан (соц. инженерия, поддельные сайты, сообщения и т.п.)

Соц. Инженерия

(как метод для получения доступа в систему ДБО)



- классические способы "развода" клиента (выигрыши ценных подарков, с просьбой оплаты налогов, взломы скайпов с просьбой перевести денег, звонки от "службы безопасности" и т.д.), "развод" с целью дальнейшего взлома ДБО клиента.
- фэйк-страницы банк-клиентов, размещение в сети (в т.ч. мобильных) зараженных приложений, смс-рассылки с вредоносным файлом, под видом ссылок на объявления и т.д.
- точечные атаки на состоятельных клиентов, суть атаки заключается в взломах обычных сервисов «icloud», и восстановлении резервных копий на устройствах клиентов....

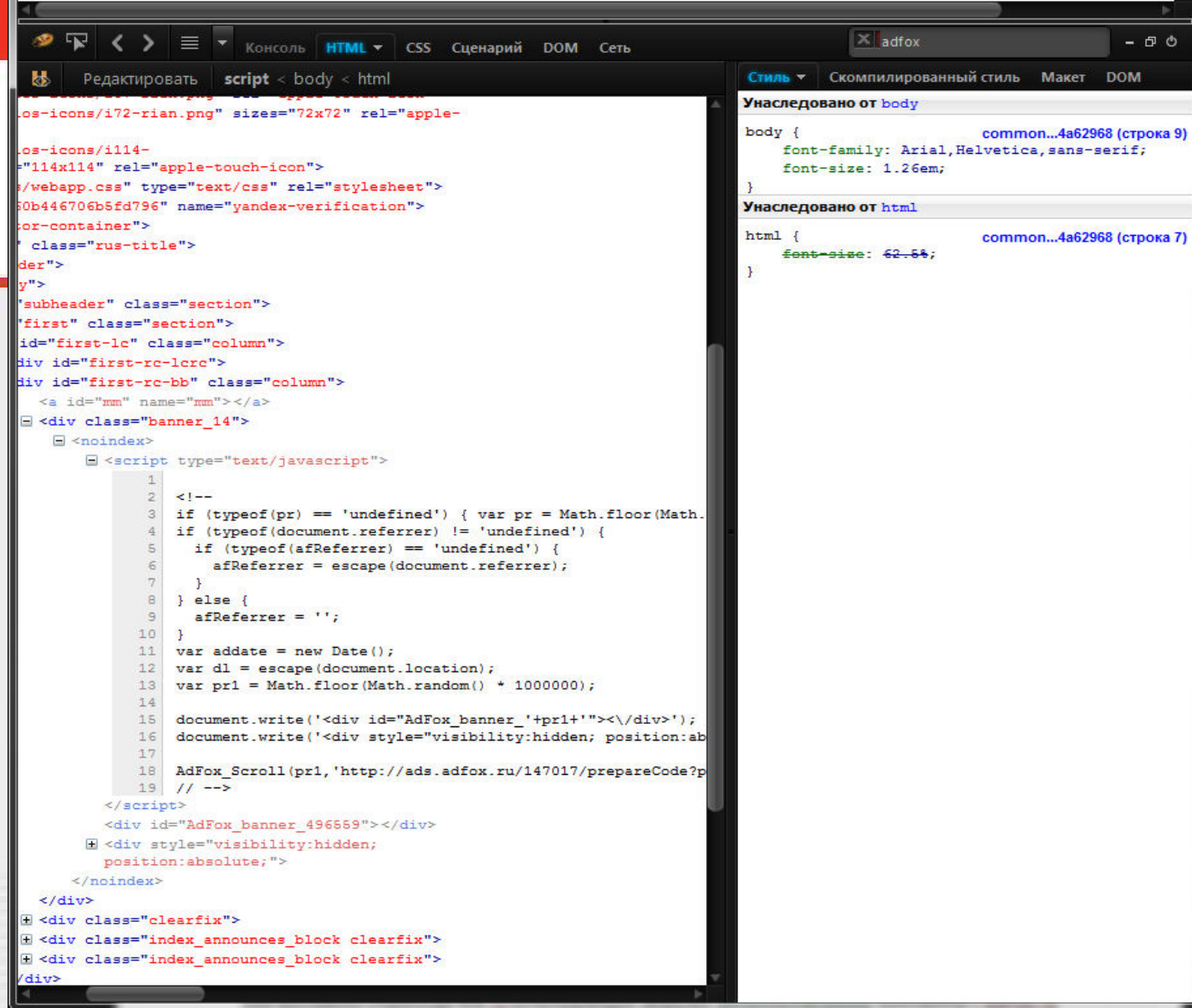
ДБО (юр. лица)

- в 2016 активно работают несколько групп по веб-инжектам и подмене реквизитов

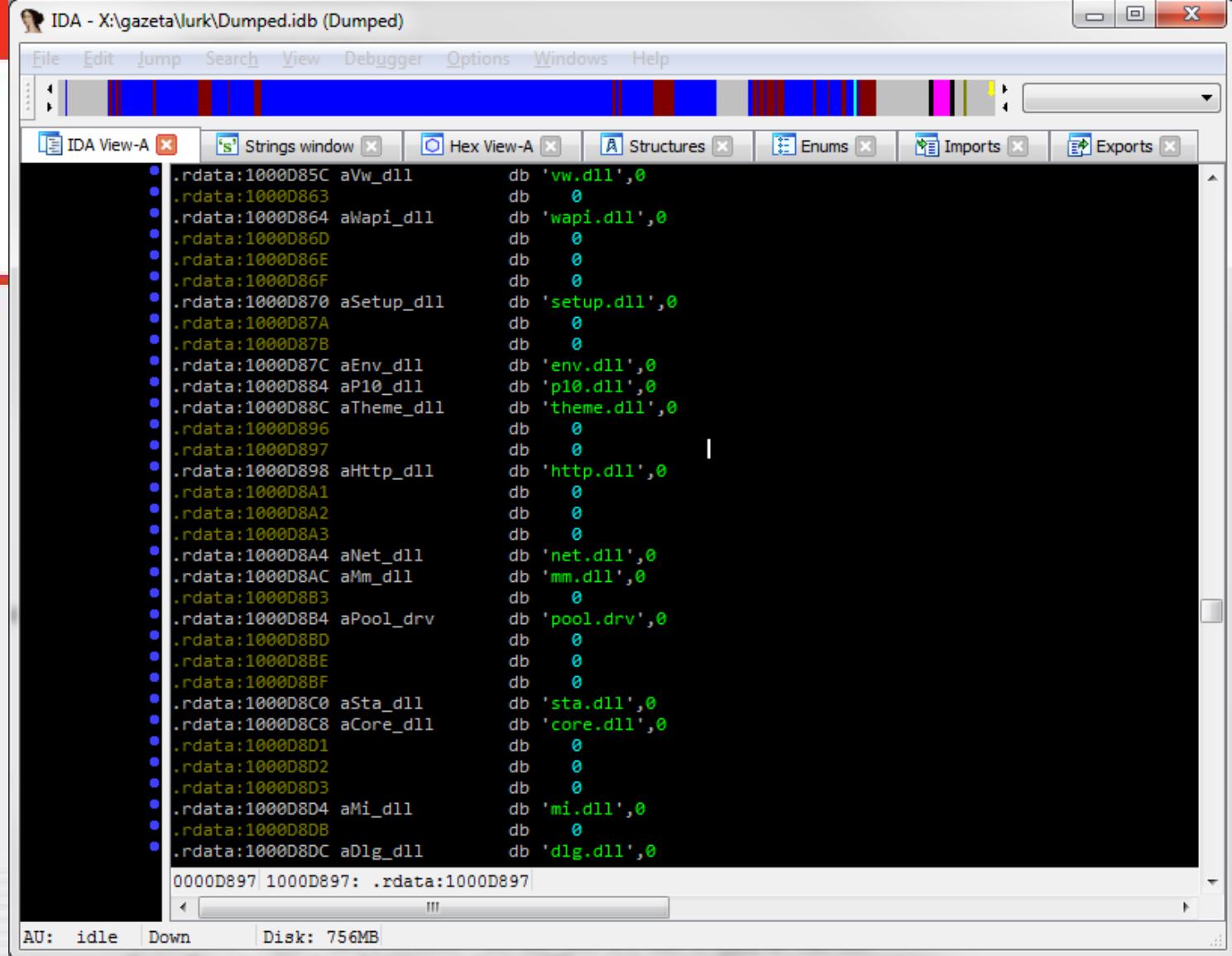
В платежных поручениях, так
небезызвестный «Lurk» с инжектом в браузере, «Fibbit» с функционалом подмены реквизитов на уровне экспорта реестра платежей из бухгалтерских программ.

Модель атаки строится на вводе в заблуждение клиента путем отправки письма с бухгалтерской тематикой, и прикрепленным вредоносным файлом. Далее, при заведении платежки автоматически происходит подмена реквизитов получателя, при этом наименование получателя остается прежним, а ИНН и счет изменяются





Код главной страницы RIA.ru, использующийся для загрузки дополнительного контента («разведка» атакованного РС, установка на «интересный РС» доп. зловреда)



Часть кода зловреда Lurk, отвечающего за загрузку дополнительных модулей

ВАКАНСИИ

- [➤ Все вакансии](#)
- [➤ Поиск вакансий](#)
- [➤ Добавить вакансию](#)

РЕЗЮМЕ

- [➤ Все резюме](#)
- [➤ Поиск резюме](#)
- [➤ Добавить резюме](#)

РАБОТА В УКРАИНЕ

- [➤ Работа в Белой Церкви](#)
- [➤ Работа в Виннице](#)
- [➤ Работа в Днепропетровске](#)
- [➤ Работа в Донецке](#)
- [➤ Работа в Житомире](#)
- [➤ Работа в Запорожье](#)
- [➤ Работа в Ивано-Франковске](#)
- [➤ Работа в Кировограде](#)
- [➤ Работа в Киеве](#)

ПОИСК ВАКАНСИЙ И РЕЗЮМЕ

Раздел:  IT Руководители
не более  Программисты С, С++, С#
одного раздела Программисты .NET
Программисты Java, J2EE, JSP
Специалисты по IT безопасности 

Работа в 

Фраза: 

вакансии ☐

резюме ☐

Поиск

ТРЕБУЕТСЯ СПЕЦИАЛИСТ ПО JAVA/FLASH

23.10.2014

Зарплата от: 2500
у.е

Опыт работы от 2 лет

Город: работа в Одессе

Требуется специалист по java/flash

Требования:

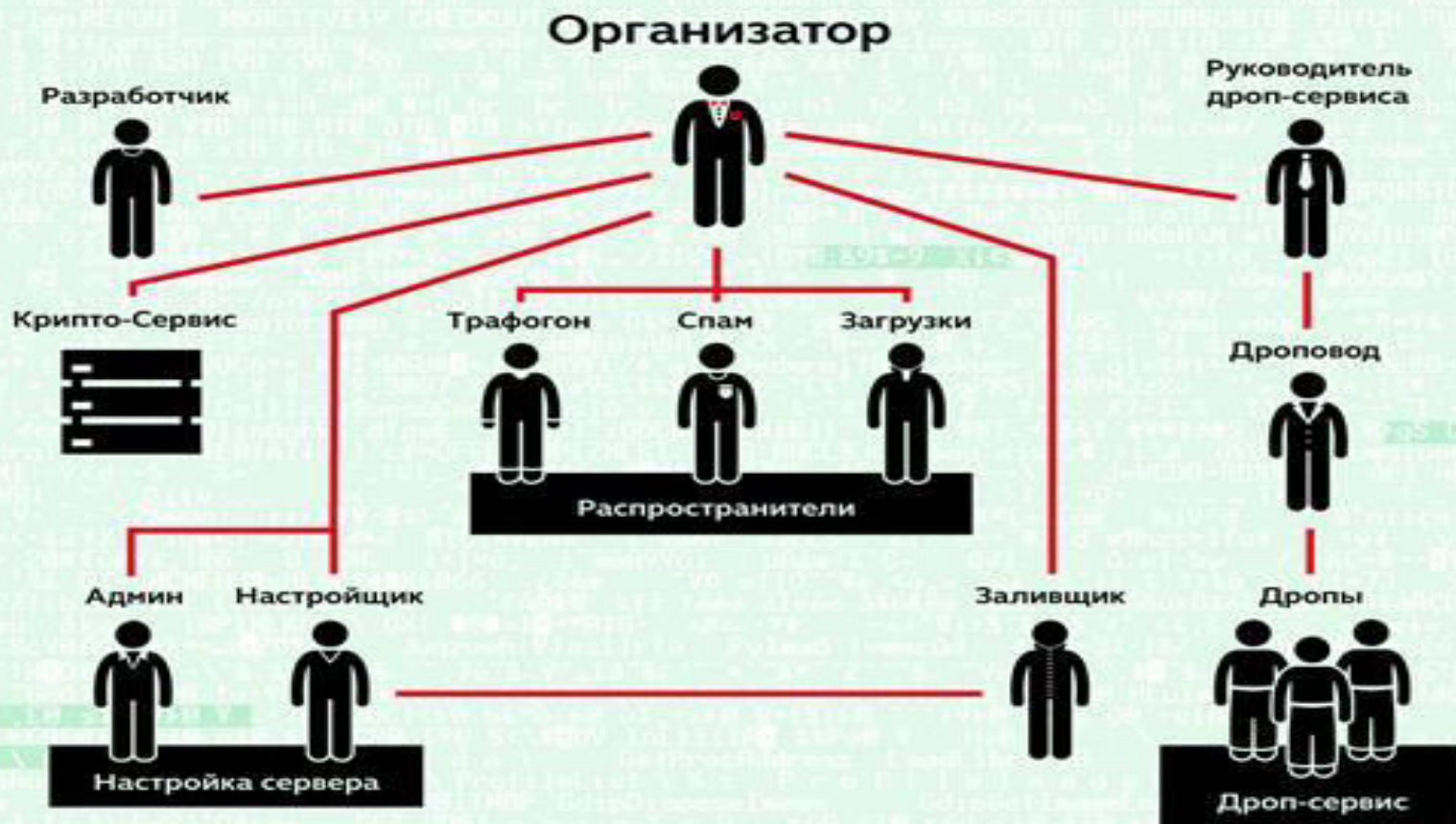
- хороший уровень программирования java (только SE, никаких серверных разработок)
- хороший уровень на flash (action script 3)
- уверенное знание спецификаций JVM/AVM, т.е. — формат файлов, умение читать и понимать байткод, умение восстанавливать алгоритмы по байткоду, умение работать с программными фреймворками по модификации форматов спецификаций, умение работать с обфусцированными файлами форматов
- опционально — программирование python, хотя бы начальный уровень

Условия работы:

- удаленная работа на постоянной основе;
 - полная занятость;
- Зарботная плата 2500\$.

Схема организованной киберпреступной группы

«Лаборатория Касперского» исследует деятельность пяти крупных киберкриминальных групп, специализирующихся на финансовых преступлениях.

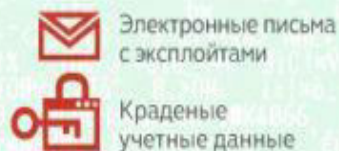
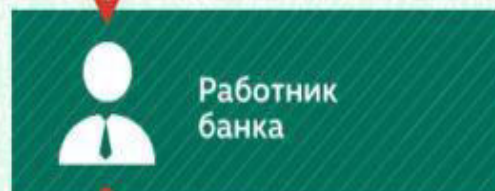


Заливщик переводит деньги со счетов атакованной финансовой организации на счета, предоставляемые дроповодом. Дроповод указывает дропам, куда перевести деньги. Часть похищенных денег остается у руководителя дроп-сервиса, а остальные суммы переводятся организатору криминальной группы.

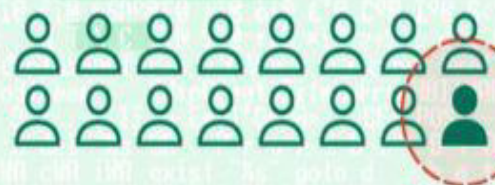
Как кибербанда Carbanak ukrала миллиард долларов

Целевая атака на банк

1. Заражение



Сотни машин заражены в поисках компьютера администратора



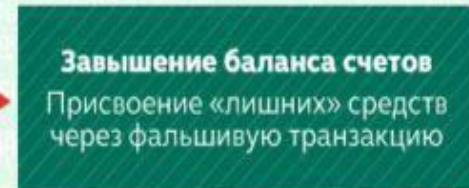
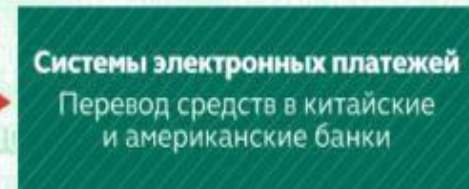
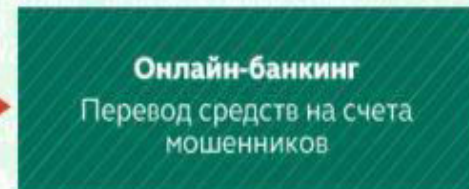
2. Сбор разведданных

Перехват данных с экранов служащих



3. Действия от имени сотрудников

Как были украдены средства





MainCPs.txt
Collectors.txt

Encryption key

Connector interval (sec)

Kill Zeus:

☐ Jabber Notification

Clear cookies and sessions:

☐ VNC Module (with back-connect)

Brute-force certificates:

☐ Auto-Spreading

Log only important (https) URL's:

☐ Auto-Update

Compress with Unique Stub Generator:



Enable screenshot configuration:



[WebInjects]

[ScreenShots]

[Plugins]

* EXE name :

* Mutex name :



Generate config & FUD an EXE file

Are you infected by SpyEye or Zeus?

«Lurk»

ФСБ & МВД. Задержание 05.2017. Задержано 50 хакеров (14 – в Е-бурге). 86 обысков в 15-ти регионах РФ. Похищено 1,7 млрд. руб. (Изъято 12 млн. р., 1000 симкарт, 100 ноутбуков, > 200 телефонов)





Соцсети им в помощь..

Обнаружение: 15.05.2016 зафиксирован рост числа авторизаций в Альфа-Мобайл, в ходе анализа активности установлено следующее: -все запросы подписывались одним cookie, все авторизации шли через калужский дата-центр (прокси), Cookie «засветился» 13.05.2016 при входе в ДБО Альфа-Мобайл

Способ хищения: подошедшие аутентификационные данные использовались для входа в Альфа-Мобайл, совершение платежей на тел. МТС – QIWI, Webmoney – личная карта

Маскирование: Использование анонимайзера Hideme.ru

Аутентификационные данные: собраны из публичных источников, за логин взят ник-нейм от страницы вКонтакте, за пароль - дата рождения\телефон из страницы VK. Собрано было порядка 40 тысяч связок аутентификационных данных.

Результат атаки: получен доступ к 105 клиентам банка, хищение у 4 клиентов на сумму порядка 60 тысяч рублей. + **Уг. Дело по ст. 159.6.2**



Биометрия – новые угрозы!?



ИБ-исследователи из FireEye обнаружили способ похищения данных об отпечатках пальцев пользователей таких мобильных устройств с биометрическими сканерами, как Samsung Galaxy S5 и HTC One Max. (обнаружено, что в HTC One Max отпечатки пальцев хранятся в виде незашифрованного граф. файла dbgraw.bmp. Мошенники с помощью любого непривилегированного процесса или приложения могут получить доступ к данному изображению, причем в высоком разрешении)

Злоумышленники могут также использовать поддельные экраны блокировки для аутентификации личности в популярных платежных системах с целью перехвата денежных переводов и хищения средств.

Многие производители моб. устройств на базе Android не используют технологию TrustZone для защиты биометрических данных. К 2019 году половина всех проданных мобильных устройств будет оснащена сканером отпечатков пальцев. Удаленное выполнения кода позволит похищать биометрические данные массово. Вероятно, что хакеры также смогут добавлять свои отпечатки пальцев, имея физ. доступ к моб. устройству пользователя.

IT безопасность –
техническая/организационная?! Да!  Альфа-Банк

НО

!Никакая «Безопасность» не исключит риск мошеннической атаки на 100%, но создаст для злоумышленников значительные трудности к достижению преступной цели и серьезно увеличит вероятность того, что в преодолении эти «трудностей» они совершат «ошибки», что поможет и облегчит работу правоохранительным органам и экспертам по информационной безопасности при раскрытии и предотвращению преступлений.

Основные механизмы хищений в каналах ДБО



- ДБО физ. лиц



- Заражение PC
- Перенаправление пользователя на фишинговый сайт и перехват / выманивание одноразового пароля от имени сотрудника Банка

Фирма ищет
нового бухгалтера!
И старого тоже!



- ДБО юр. лиц

- Проникновение в корп. сеть, заражение
- Подмена платеж. поруч.,
- Удаленный доступ,
- Неконтролируемые действия уполномоченных сотрудников

Авторы многочисленных статей по социальной инженерии предлагают несколько видов защиты:



1. Технологическая (антивирусы, антиспам, токены и др.) *напр. Альфа-Банк – App «Альфа-Ключ»*
2. Антропогенная (обучение клиентов)
 - попросите номер и перезвоните. По возможности проверяйте личность человека
 - никому не нужна ваша личная информация, пароли, никто не должен просить вас установить какое-либо ПО
 - при любых проблемах лучше обращаться к проверенным людям

Fraudmonitoring@alfabank.ru



Что мы мониторим?



ДБО - Физ. Лица

- Переводы на (др. счета, телефоны, эл. кошельки, карты).
- Переводы* с (карты на карту, счета на счет (внутр./внеш.))
- SMS переводы.

ДБО - Юр. Лица

- Переводы*

*в т.ч. входящие

Отделения

- Заккрытие депозитов
- Заказ / снятие крупных сумм
- Переводы

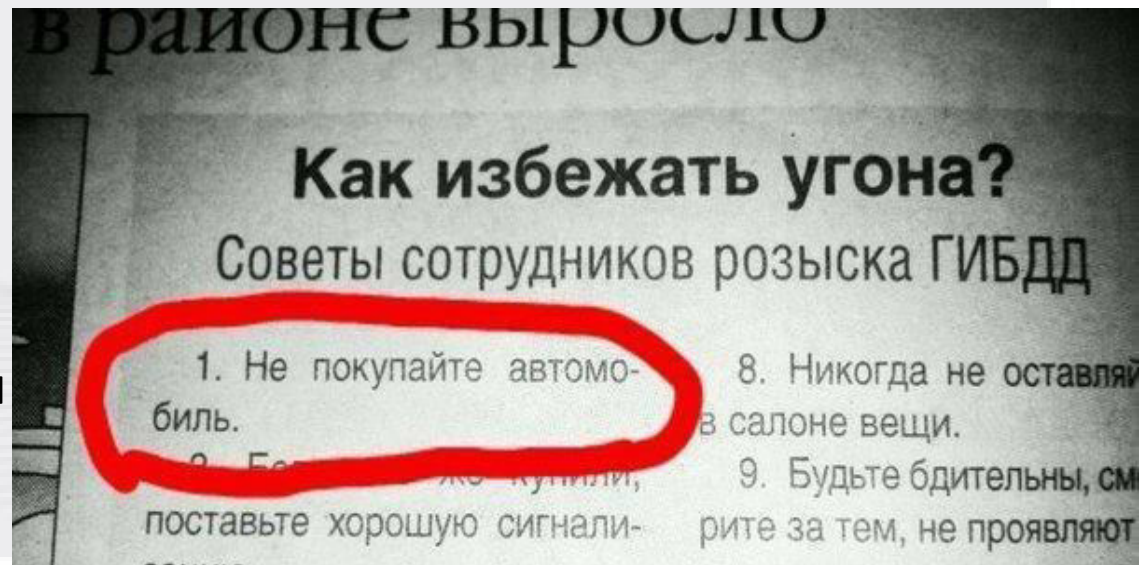


Основные требования к системе мониторинга



- Интеграция в единую архитектуру
- Комплексность («эшелонированная оборона», диверсификация методов и средств)
- Общее управление (единая стратегия и политика, централизация информации)
- Неразрушающий контроль (минимизация воздействия на основные процессы, «малозаметность»)

- Быстродействие
- Надежность (mission critical)
- Встраивание в бизнес-логику транзакций
- Гибкость «тюнинга»



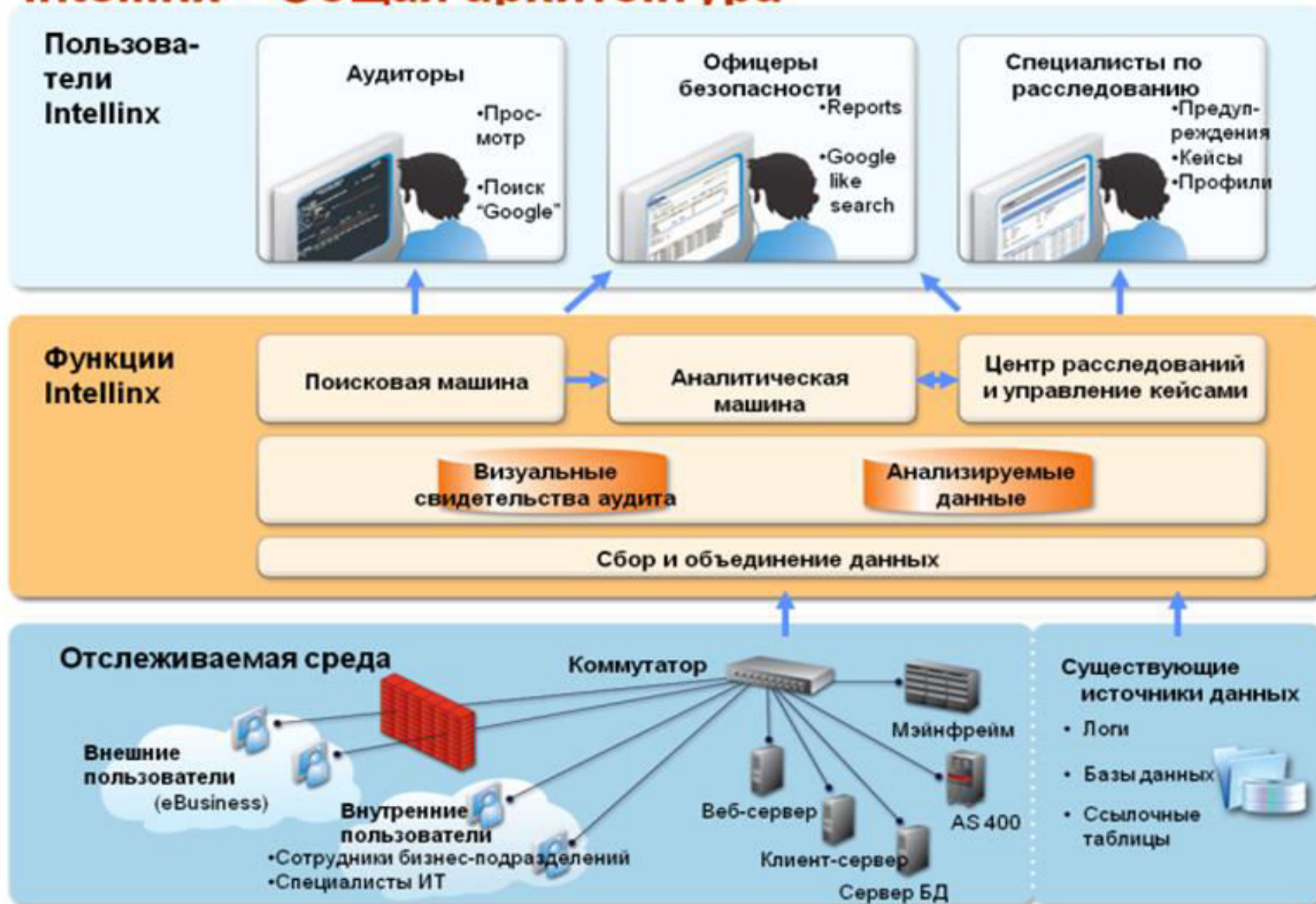


ЭКСПАНСИЯ НАТО?!
нам есть чем дать отпор

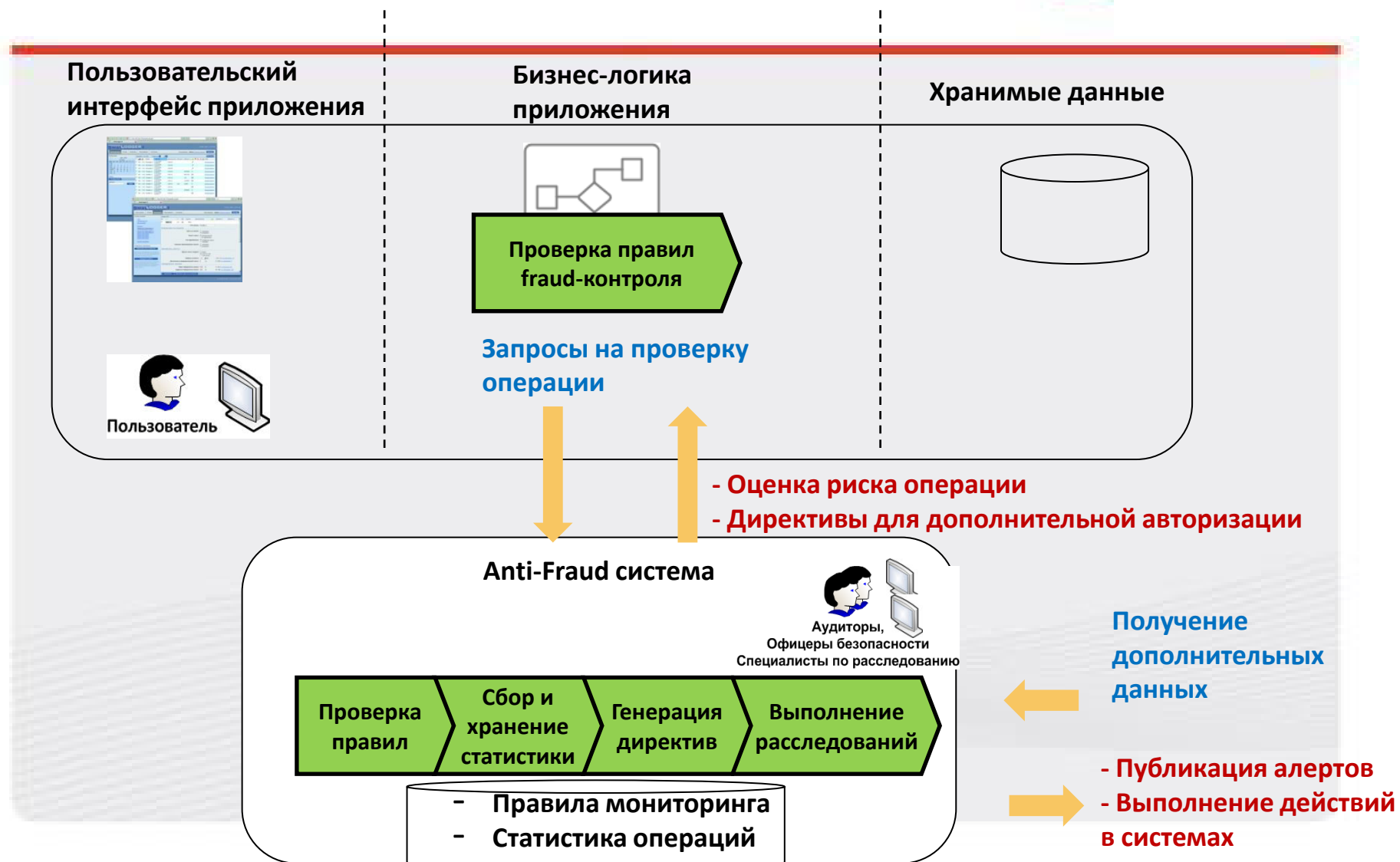


Solution Demonstration
Intellinx in Action

Intellinx – Общая архитектура



ТРАНЗАКЦИОННЫЙ FRAUD-КОНТРОЛЬ



Пример экранной формы он-лайн отчета



Home

Refresh

Customize

Alert Report

Results 1 - 100 of 10000

1 Go

Cases	Alert #	EQID отправителя	Description	Сумма	Назначение платежа	Код операции	Дата	По чёрному списку	Статус	Был звонок
	61930	AEBLJE	На новый счёт	13,600	Оплата счета N 111 от 23.01.12	301	24.01.2012 15:04	0	-1	
	61929	ABM1EJ	На новый счёт	20,000	Частный перевод, без НДС	321	24.01.2012 15:04	0	-1	
	61928	J12211	На новый счёт	8,921	частный перевод без НДС	321	24.01.2012 15:04	0	-1	
	61927	K03308	На новый счёт	10,000	Перевод	301	24.01.2012 15:03	0	-1	
	61926	ADDDXM	На новый кошелек	3,000		397	24.01.2012 15:03	0	46	
	61925	AANZWZ	На новый счёт	8,452.05	платеж от Поминова В.А. в адрес ООО "Газпром межрегионгаз Оренбург" за природный газ за декабрь 2...	301	24.01.2012 15:02	0	-1	
	61924	AA6EVI	На новый счёт	11,000	Перевод собственных средств	301	24.01.2012 15:02	0	-1	
	61923	AADXPC	На новый счёт	10,000	перевод собственных средств	321	24.01.2012 15:02	0	-1	
	61922	I88398	На новый счёт	31,283.72	Оплата за игрушки(НЮ196-196/2011.N104 24.01.2012) сумма 31283,72 НДС 2939,66.Плательщик ИП Космаче...	301	24.01.2012 15:02	0	-1	
	61921	ADA1NG	На новый счёт	6,344	Консультативные услуги	301	24.01.2012 15:01	0	-1	
	61919	AC06I6	На новый счёт	10,660	Пополнение счета	321	24.01.2012 15:01	0	-1	
	61920	ACEV3E	На новый счёт	18,600	частный платеж (продвижение моды)	321	24.01.2012 15:01	0	-1	
	61918	ABE24F	Большая транзакция на счёт	100,000	Перевод Кайсину А.Р.	321	24.01.2012 15:01	0	-1	
	61917	N88213	Большая транзакция на счёт	100,000	Частный перевод. НДС нет	321	24.01.2012 15:01	0	46	
	61916	AC3PLR	На новый счёт	19,500	Оплата коммунальных услуг за квартиру по адресу г.Красноярск ул. Молокова 50-291 л/с 03491	301	24.01.2012 15:00	0	-1	
	61915	AAXDRT	На новый кошелек	3,000		367	24.01.2012 15:00	0	-1	
	61914	AD2D4H	На новый счёт	25,000	Погашение займа по договору N10/09-1з от 10.09.2010	301	24.01.2012 15:00	0	-1	
	61913	C52635	На новый счёт	7,937.72	Доплата за эл-во., N аб.05543 035 69, Алейников В.В., г. Долгопрудный, Лаврентьева, 27, 35	301	24.01.2012 14:59	0	-1	
	61912	AEA0K8	На новый счёт	25,731	Оплата за товар по счетам N 83 от 20.01.12 и N 85 от 23.01.12 .Без НДС.	301	24.01.2012 14:59	0	-1	
	61911	ABHFNE	На новый счёт	7,800	За комфортное доруливание	321	24.01.2012 14:58	0	-1	
	61910	ADH000	Большая транзакция на счёт	30,000		367	24.01.2012 14:58	0	-1	

ИБ для физлиц «Альфа - Клик»:

- сохранено на счетах клиентов > 6 млн.руб.
- В среднем в сутки обрабатывается до 100 000 платежей клиентов (общее кол-во транзакций ~ 1 200 000).
- Фрод 0,025BP (0,00025%)

Корпоративные каналы:

- Сохранено на счетах клиентов > 205 млн.руб.
- В среднем в сутки обрабатывается до 150 000 платежей клиентов.
- Фрод 0,01BP (0,0001%)



а-Банк

СПАСИБО ЗА
ВНИМАНИЕ !

Алексей Голенищев
agol@alfabank.ru



CEMEA Security Summit 2015
Enhancing Security through Innovation
28-30 April 2015 | Grand Hyatt Dubai, UAE



L.E.A.D.E.R Award 2015

The Visa LEADER award is presented to **Alfa-Bank**
for excellence in fraud risk management and
supporting Visa's efforts to maintain trust and security
in the payments industry in **Russia** for the year 2015

A handwritten signature in black ink, appearing to read 'Ingo Noka'.

Ingo Noka
Regional Risk Officer
Central Europe, Middle East and Africa