конференция
РусКрипто'2013

http://www.ruscrypto.ru/conference/

Противодействие мошенничеству в сервисе online-платежей Яндекс.Деньги

Армарчук Анна

РусКрипто 2013

Что это такое

Настоящие деньги, только электронные *(161-ФЗ)*

- более 13 000 000 счетов
- каждый день 9 000 новых счетов и 120 000 транзакций

Результаты опроса агентства TNS за апрель 2012:

	Яндекс.Деньги	**WebMoney**	**Деньги@Mail.ru**	**QIWI**	**PayPal**
Знают	**78%**	65%	46%	35%	27%
Платят	**15%**	10%	2%	10%	6%

Почему пользуются?

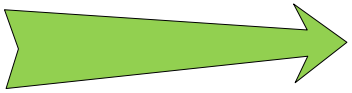
- расчеты в режиме реального времени
- мобильный доступ к счету

- 20 000 мерчантов

- возможность проведения части расчетов без идентификации

Движение денежных средств

Пополнить



С банковской карты

Банковский перевод

Наличными

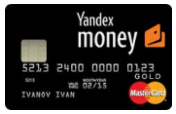
Электронной валютой

Карты предоплаты

Потратить

Совершить покупку в интернет-магазине

Перевести другому пользователю



Потратить offline с помощью банковской карты Яндекс.Деньги

Забрать

Вывести через Contact

На любую банковскую карту

Перевести в электронную валюту

Вывести на счет в банке

Яндекс деньги

Основные аутентификационные данные
Логин в Яндексе, № счета 41001XXXXXXXX
+
Платежный пароль или средства усиленной аутентификации

Дополнительные аутентификаторы

Веб портал / Мобильный веб портал
Мобильные приложения
API

Внешние воздействия:
платежи (терминалы, кассы, ДБО, ...)
привязка карт через банкомат

Меры безопасности для пользователя

- ✓ Привязка телефона к счету
- ✓ Информирование об операциях по счёту:
  - e-mail
  - SMS
- ✓ Одноразовые платежные пароли:
  - По SMS
  - Таблица кодов
  - Электронный токен
- ✓ Блокировка на SMS при доступе к счету с нового устройства

Основные виды мошенничества

Кража

НСД к счету пользователя
использование украденных аутентификационных данных

Использование ворованных банковских карт
Взлом ДБО и др. внешних систем

Взлом терминалов и банкоматов

...

Обман

Пирамиды
Волшебные кошельки

Непредоставление товара

Фиктивная работа
Фиктивные акции
Фиктивная благотворительность

Шантаж
- вредоносное ПО
- по телефону
- автомобильные номера

...

Яндекс деньги

Портрет пострадавшего

- ✓ Жертвы обмана страдают из-за собственной наивности

- ✓ Ни одного случая НСД к счету, использующему средства усиленной авторизации *(кроме случаев хранения пользователем ключа во взломанном аккаунте Яндекс.Почты)*

- ✓ Пользователи, пострадавшие от НСД к счету:
  - не имели привязанного телефона
  - подтвердили действия мошенника

Яндекс деньги

Блокировка на SMS при доступе с нового устройства

Обращения пользователей

«Я удалила все… меня муж убьёт!!!! Обещал привезти 1г.гашиша за 1000рублей!!!! Сказал после оплаты яндекс деньги.. Он сразу будет выезжать….. Потом я положила… он написал что не пришло!!! Он мне прислал другой номер счета… другой!! Сказал что он не тот номер написал… и незнает его… ну ядура пошла еще положила.. Я знала что это развод но все равно повелась!!!!»

«Да, вот именно, я сама ввела код. Но там не было информации о никаком переводе. Я была на своей странице Яндекс.Деньги. Я и не собиралась никому ничего переводить.»

«Здравствуйте!!! Это письмо для разработчиков игры, я занемаюсь взломами программ и игр! Пару дней назад я взломал ваш World of Tanks ! Теперь я магу добавить в акаунт за пару минут любые танки, тагже запчасти… ВОТ МОЙ ЯНДЕКС КОШЕЛЕК XXX на него вы в течении 6 дней должны перечислить 15000 рублей. В противном случае я ВЫЛОЖУ ИНФОРМАЦИЮ В СЕТЬ. …. Разайдется как ветер…»

Яндекс деньги

Откуда мы узнаем о мошенничестве

- ✓ **Обращения пользователей**
- ✓ Глобальная репутационная база (Threatmetrix)

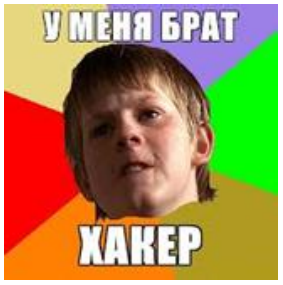
- ✓ Мониторинг упоминаний в интернете
- ✓ Взаимодействие с производителями антивирусного ПО:
  - БД фишинговых сайтов
  - Бот-неты
- ✓ Сеть honey-pot аккаунтов

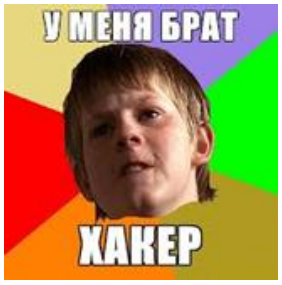
- ✓ Информация от
  - клуба Антидроп
  - правоохранительных органов
  - других платежных систем и сотовых операторов

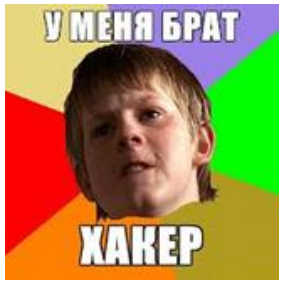
«Пионер»

- ✓ Мелкий обман
- ✓ Пирамиды
- ✓ Фишинг
- ✓ Family fraud
- ✓ Взламывает случайные счета и ворует копейки

- ✓ Не может обойти защитные меры. Ищет готовые схемы и скрипты на форумах. Своих идей нет. Сам жертва разводов. Многочисленны







«Профессионал»

- ✓ Целенаправленная атака на счета с большими суммами
- ✓ Использует средства автоматизации
- ✓ Использует сложные транзитные схемы

- ✓ Самостоятельно исследует систему с целью обхода дополнительных средств защиты

Управление безопасностью

Служба безопасности и противодействия мошенничеству

Отдел ИБ

Аналитическая группа

Претензионный отдел

Отдел взаимодействия с правоохранительными органами

Call центр
Служба технической поддержки

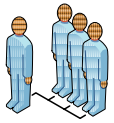
Проектный офис

Портал / Мобильные приложения

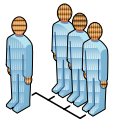
Ядро платежной системы

Разработка аналитических сервисов и средств BI

...



Юристы



ПОД/ФТ 115-ФЗ

Яндекс деньги

Некоторые характеристики поведения мошенников

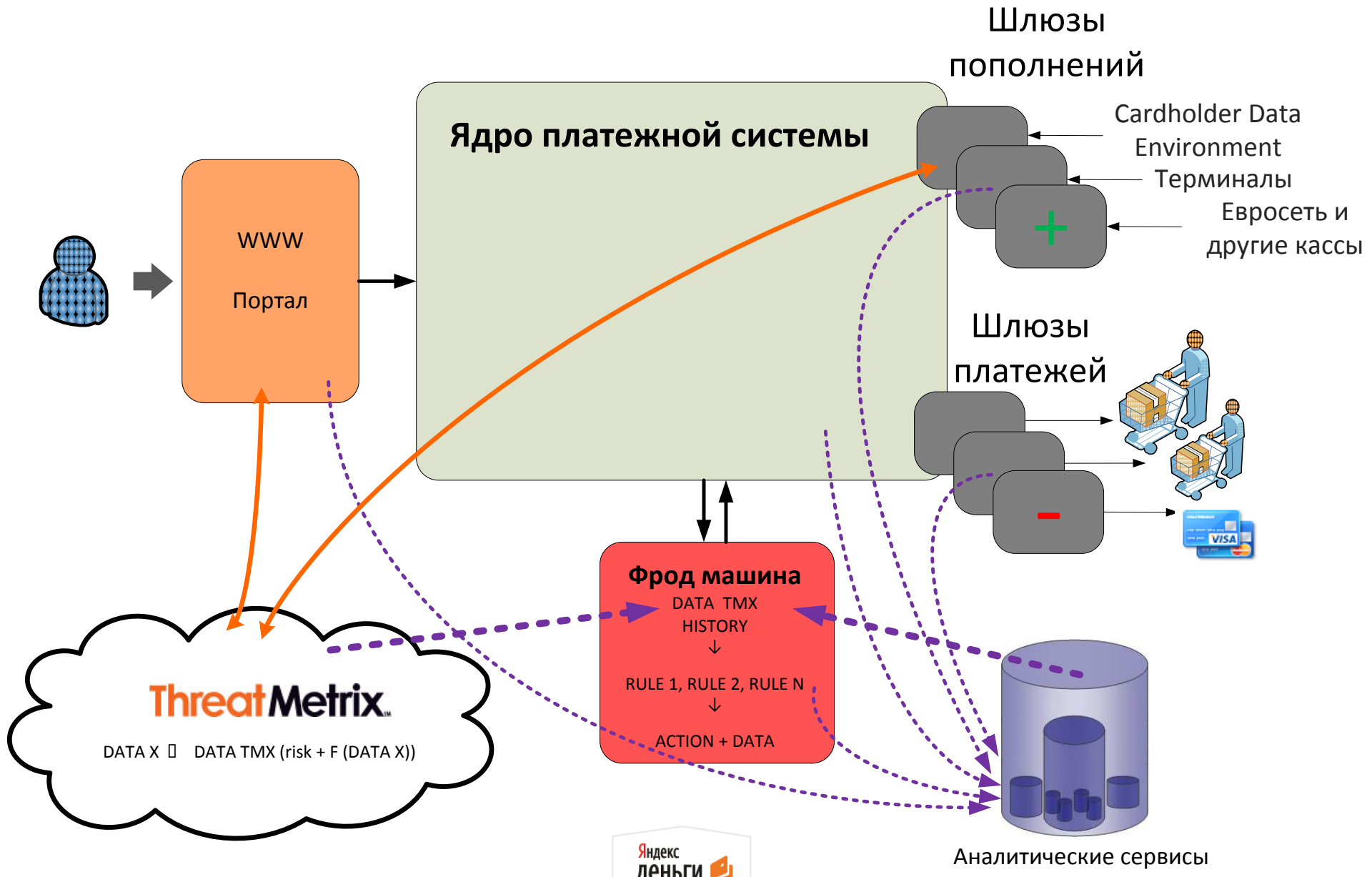
- ✓ Создаёт много «одноразовых» счетов и платит за короткое время

- ✓ Использует GPRS ip pool, proxy, VPN

- ✓ Заходит в систему из разных стран

- ✓ Стремится быстро вывести деньги

Общая архитектура платежной системы



Threatmetrix

Выявление фрода в режиме реального времени на основе идентификации устройств

Этапы профилирования:

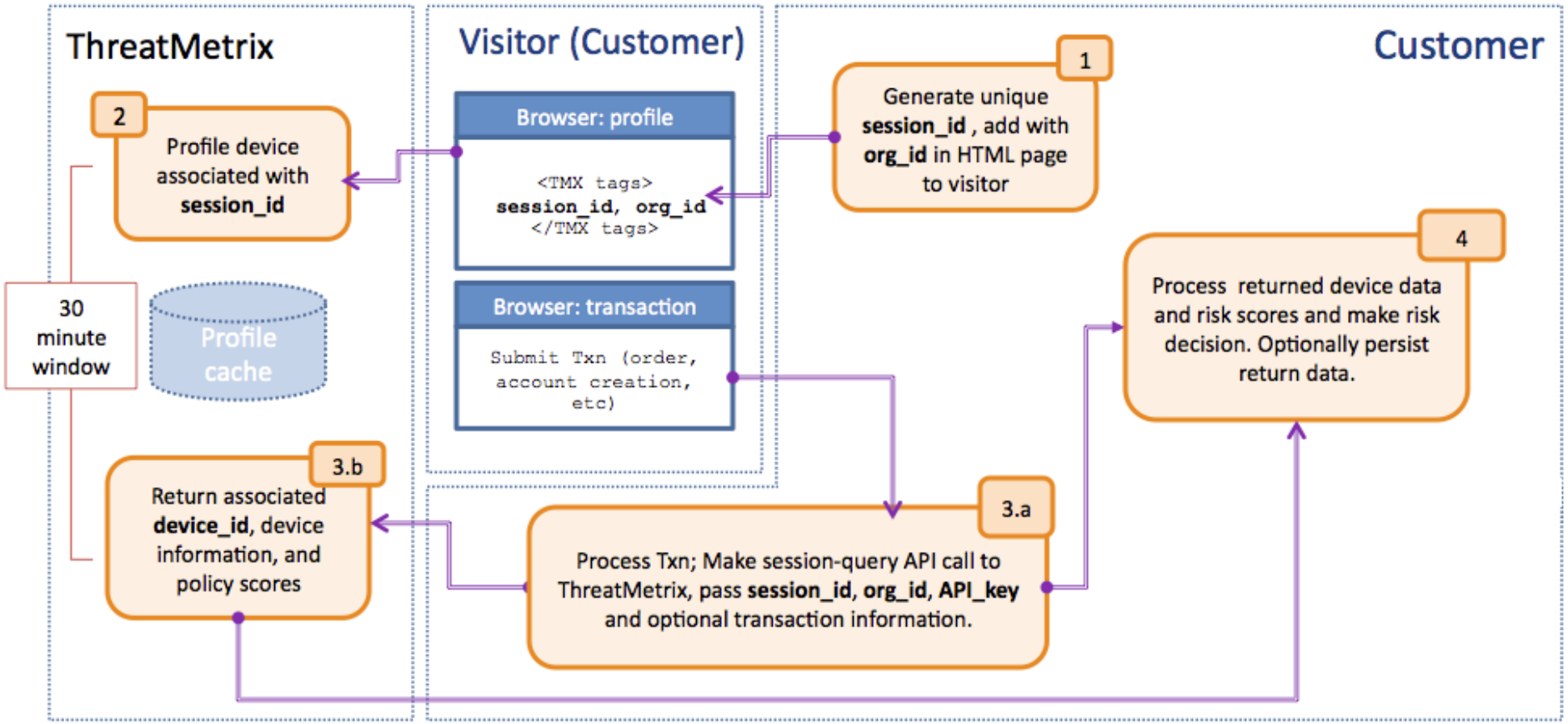
1. Генерация данных - создание объектов и вызов различных скриптов на стороне пользователя
2. Обработка данных провайдером услуги в облаке
3. Запрос, получение и обработка данных компонентами системы

Глобальная репутационная база содержит:

- **уникальный идентификатор устройства**
- IP, ISP + определение proxy, VPN
- PAN
- аккаунты пользователя в других системах
- …

Яндекс деньги

TrustDefender ID
Схема профилирования пользователей



Яндекс деньги

Фрод-машина. Этапы развития

Ручные блокировки по обращениям и результатам мониторинга

Мечты об автоматизации

ФМ2 real-time

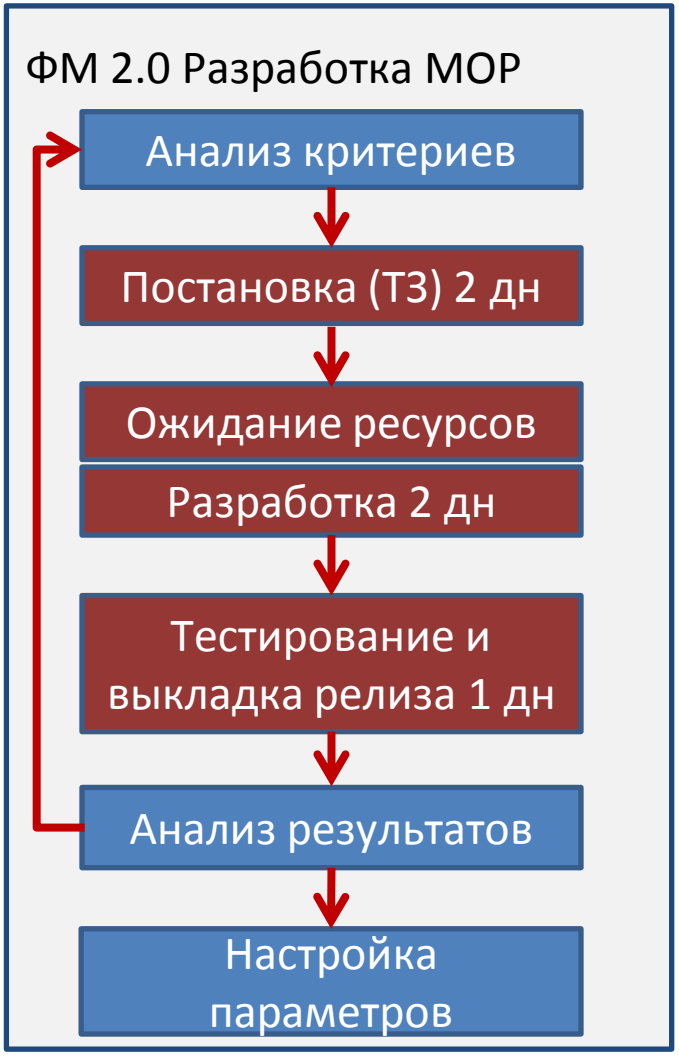
Транзакция → MOP 1, MOP 2, MOP N → ∑R{0÷1}

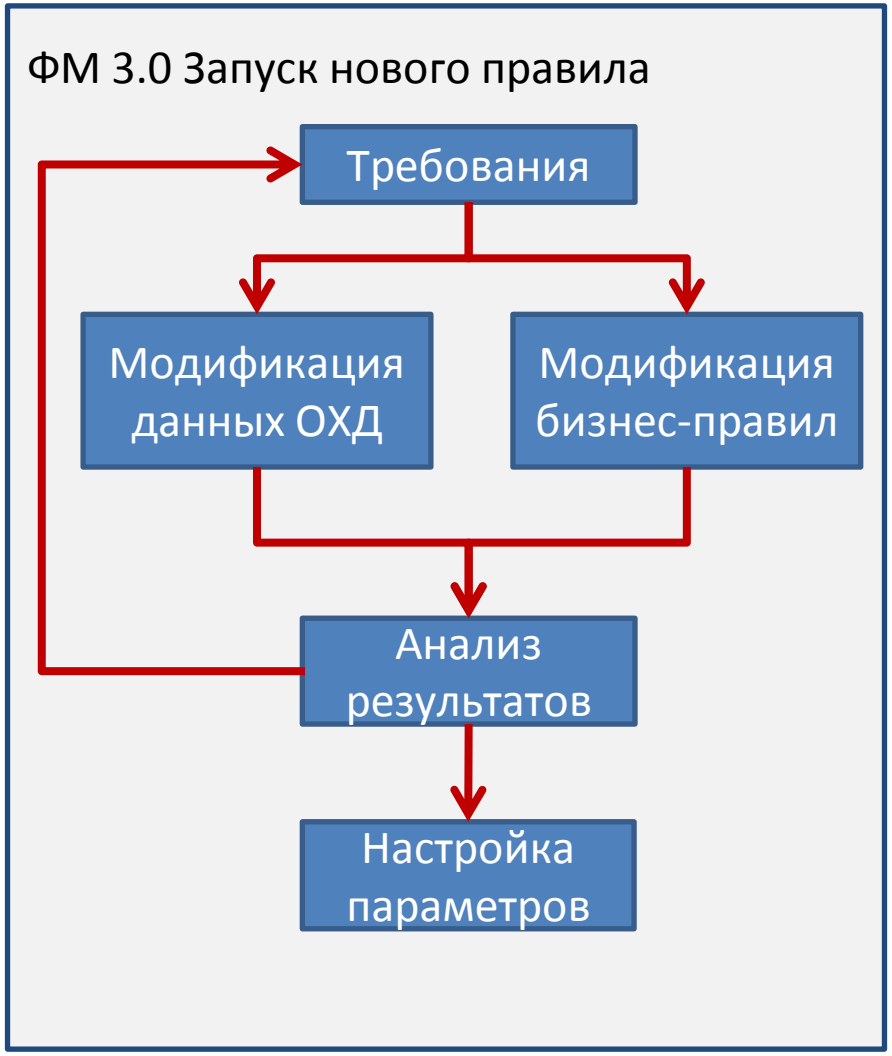
ФМ3 real-time ad-hoc

Оперативный запуск и модификация правил
История поведения (платежи,события)

Яндекс деньги

Внедрение новых эвристик

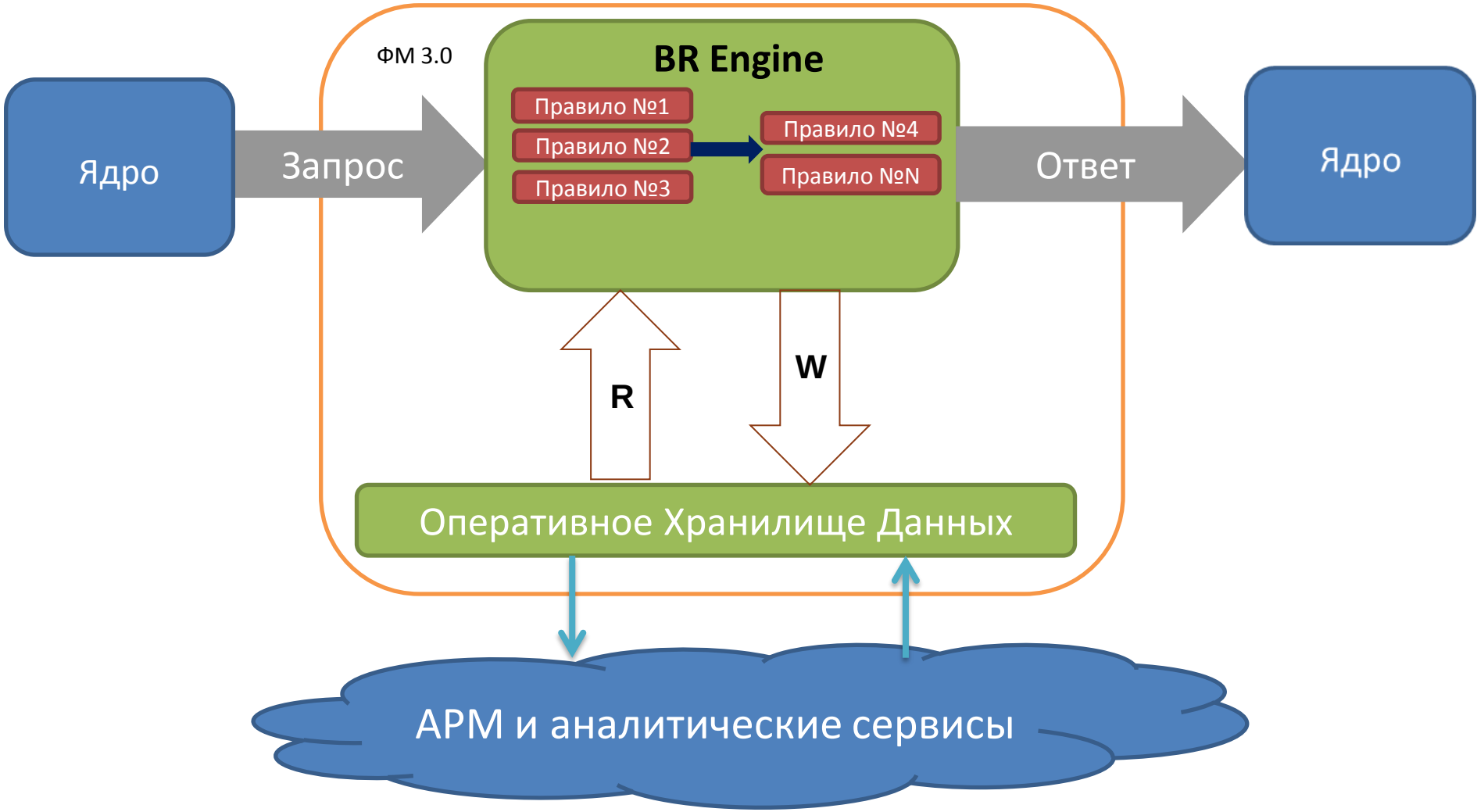




Сравнение BRM систем

Система	Плюсы	Минусы	Цена
Web Rule http://rule.codeeffects.com/	Производительность движка Развитие функциональности в желаемом направлении Быстрое внедрение	Упрощенная реализация концепции Ряд ограничений на бизнес-объекты и структуру правил Недостаточная документация	$
Drools http://www.jboss.org/drools/	Широкие возможности, гибкость Отличная документация Создание правил кодом или через таблицы Excel	Высокие входные трудозатраты из-за сложности системы	$
InRule http://www.inrule.com/	Продвинутый вариант для .NET Гибкий интерфейс создания правил вплоть до плагина в Word	Политика лицензирования	$$
BizTalk BRE http://www.microsoft.com/biztalk/en/us/business-rule-framework.aspx	Интегрируемое решение для SQL Server и .NET Гибкий интерфейс пользователя Встроенная система тестирования	Лишняя функциональность	$$$
...	...	...	...

Фрод-машина. Архитектура решения

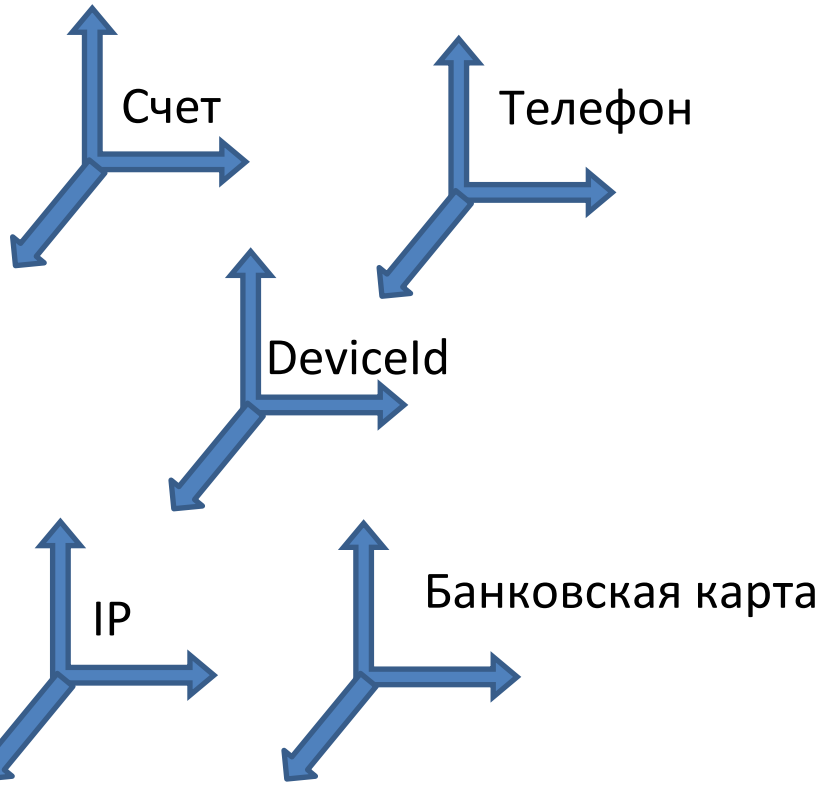


Эволюция модели данных: от скаляра ко множеству динамических объектов

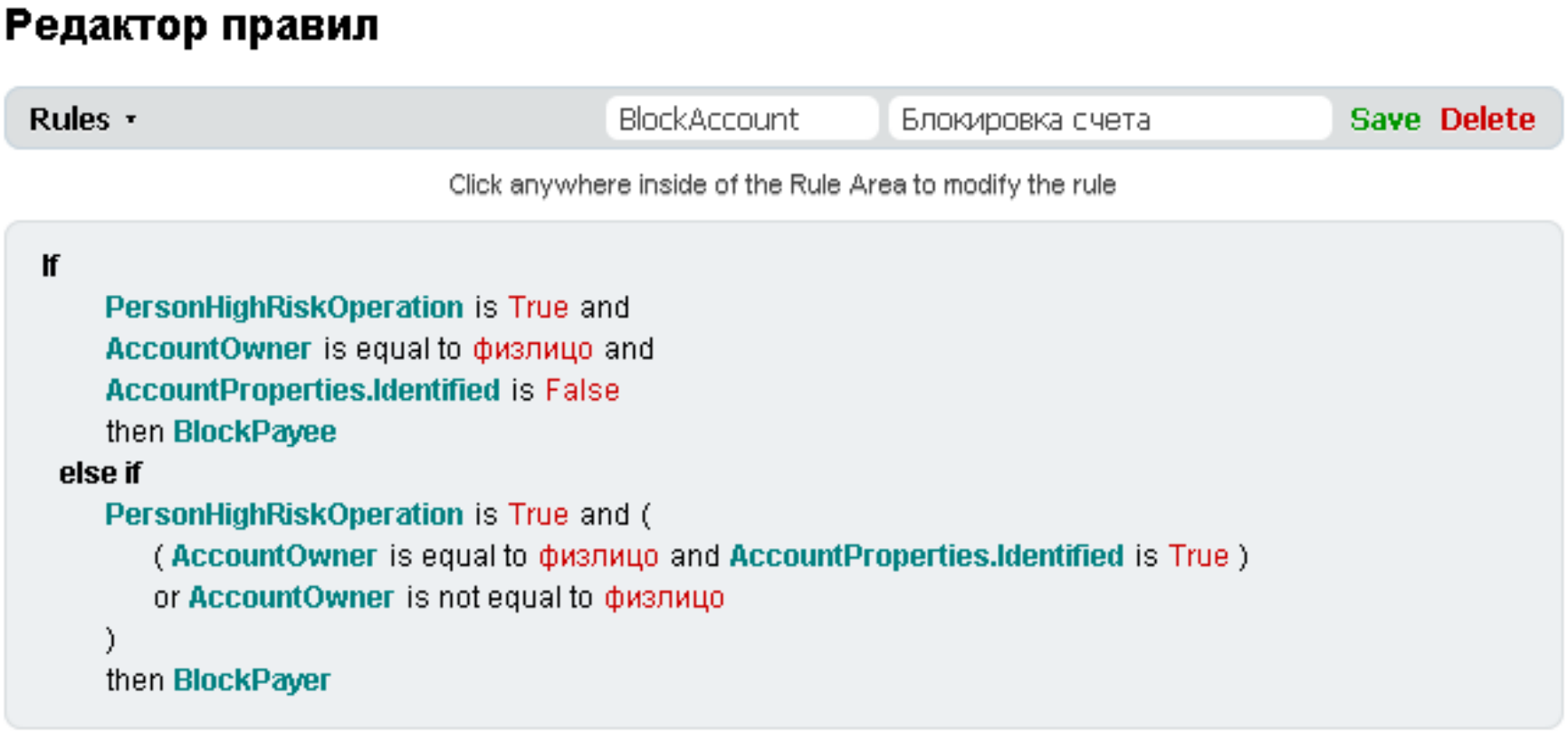
ФМ 2.0

Карма счета

ФМ 3.0



Интерфейс редактора правил



Яндекс деньги

Фрод-машина. Условные примеры правил

Удачные правила:

динамика разных стран и ISP

управляемая лавина при обработке chargeback – блокировка связанных объектов:

- ✓ идентификаторов устройств,
- ✓ телефонов, за которые платил счет,
- ✓ счета, которые пытались использовать ту же карту
- ✓ …

Неудачное правило:

мгновенный вывод денег на карту после пополнения счета с другой карты оказался нормальным пользовательским сценарием для p2p платежа.

Правило не было запущено в боевой режим.

Развитие… Новые правила и данные

Отдельные виды мошенничества удалось заметно сократить или свести к нулю

Дальнейшее накопление данных по большему количеству объектов позволит строить более эффективные правила

Спасибо !!1

armarchuk@yamoney.ru

Яндекс деньги