Афанасьев Сергей
КБ «Ренессанс Кредит»
г. Москва

Антифрод в розничном банкинге

Практический семинар

Минск, 10 августа 2018 г.

План семинара

Часть 1 Организация антифрода

- Организация антифрода
- Генезис мошенничества
- Формула мошенничества

Часть 2 Кейсы и аналитика

- Мошеннические кейсы
- Транзакционный антифрод

Часть 3 ИИ в антифроде

- Предиктивная фрод-аналитика
- Нейронные сети в антифроде
- Уязвимости нейронных сетей

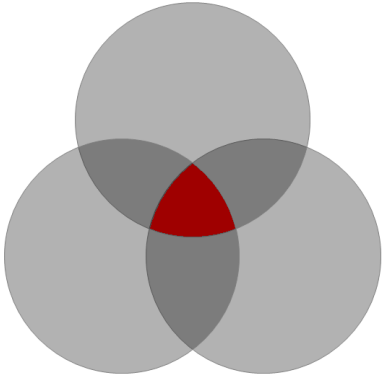
10:00	Начинаем
11:40-12:00	Кофе-брейк
13:30-14:20	Обед
15:50:16:10	Кофе-брейк
18:00	Заканчиваем

Вопросы приветствуются!

Часть 1.1

Организация антифрода в банке

Антифрод в банке:



Аудит

Сплошная и выборочная проверки, документальная ревизия, аналитическая проверка, инспектирование и т.д.

Криминалистика

Сбор улик, задержания, допросы, очные ставки, обыски, криминалистическая экспертиза и пр.

Аналитика

Поиск аномалий, выявление fraud-концентраций, разработка правил и моделей, финансовая оценка и др.

Аудит

R.H. Montgomery

(1872–1953)

Автор книги «Аудит Монтгомери»

(первое название «Аудит: теория и практика»)

В своих работах Монтгомери высказал мысль, что аудит - это выяснение фактических финансовых условий и величины доходов предприятия в интересах его собственников, пользователей, банкиров и других инвесторов. Старый взгляд, согласно которому задача аудитора сводилась к раскрытию ошибок и искоренению злоупотреблений, был отброшен. До сих пор аудит выполняется не ради абстрактной идеи, а в интересах самой организации.

Криминалистика

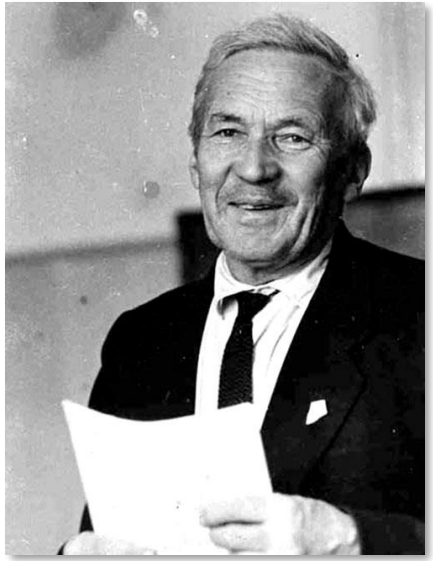
E.H. Sutherland

(1883–1950)

Автор теории дифференциальных связей:

«Контактируя с другими людьми, каждый человек подвергается определенному воздействию, которое может определить его дальнейшие поступки. Преступное или законопослушное поведение человека определяется характером его ближайшей среды. Если в этой среде преобладают преступные элементы, то человек усваивает их ценности и модели поведения, обучается этим моделям и становится преступником.»

Аналитика



А.Н. Колмогоров

(1903–1987)

Один из основоположников современной теории вероятностей

В дискуссии на тему **«Может ли машина мыслить?»** в 1964 году заявил:

«Принципиальная возможность создания полноценных живых существ, построенных полностью на дискретных (цифровых) механизмах переработки информации и управления, не противоречит принципам материалистической диалектики.»

Типы инструментов

Директивные

Детективные

Превентивные

Бывают исключения

Слабые превентивные

Сильные директивные

Задание 1.

Приведите примеры антифрод-мероприятий по типу контроля, используемых в вашем Банке

Директивные	Детективные	Превентивные
1.	1.	1.
2.	2.	2.
3.	3.	3.
4.	4.	4.
5.	5.	5.

Три линии защиты

Front	Сотрудники банковских офисов Кредитные представители
Middle	Андеррайтеры Колл-центр Бэк-офис
Back	Служба безопасности Департамент рисков Внутренний аудит и СВК

Задание 2.

Приведите примеры антифрод-мероприятий, используемых в вашем Банке на разных уровнях

Front (Офисы продаж, Агенты)	Middle (Андеррайтинг, Бэк-офис)	Back (СБ, Риски)
1.	1.	1.
2.	2.	2.
3.	3.	3.
4.	4.	4.
5.	5.	5.

Бизнес-процессы

Персонал
- Проверка сотрудников
- Обучение
- Организация процессов
- Мотивационная схема
- Мониторинг деятельности

Клиенты
- Идентификация клиента
- Визуальная оценка
- Андеррайтинг

Партнеры
- Партнерский договор
- Проверка партнеров
- Мониторинг деятельности

Процессы
- Аудит процессов
- Согласование инициатив
- Автоматизация процессов

Аналитика

Репорты
- Fraud Report
- Concentration Report
- Block Report

Анализ портфеля
- Анализ fraud-сегментов
- Исследования (FTI)
- Ad hoc

Модели
- Предиктивная аналитика
- Разработка правил
- Machine Learning

Оценка
- CBA антифрод-процессов
- CBA антифрод-систем
- Оценка fraud-потерь

Антифрод-системы

Внутренние системы
- Warning System
- AFS (local) и др.
- Black-lists
- Биометрия

Внешние сервисы
- FPS, AFS (межбанк)
- FPS.Bio
- Телеком (Мегафон и др.)
- Соцсети (Mail.ru и др.)
- Cookie (Rambler и др.)
- СПАРК, Контур.Фокус и др.
- Банкроты (Interfax)

Гос. сервисы
- ФМС
- ФССП
- ПФР
- ФНС

Организация процессов

1. Ограничение полномочий

Сотрудник наделяется только теми полномочиями, которые необходимы для выполнения его рабочих обязанностей (подписание чеков, выдача кредитов, оформление документов, подписание приказов и т.д.) Избыточные полномочия не предоставляются.

2. Конфликт интересов

Организационный конфликт интересов подразумевает выполнение одним сотрудником конфликтующих рабочих обязанностей (например, функции продаж и функции риск-менеджмента). Для минимизации рисков внутреннего мошенничества организационная структура в банке должна быть выстроена таким образом, чтобы количество конфликтующих рабочих функций внутри каждого подразделения было минимальным.

3. Разделение труда

Разделение труда позволяет ограничить полномочия сотрудников и доступы к ИТ-системам банка. Разделение труда хорошо подходит для конвейерных бизнес-процессов, например, для процесса выдачи кредитов.

4. Разграничение доступов

Сотруднику предоставляются только те доступы в ИТ-системы банка, которые необходимы для выполнения его рабочих обязанностей.

5. Автоматизация

Автоматизация снижает влияние человеческого фактора на банковские процессы, ограничивает полномочия и доступы для сотрудников, то есть позволяет обезопасить банк от внешних и внутренних угроз.

6. Принцип «четырех глаз»

Согласно принципу "четырех глаз" для подтверждения каждой значимой операции требуется согласование минимум двух сотрудников. Использование принципа "четырех глаз" снижает риски мошенничества, поскольку для совершения противоправных действий требуется сговор всех сотрудников, участвующих в согласовании.

7. Принцип «большого брата»

Согласно принципу "Большого брата" за действиями каждого сотрудника должен кто-то наблюдать. Функцию "большого брата" может выполнять второй сотрудник, а также технические решения, такие как - видеонаблюдение, запись телефонных звонков, логгирование операций в ИТ-системах и др. Рассылка информационных материалов и публикации в СМИ о раскрытых фактах мошенничества также выполняют эту функцию.

8. Текущий и последующий контроль

Текущий и последующий контроль являются модификациями принципов "четырех глаз" и "большого брата". Текущий и последующий контроль может осуществляться по выборочным операциям. Например, случайную выборку кредитных заявок можно отправлять на дополнительные проверки андеррайтинга (текущий контроль), или сотрудники бэк-офиса могут проверять комплекты документов на признаки совершения мошеннических действий (последующий контроль).

9. Метод «тайный покупатель»

Согласно методу "тайный покупатель" специально подготовленные люди осуществляют проверки под видом потенциальных/реальных клиентов. В целях снижения фрод-рисков проверки проводят сотрудники безопасности банка, которые фиксируют нарушения и мошеннические действия со стороны сотрудников.

10. Ротация персонала

Ротация персонала между офисами банка позволяет снизить число мошеннических сговоров как между сотрудниками банка, так и с внешними преступными группировками.

11. Ограничение доступов в нерабочее время

Ограничив доступы сотрудников к рабочему месту и к ИТ-системам банка в нерабочее время, можно снизить уровень внутреннего мошенничества, уменьшив возможности для совершения противоправных действий в условиях отсутствия в офисе посторонних наблюдателей. Для возможности сверхурочной работы необходимо получить согласование от руководителя и от сотрудников службы безопасности банка.

Бизнес-кейс 1

Карточная афера

Чек-лист уязвимостей

Офисы (БО)

Обслуживание клиента
- Изменение ПД;
- Принцип «Четырех глаз»;
- Ограничение полномочий;
- Пост-контроль

Доступы к ПД
- Фронт-системы;
- Списки (файлы);
- Досье клиентов

Доступы к ПК сотрудников
- Контроль передачи «Логинов-паролей (подтверждение смс-кодом, биометрия и т.п.);
- Доступы в рабочее помещение (по пропуску/биометрии)

Колл-центр

Изменение ПД
- Проверки КЦ

Аутентификация клиента
- ФИО+ДР;
- Проверенный моб. тел.;
- Кодовое слово

Обработка входящих
- Обращение клиента («операцию не совершал»)

Бизнес-процессы

Продукты/Процессы
- Проработка слабых мест продукта/процесса на этапе согласования

Персонал:
- Обучение;
- Принцип «неотвратимости наказания»

Антифрод-системы

Биометрия
- Фотографирование клиентов и выявление мошенничества

Fraud-правила
- Скачки продаж;
- Круглые суммы;
- Время оформления кредита и время вывода средств;
- Пересечения клиентских данных (мобильные телефоны);
- Использование данных логов/куков;
- Настройка правил на раннее обнаружение внутреннего фрода

Удаленные доступы

Тонкие клиенты
- Ограничение доступов в нерабочее время;
- Дополнительный контроль удаленных операций

Прочее

Оповещение клиента
- Отправка смс о смене ПД на старый номер мобильного телефона

Кофе?

Часть 1.2

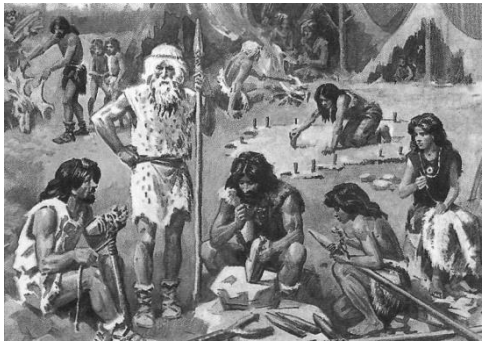
Генезис мошенничества

- Почему Вы грабите банки?
- Потому что там деньги

Вилли Саттон
(грабитель банков)

История развития мошенничества

Первобытно-общинный строй



Появление мошенничества уходит корнями в доисторическую эпоху, когда наши предки, спасая себя от голода, **прятали друг от друга еду**, прибегая к обману своих соплеменников.

Классовое общество

При переходе к классовому строю появились первые собственники и неимущие. Владение имуществом подтверждалось наличием документов на право собственности. Так появился один из древнейших способов мошенничества - **подделка документов**.

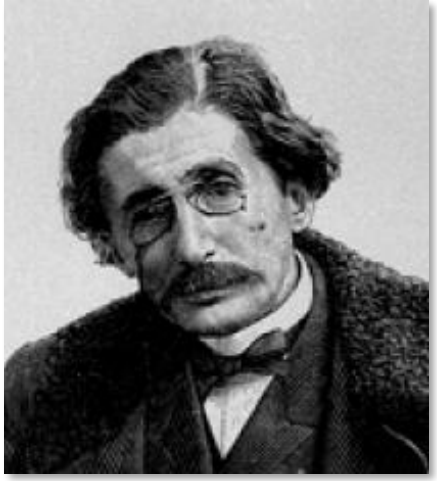
Российская история

Иностранцы часто жаловались на плутовство русских торговцев. Практиковалась **подделка товара**, продажа подкрашенного старого меха под видом нового, или подмешивание в товар высокого качества низкосортной продукции.

Определение мошенничества

Толковый словарь Ожегова	Мошенничество - это обман, жульнические действия с корыстной целью
Уголовный Кодекс РФ (159-УК)	Мошенничество - это хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием
Association of Certified Fraud Examiners (ACFE)	Мошенничество в профессиональной деятельности - это использование своего положения в целях личного обогащения путем преднамеренного неэффективного использования ресурсов нанимающей организации
Банковское определение	Финансовое мошенничество - это любое умышленное действие сотрудника, партнера, клиента или третьего лица, которое совершено с целью личного обогащения и в результате которого финансовая организация терпит убытки

Теория подражаний



Габриель Тард

(1843–1904)

Основой развития общества выступает социально-коммуникационная деятельность индивидов в форме подражания (имитации). Процессы имитации и копирования поведения способствуют сохранению целостности общества, а также позволяют обществу развиваться, за счет изобретений и нововведений от авторитетов, которым подражают.

Теория дифференциальных связей

Эдвин Сазерленд

(1883–1950)

Если в окружении индивида преобладают преступники, то он усваивает их ценности и модели поведения и сам становится преступником. Сила и влияние связей зависят от характеристик общения индивида с преступниками:

- **Частота** – как часто и регулярно;
- **Продолжительность** – как давно и насколько долго;
- **Очередность** – с какого возраста.

Соответственно наиболее сильное влияние на человека обычно оказывают его родственники.

Треугольник мошенничества

Дональд Кресси

(1919–1987)

Причины, необходимые человеку для совершения мошеннических действий:

- **Мотивация** – человек должен испытывать давление (финансовое или иное);
- **Возможность** – у человека должна быть возможность совершить и некоторое время скрывать акт мошенничества;
- **Обоснование** – человек должен оправдать свое действие перед самим собой.

Задание 3.

Какие антифрод-мероприятия необходимы, чтобы снизить мотивацию, возможность и обоснование?

Мотивация	Возможность	Обоснование
1.	1.	1.
2.	2.	2.
3.	3.	3.
4.	4.	4.

Треугольник Кресси по Альбрехту

Мотивация

1. Финансовое давление;
2. Давление пороков и пагубных пристрастий;
3. Давление, связанное с работой;
4. Прочие виды давления внешних обстоятельств

Возможность

1. Отсутствие или недостаточность мер контроля, позволяющих предупредить/выявить мошенничество;
2. Невозможность или неспособность оценить качество выполненной работы;
3. Отсутствие производственной дисциплины;
4. Предоставление искаженной или недостаточной информации;
5. Равнодушие к происходящему со стороны начальства и/или коллег;
6. Отсутствие ревизий и/или аудиторских проверок;

---

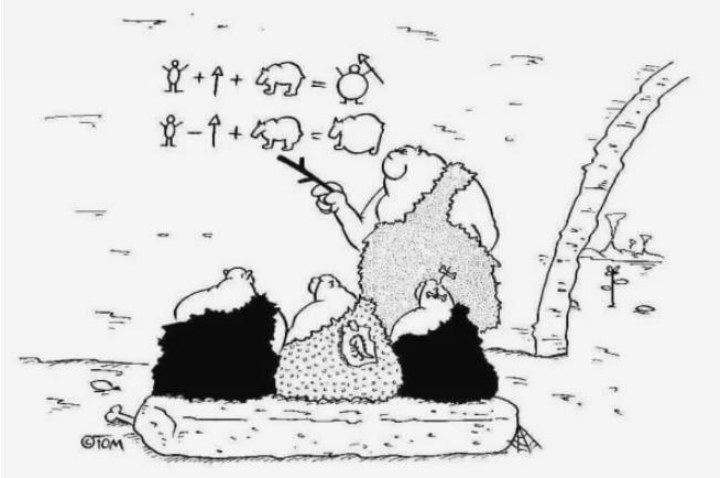
7. Расширенные полномочия;
8. Несовершенство бизнес-процессов и ИТ-систем;
9. Особенности менталитета, в частности круговая порука в коллективе;
10. Отсутствие принципа неотвратимости наказания

Обоснование

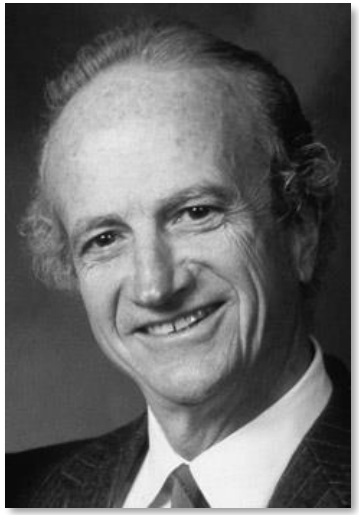
1. Моя фирма или организация мне задолжала;
2. Я одолжу на время деньги и сразу же их верну;
3. От этого хуже никому не будет;
4. Я заслуживаю большего;
5. Это направлено на благие цели;
6. Все воруют, и я ворую;
7. Чем-то надо жертвовать — или своей репутацией, или собой;
8. Я не знал, что делаю что-то противозаконное

Часть 1.3

Формула мошенничества



Экономика преступления и наказания



Гэри Беккер

(1930–2014)

Преступность можно рассматривать как специфичный рынок, на котором существует спрос и предложение. Предложение определяется готовностью преступников совершать правонарушения и зависит от таких факторов, как строгость наказания или легальных альтернатив заработка. Спрос формируется из потребности людей в результатах нелегальной деятельности, например, спрос на наркотики или краденое имущество.

Формула Беккера

$$(1-\pi)U(W_C)-\pi S > U(W_L)$$

π – вероятность быть пойманным;

U( ) – функция полезности индивида;

S – санкции, понесённые в случае поимки (например, штраф);

W_C и W_L – соответственно доходы от преступной и легальной деятельности.

Левая часть неравенства характеризует то, что связано с преступностью, правая - полезность от законного заработка. Логично, что если неравенство будет выполнено, индивид при прочих равных предпочтёт нарушить закон.

Основные факторы образования равновесного уровня преступности:

- Готовность людей совершать преступления ради выгоды: вероятность ареста, осуждения и наказания; меры наказания; доходы от альтернативных видов легальной и нелегальной деятельности; риск безработицы; изначальный уровень благосостояния.
- Поведение потенциальных жертв и потребителей нелегальных товаров: величина спроса на нелегальные товары; спрос на средства защиты (сейфы, сигнализацию, охрану).
- Меры, принимаемые государством: осуществляя поимку преступников, государство вводит своеобразный «налог» на преступные виды деятельности, выражаемые в риске быть пойманным.

Формула мошенничества

Похищенная сумма | Затраты мошенника | Вероятность поимки | Возвращенные средства | Санкции после поимки

$$FP = FE - FC - PFD \times (FE \times LGFD + CSE \times CSR)$$

Прибыль от мошенничества (*Fraud Profit – **FP***) – прибыль, которую ожидает получить мошенник, учитывая свои риски и издержки;

Подверженность риску мошенничества (*Fraud Exposure – **FE***) – экономическая оценка похищенных мошенниками активов;

Стоимость трудозатрат мошенника (*Fraud Costs – **FC***) – складывается из стоимости потраченного времени, вложенных инвестиций и других расходов мошенника;

Вероятность раскрытия мошенничества (*Probability Fraud Detection – **PFD***) – оценивается путем статистического анализа раскрытых и нераскрытых мошеннических фактов;

Уровень возвращенных средств (*Loss Given Fraud Detection – **LGFD***) – доля возвращенных средств, в случае раскрытия мошенничества;

Подверженность уголовному наказанию (*Criminal Sanction Exposure – **CSE***) – стоимость максимальных личных потерь мошенника вследствие уголовного наказания (штраф, потеря оплачиваемой работы на период отбывания наказания, потеря репутации и т. д.);

Степень жесткости наказания (*Criminal Sanction Ratio – **CSR***) – уровень личных потерь, понесенных вследствие смягчения наказания (штраф вместо уголовного наказания, условный или неполный срок и т.д.).

Бизнес-кейс 2

Мошенничество в ФК «Открытие»

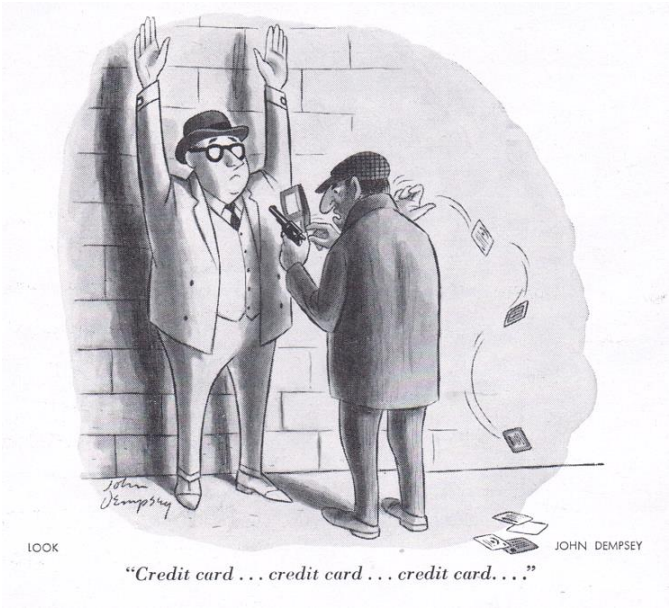
▪ Стоимость затрат на мошенничество (*Fraud Costs*): затраты на сделку «приманку» $2,45 млн, т.е. по 0,8 млн на каждого из трех участников;
▪ Сумма похищенных средств (*Fraud Exposure*): $175 млн ($25 млн гарант + $150 млн прибыль от сделки), т.е. по $58,3 млн на участника;
▪ Уровень возвращенных средств (*Loss Given Fraud Detection*): 114%, т.к. по решению суда мошенники должны выплатить открытию $200 млн с учетом процентов и судебных издержек;
▪ Вероятность раскрытия мошенничества (*Probability Fraud Detection*): предположим PFD=33% (наверняка сами мошенники этот показатель сильно занижали);
▪ Подверженность уголовному наказанию (*Criminal Sanction Exposure*) оценивается как максимальные личные потери, в случае раскрытия мошенничества. Определим личные потери через доход, который мошенники могли бы заработать легально по специальности, если бы не попали в тюрьму.
- Доход трейдеров в 2010-2011 гг. с бонусами составлял $1-2 млн в год.
- Наказание по 159-УК РФ до 10 лет лишения свободы.
Если бы мошенники остались на свободе, то за 10 лет каждый мог бы заработать по $10-20 млн (оптимистичный прогноз). Также необходимо учитывать, что после отбывания наказания репутация мошенников скорее всего будет разрушена и они вряд ли смогут найти работу с достойным заработком. Для простоты расчетов будем считать, что подверженность уголовному наказанию равна нижней границе оценки, т.е. $10 млн. для каждого члена мошеннической группы;
▪ Степень жесткости наказания (*Criminal Sanction Ratio*) оценивается как отношение реального срока к максимально возможному. Предположим, что при условии полного возмещения ущерба, мошенникам дали по 3 года. Это значит, что *CSR* составил 30% (от максимального срока 10 лет);

FP = $58,4 млн – $0,8 млн – 0,33 * ($58,4 млн * 1,14 – $10 млн * 0,3) = $34,6 млн

Переменная	Антифрод-мероприятия
FC Стоимость затрат мошенника	▪ Ограничение полномочий ▪ Разграничение прав доступа к ИТ-системам ▪ Принцип «четырех глаз» (контрольные подписи, согласования) ▪ Функция «Большого брата» (видеонаблюдение, записи телефонных звонков, логирование и т.д.) ▪ Текущий и последующий контроль (верификация и андеррайтинг, проверки бэк-офиса и др.) ▪ Ротация персонала ▪ Ограничение доступов в нерабочее время
FE Похищенные средства	▪ Лимитирование операций: по сделкам на крупные чеки вводить дополнительный контроль
PFD Вероятность раскрытия мошенничества	▪ Эффективная коммуникация о раскрытых фактах мошенничества ▪ Внедрение процесса и систем выявления внутреннего мошенничества.
LGFD Доля возврата	
CSE Потери вследствие понесенного наказания	▪ У сотрудников с доступом к крупным сделкам должна быть достойная финансовая компенсация: оклады, бонусы, опционы ▪ Проверка кандидатов на высокий уровень социальной ответственности (наличие семьи, детей, друзей), а также создание высокого уровня социальной ответственности (корп. культура)
CSR Смягчение наказания	▪ Не идти на сделки и заводить уголовные дела. ▪ Добиваться максимальных сроков наказания.

Часть 2.1

Аналитика транзакционного мошенничества



Задание 4.

Приведите примеры схем транзакционного мошенничества с картами и интернет-платежами

1.

2.

3.

4.

5.

6.

7.

8.

9.

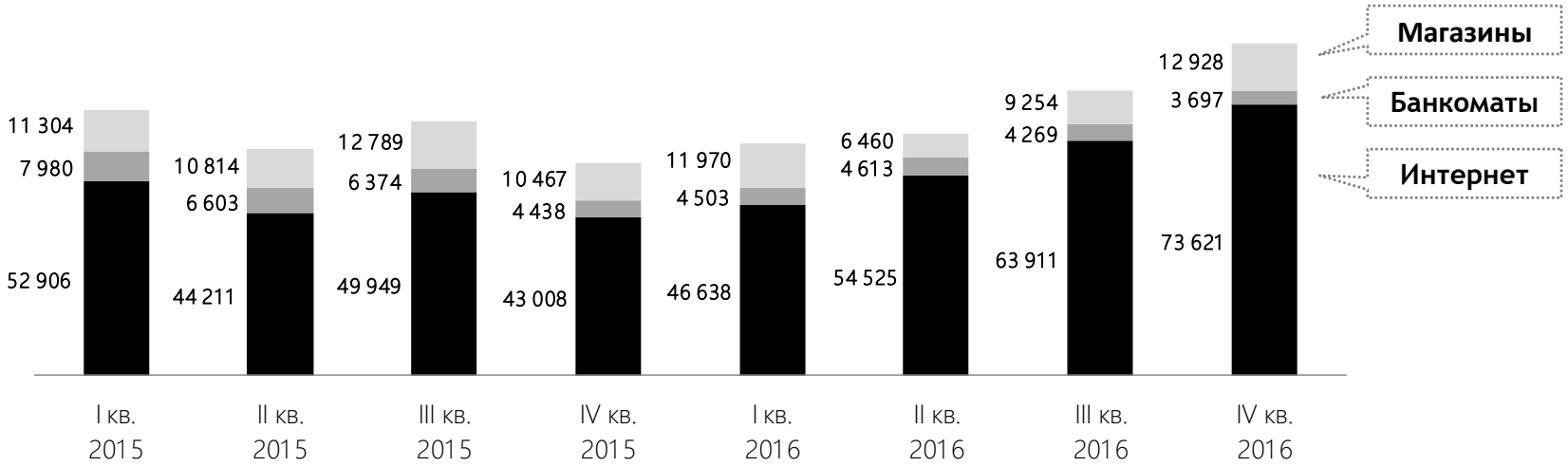
10.

11.

12.

Количество фрод-транзакций растет

Количество несанкционированных операций с использованием платежных карт в разрезе места их совершения



Количество несанкционированных операций, совершенных в организациях торговли (услуг), ед.

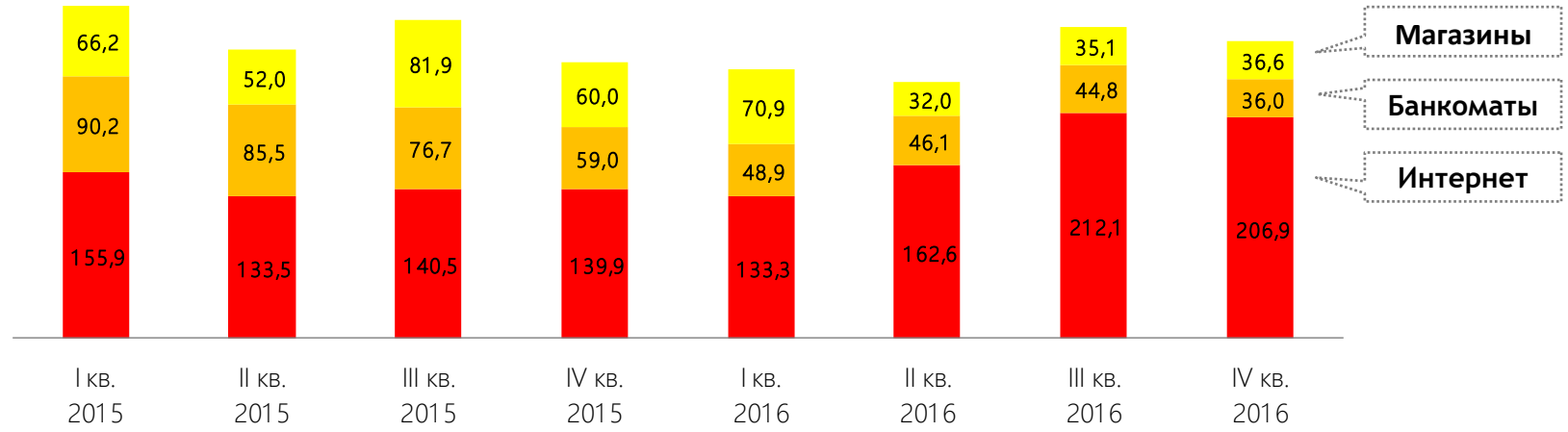
Количество несанкционированных операций, совершенных посредством банкоматов, ед.

Количество несанкционированных операций, совершенных посредством сети Интернет и мобильных устройств, в том числе интернет-банка, ед.

Источник: www.cbr.ru

Растет объем фрода в интернете

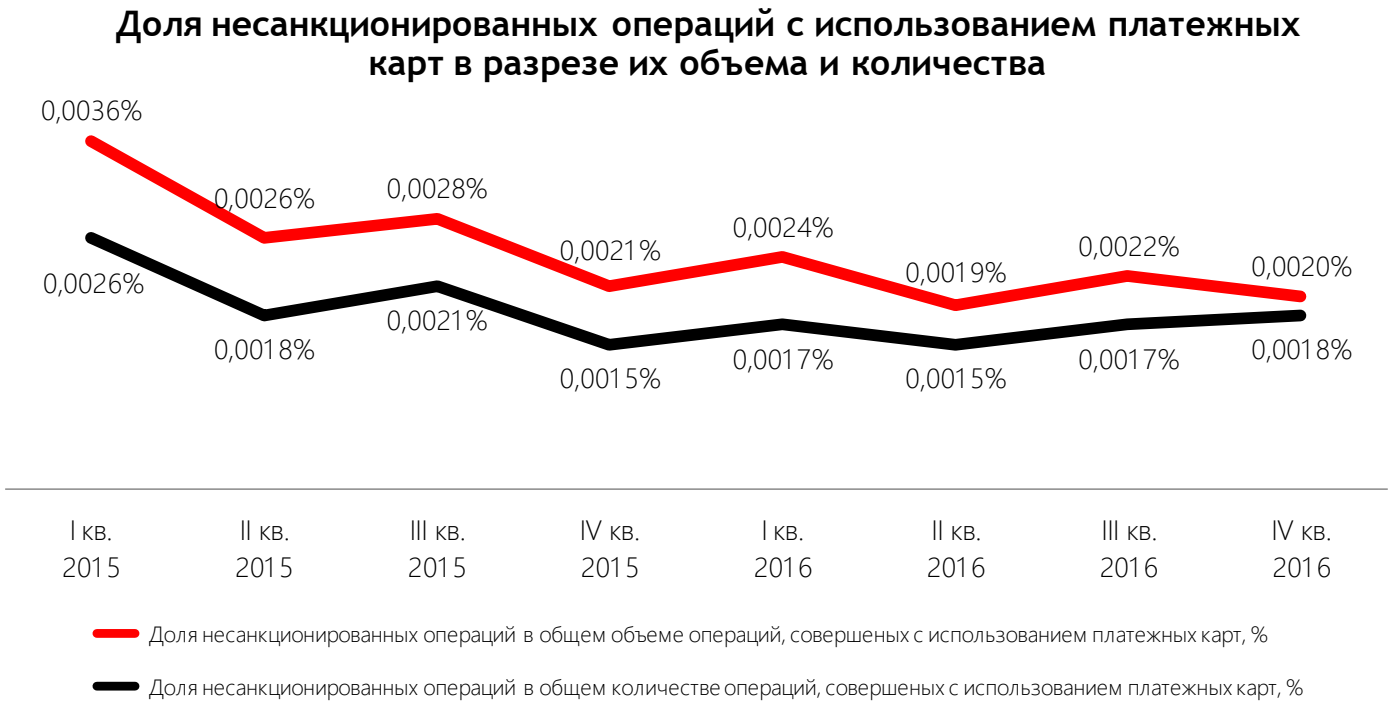
Объем несанкционированных операций с использованием платежных карт в разрезе места их совершения



- Объем несанкционированных операций, совершенных в организациях торговли (услуг), млн руб.
- Объем несанкционированных операций, совершенных посредством банкоматов, млн руб.
- Объем несанкционированных операций, совершенных посредством сети Интернет и мобильных устройств, в том числе интернет-банка, млн руб.

Источник: www.cbr.ru

Уровень карточного фрода падает



Источник: www.cbr.ru

Россия невыгодна для мошенников

Согласно исследованию компании FICO в России пользоваться картой в 3,7-4,7 раз безопаснее, чем в Англии, Франции и Греции – европейских лидерах по уровню карточного мошенничества.

По данным ЦБ средний объем транзакций за 2010 год в пересчете на одну российскую карту составил 2 529$. Во Франции и Англии данные показатели составили 7 325$ и 6 582$ соответственно, т.е. в 2,5-3 раза больше.

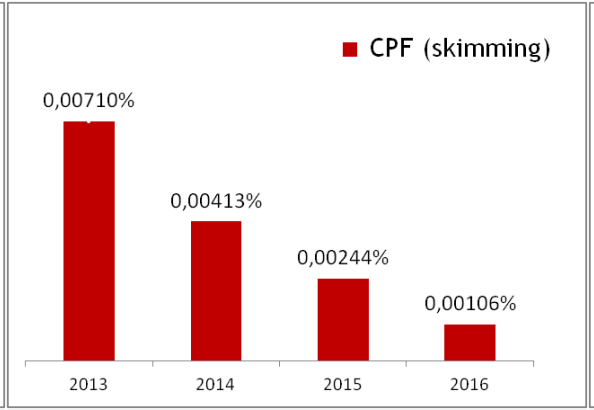
Если учитывать соотношение POS и CASH-транзакций, то можно оценить, что суточные остатки на картах французов и англичан в 4-4,5 раз выше, чем на российских. Это значит, что воровать с европейских карточек в несколько раз выгоднее, чем с российских.

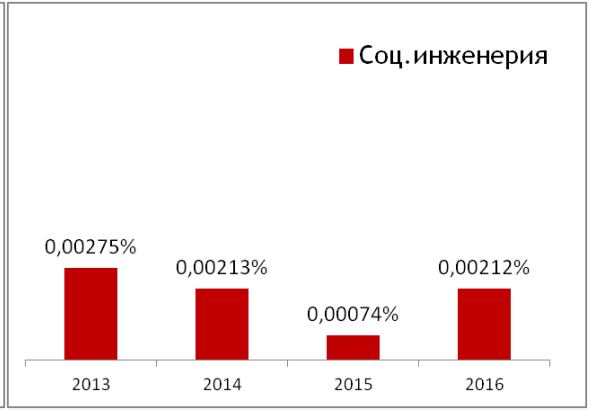
2010 год	Кол-во транзакций (млн)		Сумма (млрд $)			CASH/POS	Средний чек		Эмиссия карт (млн)	Средние траты в год (на 1 карту)	Население (млн чел.)	Ср. траты в год на человека
	POS	CASH	POS	CASH	СУММ		POS	CASH				
Англия	8 425	2 786	661	298	959	0,5	$78	$344	146	$6 582	62	$15 468
Франция	7 147	1 601	456	163	619	0,4	$64	$387	85	$7 325	65	$9 523
Германия	2 506	2 040	200	417	617	2,1	$80	$302	127	$4 854	82	$7 524
Бразилия	6 249	2 936	277	420	697	1,5	$44	$237			201	$3 468
Россия	507	2 001	28	321	349	11,5	$55	$174	138	$2 529	139	$2 511
Россия (2016)	11 530	4 538	184	576	759	3,1	$16	$167	255	$2 978	146	$5 202
Индия	484	4 228	21	242	263	11,5	$43	$62			1173	$224
Китай	4 849	8 358	1 540	1 357	2 897	0,9	$318	$347			1330	$2 178

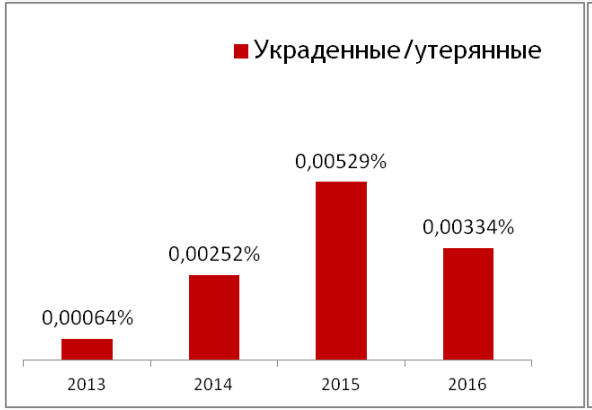
Источник: www.cbr.ru

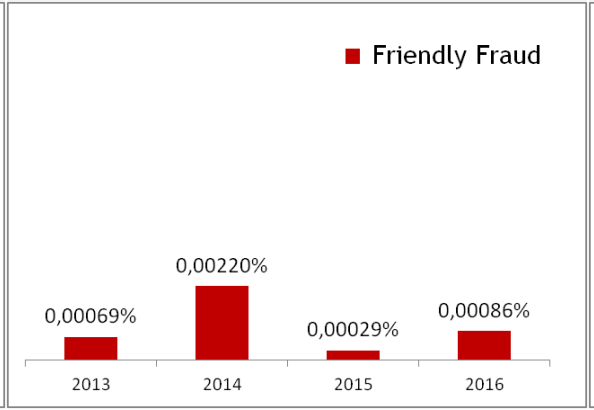
Тренды карточного мошенничества

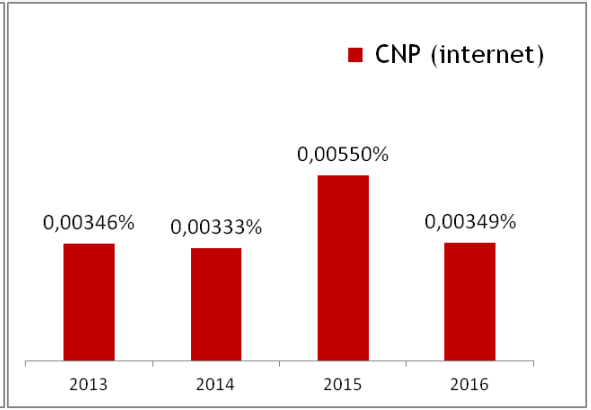
- Скимминг упал в 7 раз благодаря переходу на EMV-чипы;
- Социальная инженерия растет и переходит в интернет;
- Фрод по утерянным картам по-прежнему высокий (операции с ПИН-кодом);
- Интернет-фрод остается на высоком уровне, растет объем интернет-транзакций



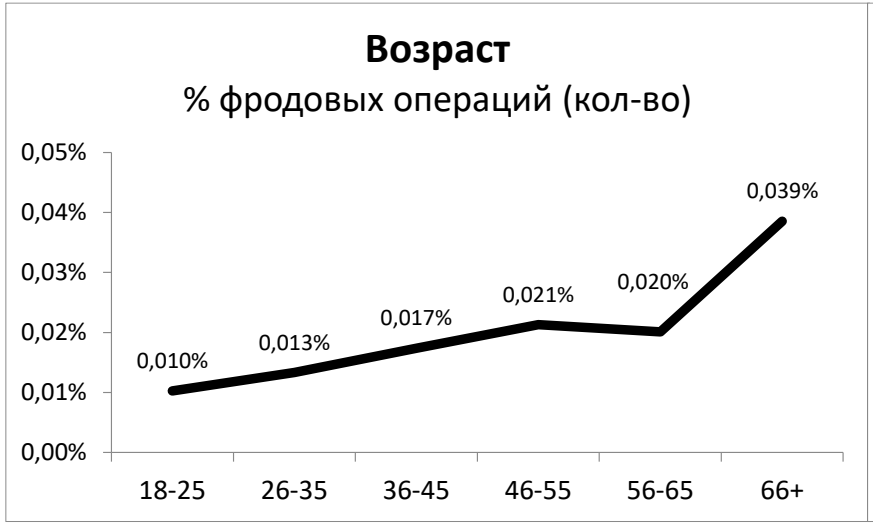


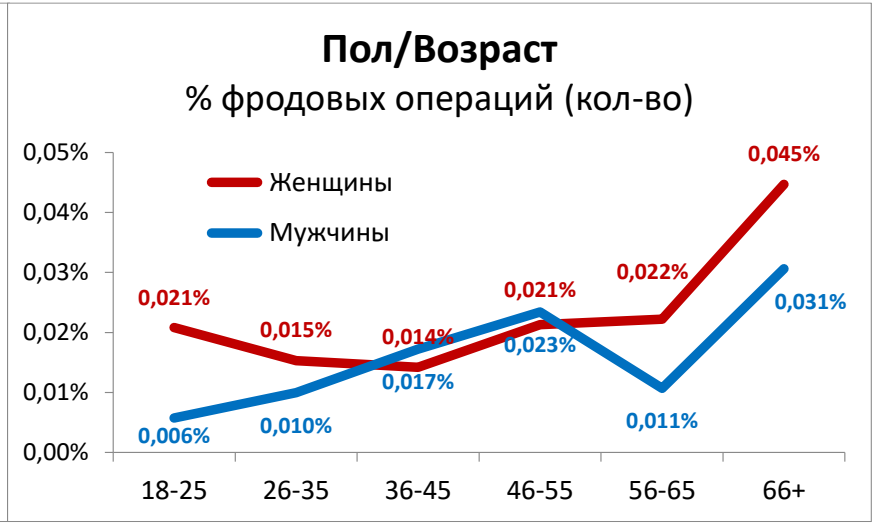




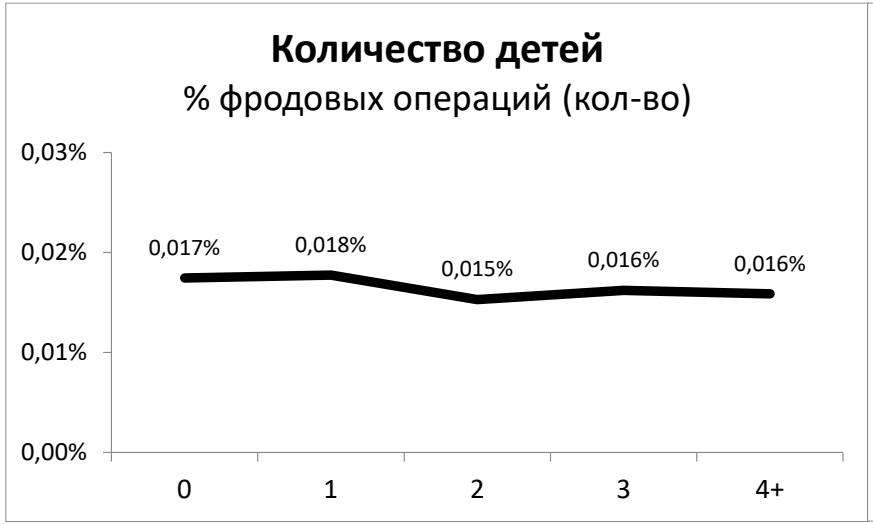


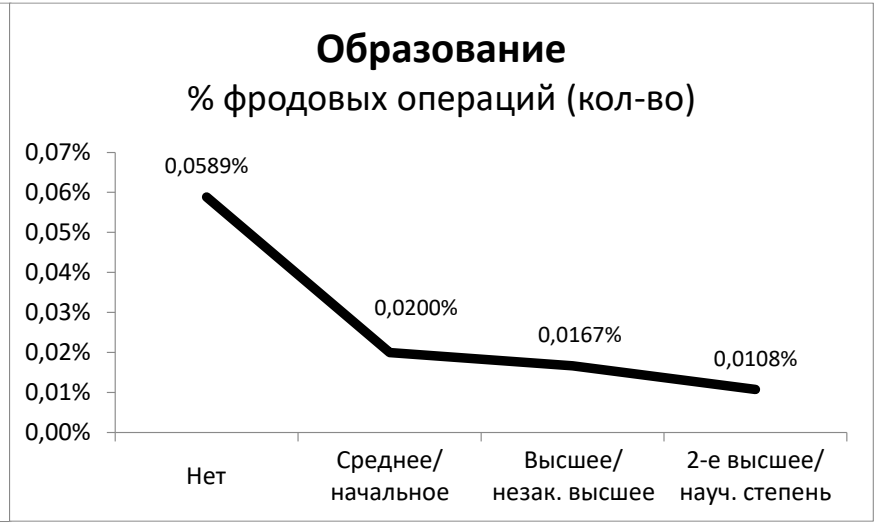
Портрет жертвы карточного мошенника



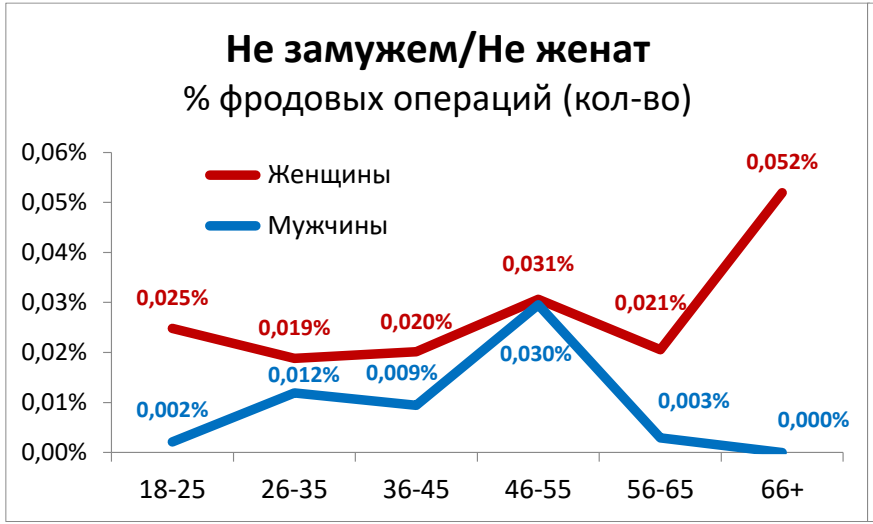


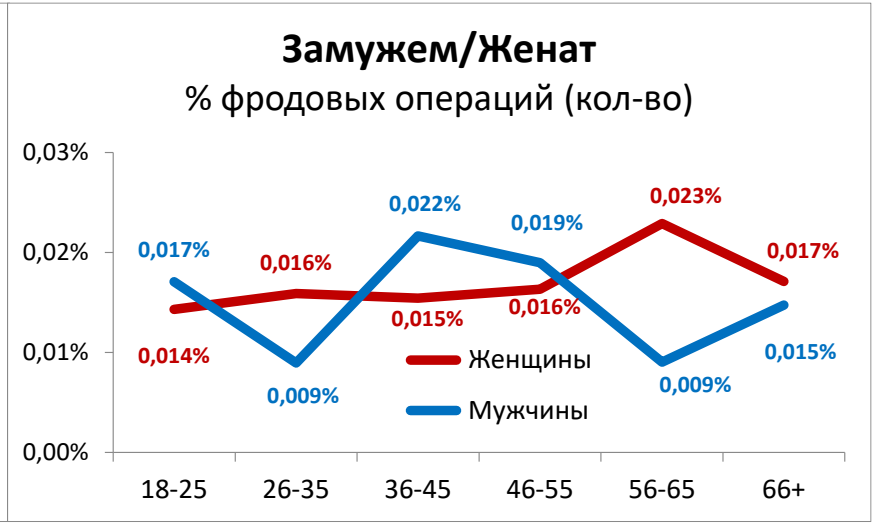
Портрет жертвы карточного мошенника



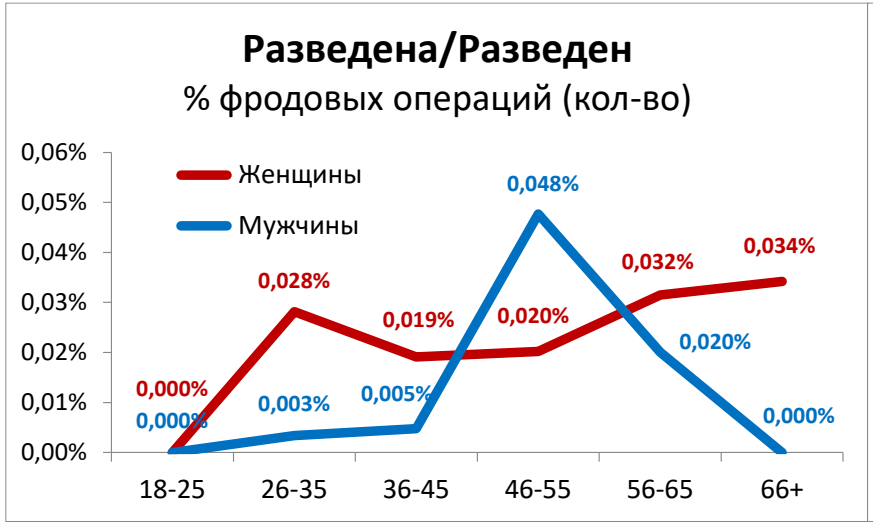


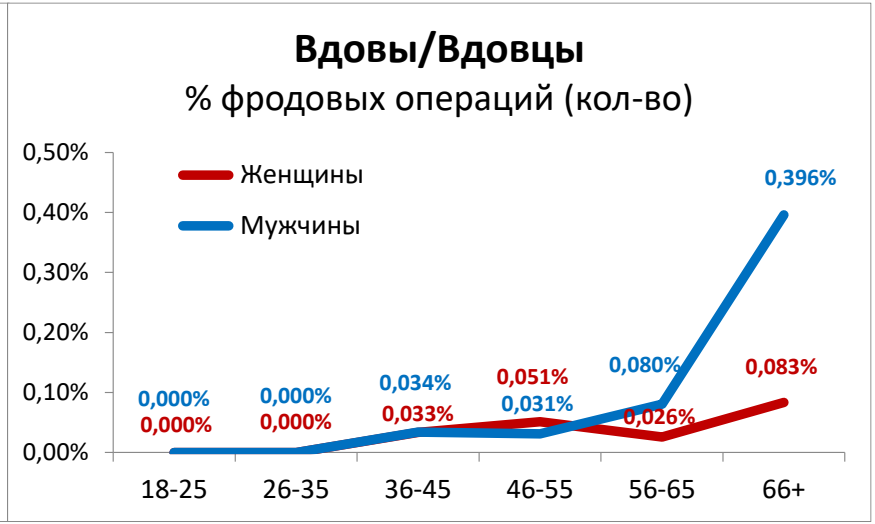
Портрет жертвы карточного мошенника



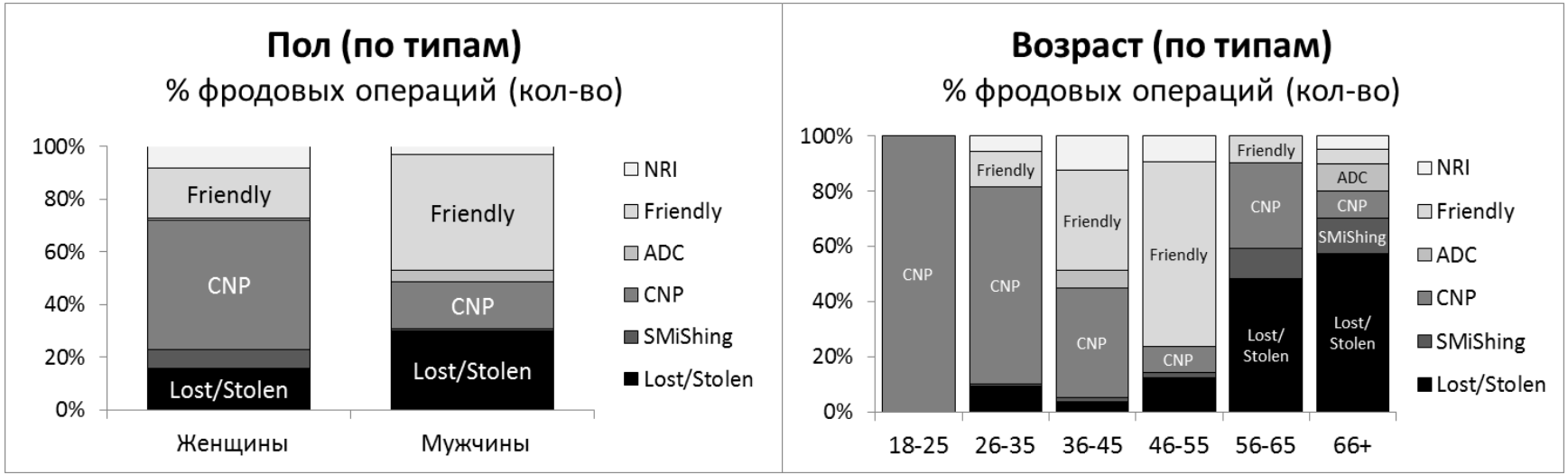


Портрет жертвы карточного мошенника



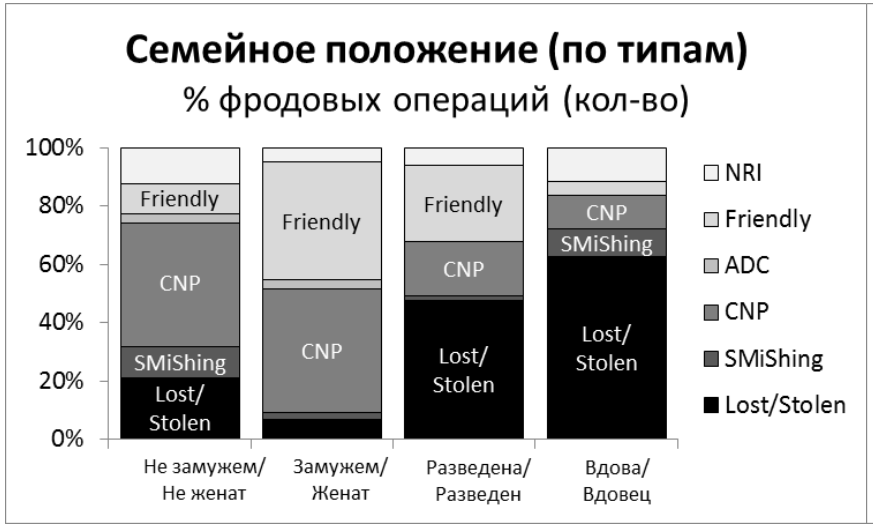


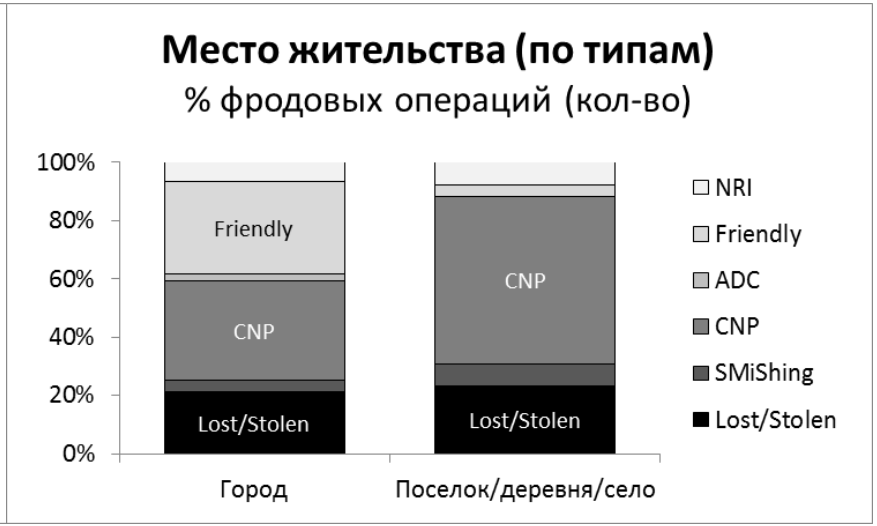
Портрет жертвы карточного мошенника



Account Data Compromise (ADC) — компрометация реквизитов карты до момента совершения несанкционированных операций;
Card-Not-Present (CNP) — операция без физического предъявления карты (интернет-платежи, заказ по почте/телефону, p2p/c2c социальная инженерия, фишинг и т.д.);
Friendly Fraud — операции с использованием подлинной карты/ реквизитов подлинной карты без разрешения клиента (знакомые, родственники);
Lost/Stolen (LST/STLC) — операции по утерянным/ украденным картам;
Not-received-as-issued (NRI) — операции по недоставленным карта (клиент карту не получил);
SMiShing — операции в результате СМС-мошенничества (социальная инженерия)

Портрет жертвы карточного мошенника





Account Data Compromise (ADC) — компрометация реквизитов карты до момента совершения несанкционированных операций;
Card-Not-Present (CNP) — операция без физического предъявления карты (интернет-платежи, заказ по почте/телефону, p2p/c2c социальная инженерия, фишинг и т.д.);
Friendly Fraud — операции с использованием подлинной карты/ реквизитов подлинной карты без разрешения клиента (знакомые, родственники);
Lost/Stolen (LST/STLC) — операции по утерянным/ украденным картам;
Not-received-as-issued (NRI) — операции по недоставленным карта (клиент карту не получил);
SMiShing — операции в результате СМС-мошенничества (социальная инженерия)

Обед?

Часть 2.2

Кредитный фрод: кейсы и аналитика

Бизнес-процессы

Персонал
- Проверка сотрудников
- Обучение
- Организация процессов
- Мотивационная схема
- Мониторинг деятельности

Партнеры
- Партнерский договор
- Проверка партнеров
- Мониторинг деятельности

Процессы
- Аудит процессов
- Согласование инициатив
- Автоматизация процессов

Аналитика

Репорты
- Fraud Report
- Concentration Report
- Block Report

Анализ портфеля
- ментов
- исследо)
- Ad

Модели
- Предиктивная аналитика
- тка правил
- Learning

Оценка
- СВА антифрод-процессов
- СВА антифрод-систем
- Оценка fraud-потерь

Антифрод-системы

Внутренние системы
- Warning System
- AFS (local) и др.
- Black-lists
- Биометрия

Внешние сервисы
- FPS, AFS (межбанк)
- FP
- Те м (Мегафон и др.)
- Co и (Mail.ru и др.)
- Cookie (Rambler и др.)
- СПАРК, Контур.Фокус и др.
- Банкроты (Interfax)

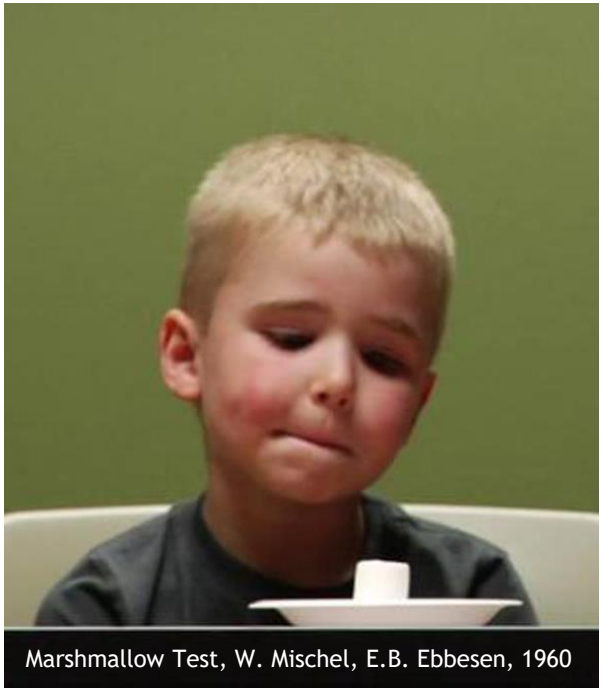
Гос. сервисы
- ФМС
- ФССП
- ПФР
- ФНС

80%

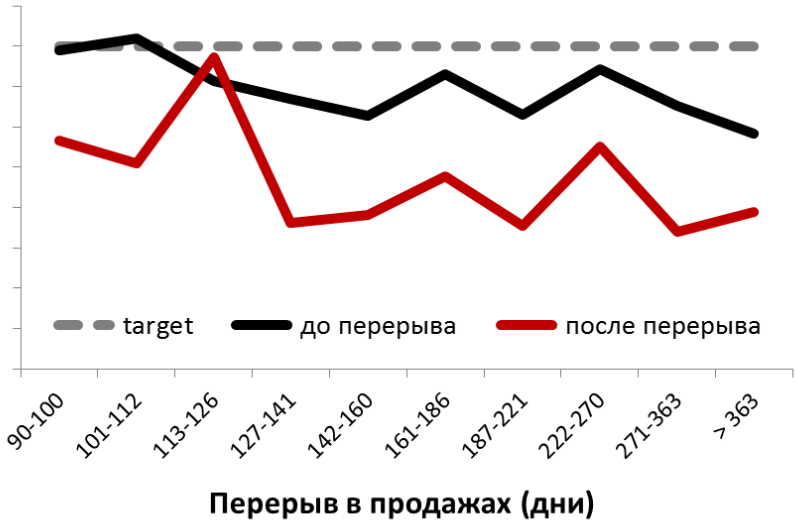
?

20%

Зефирный тест



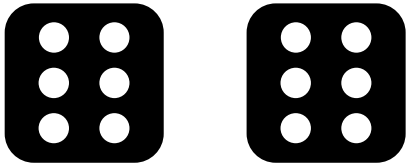
Риски по «спящим» точкам ниже после «пробуждения»



Бином Ньютона

P – вероятность того, что *k* и более контрактов случайно попадут в просрочку fpd (0 ≤ k ≤ n) при средней просрочке *d*.

$$P = \sum_{i=k}^{i=n} C_n^i d^i (1-d)^{n-i}$$



n=2, k=2, d≈16,7%: P≈2,8%

Теория

Вероятность случайного выпадения в fpd (при d=3,7%)

k \ n	1	2	3	4	5
1+	3,70%	7,27%	10,70%	14,01%	17,19%
2+		0,14%	0,40%	0,78%	1,27%
3+			0,01%	0,02%	0,05%
4+				0,00%	0,00%
5+					0,00%

Диапазон ошибки (P):

< 1%	1-5%	> 5%

Практика

Уровень fpd за 12 месяцев работы после расчетного fpd

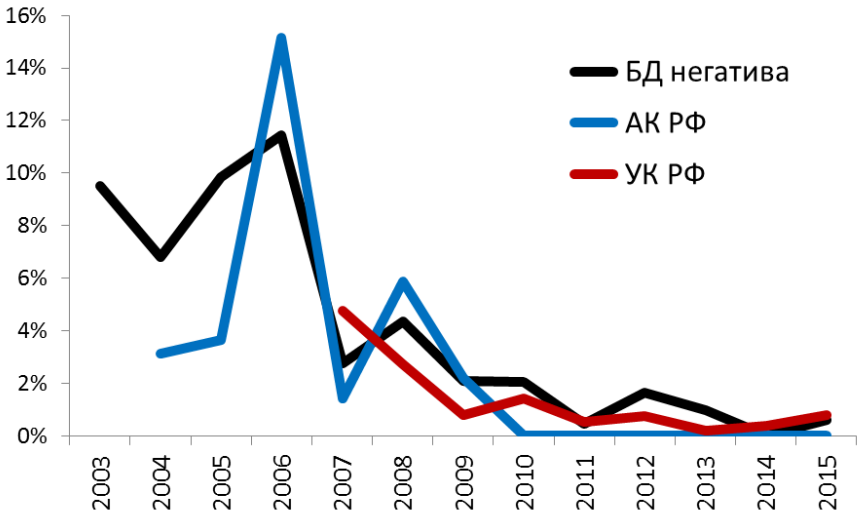
k \ n	1	2	3	4	5
1+	6,1%	5,6%	5,6%	4,9%	5,2%
2+		7,1%	7,1%	5,4%	6,9%
3+			13,4%	7,7%	10,5%
4+				10,0%	22,2%
5+					56,3%

Диапазон fpd (Target = 4,8%):

> 2*T	1*T ÷ 2*T	< T

Эксперимент «Обе белые»

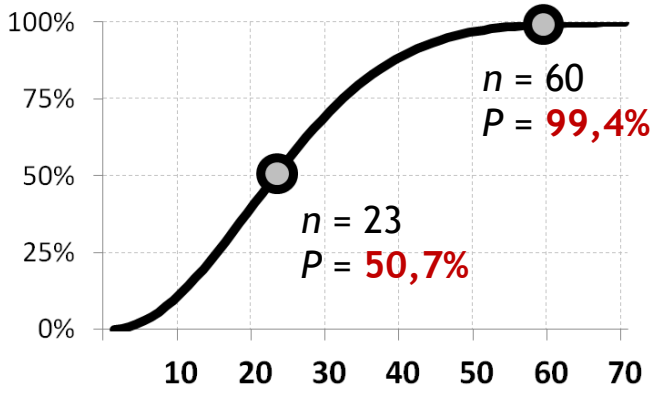
После 2006 года просрочка по Экспертизе сильно снизилась



Задача о близнецах

Вероятность того, что в группе из *n* человек хотя бы **у двух совпадут дни рождения:**

$$P = 1 - \frac{365!}{365^n (365 - n)!}$$

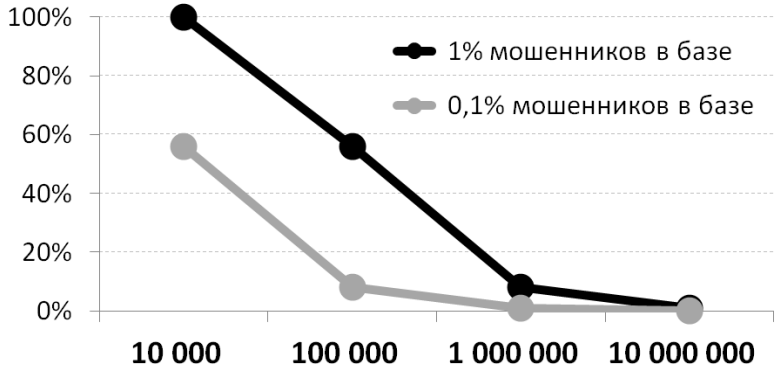


n – количество человек в группе

Вероятность случайного выявления мошенника:

$$P = 1 - \left(1 - \frac{C_{N-1}^{T} - C_{N-K}^{T}}{C_{N-1}^{T} N} MK\right)^{R}$$

R – кол-во сегментов, *M* – кол-во мошенников в сегменте, *K* – кол-во фото на мошенника (*K*≈6), *T* – кол-во фото в топовом пуле, *N* – кол-во фото в базе



N – размер базы

Особенности культур

Geert Hofstede

(1928)

В 1960-1970-х гг. Хофстеде разработал совокупность показателей, определяющих культурные характеристики различных народов:

1. Дистанцированность от власти — восприятие власти, показывает насколько в культуре ценится иерархия, испытывают ли члены общества уважение к пожилым людям, пользуются ли власть имущие особыми привилегиями;

2. Обособленность (индивидуализм) — измеряет степень тяготения к личностным целям, является противоположностью сплочённости (коллективизму);

3. Напористость — нацеленность на достижение результата любой ценой;

4. Избегание неопределённости — степень восприятия и реагирования на незнакомые ситуации;

5. Стратегическое мышление — ориентированность на решение стратегических, долгосрочных целей, желание заглядывать в будущее.

Дистанцированность от власти

#	Страна	Индекс
1.	Малайзия	100
2.	Словакия	100
3.	Гватемала	95
4.	Ирак	95
5.	Панама	95
6.	Саудовская Аравия	95
7.	Бутан	94
8.	Филиппины	94
9.	Россия	93
10.	Украина	92
11.	Албания	90
12.	Кувейт	90
13.	Румыния	90
14.	ОАЭ	90
15.	Сербия	86
16.	Мозамбик	85
17.	Суринам	85
18.	Ангола	83
19.	Мексика	81
20.	Венесуэла	81
21.	Бангладеш	80
22.	Китай	80
23.	Гана	80
24.	Гондурас	80
25.	Ливия	80

#	Страна	Индекс
26.	Нигерия	80
27.	Шри Ланка	80
28.	Сирия	80
29.	Эквадор	78
30.	Фиджи	78
31.	Индонезия	78
32.	Индия	77
33.	Капе Верде	75
34.	Ливан	75
35.	Сингапур	74
36.	Хорватия	73
37.	Словения	71
38.	Болгария	70
39.	Буркина Фасо	70
40.	Египет	70
41.	Эфиопия	70
42.	Иордания	70
43.	Кения	70
44.	Малави	70
45.	Марокко	70
46.	Сенегал	70
47.	Сьерра-Леоне	70
48.	Танзания	70
49.	Вьетнам	70
50.	Бразилия	69

#	Страна	Индекс
51.	Франция	68
52.	Гонг Конг	68
53.	Польша	68
54.	Колумбия	67
55.	Сальвадор	66
56.	Турция	66
57.	Бельгия	65
58.	Доминикана	65
59.	Намибия	65
60.	Непал	65
61.	Перу	64
62.	Тайланд	64
63.	Чили	63
64.	Португалия	63
65.	Уругвай	61
66.	Греция	60
67.	Южная Корея	60
68.	Замбия	60
69.	Иран	58
70.	Тайвань	58
71.	Чехия	57
72.	Испания	57
73.	Мальта	56
74.	Пакистан	55
75.	Япония	54

#	Страна	Индекс
76.	Италия	50
77.	Аргентина	49
78.	ЮАР	49
79.	Тринидад и Тобаго	47
80.	Венгрия	46
81.	Ямайка	45
82.	Латвия	44
83.	Литва	42
84.	Эстония	40
85.	Люксембург	40
86.	США	40
87.	Канада	39
88.	Нидерланды	38
89.	Австралия	36
90.	Коста-Рика	35
91.	Германия	35
92.	Великобритания	35
93.	Швейцария	34
94.	Финляндия	33
95.	Норвегия	31
96.	Швеция	31
97.	Исландия	30
98.	Ирландия	28
99.	Новая Зеландия	22
100.	Дания	18
101.	Израиль	13
102.	Австрия	11

Источник: https://geerthofstede.com/

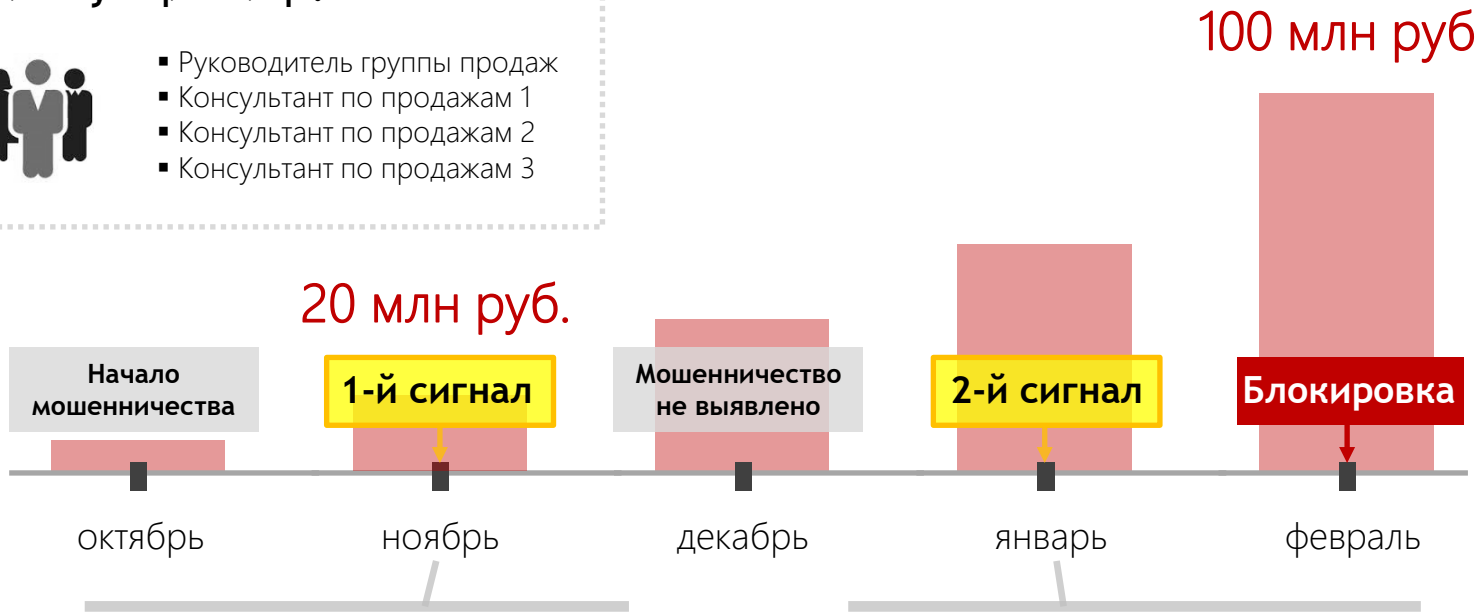
Бизнес-кейс 3

Мошенничество на 100 млн руб.

Как украсть миллионы?

Действующие лица:

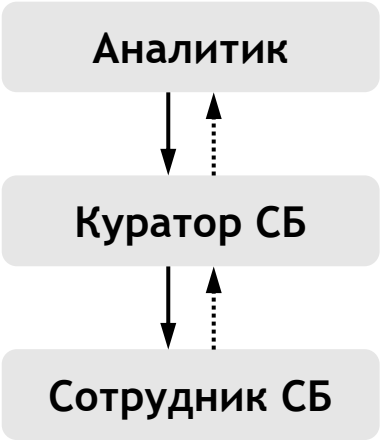
- Руководитель группы продаж
- Консультант по продажам 1
- Консультант по продажам 2
- Консультант по продажам 3



- Кредиты по украденным паспортам (ФМС)
- У разных заемщиков совпадают номера вторых документов (страх. свидетельство)
- Одинаковые телефоны у разных заёмщиков

- Кредиты по украденным паспортам (ФМС)
- У разных заемщиков совпадают номера страховых
- Неверные контактные данные (обзвон)
- Централизованное внесение платежей

Коммуникация



Коммуникация через руководство СБ повышает ответственность аналитиков и сотрудников СБ

Прямая коммуникация приводит к проблеме «отцов и детей»

Fraud News

- Новости о раскрытых мошеннических схемах и манипуляциях;
- Статистика нарушений по регионам;
- Новинки в antifraud-процессах;
- Регулярная (ежемесячная) рассылка всем сотрудникам банка, агентам, сотрудникам партнеров и т.д.

Отчетность

- Реестр всех выявленных мошеннических кейсов за период;
- Описание мошеннической схемы, сумма ущерба, предпринятые меры;
- Регулярная (еженедельная/ежемесячная) рассылка руководству банка.

Кофе?

Часть 3.1

История развития Искусственного Интеллекта

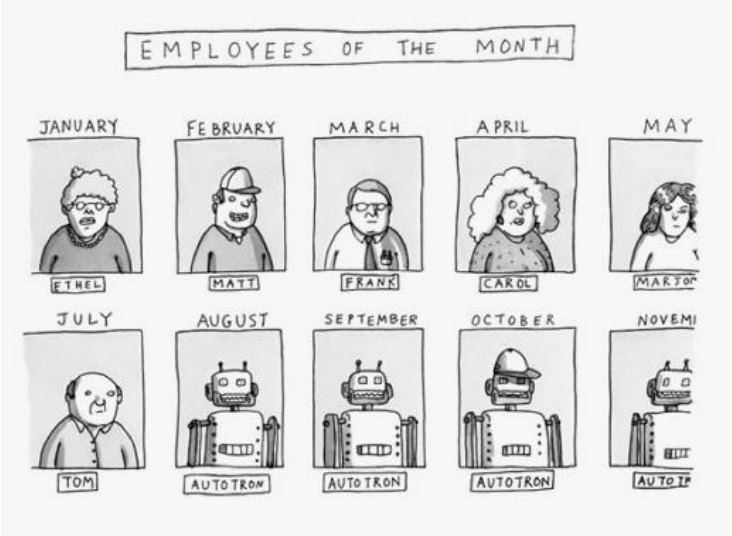
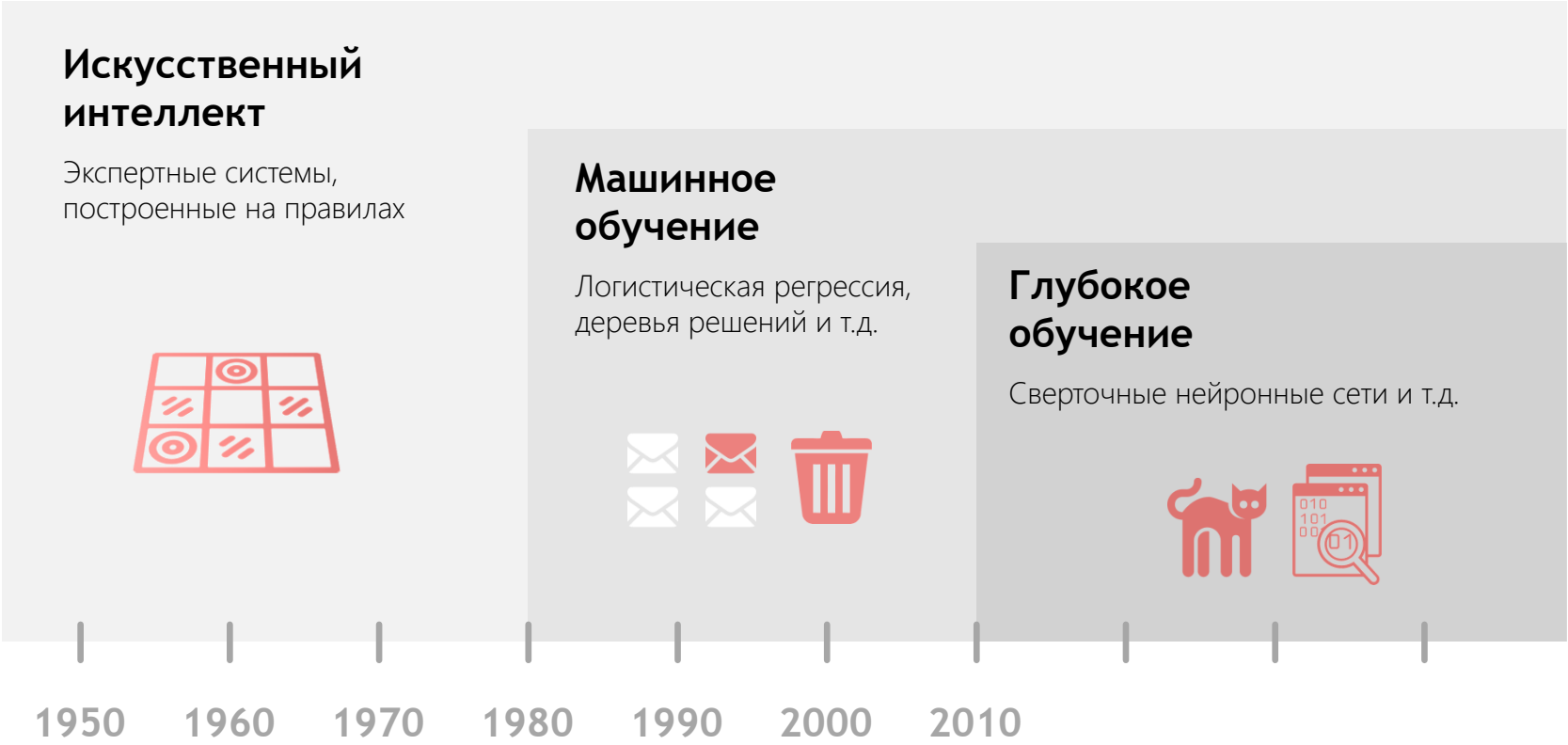
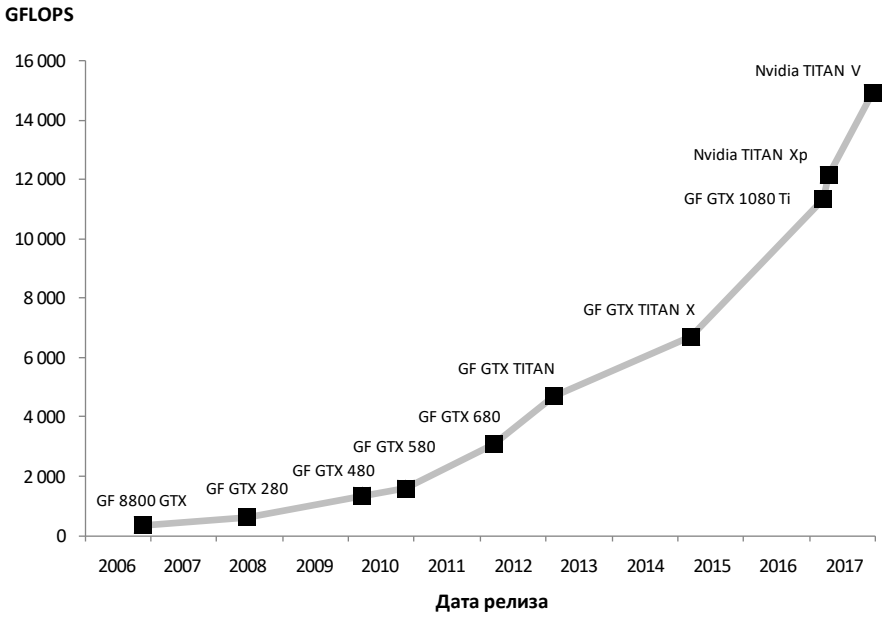


Диаграмма Венна



Производительность GPU-карт растет



Цена на дату релиза	
Nvidia TITAN V (14899 GFLOPS)	$2999
Nvidia TITAN Xp (12150 GFLOPS)	$1199
GeForce GTX 1080 Ti (11340 GFLOPS)	$699
GeForce GTX TITAN X (6691 GFLOPS)	$999
GeForce GTX TITAN (4709 GFLOPS)	$999
GeForce GTX 680 (3090 GFLOPS)	$499
GeForce GTX 580 (1581 GFLOPS)	$499
GeForce GTX 480 (1345 GFLOPS)	$499
GeForce GTX 280 (622 GFLOPS)	$649
GeForce 8800 GTX (346 GFLOPS)	$599

Источник: https://technical.city/

2002

Earth Simulator – до 2004 года самый быстрый в мире вычислительный комплекс

Стоимость: $350 000 000

Площадь: четыре теннисных корта

Производительность: 36 TFLOPS

2017

Nvidia's Titan V desktop GPU – GPU для нейронных сетей

Стоимость: $2 999

Площадь: помещается в сумочку

Производительность: до 15 TFLOPS

Часть 3.2

Предиктивная fraud-аналитика

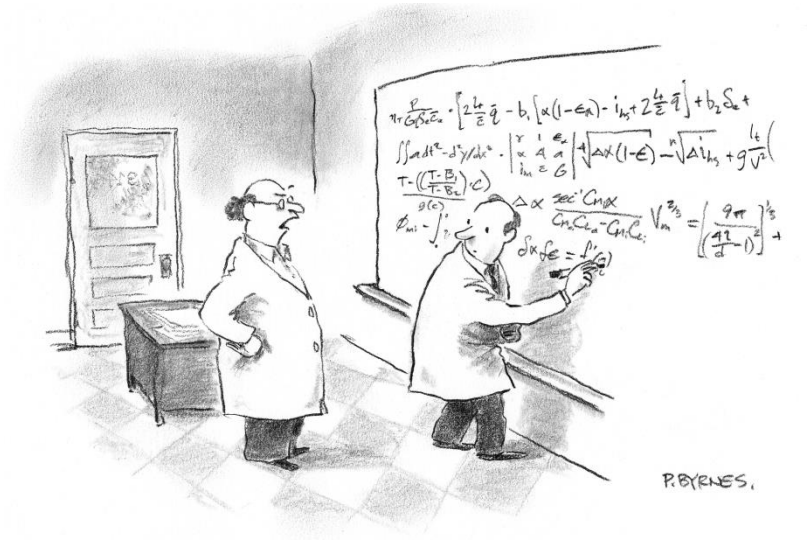
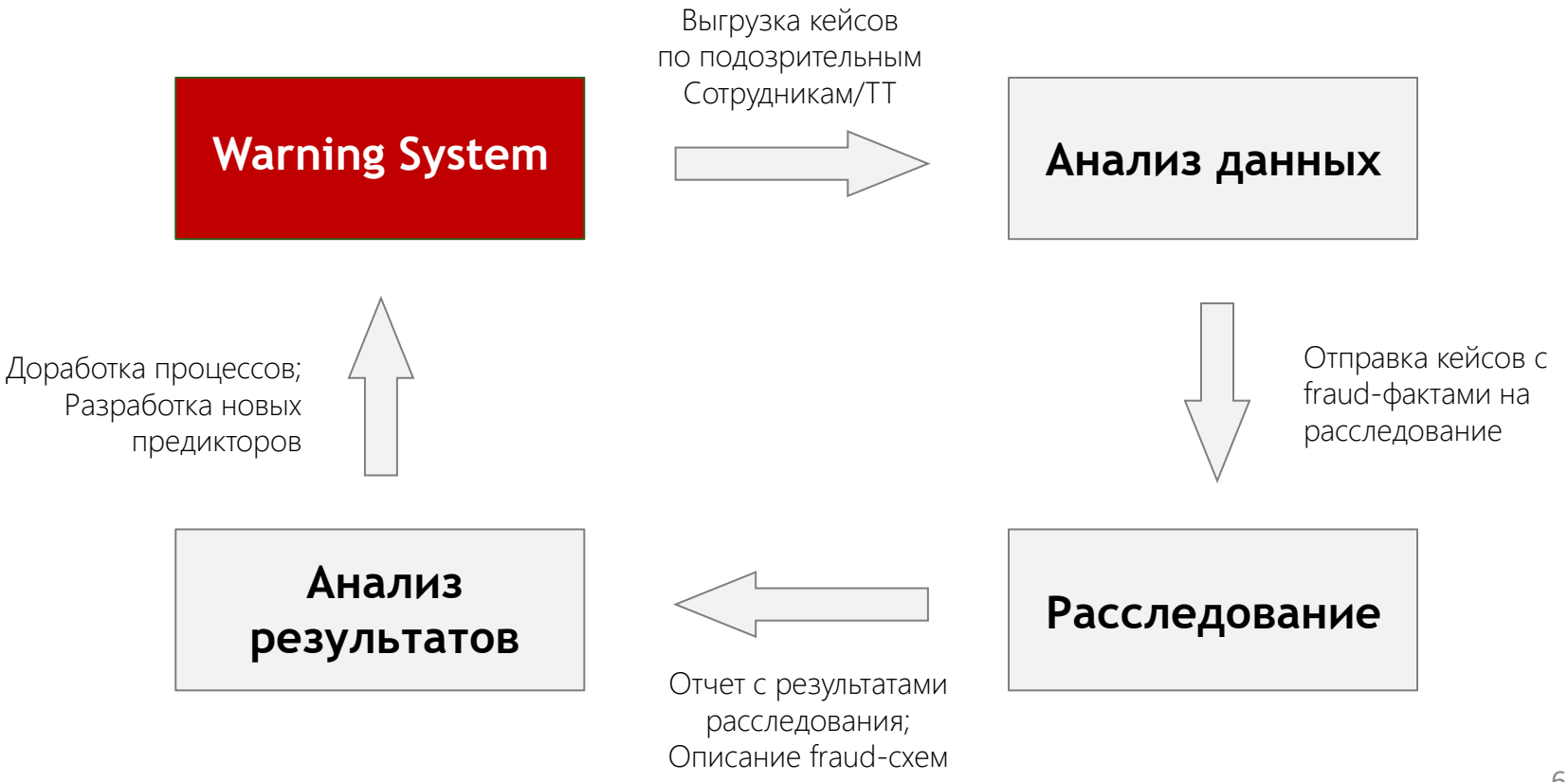


Схема проведения расследования



Цели процесса

Минимизация fraud-потерь

Оперативное выявление внутреннего мошенничества по сотрудникам/ТТ

Снижение просрочки

Оперативное выявление нарушений и манипуляций по сотрудникам/ТТ

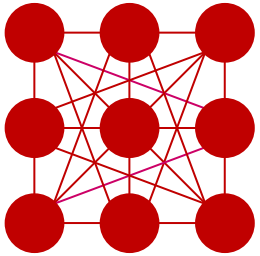
Предотвращение fraud-потерь

Выявление и устранение уязвимостей в бизнес-процессах Банка

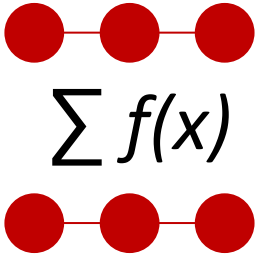
Процесс разработки триггеров

Предикторы → **Правила** → **Триггеры**

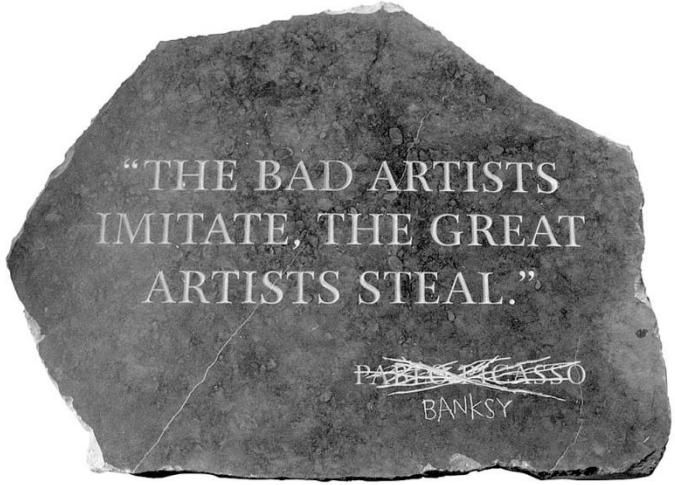
- 1 заемщик + разные дом. тел.
- 1 заемщик + разные адреса
- 2 заемщика + один дом. тел.



- 1 заемщик + разные дом. тел. + один адрес
- 2 заемщика + один дом. тел. + разные адреса



- 1 заемщик + разные дом. тел. + один адрес (за X дней)
  &
- 2 заемщика + один дом. тел. + разные адреса (за X дней)



Предикторы на данных FPS

Список правил FPS

1-й набор

Разные заемщики с одним телефоном (не родственники)

2-й набор

У заемщика разные личные данные (адрес, телефон и др.)

3-й набор

Специальные правила (странная активность, поведение и др.)

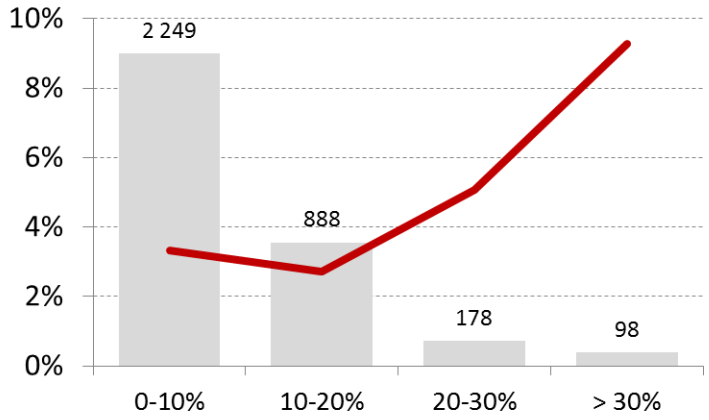
FPS_1.11	Один телефон, разные клиенты + доп.условия на ФИО, адреса и др.
FPS_1.12	Один телефон, разные клиенты + доп.условия на ФИО, адреса и др.
FPS_1.13	Использование подставных телефонов
FPS_1.14	Один телефон, разные клиенты + доп.условия на ФИО, адреса и др.
FPS_1.15	Телефон используется разными заёмщиками в нескольких банках
FPS_1.16	Телефон встречается у разных заёмщиков с разными адресами + доп.условия
FPS_1.17	Телефон встречается у разных заёмщиков с разными адресами + доп.условия
FPS_1.18	Телефон используется разными заёмщиками в нескольких банках
FPS_2.11	Частая смена мобильного телефона
FPS_2.12	Подозрительное поведение
FPS_2.13	Подозрение на поддельные документы
FPS_2.14	Значительные изменения в данных
FPS_2.15	Значительные изменения в контактных данных
FPS_2.16	Изменение контактных данных заёмщика за короткий срок
FPS_2.17	Значительные изменения в контактных данных
FPS_2.18	Изменение контактных данных заёмщика за короткий срок
FPS_2.19	После заявки на КЕШ через короткий срок заёмщик оформляет заявку на ПОС
FPS_2.20	После отказанной заявки на КЕШ через короткий срок заёмщик оформляет заявку на ПОС
FPS_2.21	Высокая кредитная активность заёмщика
FPS_2.22	Изменение данных работодателя при посещении других банков
FPS_2.23	Кредитная активность заёмщика в высокорисковом сегменте
FPS_2.24	Кредитная активность заёмщика в высокорисковом сегменте
FPS_2.25	Высокая кредитная активность заёмщика
FPS_2.26	Кредитная активность заёмщика в высокорисковом сегменте
FPS_2.27	Высокая кредитная активность заёмщика

Параметры калибровки

FPS-концентрации

Высокая концентрация сработавших правил FPS на ТТ или Сотруднике повышает вероятность внутреннего мошенничества

Доля выявленных мошеннических ТТ



Концентрация срабатываний FPS на ТТ

Параметры

Минимальное кол-во хитовых заявок на ТТ	Анализируемый период	Концентрация хитовых заявок на ТТ
>= 3	7 дней	>=5%
>= 5	14 дней	>=10%
>= 10	30 дней	>=15%
		>=20%
		>=25%
		>=30%
		>=35%
		>=40%
		>=45%
		>=50%
		>=55%
		>=60%
		>=65%

3 x 3 x 13 = 117 комбинаций

FPS-триггеры

Target variable: 30+mob3 >= 15%

Min hit:			>= 3
	Period (days)		
Hit-rate	7	14	30
>=30%			
>=35%			
>=40%			
>=45%			
>=50%			
>=55%			

Min hit:			>= 5
	Period (days)		
Hit-rate	7	14	30
>=30%			
>=35%			
>=40%			
>=45%			
>=50%			16%
>=55%			18%

4th iteration

3rd iteration

Min hit:			>= 10
	Period (days)		
Hit-rate	7	14	30
>=30%	15%		
>=35%			24%
>=40%			
>=45%			
>=50%			
>=55%	69%		

5th iteration

2nd iteration

1st iteration

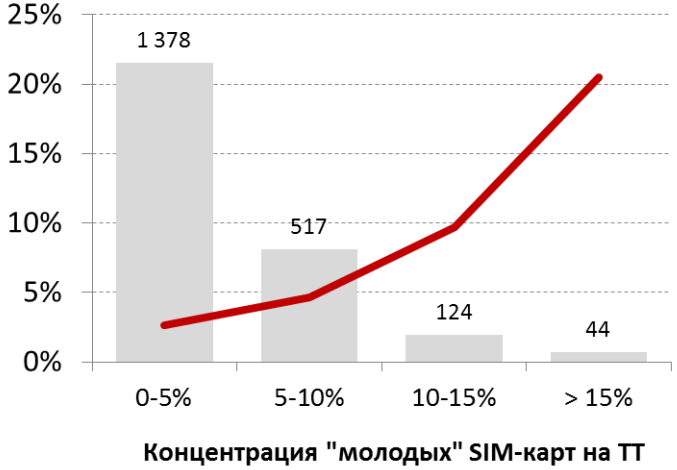
Предикторы на данных Мегафона

Параметры калибровки

Молодая SIM-карта

Высокая концентрация заявок с «молодыми» SIM-картами на ТТ/Сотруднике повышает вероятность внутреннего фрода

Доля выявленных мошеннических ТТ



Параметры

Минимальное кол-во "молодых" SIM-карт на ТТ	"Возраст" SIM-карты	Анализируемый период	Концентрация "молодых" SIM-карт на ТТ
>= 4	0-30 дней	7 дней	>=55%
>= 5	0-90 дней	14 дней	>=60%
>= 6		30 дней	>=65%
>= 7			>=70%
>= 8			>=75%
>= 9			=100%
>= 10			

7 x 2 x 3 x 6 = 252 комбинаций

Триггеры

Период (дни):							7
Возраст сим-карты (дни):							0-30
	Min hit (кол-во)						
Hit-rate	4	5	6	7	8	9	10
>=55%							51%
>=60%							
>=65%							
>=70%							
>=75%							
=100%							

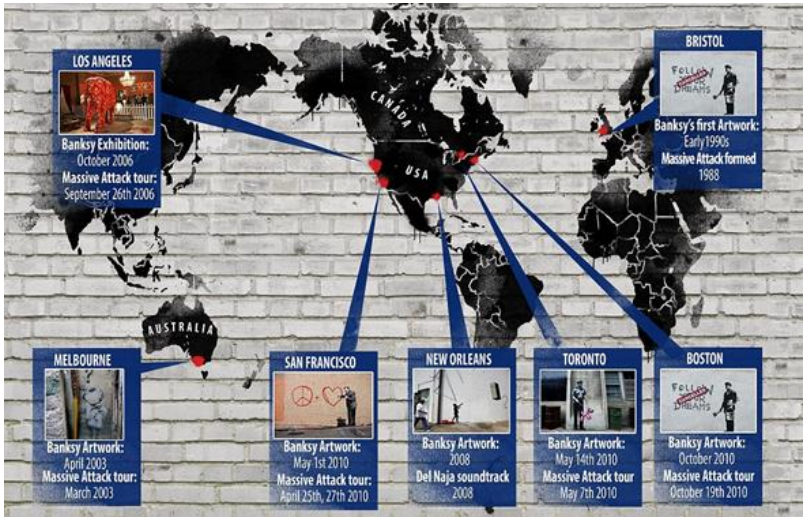
Период (дни):							14
Возраст сим-карты (дни):							0-30
	Min hit (кол-во)						
Hit-rate	4	5	6	7	8	9	10
>=55%							
>=60%							
>=65%							
>=70%							
>=75%							
=100%	46%						

Период (дни):							30
Возраст сим-карты (дни):							0-30
	Min hit (кол-во)						
Hit-rate	4	5	6	7	8	9	10
>=55%							44%
>=60%							
>=65%							
>=70%							
>=75%							
=100%							

Период (дни):							7
Возраст сим-карты (дни):							0-90
	Min hit (кол-во)						
Hit-rate	4	5	6	7	8	9	10
>=55%							
>=60%							
>=65%							47%
>=70%							
>=75%							
=100%							

Период (дни):							14
Возраст сим-карты (дни):							0-90
	Min hit (кол-во)						
Hit-rate	4	5	6	7	8	9	10
>=55%							
>=60%							
>=65%							
>=70%							
>=75%						66%	
=100%							

Период (дни):							30
Возраст сим-карты (дни):							0-90
	Min hit (кол-во)						
Hit-rate	4	5	6	7	8	9	10
>=55%							
>=60%							
>=65%							
>=70%							
>=75%				59%			
=100%			78%				

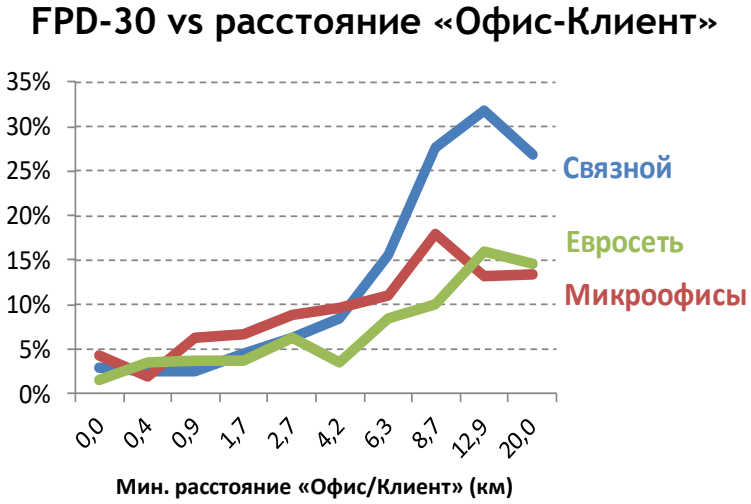


Предикторы на данных геолокаций

Параметры калибровки

GPS-зависимости

Чем дальше от офиса продаж живет или работает заемщик, тем выше вероятность того, что он мошенник



Параметры

Расчетное расстояние "ТТ <-> Клиент"	Минимальное кол-во "отдаленных" клиентов	Минимальное расстояние "ТТ <-> Клиент"	Анализируемый период	Концентрация "отдалённых" клиентов
ТТ <-> Факт. адрес	>= 3	0-1 км	7 дней	>=5%
ТТ <-> Рег. адрес	>= 5	1-2 км	14 дней	>=10%
ТТ <-> Работа	>= 10	2-3 км	30 дней	>=15%
		3-5 км	60 дней	>=20%
		5-7 км		>=30%
		7-10 км		>=50%
		10-20 км		>=70%
		>= 20 км		=100%

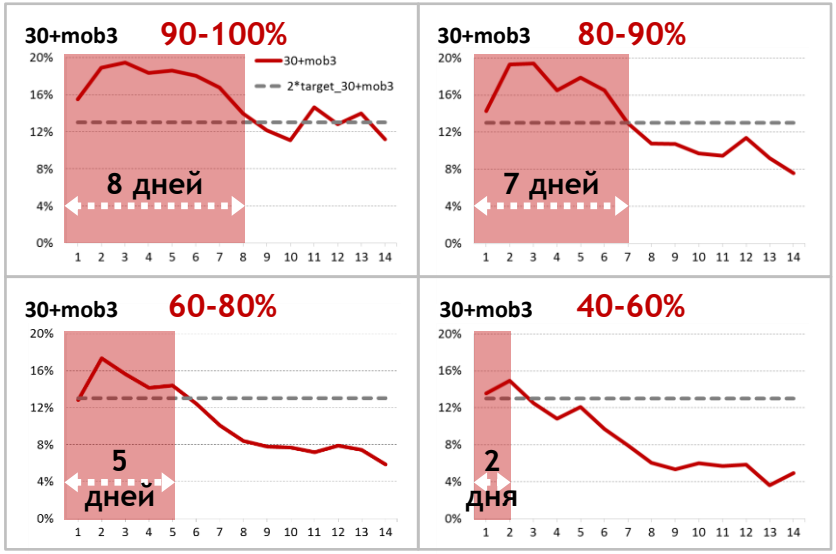
3 x 8 x 4 x 8 = 768 комбинаций

Предикторы для кредитных карт

Параметры калибровки

Скорость утилизации

Мошенники обналичивают 90-100% лимита карты в течении первых нескольких дней после активации.



Параметры

Минимальное кол-во быстрых утилизаций	Доля утилизируемого лимита	Период утилизации	Анализируемый период	Концентрация быстрых утилизаций
>= 3	20% - 40%	1 день	7 дней	>=5%
>= 5	40% - 60%	2 дня	14 дней	>=10%
>= 10	60% - 80%	3 дня	30 дней	>=15%
	80% - 100%	4 дня	60 дней	>=20%
		5 дней		>=30%
		6 дней		>=50%
		7 дней		>=70%
		8 дней		=100%
		9 дней		
		10 дней		

3 x 4 x 10 x 4 x 8 = 3 840 комбинаций

Триггеры

Min number of "Quick Utilization"	>=3								>=5								>=10								>=3								>=5								>=10							
Hit-rate	>= 70%	% utilized limit						>= 20%	>= 70%	% utilized limit						>= 20%	>= 70%	% utilized limit						>= 20%	>= 70%	% utilized limit						>= 40%	>= 70%	% utilized limit						>= 40%	>= 70%	% utilized limit						>= 40%
Period	Period of utilization								Period of utilization								Period of utilization								Period of utilization								Period of utilization								Period of utilization							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
7																			28%																															
14																																												28%						
30																																																	
60																	20%																																	

Min number of "Quick Utilization"	>=3								>=5								>=10								>=3								>=5								>=10							
Hit-rate	= 100%	% utilized limit						>= 20%	= 100%	% utilized limit						>= 20%	= 100%	% utilized limit						>= 20%	= 100%	% utilized limit						>= 40%	= 100%	% utilized limit						>= 40%	= 100%	% utilized limit						>= 40%
Period	Period of utilization								Period of utilization								Period of utilization								Period of utilization								Period of utilization								Period of utilization							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
7																																																
14																											21%		23%																				
30																																														61%			
60									23%														26%																										

Min number of "Quick Utilization"	>=3								>=5								>=10								>=3								>=5								>=10							
Hit-rate	>= 50%	% utilized limit						>= 60%	>= 50%	% utilized limit						>= 60%	>= 50%	% utilized limit						>= 60%	>= 50%	% utilized limit						>= 80%	>= 50%	% utilized limit						>= 80%	>= 50%	% utilized limit						>= 80%
Period	Period of utilization								Period of utilization								Period of utilization								Period of utilization								Period of utilization								Period of utilization							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
7																		37%																															
14																																																	
30																																																	
60																																																	

Min number of "Quick Utilization"	>=3								>=5								>=10								>=3								>=5								>=10							
Hit-rate	>= 70%	% utilized limit						>= 60%	>= 70%	% utilized limit						>= 60%	>= 70%	% utilized limit						>= 60%	>= 70%	% utilized limit						>= 80%	>= 70%	% utilized limit						>= 80%	>= 70%	% utilized limit						>= 80%
Period	Period of utilization								Period of utilization								Period of utilization								Period of utilization								Period of utilization								Period of utilization							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
7																			31%																															82%
14																																																	
30																					28%																									26%			
60																																											88%						

Min number of "Quick Utilization"	>=3								>=5								>=10								>=3								>=5								>=10							
Hit-rate	= 100%	% utilized limit						>= 60%	= 100%	% utilized limit						>= 60%	= 100%	% utilized limit						>= 60%	= 100%	% utilized limit						>= 80%	= 100%	% utilized limit						>= 80%	= 100%	% utilized limit						>= 80%
Period	Period of utilization								Period of utilization								Period of utilization								Period of utilization								Period of utilization								Period of utilization							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
7	24%												20%													26%		23%										48%	39%	23%									
14													22%																												27%								
30																20%																			100%	33%									100%				
60																																	25%													100%			

Б-тесты — аномалии в клиентских данных

История

1881 г.
Саймон Ньюкомб

Обнаружил, что в логарифмических таблицах единиц больше чем двоек, двоек больше чем троек и т.д.

1938 г.
Фрэнк Бенфорд

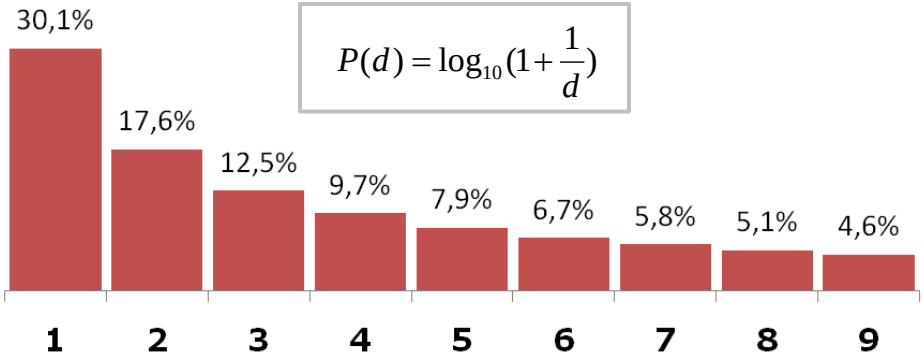
Проанализировал различные справочники с данными и построил эмпирический закон распределения цифр

1990-е
Марк Нигрини

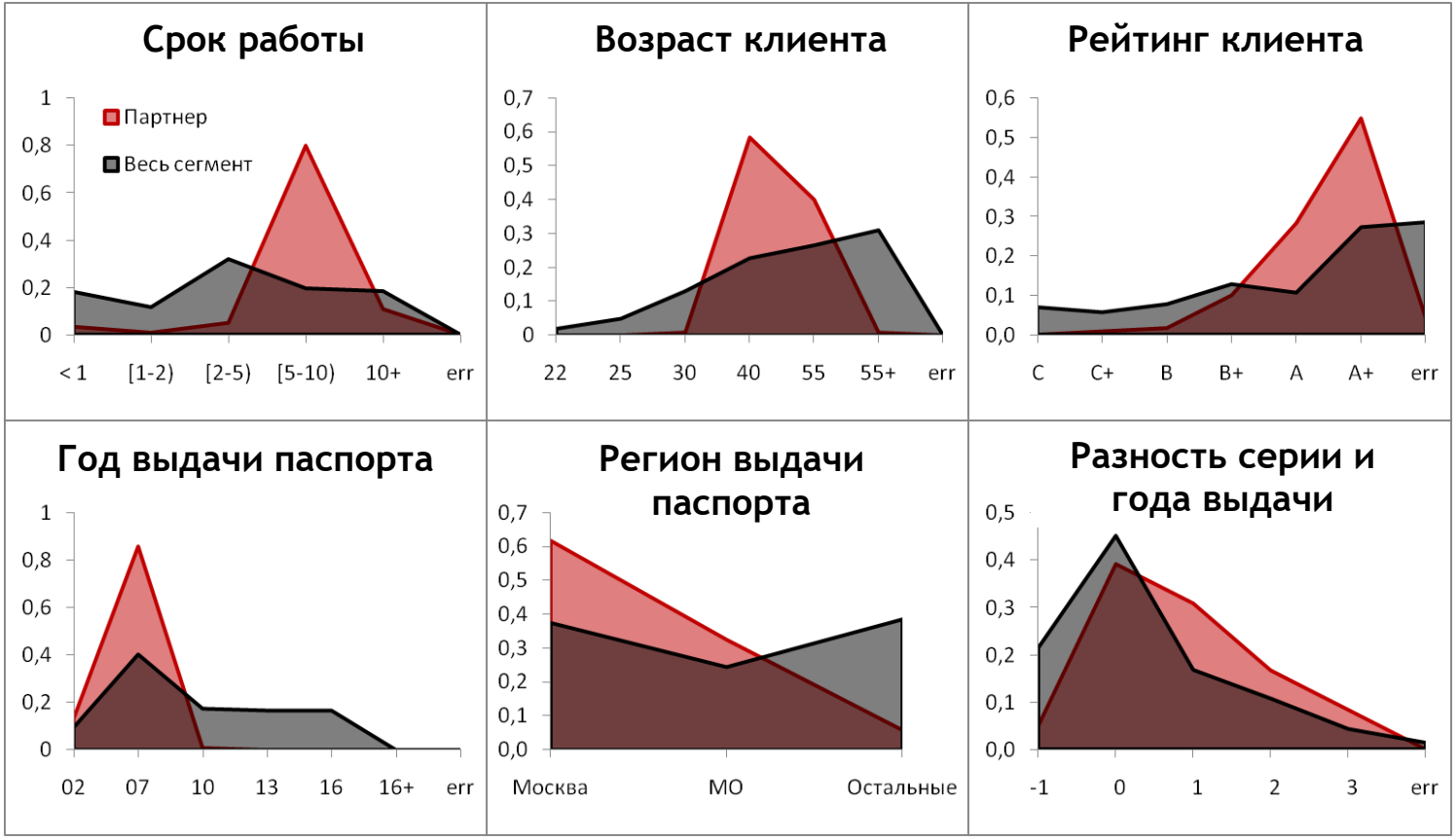
Разработали тесты для аудита финансовой отчетности компаний и выявления поддельных данных

Распределение Бенфорда

$$P(d) = \log_{10}(1 + \frac{1}{d})$$



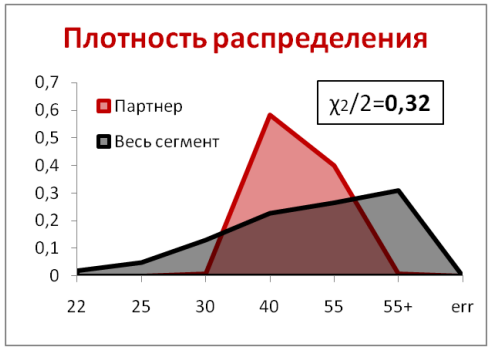
Аномалии в клиентских данных



Метрики для калибровки

Хи-квадрат

$$\chi^2 = \sum_{i=1}^{n} \frac{(a_i - b_i)^2}{a_i + b_i}$$



Минусы:
Значения нормированной статистики Хи-квадрат чаще сосредоточены у нуля и реже у единицы

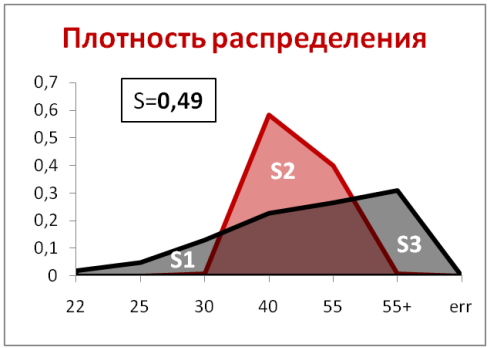
KS-тест

$$KS = \max_i |F(a_i) - F(b_i)|$$

Минусы:
Для распределений с несколькими локальными максимумами статистика KS может быть заниженной

S-статистика

$$S = \sum_{i=1}^{n} \frac{|a_i - b_i|}{2}$$

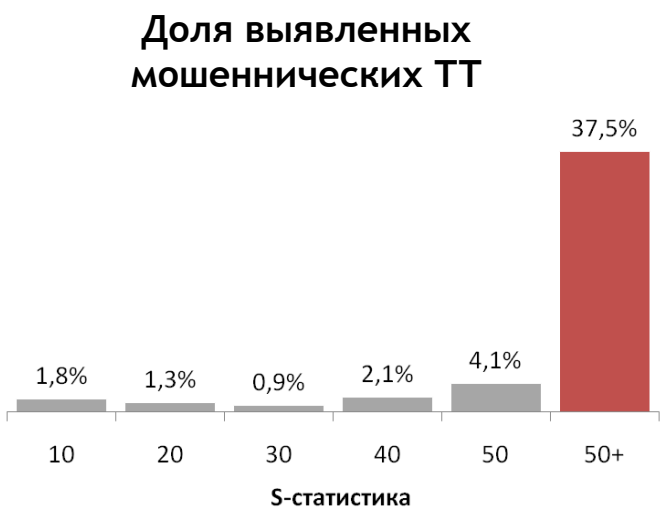


Плюсы:
S-статистика просто интерпретируется – это половина площади под непересекающимися областями

Параметры калибровки

Б-тесты

Триггер позволяет выделить высокорисковую группу ТО и Сотрудников, у которых значение S-статистики высокое



Параметры

Минимальное кол-во заявок	Кол-во категорий в распределении	Анализируемый период	Порог S-статистики
>= 10	2	7 дней	>=5%
>= 25	3	14 дней	>=10%
>= 20	5	30 дней	>=20%
>= 30	10	60 дней	>=30%
>= 50			>=40%
			>=50%
			>=60%
			>=70%
			>=80%
			>=90%

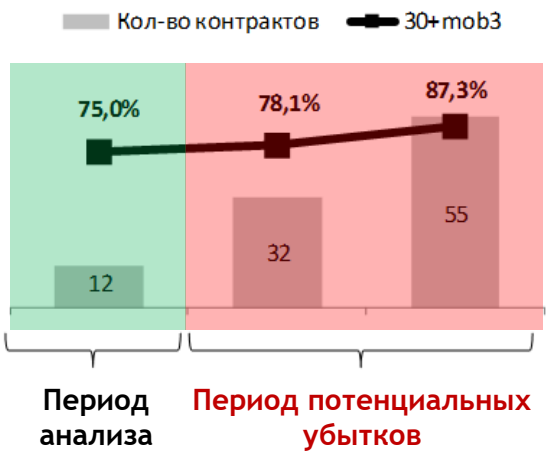
5 x 4 x 4 x 10 = 800 комбинаций

Примеры Б-тестов

№	Б-тест	$\chi^2/2$	KS	S
1.	Отрасль работодателя клиента	0,70	0,48	**0,80**
2.	5-я цифра дохода (с конца)	0,43	0,55	**0,61**
3.	Стаж работы клиента	0,39	0,53	**0,60**
4.	Должность клиента	0,40	0,54	**0,59**
5.	Совпадение адресов (факт/рег)	0,37	0,56	**0,56**
6.	Год по серии паспорта	0,31	0,50	**0,50**
7.	Год выдачи паспорта	0,33	0,50	**0,50**
8.	Возраст клиента	0,32	0,30	**0,49**
9.	Рейтинг клиента (скор.бал)	0,25	0,24	**0,45**
10.	Регион ТТ = Региону по паспорту клиента	0,16	0,34	**0,34**
11.	Регион по серии паспорта клиента	0,16	0,33	**0,33**
12.	Пол клиента	0,11	0,32	**0,32**
13.	Год по серии паспорта минус год выдачи паспорта	0,09	0,23	**0,24**
14.	4-я цифра дохода (с конца)	0,07	0,20	**0,22**

Целевая переменная

$$TV_{(T_l - T_a)} = S\,\frac{D - D_0}{1 - D_0}$$



$TV_{(T_l - T_a)}$ – целевая переменная (Target Variable), показывающая потери на периоде $(T_l - T_a)$ после срабатывания предиктора;

T_l – рассматриваемый период потерь;

T_a – анализируемый период, на котором срабатывает предиктор;

$T_l - T_a$ – период после срабатывания предиктора;

D – уровень просрочки по выдачам сотрудника (или партнера) за период $(T_l - T_a)$

D_0 – «нулевой таргет» просрочки на периоде $(T_l - T_a)$

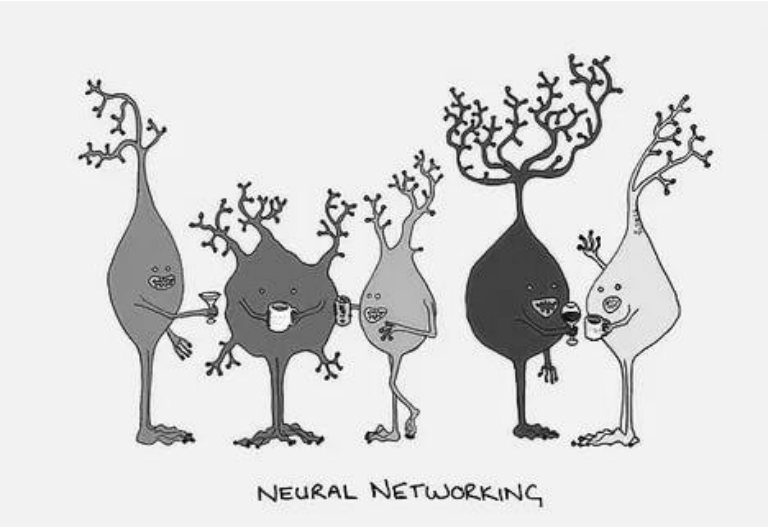
S – выданная сотрудником (или партнером) сумма кредитов за период $(T_l - T_a)$

Триггеры

№ триггера	Параметры					Средний потенциальный убыток на одну ТТ	Кол-во ТТ	% ТТ (hit-rate)
	Период анализа	Количество заявок	Кол-во категорий	Порог S-статистики	Период потерь			
Триггер 1	14	10	10	>=90%	90	3 941 610р.	1	0,0007%
Триггер 2	30	50	3	>=30%	90	317 036р.	13	0,0474%
Триггер 3	7	15	10	>=70%	60	107 805р.	1	0,0011%
Триггер 4	7	20	3	>=50%	60	61 220р.	3	0,0051%
Триггер 5	14	20	3	>=40%	90	57 841р.	30	0,0401%
Триггер 6	30	15	6	>=50%	90	32 441р.	19	0,0243%
Триггер 7	14	10	3	>=50%	90	30 537р.	63	0,0444%
Триггер 8	7	15	6	>=60%	60	15 483р.	8	0,0088%
Триггер 9	7	10	10	>=70%	90	9 381р.	35	0,0222%
Триггер 10	14	20	10	>=50%	90	9 555р.	67	0,0907%
Триггер 11	30	20	6	>=40%	90	6 777р.	79	0,1203%
Триггер 12	7	10	3	>=60%	90	5 442р.	13	0,0084%
Триггер 13	14	15	3	>=40%	60	4 186р.	70	0,0716%
Триггер 14	14	20	6	>=40%	90	3 896р.	127	0,1751%
Триггер 15	14	50	10	>=40%	90	60 301р.	3	0,0161%
Триггер 16	30	50	6	>=30%	90	16 305р.	20	0,0763%
Триггер 17	7	20	3	>=40%	90	8 372р.	26	0,0456%
Триггер 18	14	30	10	>=40%	90	2 502р.	74	0,1815%

Часть 3.3

Нейронные сети в антифроде

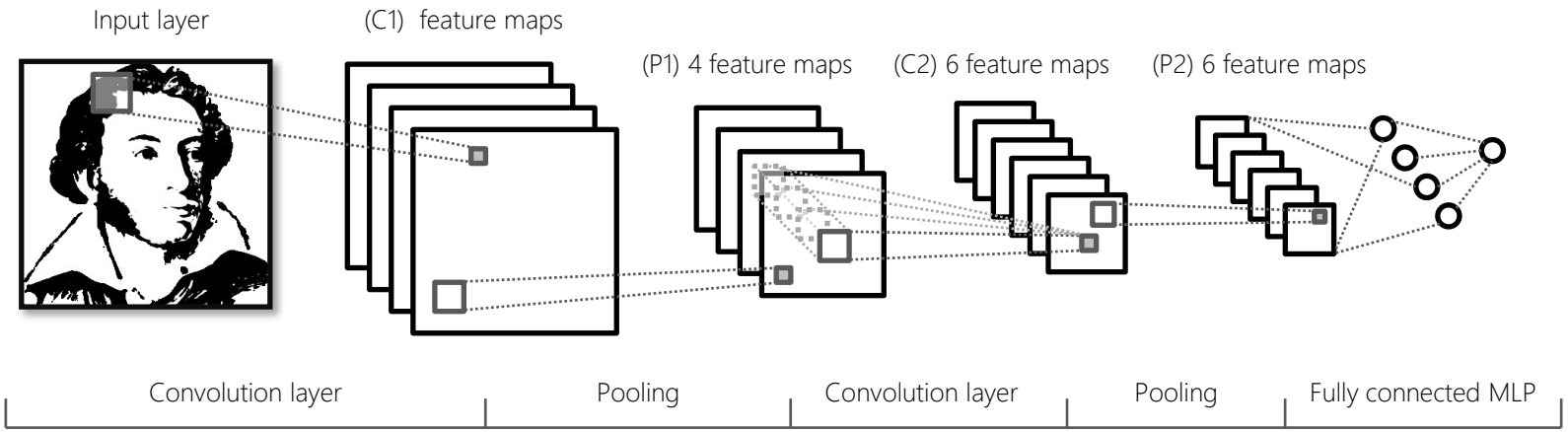


«Назовите мне типы нейронных сетей? Не знаете, двоечники! Хочу вам сказать, что это недопустимо. Вы — студенты вчерашнего дня»

Герман Греф

1. Свёрточные нейронные сети

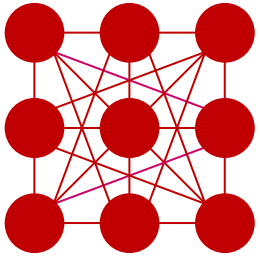
Convolutional neural network (CNN)



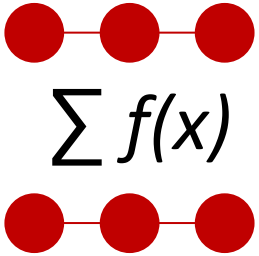
CNN для сложных fraud-правил

Предикторы → **Правила** → **Триггеры**

- 1 заемщик + разные дом. тел.
- 1 заемщик + разные адреса
- 2 заемщика + один дом. тел.



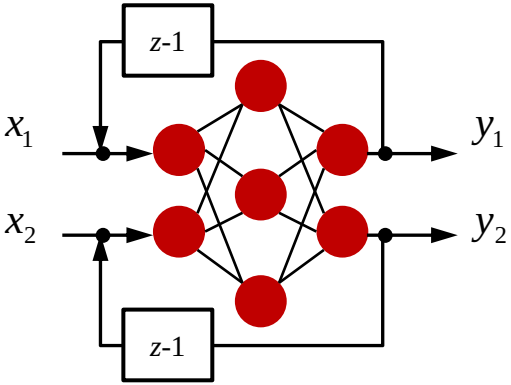
- 1 заемщик + разные дом. тел. + один адрес
- 2 заемщика + один дом. тел. + разные адреса

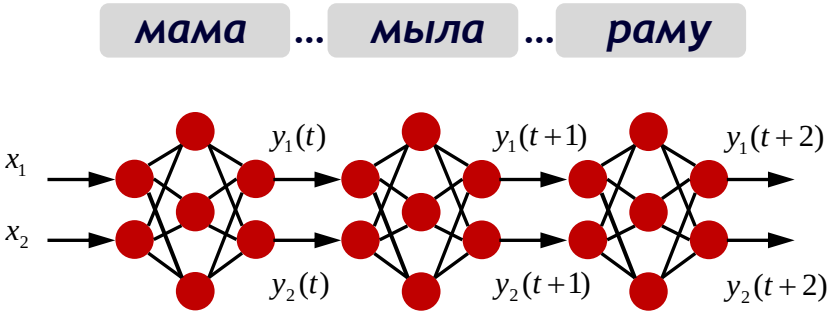


- 1 заемщик + разные дом. тел. + один адрес (за X дней)
  &
- 2 заемщика + один дом. тел. + разные адреса (за X дней)

2. Рекуррентные нейронные сети

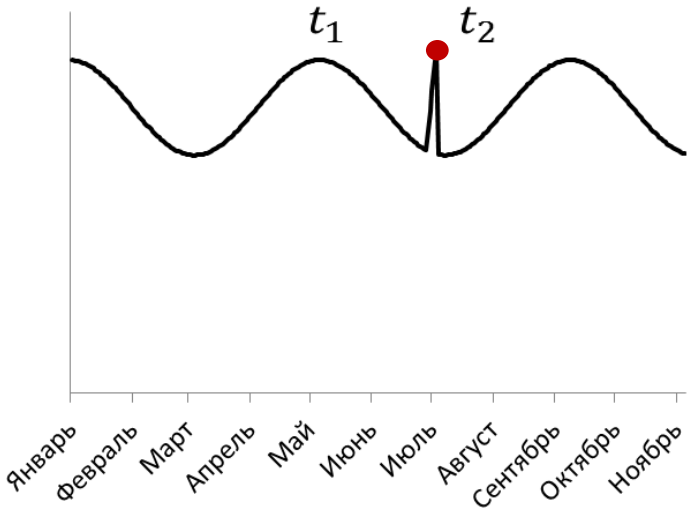
Recurrent neural network (RNN)



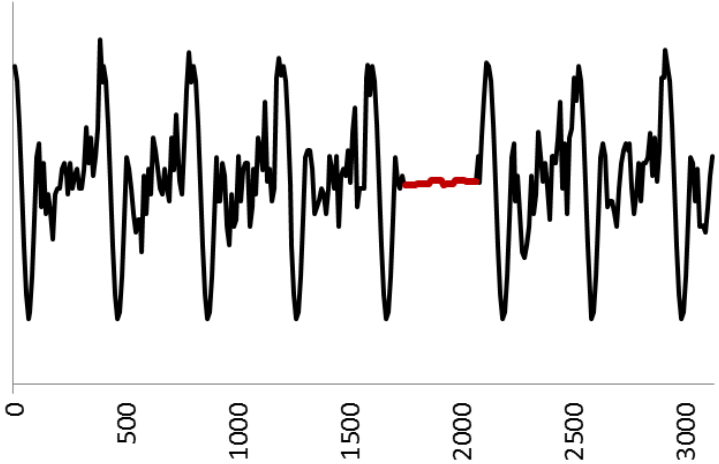


RNN для временных рядов

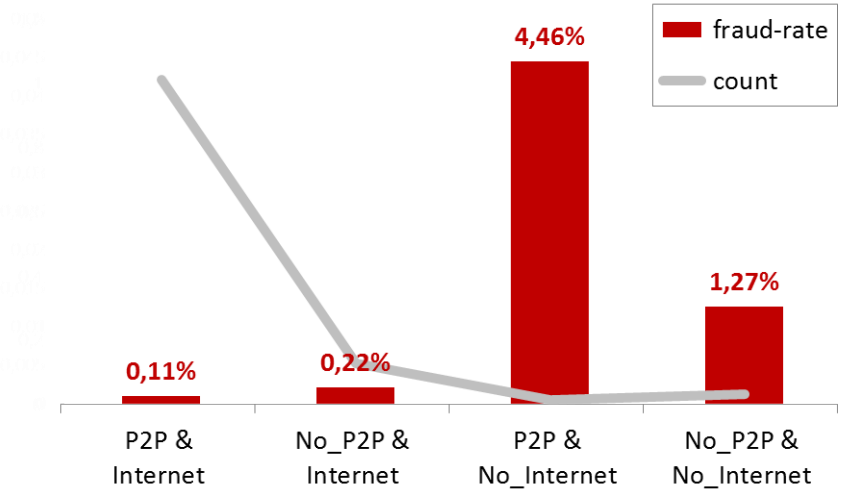
Контекстные аномалии



Групповые аномалии

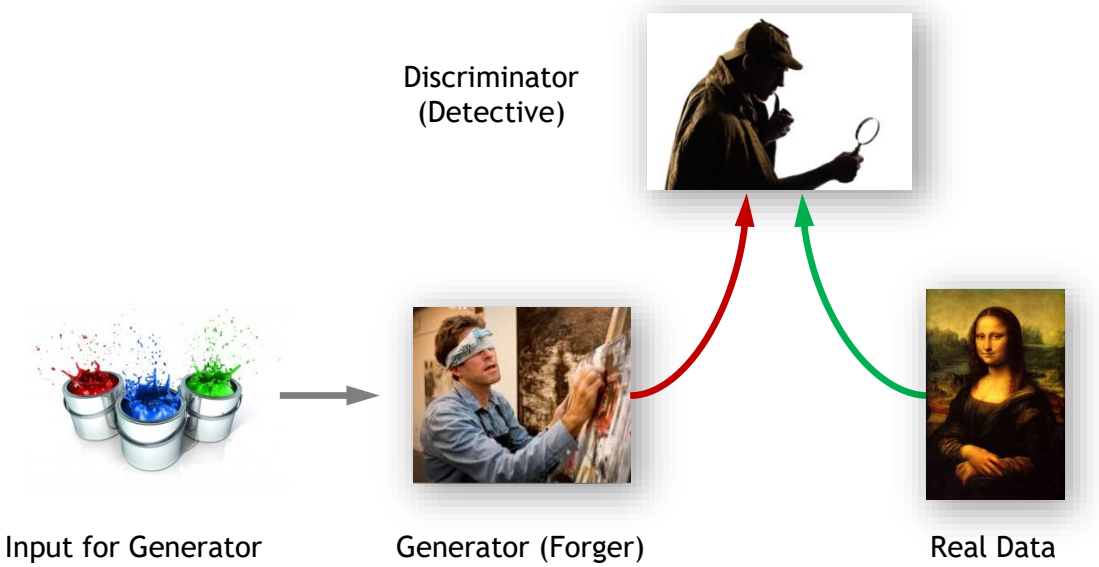


RNN для транзакционных fraud-правил

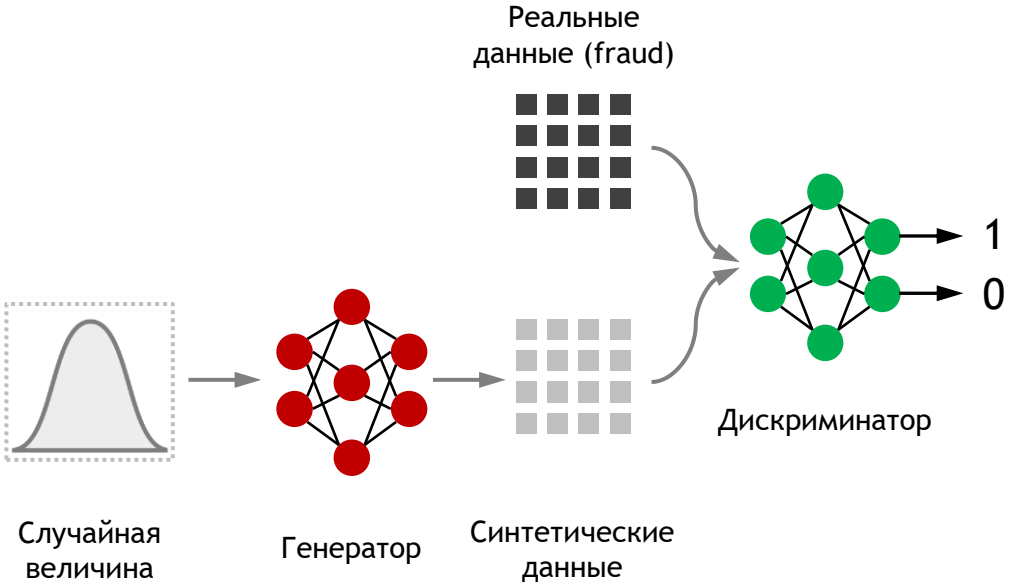


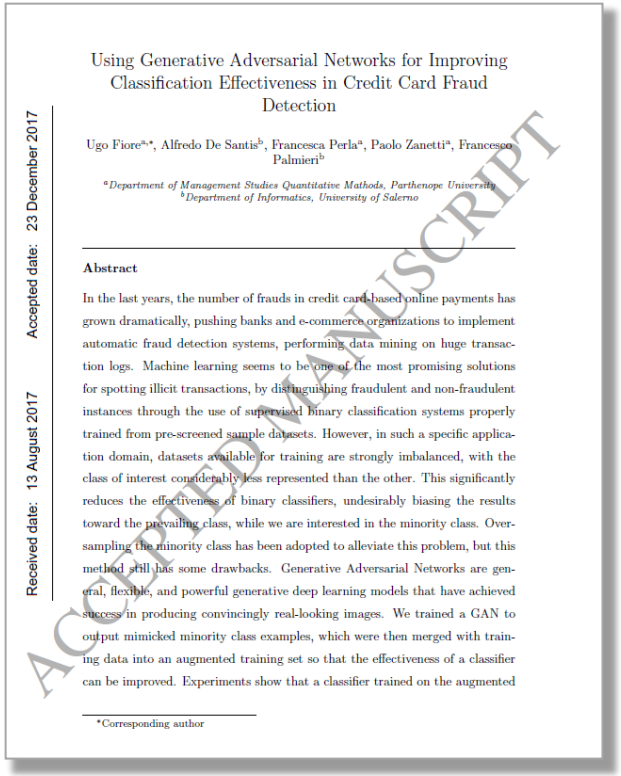
3. Генеративно-состязательные сети

Generative adversarial network (GAN)



GAN для сэмплинга fraud-выборки





Using Generative Adversarial Networks for Improving Classification Effectiveness in Credit Card Fraud Detection

Ugo Fiore[a,*], Alfredo De Santis[b], Francesca Perla[a], Paolo Zanetti[a], Francesco Palmieri[b]

[a]Department of Management Studies Quantitative Mathods, Parthenope University
[b]Department of Informatics, University of Salerno

Received date: 13 August 2017 Accepted date: 23 December 2017

ACCEPTED MANUSCRIPT

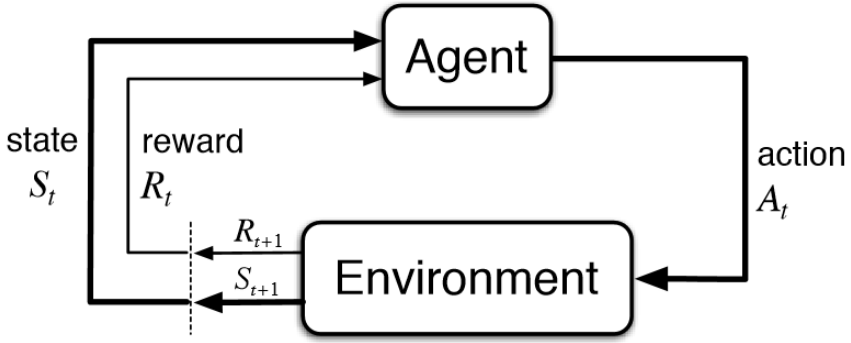
Abstract

In the last years, the number of frauds in credit card-based online payments has grown dramatically, pushing banks and e-commerce organizations to implement automatic fraud detection systems, performing data mining on huge transaction logs. Machine learning seems to be one of the most promising solutions for spotting illicit transactions, by distinguishing fraudulent and non-fraudulent instances through the use of supervised binary classification systems properly trained from pre-screened sample datasets. However, in such a specific application domain, datasets available for training are strongly imbalanced, with the class of interest considerably less represented than the other. This significantly reduces the effectiveness of binary classifiers, undesirably biasing the results toward the prevailing class, while we are interested in the minority class. Oversampling the minority class has been adopted to alleviate this problem, but this method still has some drawbacks. Generative Adversarial Networks are general, flexible, and powerful generative deep learning models that have achieved success in producing convincingly real-looking images. We trained a GAN to output mimicked minority class examples, which were then merged with training data into an augmented training set so that the effectiveness of a classifier can be improved. Experiments show that a classifier trained on the augmented

*Corresponding author

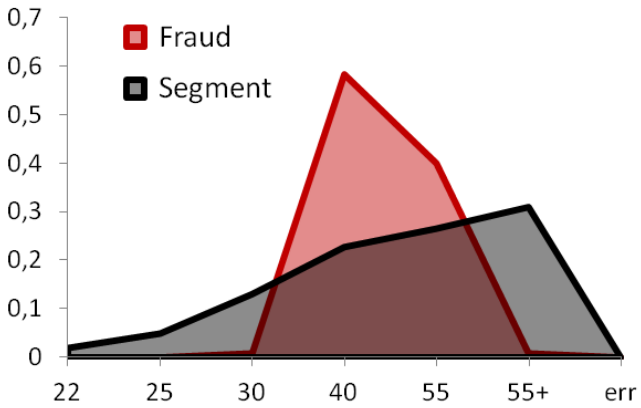
4. Обучение с подкреплением

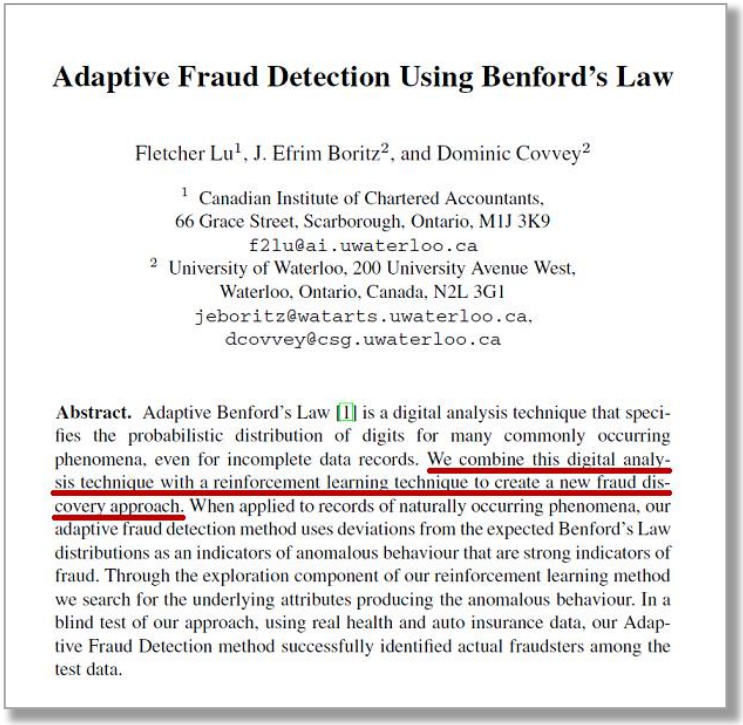
Reinforcement learning (RL)



RL для выявления fraud-аномалий

Б-тесты (аномалии)





Adaptive Fraud Detection Using Benford's Law

Fletcher Lu[1], J. Efrim Boritz[2], and Dominic Covvey[2]

[1] Canadian Institute of Chartered Accountants,
66 Grace Street, Scarborough, Ontario, M1J 3K9
f2lu@ai.uwaterloo.ca
[2] University of Waterloo, 200 University Avenue West,
Waterloo, Ontario, Canada, N2L 3G1
jeboritz@watarts.uwaterloo.ca,
dcovvey@csg.uwaterloo.ca

Abstract. Adaptive Benford's Law [1] is a digital analysis technique that specifies the probabilistic distribution of digits for many commonly occurring phenomena, even for incomplete data records. We combine this digital analysis technique with a reinforcement learning technique to create a new fraud discovery approach. When applied to records of naturally occurring phenomena, our adaptive fraud detection method uses deviations from the expected Benford's Law distributions as an indicators of anomalous behaviour that are strong indicators of fraud. Through the exploration component of our reinforcement learning method we search for the underlying attributes producing the anomalous behaviour. In a blind test of our approach, using real health and auto insurance data, our Adaptive Fraud Detection method successfully identified actual fraudsters among the test data.

CRISP-DM:

1. **Business understanding**
2. **Data understanding**
3. **Data preparation**
4. **Modeling**
5. **Evaluation**
6. **Deployment**

Рекомендации:

Для понимания задачи и подготовки переменных необходима экспертиза антифрод-экспертов

Для антифрод-задач лучше использовать модели, восстанавливающие нелинейные зависимости: Random Forest, Boosting, Neural Network

Качество fraud-моделей необходимо оценивать с помощью Recall или F-score

Чем меньше переменных, тем проще внедрение

Задание 5.

Напишите типы нейронных сетей и виды обучения в Machine Learning

Нейронные сети

1.

2.

3.

4.

Виды обучения

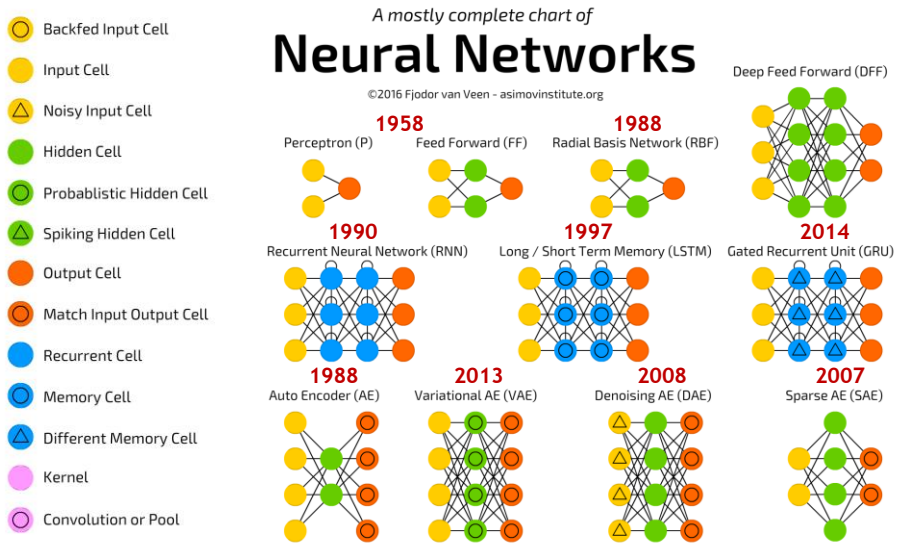
1.

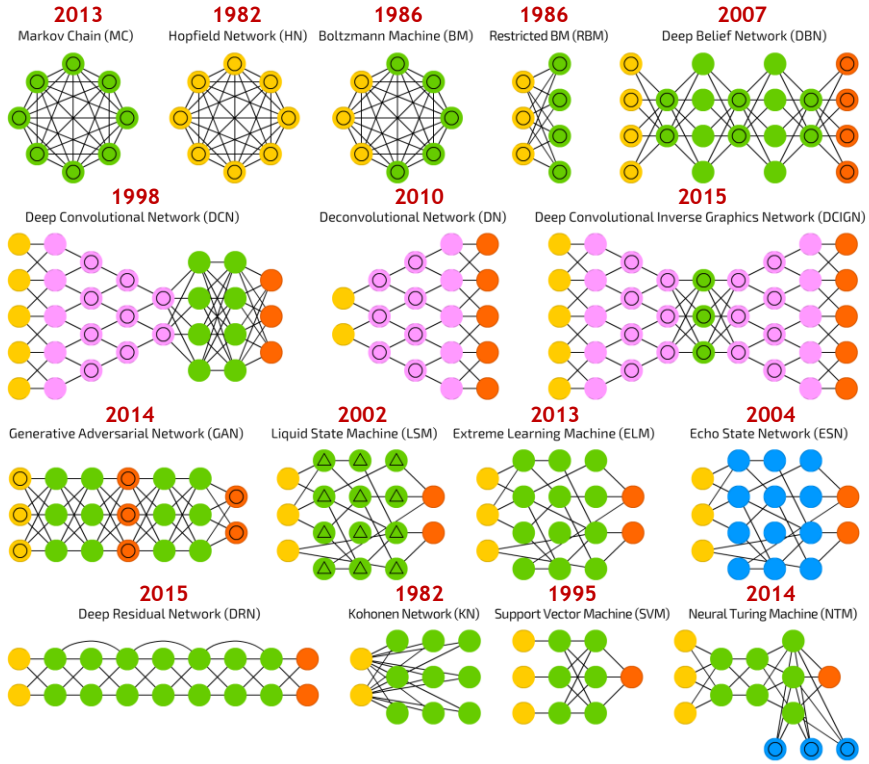
2.

3.

4.

Еще архитектуры

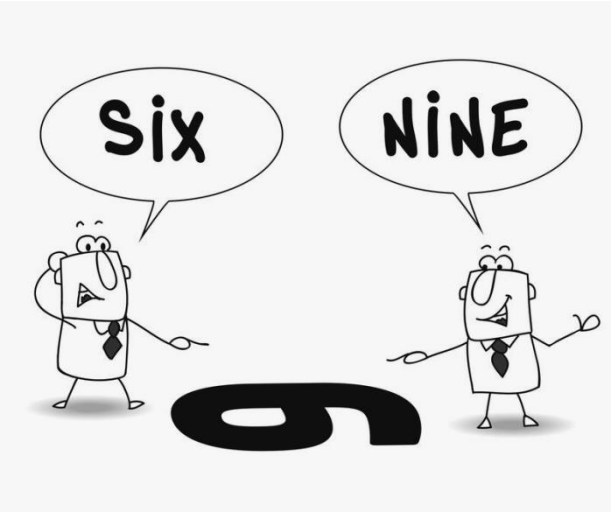




http://www.asimovinstitute.org/neural-network-zoo/

Часть 3.4

Уязвимости нейросетевых технологий



Задание 6.

Перечислите виды биометрических систем, которые используются в вашем Банке и которые не используются (какие знаете)

Используются в банке

1.

2.

3.

4.

5.

6.

Не используются

1.

2.

3.

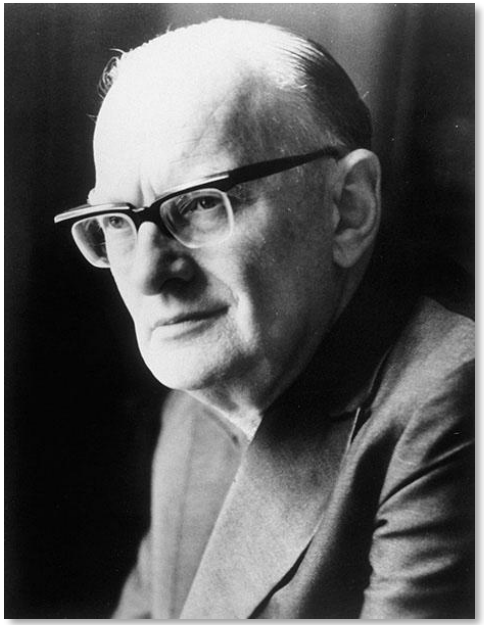
4.

5.

6.

«Если знаменитый, но старый ученый утверждает, что нечто возможно, он почти определенно прав. Если он утверждает, что нечто невозможно, он, очень вероятно, ошибается»

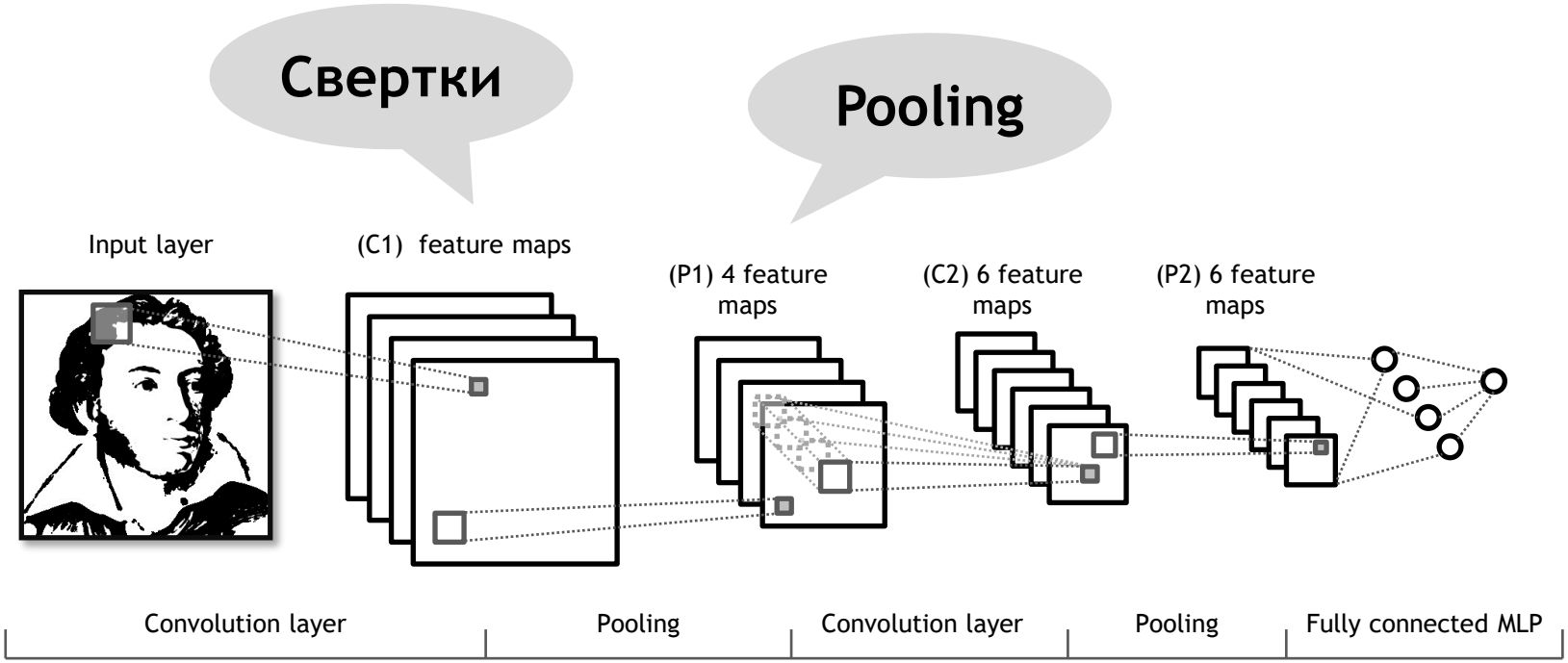
Артур Кларк



Как работает фото-биометрия?

Полиция американского города Ланкастер (штат Пенсильвания) смогла установить личность подозреваемого в краже благодаря портрету, который нарисовал один из свидетелей. При том, что портрет был, мягко говоря, схематичным. Уже на следующий день полиция установила личность предполагаемого преступника — им оказался бездомный по имени Хунг Фыок Нгуен.

Сверточные сети — это просто!



Фотобиометрия уязвима

Макияж от Яндекса

Григорий Бакунов, занимающий в Яндексе должность директора по распространению технологий, рассказал о своем стороннем проекте — сервисе, проектирующем уникальный случайный макияж, который бы защищал лицо пользователя от идентификации системой распознавания лиц.

Фотобиометрия уязвима — 2

Невидимая маска

Китайские исследователи создали бейсбольную кепку, оснащенную миниатюрными инфракрасными светодиодами, которые размещены таким образом, что лучи, падающие на лицо владельца головного убора, помогают не только скрыть его личность, но и «выдать себя за другого человека для прохождения биометрической аутентификации».

Invisible Mask: Practical Attacks on Face Recognition with Infrared

Zhe Zhou[1], Di Tang[2], Xiaofeng Wang[3], Weili Han[1], Xiangyu Liu[4], Kehuan Zhang[2]
[1]Fudan Univiersity, [2]CUHK, [3]IUB, [4]Alibaba Inc.
[1]zhouzhe@fudan.edu.cn

***Abstract*—Accurate face recognition techniques make a series of critical applications possible: policemen could employ it to retrieve criminals' faces from surveillance video streams; cross boarder travelers could pass a face authentication inspection line without the involvement of officers. Nonetheless, when public security heavily relies on such intelligent systems, the designers should deliberately consider the emerging attacks aiming at misleading those systems employing face recognition.**

We propose a kind of brand new attack against face recognition systems, which is realized by illuminating the subject using infrared according to the adversarial examples worked out by our algorithm, thus face recognition systems can be bypassed or misled while simultaneously the infrared perturbations cannot be observed by raw eyes. Through launching this kind of attack, an attacker not only can dodge surveillance cameras. More importantly, he can impersonate his target victim and pass the face authentication system, if only the victim's photo is acquired by the attacker. Again, the attack is totally unobservable by nearby people, because not only the light is invisible, but also the device we made to launch the attack is small enough. According to our study on a large dataset, attackers have a very high success rate with a over 70% success rate for finding such an adversarial example that can be implemented by infrared. To the best of our knowledge, our work is the first one to shed light on the severity of threat resulted from infrared adversarial examples against face recognition.

Fig. 2: A cap mounting our device.

GANы против фотобиометрии

Deepfakes

Пользователь Reddit под ником deepfakes в декабре 2017 года опубликовал фейковые порнографические ролики с участием голливудских актрис, созданные с помощью нейронных сетей. Уже в январе 2018 вышло десктопное приложение FakeApp, которое позволяет создавать подобные ролики пользователям, не обладающих навыками программирования.

А кто против GANов

XceptionNet

Европейские ученые научили алгоритм XceptionNet выявлять подмену лиц в видеороликах. Для обучения модели исследователи создали масштабный датасет FaceForensics из полумиллиона изображений, которые взяты из более чем тысячи видео, созданных с использованием алгоритма face2face. По точности распознавания XceptionNet превосходит уже существующие алгоритмы в несколько раз даже при оценке сжатых видео.

FaceForensics: A Large-scale Video Dataset for Forgery Detection in Human Faces

Andreas Rössler[1] Davide Cozzolino[2] Luisa Verdoliva[2] Christian Riess[3]
Justus Thies[1] Matthias Nießner[1]

[1]Technical University of Munich [2]University Federico II of Naples
[3]University of Erlangen-Nuremberg

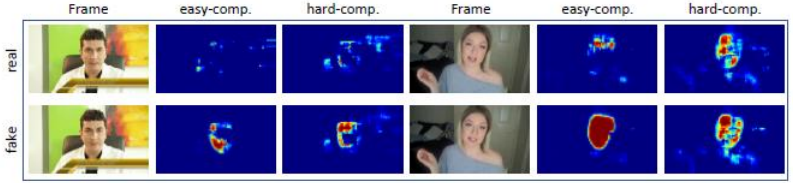
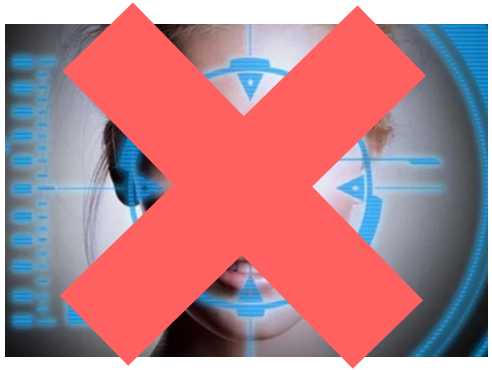


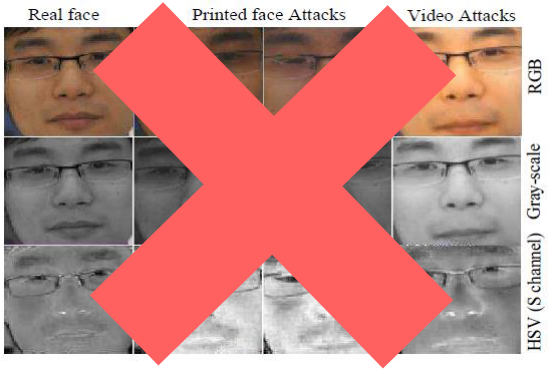
Fig. 6. Forgery segmentation vs. compression. With increasing compression rate, the segmentation results get worse. The XceptionNet-based method is still able to segment the manipulation in most cases, even under hard compression.

А что насчет Liveness Detection?

Интерактив



Текстуры

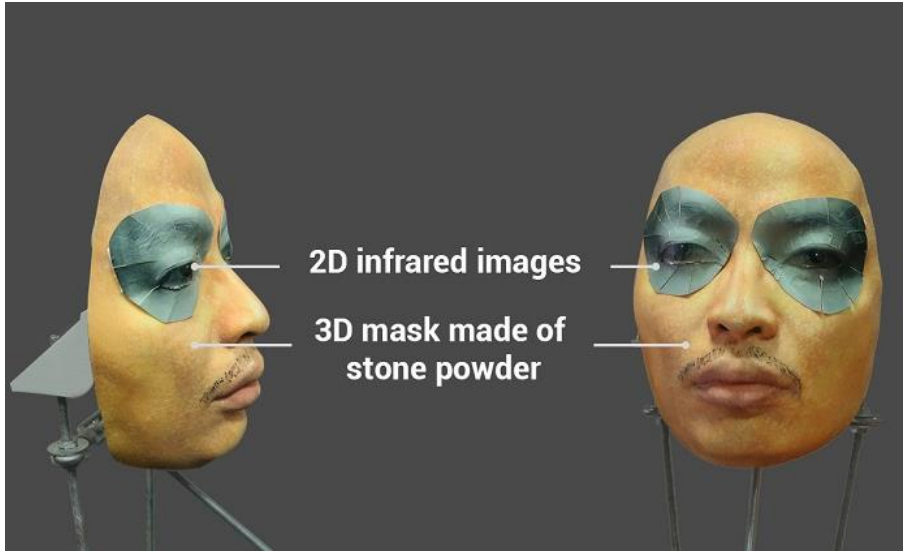


3D-камеры

3D-биометрия не спасет

FaceID взломан

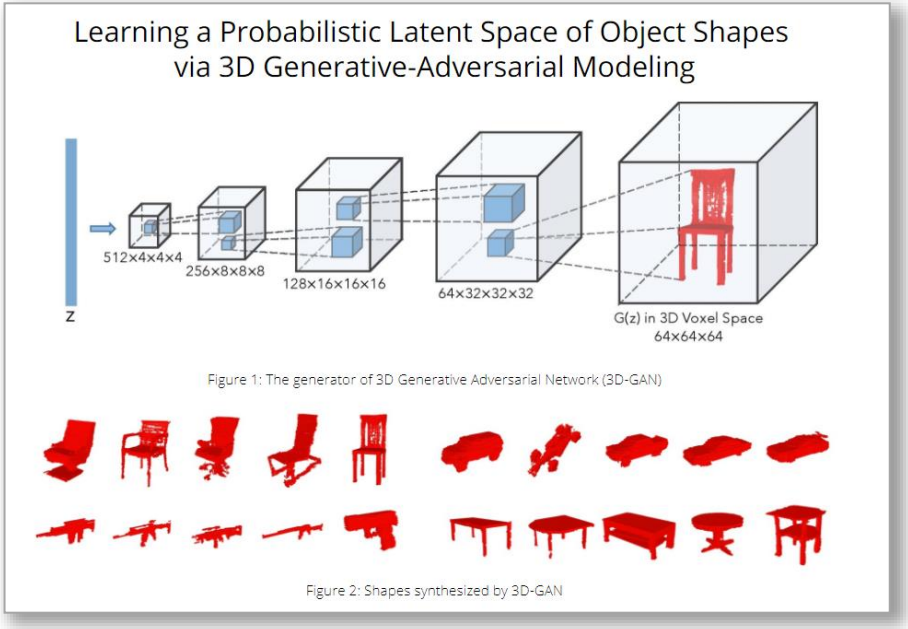
Через несколько недель после выхода iPhone X вьетнамская компания Bkav создала маску для обхода защиты FaceID. Первая версия маски состояла из четырех компонентов: основы, напечатанной на 3D-принтере; силиконовой копии носа; двухмерных изображений глаз; а также «специально рассчитанных» областей лица. Во второй версии использовалась только 3D-основа из каменного порошка и двумерные изображения глаз.



Генерация 3D-объектов

3D-GAN vs. IM2CAD

Ученые из MIT CSAIL и Google Research разработали ИИ на основе генеративно-состязательных сетей (GAN), который умеет генерировать 3D-объекты высокого качества. 3D-GAN превосходит по качеству предшествующие CAD-модели, которые умеют восстанавливать 3D-объекты по фотографиям.

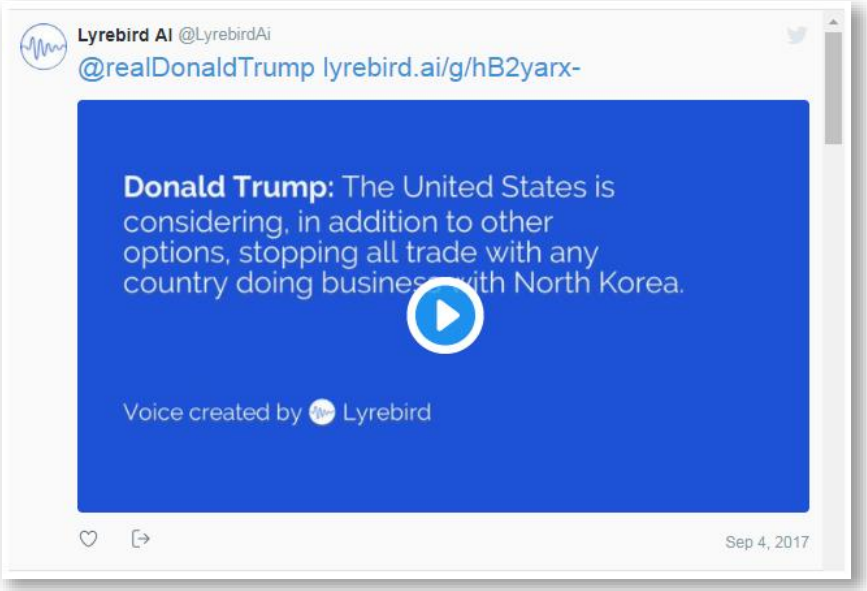


Голосовая биометрия не поможет

Lyrebird AI

TNW с испугом пишет о потенциале проекта Lyrebird для преступников. Эта система позволяет загрузить минуту своего голоса, а потом получить текст-ту-спич с голосом, похожим на ваш. Автор прав, сделать из, скажем, 2-3 часов речи очень приличный TTS можно, причем для этого подойдут уже готовые опенсорсные технологии.

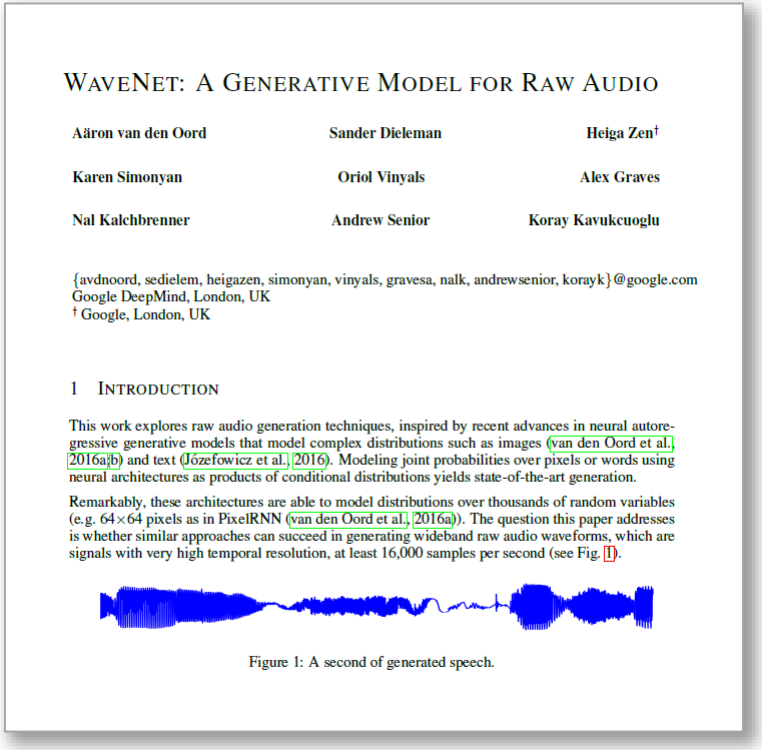
Григорий Бакунов, Яндекс



А как же Liveness Detection?

WaveNet

Компания Google DeepMind разработала нейронную сеть WaveNet, позволяющую генерировать речь по технологии TTS (text-to-speech). В основе WaveNet лежат разработанные ранее в DeepMind сверточная и рекуррентная архитектуры PixelCNN и PixelRNN. Компания DeepMind отмечает, что качество сгенерированной WaveNet речи практически неотличимо от настоящей. В первых релизах 2016 года отмечалось, что генерация 1 секунды речи занимала 1-2 минуты. Но позже эту проблему решили и уже в сентябре 2017 года WaveNet была встроена в Google Assistant.



WAVENET: A GENERATIVE MODEL FOR RAW AUDIO

Aäron van den Oord, Sander Dieleman, Heiga Zen†
Karen Simonyan, Oriol Vinyals, Alex Graves
Nal Kalchbrenner, Andrew Senior, Koray Kavukcuoglu

{avdnoord, sedielem, heigazen, simonyan, vinyals, gravesa, nalk, andrewsenior, korayk}@google.com
Google DeepMind, London, UK
† Google, London, UK

1 INTRODUCTION

This work explores raw audio generation techniques, inspired by recent advances in neural autoregressive generative models that model complex distributions such as images (van den Oord et al., 2016a;b) and text (Józefowicz et al., 2016). Modeling joint probabilities over pixels or words using neural architectures as products of conditional distributions yields state-of-the-art generation.

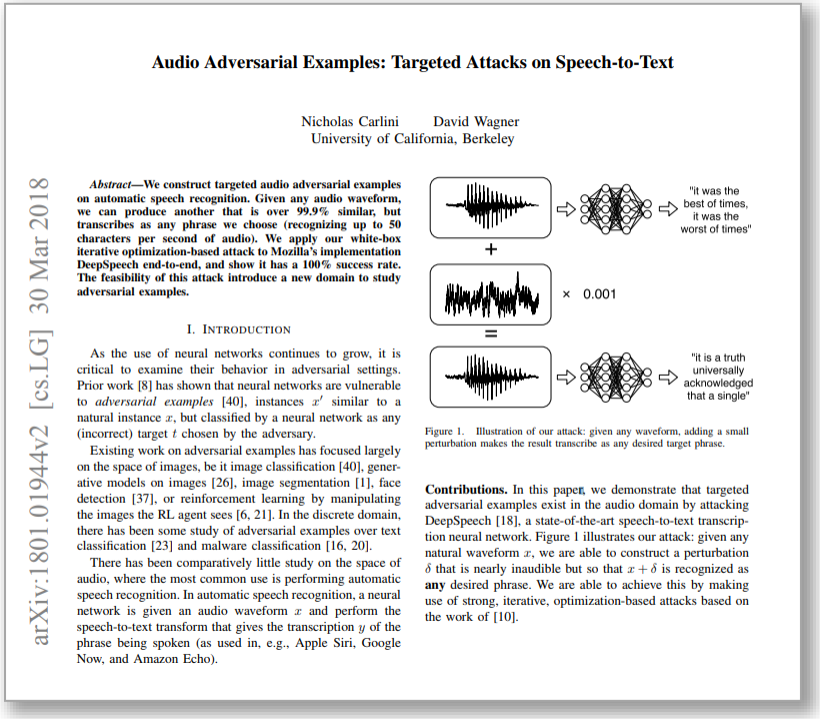
Remarkably, these architectures are able to model distributions over thousands of random variables (e.g. 64×64 pixels as in PixelRNN (van den Oord et al., 2016a)). The question this paper addresses is whether similar approaches can succeed in generating wideband raw audio waveforms, which are signals with very high temporal resolution, at least 16,000 samples per second (see Fig. 1).

Figure 1: A second of generated speech.

Атака на голосовые помощники

(Не)случайный шум

Исследователи из Китая и США показали, что они могут отправлять набор звуков, за пределами человеческой слышимости (или замаскированных среди музыки), которые Siri, Alexa или помощник Google воспринимают как команды. Исследователи смогли тайно активировать системы ИИ на смартфонах и смарт-динамиках, заставляя их набирать номера телефонов или открывать веб-сайты. В руках преступников технология может быть использована для разблокировки дверей, перевода денег или покупки вещей в интернете — просто с музыкой, играющей по радио.



Audio Adversarial Examples: Targeted Attacks on Speech-to-Text

Nicholas Carlini David Wagner
University of California, Berkeley

arXiv:1801.01944v2 [cs.LG] 30 Mar 2018

***Abstract*—We construct targeted audio adversarial examples on automatic speech recognition. Given any audio waveform, we can produce another that is over 99.9% similar, but transcribes as any phrase we choose (recognizing up to 50 characters per second of audio). We apply our white-box iterative optimization-based attack to Mozilla's implementation DeepSpeech end-to-end, and show it has a 100% success rate. The feasibility of this attack introduce a new domain to study adversarial examples.**

I. Introduction

As the use of neural networks continues to grow, it is critical to examine their behavior in adversarial settings. Prior work [8] has shown that neural networks are vulnerable to *adversarial examples* [40], instances x' similar to a natural instance x, but classified by a neural network as any (incorrect) target t chosen by the adversary.

Existing work on adversarial examples has focused largely on the space of images, be it image classification [40], generative models on images [26], image segmentation [1], face detection [37], or reinforcement learning by manipulating the images the RL agent sees [6, 21]. In the discrete domain, there has been some study of adversarial examples over text classification [23] and malware classification [16, 20].

There has been comparatively little study on the space of audio, where the most common use is performing automatic speech recognition. In automatic speech recognition, a neural network is given an audio waveform x and perform the speech-to-text transform that gives the transcription y of the phrase being spoken (as used in, e.g., Apple Siri, Google Now, and Amazon Echo).

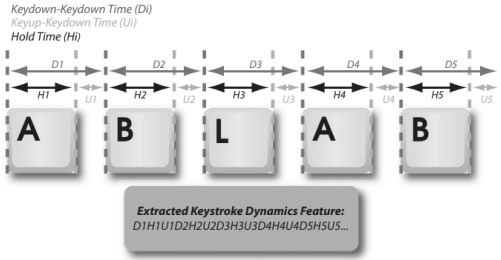
Figure 1. Illustration of our attack: given any waveform, adding a small perturbation makes the result transcribe as any desired target phrase.

Contributions. In this paper, we demonstrate that targeted adversarial examples exist in the audio domain by attacking DeepSpeech [18], a state-of-the-art speech-to-text transcription neural network. Figure 1 illustrates our attack: given any natural waveform x, we are able to construct a perturbation δ that is nearly inaudible but so that $x + \delta$ is recognized as **any** desired phrase. We are able to achieve this by making use of strong, iterative, optimization-based attacks based on the work of [10].

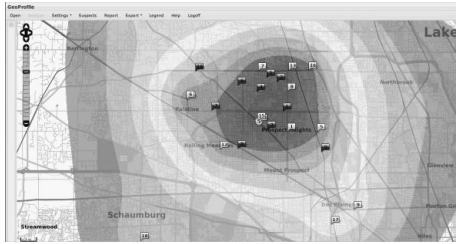
Может тогда Behavioral Biometrics?

Classification of the various types of behavioural biometrics	Direct human computer interaction			Indirect human computer interaction	Motor skill	Purely behavioural	Properties of behavioural biometrics			
	Authorship	Input device interaction based	Software interaction based				Enrolment time	Verification time	Identification	Required hardware
Audit logs				•			D	D	N	Computer
Biometric sketch	•					•	M	S	N	Mouse
Blinking					•		M	S	N	Camera
Call-stack				•			D	H	N	Computer
Calling behaviour						•	D	D	N	Phone
Car driving style						•	H	M	N	Car sensors
Command line lexicon			•			•	H	H	N	Computer
Credit card use						•	D	D	N	Credit card
Dynamic facial features					•		M	S	N	Camera
E-mail behaviour	•		•			•	D	M	N	Computer
Gait/stride					•		M	S	N	Camera
Game strategy			•			•	H	H	N	Computer
GUI interaction				•			D	H	N	Computer
Handgrip					•		M	S	N	Gun sensors
Haptic		•			•		M	M	N	Haptic
Keystroke dynamics		•			•		M	S	N	Keyboard
Lip movement					•		M	S	N	Camera
Mouse dynamics		•			•		M	S	N	Mouse
Network traffic				•			D	D	N	Computer
Painting style	•					•	D	D	N	Scanner
Programming style	•		•			•	H	H	N	Computer
Registry Access				•			D	H	N	Computer
Signature/Handwriting					•		M	S	Y	Stylus
Storage Activity				•			D	D	N	Computer
System Calls				•			D	H	N	Computer
Tapping					•		M	S	N	Sensor
Text Authorship	•					•	H	M	N	Computer
Voice/Speech/Singing					•		M	S	Y	Microphone

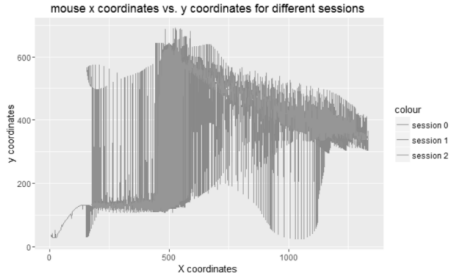
Keystroke Dynamics



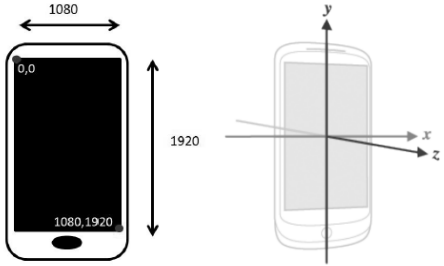
GPS (geo profiling)



Mouse movements



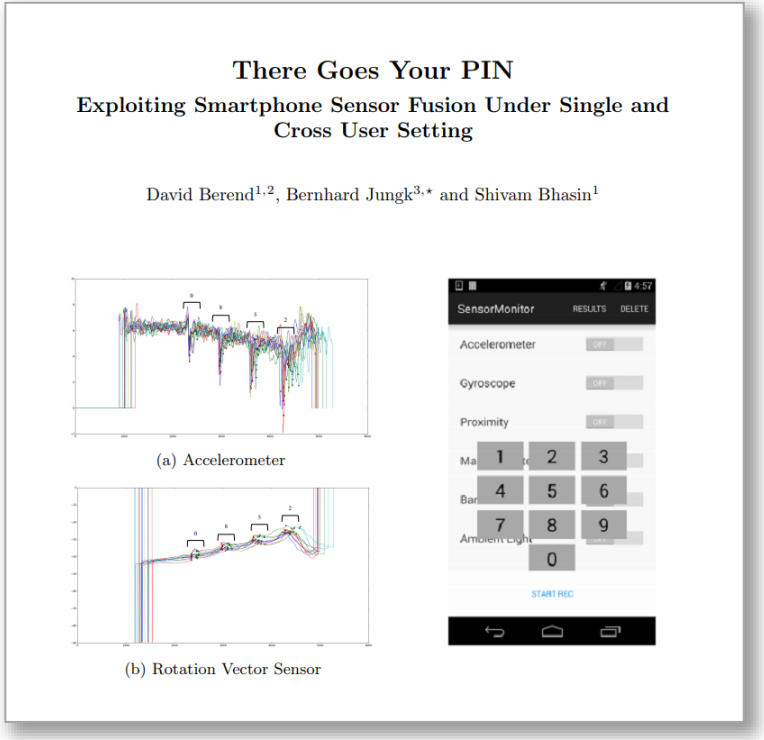
Sensor Fusion



… если не закроют данные

PIN-коды не надежны

Нейросеть научили распознавать PIN-код пользователя с точностью 84%. Исследователи в области информационной безопасности использовали для определения PIN-кода смартфона данные с его датчиков. Они написали приложение для Android-смартфонов, которое собирает данные с шести датчиков (для их использования приложению не нужно получать разрешение пользователя): акселерометр, гироскоп, датчик вращения, магнитометр и датчик освещенности.



There Goes Your PIN

Exploiting Smartphone Sensor Fusion Under Single and Cross User Setting

David Berend[1,2], Bernhard Jungk[3,*] and Shivam Bhasin[1]

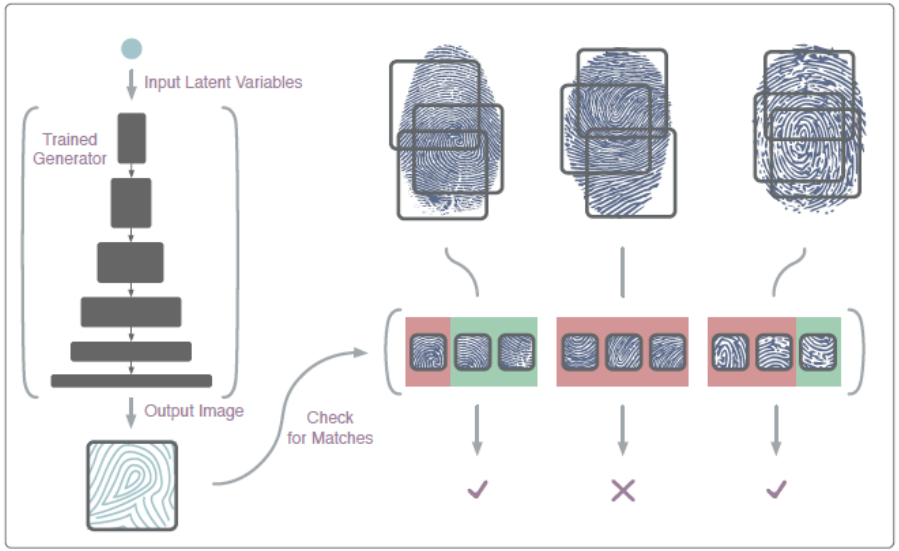
(a) Accelerometer

(b) Rotation Vector Sensor

Отпечатки не панацея…

DeepMasterPrints

Ресерчеры из NYU обучили генеративную нейронную сеть для создания искусственных отпечатков пальцев, которые работают как «главный ключ» для биометрических систем идентификации. Метод работает по принципу «атаки словаря» против паролей, когда хакер подбирает пароль по заранее сгенерированному списку общих паролей к системе безопасности.

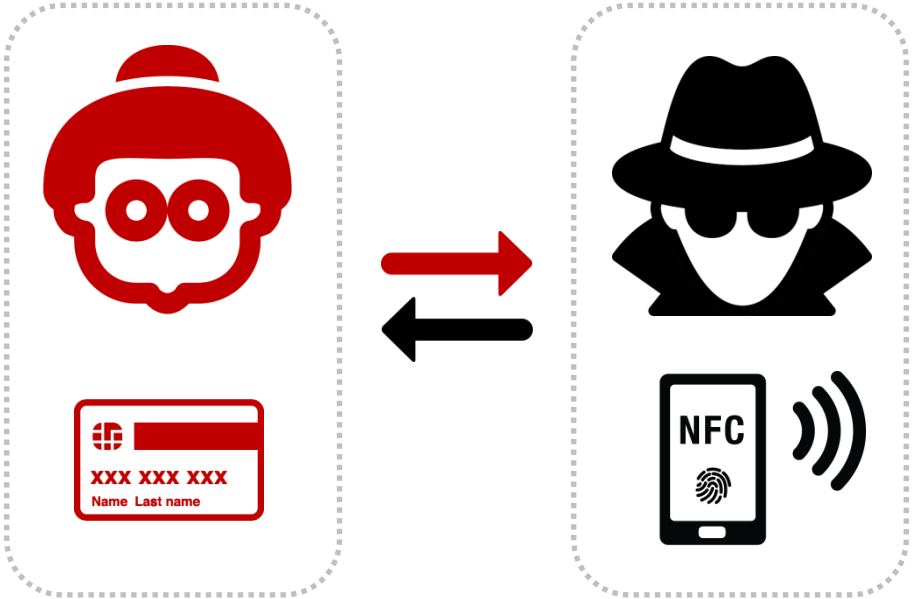


Latent Variable Fitness Function

… и помогают мошенникам

Fraud Apple Pay

Мошенники привязывают к своим Apple-кошелькам скомпрометированные карты клиентов. Данные по картам, включая одноразовые SMS-пароли, злоумышленники получают методами социальной инженерии. После этого мошенники могут беспрепятственно использовать свой iPhone для оплаты товаров и услуг в магазинах.



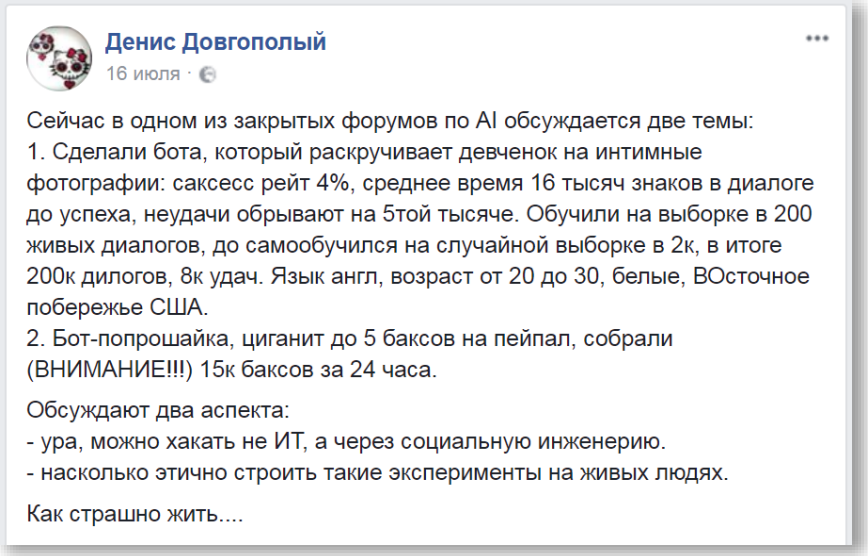
Социальная инженерия

Сейчас

Интервью со Skype-мошенником
https://habrahabr.ru/post/255225/

1. Нанимают студентов
2. Обучают их психологии
3. Выдают ворованные Skype-логины
4. Платят 50% с выручки
5. Profit

Скоро… или сейчас?



Денис Довгополый
16 июля ·

Сейчас в одном из закрытых форумов по AI обсуждается две темы:
1. Сделали бота, который раскручивает девченок на интимные фотографии: саксесс рейт 4%, среднее время 16 тысяч знаков в диалоге до успеха, неудачи обрывают на 5той тысяче. Обучили на выборке в 200 живых диалогов, до самообучился на случайной выборке в 2к, в итоге 200к дилогов, 8к удач. Язык англ, возраст от 20 до 30, белые, ВОсточное побережье США.
2. Бот-попрошайка, циганит до 5 баксов на пейпал, собрали (ВНИМАНИЕ!!!) 15к баксов за 24 часа.

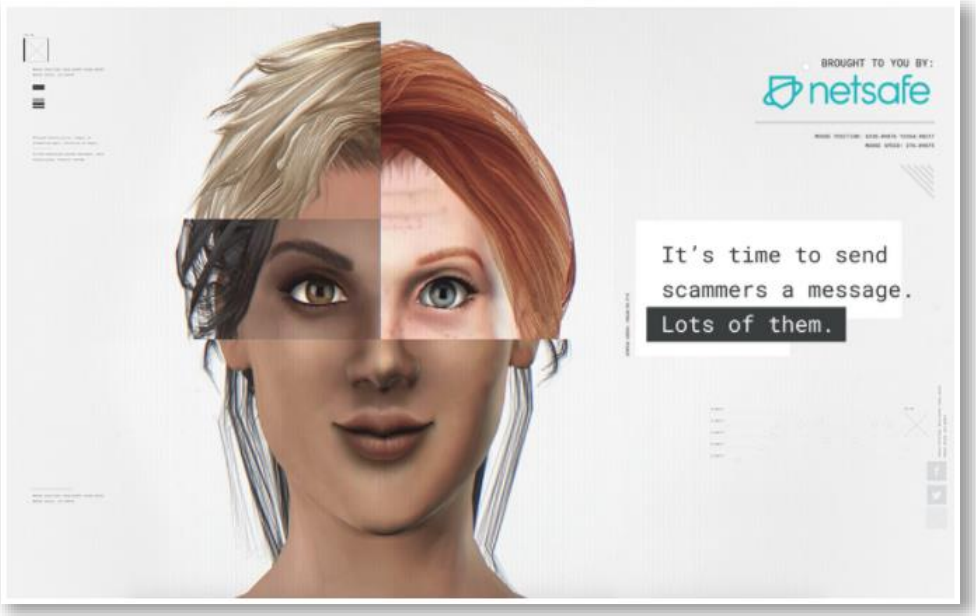
Обсуждают два аспекта:
- ура, можно хакать не ИТ, а через социальную инженерию.
- насколько этично строить такие эксперименты на живых людях.

Как страшно жить....

Чат-бот «Отвлекайка»

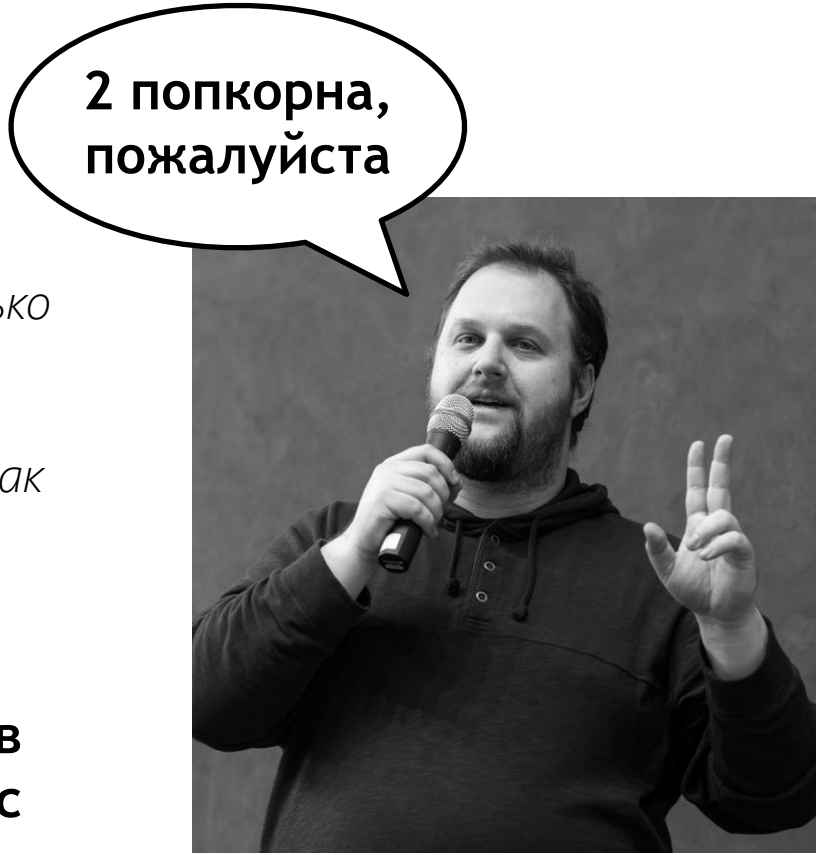
RE:SCAM

Чат-бот умеет распознавать тип фишинговых писем, подстраиваться под них и задавать мошенникам бесконечную серию вопросов. Чат-бот выражает заинтересованность в теме «нигерийских» писем, пытаясь узнать подробности, шутить и казаться «наивным». По мнению Netsafe, такое общение должно снизить эффективность мошенников — у них не будет времени на «живых» пользователей.



«Следующие 10 лет мы будем не только учиться создавать искусственный интеллект, но и обманывать его, делать анти-обманные системы и так далее. Война предстоит не хуже, чем вирусно-антивирусная, готовьтесь!»

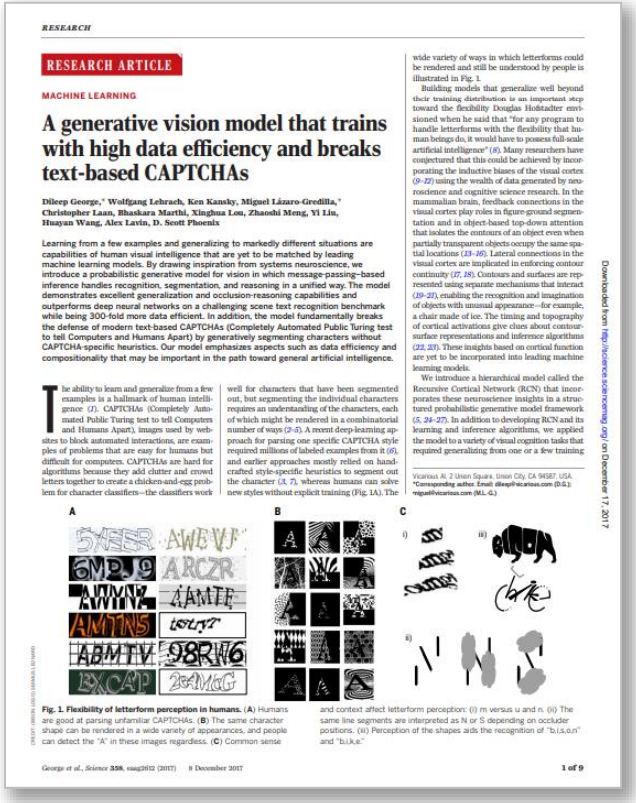
Григорий Бакунов
Яндекс



Капчу взломали! Расходимся!

RCN vs. CAPTCHA

Разработчики американской компании Vicarious создали алгоритм, эффективно расшифровывающий капчу — самый распространенный на сегодняшний день способ отличить человека от робота. Такой алгоритм работает на основе компьютерного зрения и рекурсивной кортикальной нейросети, и может расшифровать капчу на многих популярных интернет-платформах, в том числе на PayPal и Yahoo. Работа опубликована в журнале Science.



RESEARCH

RESEARCH ARTICLE

MACHINE LEARNING

A generative vision model that trains with high data efficiency and breaks text-based CAPTCHAs

Dileep George,* Wolfgang Lehrach, Ken Kansky, Miguel Lázaro-Gredilla,* Christopher Laan, Bhaskara Marthi, Xinghua Lou, Zhaoshi Meng, Yi Liu, Huayan Wang, Alex Lavin, D. Scott Phoenix

Learning from a few examples and generalizing to markedly different situations are capabilities of human visual intelligence that are yet to be matched by leading machine learning models. By drawing inspiration from systems neuroscience, we introduce a probabilistic generative model for vision in which message-passing–based inference handles recognition, segmentation, and reasoning in a unified way. The model demonstrates excellent generalization and occlusion-reasoning capabilities and outperforms deep neural networks on a challenging scene text recognition benchmark while being 300-fold more data efficient. In addition, the model fundamentally breaks the defense of modern text-based CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart) by generatively segmenting characters without CAPTCHA-specific heuristics. Our model emphasizes aspects such as data efficiency and compositionality that may be important in the path toward general artificial intelligence.

The ability to learn and generalize from a few examples is a hallmark of human intelligence (*1*). CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart), images used by websites to block automated interactions, are examples of problems that are easy for humans but difficult for computers. CAPTCHAs are hard for algorithms because they add clutter and crowd letters together to create a chicken-and-egg problem for character classifiers—the classifiers work well for characters that have been segmented out, but segmenting the individual characters requires an understanding of the characters, each of which might be rendered in a combinatorial number of ways (*2*–*5*). A recent deep-learning approach for parsing one specific CAPTCHA style required millions of labeled examples from it (*6*), and earlier approaches mostly relied on hand-crafted style-specific heuristics to segment out the character (*3*, *7*), whereas humans can solve new styles without explicit training (Fig. 1A). The wide variety of ways in which letterforms could be rendered and still be understood by people is illustrated in Fig. 1.

Building models that generalize well beyond their training distribution is an important step toward the flexibility Douglas Hofstadter envisioned when he said that "for any program to handle letterforms with the flexibility that human beings do, it would have to possess full-scale artificial intelligence" (*8*). Many researchers have conjectured that this could be achieved by incorporating the inductive biases of the visual cortex (*9*–*22*) using the wealth of data generated by neuroscience and cognitive science research. In the mammalian brain, feedback connections in the visual cortex play roles in figure-ground segmentation and in object-based top-down attention that isolates the contours of an object even when partially transparent objects occupy the same spatial locations (*13*–*16*). Lateral connections in the visual cortex are implicated in enforcing contour continuity (*17*, *18*). Contours and surfaces are represented using separate mechanisms that interact (*19*–*21*), enabling the recognition and imagination of objects with unusual appearance—for example, a chair made of ice. The timing and topography of cortical activations give clues about contour-surface representations and inference algorithms (*22*, *23*). These insights based on cortical function are yet to be incorporated into leading machine learning models.

We introduce a hierarchical model called the Recursive Cortical Network (RCN) that incorporates these neuroscience insights in a structured probabilistic generative model framework (*5*, *24*–*27*). In addition to developing RCN and its learning and inference algorithms, we applied the model to a variety of visual cognition tasks that required generalizing from one or a few training

Vicarious AI, 2 Union Square, Union City, CA 94587, USA.
*Corresponding author. Email: dileep@vicarious.com (D.G.); miguel@vicarious.com (M.L.-G.)

Downloaded from http://science.sciencemag.org/ on December 17, 2017

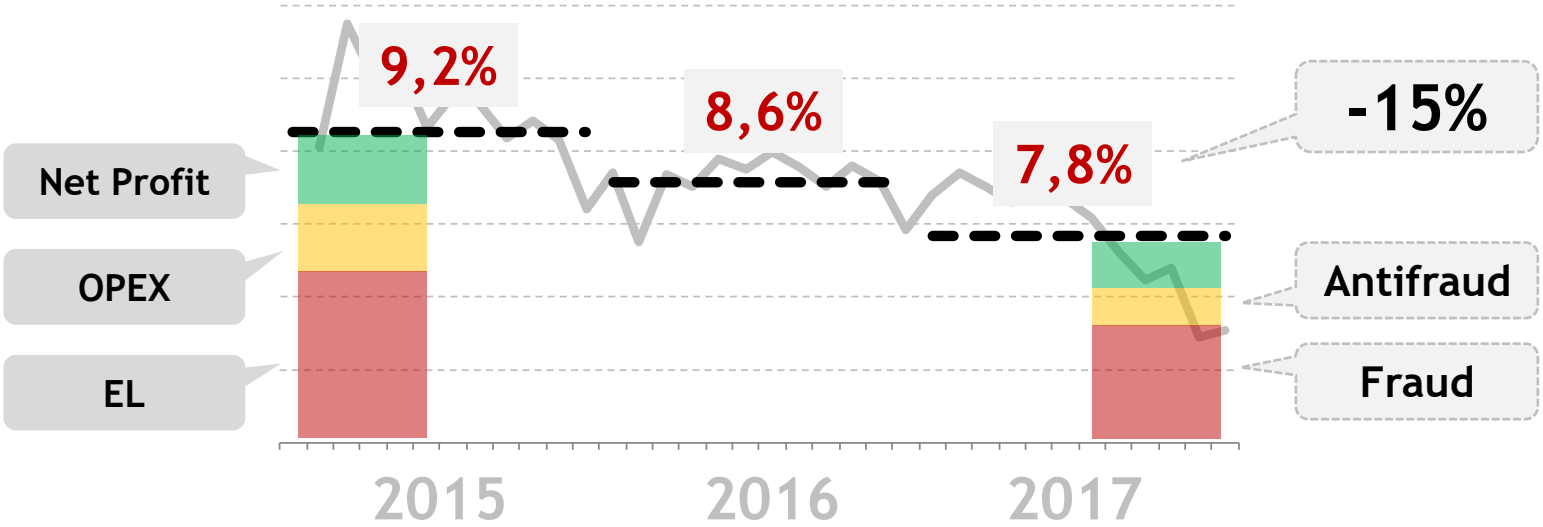
Fig. 1. Flexibility of letterform perception in humans. (**A**) Humans are good at parsing unfamiliar CAPTCHAs. (**B**) The same character shape can be rendered in a wide variety of appearances, and people can detect the "A" in these images regardless. (**C**) Common sense and context affect letterform perception: (i) m versus u and n. (ii) The same line segments are interpreted as N or S depending on occluder positions. (iii) Perception of the shapes aids the recognition of "b,i,s,o,n" and "b,i,k,e."

Заключение

Антифрод — трансформация или смена парадигмы?

Процентная маржа снижается

«Кредиты–Депозиты» **свыше 1 года**



Источник: www.cbr.ru

DarkNet

Найдется всё

Free

http://moneymaker.hk/

http://fsell.info/

https://hpc.name/index.html

http://darkmoney.cc/

Tor

https://dark3zzgex3xwmcj.onion.link/forums/

https://dublik2uqiorycsj.onion/forums/

https://y3pggjcimtcglaon.onion/

http://olimpik4w3pb6p4u.onion/index.php?/forum/

Ваши карты продают дропам

Опции темы

2 недель(и) назад #1

Markus2017
Новенький

Регистрация: 14.05.2017
Сообщений: 52
Сказал(а) спасибо: 4
Поблагодарили 2 раз(а) в 1 сообщении

Почтабанк на ваши данные

Продам карты почта банк на ваши сканы.
1 карта = 4.000
телеграмм @Oliver0803
карты будут оформляться на ваши сим.
PS Работа через гарант

Не гонитесь за дешевизной. Уважающие свою работу продавцы имеют достаточно клиентов и хорошо знают рынок, потому никогда не станут продавать свои товары/услуги за копейки. Дешевая цена – инструмент мошенников, а ваша жадность может привести к бедности.

http://fsell.info/showthread.php?t=68236

Ваш андеррайтинг у мошенников

28.03.2016, 20:02 #1

Archie Goodwin
Подающий надежды

Регистрация: 01.01.2016
Сообщений: 26
Депозит: 0 р.
Сделок через ГАРАНТ: 0
Покупок через ГАРАНТ:

Инструкции для андеррайтеров

Доброго времени, участники форума. Возможно кому то будет интересно, предлагаю вашему вниманию 2 инструкции по рассмотрению заявок для андеррайтеров одного крупного московского банка. Скажу сразу "слизана" практически полностью у сбербанка. Для себя Вы можете почерпнуть много нового, узнать что происходит с заявкой после подачи, также раскрываются такие моменты, как "Основные признаки полной или частичной подделки документов", "Порядок проверки клиента по информационным массивам", "Верификация", Оценка кредитоспособности", "Алгоритмы определения кредитной истории", "Факторы принятия решения". Думаю будет интересно всем, от посредников до брокеров. Все представлено в цифровом варианте(отсканировано). 2 файла по 100 стр. Стоимость 4к. Гарант за ваш счет. Писать СТРОГО в ЛС или Jabber.

Оглавление [Ссылки могут видеть только зарегистрированные пользователи. Зарегистрироваться...]

_____

Все сделки и реквизиты подтверждать в ЛС.
Связь только в ЛС или jabber+OTR
[Ссылки могут видеть только зарегистрированные пользователи. Зарегистрироваться...]

ЦИТАТА

http://moneymaker.hk/klassicheskie-kredity-zaimy-29/instrukcii-dlya-anderraiterov-19377/

Ваших сотрудников “хантят”

18.04.2016, 19:56 #1

Мри
Подающий надежды

Регистрация: 18.04.2016
Сообщений: 2
Депозит: 0 р.
Сделок через ГАРАНТ: 0
Покупок через ГАРАНТ:

Требуется "свой" человек в банке

Нужен человек в банке, желательно на уровне одобрения кредита. СПб. Для тесного сотрудничества. Связь ICQ 695 479 631

Последний раз редактировалось Мри; 24.04.2016 в 20:21.

ЦИТАТА

http://moneymaker.hk/klassicheskie-kredity-zaimy-29/trebuetsya-svoi-chelovek-v-banke-19488/

Ваших клиентов продают в Telegram

Ваших клиентов продают в Telegram — 2

Банки
- Сбербанк – 5.000 руб./месяц
- ВТБ – 5.000 руб./месяц
- Альфа-банк – 5.000 руб./месяц
- Тинькофф – 5.000 руб./месяц

Владелец мобильного телефона (ФИО и паспорт)
- МТС – 700-1.000 руб.
- Билайн – 500-800 руб.
- Мегафон – 2.000-2.500 руб.
- ТЕЛЕ2 – 2.000-2.500 руб.
- ЙОТА – 4.000-4.500 руб.

Операторы (дополнительные услуги)
- Текст СМС – 100.000-130.000 руб./месяц
- Пробив IMEI – 60.000-90.000 руб.
- Зонтик «5 ближайших телефонов к абоненту» – 90.000 руб.
- Прослушка – от 2.000 евро/сутки
- Перехват интернет-трафика – от 400.000 руб.

Детализация звонков и смс без базовых станций/с баз. станциями
- МТС – от 10.000 руб./месяц
- Билайн – от 1.800 руб./месяц
- Мегафон – от 12.000 руб./месяц
- ТЕЛЕ2 – от 6.000 руб./месяц
- ЙОТА – от 45.000 руб./месяц

Вспышка
- Местоположение владельца сим-карты с точностью 100% – 20.000-40.000 руб.

Передвижение
- Авиа и ЖД по РФ – 7.000 руб./год
- Бронь билетов – 8.000 руб./месяц
- Список пассажиров – 15.000 руб.
- Мигрант – 4.000 руб.
- Магистраль – 7.000 руб.
- Пересечение границы – 6.000 руб./год
- Флажок на человека (мгновенное оповещение при выезде/въезде) – 100.000 руб./месяц

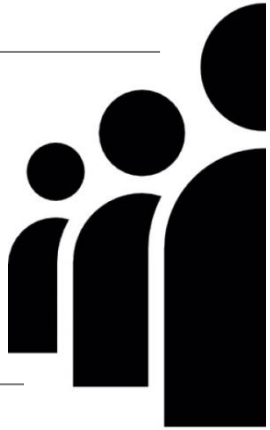
Пробив по госструктурам
- МВД – 2.000 руб.
- Розыск – 2.000 руб.
- ГИБДД – 1.500 руб.
- ЗАГС – 6.000 руб.

Авто
- Пробив авто – 500 руб.
- Подбор ВУ – 1.500 руб.
- Подбор авто для свидетельства о регистрации (СОР) – 2.000 руб.

Социальные сети
- Поиск номера привязанного к странице Вконтакте
- Поиск страницы Вконтакте по номеру телефона
- Поиск страницы Instagram по номеру телефона
- Поиск страницы Facebook по номеру телефона
- Поиск e-mail по странице ВКонтакте

Источник: https://telegra.ph/Obzor-uslug-po-probivu-08-09

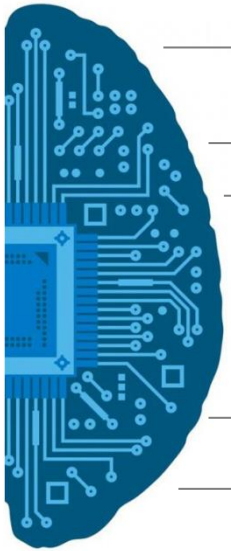
Антифрод в банке



Аудит

Криминалистика

Аналитика



Аудит

Криминалистика

Аналитика

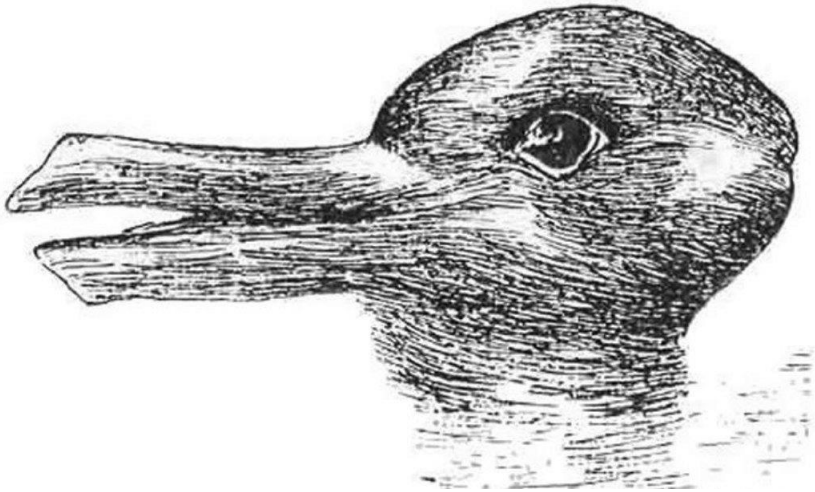
Экономика

IT security

Machine Learning

Block chain

Трансформация или смена парадигмы?



Спасибо за внимание!

Афанасьев Сергей

Исполнительный директор
Начальник управления статистического анализа

КБ «Ренессанс Кредит»

svafanasev@gmail.com

APPENDIX

Курсы на coursera.org

Введение в машинное обучение
Воронцов К.В., Соколов Е.
National Research University Higher School of Economics, Yandex School of Data Analysis

Machine Learning
Andrew Ng
Stanford University

Neural Networks and Deep Learning
Andrew Ng
deeplearning.ai

Improving Deep Neural Networks
Andrew Ng
deeplearning.ai

Structuring Machine Learning Projects
Andrew Ng
deeplearning.ai

Convolutional Neural Networks
Andrew Ng
deeplearning.ai

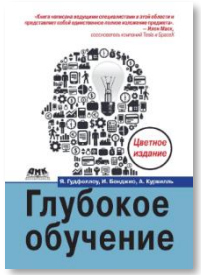
Sequence Models
Andrew Ng
deeplearning.ai

Книги на русском языке

Введение в машинное обучение с помощью Python

Мюллер А., Гидо С.

O'Reilly Media, 2017. — 392 с.



Глубокое обучение

Ян Гудфеллоу, Иошуа Бенджио, Аарон Курвилль

ДМК-Пресс, 2018. — 652 с.

Глубокое обучение: погружение в мир нейронных сетей

Николенко С., Кадурин А., Архангельская Е.

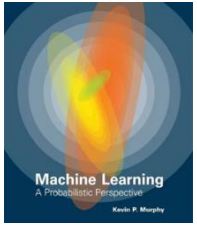
СПб.: Питер, 2018. — 480 с.

Библиотека Keras — инструмент глубокого обучения

Антонио Джулли, Суджит Пал

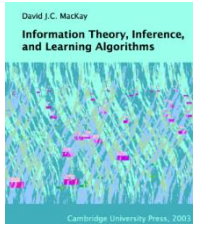
ДМК-Пресс, 2017. — 296 с.

Книги на английском языке



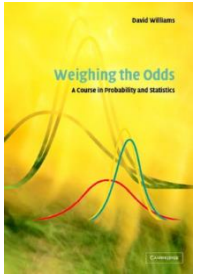
Machine Learning: A Probabilistic Perspective
Murphy K.P.

Massachusetts Institute of Technology, 2012. — 1067 p.



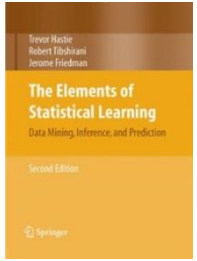
Information Theory, Inference, and Learning Algorithms
MacKay D.J.C.

Cambridge University Press, 2003. — 640 p



Weighing the Odds: A Course in Probability and Statistics
David Williams

Cambridge University Press, 2001. — 568 p.



The Elements of Statistical Learning: Data Mining, Inference, and Prediction
Hastie T., Tibshirani R., Friedman J.

Second Edition (corrected 5th printing). — Springer, 2009. — 763 p.

Лекции и полезные ресурсы

https://www.youtube.com/playlist?list=PLJOzdkh8T5kp99tGTEFjH_b9zqEQiiBtC

Лекции ШАД от Константина Воронцова (д.ф.м.н. МФТИ, ВШЭ)

https://www.lektorium.tv/speaker/2691

Лекции Сергея Николенко (автор книги «Глубокое обучение: погружение в мир нейронных сетей»)

http://efimov-ml.com/

Сайт с лекциями Дмитрия Ефимова, а также с Python-скриптами (Jupiter Notebooks), презентациями и ссылками

http://deepbayes.ru/2017/

Лекции ВШЭ по Байесовским методам в глубинном обучении. Лекторы: Дмитрий Ветров, Дмитрий Кропотов, Евгений Соколов, Сергей Бартунов, Арсений Ашуха и др.

https://arxiv.org/

Ресурс с самыми свежими препринтами научных статей по ML/AI/DS (см. раздел Computer Science)

http://scikit-learn.org/
http://www.numpy.org/
https://pandas.pydata.org/
https://keras.io/
http://devdocs.io/tensorflow/

Подробные мануалы популярных библиотек в Python

https://stackoverflow.com/

Ресурс для обсуждения практических вопросов по программированию на Python и других языках

http://ods.ai/

Русскоязычное сообщество датасайнтистов