



Антифрод в банке

И роль аналитики в банковском антифроде

Афанасьев Сергей
КБ «Ренессанс Кредит»

Ноябрь, 2017
Москва

Антифрод в банке:



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



Е.Н. 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



Слабые превентивные



Сильные директивные



Автоматизация процессов
Согласование инициатив
СВА антифрод-систем
Мониторинг деятельности
ФМС
Анализ fraud-сегментов
Проверка сотрудников
Fraud Report
Биометрия
Мотивационная схема
Ad hoc
Warning System
Концентрация
Банкроты (Interfax)
Concentration Report
Телеком (Мегафон и др.)
Обучение сотрудников
Исследования (FTI)
Предиктивная аналитика
Организация процессов
ФССП
Разработка правил
Партнерский договор
Аудит процессов
ПФР
ФНС
Визуальная оценка
Machine Learning
СВА антифрод-процессов
СПАРК, Контур.Фокус и др.
Идентификация клиента
Block Report
Black-lists
FPS, AFS (межбанк)
Проверка партнеров
Оценка fraud-потерь
Соцсети (Mail.ru и др.)
AFS (local) и др.

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

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

Антифрод-системы



Внутренние системы

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



Внешние сервисы

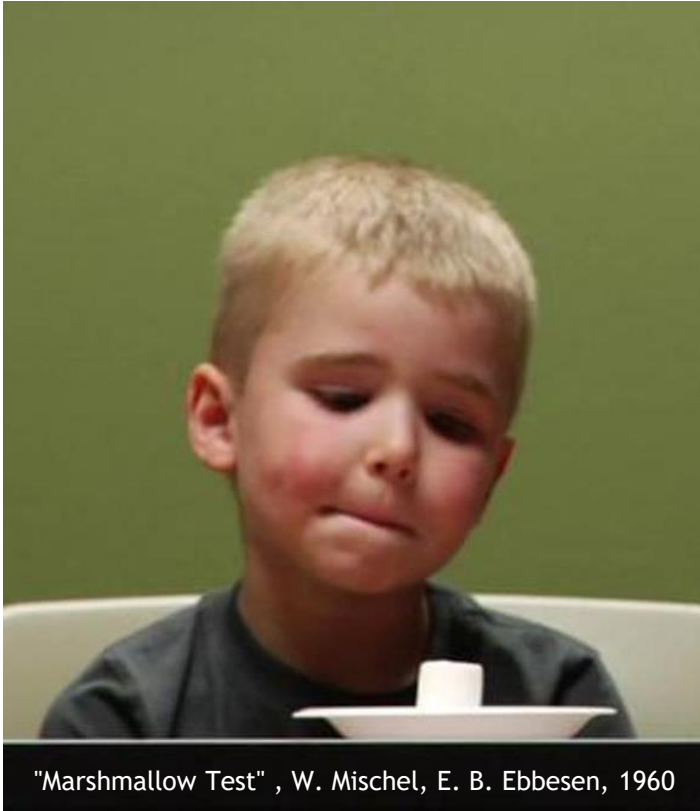
- FPS, AFS (межбанк)
- FPS.Bio
- Телеком (Мегафон и др.)
- Соцсети (Mail.ru и др.)
- Cookie (Rambler и др.)
- СПАРК, Контур.Фокус и др.
- Банкроты (Interfax)



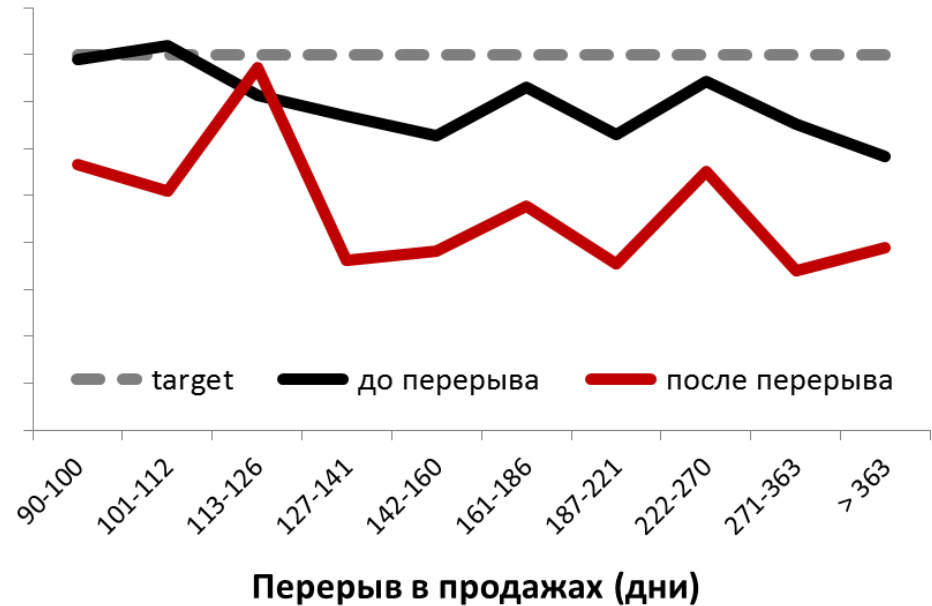
Гос. сервисы

- ФМС
- ФССП
- ПФР
- ФНС

Зефирный тест



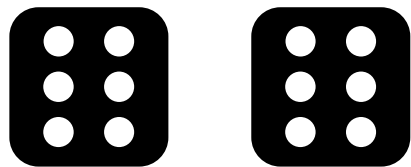
Риски по «спящим» точкам
ниже после «пробуждения»



Бином Ньютона

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

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



$n=2, k=2, d \approx 16,7\%: P \approx 2,8\%$

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

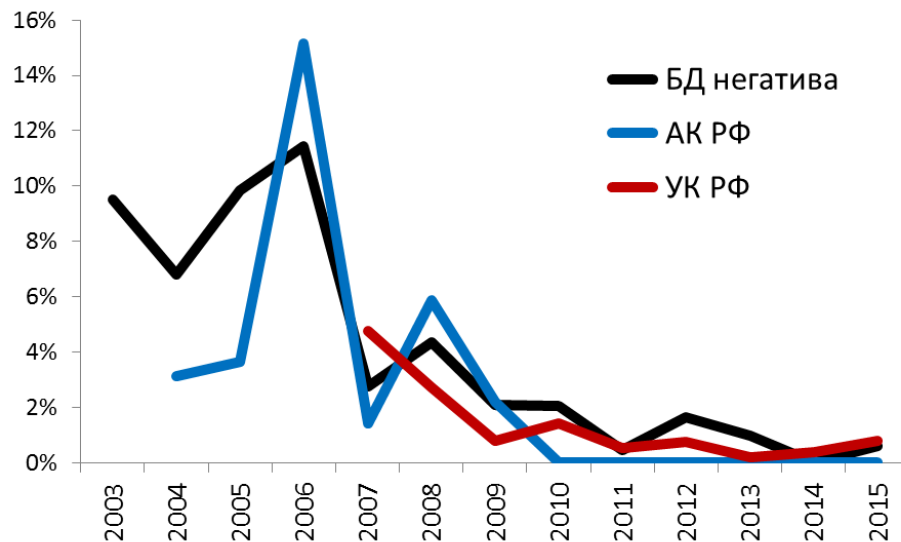
1*T ÷ 2*T

< T

Эксперимент «Обе белые»



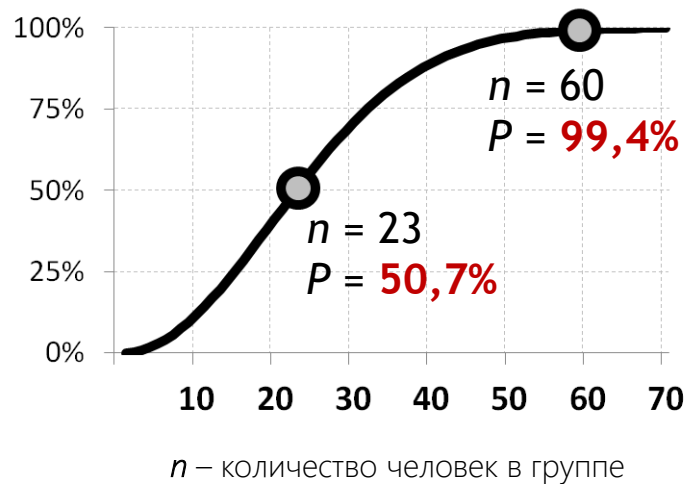
После 2006 года просрочка по Экспертизе сильно снизилась



Задача о близнецах

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

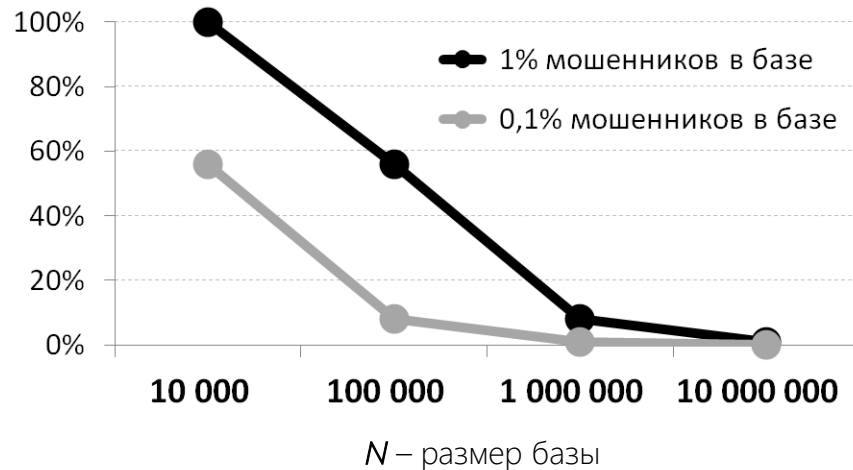
$$P = 1 - \frac{365!}{365^n (365 - n)!}$$

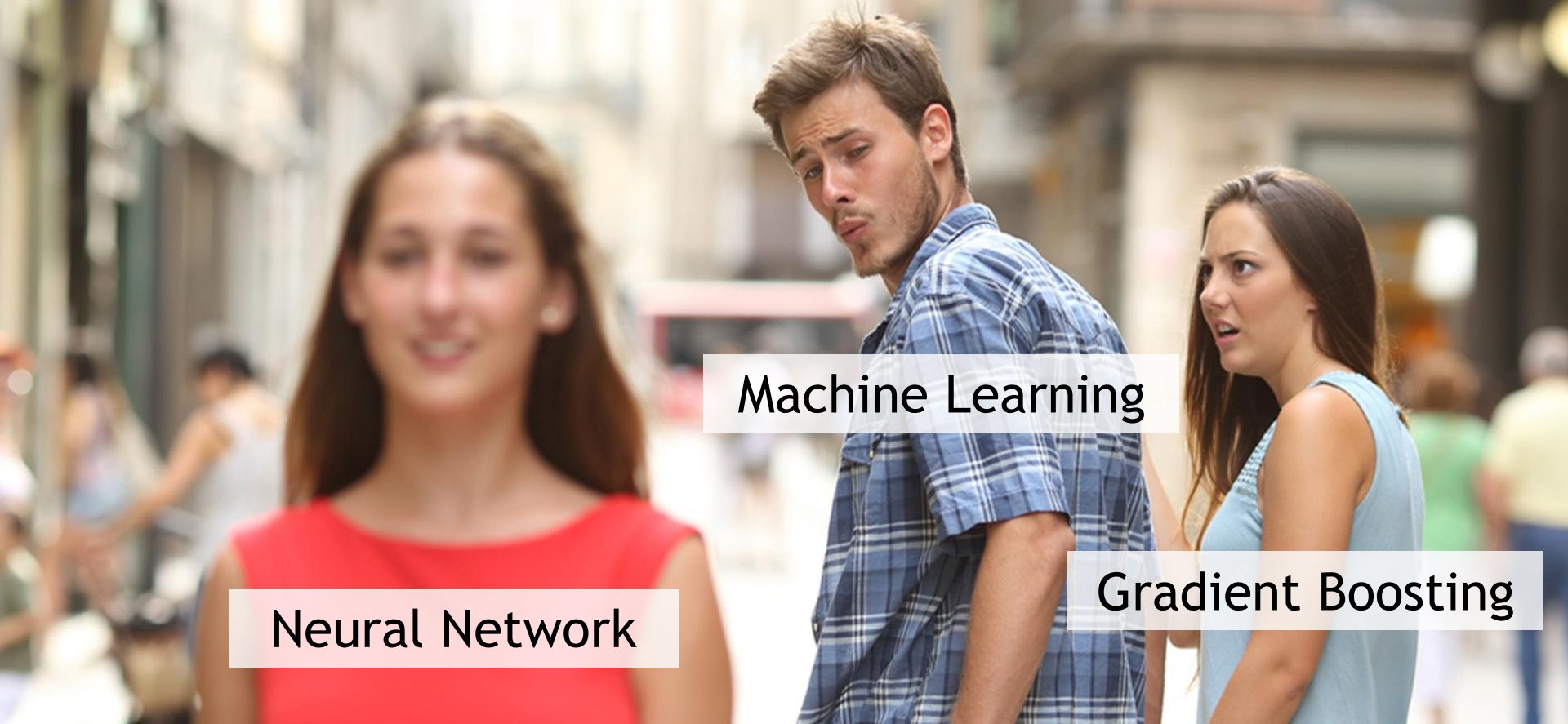


Вероятность случайного выявления мошенника:

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

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





Machine Learning

Neural Network

Gradient Boosting

О машинном обучении...



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

Герман Греф

2002



Earth Simulator – один из самых быстрых вычислительных комплексов (до 2004 года самый мощный в мире).

Стоимость: **\$350 000 000**

Площадь: четыре теннисных корта

Производительность: **36** Тфлопс

2017



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

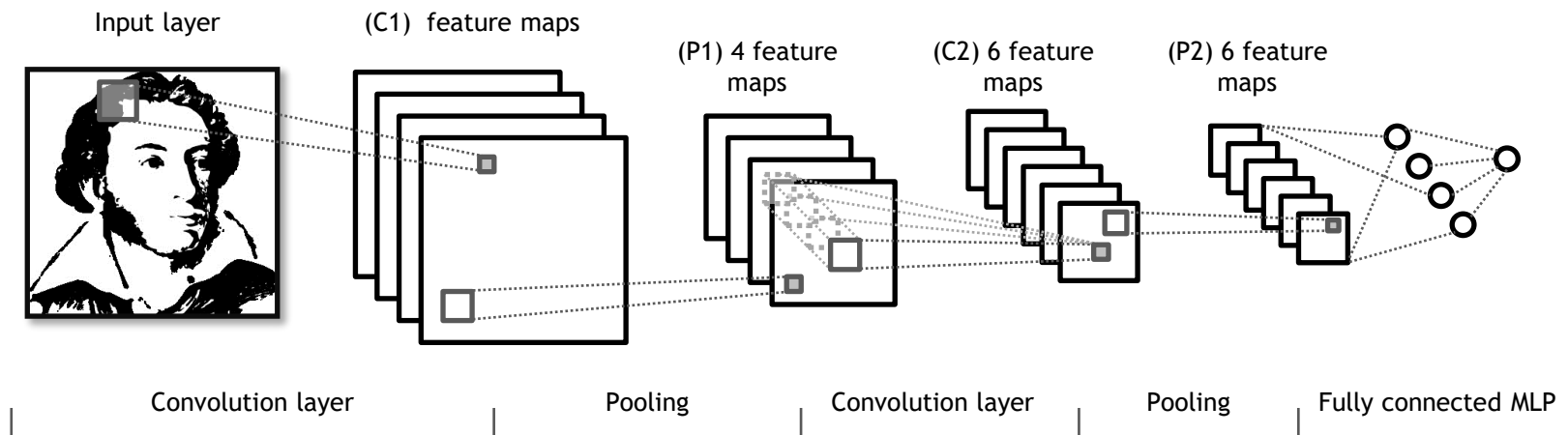
Стоимость: **\$2 999**

Площадь: помещается в сумочку

Производительность: до **110** Тфлопс

1. Сверточная нейронная сеть

Convolutional neural network (CNN)



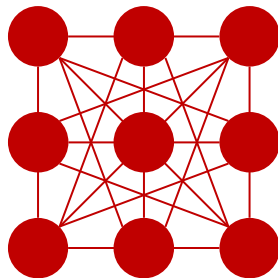
CNN для сложных правил

Предикторы



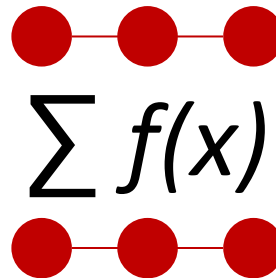
- 1 заемщик + разн. дом. тел.
- 1 заемщик + разные адреса
- 2 заемщика + один дом. тел.

Правила



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

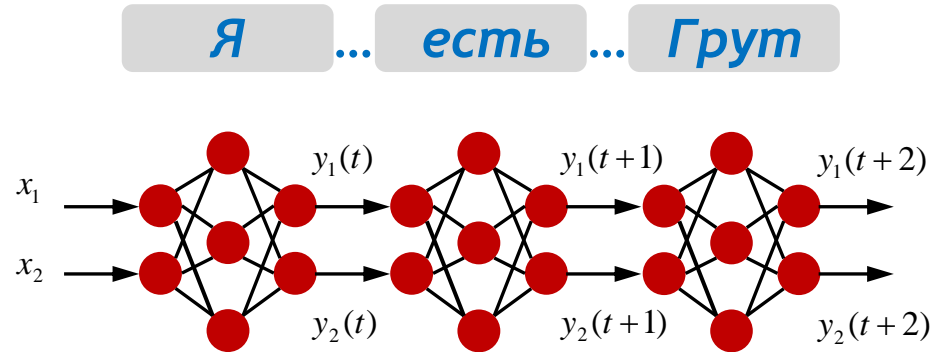
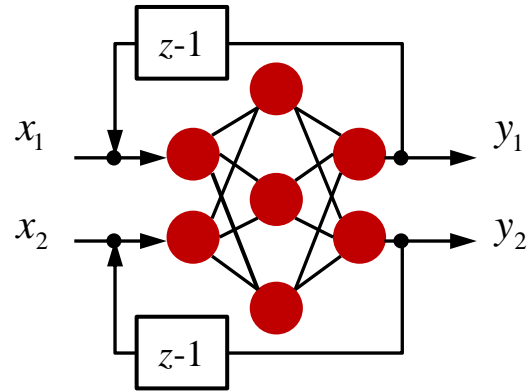
Триггеры



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

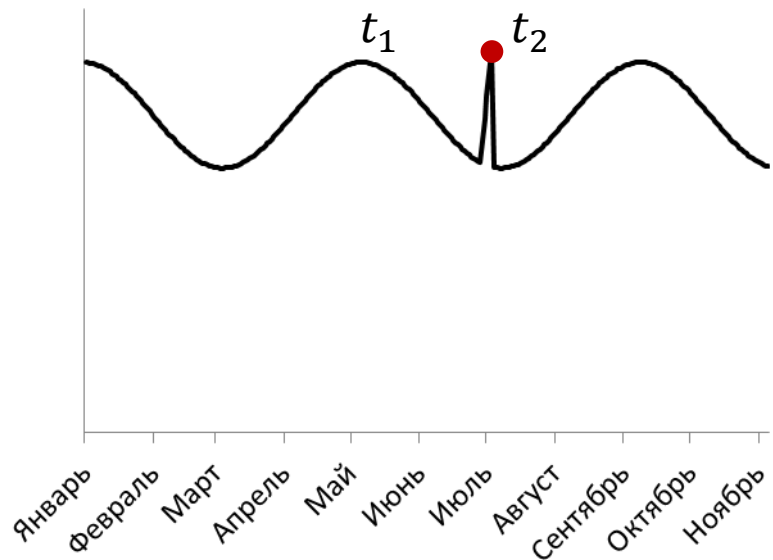
2. Рекуррентная нейронная сеть

Recurrent neural network (RNN)

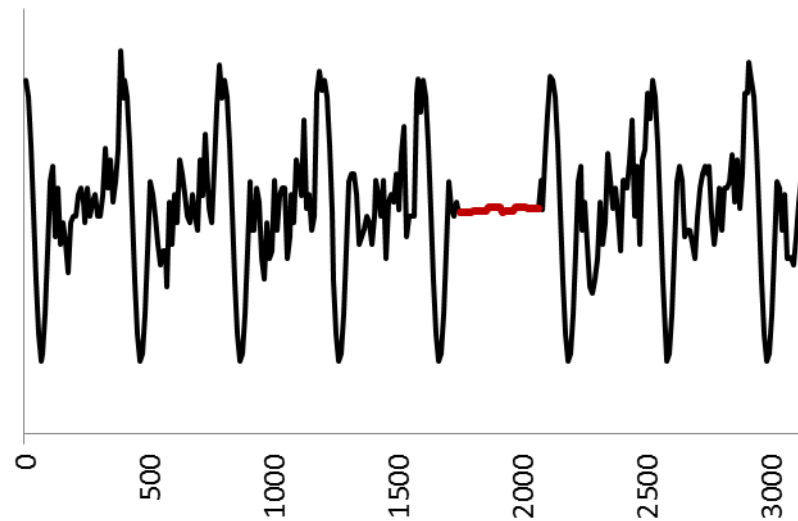


RNN для временных рядов

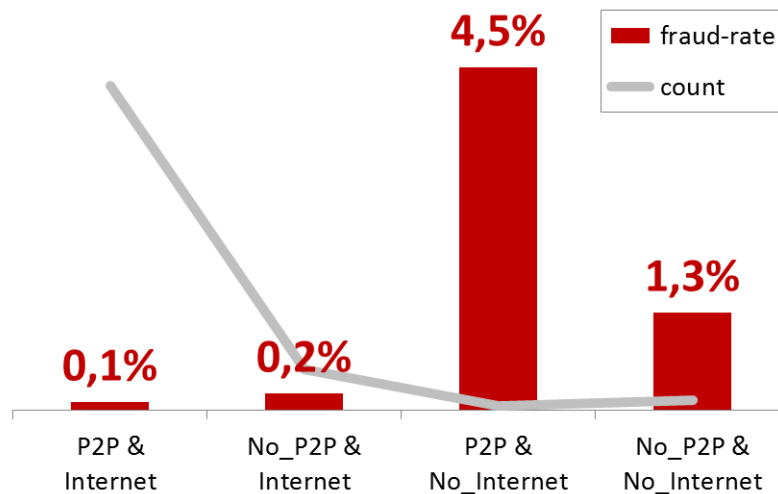
Контекстные аномалии



Групповые аномалии



RNN для транзакционных правил



Социальная инженерия

Сейчас

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

Как эков принуждают заниматься
телефонным мошенничеством
<https://meduza.io/feature/2017/06/07/polovinu-otdavali-administratsii-polovinu-polozhentsu>

Скоро... или сейчас?



Денис Довгопольный

16 июля · 🌐

...

Сейчас в одном из закрытых форумов по AI обсуждается две темы:

1. Сделали бота, который раскручивает девочек 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 диалогов, 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.

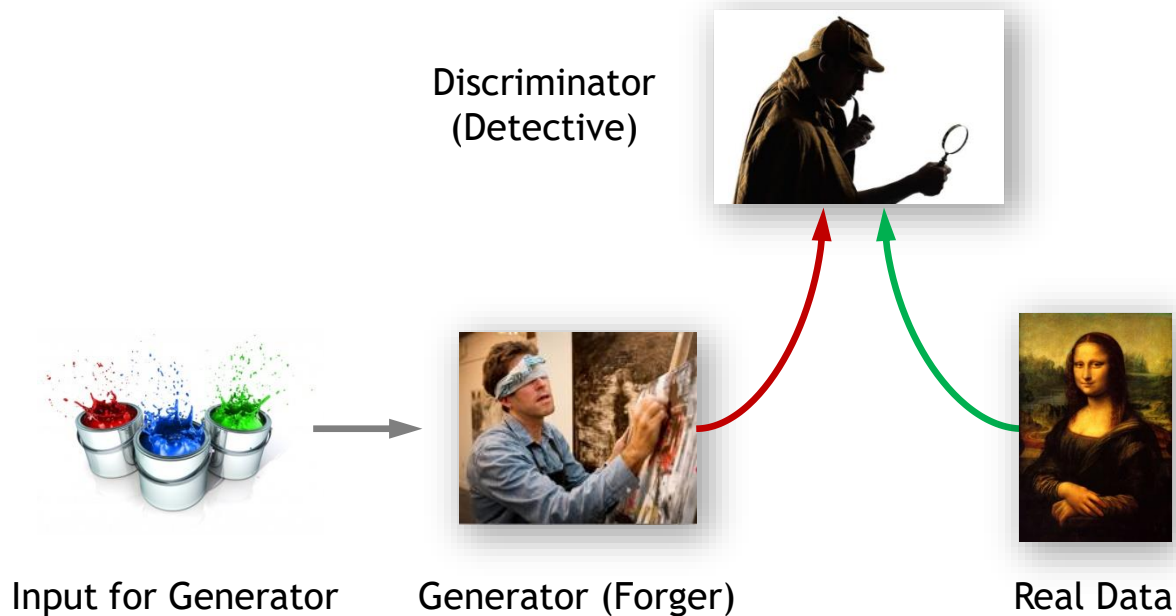
Обсуждают два аспекта:

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

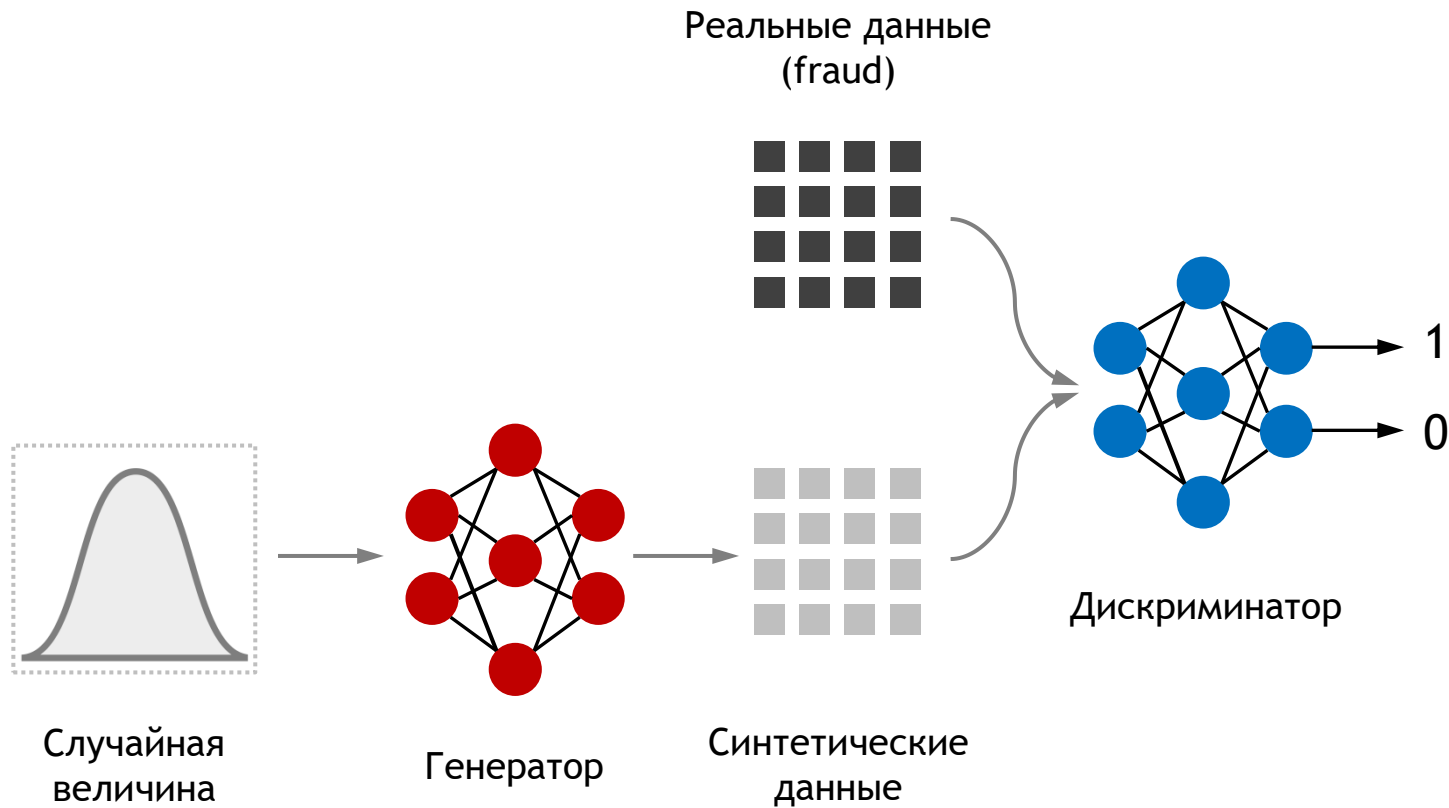
Как страшно жить....

3. Генеративно-сопоставительная сеть

Generative adversarial network (GAN)

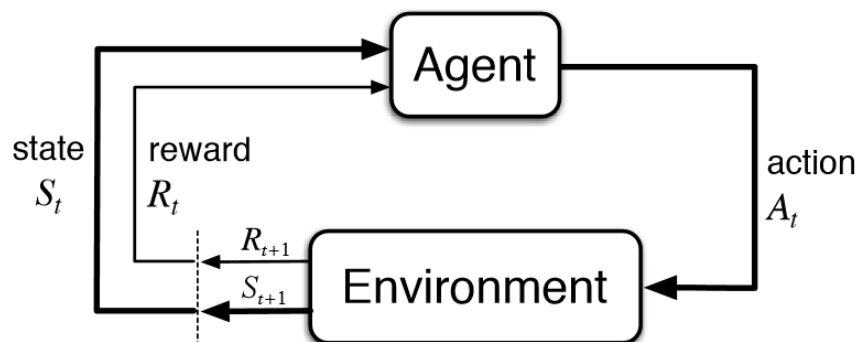


GAN для сэмплинга



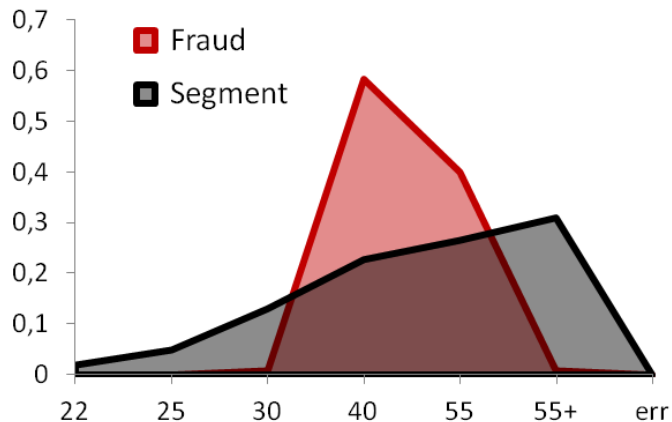
4. Обучение с подкреплением

Reinforcement learning (RL)



RL для выявления аномалий

Б-тесты (аномалии)



Adaptive Fraud Detection Using Benford's Law

Fletcher Lu¹, J. Efrim Boritz², and Dominic Covvey²

¹ Canadian Institute of Chartered Accountants,
66 Grace Street, Scarborough, Ontario, M1J 3K9
f21u@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

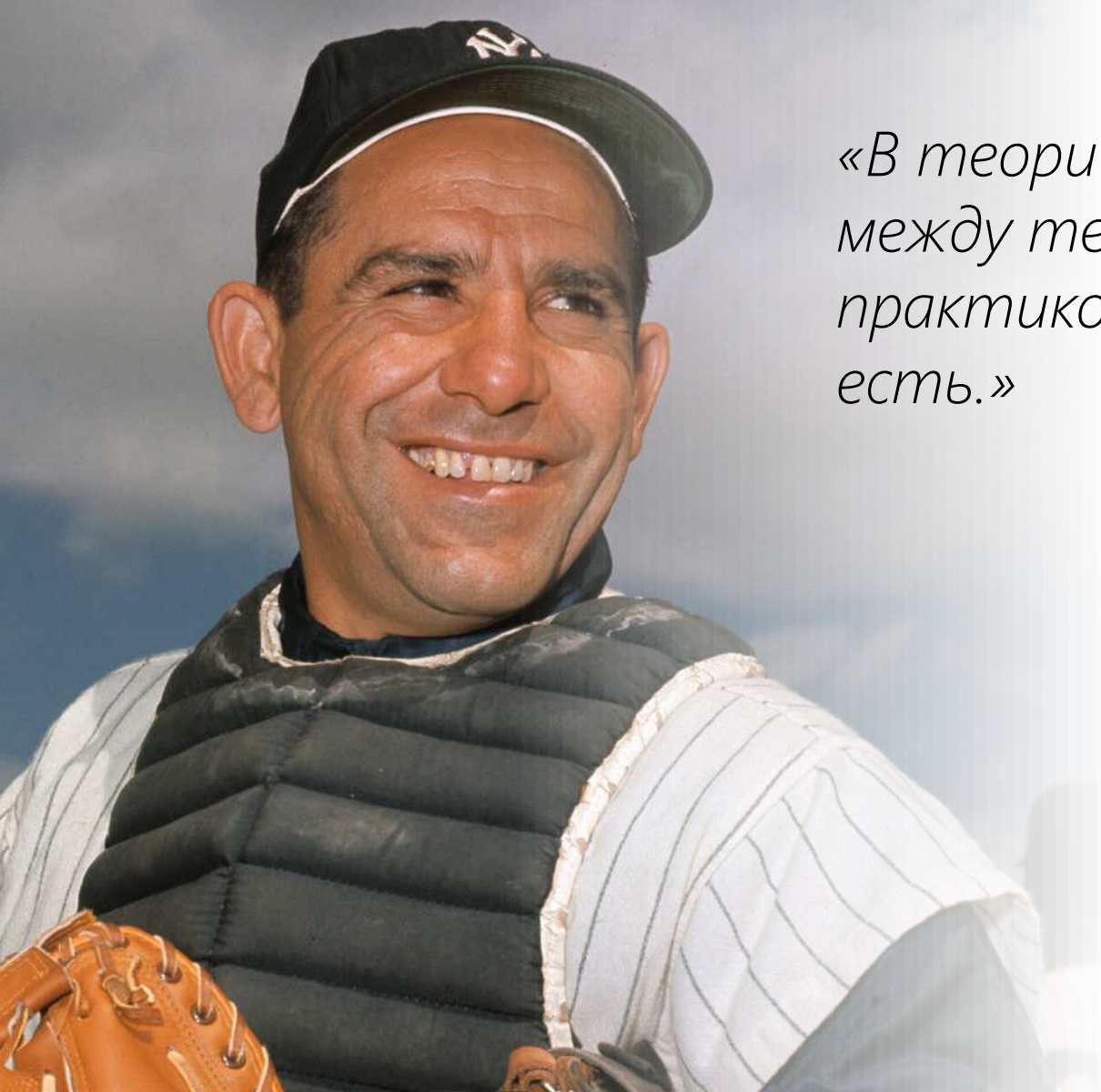
Рекомендации:

Для понимания сути задачи необходима
экспертиза антифрод-специалистов

Для антифрод-задач лучше использовать
модели, восстанавливающие нелинейные
зависимости: random forest, gradient
boosting, neural network

Качество fraud-моделей лучше оценивать
с помощью метрик recall или F-measure

Меньше переменных - проще внедрение



*«В теории нет разницы
между теорией и
практикой. А на практике
есть.»*

Йоги Берра

Спасибо за внимание!

Афанасьев Сергей

Исполнительный директор

Начальник управления расследования мошенничества

КБ «Ренессанс Кредит»

svafansev@gmail.com

safanasev@rencredit.ru