

«Инновационные направления исследований лаборатории «МФТИ-Сбербанк» в области информационной безопасности»

Директор ФПМИ*, зав. лаб., Доктор физико-математических наук, профессор Андрей Михайлович РАЙГОРОДСКИЙ
mraigor@yandex.ru

*Федеральное государственное автономное образовательное учреждение высшего образования «Московский физико-технический институт (государственный университет)» Физтех-школа прикладной математики и информатики (ФПМИ), Лаборатория прикладных исследований "МФТИ-Сбербанк"

Суздаль 2018

ФПМИ – это интегрированная структура 2-х факультетов МФТИ по направлениям «образование» и «наука»



* Представлены лишь некоторые кафедры. Более подробную информацию можно получить на сайтах факультетов

ФПМИ призвана собрать в стенах МФТИ все самые современные компетенции в области математики, информатики и их приложений

Ключевые направления развития ФПМИ

Фундаментальная математика и информатика

- Вероятностные, алгебраические и топологические методы в комбинаторике
- Графы, гиперграфы случайность
- Алгоритмы и сложность вычислений
- Дискретная и вычислительная геометрия
- Дискретные функции и оптимизация
- Теория чисел и криптография
- Теория вероятностей, математическая статистика, случайные процессы
- Алгебра, логика, топология

Аналитика больших данных

- Прикладная статистика
- Машинное обучение
- Статистическая теория обучения
- Глубокие нейронные сети
- Моделирование сложных сетей в интернете, экономике, биологии
- Параллельные и распределенные вычисления
- СУБД (системы управления базами данных)
- Суррогатное моделирование

Математическое моделирование и суперкомпьютерные технологии

- Качественная теория дифференциальных уравнений и уравнений в частных производных (теория динамических систем)
- Численное моделирование (вычислительная математика)
- Разработка суперкомпьютерных технологий и параллельных алгоритмов
- Обратные задачи
- Основы разностных схем
- Групповой анализ
- Вариационное исчисление

Теория управления, оптимизация и управление в сложных технических и социально-экономических системах

- Математическая экономика
- Финансовая математика
- Оптимизация и выпуклый анализ
- Оптимальное управление
- Сетевая оптимизация (алгоритмы на графах)
- Исследование операций (теория систем массового обслуживания, динамическое программирование)
- Элементы топологии и теории неподвижных точек
- Численные методы оптимизации
- Многомерный анализ данных
- Задачи классификации и кластеризации
- Исследование нелинейных нестационарных временных рядов

Лаборатория прикладных исследований МФТИ-Сбербанк

Год создания: 2017

Область научных интересов



- Разработка систем кибербезопасности
- Моделирование поведения пользователя
- Противодействие мошенническим действиям

Лаборатория занимается повышением уровня защищенности и противодействия киберугрозам, разработкой новых методов предсказания финансовой активности клиентов банка, а также предсказанием совершения мошеннических действий на больших гетерогенных данных



Руководитель: Райгородский Андрей Михайлович
Доктор физико-математических наук, профессор



Адрес: 141700, Московская обл., г. Долгопрудный, Институтский пер., 9
Сайт лаборатории: <https://mipt.ru/science/labs/mipt-sberbank-applied-research/>

Партнеры



СБЕРБАНК

Проекты



- Технология блокчейн
- Биометрическая идентификация
- Создание технологии выявления и семантического анализа поведенческих паттернов в транзакциях по картам банка
- Исследование возможности поиска по внутренним и внешним источникам данных потенциально скомпрометированных учетных записей клиентов и сотрудников для использования этой информации в процедурах риск-ориентированной аутентификации
- Исследование возможности поиска инсайдера среди сотрудников, имеющих легальный доступ в Big Data
- Разработка математической модели структуры графа «кредитной фабрики»

Ключевые сотрудники лаборатории

Тематика исследований: **машинный интеллект и анализ больших данных.**

Зам. заведующего лаборатории,
д.ф.-м.н., профессор РАН
Воронцов Константин
Вячеславович



Тематика исследований: **средства технической защиты информации, новая биометрия.**

Ведущий научный сотрудник,
д.т.н., профессор, Конявский
Валерий Аркадьевич



Тематика исследований: **Теоретические основы защиты информации и методы искусственного интеллекта в задачах кибербезопасности.**

Ведущий научный сотрудник, д.ф.-
м.н., член-корреспондент
Академии криптографии РФ,
Грушо Александр Александрович



Ведущий научный сотрудник,
д.ф.-м.н., Забежайло Михаил
Иванович



Основные направления работы лаборатории в области кибербезопасности

За время работы лаборатории разработаны новые математические модели:

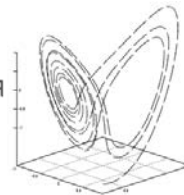
- Графовая модель выявления мошеннической активности при подачи заявки на кредитование.
- Модели выявления подозрительных событий по следам активности пользователей корпоративной системы в данных журналов безопасности Active Directory.
- Модель, определяющая множество потенциальных нарушителей среди пользователей Big Data с помощью статистических методов.
- Модель выявления автоматически сгенерированных доменных имен.

В настоящий момент в работе лаборатории выделено 2 крупных направления (проекта), работа над которыми поддержана центром компетенции в области искусственного интеллекта НТИ.

Проекты центра компетенции ИИ:

Национальная
технологическая
инициатива

Пространство возможного



- Распределенная платформа сбора и интеллектуального анализа гетерогенных данных о клиентской и внутрикорпоративной активности
 - Мошенничество в банковской рознице
 - Кибербезопасность больших корпоративных сетей
 - Эффективность и надежность работы больших кластеров
- Новая биометрия
 - Аутентификация на недоверенных устройствах
 - Решение проблемы виталентности

Технологии

- Автоматическое формирование модели нормального режима работы распределенной информационной системы на основе интенсивного потока данных наблюдений при ограниченной помощи экспертов в интерпретации и разметке данных
- Децентрализованное активное отслеживание состояния безопасности информационной системы с использованием механизмов внимания и проверки гипотез для фильтрации на ранних стадиях нерелевантной информации и уменьшения объема данных, обрабатываемых на более поздних стадиях
- Моделирование потребления вычислительных ресурсов в распределенной системе с уточнением параметров модели в процессе штатной работы
- Обнаружение инсайдеров в системах обработки больших данных
- Идентификация пользователей путем анализа и интеллектуальной обработки рефлекторных реакций человека при случайных динамических стимулах. (Анализ динамических характеристик зрачка, пульсовой волны и других модальностей)

Технологии и основные технологические барьеры

Технологии	Барьеры
Автоматическое формирование модели нормального режима работы распределенной информационной системы на основе интенсивного потока данных наблюдений при ограниченной помощи экспертов в интерпретации и разметке данных	Высокое количество ложноположительных срабатываний существующих систем обнаружения вредоносной активности (проблема разметки)
Децентрализованное активное отслеживание состояния безопасности информационной системы с использованием механизмов внимания и проверки гипотез для фильтрации на ранних стадиях нерелевантной информации и уменьшения объема данных, обрабатываемых на более поздних стадиях	Нехватка вычислительной мощности централизованных решений обработки телеметрических данных для применения современных интеллектуальных методов
Моделирование потребления вычислительных ресурсов в распределенной системе с уточнением параметров модели в процессе штатной работы	Низкий уровень предсказательной силы существующих высокоуровневых моделей больших облачных систем приводит к необходимости разработки технологии высокодетального моделирования на основе архитектурных описаний
Обнаружение инсайдеров в системах обработки больших данных	Низкий уровень защищенности систем аналитики больших данных от вредоносной активности сотрудников
Идентификация пользователей путем анализа и интеллектуальной обработки рефлекторных реакций человека при случайных динамических стимулах. (Анализ динамических характеристик зрачка, пульсовой волны и других модальностей)	Используемые сегодня технологии биометрической идентификации, основанные на использовании статических биометрических характеристик, требуют использования доверенных технических средств, что возможно в криминалистике, но невозможно в обществе. Преодоление этого барьера позволит перевести биометрическую идентификацию на новый технологический уровень

Направление 1:

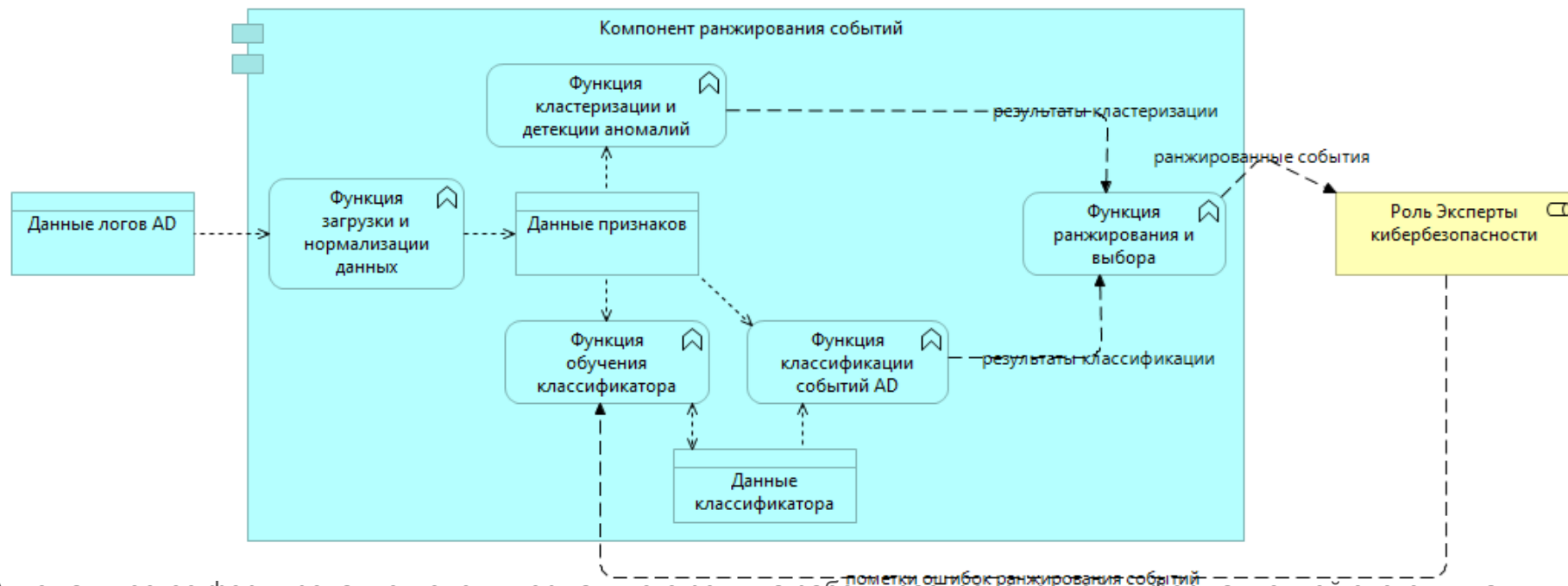
Распределенная платформа
сбора и интеллектуального анализа
гетерогенных данных о клиентской и
внутрикорпоративной активности

Особенности платформы

- Технологии больших данных
 - Близкая к линейной масштабируемость при росте объема и скорости данных
 - Интеграция разнородной информации в data lake
 - Интеграция разнородных моделей, актуализация их состояния по телеметрии
 - Архитектурные модели технических систем
 - Социальные модели и модели деятельности
- Edge computing
 - Децентрализованная обработка данных и принятие решений на источниках информации
 - Возможность отслеживать большой объем информации
- Графовые и гиперграфовые модели с распределенной обработкой
 - Аннотирование потока событий, телеметрии, журналов
 - Интеграция с системами представления знаний (онтологии и вывод, нейросети для выучивания онтологий)
- Машинное обучение
 - В том числе проблемы обучения в условиях противодействия (Adversarial machine learning)
- Мультиагентные и Self* системы
 - Интеллектуальные искусственные Ис-следователи, реагирующие на признаки и проводящие более глубокий анализ
 - Само-мониторинг, само-управление (Model-Based Predictive Control)

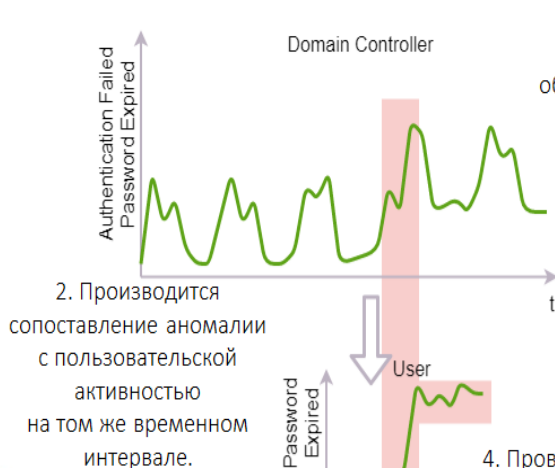
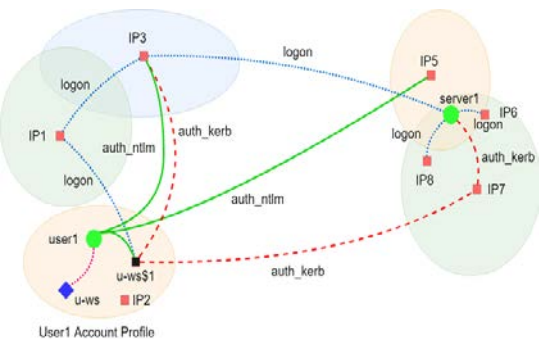
Детекция аномалий + обратная связь от эксперта = решение проблемы разметки

Архитектура системы с обратной связью:



Автоматическое формирование модели нормального режима работы распределенной информационной системы на основе интенсивного потока данных наблюдений при ограниченной помощи экспертов в интерпретации и разметке данных на примере записей журнала службы каталогов

Пример выявления аномалий: анализ следов пользовательской активности по данным AD



2. Производится сопоставление аномалии с пользовательской активностью на том же временном интервале.

3. Выполняется обнаружение пользователей с аномальной активностью.

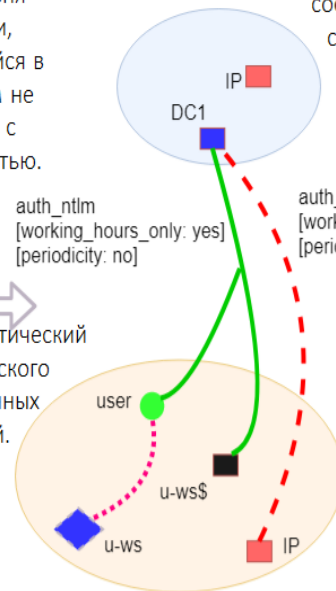
1. При анализе временного ряда обнаруживается резкий скачок уровня активности, сохраняющийся в дальнейшем не связанный с периодичностью.

4. Проводится автоматический анализ поведенческого профиля выявленных пользователей.

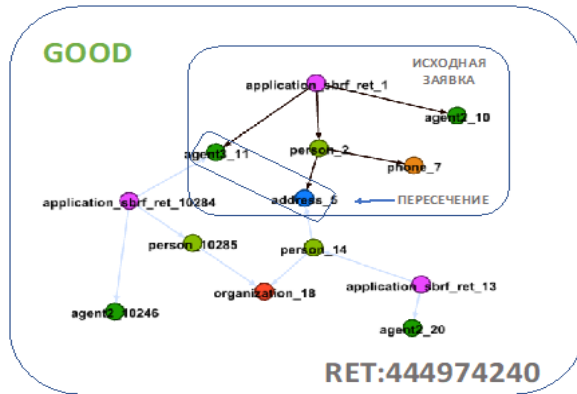
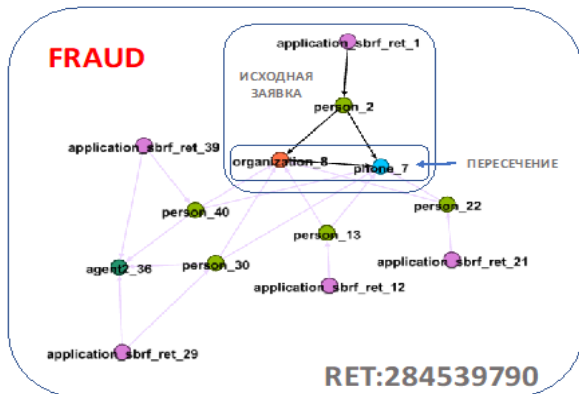
Поведенческий профиль обнаруженных пользователей соответствует активности рядовых сотрудников, не обладающих административными привилегиями.

5. Оценивается степень влияния ошибки на безопасность в модели угроз.

6. Генерируется сигнал об аномальной активности.



Графовые модели (некоторые результаты):



Модель детекции кредитного мошенничества на основе графа связей заявки:

- Более 110 факторов;
- Стабильный интегральный показатель AUC ROC 0.87



Модель выявления аномалий в транзакционных данных и данных систем детекции вторжений:

- До 0.9998 точности при высокой полноте в задачах детекции специфических типов атак.

Место результатов проекта в стеке технологий

Функциональные уровни	Результаты работы лаборатории	Описание	Примеры модулей
Приложения	Стартапы в прикладных областях	Стартапы в различных прикладных областях, связанные с анализом больших данных и использованием результатов в принятии решений	
ИИ сервисы	Сервисы в областях безопасности, поиска мошенничества и пр.	Сервисы выдачи рекомендаций и воздействия на аномалии для конкретных предметных областей, обеспечиваемые агентами	Oracle Cloud Control
Инфраструктура платформы и библиотеки агентов-анализаторов	Платформа сбора и интеллектуального анализа	Агенты автоматического построения моделей, определения нормы, обнаружения и исследования аномалий, выдачи рекомендаций и воздействия на аномалии для конкретных предметных областей	EDR (LimaCharlie)
Библиотеки моделей для конкретных предметных областей		Библиотеки моделей для анализа данных при поддержке больших кластеров, обеспечении кибербезопасности, управлении процессами производства продукции, управлении образовательным процессом	Apache Spot, Apache Metron, Google Timesketch
Библиотеки алгоритмов и представления данных	Out of scope	Библиотеки алгоритмов анализа, обучения, выявления аномалий	SparkML, GraphX, SPMF, ElasticSearch
Модели вычислений		Распределенные и поточные вычисления, Actor Model, Messaging	Akka, Kafka, Spark, Spark Streams
Кластеры, облака, микро-сервисы, виртуализация		Контейнеризация и оркестрация, планирование нагрузки, распределенные файловые системы, программно-определяемая инфраструктура	Docker, Kubernetes, Ceph, HDFS, Flannel, CoreOS, Tectonic

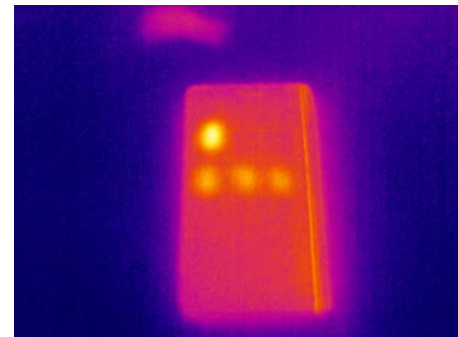
Направление 2

Новая биометрия

Новая биометрия: революционная технология биометрической аутентификации

Особенности

- Аутентификация на недоверенных устройствах
- Решение проблемы виталентности



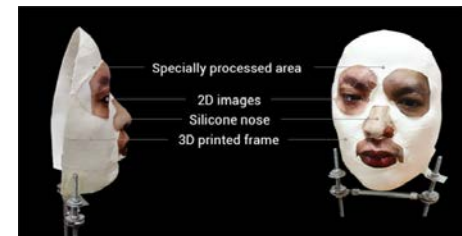
Проблема недоверенного устройства

Способы аутентификации

- Пароль
- Отпечаток пальца
- Рисунок радужной оболочки
- 3d - модель лица
- Образец голоса

На недоверенном устройстве

- можно подсмотреть
- легко подделать
- можно подделать
- можно подделать
- легко подделать



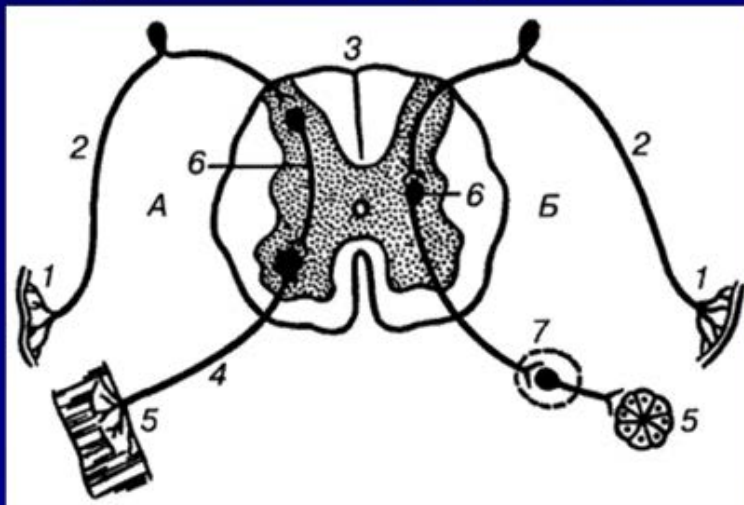
Новая идея: использовать рефлекторную дугу

Можно оценивать различные динамические реакции человека на случайные раздражители. В первую очередь:

- характер движения зрачков при слежении за объектом
- изменение динамики кровонасыщения (пульсовую волну)

Рефлекторная дуга

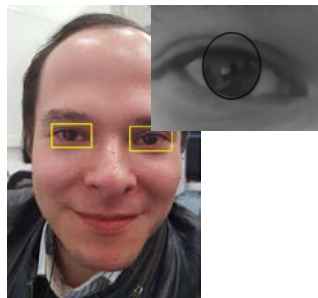
Рефлекторная дуга (нервная дуга) — путь, проходимый нервными импульсами при осуществлении рефлекса.



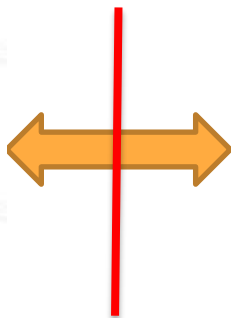
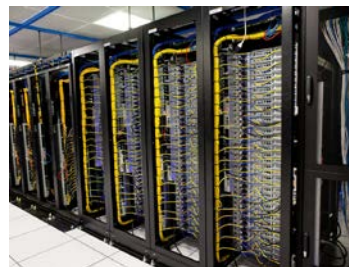
1. Рецептор
2. Чувствительный путь
3. ЦНС (спинной мозг)
4. Двигательный путь
5. Рабочий орган
6. Вставочный нейрон
7. Двигательный нейрон

Концептуальная архитектура системы новой биометрической аутентификации

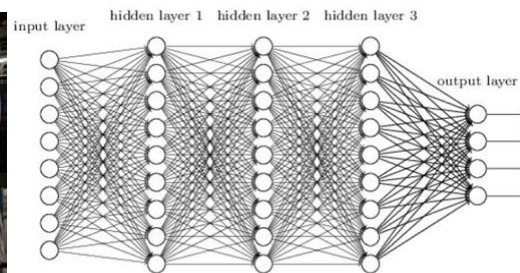
Недоверенное
клиентское
устройство



Доверенный центр
обработки данных



Deep neural network



1. Пользователь хочет
аутентифицироваться в
мобильном приложении

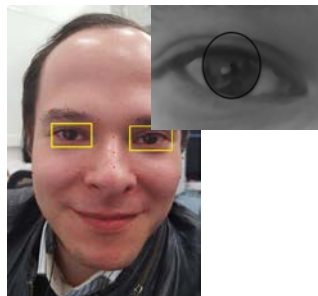
2. Для него генерируется
раздражитель и
зафиксированные реакции
пересылаются в центр
обработки данных

3. Система на основе
нейросети
подтверждает личность
пользователя

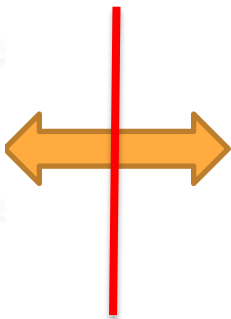
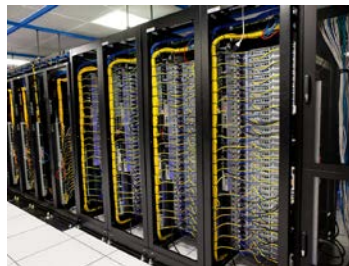
Сложно построить модель функционирования нервной системы.
На сегодняшний день таких моделей просто нет! Это дает возможность
использовать рефлекторную дугу для одновременного решения проблем
аутентификации на недоверенном устройстве и виталентности.

Ключевые особенности

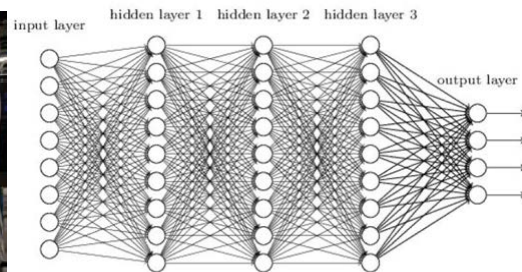
Недоверенное
клиентское
устройство



Центр обработки
данных



Deep neural network



- Случайные раздражители гарантируют невозможность простого копирования реакций

- Сложная обратная задача: по реакциям определить идентификатор человека можно (с помощью нейросети), а по идентификатору построить модель реакции человека - невозможно (невозможно обратить нейросеть)

Перспективы бизнес применения технологий (ближний горизонт на примере возможных продуктов)

- SIEM (Security information and event management) нового поколения
- Fog-computing система глубокого мониторинга событий безопасности
- Система мониторинга распределенной информационной системы на основе архитектурных моделей
- «Новая биометрия». Разработка и поставка новых биометрических механизмов на рынок интеллектуальных сервисов
- «Национальный оператор идентификации». Предоставление услуг по биометрической идентификации на основе динамических рефлексных реакций для бизнеса, информационных систем цифровой экономики и госуслуг

Некоторые перспективы с точки зрения современной науки и технологий:

- Графовые модели
 - Новые алгоритмы Personalized PageRank и модели случайных графов для обнаружения аномалий по аналогии с моделями обнаружения поискового спама
 - Быстрое вероятностное обнаружение подграфов в больших графах при потоковой обработке
- Новые алгоритмы машинного обучения для обнаружения следов вредоносной активности.
- Повышение производительности систем обработки потоков данных и больших данных
 - Многоуровневое кэширование HDD, NVMe SSD, RAM в распределенных файловых системах (Ceph, HDFS)
 - Обработка поточных данных в темпе процесса на кластере с GPU и СУБД на GPU
 - Построение моделей производительности вычислительного кластера на основе мониторинга производительности кластера, тестирования производительности и трассировки работы микросервисов

Спасибо за внимание!

Директор ФПМИ*, зав. лаб., Доктор физико-математических наук, профессор Андрей Михайлович РАЙГОРОДСКИЙ

mraigor@yandex.ru

Н.с. лаб. прикл. исслед. Сергей Алексеевич ТРЕНИН

s.trenin@gmail.com

*Федеральное государственное автономное образовательное учреждение высшего образования «Московский физико-технический институт (государственный университет)» Физтех-школа прикладной математики и информатики (ФПМИ), Лаборатория прикладных исследований "МФТИ-Сбербанк"

Суздаль 2018