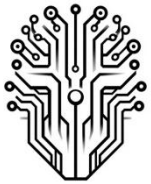
РусКрипто XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

БИОМЕТРИЧЕСКАЯ АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ НА ОСНОВЕ АНАЛИЗА ЭЛЕКТРИЧЕСКОЙ АКТИВНОСТИ МОЗГА С ПОМОЩЬЮ НЕЙРОСЕТЕВЫХ МОДЕЛЕЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Сулавко Алексей Евгеньевич
профессор кафедры «Комплексная защита информации», ОмГТУ
генеральный директор ООО «АИ ЗИОН»

Омская научная школа



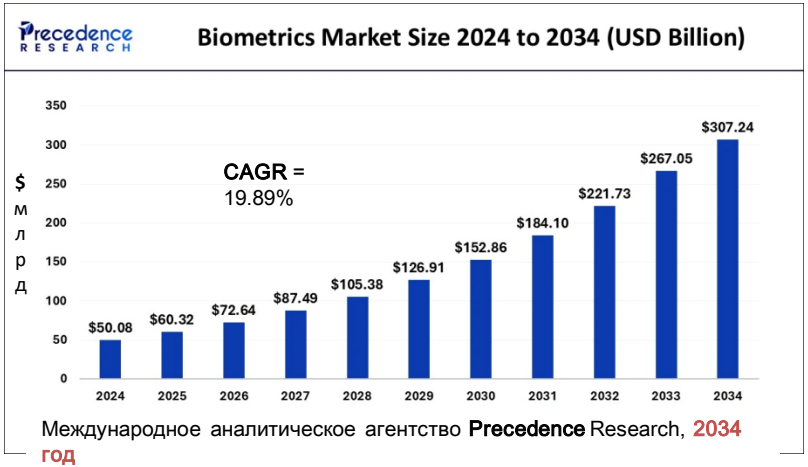
AI ZION

Нами ведется активная научная деятельность по следующим основным направлениям:

- Машинное обучение с использованием малых тренировочных выборок данных
- Ансамбли моделей машинного обучения
- Распознавание образов с учетом корреляционных свойств пространства признаков
- Высоконадежная биометрическая аутентификация и нейроинтерфейсы на базе электроэнцефалографии (ЭЭГ)
- Искусственные нейронные сети
- Биоинспирированные модели и алгоритмы машинного обучения (искусственные иммунные системы)
- Защищенный режим исполнения нейросетевых моделей и алгоритмов ИИ

Актуальность исследования

Объем мирового рынка биометрических систем



Международное аналитическое агентство **Precedence** Research, 2034 год

Прогноз рынка мобильной биометрии от **Transparency Market Research** до 2031 года:

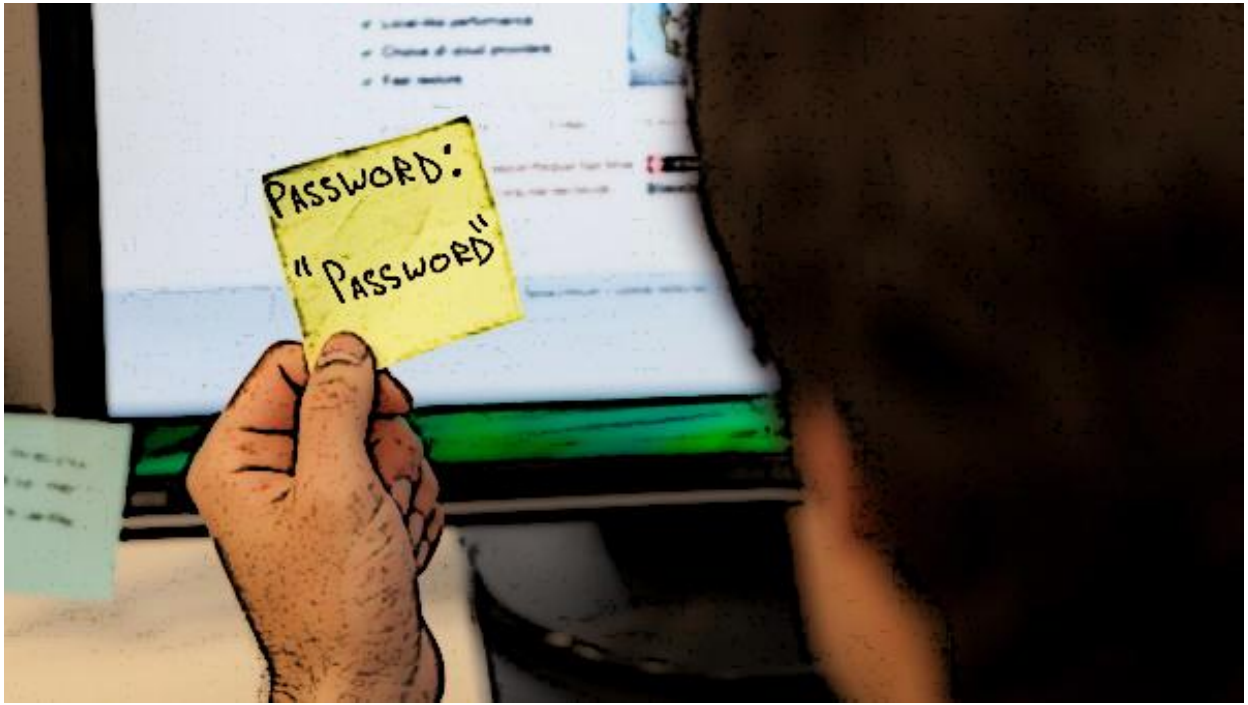
- в 2021 году объем отрасли оценивался в 44,2 млрд долларов
- до 2031 года среднегодовой темп роста составит 20,1%
- в 2031 году объем отрасли достигнет 267,7 млрд долларов
- сегмент лицевой биометрии достигнет $20,5 млрд.
- сегмент бесконтактной и многофакторной биометрической аутентификации – $59,5 млрд.
- крупные инвестиции направлены на сегменты **голосовой** и **лицевой** биометрии

Ключевые проблемы

- Подверженность компьютерным атакам, атакам предъявления (биометрия в целом)
- Подверженность лицевой и голосовой биометрии deep fake’ам
- Компрометация открытых биометрических образов в естественной среде (голос, лицо, отпечаток пальца, радужка и др.)
- Невысокая надежность лицевой и голосовой биометрии*

*показатели вероятностей «ложного отказа» **FRR** и «ложного допуска» **FAR** гораздо выше, чем для технологий, основанных на отпечатке пальца или радужке

«Человеческий фактор» – самая серьезная угроза информационной безопасности



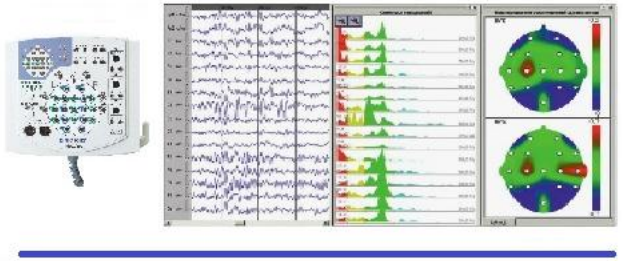
Технология аутентификации по ЭЭГ

Как это использовать на практике?

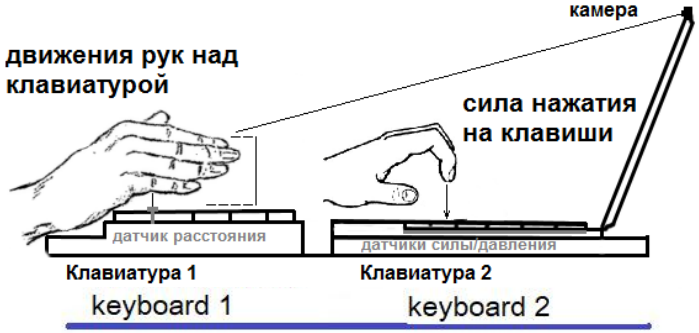
Технология аутентификации по ЭЭГ

Как подсознательные движения формируют сигнал ЭЭГ

Уровень 1 – намерение совершить осознанное движение (параметры ЭЭГ)



Уровень 2 – движения (траектории перемещения рук, сила нажатия на клавиши)

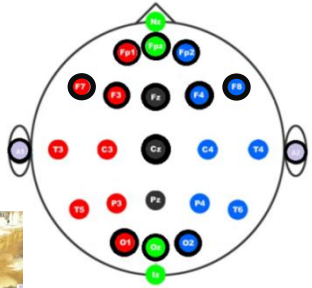


Уровень 3 – остаточная информация о взаимодействии с устройством (временные параметры нажатия клавиш)

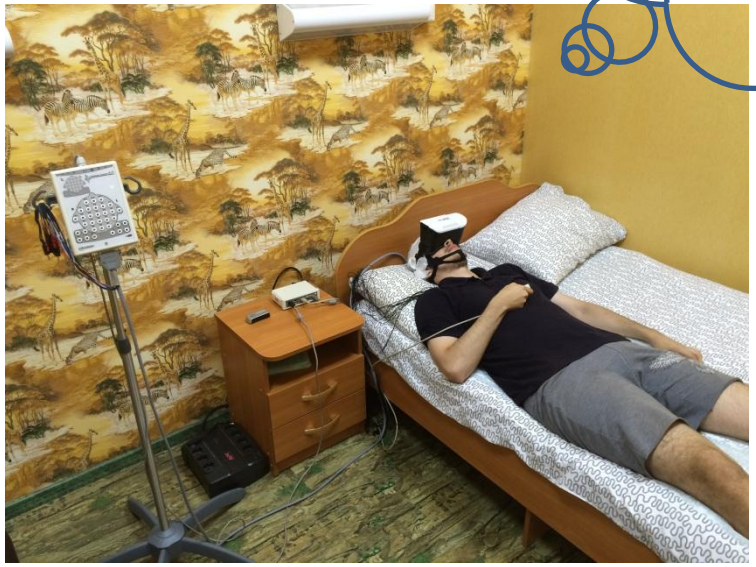
Формирование базы ЭЭГ образов с использованием визуальных стимулов

конференция РусКрипто

Схема подключения (по системе «20-10»)



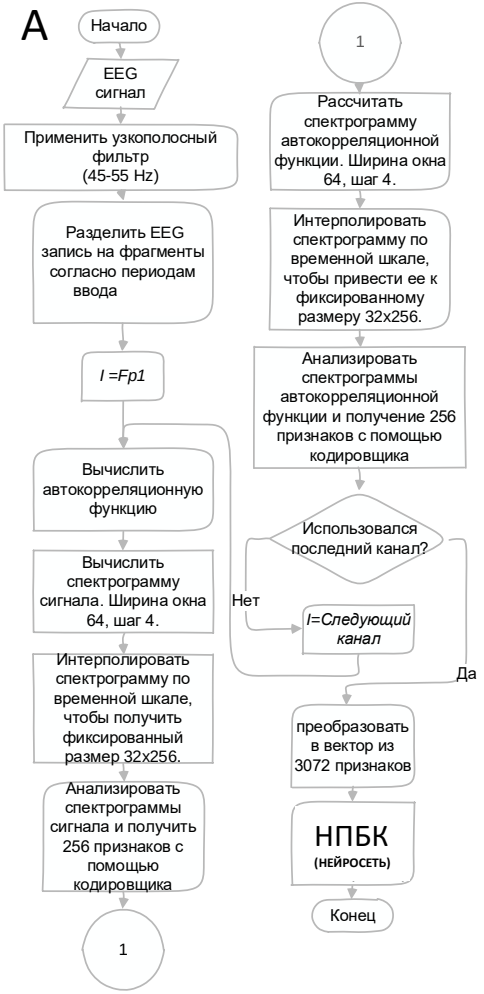
Визуальные стимулы («пятна» Роршаха)



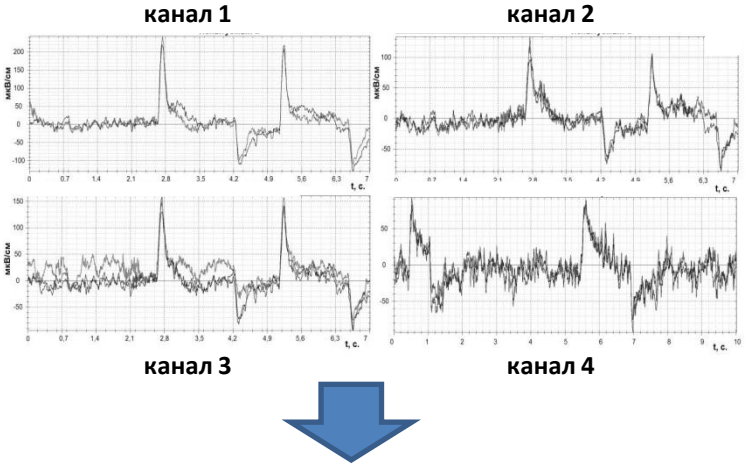
Обработка сигналов ЭЭГ

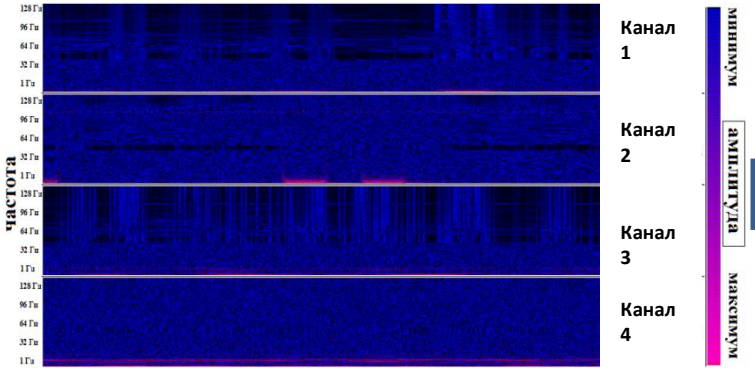
конференция РусКрипто

А

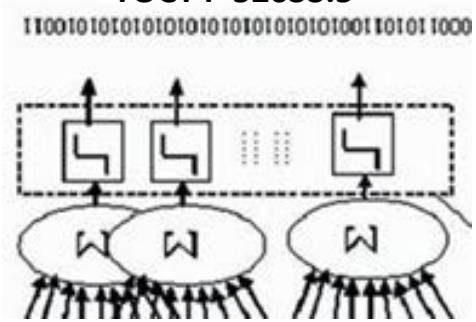


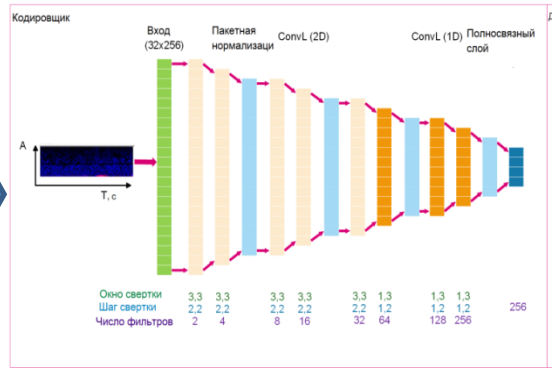
Б





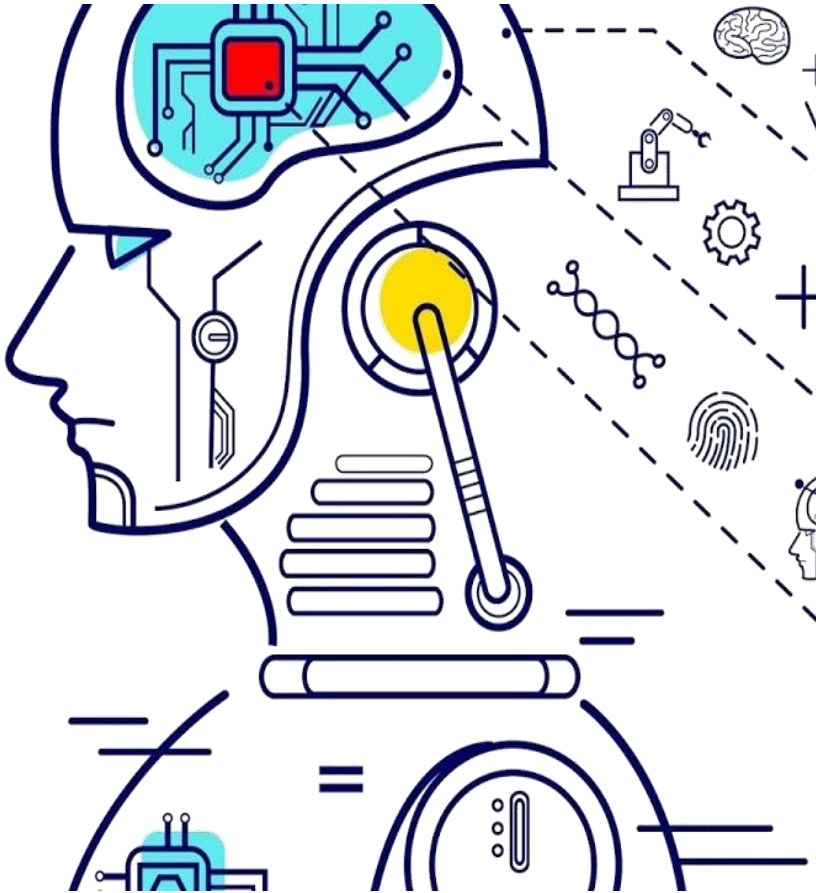
Нейросеть, обученная по ГОСТ Р 52633.5





Защищенное исполнение нейросетевых алгоритмов доверенного ИИ в задачах биометрической аутентификации

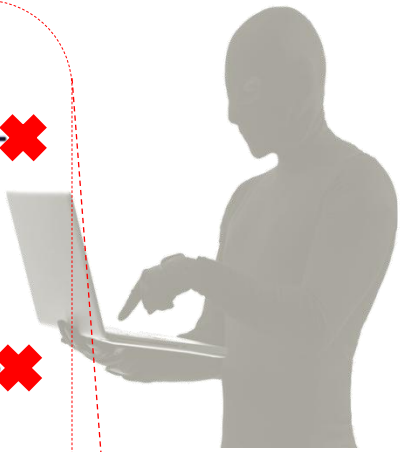
конференция РусКрипто



Анализ логики работы и операций, совершаемых ИИ

Несанкционированное управление, манипуляции с моделями ИИ, атаки предъявления, deep fakes

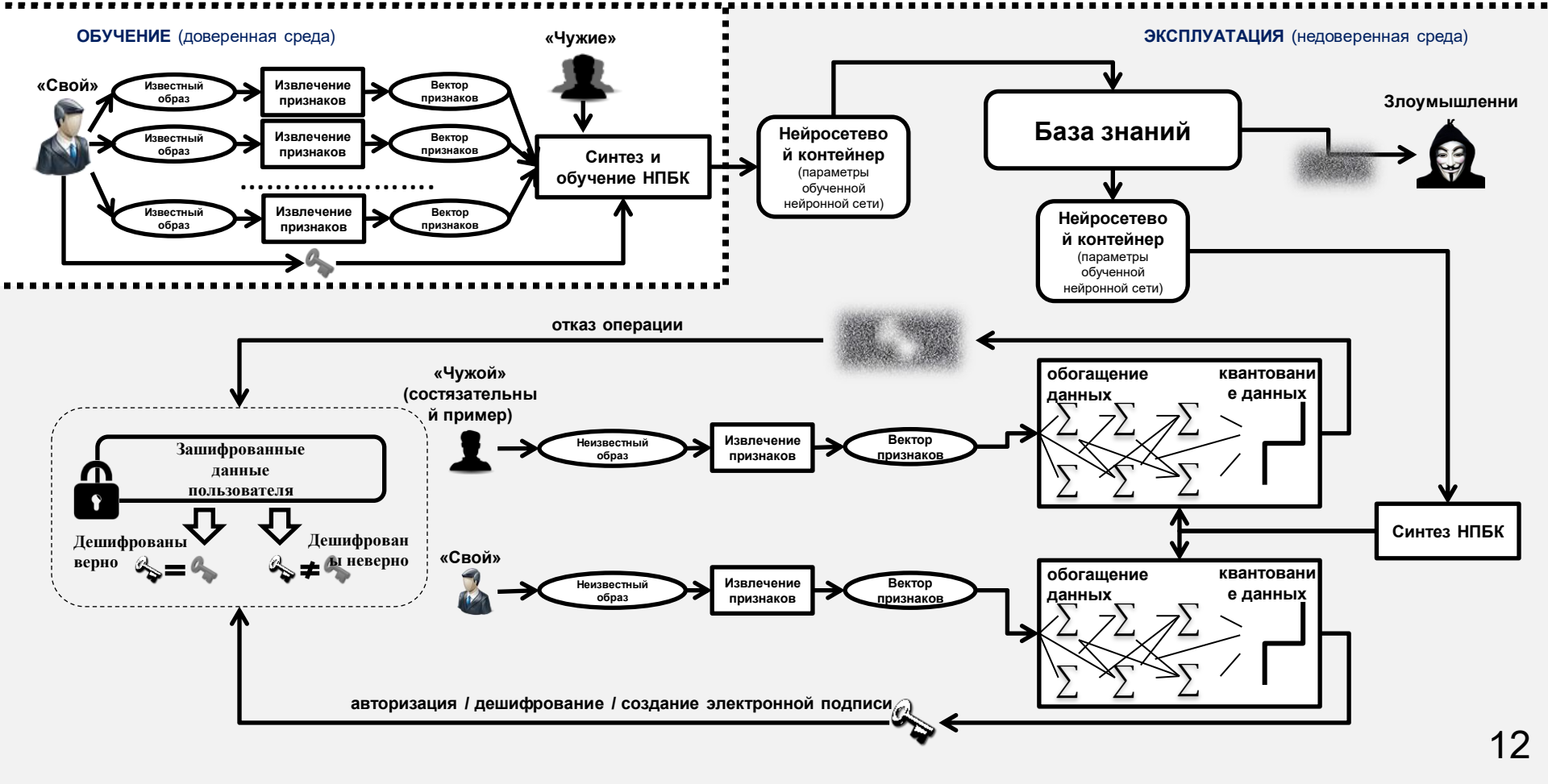
Извлечение и интерпретация знаний из памяти ИИ, подготовка состязательных примеров и муляжей



1. **ЭЭГ**
2. **НПБК**

Нейросетевые преобразователи биометрия-код (НПБК)

конференция РусКрипто



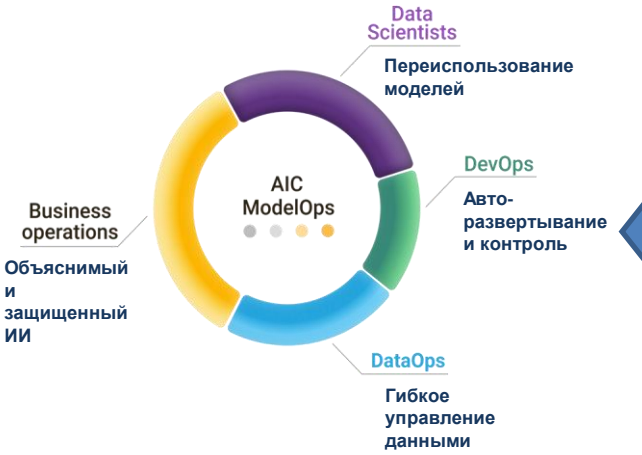
Результаты

Публикация	Набор данных	Точность, %
Thomas, K.P.; Vinod, A.P. EEG-Based Biometric Authentication Using Gamma Band Power During Rest State. Circuits Syst. Signal Process. 2017, 37, 277–289	109 испытуемых, PhysioNet	98.04
Akbarnia, Y.; Daliri, M.R. EEG-based identification system using deep neural networks with frequency features. Heliyon 2024, 10, e25999	109 испытуемых, PhysioNet	99.19
Nguyen, D.; Tran, D.; Sharma, D.; Ma, W. On the Study of Impacts of Brain Conditions on EEG-based Cryptographic Key Generation Systems. Procedia Comput. Sci. 2018, 126, 713–722	80 испытуемых, AEEG	97.42
Li, Y.; Zhao, Y.; Tan, T.; Liu, N.; Fang, Y. Personal Identification Based on Content-Independent EEG Signal Analysis. In Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2017; pp. 537–544	DEAP multimodal dataset	94
Damaševi˘cius, R.; Maskeli ¯ unas, R.; Kazanavi˘cius, E.;Wo´zniak, M. Combining Cryptography with EEG Biometrics. Comput. Intell. Neurosci. 2018, 2018, 1867548	42 испытуемых	97.6
Nguyen, D.; Tran, D.; Sharma, D.; Ma,W. Emotional Influences on Cryptographic Key Generation Systems using EEG signals. Procedia Comput. Sci. 2018, 126, 703–712	16 канальные ЭЭГ, DEAP	97.88
Zhao, H.; Wang, Y.; Liu, Z.; Pei, W.; Chen, H. Individual Identification Based on Code-Modulated Visual-Evoked Potentials. IEEE Trans. Inf. Forensics Secur. 2019, 14, 3206–3216	25 испытуемых	99.43
Предлагаемый метод	109 испытуемых, PhysioNet	99
	95 человек	99.2

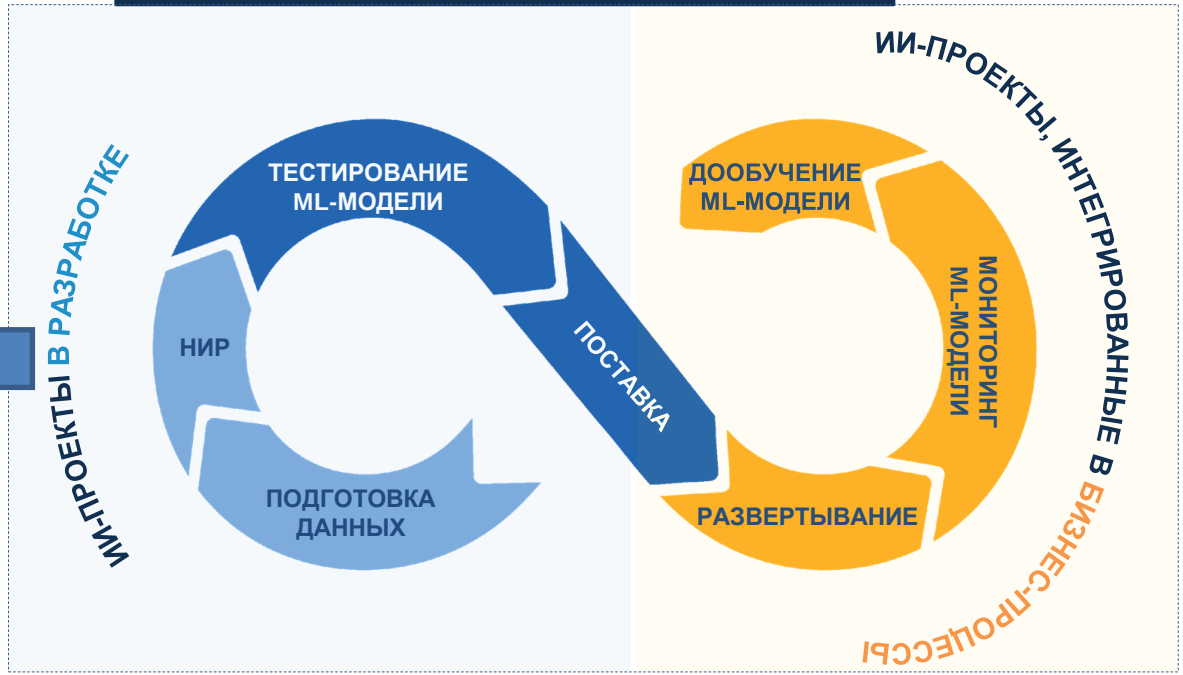
AIC Platform

корпоративная среда управления жизненным циклом искусственного интеллекта

конференция РусКрипто



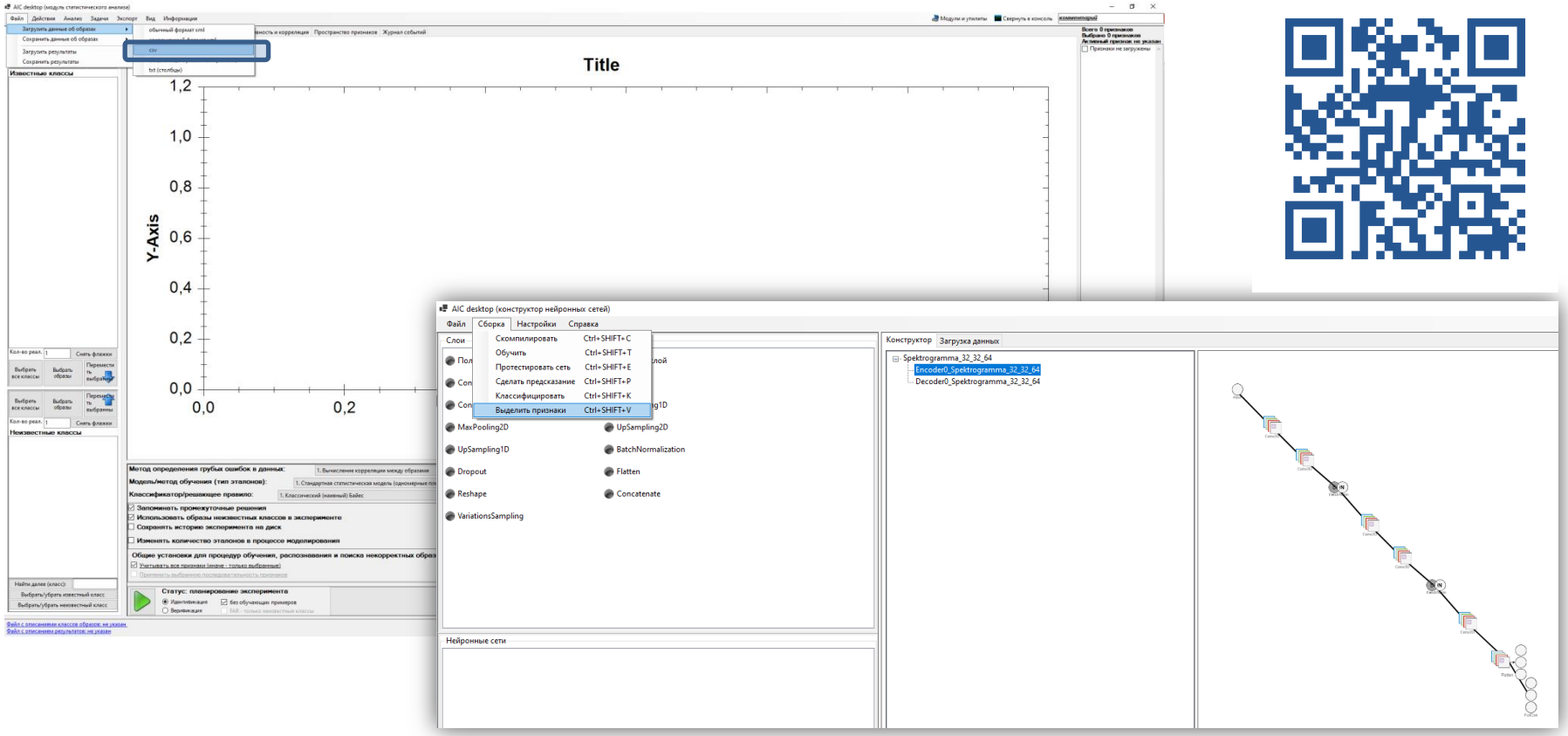
ЖИЗНЕННЫЙ ЦИКЛ ИИ-МОДЕЛЕЙ



- ✔ Сквозное управление жизненным циклом ИИ, аналитики и моделей принятия решений в единой консоли
- ✔ Мониторинг ИИ-модели позволяет выявить дрейф данных и концепций, попытки реализации состязательных атак и другие проблемы
- ✔ Объяснимость выделяет сильные и слабые стороны ИИ-модели, объясняет решения ИИ-модели, выявляет предвзятость
- ✔ Встроенный в платформу ИИ формирует рекомендации относительно того, какие параметры ИИ-модели нужно изменить для достижения лучшей производительности

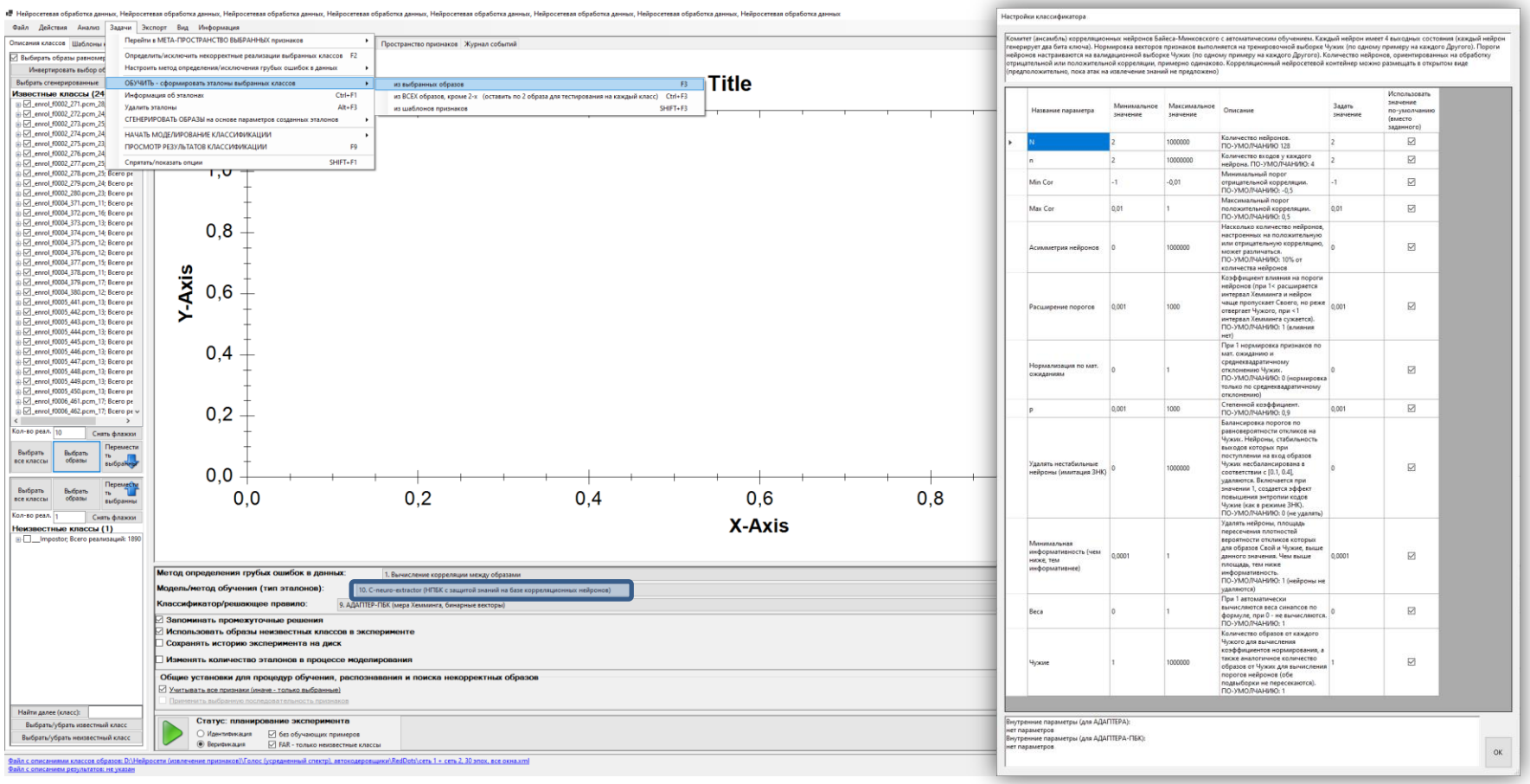
AIC desktop

конференция РусКрипто



AIC desktop

конференция РусКрипто



Подробнее о направлениях наших исследований вы можете узнать на сайте

О нас

Наши проекты

Алексей Сулавко
(ОмГТУ), д.т.н.

AIC Platform

AIC desktop

Контакты:
sul@aiconstructor.ru
+7 953 394-90-54