



AI DeepFake

Система выявления
фальсифицированного контента.

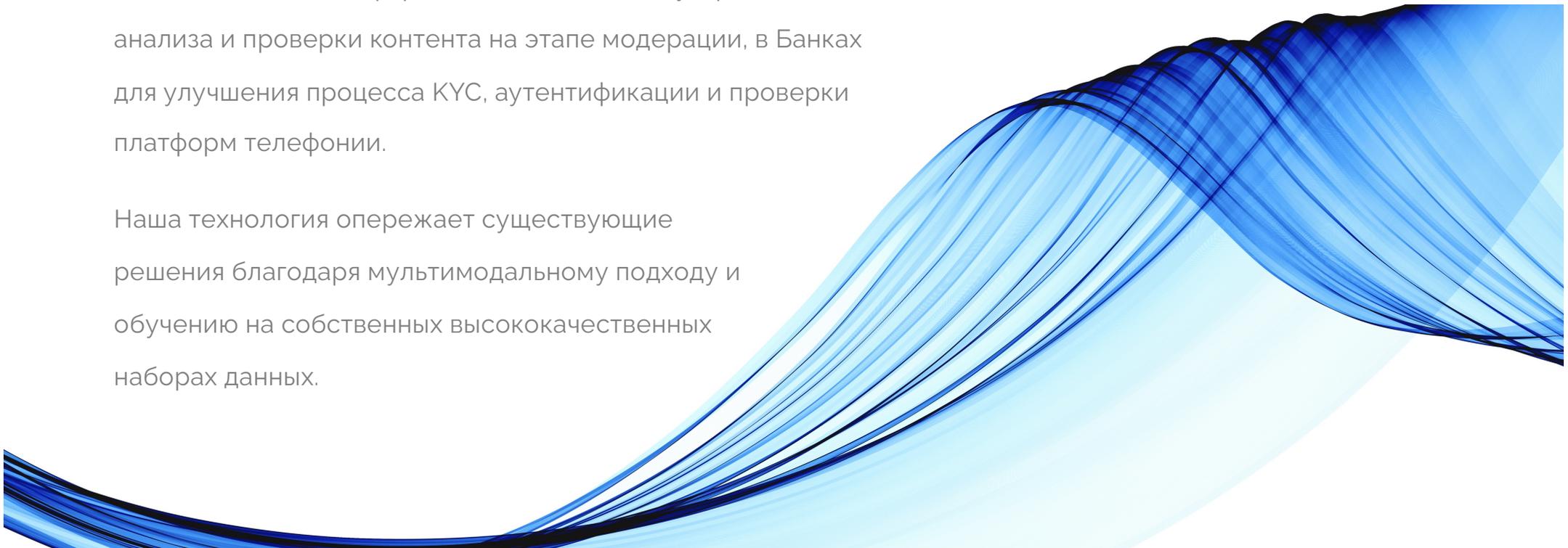
О Компании

Компания aIDeepFake

Разработчик отечественного программного обеспечения для противодействия технологии deepfake. Команда специалистов разрабатывает решение на базе нейронных сетей и алгоритмов глубокого обучения для выявления фальсифицированного контента.

Решение aIDeepFake может использоваться для борьбы с политической дезинформацией, в медиа индустрии для анализа и проверки контента на этапе модерации, в Банках для улучшения процесса KYC, аутентификации и проверки платформ телефонии.

Наша технология опережает существующие решения благодаря мультимодальному подходу и обучению на собственных высококачественных наборах данных.



Что такое "deepfake" и почему это проблема?

"Deepfake" - это искусственно созданные аудио или видео материалы, в которых лицо или голос человека подделываются с помощью технологий машинного обучения и ИИ.

Распространение дезинформации

Нарушение конфиденциальности

Манипуляция общественным мнением



Вызовы для биометрических систем

Атака типа Liveness – известна бизнесу и есть инструменты для ее выявления и предотвращения.

Атака на биометрию, когда злоумышленник пытается атаковать момент захвата изображения лица с помощью заранее подготовленных фейков.

Атака типа DeepFake – Может использоваться для атаки на интерактивный Liveness, как часть атаки с помощью виртуальной камеры, онлайн-атаки.

Атака на биометрическую систему, при которой происходит попытка подмены исходного видеопотока или изображения через соединения и наложения существующих изображений и видео на исходные в момент передачи или загрузки данных.

Типы атак: Face Reenactment – перенос выражения лица, Face Synthesis – генерация лиц, Face Swap – перенос изображения, Lip sync - синхронизация движения губ и звукового ряда.

Виртуальная камера - Может использоваться для атаки на интерактивный Liveness и на верификацию пользователя во время видео звонка.

Атака на сенсор, при которой исходный видеопоток подменяется на альтернативный (заранее подготовленный) / сгенерированный с помощью DeepFake.

Решение -aiDeepFake

Комплексный Анализ

Наша система использует сочетание методов компьютерного зрения, анализа звука и машинного обучения для всестороннего обнаружения deepfake.

Высокая Точность

Наше решение демонстрирует высокую точность распознавания.

Простота Использования

Интуитивно понятный интерфейс и автоматизированные процессы делают наше решение доступным для любого пользователя.



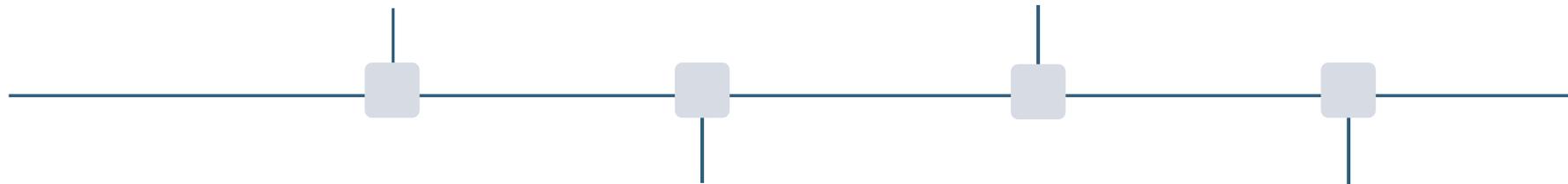
Технология

Обучение на больших данных

Модели глубокого обучения требуют огромных наборов размеченных данных для эффективного обнаружения различных типов подделок.

Непрерывное обновление

Технологии deepfake постоянно совершенствуются, поэтому модели детекции должны регулярно обновляться для поддержания актуальности.



Мультимодальный подход

Комбинирование методов компьютерного зрения, обработки аудио и анализа метаданных повышает точность обнаружения.

Масштабируемость

Технология может быть масштабирована на международные рынки

Достижения проекта



MOSCOW
AGENCY
OF INNOVATIONS



Участник академии инноваторов (3 поток)



Резидент ИТ-парка им. Башира Рамеева



Номинант премии в области финансов FinNext 2024



Участник питч-сессии стартапов, в сфере ИИ, международного форума Kazan Digital Week 2024



Участник акселерации ИТМО 2024

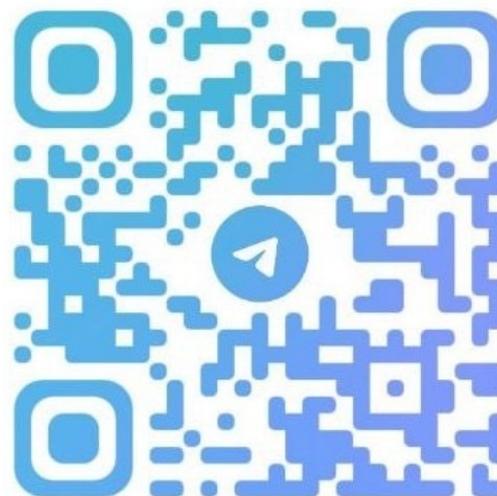


Победитель ежегодной всероссийской премии молодежного предпринимательства Young Awards 2024 в номинации «Безопасность» от RB.RU и Альфа-Банка.



Участник Преакселератора 3.0 Сколково

Контакты



e.kornyushina@aideepfake.ru

www.aideepfake.ru

+7 929 573 85 93 Екатерина

Адрес: 121205 Москва Территория
инновационного центра Сколково, ул. Нобеля 7
ОКПО 01929672, ОГРН 1247700498473
ИНН/КПП 9731137991 /773101001