



Будущее цифровой безопасности детей и подходы к прогнозированию рисков: подходы оператора связи

Подход 1: выявлять и отрабатывать новые угрозы

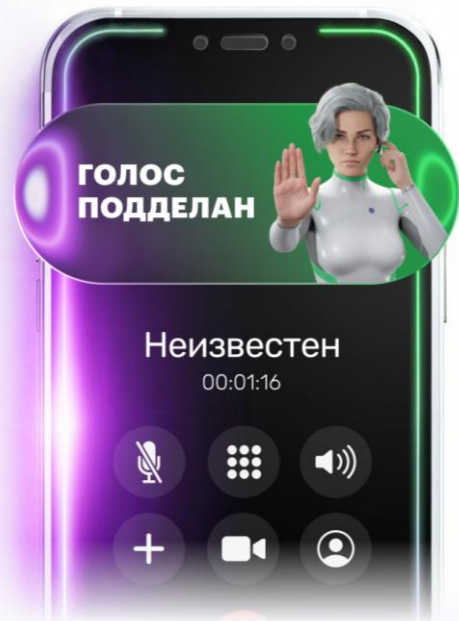
Растет мошенничество с помощью voice-deerfake, дети в зоне риска, нужны новые решения для безопасности







+500% рост случаев мошенничества с сети использованием voice deerfake

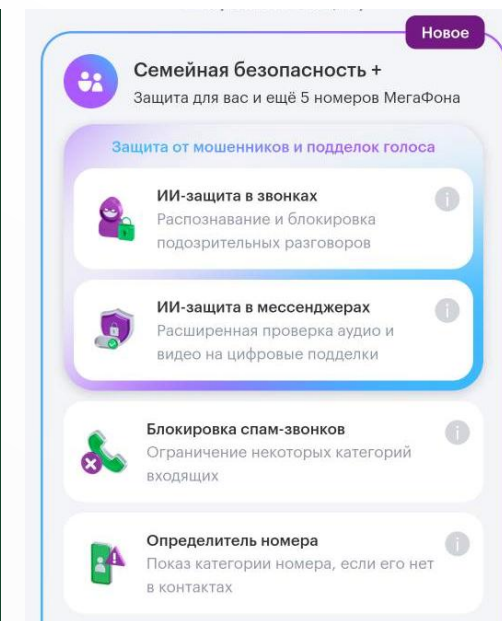
до 15 сек сократилась необходимая длина сэмпла голоса для клонирования

Голоса **родителей и детей** утекают через взлом мессенджеров, где хранятся «войсы» и «кружочки»

МегаФон реагирует запуском новых технологий защиты...



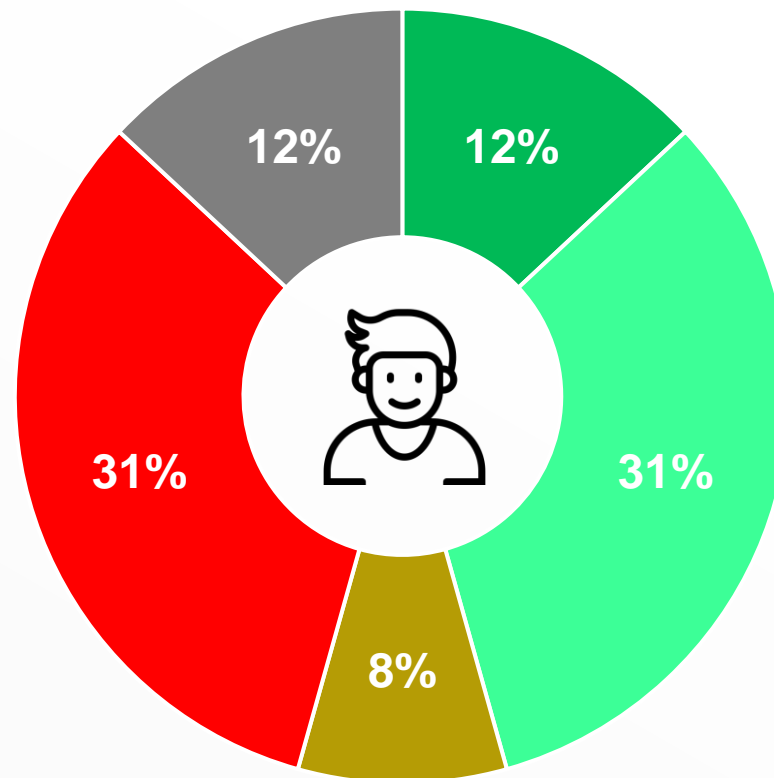
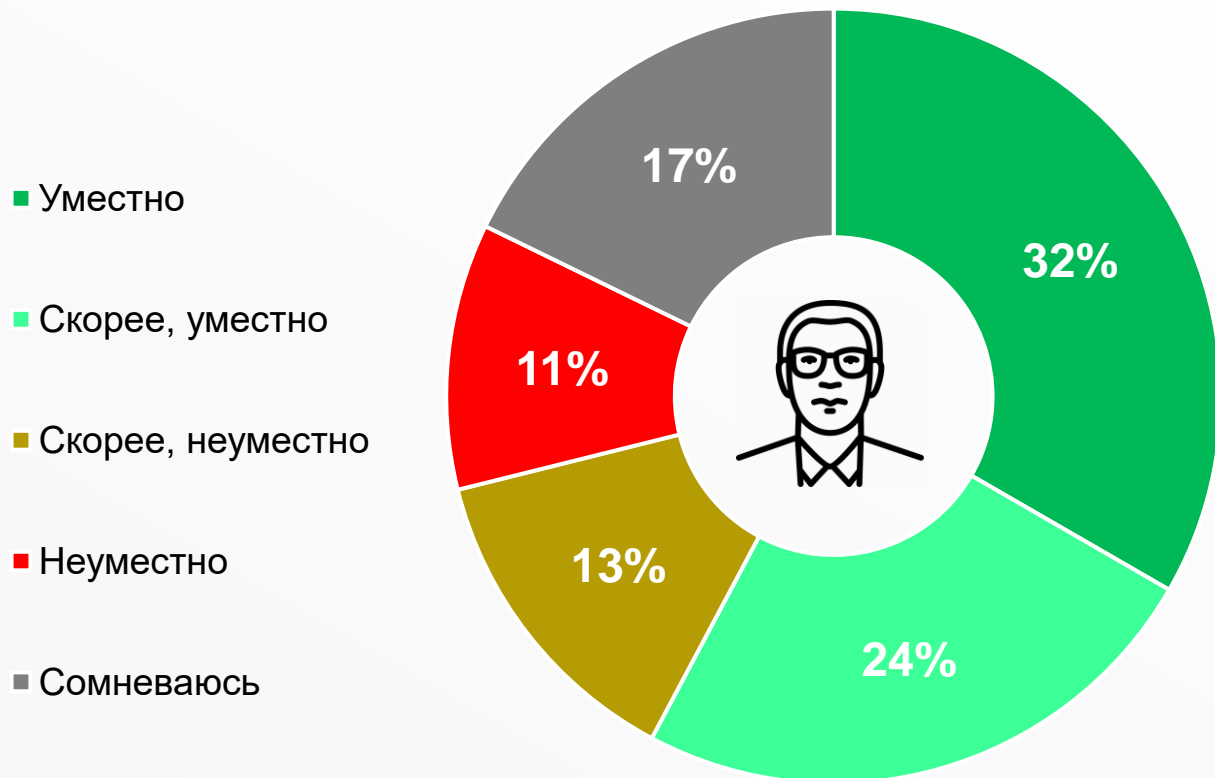
	Ищет неестественные проявления в окружающих шумах		Проверяет соответствие тона и тембра голоса передаваемой эмоции
	Находит ошибки в произношении, ударениях, акцентах		Проверяет паузы, вызванные дыханием
	Выявляет цифровые следы, указывающие на подделку		Ищет неестественные отклонения в ритме речи



Подход 2: не бояться использовать ИИ

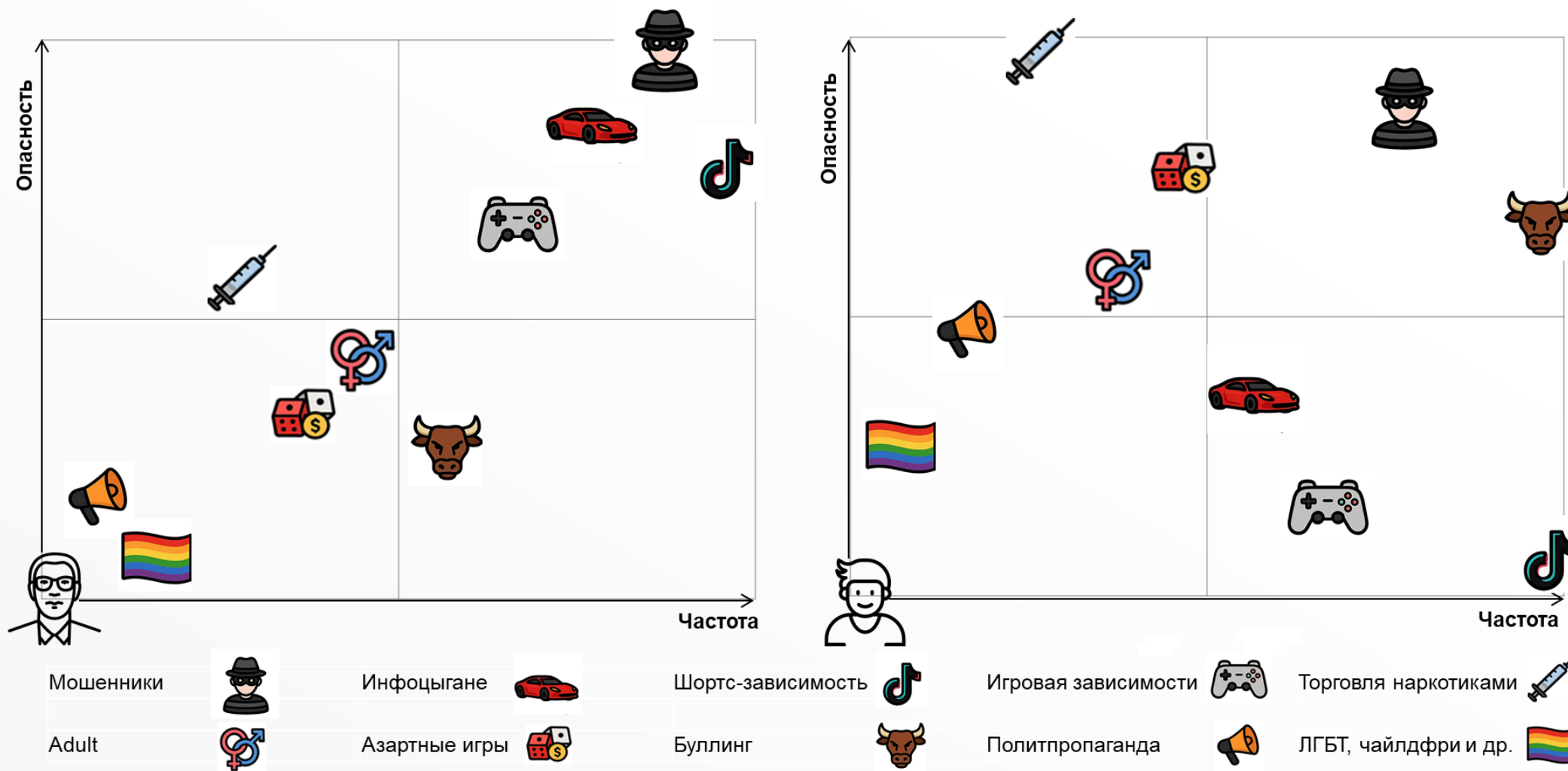
Пользователи допускают применение ИИ для анализа цифровой активности детей и сигнализации об угрозах

Уместно ли для предотвращения наиболее критичных рисков в интернете использовать AI-системы, которые будут анализировать цифровую активность ребёнка и оповещать родителей при выявлении рисков?



Подход 3: прислушиваться к мнению детей об угрозах

Мнение детей и родителей об актуальных цифровых угрозах значительно различается...



Спасибо!

Контакты для сотрудничества и вопросов:

Дмитрий Кишилов, директор бизнес-юнита дополнительных продуктов МегаФон

dmitry.kishilov@megafon.ru

+7 (916) 691 93 79