

Краткий вывод

Комплексное фрод-детектирование в голосовом канале сейчас строится не вокруг одной модели, а вокруг **многослойной архитектуры**: голосовая биометрия, anti-spoofing/deepfake detection, проверка liveness, анализ устройства/сети/ANI/SIP/RTP, поведенческая аналитика, консорциумные fraud-листы, risk scoring и step-up MFA. Такой подход явно продвигают Pindrop, NICE, Nuance/Microsoft, Phonexia, ValidSoft, Daon и Omilia. (pindrop.com)

Open-source-стек пока покрывает в основном **исследовательские компоненты**: speaker verification, anti-spoofing, deepfake detection, embeddings, baseline-модели ASVspoof/SASV. Полноценного open-source-продукта уровня enterprise contact-center fraud platform с готовыми кейсами, консорциумными списками, IVR-интеграцией и расследовательским workflow я не нашёл.

Вендоры и стартапы для голосового fraud detection

Компания / продукт	Тип решения	Что закрывает	Ключевые технологии	Комментарий
Pindrop Protect / Pulse / Passport	Enterprise vendor / scale-up	Fraud scoring звонков, IVR fraud, deepfake detection, voice authentication	Voiceprint, device/audio fingerprinting, metadata, behavior analysis, consortium intelligence, risk score	Pindrop Protect заявлен как multifactor fraud detection для контакт-центров с risk score с IVR до общения с агентом; Pulse добавляет deepfake detection. (pindrop.com)
NICE Enlighten AI Fraud Prevention	Enterprise contact-center vendor	Выявление известных и неизвестных мошенников, анализ миллионов звонков	Voice biometrics, AI-поведенческая аналитика, cross-call correlation	NICE позиционирует решение как end-to-end fraud prevention для контакт-центров с voice biometrics и AI-анализом взаимодействий во времени. (nice.com)
Nuance Gatekeeper / Microsoft	Enterprise biometrics	Аутентификация клиента и fraud prevention	Voice biometrics, biometric authentication, omnichannel identity	Nuance Gatekeeper описывается Microsoft как biometric authentication and fraud prevention technology для интеграции с Dynamics 365 Customer Service. (microsoft.com)
Phonexia Voice Fraud Prevention	Voice biometrics vendor	Fraud prevention в call center, deepfake/manipulation detection	Voice biometrics, speaker identification/verification, deepfake detection, REST/gRPC, on-prem	Phonexia подчёркивает on-prem voice biometrics и detection of morphed, synthetic, cloned voices. (phonexia.com)
ValidSoft VIP / Voice Verity	Voice identity platform	Voice biometrics, deepfake detection, fraud defense	Passive voice biometrics, liveness/deepfake	ValidSoft позиционирует VIP как voice identity

Компания / продукт	Тип решения	Что закрывает	Ключевые технологии	Комментарий
			detection, real-time scoring	platform, a Voice Verity — как real-time deepfake/audio detection. (validsoft.com)
Daon Contact Center Authentication / xDeTECH	Identity vendor	Caller authentication, synthetic voice detection, step-up MFA	Voice biometrics, liveness, synthetic voice detection, MFA	Daon заявляет real-time synthetic voice detection и caller authentication для контакт-центров. (daon.com)
Omilia TalkGuard	Conversational Deepfake и fraud AI / contact-center security центре		ANI spoofing risk analysis, metadata/network checks, voice anti-spoofing	Omilia явно выделяет многослойную защиту: ANI spoofing, suspicious numbers, synthetic/recorded voice. (omilia.com)
Auraya EVA	Voice Contact center voice biometrics ID, synthetic voice vendor detection		Voice ID, synthetic voice detection, fraud prevention	Auraya продвигает EVA for Contact Centers с voice ID и synthetic voice detection. (aurayasystems.com)
Voxmind	Startup / newer Deepfake-resistant vendor voice biometrics		Voiceprints, phoneme-level analysis, deepfake detection	Заявляет voice biometrics + deepfake detection для contact center / voice AI. (voxmind.ai)
Vocos Bouncer	Startup / voice AI security от TTS/voice cloning	Защита voice agents	TTS/voice-clone detection, audio intelligence, real-time screening	Ориентирован на voice agents и детекцию современных TTS/clone атак. (vocos.io)
teleVoice teleSecure	Contact-center Secure contact center vendor authentication		Voice biometrics, MFA, call screening	Подходит как слой contact-center security, но меньше публичных технических деталей. (televoice.com)

Исследования, датасеты и направления R&D

Направление / работа	Что решает	Технологии	Метрики / бенчмарки	Практический смысл
ASVspoof challenges	Детекция spoofed speech: TTS, voice conversion, replay, deepfake	Countermeasure-модели, LA/PA/DF-треки	EER, min-tDCF, challenge protocols	Главный академический бенчмарк для anti-spoofing и speech deepfake detection. (asvspoof.org)
SASV 2022	Совместная задача speaker verification	Integrated ASV + CM pipeline	SASV-EER, SV-EER, SPF-	Ближе к реальному fraud-сценарию: надо понять и

Направление / работа	Что решает	Технологии	Метрики / бенчмарки	Практический смысл
	+ spoofing awareness		EER	«Тот ли человек», и «живой ли/не синтетический ли голос». (arxiv.org)
AASIST	Универсальная anti-spoofing модель без тяжёлого ensemble	Spectro-temporal graph attention network	EER, t-DCF на ASVspoof	Один из сильных open-source baseline-подходов для audio anti-spoofing. (arxiv.org)
RawNet2 anti-spoofing	End-to-end обработка raw waveform для spoofing detection	Raw waveform CNN/ResNet-like encoder	EER, t-DCF на ASVspoof 2019 LA	Хороший baseline для low-level audio artifacts без ручных признаков. (arxiv.org)
Speaker-aware anti-spoofing	Anti-spoofing с учётом enrollment-записи целевого пользователя	Speaker embeddings + CM model	EER, min t-DCF	Перспективно для банков/телекомов, где уже есть voiceprint клиента. (arxiv.org)
Voice spoofing countermeasures survey	Таксономия атак и защит	Hand-crafted features, DL, end-to-end, universal CM	EER, t-DCF, generalization tests	Полезно как карта угроз: TTS, VC, replay, adversarial/anti-forensics. (arxiv.org)

Перечень технологий для комплексного решения

Слой	Технология	Что измеряет / ловит	Примеры сигналов
1. Identity / voice biometrics	Speaker verification 1:1	Является ли звонящий заявленным клиентом	Speaker embeddings, cosine/PLDA score, ECAPA-TDNN, x-vector
2. Watchlist / fraudster detection	Speaker identification 1:N	Совпадает ли голос с известным мошенником	Поиск по базе fraud voiceprints
3. Anti-spoofing	Spoofed speech detection	TTS, voice conversion, replay, cloned voice	LFCC/CQCC, raw waveform, spectrogram, SSL embeddings, AASIST/RawNet2
4. Liveness detection	Passive / active liveness	Живой человек или запись/синтетика	Micro-prosody, phase artifacts, breath/noise patterns, challenge-response
5. Audio forensics	Channel/device/acoustic fingerprinting	Подмена канала, injection, virtual audio device	Codec hops, RTP timing, room impulse, background consistency
6. Telephony intelligence	ANI/SIP/RTP/network analysis	Spoofed caller ID, suspicious routing, VoIP farms	ANI reputation, SIP headers, carrier metadata, geolocation mismatch
7. Behavioral analytics	Поведение в IVR и разговоре	Account reconnaissance, social engineering, unusual intent	DTMF patterns, retry rate, menu traversal, agent manipulation patterns
8. NLP / conversation risk	ASR + intent/entity/risk extraction	Рискованные сценарии	Change address, reset MFA, new payee, urgent transfer
9. Device intelligence	Device fingerprinting	Подозрительное устройство/софтфон	Softphone, emulator, virtual audio driver, device reuse

Слой	Технология	Что измеряет / ловит	Примеры сигналов
10. Graph / consortium intelligence	Связи между звонками, аккаунтами, устройствами	Fraud rings	Shared phone/device/voice/account graph
11. Decisioning	Risk score + policy engine	Итоговое решение	Allow, step-up MFA, transfer to fraud team, block
12. Case management	Investigation workflow	Разбор инцидентов	Timeline, evidence pack, analyst feedback loop

Метрики оценки качества

Группа метрик	Метрика	Что показывает	Когда использовать
Биометрия	FAR / FMR	Доля ложных допусков: мошенник принят за клиента	Критично для банковских сценариев
Биометрия	FRR / FNMR	Доля отказов настоящим клиентам	Важно для CX и нагрузки на операторов
Биометрия	EER	Точка, где FAR = FRR	Для сравнения моделей speaker verification
Anti-spoofing	EER	Ошибки bona fide/spoof классификации	Базовая метрика ASVspoof
Anti-spoofing	min t-DCF	Стоимость tandem-системы ASV + spoofing CM	Лучше EER, если модель встроена в голосовую биометрию
Fraud detection	Precision	Сколько flagged calls реально fraud	Важно для нагрузки fraud-аналитиков
Fraud detection	Recall / Detection Rate	Сколько fraud-звонков поймано	Важно для снижения потерь
Fraud detection	FPR на 1 000 звонков	Сколько ложных тревог на операционный объём	Практичнее, чем абстрактный FPR
Fraud detection	AUC-ROC / PR-AUC	Качество risk score при разных порогах	PR-AUC лучше при редком fraud
Операционные	Time-to-detect	Через сколько секунд после начала звонка есть сигнал	Критично для IVR / real-time сценариев
Операционные	Latency p95/p99	Задержка inference	Нужна для интеграции в live call
Операционные	Containment rate	Доля fraud, остановленная до агента/транзакции	Хорошая бизнес-метрика
Экономика	Fraud loss reduction	Снижение прямых потерь	Главная метрика для бизнеса
Экономика	Cost per reviewed case	Стоимость расследования одного кейса	Важно для SOC/fraud team
CX	Step-up rate	Сколько клиентов отправлено на доп. проверку	Баланс безопасности и UX
CX	Average Handle Time impact	Влияние на длительность звонка	Важно для контакт-центра
Robustness	Cross-dataset EER	Переносимость на новые атаки/каналы	Обязательно для deepfake detection
Robustness	Attack-specific recall	Recall по TTS, VC, replay, injection	Позволяет видеть слепые зоны
Fairness	EER/FAR/FRR по сегментам	Смещения по языку, полу, возрасту, акценту, каналу	Нужно для регуляторных и reputational risks

Open-source решения и компоненты

Open-source решение	Тип	Что даёт	Готовность для enterprise fraud	Ограничения
clovaai/aasist	Anti-spoofing / speech deepfake detection	PyTorch-реализация AASIST для synthetic/manipulated speech detection	Средняя как ML-компонент , низкая как продукт	Нужны адаптация к телефонии, мониторинг, MLOps, интеграция с IVR/SIP, case workflow. (github.com) Уязвимость к domain shift; надо тестировать на ваших кодеках, шуме, RTP, call-center audio. (github.com)
eurecom-asp/rawnet2-antispoofing	Anti-spoofing baseline	End-to-end RawNet2 для ASVspoof 2019 LA	Средняя как исследовательский baseline	Нет готового fraud decisioning; anti-spoofing надо добавлять отдельно. (github.com) Обучен на VoxCeleb; для телефонного канала нужна калибровка/дообучение; не ловит deepfake сам по себе. (huggingface.co)
SpeechBrain	Speech toolkit	Speaker recognition, embeddings, ECAPA-TDNN, x-vectors, recipes	Высокая как toolkit , не fraud-продукт	Не являются production-системой; лицензии и доступ к данным надо проверять отдельно. (asvspoof.org) Не специализирован под fraud, нет telephony intelligence и anti-spoofing по умолчанию. (localai.io)
speechbrain/spkrec-ecapa-voxceleb	Pretrained speaker verification	Готовые speaker embeddings и verification pipeline	Хороший старт для voiceprint ROC	
ASVspoof baselines / challenge repos	Бенчмарки и baseline-модели	Протоколы, датасеты, метрики для spoofing/deepfake detection	Высокая ценность для оценки	
LocalAI speaker-recognition backend	Локальный inference/service layer	Speaker verification / identification через SpeechBrain backend	Полезно для прототипа API	

Рекомендуемая целевая архитектура для ROC

Блок	Open-source вариант	Enterprise вариант	Что проверять
Speaker verification	SpeechBrain ECAPA-TDNN	Nuance, Phonexia, ValidSoft, Daon, NICE	EER, FAR@target FRR, latency

Блок	Open-source вариант	Enterprise вариант	Что проверять
Deepfake / spoof detection	AASIST, RawNet2, ASVspoof baselines	Pindrop Pulse, Phonexia Deepfake Detection, ValidSoft Voice Verity, Daon xDeTECH	EER, min t-DCF, recall по TTS/VC/replay
Voice watchlist	Speaker embeddings + vector DB	Pindrop, NICE, Phonexia	TPIR@FPIR, идентификация fraudsters
IVR behavior analytics	Собственная feature engineering + ML	Pindrop Protect, NICE Enlighten	Recall fraud reconnaissance, FPR на 1 000 звонков
Network/telephony risk	SIP/RTP/ANI feature extraction	Omilia TalkGuard, Pindrop, carrier intelligence	Detection of ANI spoofing, suspicious VoIP routes
Risk engine	Rules + calibrated ML score	Vendor policy engine	Precision/Recall, PR-AUC, business loss reduction
Case management	SIEM/SOAR/Jira + custom dashboard	Vendor fraud console	Analyst productivity, time-to-resolution

Практический вывод

Если нужна **быстрая промышленная защита контакт-центра**, стоит смотреть Pindrop, NICE, Nuance/Microsoft, Phonexia, ValidSoft, Daon и Omilia: они закрывают не только модель, но и интеграцию в IVR/agent flow, risk score, fraud workflow и real-time decisioning.

Если нужна **собственная R&D-платформа**, базовый open-source набор: **SpeechBrain ECAPA-TDNN** для **speaker verification** + **AASIST/RawNet2** для **anti-spoofing** + **ASVspoof/SASV-протоколы** для **оценки** + **собственный risk engine**.

Главный риск open-source-подхода — не качество модели на публичном датасете, а **domain shift**: телефонные кодеки, шум, язык, акценты, SIP/RTP-инъекции, replay через разные устройства, новые TTS/voice-cloning модели и реальные fraud-паттерны контакт-центра. Поэтому метрики надо считать не только на ASVspoof, но и на внутреннем наборе звонков с реалистичными атаками.