

Ученые из AIRI, МТУСИ, Сбера и VeinCV представили новый способ защиты голосовых данных в открытом цифровом пространстве. Разработка предназначена для того, чтобы не допустить автоматического сбора и анализа биометрических характеристик голоса из публично доступных аудиозаписей.

Метод основан на технологии универсальных состязательных патчей (UAP), которые встраиваются прямо в аудиофайл. Эта цифровая «маскировка» делает голос неузнаваемым для автоматических алгоритмов идентификации и анализа, но при этом не искажает смысл сказанного и не мешает восприятию речи человеком.

Особенность технологии — в нарушении работы алгоритмов, отвечающих за извлечение уникальных признаков диктора. Это позволяет защитить голос от попыток несанкционированного профилирования, создания голосовых подделок и взлома по биометрии. При этом аудиофайлы остаются пригодными для транскрипции, перевода и других задач, не связанных с определением личности говорящего.

Новая защита особенно актуальна для тех, кто регулярно публикует голосовой контент — от преподавателей и спикеров до подкастеров и видеоблогеров. Она также может быть полезна бизнесу и образовательным платформам для охраны конфиденциальных материалов, включая вебинары и внутренние лекции.

Технология подходит для файлов любой длины — от коротких реплик до часовых выступлений. Разработка была принята к публикации на международной конференции Interspeech 2025 в Роттердаме и уже доступна в открытом доступе.