Российские банки начали тестировать удаленную идентификацию клиентов через видеосвязь, но эксперты предупреждают о рисках подмены личности с помощью deepfake. Об этом рассказал Дмитрий Крюков, руководитель отдела машинного обучения «МТС Линк».

Основная угроза — использование мошенниками нейросетей для создания фейковых видео. Например, злоумышленники могут «наложить» чужое лицо на изображение и получить доступ к банковским услугам.

Распознать подделку можно по неестественной мимике, задержкам между речью и движением губ, а также нехарактерным интонациям. Дополнительные признаки фейка — размытое изображение, микроколебания цвета или артефакты, которые появляются при резких движениях.

Крюков рекомендует использовать платформы видеосвязи с защитой от DDoS-атак, шифрованием данных и двухфакторной аутентификацией. Например, биометрические системы вроде VisionLabs анализируют направление взгляда, одежду и движения, определяя, живой человек в кадре или цифровая копия.

Еще один способ повысить безопасность — интеграция с SIEM-системами, которые отслеживают действия пользователей в реальном времени. Однако эксперт подчеркнул, что технологии deepfake постоянно совершенствуются, и полностью исключить риск пока невозможно.