

УДК 004.934.8'1

**РАЗРАБОТКА МЕТОДИКИ ВЫЯВЛЕНИЯ СИНТЕЗИРОВАННОГО ГОЛОСОВОГО
ОБРАЗА ДЛЯ ПОВЫШЕНИЯ НАДЕЖНОСТИ БАНКОВСКИХ СИСТЕМ
ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ**

Муртазин Р.А. (Университет ИТМО), **Фёдоров Е.А.** (Университет ИТМО)
Научный руководитель – к.т.н., Кузнецов А.Ю. (Университет ИТМО)

Разработан алгоритм выявления синтезированной голосового образа и создан алгоритм, позволяющий повысить устойчивость банковских систем голосовой биометрии к атакам посредством синтеза голосовой последовательности.

Введение. Использование голосовой биометрии является перспективным и, теоретически, одним из наиболее надежных способов идентификации и аутентификации пользователей, в том числе удаленной. Целью данной работы является определение характерных различий синтезированного и подлинного голосовых образов и способов их выявления для повышения устойчивости голосовых биометрических систем к атакам посредством синтеза голосовой последовательности.

Основная часть. Надежность банковских систем голосовой биометрии для идентификации и аутентификации пользователей зависит от их устойчивости в том числе к атакам посредством синтеза голосовой последовательности. Разработанная методика подразумевает наличие в ГБС подсистемы проверки подлинности пользователя, функционирующей совместно с подсистемой идентификации.

При подаче сигнала на вход в банковскую информационную систему он проходит предобработку, включающую преобразование типа файла, содержащего голосовой образец в формат WAV, нормализацию способом RMS, децимацию для сокращения времени обучения системы, микширование и удаление неинформативных участков сигнала.

На стадии извлечения речевых признаков сигнал подвергается преобразованию Фурье и Q-константному преобразованию для получения мел-частотных и Q-константных кепстральных коэффициентов соответственно. Выбор данных признаков обусловлен их эмпирически доказанной эффективностью для выявления синтезированных голосовых образов, а также возможностью оптимизации ГБС за счет использования MFCC и CQCC в том числе и для идентификации пользователей.

Затем речевые признаки подаются на вход классификатора, которым является модификация сверточной и рекуррентной нейронных сетей на базе SVM. Модель диктора строится на алгоритме обучения GMM. Сопоставление текущей модели с соответствующим образцом из базы эталонных моделей позволяет принять решение о подлинности пользователя или выявить атаку посредством синтеза голосовой последовательности.

Выводы. Составленный алгоритм по разработанной методике и его программная реализация могут быть применены в банковской сфере для повышения надежности голосовых биометрических систем и их устойчивости к атакам посредством синтеза голосового образа.

Муртазин Р.А. (автор)

Кузнецов В.Ю. (научный руководитель)
