**УДК 004.934.8’1**

# РАЗРАБОТКА СИСТЕМЫ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ БАНКОВСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ С УЧЕТОМ ОСОБЕННОСТИ СИНТЕЗА РЕЧИ

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

Разработан алгоритм голосовой идентификации со встроенной системой распознавания синтезированного голоса для предотвращения проведения успешных спуфинг атак. Разработанный алгоритм основан на характеристиках голоса, позволяющие как идентифицировать человека, так и выявить факт спуфинг атаки с помощью синтезированного голоса, тем самым повышая устойчивость самого метода идентификации.

**Введение.** Развитие систем безопасности, и в частности способов аутентификации человека, позволяют реализовывать новые механизмы ограничения и предоставления доступа. Целью работы является повышение надежности голосовой идентификации за счет дополнительной проверки голоса на подлинность и выявления спуфинг атак.

**Основная часть.** Надежность работы систем идентификации и аутентификации определяется с помощью вычисления ошибок первого (FAR) и второго (FRR) рода. Разработанный алгоритм основывается на вычислении частотно временных характеристиках голоса человека, пропуская извлеченные параметры через обученный классификатор на основе рекуррентной (RNN) и сверточной (CNN) нейронных сетей. Изъятые характеристики одновременно участвуют и в идентификации и верификации пользователя, и в анализе голоса на предмет его возможной подделки.

Весь алгоритм, уже в достаточно установленном виде, делится на Front- и Backend. Frontend содержит в себе предобработку – преобразование сигнала в определенный формат, нормализацию, микширование, удаление неинформативных участков в сигнале. Затем из него извлекаются необходимые характеристики голоса за счет преобразованию Фурье для получения мел-частотных коэффициентов (MFCC) и Q-константному преобразованию для получения и Q-константных кепстральных коэффициентов (CQCC). Также, из-за более показательных различий подлинного и синтезированного голоса в высокочастотной области, извлекаются дополнительные характеристики – инвертированные мел-частотные коэффициенты (IMFCC) и преобразование перекрывающихся блоков на основе инвертированного речевого сигнала (ISOBT).

Backend отвечает за обработку извлеченных данных – параллельно идентифицируется человек и проверяется его голос на происхождение (настоящий или синтезирован) с помощью классификатора. Далее на основе полученных оценок формируется вывод о том, прошел ли человек проверку и имеет ли право доступа в систему. При этом, алгоритм может потребовать провести дополнительную проверку, тем самым конечный вывод условно делится на три уровня – проверка полностью пройдена, необходимо провести дополнительные проверки, проверка не пройдена.

**Выводы.** Разработанный алгоритм идентификации пользователя с параллельной проверкой на синтезированный голос для выявления спуфинг атак может быть применен в банковской сфере, телекоме и медецине для более надежного, устойчивого и удобного способа идентификации клиентов.

Фёдоров Е.А. (автор) _____

Кузнецов А.Ю. (научный руководитель) _____