УДК 004.056.53

АНАЛИЗ ТИПОВ НАПРАВЛЕННЫХ АТАК НА ГОЛОСОВЫЕ БИОМЕТРИЧЕСКИЕ СИСТЕМЫ

А.Е. Сальников, А. А. Двойникова, А.Ю. Кузнецов.

Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики». Санкт-Петербург, Россия

Научный руководитель: А.Ю. Кузнецов.

Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики». Санкт-Петербург, Россия

В статье был проведен анализ спуфинг атак на информационные системы, использующие голосовую биометрию. Рассмотрены наиболее известные типы атак, разобраны их преимущества и недостатки, произведена сравнительная характеристика.

Ключевые слова: *спуфинг, имперсонализация, повторное воспроизведение, преобразование речи, синтез речи.*

Введение. Системы автоматической идентификации и верификации пользователя по голосу широко используются во многих сферах человеческой жизни. Данные системы более удобны, надежны и экономически выгоднее альтернативных вариантов, предоставляющих доступ к информации. Однако, несмотря на то, что данная система широко распространена на рынке, она до сих пор остается уязвимой к спуфинг атакам.

Цель работы: проанализировать направленные атаки на системы, использующие голосовую биометрию пользователя.

Обзор предметной области. Спуфинг-атаки на системы, использующие голосовую биометрию, разделяются на направленные и ненаправленные в соответствии с уровнем, на котором они совершаются.

Наиболее распространенными типами направленных атак:

1. Имперсонализация
2. Повторное воспроизведение
3. Преобразование речи
4. Синтез речи

Сравнительная характеристика типов атак. Приведенная ниже таблица позволяет представить и наглядно сравнить наиболее распространенные типы атак на системы, использующие голосовую биометрию.

Каждая характеристика оценивается по условной шкале от 1 до 5:

Тип атаки	**Необходимый уровень знаний для реализации метода**	**Требуемое программно-аппаратное обеспечение**	**Устойчивость атаки к методикам защиты систем**	**Коэффициент эффективности спуфинг атаки**
Имперсонализация	1	1	1	0.66
Повторное воспроизведение	2	2	3	0.85
Преобразование речи	5	5	4	0.92
Синтез речи	5	5	5	0.93

Заключение. Проведен сравнительный анализ характеристик наиболее распространенных типов атак на системы, использующие голосовую биометрию. Рассчитан коэффициент успешной реализации спуфинг атаки на основе условных атрибутов. Результаты данного анализа могут пригодиться при моделировании угроз на системы с голосовой биометрией пользователя.