

УДК 681.31

П.Ю. Юрков

РАЗРАБОТКА СИСТЕМЫ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ ПО ГОЛОСУ, УСТОЙЧИВОЙ К “REPLAY”-АТАКЕ*

На современном этапе развития систем автоматической аутентификации личности по голосу особое внимание уделяется защите их от возможных атак злоумышленников. Наиболее часто применяемой является “replay”-атака, суть которой заключается в том, что в систему передаются биометрические признаки, предъявлявшиеся ранее.

Известные в настоящее время системы аутентификации основаны на одной парольной фразе, множестве парольных фраз и множестве ключевых слов.

Анализ этих систем с точки зрения устойчивости их к “replay”-атаке позволяет сделать следующие выводы. Система первого типа является наименее устойчивой, поскольку для проведения “replay”-атаки злоумышленнику требуется записать всего одну фразу, а затем воспроизвести ее с помощью диктофона. Провести “replay”-атаку для систем второго и третьего типа будет более сложно. Для этого злоумышленнику необходимо сформировать базу с записями парольных фраз (или ключевых слов), а также иметь специализированное устройство, позволяющее быстро найти и воспроизвести требуемую запись. В данных системах редко производится смена парольных фраз (ключевых слов) и, следовательно, у злоумышленника есть неограниченный запас времени для формирования соответствующей базы записей. В них используются небольшие по объему множества парольных фраз (ключевых слов), что позволяет злоумышленнику, с одной стороны, быстро сформировать все множество записей, а с другой – легко находить и воспроизводить требуемую запись при осуществлении “replay”-атаки.

Следовательно, система аутентификации по голосу, устойчивая к “replay”-атаке и лишенная указанных недостатков, должна обладать следующими свойствами. Во-первых, быть инвариантной к смене множества парольных фраз (ключевых слов). Во-вторых, контролировать правильность произнесенных фраз (слов). В-третьих, иметь возможность быстрой смены всего множества парольных фраз (ключевых слов) без привлечения пользователей системы; при этом объем множества зависит от интенсивности использования системы пользователем.

В данной работе система аутентификации по голосу, состоящая из текстонезависимого модуля распознавания голоса диктора и дикторонезависимого модуля распознавания слов. Основным достоинством системы является возможность быстрой смены всего множества ключевых слов за счет возможности формирования эталонной модели слова, минуя этап обучения.

* Работа поддержана РФФИ, грант №06-07-89010.