С. Ю. Мельников, М. В. Федюкин (Москва, ООО «Линфо»).
К вопросу об информационной защищенности систем обработки и анализа речевых и текстовых сообщений от пассивных атак.

В последние годы появилось большое количество работ ([1] и др.), в которых анализируются различные аспекты информационной безопасности биометрических систем идентификации. Наибольший практический интерес представляют пассивные атаки, когда злоумышленник не имеет доступа к внутренним процессам обработки информации в системе. В работе [2] рассматривается так называемая «атака на устройство ввода» в системах текстозависимой идентификации диктора по голосу (парольной фразе). Выделяются три типа атак: принудительная, когда диктора заставляют говорить нужную фразу, имитационная атака, когда подделывается голос диктора, и атака воспроизведения, когда речевое сообщение истинного диктора повторяется. Цель таких атак — заставить ошибиться систему биометрической идентификации. Злоумышленник стремится к тому, чтобы система «приняла чужого за своего». Исследуемые в литературе системы относятся к классу систем верификации и предназначены в основном для предоставления определенных прав (например, права доступа) зарегистрированному пользователю.

Однако системы идентификации автора или иных признаков сообщения могут предназначаться и для других целей. В ряде приложений целью функционирования систем идентификации является выявление в потоке речевых материалов сообщений заданного множества дикторов, выявление в потоке речевых и текстовых материалов сообщений на заданных языках или относящихся к заданной тематике. Как правило, такие системы идентификации основаны на использовании статистических критериев, применяемых ко всему содержанию сообщения.

Цель злоумышленников (автора сообщений или сообщников) заключается в пропуске системой целевого сообщения. Опишем одну из легко реализуемых атак. Если злоумышленник хочет передать сообщение S_0, то он передает сообщение $S = (S_0, S_1)$, полученное присоединением к исходному нового сообщения S_1. При получении сообщения адресат просто отбрасывает S_1. Система обработки и анализа может быть «введена в заблуждение» путем специального подбора S_1. Отметим, что присоединение дополнительного сообщения может осуществляться более сложным способом, чем элементарная конкатенация. Например, результирующее сообщение $S = (S_0, S_1)$ может быть получено из последовательности чередующихся фрагментов сообщений S_0 и S_1.

В случае применения такого подхода к речевому сообщению большинство существующих систем идентификации дикторов не смогут с достаточной надежностью определить автора сообщения S_0.

Возможный способ защиты от этой и подобных атак основан на разбиении анализируемых сообщений на фрагменты и обработки их по отдельности. Однако это может привести к снижению точности и увеличению трудоемкости обработки.

СПИСОК ЛИТЕРАТУРЫ

1. *Roberts C.* Biometric attack vectors and defences. — Computers and Security, 2007, v. 26, № 1, p. 14–25.
2. *Ручай А. Н.* Модель атак и защиты биометрических систем распознавания диктора. — Доклады ТУСУР, июнь 2011, № 1 (23), p. 96–100.