А. Е. Сулавко, *канд. техн. наук, Омский государственный технический университет, sulavich@mail.ru*
А. В. Еременко, *канд. техн. наук, Омский государственный университет путей сообщения, 4eremenko@gmail.com*
Р. В. Борисов, *Luxoft (Люксофт), г. Омск, brv1986@yandex.ru*

Генерация криптографических ключей на основе голосовых сообщений[1]

Рассмотрена проблема генерации ключевых последовательностей на основе биометрических данных. Предложены два пространства признаков голоса человека (зависимое и не зависимое от произносимой фразы), способы генерации ключей на основе голосовых сообщений на основе метода нечетких экстракторов с использованием кодов Адамара и БЧХ, исправляющих ошибки. Произведена оценка эффективности описанных способов.

Ключевые слова: голосовые сообщения, нечеткий экстрактор, помехоустойчивое кодирование, биометрия, идентификация диктора.

Введение

На сегодняшний день киберпреступность беспокоит не только специалистов по информационным технологиям и информационной безопасности. Инциденты в сфере кибербезопасности затрагивают интересы и высшего руководства организаций. По данным глобальных аналитических исследований PwC (PricewaterhouseCoopers), число инцидентов и объем причиняемого ими ущерба неуклонно растут. В 2014 г. количество инцидентов составило 42,8 млн. Это означает, что каждый день совершалось в среднем 117 339 кибератак. Если анализировать ситуацию за длительный период, то с 2009 г. совокупный среднегодовой темп роста числа выявленных инцидентов информационной безопасности ежегодно увеличивался на 66% [1]. Общую сумму убытков от киберпреступности в мировом масштабе узнать невозможно, поскольку о многих кибератаках просто не сообщается, а ценность некоторых видов информации определить нелегко. Авторы исследования [2] пришли к выводу, что размер ежегодных убытков от киберпреступности для мировой экономики составляет от 375 млрд до 575 млрд долл. США.

Защита данных от несанкционированного доступа на уровне хранения обеспечивается их шифрованием. Современные методы шифрования надежны, если использовать стойкие ключи (пароли). Но проблема человеческого фактора сводит на нет использование сложных паролей и длинных ключей шифрования. Даже если необходимые требования к генерации надежных паролей и ключей на практике выдерживаются (что в подавляющем большинстве случаев не так), остаются актуальными проблемы безопасного хранения паролей (ключей), социальной инженерии (обманных способов выведывания злоумышленником паролей у пользователей). Кроме того, не секрет, что длинный пароль или ключ шифрования создают существенные неудобства для работника организации (или обычного пользователя), по причине чего владе-

[1] Работа выполнена при финансовой поддержке РФФИ (грант № 15-07-09053).