А. В. Еременко, *канд. техн. наук, ФГБОУ ВПО «Омский государственный университет путей сообщения», nexus-@mail.ru*

А. Е. Сулавко, *канд. техн. наук, ФГБОУ ВПО «Омский государственный технический университет», sulavich@mail.ru*

Двухфакторная аутентификация пользователей компьютерных систем на удаленном сервере по клавиатурному почерку[1]

Рассматривается проблема защиты биометрических данных пользователя, используемых для удаленной аутентификации. Предложен способ доказательства принадлежности субъекта к доверенной группе лиц на основе выполнения помехоустойчивого кодирования его биометрических данных. Разработанный способ основан на методе «нечетких экстракторов» и позволяет хранить только фрагменты биометрического эталона на сервере, похищение которых не позволяет восстановить эталон.

Ключевые слова: клавиатурный почерк, нечеткий экстрактор, помехоустойчивое кодирование, биометрия, двухфакторная аутентификация.

Введение

С развитием информационных технологий и сети Интернет возрастает потребность в обеспечении аутентичности данных, передаваемых по Сети. Фальсификация личности на сегодняшний день представляет большую опасность в отношении наносимого финансового ущерба. По оценкам Zecurion Analytics за 2013 и 2014 гг., совокупные потери мировой экономики от подобных атак составили более 42 млрд долл. [1]. Традиционные процедуры аутентификации основаны на проверке пароля, аппаратного идентификатора или биометрических данных пользователя.

Слабое звено паролей — человеческий фактор. Даже стойкий пароль, удовлетворяющий современным требованиям безопасности, не является гарантией надежной защиты, так как пользователь сам может сообщить его злоумышленнику (наглядный пример — осужденный за свои преступления К. Митник, который узнавал пароли при помощи методов социальной инженерии [2]) либо хранить пароли в ненадежном месте. Аппаратный идентификатор можно украсть или потерять. Последний способ (использование биометрии) является наиболее надежным, однако также не лишен недостатков. Физиологические признаки человека находятся «на виду», и существует множество способов их хищения незаметно для владельца.

В настоящее время разработаны технологии изготовления муляжей отпечатков пальцев, радужки, изображения лица и других биометрических признаков. Использование злоумышленником этих технологий для совершения криминальных преступлений является вполне вероятным событием и вопросом соответствующей ситуации. По данным глобальных аналитических исследований

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