Труды научно-технической конференции кластера пензенских предприятий,
обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.**
Том 10, Пенза-2016, с. 58-59 (http://пниэи.рф/activity/science/BIT/T10-p58.pdf)

УДК: 519.2, 612.087, 621.319.7

Ефимов О.В.

Перспективы широкого использования защищенных биометрических технологий в ответственных гражданских приложениях

В настоящее время биометрия находит все большее и большее применение в повсеместной жизни людей. Это доступ на предприятия через проходные, распознавание своего хозяина планшетами и сотовыми телефонами. Уже присутствуют на зарубежных рынках двери с замками, распознающими лицо человека, уже используются банкоматы, анализирующие пол предъявителя банковской карты. Круг приложений биометрической аутентификации непрерывно расширяется.

Множество приложений биометрии следует разделить на две категории:

- обычные биометрические приложения;
- ответственные биометрические приложения (платежные системы, системы формирования цифровой подписи и т. д.).

Для обычных бытовых приложений возможно применение импортных средств сканирования биометрии [1] и программного обеспечения обработки данных зарубежных производителей с использованием так называемых «нечетких экстракторов» [2, 3]. Замена иностранного программного обеспечения на отечественное желательное, но не обязательное условие для обычной биометрии.

Использование отечественного программного обеспечения в защищенном исполнении становится обязательным, если речь идет об ответственных биометрических приложениях. Более того, для ответственных биометрических приложений сканеры биометрических образов так же должны быть отечественного производства, а для программ обработки биометрии должна использоваться доверенная вычислительная среда так же отечественного производства. Обязательным становится применение защищенного исполнения программного обеспечения с использованием отечественной криптографии.

Научно-технический задел по созданию технологии защищенной нейросетевой обработки биометрических данных уже создан. Разработаны и введены в действие отечественные стандарты техническим комитетом ТК 362 («Защита информации»), регламентирующие требования к искусственным нейронным сетям [4, 5, 6]. Этих стандартов вполне достаточно для защиты от НСД компьютеров, сотовых телефонов, домофонов, и т.д.

Уже разработанные нейросетевые технологии вполне пригодны для защиты аппаратно-программных средств ответственных приложений биометрии. Такие приложения обязательно используют криптографические функции для защиты своих данных. Однако, вопрос о том, на сколько биометрическая защита надежна, пока остается открытым. Необходимо провести исследования в этом направлении и определить то, на сколько механизмы биометрической защиты ослабляют криптографию при ее массовом использовании. В настоящее время разработано несколько механизмов защиты биометрических данных и идет публичное обсуждение технической спецификации одного из таких механизмов в ТК 26 «Криптографическая защита информации» [7].

К сожалению, инициатива по разработке отечественных механизмов криптографической защиты биометрических данных поддерживается только

научно-технической общественностью г. Пензы. По нашему мнению, проблема широкого применения биометрии в «Национальной платежной системе» не может быть решена без предложений со стороны нескольких предприятий. Мы считаем, что необходимо создать и исследовать несколько разнотипных механизмов защиты биометрии, разработанных разными творческими коллективами. Тогда, уже на альтернативной основе, регулятор рынка сможет провести полноценные исследования и даст свои рекомендации по улучшению каждого из предложенных механизмов.

Вопрос наличия биометрии в «национальной платежной системе» - это вопрос организации отечественного серийного производства биометрических приложений. Если в ближайшее время будет принято решение о применении в «Национальной платежной системе» отечественных биометрических технологий, то серийное производство отечественных биометрических сканеров и защищенного программного обеспечения будет налажено.

Острую необходимость в биометрических технологиях проще всего пояснить на примере корпоративного электронного документооборота, поддерживающего цифровую подпись. Сейчас один служащий может передать другому служащему право формирования своей цифровой подписи. Для этого достаточно отдать соседу носитель ключа и сообщить пароль доступа. Администрация предприятия никак не может установить факт подмены. Если же пароль доступа будет усилен биометрической защитой, то один человек не может передать другому человеку право формирования цифровой подписи. Злоупотребления подмены лиц, формирующих цифровую подпись, должны прекратиться при широком использовании биометрического контроля доступа к криптографическому ключу формирования цифровой подписи.

Литература

1. Болл Руд и др. Руководство по биометрии. / Болл Руд, Коннел Джонатан Х., Панканти Шарат, Ратха Налини К., Сеньор Эндрю У. // Москва: Техносфера, 2007. -368 с., (перевод с английского).
2. Dodis Y., Reyzin L., Smith A. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy // Proc. EUROCRYPT, April 13, pages 523-540, 2004.
3. Monrose F., Reiter M., Li Q., Wetzel S. Cryptographic key generation from voice. //Proc. IEEE Symp. on Security and Privacy, pp. 202-213, 2001.
4. ГОСТ Р 52633.0-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации».
5. ГОСТ Р 52633.3-2011 «Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора».
6. ГОСТ Р 52633.5-2011 «Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа».
7. Техническая спецификация (проект) ЗАЩИТА НЕЙРОСЕТЕВЫХ КОНТЕЙНЕРОВ С КРИПТОГРАФИЧЕСКИМ КЛЮЧОМ И ДАННЫМИ БИОМЕТРИЧЕСКОГО ОБРАЗА ПОЛЬЗОВАТЕЛЯ /сайт ТК26- www.tc26.ru (публичное обсуждение).

Статья поступила 23.11.2016, опубликована 07.12.2016
по положительной рецензии д.т.н. Малыгина А.Ю.