МЕТОДИКА ФОРМИРОВАНИЯ БАЗ БИОМЕТРИЧЕСКИХ ОБРАЗОВ

Б.С. Ахметов, д.т.н., профессор, Н.А. Сейлова, к.т.н., доцент, Ж.К. Алимсеитова, старший преподаватель, А. Балтабай магистрант
Казахский национальный исследовательский технический университет имени К.И. Сатпаева, г. Алматы, Республика Казахстан
snurgula@gmail.com

Биометрический образ - это континуум множества биометрических примеров, однако с конечной погрешностью континуум примеров может быть представлен всего несколькими различающимися примерами. Биометрический образ «Свой»: биометрический образ легального пользователя, то есть пользователя зарегистрированного в системе. Биометрический образ «Чужой»: биометрический образ злоумышленника, пытающегося преодолеть биометрическую защиту [1].

При разработке средств биометрической аутентификации необходимо их тестировать [2]. Для тестирования данных средств биометрической аутентификации личности возникает необходимость формирования баз биометрических образов "Свой" и "Чужой", размеры которых обеспечивают подтверждение заданных характеристик тестируемых средств.

Необходимые для достоверного тестирования размеры баз биометрических образов "Свой" малы, и формирование таких баз легко осуществимо, а для образов "Чужой" велики. В связи с этим, создание баз биометрических образов "Чужой" является достаточно длительным и трудоемким процессом. Создать базы такого размера в короткие сроки крайне затруднительно. При тестировании приходится ограничиваться усеченными базами образов "Чужой", непосредственно полученными с тестируемого средства аутентификации. Дополнять такие базы приходится биометрическими образами "Чужой", ранее полученными при тестировании средств аутентификации с аналогичными биометрическими преобразователями.

Описание методики. При формировании баз биометрических образов используются методика, с участием доноров - лица, добровольно участвующее в формировании базы естественных биометрических образов путем предоставления своих собственных биометрических образов для преобразования их в цифровую форму. Условия сбора биометрических данных – в аудитории под контролем персонала, психофизиологическое состояние доноров - нормальное без нагрузок и внешних раздражителей.

Всем донорам перед началом работы также должны быть доведены цели, задачи сбора и обработки личных биометрических данных. С каждым донором проводятся занятия по правилам пользования программой сбора биометрических образов.

Время сбора биометрических образов распределено следующим образом:

1 этап (20 мин.) – ознакомление с программой, тренировка, определение класса пользователя, контрольная проверка-тест, закрепление полученных навыков.

2 этап – сбор биометрических данных (60 мин.). Перед каждым новым сеансом следующего дня обязательное повторение и закрепление навыков пользования с обязательным контролем.

В качестве программного обеспечения используется программа «НейроТест 1.2», предназначенная для преобразования рукописного слова-пароля в обычный длинный пароль или ключ. Запомнить одно или два коротких слова для человека намного проще, чем запомнить пароль из 20 случайных символов или ключ из случайной последовательности из 256 бит. Слова парольной фразы должны обязательно воспроизводиться

рукописным почерком легального пользователя. Нелегально извлечь из программы рукописный пароль или личный ключ пользователя практически невозможно.

В данной программе используется эмулятор искусственной нейронной сети, имеющей множество выходов. Число выходов искусственной нейронной сети определяется длиной порождаемого ею биометрического ключа [3-4]. Это исключает взлом программы через обнаружение и подмену последнего бита решающего правила. Программа «НейроТест 1.2» имеет многобитовое решающее правило, сочетание значений бит которого уникально и злоумышленнику неизвестно. В программе использован алгоритм быстрого автоматического обучения искусственной нейронной сети с 256 выходами.

В первом этапе сбора рукописных биометрических образов имеются несколько режимов.

Режим обучения. Обучение начинается с инициализации режима обучения. После ввода рукописного слова, данное слово добавляется, при этом линованное поле очищается, а в правой части окна появляется номер очередного введенного примера. Если при вводе рукописного слова-пароля дрогнула рука, или образ записи не характерен, то необходимо очистить и ввести снова данный пароль. При этом слово удаляется без занесения в базу примеров.

Контроль распознавания «Своего». После обучения нейросети необходимо проверить качество узнавания системой «Своего». Проверка обучения осуществляется путем воспроизведения рукописного слова и проверки.

Режим тестирования. Тестирование системы начинается с инициализации режима тестирования.

- Самостоятельное статистическое тестирование системы
- Оценка вероятности ошибок первого рода (отказ «Своему»).

Написав 40 требуемых образов «Свой» пользователь может приступать к формированию базы образов «Чужой». Для этого необходимо активизировать формирование (становится активной после ввода всех образов «Свой»).

Имеется функция, которая отменяет сеанс данного пользователя, вся введённая пользователем информация (имя, фамилия и рукописные образы) не сохраняется.

Режим ввода образов «Чужой» очень похож на режим ввода образов «Свой». Единственное отличие в том, что пользователю приходится писать не одно и то же слово, а случайно выдаваемые системой слова [5-7].

Заключение. Для тестирования и подтверждения соответствия (сертификации) средств высоконадежной биометрической аутентификации, для каждого конкретного первичного биометрического преобразователя создается своя база естественных биометрических образов, обладающая достаточной полнотой. Полная база должна быть способна совместно с базами других близких по типу биометрических преобразователей обеспечивать тестирование всего многообразия средств, использующих конкретный биометрический преобразователь.

Первое тестирование средства с новым первичным биометрическим преобразователем всегда связано с необходимостью создавать для него новую базу его естественных биометрических образов. Формирование такой базы должно обеспечить возможность будущего тестирования и сертификации других средств биометрической аутентификации с аналогичным первичным биометрическим преобразователем.

Список литературы:

1. ГОСТ Р 52633.0-2006 , Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации

2. ГОСТ Р 52633.1-2009 , Защита информации. Техника защиты информации.

Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации

3. Олейник Ю.И., Малыгина Е.А., Малыгин А.Ю. Биометрия: проблемы тестирования. "Труды Международного симпозиума «Надежность и качество», Том1-2005г.

4. Ахметов Б.С., Горбачено В.И. Нейронные сети. Лабораторный практикум. – Алматы Издательство КазНТУ имени К.И.Сатпаева, 2015г. – 97с.

5. Ахметов Б.С., Горбаченко В.И., Кузнецова О.Ю. Нечеткие системы и сети. Учебное пособие.– Алматы:Издательство КазНТУ имени К.И.Сатпаева, 2014.– 68с.

6. Ахметов Б.С., Иванов А.И., Картбаев Т.С. Угрозы средствам нейросетевой биометрической защиты информации. Вестник КБТУ. 2014. - № 4(31). - С. 48-54

7. B. Akhmetov, S. Akhmetova, A. Ivanov, A. Malyghin, K. Mukapil. Application of Iterative Algorithm of Training of Single Neuron in Biometric Appendices. International Conference on Innovative Trends in Multidisciplinary Academic Research, October 20-21, 2014. ITMAR © 2014 Istanbul, Turkey.