УДК 004.056.5

С. М. Гончаров, Г. А. Квачук, А. Е. Боршевников

ВОЗМОЖНОСТЬ ПРИМЕНЕНИЯ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ НА ОСНОВЕ БИОМЕТРИЧЕСКИХ ДАННЫХ

В настоящее время идет активное развитие биометрических технологий. Одним из направлений развития являются методы высокоточной биометрические аутентификации человека. В данной статье мы рассмотрим систему, в которой будет применяться двухфакторная аутентификация, где первым фактором будет аутентификация по трёхмерной геометрии лица, а вторым – аутентификация по ЭЭГ с использованием нейросетевого преобразователя «Биометрия - код доступа». В рассматриваемой системе будет использоваться персональный идентификатор пользователя со встроенной микросхемой, на которой будут храниться данные необходимые для процедур аутентификации.

Рассмотрим первый фактор аутентификации. Системы биометрической аутентификации, основанные на трехмерной геометрии лица, обладают следующими преимуществами:

1. такие системы не требуют прямого физического контакта с пользователем.
2. снятие изображений лиц при помощи камер не представляет никаких технических трудностей.

Недостатком данного метода является то, что данные хранятся в открытом виде. И компрометация базы данных эталонных значений дает возможность сделать муляж биометрического признака [1]. Поэтому при подделке личности или при необходимости проведения более жесткой проверки подлинности личности (например, для организации защиты в критических приложениях) в качестве второго уровня аутентификации можно применить аутентификацию на основе ЭЭГ. У этого вида биометрии существует свой ряд неоспоримых преимуществ:

– данные полученные из ЭЭГ конфиденциальны, их крайне сложно подделать;

– снятие ЭЭГ возможно только на расстоянии не более 1мм от поверхности головы пользователя, что обеспечивает дополнительную защищенность от перехвата злоумышленником и невозможность незаметного для пользователя съема данных.

Недостатком же данного метода является сложность реализации поддерживающей его инфраструктуры, которая позволяет использовать данный метод только как дополнительный механизм аутентификации [2,3].

ЭЭГ является трудно подделываемой неотъемлемой частью пользователя, но сама по себе слишком громоздка и неочевидна. Поэтому данные ЭЭГ используют для генерации уникального ключа, на основе которого и будет производиться аутентификация пользователя. Одним из

методов генерации секретного ключа является использование нейросетевых преобразователей «Биометрия – код доступа». Нейросетевой преобразователь «Биометрия – код доступа» – это заранее обученная искусственная нейронная сеть с большим числом входов и выходов, преобразующая частично случайный вектор входных биометрических параметров «СВОЙ» в однозначный код криптографического ключа и преобразующая любой иной случайный вектор входных данных «ЧУЖОЙ» в случайных выходной код. Описанию данного нейросетевого преобразователя посвящена линейка стандартов ГОСТ Р 52633.

Во время генерации ключевой последовательности на основе данных ЭЭГ пользователя на выходе нейросетевого преобразователя мы получаем набор данных $k;\mu$, где k–сгенерированная ключевая последовательность, а μ –весовые коэффициенты нейронной сети. Значение криптографической хеш-функции от секретного ключа и набор весовых коэффициентов записываются в микросхему вместе с данными о трехмерной геометрии лица для дальнейшего использования в процедуре аутентификации.

Во время аутентификации нейросетевой преобразователь «Биометрия – код доступа» автоматически обучается под полученные от пользователя весовые коэффициенты нейронной сети. Далее происходит снятие ЭЭГ пользователя и генерация секретной ключевой последовательности на уже обученной нейронной сети и полученных биометрических данных. Аутентификация проходит успешно, если значение хеш-функции от полученной секретной ключевой последовательности и от содержащейся в микросхеме пользователя совпадут.

В заключение стоит сказать, что реализация описанной выше системы вполне осуществимая задача. Планируется проведение экспериментов по реализации двухфакторной аутентификацию на основе геометрии лица и ЭЭГ пользователя.

Список литературы

1. Гончаров С.М. Генерация ключевой пары на основе 3-мерной геометрии лица с использованием дифференциально-геометрического представления / С.М. Гончаров, А.В. Первак // Доклады Томского государственного университета систем управления и радиоэлектроники: Научный журнал. – Томск: Изд-во ТУСУР, 2012. – № 1 (25), часть 2 – С. 161–165.

2. Боршевников А.Е. Результат эксперимента по восстановлению секретного ключа по ЭЭГ с использованием нейросетевого преобразователя "Биометрия - код доступа" / А.Е. Боршевников, М.Е. Маркин // Сборник докладов 61-й международной молодежной научно-технической конференции «Молодежь. Наука. Инновации», 21-22 ноября 2013 г. – Владивосток: Мор. гос. ун-т, 2013.- Т. 1.- С. 126-128.

3. Перцев А.О. Использование устойчивых мысленных образов в качестве элементов словаря для аутентификации / А.О. Перцев, М.Е. Маркин, Г.А. Любавский // Сборник докладов 61-й международной молодежной научно-технической конференции «Молодежь. Наука. Инновации», 21-22 ноября 2013 г. – Владивосток: Мор. гос. ун-т, 2013.- Т. 1.- С. 139-142.