УДК 004.89

А.В. Чуйков, А.М. Вульфин, В.И. Васильев

Нейросетевая система преобразования биометрических признаков пользователя в криптографический ключ

Работа посвящена совершенствованию алгоритмов биометрической аутентификации за счет преобразования биометрических признаков в криптографический ключ на основе нейросетевых алгоритмов анализа изображений. Разработан алгоритм нейросетевого преобразования исходных биометрических признаков в криптографический «закрытый» ключ, разработана структура биометрической криптографической системы аутентификации, основанная на использовании нейросетевых алгоритмов, отличающаяся способом формирования и сжатия выделяемых признаков образов с помощью самоорганизующейся двумерной карты Кохонена, свёрточной нейронной сети и вероятностного метода главных компонент. Для однозначного сопоставления пар «биометрический образ» – «криптографический ключ» используются двунаправленная гетероассоциативная память и многослойный персептрон, что позволяет снизить вероятность возникновения ошибки второго рода и достичь оптимальных результатов в процессе генерации криптографического ключа, вследствие чего отсутствует осуществляемая возможность компрометации конфиденциальных данных в процессе аутентификации.

Ключевые слова: биометрическая аутентификация, самоорганизующаяся двумерная карта Кохонена, свёрточные нейронные сети, многослойный персептрон, вероятностный метод главных компонент, AlexNET, двунаправленная гетеро-ассоциативная память.

doi: 10.21293/1818-0442-2018-21-3-35-41

На сегодняшний день существуют два основных направления применения биометрических методов: решение задачи аутентификации пользователя и их интеграция с криптографическими системами [1–3].

Один из основных недостатков криптографических систем заключается в необходимости обеспечения надежного хранения секретных криптографических ключей.

Перспективным направлением повышения эффективности систем аутентификации является интеграция биометрических и криптографических методов. Биометрические методы в криптографических системах первоначально применялись для защиты от несанкционированного доступа злоумышленника к секретным ключам. На сегодняшний день их основным применением стало преобразование биометрических параметров в код ключа доступа (криптографический ключ) [3].

Исходные биометрические признаки пользователя нечетко воспроизводимы, что затрудняет их использование в биометрических криптографических преобразованиях, требующих точного значения ключа [1, 3].

Биометрические системы аутентификации на основе применения технологий искусственного интеллекта чаще всего аппроксимируют нелинейное функциональное отображение, позволяют отнести распознаваемый биометрический образ к одному из заранее заданных классов. Такие системы подвержены атаке на «последний бит» [4]. Системы биометрической аутентификации на основе наиболее распространенного инструмента искусственного интеллекта (нейросетевых технологий) также имеют ряд недостатков:

1) необходимость переобучения нейронной сети при добавлении пользователя, что может быть решено с помощью модульной структуры системы;

2) данные системы подвержены ошибке второго рода, которая выражается в вероятности допущения в систему нелегитимного пользователя.

Следовательно, необходимо совершенствовать биометрические системы аутентификации за счет создания комплексных систем, учитывающих несколько источников биометрических образов, и использовать методы, например искусственного интеллекта, для однозначного сопоставления пары «биометрический образ» – «криптографический ключ».

Цели и задачи

Целью работы является совершенствование алгоритмов биометрической аутентификации за счет нейросетевого преобразования биометрических признаков в криптографический ключ.

Для достижения данной цели были поставлены следующие задачи:

- 1) анализ существующих биометрических криптографических систем;
- 2) разработка структуры системы аутентификации с нейросетевым преобразованием исходных биометрических признаков в криптографический закрытый ключ;
- 3) реализация алгоритма нейросетевого преобразования исходных биометрических признаков в криптографический закрытый ключ;
- 4) разработка программного модуля, реализующего предложенный алгоритм биометрической аутентификации, и оценка эффективности предложенного решения на натурных данных.

Анализ существующих криптографических биометрических систем

Сравнительная характеристика существующих решений представлена в табл. 1 [1–6].

В [1–3] отмечается, что во многих исследованиях длина используемых криптографических ключей очень мала, а вероятность ошибки второго рода пре-

вышает допустимые нормы для практического применения.

Для генерации ключей на основе биометрических образов сегодня используются два основных инструмента, удовлетворяющих требованиям современной криптографии и обладающих низкой вероятностью ошибки второго рода: нейросетевой преобразователь «биометрия – код» и нечеткие экстракторы.

Нейросетевой преобразователь «биометрия – код» [4, 5] основан на использовании нейронной сети с небольшим количеством скрытых слоев или вовсе без них. Размерность пространства признаков и выходного вектора сети, напротив, велико, что позволяет реализовать преобразование нечеткого входного вектора биометрических признаков «свой» в соответствующий криптографический ключ, а иной случайный входной вектор (образ «чужой») – в случайный выходной образ [1].

Таблица 1

Сравнительный анализ существующих криптографических биометрических систем

	С освобождением ключа «key release cryptosystems»	Со связыванием ключа «key binding cryptosystems»	С генерацией ключа «key generation cryptosystems»
Особенности	Биометрический эталон и ключ хранятся отдельно;	Криптографический ключ и биометрический эталон связаны с помощью алгоритма замещения небольшого количества секретных битов криптографическим ключом; используются корректирующие коды; нечеткий контейнер (fuzzy vault) – наиболее распространенная схема	Криптографический ключ извлекается из биометрических данных и для него не требуется хранения в базе данных; большие искусственные нейронные сети; нечеткие экстракторы (fuzzy extractors)
Достоинства	Простота реализации	Безопасность метода обусловлена секретностью алгоритмов закрытия и восстановления ключа	Криптографический ключ не хранится в базе данных
Недостатки	Биометрические эталоны хранятся локально; требуется доступ к хранящимся локально незащищенным и незашифрованным биометрическим эталонам;	Детерминированные алгоритмы закрытия ключа могут быть скомпрометированы; алгоритмы сложны в реализации из-за изменчивости биометрических признаков	Высокая сложность реализации системы; биометрические данные неточно воспроизводимы, что затрудняет их использование в качестве основы устойчивой генерации ключа
Уязвимости и атаки	Подмена злоумышленником с помощью вредоносного ПО модуля сравнения образов	Корреляционная атака (correlation attacks, attacks via record multiplicity – ARM); атака с инверсией ключа (surreptitious key-inversion attacks – SKI); атака подстановки со смешиванием (blended substitution attacks)	

Нечеткие экстракторы (fuzzy extractors) [2, 3, 6] позволяют однозначно восстанавливать секретный ключ из нечеткого биометрического образа за счет использования дополнительной информации [7, 8] (helper data). В основе работы нечеткого экстрактора лежит возможность извлечения случайной равномерно распределенной последовательности из биометрического образа и последующее корректное восстановление ее из размытого биометрического образа.

Одной из актуальных проблем создания криптографических биометрических систем аутентификации является проблема их тестирования. Требуется создание баз биометрических образов (двухмерных и трехмерных изображений лица и т.д.) значительной размерности, что сопряжено с определенными трудностями. Использование изображения лица человека для формирования биометрического образа имеет ряд преимуществ по сравнению с другими методами: для этого не требуется специальное оборудование и не нужен физический контакт с устройством.

Разработка структуры и алгоритма функционирования системы аутентификации с нейросетевым преобразованием исходных биометрических признаков в криптографический закрытый ключ

Предлагаемая структура нейросетевой системы (НС) биометрической аутентификации приведена на рис. 1.

При разработке структуры системы аутентификации с нейросетевым преобразованием исходных биометрических признаков в криптографический закрытый ключ алгоритм разделен на пять условных этапов:

- 1) предобработка признаков;
- 2) генерация признаков;
- 3) создание базы биометрических образов;
- 4) нейросетевое сопоставление образов и ключей;
- 5) восстановление ключа.

Задача блока предобработки признаков заключается в унификации изображения лица человека и построении первичного вектора признаков.

Рис. 1. Структура нейросетевой системы биометрической идентификации

Далее векторы признаков подаются в блок генерации признаков, где происходит их преобразование в компактные векторы признаков, содержащие минимальный и достаточный объем информации.

Если текущей является задача добавления пользователя в систему, то компактный вектор признаков подается на вход блока создания базы биометрических образов, где выполняется нейросетевое сопоставление закрытого ключа и подаваемого вектора.

Блок восстановления ключа необходим для трансформации компактного вектора признаков в требуемый ключ пользователя (при несанкционированной авторизации система выдает случайный ключ, неиспользуемый в системе).

Экспериментальная часть

На этапе предобработки осуществляется создание двух обучающих выборок: позитивной и негативной. В видеопотоке зафиксированы разные углы наклона головы в меняющихся условиях освещения, а также с однородным фоном. Исходные кадры имели разрешение 1280×720 пикселей, затем на каждом из них произведен поиск области, содержащей лицо человека (ROI – region of interest), с помощью алгоритма Виолы–Джонса [9]. Выделенные области размечены и масштабированы до размера 256×256 пикселей таким образом, чтобы содержать минимальное количество пикселей за пределами интересующего нас лица. Дополнительно производилась нормализация изображений выравниванием гистограммы для нормализации участков кадров с различными яркостями.

Первая выборка содержит достаточное количество изображений лиц каждого пользователя системы. Негативная выборка образована изображениями произвольных предметов, пейзажей и т.п. и служит для изоляции позитивных примеров в пространстве признаков.

Кодирование признаков предлагается выполнять с помощью следующей схемы: изображения всех классов позитивной и негативной выборок представляются в виде целочисленной матрицы унифицированного размера $[n, n]$, разбиваемой построчно в вектор-столбец размером $[n \times n, 1]$, что обеспечивает инвариант к смещению области интереса в вертикальном направлении. Каждый элемент вектор-столбца может быть преобразован в рефлексивный двоичный 8-разрядный код Грея [10], в таком представлении два соседних значения цветовой шкалы отличаются только в одном разряде [11]. Открытые и закрытые ключи созданы в криптографической системе с использованием асимметричного алгоритма RSA. Закрытый ключ представляется в виде целочисленного вектор-столбца $[m, 1]$ длиной $m = 132$. Каждый элемент вектора преобразуется в рефлексивный двоичный 8-разрядный код Грея, а затем полученная матрица снова делится на строки. Из полученных строк строится вектор-столбец $[8 \times m, 1]$.

Генерация признаков заключается в проецировании первичного вектора в новое пространство признаков и формировании компактного вектора признаков каждого образа для последующей нейросетевой обработки. Этот вектор подается в нейросетевой блок в форме двоичного вектора или в форме целочисленного вектора, который, в свою очередь, генерирует закрытый ключ, подаваемый на вход модуля криптографической системы.

Для генерации признаков предлагается использовать следующие подходы:

- 1) самоорганизующаяся двумерная карта Кохонена (self-organizing map, SOM) [12];
- 2) вероятностный метод главных компонент (BMГК, probabilistic principal component analysis, PPCA) [13];
- 3) сверточная нейронная сеть (convolutional neural network, CNN) AlexNet [14].

Сопоставление компактных векторов биометрических образов и криптографических ключей реализовано с помощью следующих методов:

1) построение и обучение двунаправленной ассоциативной памяти на основе нейронной сети Б. Коско в варианте Й. Ванга (ВАМ) [15];

2) построение и обучение однослойных и многослойных нейронных сетей прямого распространения на основе персептронов (МСП).

Параметры проведения экспериментов приведены в табл. 2, где

1) исходное изображение – в градациях серого или в RGB в виде целочисленной матрицы;

2) satlins – кусочно-линейная функция активации, симметричная [16];

3) elliotstsig – аппроксимация сигмоидальной функции активации вида гиперболический тангенс [17];

4) hardlim – пороговая функция активации, не симметричная.

Таблица 2

Сравнительные архитектуры НС-блока и условия эксперимента

Параметры	Эксперимент				
	1	2	3	4	5
	МСП	ВМГК + МСП	Двумерная карта Кохонена + МСП	AlexNET + МСП	ВАМ
Исходные изображения	[64, 64, 1]	[64, 64, 1]	[64, 64, 1]	[227, 227, 3] в цветовой схеме RGB	[64, 64, 1]
Генерация компактного вектора признаков	Нет	С помощью ВМГК отобрано 64 главных компоненты	Двумерная карта Кохонена, 15×15 нейронов с гексагональной решеткой	Сверточная НС AlexNET (активации fc8 слоя)	Нет
Архитектура НС блока сопоставления					
Размерность входного вектора	4096	64	225	1000	4096
Тип входного вектора	Десятичные целые числа [0, 255]	Вещественные числа	Бинарный вектор активностей нейронов выходного слоя карты Кохонена	Вещественные числа	Двоичный код Грея
Размерность выходного вектора	132 или 1056	1056	1056	1056	1056
Тип выходного вектора	Десятичные целые числа [0, 255] или двоичные в коде Грея	Двоичный код Грея	Двоичный код Грея	Двоичный код Грея	Двоичный код Грея
Тип НС	МСП	МСП	МСП	МСП	ВАМ
Количество нейронов по слоям	4096, 2018, 1056	64, 1056	225, 1056	1000, 1056	4096, 1056
Функции активации нейронов по слоям	Elliotstsig, elliotstsig, satlins	Elliotstsig, satlins	Elliotstsig, satlins	Elliotstsig, satlins	Satlins, satlins
Постобработка выхода НС	Нет / hardlim	Hardlim	Hardlim	Hardlim	Hardlim

Таблица 3

Сравнительные результаты экспериментов

Параметры	Обучение					Тестирование				
	МСП	ВМГК + МСП	Двумерная карта Кохонена + МСП	AlexNET + МСП	ВАМ	МСП	ВМГК + МСП	Двумерная карта Кохонена + МСП	AlexNET + МСП	ВАМ
Абсолютное количество ошибок / примеров	394 [4500]	362 [4500]	281 [4500]	273 [4500]	23 [450]	133 [1500]	124 [1500]	95 [1500]	88 [1500]	8 [150]
Доля корректно распознанных образов, %	91,24	91,96	93,76	93,93	94,89	91,13	91,73	93,67	94,13	94,67
Чувствительность	0,9688	0,9825	0,9784	0,9729	0,9865	0,9828	0,9806	0,9808	0,9808	1
Специфичность	0,9727	0,9753	0,9830	0,9811	0,9628	0,9763	0,9775	0,9774	0,9774	0,9758
Положительная прогностическая значимость	0,8794	0,8869	0,9188	0,9101	0,8391	0,8837	0,9004	0,9011	0,9014	0,8966
Прогностическая ценность отрицательных результатов	0,9934	0,9965	0,9957	0,9946	0,9972	0,9968	0,9959	0,9959	0,9959	1

Стоит отметить, что во всех экспериментах, кроме эксперимента с ВАМ, обучающие выборки состояли из позитивной (5 классов по 1000 примеров) и негативной (1000 примеров). В случае с ВАМ обучающая выборка состояла из позитивной (5 классов по 100 примеров) и негативной (100 примеров). Разделение всех выборок в процентном соотношении было следующим: обучающая выборка составляла 75%, а тестовая – 25%.

В ходе экспериментов, результаты которых отражены в табл. 3, было установлено преимущество карт Кохонена в показателях ошибки первого рода, но в свою очередь данный метод связан с проблемами долгого обучения и повышенной сложности добавления пользователей, чего лишен метод главных компонент.

Свёрточные сети требуют существенных вычислительных ресурсов для выделения метапризнаков и позволяют получить лучшие показатели чувствительности и специфичности.

Использование гетероассоциативной памяти на основе нейронной сети ВАМ показало хорошие результаты сопоставления, однако емкость подобной сети очень мала.

Для сопоставления компактного вектора признаков, выделенных из биометрического образа, и закрытого криптографического ключа использованы многослойные персептроны и гетероассоциативная память на основе нейронной сети ВАМ.

Количество изменяемых параметров очень велико и не позволяет сопоставлять большое количество входных образов высокой размерности (n) и выходных ключей (p) достаточной длины. Общее количество запоминаемых сетью образов выражается соотношением $m = \sqrt{\min(n, p)}$.

Установлено, что достаточно одного скрытого слоя для успешного отображения входного образа в выходной ключ. Использование примеров проверочной выборки, не вошедших в обучающую и тестовую (порядка 30 тыс. изображений лиц и негативных примеров), показало возможность сети генерировать ключ, не принадлежащий ни одному из легитимных пользователей. При использовании только позитивной выборки 42% примеров класса «чужой» нейронная сеть относит к одному из имеющихся классов – порождает ключ легитимного пользователя.

Предположительно такое поведение обусловлено особенностью расположения порождаемых персептронами разделяющих гиперплоскостей и построения незамкнутых областей расположения выходных образов.

Заключение

В работе предложен подход на основе интеграции биометрической системы и криптографического модуля, что обеспечивает распределенное хранение базы биометрических образов и позволяет использовать в качестве выхода нейронной сети генерируемый на основе образа секретный криптографический ключ.

Для достижения поставленной цели разработана структура системы биометрической аутентифи-

кации, которая выделяет биометрические признаки двухмерного изображения лица из видеопоследовательности путем применения алгоритмов цифровой обработки изображений, отличающейся способом формирования и сжатия выделяемых первичных признаков биометрических образов с помощью самоорганизующейся карты Кохонена, вероятностного алгоритма главных компонент, двунаправленной гетероассоциативной памяти и многослойной нейронной сети, что позволяет порождать уникальные приватные ключи для легитимных пользователей в процессе аутентификации без возможности компрометации сжатого устойчивого вектора биометрических признаков, поскольку весь процесс проходит в нейросетевом базисе, представляющем собой «черный ящик».

В результате сравнительного анализа алгоритмов извлечения первичных биометрических признаков и сопоставления сформированного образа с закрытым ключом в рамках предложенной системы аутентификации установлено, что наиболее эффективным на тестовых данных является подход с использованием глубоких свёрточных сетей и нейросетевой двунаправленной гетероассоциативной памяти.

Литература

1. Васильев В.И. Интеллектуальные системы защиты информации: учеб. пособие / В.И. Васильев. – 2-е. изд. – М.: Машиностроение, 2012. – 199 с.
2. Куликова О.В. Биометрические криптографические системы и их применение // Безопасность информационных технологий. – 2009. – Т. 16, № 3. – С. 53–58.
3. Сидоркина И.Г., Меркушев О.Ю. Использование биометрической криптографии в системе управления доступом [Электронный ресурс]. – Режим доступа: <https://cyberleninka.ru/article/n/ispolzovanie-biometricheskoy-kriptografii-v-sisteme-upravleniya-dostupom>, свободный (дата обращения: 12.03.2018).
4. Иванов А., Малыгин А. Высоконадежная биометрическая аутентификация пользователя: последний дюйм первой мили // Первая миля. – 2007. – Т. 2, № 2. – С. 20–24.
5. Ахметов Б.С. Технология использования больших нейронных сетей для преобразования нечетких биометрических данных в код ключа доступа / Б.С. Ахметов, А.И. Иванов, В.А. Фунтиков и др. // Алматы: ТОО «Изд-во LEM», 2014. – 144 с.
6. Dodis Y., Ostrovsky R., Reyzin L. et al. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data // Siam Journal on Computing – 2006. – Vol. 38, № 1. – P. 97–139.
7. Riaz N., Riaz A., Khan S.A. Biometric template security: an overview // Sensor Review. – 2018. – Vol. 38, № 1. – P. 120–127.
8. Biometrics-based Key Generation Research: Accomplishments and Challenges [Электронный ресурс]. – Режим доступа: http://kism.or.kr/file/memoir/6_2_2.pdf, свободный (дата обращения: 20.08.2018).
9. Чуйков А.В., Вульфин А.М. Система распознавания жестов на основе нейросетевых технологий // Вестник УГАТУ. – 2017. – Т. 21, № 3. – С. 113–122.
10. Код Грея [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Код_Грея, свободный (дата обращения: 12.03.2018).

11. Гонсалес Р., Вудс Р. Цифровая обработка изображений. – М.: Техносфера, 2005. – Т. 1072. – С. 2.
12. Осовский С. Нейронные сети для обработки информации / пер. с пол. И.Д. Рудинского. – М.: Финансы и статистика, 2004. – 344 с.
13. Байесовский метод главных компонент [Электронный ресурс]. – Режим доступа: http://www.machinelearning.ru/wiki/images/7/73/BMMO11_11.pdf, свободный (дата обращения: 12.03.2018).
14. Сверточная нейронная сеть. – Ч. 1: Структура, топология, функции активации и обучающее множество [Электронный ресурс]. – Режим доступа: <https://habrahabr.ru/post/348000/>, свободный (дата обращения: 12.03.2018).
15. Kosko B. Bidirectional associative memories // IEEE Transactions on Systems, man, and Cybernetics. – 1988. – Т. 18, № 1. – Р. 49–60.
16. Функции активации в нейронных сетях. [Электронный ресурс]. – Режим доступа: <http://www.aiportal.ru/articles/neural-networks/activation-function.html>, свободный (дата обращения: 12.03.2018).
17. Elliot symmetric sigmoid transfer function [Электронный ресурс]. – Режим доступа: <https://www.mathworks.com/help/nnet/ref/elliotsig.html>, свободный (дата обращения: 12.03.2018).

Чуйков Артём Валерьевич

Студент каф. вычислительной техники и защиты информации (ВТиЗИ) Уфимского государственного авиационного технического университета (УГАТУ)
К. Маркса ул., д. 12, г. Уфа, Республика Башкортостан, Россия, 450008
Тел.: +7-927-351-99-53
Эл. почта: artem.guy@gmail.com

Вульфин Алексей Михайлович

Канд. техн. наук, доцент каф. ВТиЗИ УГАТУ
К. Маркса ул., д. 12, г. Уфа, Республика Башкортостан, Россия, 450008
Тел.: +7-917-400-21-89
Эл. почта: vulfin.alexey@yandex.ru

Васильев Владимир Иванович

Д-р техн. наук, профессор каф. ВТиЗИ УГАТУ
К. Маркса ул., д. 12, г. Уфа, Республика Башкортостан, Россия, 450008
Тел.: +7-917-350-11-39
Эл. почта: vasilyev@ugatu.ac.ru

Chuikov A.V., Vulfin A.M., Vasilyev V.I.

Neural network system for converting the user biometric characteristics into a cryptographic key

The goal of this work is to improve the algorithms of biometric authentication by converting biometric features into a cryptographic key based on neural network technologies. To achieve this goal, an algorithm for the neural network transformation of the original biometric features into a cryptographic «private» key has been developed. The structure of the biometric cryptographic authentication system has also been developed, this structure is based on the use of neural network algorithms, distinguished by the method of forming and compressing the selected features using a self-organizing two-dimensional Kohonen map, a convolutional neural network and the probabilistic method of principal components. To unambiguously match pairs of «biometric image» – «crypto-

graphic key», bidirectional hetero-associative memory and a multilayer perceptron are used, that reduces the probability of a false negatives error and allows to achieve optimal results in the process of cryptographic key generation. As a result, there is no feasible possibility of compromising confidential data in the authentication process.

Keywords: biometric authentication, PPCA, SOM, MLP, CNN, BAM, AlexNet.

doi: 10.21293/1818-0442-2018-21-3-35-41

References

1. Vasilyev V. I. *Intellektual'nye informacionnye sistemy: uchebnoe posobie* [Intelligent protection of information systems]. Moskva: Mashinostroyeniye, 2012. 199 p.
2. Kulikova O. V. Biometricheskiye kriptograficheskiye sistemy i ikh primeneniye. *Bezopasnost' informatsionnykh tekhnologiy*, 2009, vol. 16, no. 3, pp. 53–58.
3. Sidorkina I.G., Merkushev O.Yu. Use of biometric cryptography in a control system of access. Available at: <https://cyberleninka.ru/article/n/ispolzovanie-biometricheskoy-kriptografii-v-sisteme-upravleniya-dostupom> (accessed: March 12, 2018).
4. Ivanov A., Malygin A. Vysokonadezhnaya biometricheskaya autentifikatsiya polzovatelya: posledniy dyum pervoy mili. *Pervaya milya*, 2007, vol. 2, no. 2, pp. 20–24.
5. Akhmetov B.S., Ivanov A.I., Funtikov V.A. et al. Tekhnologiya ispol'zovaniya bol'shikh neyronnykh setey dlya preobrazovaniya nechetkikh biometricheskikh dannykh v kod klyucha dostupa: monogr. [Application of large neural networks for fuzzy biometric data conversion into access key code: monograph]. Kazakhstan, Almaty: Izd-vo LEM, 2014, 144 p.
6. Dodis Y., Ostrovsky R., Reyzin L., et al. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. *Siam Journal on Computing*, 2006, vol. 38, no. 1, pp. 97–139.
7. Riaz N., Riaz A., Khan S.A. Biometric template security: an overview. *Sensor Review*, 2018, vol. 38, no. 1, pp. 120–127.
8. Biometrics-based Key Generation Research: Accomplishments and Challenges. Available at: http://kism.or.kr/file/memoir/6_2_2.pdf (accessed: August 20, 2018).
9. Chuykov A., Vulfin A. Gesture recognition system // *Vestnik UGATU*, 2017, vol. 21, no. 3, pp. 113–122. (In Russ.).
10. Gray Code. Available at: https://ru.wikipedia.org/wiki/Код_Грея (accessed: March 12, 2018).
11. Gonzalez R., Woods R. *Tsifrovaya obrabotka izobrazheniy* [Digital image processing]. Moskva: Tehnosfera, 2005, 1104 p.
12. Osovskiy S. *Neyronnyye seti dlya obrabotki informatsii* [Neural networks for information processing]. Moskva: Finansy i statistika, 2004, 344 p.
13. Bayesovskiy metod glavnykh komponent. Available at: http://www.machinelearning.ru/wiki/images/7/73/BMMO11_11.pdf (accessed: March 12, 2018).
14. Svertochnaya neyronnaya set', chast' 1: struktura, topologiya, funktsii aktivatsii i obuchayushcheye mnozhestvo. Available at: <https://habrahabr.ru/post/348000/> (accessed: March 12, 2018).
15. Kosko B. Bidirectional associative memories. *IEEE Transactions on Systems, man, and Cybernetics*, 1988, vol. 18, no. 1, pp. 49–60.
16. Funktsii aktivatsii v neyronnykh setyakh. Available at: <http://www.aiportal.ru/articles/neural-networks/activation-function.html> (accessed: March 12, 2018).
17. Elliot symmetric sigmoid transfer function. Available at: <https://www.mathworks.com/help/nnet/ref/elliotsig.html> (accessed: March 12, 2018).

Artem V. Chuykov

Student, Department of Computing Equipment and Information Protection, Ufa State Aviation Technical University
12, Karl Marx st., Ufa, The Republic of Bashkortostan,
Russia, 450008

Phone: +7-927-351-99-53

Email: artem.guy@gmail.com

Alexey M. Vulfin

Candidate of Technical Sciences, Assistant Professor,
Department of Computing Equipment and Information
Protection, Ufa State Aviation Technical University
12, Karl Marx st., Ufa, The Republic of Bashkortostan,
Russia, 450008

Phone: +7-917-400-21-89

Email: vulfin.alexey@yandex.ru

Vladimir I. Vasilyev

Doctor of Engineering Sciences, professor, Department
of Computing Equipment and Information Protection,
Ufa State Aviation Technical University
12, Karl Marx st., Ufa, The Republic of Bashkortostan,
Russia, 450008

Phone: +7-917-350-11-39

Email: vasilyev@ugatu.ac.ru