УДК 004.93.1 Вестник УрФО № 3(29) / 2018, с. 29–37

Ложников П. С.

DOI: 10.14529/SECUR180305

ИНТЕГРАЦИЯ БИОМЕТРИЧЕСКОЙ И ЭЛЕКТРОННОЙ ПОДПИСЕЙ С ПРИМЕНЕНИЕМ НЕЙРОСЕТЕВЫХ АЛГОРИТМОВ

В настоящей статье приводятся аргументы относительно возможности использования современных методов распознавания образов в задачах биометрической аутентификации: нечетких экстракторов, искусственных многослойных нейронных сетей, методов «глубокого обучения», а также сверточных, эволюционных, малых, «широких», гибридных нейронных сетей. Приводятся результаты собственных исследований по данному направлению. Предлагается два метода интеграции биометрической и электронной подписей на основе динамических параметров подписи, а также параметров лица и клавиатурного почерка.

Ключевые слова: *искусственные нейронные сети, биометрия, электронная подпись, распознавание образов.*

Lozhnikov P. S.

INTEGRATION OF BIOMETRIC AND ELECTRONIC SIGNATURES USING NEURAL NETWORK ALGORITHMS

The article provides arguments on the possibility of using modern pattern recognition methods in biometric authentication tasks: fuzzy extractors, artificial multilayer neural networks, "deep learning" methods, as well as convolutional, evolutionary, shallow, wide, hybrid neural networks. The results of our research in this area are given. Two methods of biometric and electronic signatures integration are proposed based on dynamic parameters of handwritten signature, as well as parameters of the face and keyboard handwriting.

Keywords: *artificial neural networks, biometrics, electronic signature, pattern recognition.*

Введение

Тенденции современного информационного общества связаны с переходом государств к цифровой экономике. Это приводит к тому, что целые сегменты документооборота (ДО) переносятся в цифровую среду: государственные услуги, банковское обслуживание, электронные закупки. Хотя документы создаются при помощи программного обеспечения, многие из них распространяются на бумажных носителях. Это связано с тем, что темпы повсеместного внедрения и освое-

ния современных технологий в организациях, а также развитие законодательства отстают от потенциальных возможностей, которые дают эти технологии. Поэтому в обозримом будущем во многих сферах деятельности документооборот будет смешанным, при этом электронные документы и транзакции будут превалировать.

В настоящей статье рассматривается решение проблемы интеграции биометрической и электронной подписей в среде гибридного документооборота [1]. Гибридный документ может находиться на электронном или бумажном носителе и содержать изображение автографа, защищенное с помощью электронной подписи (ЭП), а также тайных или открытых биометрических образов, благодаря чему можно быстро (за приемлемое время) проверить его целостность и аутентичность независимо от формы представления (бумажный или электронный). Ключевым атрибутом гибридного документа является ЭП, при формировании которой используется биометрический образ субъекта. При этом применяются нейросетевые алгоритмы преобразования биометрических признаков в секретный ключ ЭП. Для формирования ЭП из биометрических данных предложен гибридный преобразователь биометрия-код, способный преобразовывать вектор нечетких, неоднозначных биометрических параметров пользователя в четкий однозначный код ключа (пароля).

В качестве биометрических образов предлагается использовать так называемую биометрическую рукописную подпись (автограф) либо образ лица и параметры клавиатурного почерка субъекта при вводе им парольной фразы. Основной акцент делается на динамические биометрические образы человека, изменяющиеся с течением жизни.

1. Динамические биометрические образы

Предлагается два варианта реализации технологии генерации секретных ключей ЭП на основе биометрических образов:

1. Первый вариант подразумевает использование в качестве биометрического образа рукописную подпись. В данном случае формирование ЭП из биометрической рукописной подписи не повлияет существенным образом на имеющиеся бизнес-процессы в организации, т.к. подпись является привычным способом подтверждения аутентичности бумажных документов.

2. Второй предлагаемый метод формирования ЭП заключается в использовании для выработки секретного ключа данных от стандартного оборудования: клавиатуры и вебкамеры. В этом случае задействуются параметры лица и клавиатурного почерка субъекта. На базе данного метода также предлагается «расширенная» технология защиты для электронных реализаций документов, которая заключается в следующем. После формирования гибридного документа его владелец может ограничить доступ других лиц к произвольным его частям, а также запретить определенные действия (печать, редактирование и т.д.). При этом содержание каждой из этих частей документа будет зашифровано на открытом ключе того субъекта, которому предоставляется доступ. Если к одной из частей документа имеют доступ более одного субъекта, создается несколько копий этой части, каждая из которых шифруется на соответствующем открытом ключе. При работе пользователя с электронной реализацией гибридного документа производится непрерывный мониторинг в реальном времени параметров его лица и клавиатурного почерка. Эти параметры используются для генерации закрытого ключа, применяемого в дальнейшем для расшифровки соответствующих частей документа (рис. 1). При фиксации изменений биометрических характеристик субъекта, регистрируемых в процессе работы, документ временно «изменяет» либо «скрывает» свое содержимое целиком или полностью, блокирует часть функций по его редактированию. Пользователь не сможет пойти «в обход» системы гибридного документооборота, т.к. вся конфиденциальная информация зашифрована на соответствующих криптографических ключах. Общедоступная для всех субъектов информация не шифруется. Такая техника активной защиты получила название технологии «живого документа».

Для повышения надежности генерации ключа можно использовать многофакторный метод, сочетающих оба предложенных варианта.

1.1. Параметры рукописной подписи

В компьютерном представлении подпись может состоять из функций положения пера на планшете $x(t)$, $y(t)$ и давления пера на планшет $p(t)$, где t – это время в дискретной форме. Каждый рукописный образ подвергается спектральному и корреляционному анализу с целью вычисления фиксированного коли-

чества информативных признаков. Данный вектор состоит как из величин, характеризующих внешний вид образа (расстояния между определенными точками изображения подписи, параметры ее наклона, ширины, длины), так и динамику его воспроизведения (амплитуды гармоник функций *x(t), y(t), p(t)*, соответствующих частоте колебания руки подписанта (около 1-10 Гц), коэффициенты корреляции между этими и производными функциями, коэффициенты вейвлет-преобразования Добеши D6). Подробнее процесс вычисления данных признаков описан в работе [2].

1.2. Параметры лица и клавиатурного почерка субъектов

В качестве параметров лица использовались некоторые характеристики из работ [3] и [4], в частности:

– Расстояния между глазами, центром лица, кончиком носа (в пикселях, значения нормировались по диагонали лица в кадре).

– Площади глаз, носа, рта (значения нормировались по площади лица).

– Коэффициенты корреляции яркости и цветовых составляющих пикселей (в соответствии с моделью RGB) между всеми парами следующих областей лица: глаза, нос, рот. Данные признаки характеризуют асимметрию лица.

– Параметры, характеризующие цвет глаз и кожи.

В качестве признаков клавиатурного почерка использовались времена удержания и паузы между нажатием клавиш.

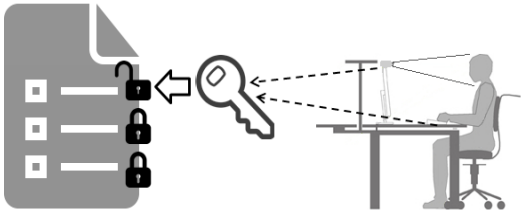

Рис. 1. Иллюстрация процесса получения доступа к фрагменту электронной реализации гибридного документа

2. Методы и технологии формирования секретного ключа электронной подписи из биометрических данных субъекта

Нечеткий экстрактор (fuzzy extractor) базируется на применении кодов, исправляющих ошибки. Криптографический ключ кодируется помехоустойчивым кодом, далее закодированная последовательность бит объединяется с биометрическими характеристиками субъекта, которые вычисляются по данным обучающей выборки. На выходе получается «открытая строка». В процессе аутентификации субъект повторно предъявляет биометрические данные, которые складываются с «открытой строкой» с помощью операции XOR. В результате высвобождается ключ, неверные биты которого корректируются. К фундаментальным недостаткам нечетких экстракторов относятся [1]:

1. Все классические коды вносят избыточность. Чем больше исправляющая способность кода, тем больше избыточности и меньше длина генерируемого ключа-пароля. В нечетком экстракторе длина ключа жестко зависит от исправляющей способности кода.

2. Классические коды не могут исправить большое количество ошибок, поэтому их невозможно использовать вместе с малоинформативными или коррелированными биометрическими параметрами (признаками).

3. Нечеткие экстракторы квантуют «сырые» (необработанные, необогащенные) биометрические данные и не учитывают параметры распределения значений признаков, в результате они должны давать более высокую долю ошибок по сравнению с нейросетевыми преобразователями биометрия-код, которые в свою очередь располагают этими данными, кодируя их весовыми коэффициентами нейронов.

Применение данного подхода по отношению к динамическим биометрическим образам не дало высоких результатов [5, 6].

Искусственные нейронные сети (ИНС) состоят из взаимосвязанных вычислительных элементов (нейронов), способных к обучению, приводящему к уличению качества решения задачи. Классические ИНС кодируют данные об особенностях признаков весовыми коэффициентами синапсов нейронов. Особое внимание в настоящее время уделяется технологиям «глубокого обучения». Популяризация данного направления поддерживается крупными организациями (NVIDIA Corporation, Intel Corporation, Google, Inc., Microsoft Corporation). На сегодняшний день под «глубоким» обучением обычно подразумевается итерационная настройка многослойных нейронных сетей прямого распространения, при которой в том или ином виде используется алгоритм «обратного распространения ошибки». Он имеет 2 типа реализации: пакетного или стохастического гради-

ентного спуска (во втором случае используются методы оптимизации ИНС) [7]. Предпринимаются попытки применения методов глубокого обучения для аутентификации субъектов по динамическим биометрическим характеристикам [8]. Однако использовать эти техники в реальной практике пока затруднительно, так как для достижения приемлемых показателей требуется значительный объем обучающей выборки (сотни примеров биометрического образа и более).

Помимо больших многослойных ИНС активные исследования ведутся в области, так называемых *малых сетей* (shallow networks). Эти ИНС способны к универсальной аппроксимации, но для этого требуется потенциально неограниченное число скрытых нейронов, которое играет роль сложности модели ИНС и является критическим фактором для практической реализации. Известен ряд работ, в которых выполнялась оценка ограничений малых ИНС и сформулирован ряд теорем [9]. Получены нижние оценки сложности неглубоких сетей в зависимости от соотношения между областью значений аппроксимируемой функции и размерностью входа [10]. Попытки создания процедур автоматической оценки минимально необходимого числа нейронов на основании данных обучающей выборки предпринимались и ранее. В [11] дана эмпирическая связь между числом примеров обучающей выборки и размером сети с целью определения верхнего порога числа нейронов скрытого слоя. Эти результаты являются важными для развития методов биометрической аутентификации, так как имеют отношение к обоснованию сложности ИНС в зависимости от ограничений на объем обучающей выборки. Малые сети могут обучаться на гораздо меньшем числе примеров.

Нейронные сети, в которых реализовано изменение весовых коэффициентов и топологии с помощью эволюционных алгоритмов, относятся к группе сетей TWEANNs (Topology & Weight Evolving Artificial Neural Networks). Данная стратегия построения и обучения ИНС относится к категории методов обучения с подкреплением и нашла применение в условиях, когда выполнить обучение с учителем практически невозможно. Эволюционная аугментация нейросетевой топологии (NeuroEvolution of Augmenting Topologies, NEAT) использует генетические алгоритмы для адаптации, как топологии, так и весов ИНС. Метод использует вариацию параметрической мутации, которая основана на эволюционных стратегиях и эволюционном программировании. Эволюция начинается с ИНС без скрытых нейронов и идет в направлении усложнения структуры. Такой подход находит применение в долго функционирующих и постоянно обучающихся ИНС на больших объемах данных (системы автопилотов автомобилей, обнаружения препятствий и др.) [12].

На сегодняшний день при сравнительно небольших обучающих выборках эволюционный подход успешно применяется для подбора топологий и весов в ИНС с одним скрытым слоем. Только с 2014 года доступность аппаратных ресурсов позволила применить нейроэволюцию к глубоким и сверточным нейронным сетям, но уже на очень больших выборках [13]. Эволюционный подход может быть положен в основу механизмов, позволяющих менять параметры ИНС пропорционально изменениям динамического биометрического образа пользователя со временем и в зависимости от его состояния.

В некотором смысле аналогом «малых» ИНС являются так называемые *«широкие» нейросети*. Эти ИНС представляют собой персептроны, которые состоят из большого количества нейронов, но малого числа слоев (один или два) и имеют принципиальные отличия от shallow networks. Главное отличие состоит в том, что для обучения «широких» ИНС не используется принцип «обратного распространения ошибки». Не итерационный и абсолютно устойчивый алгоритм обучения «широких» ИНС впервые предложен в России несколько лет назад для решения задач биометрической аутентификации [14]. Позже он лег в основу серии стандартов ГОСТ Р 52633. Обучение выполняется послойно, каждый нейрон обучается независимо от остальных нейронов сети, исходя из параметров закона распределения признаков, вычисляемых по данным обучающей выборки. Чтобы настроить автомат на распознавание определенного субъекта достаточно 20 примеров его образа. Высокая скорость работы позволяет реализовать данные алгоритмы на низкопроизводительном вычислительном устройстве.

В рамках теории «широких» ИНС стали применяться процедуры оценки информативности признаков (через площади пересечения функций плотностей вероятности) [15]. Впервые предложено создавать синапсы с учетом информативности признаков, а коли-

чество входов нейрона устанавливать, исходя из общей информативности признаков [16]. Это требование является логичным и позволяет обосновать выбор многих параметров ИНС. Теория «широких» ИНС имеет много общего с методами математической статистики и теории вероятностей. Комплексирование разных математических аппаратов позволило сдвинуться «с мертвой точки» в вопросах биометрической аутентификации.

«Широкие» нейронные сети могут быть настроены на генерацию фиксированной битовой последовательности при поступлении на вход образа, принадлежащего определенному классу, и случайной равномерно распределенной последовательности бит («белого» шума) при поступлении на вход неизвестного образа. Таким образом, данные сети могут быть использованы для интеграции биометрической и электронной подписей.

3. Гибридный подход к построению преобразователей биометрия-код, генерирующего секретный ключ электронной подписи

Активное развитие «широких» ИНС произошло в последние годы главным образом по пути гибридных нейросетевых алгоритмов. После отказа от «обратного распространения ошибки» появилась возможность менять не только активационную функцию нейрона, но и его функционал (в персептроне всегда использовался функционал взвешенного суммирования). В частности, для более эффективной обработки слабо коррелирующих биометрических параметров подходят квадратичные формы (1). Последние исследования показали, что многие функционалы обрабатывают данные гораздо эффективнее сумматоров персептрона и способны работать с сильно коррелирующими признаками [17]. Также эти исследования показывают, что сильно коррелирующие признаки позволяют создавать специальные нейроны, эффективность которых значительно выше, чем нейронов, ориентированных на обработку независимых признаков [18]. Например, такие нейроны можно построить на базе разностного (2) или гиперболического (3) многомерного Байесовского функционала. Таким образом, корреляционная зависимость между признаками может быть воспринята нейросетью как особый вид информации об образе. Это обстоятельство кардинально меняет подход: от малоинформативных и коррелированных признаков не нужно избавляться, они должны обрабатываться отдельными видами нейронов. Гибридные «широкие» ИНС имеют общие черты с сетями радиально-базисных функций, но являются более гибкими. Они могут состоять из нескольких слоев, формируемых из различных типов нейронов и иметь перекрестные связи.

$$\ddot{I} = \sqrt{\sum_{j=1}^{N} \frac{(m_j - a_j)^2}{\sigma_j^2}}, \quad (1)$$

где a_i – значение i-го биометрического параметра (входа нейрона), m_i и σ_i – математическое ожидание и среднеквадратичное отклонение i-ого признака (для образа «Свой»), соответственно, n – размерность функционала (число признаков, входов нейрона).

$$d_t = \sum_{j=1}^{N} \left| \frac{|m_t - a_t|}{\sigma_t} - \frac{|m_j - a_j|}{\sigma_j} \right|, \; j \neq t \quad (2)$$

$$g_{t-} = \sum_{j=1}^{N} \left(\frac{(m_t - a_t)^2}{\sigma_t^2} - \frac{(m_j - a_j)^2}{\sigma_j^2} \right), j \neq t, \quad (3)$$

где a_j – значение i-го параметра (входа нейрона) с высоким значением модуля корреляции $|ri,t|$ по отношению к t-му биометрическому признаку. То есть таблицы входных связей функционала Байеса должна формироваться таким образом, что бы обогащаемые им параметры были как можно сильнее коррелированны между собой.

После обогащения входных данных нейрона расчетное значение функционала поступает в функцию активации. В простейшем случае функция активации является пороговой. Именно такой случай рассматривается в рамках настоящей статьи.

Рассматриваемые гибридные ИНС ориентированы на распознавание образов при высокой размерности пространства признаков и наличии ограничений на объем обучающей выборки. Построение и обучение этих сетей детерминировано, при этом коррелированность биометрических параметров определяется только на основании малой обучающей выборки, а сами параметры определены заранее. Обучение «широкой» нейросети является послойным, т.е. каждый последующий слой обучается на выходных значениях нейронов предыдущего слоя, воспринимая их как значения признаков. Можно сказать, что каждый слой «широкой» сети состоит из нескольких подсетей, настройка нейронов каждой из которых имеет свою специфику.

При реализации преобразователя биометрия-код на практике важно позабо-

титься о том, чтобы биометрический образ и ключ пользователя не были скомпрометированы. Сегмент сети, представляющий собой персептрон, можно считать достаточно защищенным от этой угрозы [19]. Из весов нейронов нельзя за приемлемое время извлечь данные обучающей выборки и воссоздать эталон биометрического образа, как и извлечь личный ключ пользователя (это является вычислительно сложной и плохо формализуемой задачей). Однако квадратичные формы и Байесовские функционалы оперируют непосредственно параметрами законов распределения признаков, что ведет к необходимости хранения данных параметров. Если сервер, на котором хранится таблица нейросетевых функционалов, не является доверенным, то существует угроза восстановления фрагментов ключа и эталона биометрического образа пользователя по данным таблицы нейросетевых функционалов. В этом случае для защиты биометрического эталона на этапе хранения может быть применен механизм защищенного нейросетевого контейнера [19]. Данный механизм заключается в том, что параметры нейронов гибридной сети шифруются на выходах нейронов персептрона. При верной выдаче фрагмента ключа нейронами персептрона, параметры других нейронов будут расшифрованы. В противном случае, сеть сгенерирует шум, т.к. расшифрованные значения весовых коэффициентов не будут соответствовать эталону субъекта.

Корректирующие коды из работы [20] позволяют безопасно хранить синдромы ошибок и не дают возможности восстановить ключ без предъявления биометрического образа, достаточно близкого к аутентичному. В сочетании с механизмом защищенного нейросетевого контейнера [19] эти помехоустойчивые коды [20] решают проблему безопасного хранения таблицы нейросетевых функционалов. Однако открытым остается вопрос влияния механизма защищенного нейросетевого контейнера на вероятность ошибочных решений, принимаемых «широкой» нейронной сетью.

В работе [21] предлагается следующая модель гибридной сети, представленная на рисунке 2. Для каждого субъекта по данным его обучающей выборки формируется и обучается отдельная нейронная сеть. Каждая сеть способна генерировать ключ электронной подписи длиной до 2048 бит.

Надежность биометрической системы аутентификации (идентификации) определяется следующими показателями. Вероятность ошибки 2-ого рода («пропуска чужого», False Acceptance Rate, FAR) должна быть как можно ниже. При этом вероятность шибки 1-ого рода («ложный отказ в допуске своему», False Rejection Rate, FRR) должна быть приемлемой, т.к. частые отказы создают неудобства. FAR и FRR также возникают при генерации неверного ключа (при FAR=FRR говорят о Equal Error Rate, EER).

В настоящей работе нейросетевой преобразователь биометрия-код с указанной архи-

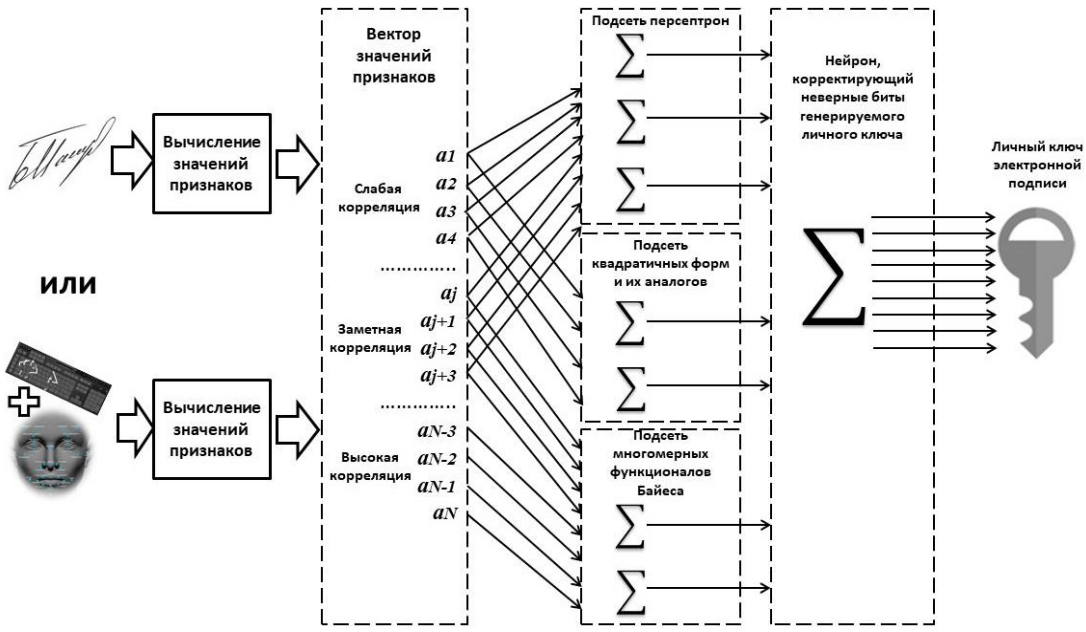

Рис. 2. Схема работы преобразователя биометрия-код на базе гибридных нейронных сетей

тектурой был реализован в виде программного комплекса с интерфейсами ввода подписей (рукописных паролей), лица и клавиатурного почерка (с использованием графического планшета, веб-камеры и клавиатуры). С использованием биометрических данных собранных в рамках исследования [21] гибридные сети (рис. 2) были перенастроены индивидуально под каждого субъекта. Далее были привлечены те же 90 испытуемых, что и в работе [21], которые многократно прошли процедуру биометрической идентификации (данные предъявлялись сразу всем нейросетевым преобразователям). Далее проводилась проверка корректности ключей, генерируемых с помощью 90 гибридных сетей (ключ должен быть корректен только в одном из 90 случаев). В результате достигнуты следующие вероятности ошибочных решений:

– при распознавании субъекта/генерации ключа по рукописным образам: FRR=18% при FAR<0,01% (EER=3,5%);

– при распознавании субъекта/генерации ключа по клавиатурному почерку и лицу: FRR=6,8% при FAR<0,01% (EER=1,7%);

– при распознавании субъекта/генерации ключа по рукописным образам, клавиатурному почерку и лицу: FRR=2,5% при FAR<0,01% (EER=0,9%).

При проведении эксперимента не применялся механизм защищенного нейросетевого контейнера, однако были учтены изменения динамического биометрического образа субъекта со временем (обучение преобразователя биометрия-код и его тестирование проводилось в различные дни с перерывом от одной до нескольких недель). В общей сложности совершено порядка 4500 попыток прохождения процедуры идентификации и последующей аутентификации.

Заключение

В рамках работы проведено аналитическое исследование методов построения преобразователей биометрия-код, используемых для интеграции биометрической и электронной подписей в качестве основы биометрических систем аутентификации и систем электронной подписи с биометрической активацией: нечетких экстракторов, искусственных многослойных нейронных сетей, методов «глубокого обучения», а также сверточных, эволюционных, малых, «широких», гибридных нейронных сетей. Протестирована модель гибридной нейронной сети на базе персептрона, сетей квадратичных форм и многомерных разностных и гиперболических функционалов Байеса. Экспериментально подтверждена высокая эффективность применения модели для решения задачи по интеграции биометрической и электронной подписей.

Литература

1. Ложников П.С. Биометрическая защита гибридного документооборота: монография / Новосибирск: Изд-во СО РАН, 2017. — 130 с.

2. Lozhnikov P.S., Sulavko A.E., Eremenko A.V., Volkov D.A. Methods of Generating Key Sequences based on Parameters of Handwritten Passwords and Signatures // Information. – 2016. – №7(4). – P. 59; DOI: 10.3390/info7040059.

3. Васильев В.И., Ложников П.С., Сулавко А.Е., Жумажанова С.С. Оценка идентификационных возможностей биометрических признаков от стандартного периферийного оборудования // Вопросы защиты информации. – 2016. – №1. – С. 12-20.

4. Ложников П.С., Сулавко А.Е., Бурая Е.В., Писаренко В.Ю. Аутентификация пользователей компьютера на основе клавиатурного почерка и особенностей лица // Вопросы кибербезопасности. – 2017. – №3. – С. 24-34.

5. Lozhnikov P.S., Sulavko, A.E., Volkov D.A. Application of Noise Tolerant Code to Biometric Data to Verify the Authenticity of Transmitting Information / Control and Communications (SIBCON), 21-23 May 2015, Omsk, Russia. – P.1-3; DOI: 10.1109/SIBCON.2015.7147126.

6. Lozhnikov P.S., Sulavko A.E., Eremenko A.V., Buraya E.V. Methods of Generating Key Sequences Based on Keystroke Dynamics // X International IEEE Scientific and Technical Conference "Dynamics of Systems, Mechanisms and Machines" (Dynamics), 15-17 November, 2016, Omsk, Russia. – P. 1-5; DOI: 10.1109/Dynamics.2016.7819038.

7. Yasuoka Y., Shinomiya Y., Hoshino Y. Evaluation of Optimization Methods for Neural Network // Soft Computing and Intelligent Systems (SCIS) and 17th International Symposium on Advanced Intelligent Systems, 25-28 August 2016, Sapporo, Japan; DOI: 10.1109/SCIS-ISIS.2016.0032.

8. Hafemann L. G. et al. Writer-independent Feature Learning for Offline Signature Verification Using Deep Convolutional Neural Networks // 2016 International Joint Conference on Neural Networks (IJCNN), 24-29 July 2016. – P. 2576-2583; DOI: 10.1109/IJCNN.2016.7727521.

9. Kůrková V., Sanguineti M. Probabilistic Lower Bounds for Approximation by Shallow Perceptron Networks // Neural Networks. – 2017. – Vol. 91.– P. 34-41.

10. Kůrková V., Sanguineti M. Model Complexities of Shallow Networks Representing Highly Varying Functions // Neurocomputing. – 2016. – Vol. 171. – P. 598-604.

11. Rogers L.L., Dowla F.U.: Optimization of Groundwater Remediation Using Artificial Neural Networks with Parallel Solute Transport Modeling //. Water Resources Research. – 1994. – Vol. 30(2). – P. 457–481.

12. Stanley K.O. Efficient Evolution of Neural Networks Through Complexification. PhD Thesis. Department of Computer Sciences, The University of Texas at Austin, 2004.

13. Koutn´ık J., Schmidhuber J., Gomez F. Evolving Deep Unsupervised Convolutional Networks for Vision-Based Reinforcement Learning // 2014 Annual Conference on Genetic and Evolutionary Computation. – 2014. – P. 541–548.

14. Волчихин В.И., Иванов А.И., Фунтиков В.А. Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации. Монография. Пенза: Изд-во Пензенского государственного университета. – 2005. – С. 273.

15. Sulavko A.E., Fedotov A.A., Eremenko A.V. Users' Identification through Keystroke Dynamics Based on Vibration Parameters and Keyboard Pressure // XI International IEEE Scientific and Technical Conference "Dynamics of Systems, Mechanisms and Machines" (Dynamics), 14-16 November, 2017, Omsk, Russia. – P. 1-7.

16. Иванов А.И. Многомерная нейросетевая обработка биометрических данных с программным воспроизведением эффектов квантовой суперпозиции. Пенза: Изд-во ПНИЭИ. – 2016. – С. 133.

17. Иванов А.И., Ложников П.С., Сулавко А.Е. Оценка надежности верификации автографа на основе искусственных нейронных сетей, сетей многомерных функционалов Байеса и сетей квадратичных форм // Компьютерная оптика. – 2017. – Т. 41. – №5. – С.765-774; DOI: 10.18287/2412-6179-2017-41-5-765-774.

18. Ivanov A.I., Lozhnikov P.S., Vyatchanin S.E. Comparable Estimation of Network Power for Chisquared Pearson Functional Networks and Bayes Hyperbolic Functional Networks while Processing Biometric Data / Control and Communications (SIBCON), 29-30 June 2017, Astana, Kazakhstan. – P.1-3; DOI: 10.1109/SIBCON.2017.7998435.

19. Ахметов Б.С., Иванов А.И., Фунтиков В.А., Безяев А.В., Малыгина Е.А. Технология использования больших нейронных сетей для преобразования нечетких биометрических данных в код ключа доступа: Монография. / Алматы: ТОО «Издательство LEM». – 2014. – С. 144.

20. Безяев А. В., Иванов А. И., Фунтикова Ю. В. Оптимизация структуры самокорректирующегося биокода, хранящего синдромы ошибок в виде фрагментов хэш-функций // Вестник УрФО. Безопасность в информационной сфере. – 2014. – № 3(13). – С. 4 -13.

21. Lozhnikov P.S., Sulavko A.E. Generation of a Biometrically Activated Digital Signature Based on Hybrid Neural Network Algorithms // Journal of Physics: Conf. Series. –2018. – № 1050; DOI: 10.1088/1742-6596/1050/1/012047.

References

1. Lozhnikov P.S. Biometricheskaya zashchita gibridnogo dokumentooborota: monografiya / Novosibirsk: Izd-vo SO RAN, 2017. — 130 s.

2. Lozhnikov P.S., Sulavko A.E., Eremenko A.V., Volkov D.A. Methods of Generating Key Sequences based on Parameters of Handwritten Passwords and Signatures // Information. – 2016. – №7(4). – P. 59; DOI: 10.3390/info7040059.

3. Vasil'yev V.I., Lozhnikov P.S., Sulavko A.Ye., Zhumazhanova S.S. Otsenka identifikatsionnykh vozmozhnostey biometricheskikh priznakov ot standartnogo periferiynogo oborudovaniya // Voprosy zashchity informatsii. – 2016. – №1. – S. 12-20.

4. Lozhnikov P.S., Sulavko A.Ye., Buraya Ye.V., Pisarenko V.YU. Autentifikatsiya pol'zovateley komp'yutera na osnove klaviaturnogo pocherka i osobennostey litsa // Voprosy kiberbezopasnosti. – 2017. – №3. – S. 24-34.

5. Lozhnikov P.S., Sulavko, A.E., Volkov D.A. Application of Noise Tolerant Code to Biometric Data to Verify the Authenticity of Transmitting Information / Control and Communications (SIBCON), 21-23 May 2015, Omsk, Russia. – P.1-3; DOI: 10.1109/SIBCON.2015.7147126.

6. Lozhnikov P.S., Sulavko A.E., Eremenko A.V., Buraya E.V. Methods of Generating Key Sequences Based on Keystroke Dynamics // X International IEEE Scientific and Technical Conference "Dynamics of Systems, Mechanisms and Machines" (Dynamics), 15-17 November, 2016, Omsk, Russia. – P. 1-5; DOI: 10.1109/Dynamics.2016.7819038.

7. Yasuoka Y., Shinomiya Y., Hoshino Y. Evaluation of Optimization Methods for Neural Network // Soft

Computing and Intelligent Systems (SCIS) and 17th International Symposium on Advanced Intelligent Systems, 25-28 August 2016, Sapporo, Japan; DOI: 10.1109/SCIS-ISIS.2016.0032.

8. Hafemann L. G. et al. Writer-independent Feature Learning for Offline Signature Verification Using Deep Convolutional Neural Networks // 2016 International Joint Conference on Neural Networks (IJCNN), 24-29 July 2016. – P. 2576-2583; DOI: 10.1109/IJCNN.2016.7727521.

9. Kůrková V., Sanguineti M. Probabilistic Lower Bounds for Approximation by Shallow Perceptron Networks // Neural Networks. – 2017. – Vol. 91.– P. 34-41.

10. Kůrková V., Sanguineti M. Model Complexities of Shallow Networks Representing Highly Varying Functions // Neurocomputing. – 2016. – Vol. 171. – P. 598-604.

11. Rogers L.L., Dowla F.U.: Optimization of Groundwater Remediation Using Artificial Neural Networks with Parallel Solute Transport Modeling //. Water Resources Research. – 1994. – Vol. 30(2). – P. 457–481.

12. Stanley K.O. Efficient Evolution of Neural Networks Through Complexification. PhD Thesis. Department of Computer Sciences, The University of Texas at Austin, 2004.

13. Koutn´ık J., Schmidhuber J., Gomez F. Evolving Deep Unsupervised Convolutional Networks for Vision-Based Reinforcement Learning // 2014 Annual Conference on Genetic and Evolutionary Computation. – 2014. – P. 541–548.

14. Volchikhin V.I., Ivanov A.I., Funtikov V.A. Bystryye algoritmy obucheniya neyrosetevykh mekhanizmov biometriko-kriptograficheskoy zashchity informatsii. Monografiya. Penza: Izd-vo Penzenskogo gosudarstvennogo universiteta. – 2005. – S. 273.

15. Sulavko A.E., Fedotov A.A., Eremenko A.V. Users' Identification through Keystroke Dynamics Based on Vibration Parameters and Keyboard Pressure // XI International IEEE Scientific and Technical Conference "Dynamics of Systems, Mechanisms and Machines" (Dynamics), 14-16 November, 2017, Omsk, Russia. – P. 1-7.

16. Ivanov A.I. Mnogomernaya neyrosetevaya obrabotka biometricheskikh dannykh s programmnym vosproizvedeniyem effektov kvantovoy superpozitsii. Penza: Izd-vo PNIEI. – 2016. – S. 133.

17. Ivanov A.I., Lozhnikov P.S., Sulavko A.Ye. Otsenka nadezhnosti verifikatsii avtografa na osnove iskusstvennykh neyronnykh setey, setey mnogomernykh funktsionalov Bayyesa i setey kvadratichnykh form // Komp'yuternaya optika. – 2017. – T. 41. – №5. – S.765-774; DOI: 10.18287/2412-6179-2017-41-5-765-774.

18. Ivanov A.I., Lozhnikov P.S., Vyatchanin S.E. Comparable Estimation of Network Power for Chisquared Pearson Functional Networks and Bayes Hyperbolic Functional Networks while Processing Biometric Data / Control and Communications (SIBCON), 29-30 June 2017, Astana, Kazakhstan. – P.1-3; DOI: 10.1109/SIBCON.2017.7998435.

19. Akhmetov B.S., Ivanov A.I., Funtikov V.A., Bezyayev A.V., Malygina Ye.A. Tekhnologiya ispol'zovaniya bol'shikh neyronnykh setey dlya preobrazovaniya nechetkikh biometricheskikh dannykh v kod klyucha dostupa: Monografiya. / Almaty: TOO «Izdatel'stvo LEM». – 2014. – S. 144.

20. Bezyayev A. V., Ivanov A. I., Funtikova YU. V. Optimizatsiya struktury samokorrektiruyushchegosya biokoda, khranyashchego sindromy oshibok v vide fragmentov khesh-funktsiy // Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. – 2014. – № 3(13). – S. 4 -13.

21. Lozhnikov P.S., Sulavko A.Ye. Generation of a Biometrically Activated Digital Signature Based on Hybrid Neural Network Algorithms // Journal of Physics: Conf. Series. –2018. – № 1050; DOI: 10.1088/1742-6596/1050/1/012047

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 16-07-01204.

ЛОЖНИКОВ Павел Сергеевич, заведующий кафедрой «Комплексная защита информации» Омского государственного технического университета, кандидат технических наук, доцент. 644050, г. Омск, проспект Мира, д. 11. E-mail: lozhnikov@gmail.com.

LOZHNIKOV Pavel Sergeevich, Head of the "Complex Information Protection" Department, Omsk State Technical University, PhD, associate professor. 644050, Omsk, Mira av., 11. E-mail: lozhnikov@gmail.com.