УДК 612.087.1:004.032.26:004.056.523 DOI: 10.18698/2541-8009-2023-5-892

ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ СИАМСКОЙ НЕЙРОННОЙ СЕТИ ДЛЯ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ ПО ПАЛЬЦЕВЫМ ВЕНАМ

А.Г. Десятов dag21um015@student.bmstu.ru
SPIN-код: 6389-6754

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Аннотация

Представлены теоретические основы сиамской нейронной сети и подробно рассмотрено ее построение для осуществления биометрической аутентификации по пальцевым венам. Проанализирован открытый набор данных пальцевых вен SDUMLA-HMT, с помощью которого были сформированы выборки обучающих и тестовых данных. В работе описана практическая реализация обучения сиамской нейронной сети на основе сформированных выборок. Для различных пороговых значений были подсчитаны вероятности ошибок I и II рода, которые являются ключевыми метриками для биометрической аутентификации. Результаты применения разработанной модели глубокого обучения проанализированы и представлены в виде графиков.

Ключевые слова

Биометрия, аутентификация, пальцевые вены, глубокое обучение, сиамская нейронная сеть, Conv2D, MaxPooling2D, Dropout, Dense, набор данных

Поступила в редакцию 27.03.2023

Введение.

Биометрическая аутентификация все чаще начинает использоваться для обеспечения безопасности защищаемой информации. Она основана на сравнении двух физиологических образцов, полученных с датчика, обычно после их обработки. Первый образец пользователь предоставляет при регистрации, второй образец принадлежит пользователю, который доказывает, что он тот самый, который предоставлял первый образец. Биометрическая аутентификация по венам является одной из самых стойких к компрометации. Для аутентификации по паролю необходимо сравнить две хеш-суммы, и только в случае их полного соответствия пользователю предоставляется доступ. В биометрической аутентификации почти невозможно добиться того, чтобы два биометрических образца совпали полностью. Система биометрической аутентификации разрабатывается так, что точное совпадение не требуется, однако эти образцы должны быть схожи по заданному пороговому значению.

Вены имеют преимущества перед другими физиологическими характеристиками. Например, образцы вен пальцев остаются неизменными в течение многих лет; обычно они не меняются совсем, т. е. пользователям не нужно повторно регистрироваться. Кроме того, рисунок вен невероятно сложно скопи-

ровать, поскольку они видны только при строго контролируемых условиях. При этом для сканирования вен пальцев не требуется специального оборудования. Например, существует уникальная программная технология биометрического сканирования рисунка вен пальцев VeinID Five Hitachi [1], которая позволяет считывать узоры вен с использованием камер ноутбуков и гаджетов, экономя затраты людей и организаций, поскольку в данном случае нет необходимости в применении специализированного оборудования для считывания. Также биометрия вен пальцев является гигиеничным методом, так как пользователю не нужно прикасаться к какой-либо поверхности.

Теоретические основы сиамской нейронной сети. В качестве модели глубокого обучения для биометрической аутентификации по пальцевым венам применяют сиамскую нейронную сеть. Сиамские нейронные сети достаточно мощные, они отвечают за сравнение входных данных разных подсетей между собой.

Известные модели глубокого обучения FaceNet, VGGFace служат примерами сиамских сетей [2]. Так как сиамские сети способны обучиться на малом количестве обучающих примеров, они являются очень эффективными. Использование сиамских нейронных сетей дает возможность использовать более продвинутые процедуры обучения, например, одноразовое обучение. Сиамские сети содержат несколько одинаковых подсетей (для биометрической аутентификации используется ровно две подсети).

На вход подсетям поступает по одному изображению. Сами подсети сиамской нейронной сети имеют не только одинаковую архитектуру, но и веса с параметрами. Обновления параметров и весов происходят одновременно и одинаково во всех подсетях. После конечных слоев подсетей можно вычислить, например, евклидово расстояние между их выходами. Это расстояние необходимо увеличивать, если на вход приходят отрицательные пары, и уменьшать, если на вход приходят положительные пары. Положительная пара состоит из двух изображений, принадлежащих одному классу, а отрицательная пара состоит из двух изображений, принадлежащих разным классам. С помощью функции потерь оценивают правильность принятия решения сиамской нейронной сети. Веса подсетей обновляются с помощью алгоритма обратного распространения.

Биометрическая аутентификация является задачей, которую сиамские нейронные сети способны решать лучше других моделей, например классификаторов. В случае классификаторов модель приходится обучать для каждого уникального человека, а в случае сиамской нейронной сети достаточно обучить модель так, чтобы она могла сравнивать входные данные разных подсетей и оценивать вероятность их принадлежности одному классу.

Еще одно преимущество сиамской нейронной сети заключается в следующем: не нужен специальный класс, в который относят все то, что не подходит

ни в один из известных классов. Сиамская сеть в таком случае просто выдает на выходе, что входные данные принадлежат разным классам [3].

Формирование выборок для обучения модели биометрической аутентификации. Для обучения нейронной сети, с помощью которой в дальнейшем будет осуществляться биометрическая аутентификация по пальцевым венам, необходимо сформировать обучающие выборки данных.

Обучающая выборка может быть получена с помощью открытого набора данных SDUMLA-HMT [4], который предоставляет исследовательская лаборатория MLA Университета Шаньдун. При формировании данного набора задействованы 106 человек, для каждого из которых были зарегистрированы по три пальца правой и левой руки, причем для каждого пальца было сделано шесть снимков. В цифровом виде эти снимки представлены изображениями размером 320×240 пикселей.

Структура набора данных представляет собой вложенные директории и снимки в самой глубокой директории. Например, название файла “Finger Vein Database/001/left/index_2.bmp” означает, что этот файл является вторым снимком вен указательного пальца (он называется index_2) левой руки (лежит в директории left) первого из 106 человек (поскольку left лежит в директории 001). Кроме снимков вен указательного пальца набор содержит снимки вен среднего (middle) и безымянного (ring) пальцев.

Изначально все изображения имеют размер 320×240 пикселей, а каждый пиксель представлен тремя числами, соответствующими красной, зеленой и синей составляющим. С помощью библиотеки PIL языка программирования Python изображения конвертируются в черно-белые снимки, после чего каждый пиксель снимков представляет собой одно число — оттенок серого цвета, это число лежит в диапазоне от 0 до 255. Все эти числа делятся на 255. На вход подсетям сиамской нейронной сети поступает матрица, составленная числами из диапазона от 0 до 1. Кроме того, изображения сжимаются до размеров 128×128 пикселей.

Для сиамской нейронной сети имеются фундаментальные требования при ее реализации. Сиамская нейронная сеть состоит из нескольких базовых подсетей, каждая из которых принимает входные данные. Для биометрической аутентификации достаточно двух подсетей, поэтому необходимо подготовить данные таким образом, чтобы на вход сиамская нейронная сеть принимала два изображения: по одному изображению на вход каждой подсети, целевое значение сети должно быть равно единице, если изображения принадлежат одному классу, а в противоположном случае — нулю [5].

Необходимо подготовить положительные и отрицательные пары. С помощью этих пар генерируется обучающая выборка, чтобы модель могла изучать сходство изображений.

В коде программы сначала происходит получение всех объектов. Переменная objects является списком списков. Так как всего 106 пользователей, у каждо-

го из которых были сняты вены шести пальцев, то размер внешнего списка objects равен 636. Каждый внутренний список содержит шесть снимков вен одного пальца.

Таким образом, objects имеет размерность 636×6 снимков. Для создания положительных пар достаточно из каждого вложенного списка выбрать два случайных снимка, т. е. взять два изображения, принадлежащих одному классу.

Для создания отрицательных пар программа проходит в цикле по внешнему списку objects. На каждой итерации цикла из внутреннего списка случайно выбирается один снимок, затем в пару ему выбирается случайный снимок из другого случайного внутреннего списка, т. е. два изображения, принадлежащих разным классам.

Таким образом, всего генерируется 636 положительных и 636 отрицательных пар, то есть всего 1272 пары, которые объединяются в один список всех пар pairs. В соответствии с положительными и отрицательными парами создается список целевых значений labels, состоящий из нулей и единиц. Заданный *i*-й элемент списка labels равен единице, если снимки *i*-й пары в списке pairs принадлежат одному классу, т. е. это два различных снимка вен одного и того же пальца. Заданный *j*-й элемент списка labels равен нулю, если снимки *j*-й пары в списке pairs принадлежат разным классам.

Перед разделением выборки на обучающие и тестовые данные необходимо случайным образом перемешать пары. Для этого берется последовательность чисел, являющихся индексами списка pairs, и перемешивается. Затем получается новая последовательность пар и целевых значений, взятых в соответствии с перемешанной последовательностью индексов. Таким образом, перемешаны пары снимков с сохранением информации о том, положительной или отрицательной является каждая пара. Затем все пары разделяют на тренировочную и тестовую выборки. Тренировочная выборка состоит из 80 % пар, а тестовая выборка — из всех остальных пар [6].

Практическая реализация сиамской нейронной сети. В этой работе описаны построение и обучение сиамской нейронной сети, применяемой для биометрической аутентификации по пальцевым венам.

Сначала определяются параметры, которые будут использоваться в дальнейшем. Во-первых, это размер обработанных изображений (в коде программы размер задается в переменной IMG_SHAPE), что будет соответствовать размеру входных данных в подсети сиамской нейронной сети. Затем задается число тренировочных объектов (BATCH_SIZE), представленных в одной партии, и число эпох обучения (EPOCHS). В данной работе IMG_SHAPE = (128, 128), BATCH_SIZE = 32, EPOCHS = 10.

Для начала необходимо реализовать базовую подсеть сиамской нейронной сети, которая представляет собой сверточную сеть с полносвязным слоем в кон-

це. Для этого используются слои библиотеки Keras: слой для входных данных Input, сверточные слои Conv2D, субдискретизирующиие слои MaxPooling2D, слои прореживания Dropout и, наконец, полносвязный слой Dense [7].

Подсеть начинается со слоя Input, в котором указаны размеры входного изображения. Затем несколько раз в модели подсети используется последовательность слоев Conv2D, MaxPooling2D и Dropout.

В сверточном слое Conv2D указывается число фильтров (в данной работе во всех сверточных слоях используется 64 фильтра), размеры ядра (3×3 пикселей) и функция активации (Relu).

В слое понижения размерности MaxPooling2D указывается вертикальный и горизонтальный масштабы понижения. Когда этот параметр равен 2, размеры уменьшатся наполовину.

Слой прореживания Dropout необходим для борьбы с переобучением нейронной сети. Параметром слоя служит уровень отсева.

Подсеть завершается полносвязным слоем Dense, в котором указывается количество нейронов, равное числу выходов из подсети сиамской нейронной сети.

Модель подсети, состоящей из перечисленных выше слоев, строится с помощью функции, но, несмотря на то, что необходимо создать две одинаковые подсети, вызываться данная функция будет один раз. Это связано с тем, что в подсетях всегда должны оставаться одинаковые параметры и веса. Данная функция создаст и вернет один объект. Этот объект можно вызывать как функцию, которая в качестве параметра принимает входной слой. После вызова этого объекта дважды будут получены две подсети сиамской нейронной сети. Итак, хотя существуют две подсети, фактически они реализованы одним объектом.

Также необходимо реализовать функцию для вычисления расстояния, которая принимает на вход два вектора, которые служат выходами подсетей, и вычисляет это расстояние между ними. Функции нахождения суммы, квадратного корня, максимума, используемые при нахождении евклидова расстояния, также импортируются из Keras.

Возможность вычислять евклидово расстояние между выходами подсетей внутри самой сиамской архитектуры является важным моментом при ее построении [8].

Реализованная функция нахождения расстояния передается конструктору пользовательского слоя Lambda, на вход которому поступают выходы подсетей. Данный слой используется для встраивания произвольных функций Keras внутри модели.

Объект класса Lambda после создания вызывается с аргументом, являющимся списком созданных подсетей. Результат данного вызова идет в последний слой сиамской нейронной сети Dense, имеющий всего один нейрон и сигмоидную функцию активации.

Наконец, создается модель сиамской нейронной сети, конструктор которой принимает список входных слоев подсетей и последний полносвязный слой.

Модель компилируется с помощью метода compile, который принимает на вход функцию потерь (в работе определена своя функция потерь), оптимизатор и метрики. Затем модель обучается с помощью метода fit, который принимает тренировочный и валидационный набор, размер партии и число эпох.

После обучения модель сериализуется и записывается на диск, чтобы в дальнейшем ее можно было использовать [9]. Историю обучения можно применять для построения различных графиков. Например, на рис. 1 представлен график зависимостей точности (Accuracy) и ошибки (Loss) от номера эпохи обучения (Epoch) на тренировочном (train) и тестовом (val) наборах.

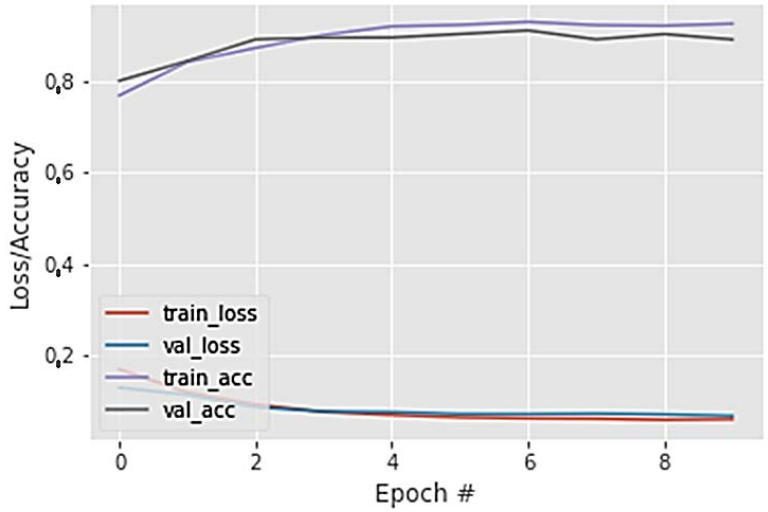

Рис. 1. Зависимости точности и ошибки от номера эпохи обучения

При расчете метрик качества на тренировочном наборе был получен график зависимости точности (Accuracy) от порога (Threshold), который является граничным значением определения сходства. Данный график представлен на рис. 2.

Оценить корректность обученной модели можно с помощью ошибок I и II рода. Ошибкой I рода является вероятность того, что обученная модель отнесет дескриптор зарегистрированного пользователя к классу нелегитимного пользователя. Ошибкой II рода является вероятность того, что обученная модель отнесет дескриптор нелегитимного пользователя к классу зарегистрированного пользователя.

Между ошибками I и II рода имеется связь. Чтобы уменьшить вероятность запрета доступа зарегистрированному пользователю (ошибку I рода), приходится увеличивать вероятность разрешения доступа нелегитимному пользователю (ошибку II рода). Ошибка первого рода заставляет легитимного пользователя

испытывать дискомфорт, однако ошибка второго рода является более важной для безопасности системы. В связи с этим необходимо найти оптимальное решение для обеих ошибок. Необходимо минимизировать ошибку II рода и наложить ограничения на ошибку первого рода в виде порогового значения [10]. График зависимости ошибок I (Error 1) и II (Error 2) рода обученной модели при различных пороговых значениях представлен на рис. 3.

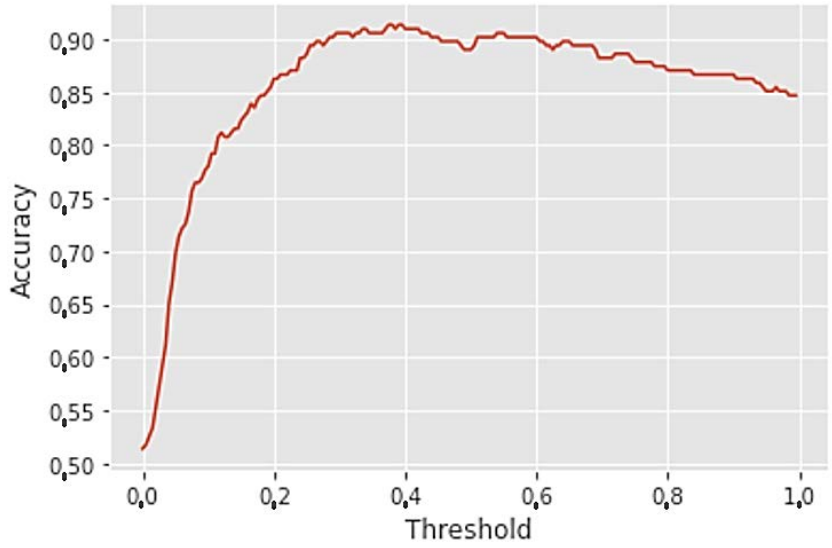

Рис. 2. Зависимость точности от порогового значения

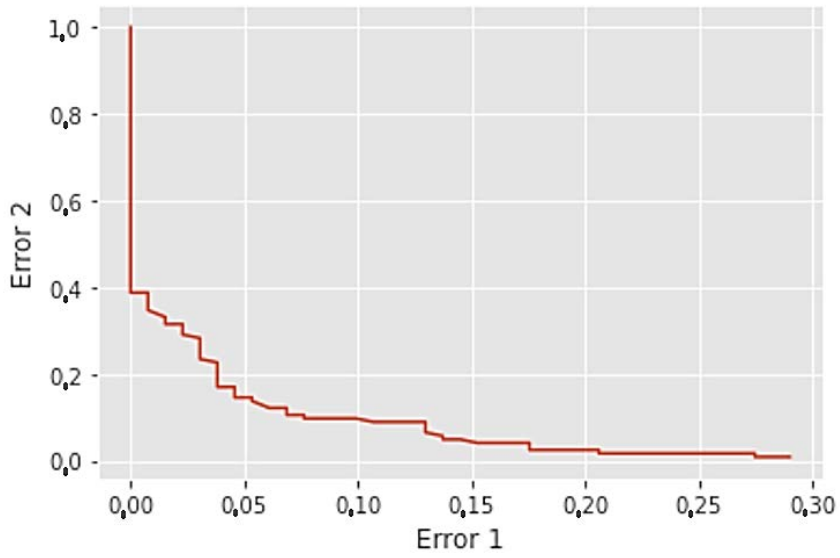

Рис. 3. Зависимость ошибок I и II рода при различных пороговых значениях

Заключение. В результате данной работы можно отметить положительные моменты. Например, при ошибке I рода, равной 0,099, ошибка II рода составляет 0,09 — это лучше, чем в опубликованных исследованиях [11] для вен левого указательного пальца.

Также стоит заметить, что при выполнении данной работы ресурсы были ограничены. В первую очередь, это касается вычислительной мощности и памяти используемых устройств. Например, размер изображений необходимо было уменьшать до применения первого сверточного слоя, чтобы не превысить ограничения оперативной памяти, при этом очевидно, что при сжатии изображений часть информации пропадала. На более быстрых вычислительных машинах также можно увеличить число эпох обучения, так как на рис. 1 заметно, что еще имеется потенциал роста точности.

Кроме того, улучшить данную модель можно следующими действиями:

– предварительно распознавать область интереса на изображениях;

– улучшить качество изображений, чтобы линии вен были видны более четко;

– использовать структуры и веса хорошо зарекомендовавших сверточных нейронных сетей;

– подобрать другие гиперпараметры, начальные веса, оптимизатор и функцию ошибок.

Литература

[1] *Introducing Hitachi's newest addition to the digital security portfolio, VeinID Five*. URL: https://digitalsecurity.hitachi.eu/products/veinid-five/ (accessed March 10, 2023).

[2] *(Group 3) Siamese Face Recognition*. URL: https://openpower.ucc.in.tum.de/group-3-siamese-face-recognition/ (accessed March 13, 2023).

[3] Li B., Yan J., Wu W., Zhu Z., Hu X. High Performance Visual Tracking with Siamese Region Proposal Network. *IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, Salt Lake City, UT, USA, IEEE, 2018. http://dx.doi.org/10.1109/CVPR.2018.00935

[4] *SDUMLA-HMT: A Multimodal Biometric Database*. URL: https://link.springer.com/chapter/10.1007/978-3-642-25449-9_33 (accessed March 17, 2023).

[5] *High Performance Visual Tracking with Siamese Region Proposal Network*. URL: http://openaccess.thecvf.com/content_cvpr_2018/papers/Li_High_Performance_Visual_CVPR_2018_paper.pdf (accessed March 15, 2023).

[6] *Building image pairs for Siamese networks with Python*. URL: https://pyimagesearch.com/2020/11/23/building-image-pairs-for-siamese-networks-with-python/ (accessed March 23, 2023).

[7] *Keras: библиотека глубокого обучение на Python*. URL: https://ru-keras.com/home/ (дата обращения 22.03.2023).

[8] *Подробное объяснение сиамской сети и сравнительной потери*. URL: https://russianblogs.com/article/74731636351/ (дата обращения 23.03.2023).

[9] *Training & evaluation with the built-in methods*. URL: https://keras.io/guides/training_with_built_in_methods/ (accessed March 23, 2023).
[10] Глущенко Н.А., Коннова Н.С. Нейросетевой подход к верификации рукописной подписи. *Политехнический молодежный журнал*, 2018, № 5. http://dx.doi.org/10.18698/2541-8009-2018-5-313
[11] Ling Jin. *Using Deep Learning for finger-vein based biometric authentication*. URL: https://towardsdatascience.com/using-deep-learning-for-finger-vein-based-biometric-authentication-3f6601635821 (accessed March 23, 2023).

Десятов Александр Геннадьевич — студент кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Ссылку на эту статью просим оформлять следующим образом:
Десятов А.Г. Практическая реализация сиамской нейронной сети для биометрической аутентификации по пальцевым венам. *Политехнический молодежный журнал*, 2023, № 05 (82). http://dx.doi.org/10.18698/2541-8009-2023-5-892

PRACTICAL IMPLEMENTATION OF THE SIAMESE NEURAL NETWORK IN BIOMETRIC PALMAR DIGITAL VEINS AUTHENTICATION

A.G. Desyatov dag21um015@student.bmstu.ru
SPIN-code: 6389-6754

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

The paper presents theoretical foundations of the Siamese neural network and considers its construction to implement the biometric palmar digital veins authentication in detail. The SDUMLA-HMT palmar digital veins open dataset was analyzed, which assisted in forming the samples of learning and test data. The paper describes practical implementation of learning a Siamese neural network based on the generated samples. For various thresholds, probabilities of type I and type II errors, which were the key metrics in biometric authentication, were calculated. Results of introducing the developed deep learning model were analyzed and are presented in the form of graphs.

Keywords

Biometrics, authentication, palmar digital veins, deep learning, Siamese neural network, Conv2D, MaxPooling2D, Dropout, Dense, dataset

Received 27.03.2023

References

[1] *Introducing Hitachi's newest addition to the digital security portfolio, VeinID Five*. URL: https://digitalsecurity.hitachi.eu/products/veinid-five/ (accessed March 10, 2023).

[2] *(Group 3) Siamese Face Recognition*. URL: https://openpower.ucc.in.tum.de/group-3-siamese-face-recognition/ (accessed March 13, 2023).

[3] Li B., Yan J., Wu W., Zhu Z., Hu X. High Performance Visual Tracking with Siamese Region Proposal Network. *IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, Salt Lake City, UT, USA, IEEE, 2018. http://dx.doi.org/10.1109/CVPR.2018.00935

[4] *SDUMLA-HMT: A Multimodal Biometric Database*. URL: https://link.springer.com/chapter/10.1007/978-3-642-25449-9_33 (accessed March 17, 2023).

[5] *High Performance Visual Tracking with Siamese Region Proposal Network*. URL: http://openaccess.thecvf.com/content_cvpr_2018/papers/Li_High_Performance_Visual_CVPR_2018_paper.pdf (accessed March 15, 2023).

[6] *Building image pairs for Siamese networks with Python*. URL: https://pyimagesearch.com/2020/11/23/building-image-pairs-for-siamese-networks-with-python/ (accessed March 23, 2023).

[7] *Keras: biblioteka glubokogo obuchenie na Python* [Keras: Python deep learning library]. URL: https://ru-keras.com/home/ (accessed March 22, 2023).

[8] *Podrobnoe ob"yasnenie siamskoy seti i sravnitel'noy poteri* [Detailed explanation of Siamese network and comparative loss].
URL: https://russianblogs.com/article/74731636351/ (accessed March 23, 2023).

[9] *Training & evaluation with the built-in methods*. URL: https://keras.io/guides/training_with_built_in_methods/ (accessed March 23, 2023).
[10] Glushchenko N.A., Konnova N.S. Neural network approach to verifying manual signature. *Politekhnicheskiy molodezhnyy zhurnal*, 2018, no. 5. (In Russ.). http://dx.doi.org/10.18698/2541-8009-2018-5-313
[11] Ling Jin. *Using Deep Learning for finger-vein based biometric authentication*. URL: https://towardsdatascience.com/using-deep-learning-for-finger-vein-based-biometric-authentication-3f6601635821 (accessed March 23, 2023).

Desyatov A.G. — Student, Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Please cite this article in English as:
Desyatov A.G. Practical implementation of the Siamese neural network in biometric palmar digital veins authentication. *Politekhnicheskiy molodezhnyy zhurnal*, 2023, no. 05 (82). (In Russ.). http://dx.doi.org/10.18698/2541-8009-2023-5-892