Чусов Андрей Александрович – ФГАОУ ВО Дальневосточный федеральный университет; e-mail: chusov.aa@dvfu.ru; г. Владивосток, Россия; тел.: +79147315896; доцент департамента электроники, телекоммуникации и приборостроения; к.т.н.

Копаева Маргарита Александровна – e-mail: rikopae@yandex.ru; тел.: +79502982261; магистрант департамента электроники, телекоммуникации и приборостроения.

Chusov Andrei Aleksandrovich – Far-Eastern Federal University, e-mail: chusov.aa@dvfu.ru; Vladivostok, Russia; phone: +79147315896; associate professor of the department of electronics, telecommunication and hardware development; cand. of eng. sc.

Kopaeva Margarita Aleksandrovna – e-mail: rikopae@yandex.ru; phone: +79502982261; graduate student at the department of electronics, telecommunication and hardware development.

УДК 004.89 DOI 10.18522/2311-3103-2022-4-192-200

В.А. Частикова, С.А. Жерлицын

НЕЙРОСЕТЕВАЯ МЕТОДИКА ИДЕНТИФИКАЦИИ ЛИЧНОСТИ ПО РИСУНКУ ВЕН ЛАДОНИ

Описывается работа по созданию нейросетевой методики идентификации личности, основанной на механизме сканирования и анализа рисунка вен ладони, как биометрического параметра. В рамках проведенного исследования описаны предпосылки, цели и причины, по которым разработка надежной системы биометрической идентификации является важным и актуальным направлением деятельности. Сформулирован ряд проблем, присущих существующим методам решения поставленной задачи: графовому методу и методу, основанному на вычислении расстояния, выраженного в различных интервальных метриках. Приведено описание принципов их работы. Сформулированы задачи, решаемые системами идентификации личности: сопоставление субъекта идентификации с его идентификатором, однозначно идентифицирующим этого субъекта в информационной системе. Описан механизм считывания рисунка вен с ладони, разработанный для анализа изображения, полученного с восприимчивой к излучению инфракрасного диапазона цифровой камеры. При нахождении в кадре ладони, подсвечиваемой светом ближнего ИК-диапазона, на изображении, полученном с камеры, становится заметен рисунок пролегающих под кожным покровом вен, сосудов и капилляров. В зависимости от организации, система идентификации может на основе предоставленного идентификатора определять соответствующий субъект доступа или проверять принадлежность того же идентификатора предполагаемому субъекту. Приведены 3 метода дальнейшего анализа биометрических данных и идентификации личности: подходы, основанные на категориальной классификации и бинарной классификации, а также комбинированный подход, при котором сначала используется идентификация по первому способу, а затем, по второму, но уже для известного идентификатора доступа, определённого на первом этапе. Приведена результирующая архитектура нейросети для категориальной классификации рисунка вен, описан способ вычисления количества параметров модели в зависимости от числа зарегистрированных субъектов. Представлены основные выводы и экспериментальные замеры точности работы системы при реализации различных методов, а также диаграммы изменения точности моделей во время обучения. Выявлены основные преимущества и недостатки приведённых методов.

Биометрическая идентификация личности; рисунок вен ладони; сверточная нейронная сеть; бинарная классификация; категориальная классификация; информационная безопасность.

V.A. Chastikova, S.A. Zherlitsyn

DEVELOPMENT OF A METHOD FOR PERSONAL IDENTIFICATION BASED ON THE PATTERN OF PALM VEINS

The article describes the work on the creation of a neural network method for identifying a person based on the mechanism of scanning and analyzing the pattern of palm veins as a biometric parameter. As part of the study, the prerequisites, goals and reasons for which the development of a reliable biometric identification system is an important and relevant area of activity are described. A number of problems are formulated that are inherent in existing methods for solving the problem: the graph method and the method based on calculating the distance expressed in various interval metrics. The description of the principles of their work is given. The tasks solved by personal identification systems are formulated: comparison of the subject of identification with its identifier, which uniquely identifies this subject in the information system. A mechanism for reading a pattern of veins from the palm of the hand, developed for analyzing an image obtained with a digital camera sensitive to infrared radiation, is described. When the palm is in the frame, illuminated by the light of the near infrared range, the image obtained from the camera becomes noticeable pattern of veins, vessels and capillaries that lie under the skin. Depending on the organization, the identification system may, based on the provided identifier, determine the appropriate access subject or verify that the same identifier belongs to the intended subject. Three methods for further analysis of biometric data and personal identification are given: approaches based on categorical classification and binary classification, as well as a combined approach, in which identification is first used by the first method, and then, by the second, but already for a known access identifier defined on the first stage. The resulting architecture of the neural network for the categorical classification of the vein pattern is presented, a method for calculating the number of model parameters depending on the number of registered subjects is described. The main conclusions and experimental measurements of the accuracy of the system when implementing various methods are presented, as well as diagrams of changes in the accuracy of models during training. The main advantages and disadvantages of the above methods are revealed.

Biometric personal identification; palm vein pattern; convolutional neural network; binary classification; categorical classification; information security.

Введение. У основных популярных факторов идентификации, таких как, например, ключи и парольная информация, несмотря на простоту и удобство их использования существуют недостатки, в числе которых возможность разглашения, подделки, подбора и утери. Использование биометрической информации минимизирует риск реализации ранее упомянутых угроз [1].

Механизм идентификации достаточно часто является критически важным компонентом системы, на его работу возлагается высокая ответственность. В числе последних тенденций развития механизмов аутентификации нельзя не выделить повышение спроса на методы, использующие биометрические характеристики субъекта [2, 3].

Целью данной работы является разработка методики идентификации личности по рисунку вен ладони на основе нейросетевого аппарата.

Актуальность. В условиях текущего уровня развития современных технологий информационные системы стали критически важными компонентами практически любого вида деятельности. Неограниченный доступ посторонних лиц к некоторым из них способен привести не только к колоссальным экономическим затратам, но в некоторых случаях и к катастрофам техногенного характера. Основным методом борьбы с такого вида угрозами является внедрение систем идентификации, а также контроля доступа [4].

Постановка задачи. На текущий момент набор применяемых для идентификации по рисунку вен ладони технологий базируется в наибольшей степени на двух основных методах: графовом и методе на основе вычисления расстояния (какой-либо интервальной метрики).

Графовый метод. Основан на сопоставлении топологии вен. Существует множество различных реализаций, однако обобщенный алгоритм состоит из следующих этапов:

- получение изображения ладони с венами;
- предварительная обработка по уменьшению шумов и выделению вен;
- построение линий, соответствующих выделенным венам;
- преобразование набора линий во взвешенный или обыкновенный граф;
- сравнение длин и весов соответствующих рёбер, углов между рёбрами в вершинах, топологического сходства.

Данный алгоритм при каждом выполнении процедуры идентификации вынужден обращаться к набору идентификационных образцов, что не позволяет изолировать систему идентификации от хранилища биометрических персональных данных.

Также минусом подобного подхода является необходимость сравнивать предоставленный образец с каждым из зарегистрированных в системе, что является крайне ресурсоёмким процессом при растущем количестве субъектов идентификации.

Среди прочих недостатков метода важно отметить следующие: крайне высокая зависимость от качества освещения, угла и изгиба ладони, зашумлённости изображения, фона, общая неустойчивость работы [5].

Метод на основе вычисления расстояния. Основан на вычислении расстояния между анализируемым и зарегистрированным изображениями по различным интервальным метрикам, таким как, косинусное расстояние, евклидово расстояние, и другие. Также в совокупности с рассматриваемым алгоритмом зачастую применяется масштабирование и поворот изображения. Такие меры повышают устойчивость работы алгоритма, однако кратно увеличивают его сложность и ресурсоёмкость. Таким образом, метод сохраняет основные минусы предыдущего – высокая вычислительная сложность при эксплуатации и невозможность разделения системы идентификации и хранилища биометрических персональных данных.

Реализация процесса идентификации на основе классификации при помощи нейронных сетей призвана компенсировать перечисленные выше недостатки существующих подходов.

Получение изображения. Задачей систем идентификации личности является сопоставление субъекта идентификации с его идентификатором, однозначно идентифицирующим этого субъекта в информационной системе. В зависимости от организации, система идентификации может на основе предоставленного идентификатора определять соответствующий субъект доступа или проверять принадлежность того же идентификатора предполагаемому субъекту [6].

Система идентификации личности по рисунку вен ладони анализирует изображение, полученное с восприимчивой к излучению инфракрасного диапазона цифровой камеры. При нахождении в кадре человеческой руки, а именно ладони, подсвечиваемой светом ближнего ИК-диапазона, на изображении, полученном с камеры, становится заметен рисунок пролегающих под кожным покровом вен, сосудов и капилляров.

Полученные таким образом изображения, тем не менее, сильно зависят от качества подсветки и не всегда обладают должной степенью контрастности, однако этот недостаток является устранимым при помощи автоматической постобработки. Пример получаемого изображения приведён на рис. 1.

Каждое изображение хранится в чёрно-белом формате, так как цветовые составляющие не несут полезной информации о рассматриваемых венах.

В данном исследовании предложено несколько вариантов реализации системы идентификации по рисунку вен ладони на основе нейросетевого анализа данных. В качестве математической основы системы выбрана свёрточная нейронная сеть с несколькими полносвязными слоями на выходе, так как именно такая комбинация моделей является наиболее распространённым способом обработки и классификации изображений.

Рис. 1. Пример необработанного снимка вен ладони

Категориальная классификация. Первый из них основан на категориальной классификации. Для прохождения идентификации производится проверка принадлежности предоставленного образца к конкретному классу из выборки [7].

Нейросеть при этом обучается сопоставлению каждого образца обучающей выборки соответствующему строго определённому заранее классу. Выходом нейросети в таком случае при предоставлении ей одного отдельно взятого образца будет являться вектор распределения вероятности принадлежности данного образца между всеми известными нейросети классами. Для минимизации количества ошибок второго рода также рационально ввести пороговое значение вероятности для идентификации личности [8]. Данное значение определяется эмпирически в ходе проведения экспериментов с заданным конкретным набором субъектов идентификации.

В рамках текущего исследования описанный подход был реализован на практике: собрана обучающая выборка, построена и обучена нейросетевая модель.

Для подхода, основанного на категориальной классификации, лучшее значение точности из серии экспериментов составило 0.9149. Графики изменения функций точности и потерь во время обучения для тестовой и валидационной подвыборок приведены на рис. 2.

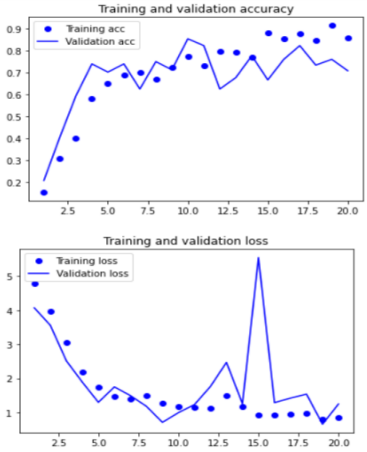

Рис. 2. Графики изменения функций точности и потерь во время обучения категориальной классификации

Результирующая нейросетевая архитектура для решения задачи категориальной классификации представлена в табл. 1. Значение n равно количеству субъектов, зарегистрированных в системе, и может варьироваться от 2 до 100 в протестированных конфигурациях, однако может быть изменено в большую сторону.

Таблица 1

Нейросетевая архитектура

Название слоя (тип слоя)	Размерность выходного вектора	Число параметров
conv2d_1 (входной слой)	(1274, 714, 64)	3200
max_pooling2d_1 (субдискретизирующий слой)	(637, 357, 64)	0
conv2d_2 (сверточный слой)	(635, 355, 128)	73856
max_pooling2d_2 (субдискретизирующий слой)	(317, 177, 128)	0
conv2d_3 (сверточный слой)	(315, 175, 128)	147584
max_pooling2d_3 (субдискретизирующий слой)	(157, 87, 128)	0
conv2d_4 (сверточный слой)	(155, 85, 128)	147584
max_pooling2d_4 (субдискретизирующий слой)	(77, 42, 128)	0
flatten_1 (линеаризующий слой)	(413952)	0
Dropout (прореживающий слой)	(413952)	0
Dense_1 (полносвязный слой)	64	26492992
Dense_2 (полносвязный слой)	n	65 * n

Бинарная классификация. Второй способ основан на принципе бинарной классификации. В данном случае задачей нейронной сети является анализ принадлежности предъявляемого идентификатора только лишь одному строго определённому субъекту. Выходом нейронной сети в данной ситуации являются два числа – вероятность соответствия и вероятность несоответствия. Для рассматриваемого способа также необходимо применение порогового значения для подтверждения соответствия [9].

В случае категориальной классификации в системе находится лишь одна единственная нейросеть, которая отвечает за проверку соответствия каждого субъекта доступа своей идентификационной записи. Для добавления нового пользователя в систему будет необходимо переобучение последних слоёв нейросети.

В случае бинарной классификации каждому субъекту доступа соответствует своя легковесная нейросеть, которая быстро обучается и проверяет корректность соответствия пользователя с идентификационной записью в системе. При этом пользователь либо должен указать на запрашиваемую идентификационную запись явным образом, либо использовать дополнительный фактор идентификации, либо система должна линейно провести проверку соответствия полученного изображе-

ния с каждой идентификационной записью. Все перечисленные варианты имеют свои плюсы и минусы и выбор итогового алгоритма зависит от способа применения механизма.

Описанный подход также был реализована на практике с использованием той же обучающей выборки и вычислительной базы.

Для подхода, основанного на бинарной классификации, точность достигала значения 0.9789. Графики изменения функций точности и потерь во время обучения для тестовой и валидационной подвыборок приведены на рис. 3.

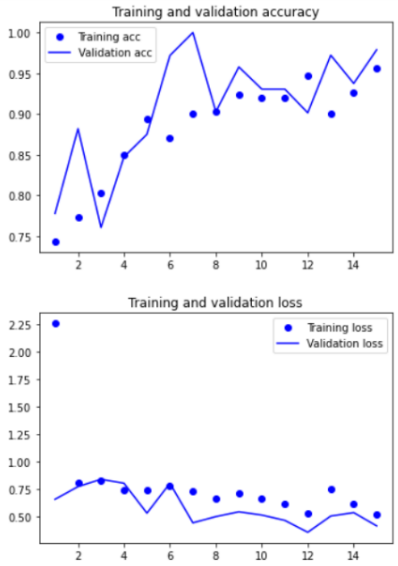

Рис. 3. Графики изменения функций точности и потерь во время обучения бинарной классификации

Комбинированный метод. Помимо вышеописанных возможен третий сценарий применения предложенных способов – комбинированный, двухэтапный. В целях повышения надёжности системы и сведения количества ошибок второго рода к возможному минимуму, используется идентификация по первому способу, а затем, по второму, но уже для известного идентификатора доступа, определённого на первом этапе [13].

Заключение. Представленная в первом способе, основанном на категориальной классификации, архитектура является наиболее ресурсоёмкой из всех используемых в каждой из реализаций методики, что позволяет дать верхнюю оценку вычислительной сложности системы в целом.

Таким образом, разработанная нейронная сеть содержит 12 слоев и от 26 865 346 до 26 871 716 параметров. Интервал количества параметров обусловлен допустимым количеством зарегистрированных субъектов – от 2-х до 100. Так как каждому субъекту соответствует свой выход нейросети, каждый дополнительный субъект добавит в модель 65 новых весов [17].

Применение многокатегориальной классификации с помощью нейросетей для распределения идентификаторов по зарегистрированным в системе пользователям превышает по вычислительной сложности одну проверку соответствия любым из классических методов, но является значительно менее ресурсоёмким [18], чем проверка соответствия с каждым из зарегистрированных субъектов, которая проводится в известных методиках.

Точность определения субъекта идентификации с применением бинарной классификации показывает лучшие результаты, по сравнению с многокатегориальной, однако в изначально описанной конфигурации проигрывает по требовательности к техническим характеристикам устройства-носителя. Предложенный комбинированный подход понижает требовательность к вычислительной мощности устройства и повышает конечную надежность системы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Частикова В.А., Жерлицын С А., Воля Я.И.* Нейросетевой метод идентификации личности по неформализованной семантической характеристике // Вестник УрФО. Безопасность в информационной сфере. – 2018. – № 4 (30). – С. 20-26. – DOI 10.14529/secur180403. – EDN YUNKCL.
2. *Частикова В.А., Жерлицын С.А., Воля Я.И., Сотников В.В.* Нейросетевая технология обнаружения аномального сетевого трафика // Прикаспийский журнал: управление и высокие технологии. – № 1 (49). – С. 20-32. – DOI 10.21672/2074-1707.2020.49.4.020-032. – EDN WUCDII.
3. *Jain A.K., Ross A. and Pankanti S.* Biometrics: a tool for information security // Trans Inform Forensics Secur. – No. 1 (2). – P. 125-143.
4. *Malatras A., Geneiatakis D. and Vakalis I.* On the efficiency of user identification: a system-based approach // Int. J. Inf. Secur. – No. 16. – P. 653-671.
5. *Im S., Park H., Kim Y, Han S., Kim S., Kang C., Chung C.* A Biometric identification system by extracting hand vein patterns // J Korean Phys Soc. – Vol. 28 (3). – P. 268-272.
6. *Sarkar A. and Singh B.K.* A review on performance, security and various biometric template protection schemes for biometric authentication systems // Multimed Tools Appl. – Vol. 79. – P. 27721-27776.
7. *Hancock J T and Khoshgoftaar T M* Survey on categorical data for neural networks // Journal of Big Data. – Vol. 7, No. 28.
8. *Chastikova V.A., Zherlitsyn S.A. and Y.I. Volya* Neural network method of identification by unformalized semantic characteristics // News of Volgograd State Technical University no. – Vol. 8 (218). – P. 63-67.
9. *Blokus A. and Krawczyk H.* Systematic approach to binary classification of images in video streams using shifting time windows // SIViP. – No. 13. – P. 341-348.
10. *Hassanat A.B., Albustanji A., Tarawneh A.S., Alrashidi M., Alharbi H., Alanazi M., Alghamdi M., Alkhazi I.S., & Prasath V.* Deep learning for identification and face, gender, expression recognition under constraints // ArXiv, abs/2111.01930, 2021.
11. *Soleymani S., Dabouei A., Taherkhani F., Iranmanesh S.M., Dawson J.M., & Nasrabadi* N.M., Quality-Aware Multimodal Biometric Recognition // ArXiv, abs/2112.05827, 2021.
12. *Mugalu B.W., Wamala R.C., Serugunda J., & Katumba A.* Face Recognition as a Method of Authentication in a Web-Based System // ArXiv, abs/2103.15144, 2021.
13. *Marattukalam F., Abdulla W.H., & Swain A.K*. 2021 N-shot Palm Vein Verification Using Siamese Networks // 2021 International Conference of the Biometrics Special Interest Group (BIOSIG). – P. 1-5.
14. *Meng Z., Altaf M.U., Juang B.* Active voice authentication // ArXiv, abs/2004.12071, 2020.
15. *Stragapede G., Vera-Rodríguez R., Tolosana R., Morales A., Acien A., & Lan G.L*. Mobile Behavioral Biometrics for Passive Authentication // ArXiv, abs/2203.07300, 2022.
16. *Fuksis R., Pudzs M., Greitans M.* Palm Vein Biometrics Based on Palm Infrared Imaging and Complex Matched Filtering // The 12th ACM Workshop on Multimedia and Security, Rome, 2009. – P. 27.
17. *Chastikova V. A., Zherlitsyn S. A., Volya Y.I*. Analysis of training of deep neural networks with heterogeneous architecture while detecting malicious network traffic // IOP Conference Series: Materials Science and Engineering, Krasnoyarsk, Russian Federation: IOP Publishing Ltd, 2021. – P. 12135. – DOI 10.1088/1757-899X/1047/1/012135.
18. *Частикова В.А., Титова А.А., Войлова Д.О*. Аналитический обзор методов идентификации личности на основе биометрических характеристик // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. – 2022. – № 1 (296). – P. 92-112.

19. *Промыслов В.Г., Семенков К.В., Менгазетдинов Н.Э.* Исследование методов аутентификации операторов в промышленных системах управления // Проблемы управления. – 2022. – № 3. – P. 40-54.
20. *Артамонов В.А., Артамонова Е.В*. Искусственный интеллект и безопасность: проблемы, заблуждения, реальность и будущее // Россия: тенденции и перспективы развития. – 2022. – № 17-1. – P. 585-594.

REFERENCES

1. *Chastikova V.A., Zherlitsyn S A., Volya Ya.I.* Neyrosetevoy metod identifikatsii lichnosti po neformalizovannoy semanticheskoy kharakteristike [Neural network method of identification by unformalized semantic characteristics*], Vestnik UrFO. Bezopasnost' v informatsionnoy sfere* [Urfu Journal. Security in the information sphere no], 2018, No. 4 (30), pp. 20-26. DOI 10.14529/secur180403. EDN YuNKCL.
2. *Chastikova V.A., Zherlitsyn S.A., Volya Ya.I., Sotnikov V.V.* Neyrosetevaya tekhnologiya obnaruzheniya anomal'nogo setevogo trafika [Neural network technology for detecting anomalous network traffic], *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian journal: Control and High Technologies], No. 1 (49), pp. 20-32. DOI 10.21672/2074-1707.2020.49.4.020-032. EDN WUCDII.
3. *Jain A.K., Ross A. and Pankanti S.* Biometrics: a tool for information security, *Trans Inform Forensics Secur,* No. 1 (2), pp. 125-143.
4. *Malatras A., Geneiatakis D. and Vakalis I.* On the efficiency of user identification: a system-based approach, *Int. J. Inf. Secur*., No. 16, pp. 653-671.
5. *Im S., Park H., Kim Y, Han S., Kim S., Kang C., Chung C.* A Biometric identification system by extracting hand vein patterns, *J Korean Phys Soc*., Vol. 28 (3), pp. 268-272.
6. *Sarkar A. and Singh B.K.* A review on performance, security and various biometric template protection schemes for biometric authentication systems, *Multimed Tools Appl*, Vol. 79, pp. 27721-27776.
7. *Hancock J T and Khoshgoftaar T M* Survey on categorical data for neural networks, *Journal of Big Data,* Vol. 7, No. 28.
8. *Chastikova V.A., Zherlitsyn S.A. and Y.I. Volya* Neural network method of identification by unformalized semantic characteristics, *News of Volgograd State Technical University no,* Vol. 8 (218), pp. 63-67.
9. *Blokus A. and Krawczyk H.* Systematic approach to binary classification of images in video streams using shifting time windows, *SIViP,* No. 13, pp. 341-348.
10. *Hassanat A.B., Albustanji A., Tarawneh A.S., Alrashidi M., Alharbi H., Alanazi M., Alghamdi M., Alkhazi I.S., & Prasath V.* Deep learning for identification and face, gender, expression recognition under constraints, *ArXiv, abs/2111.01930, 2021*.
11. *Soleymani S., Dabouei A., Taherkhani F., Iranmanesh S.M., Dawson J.M., & Nasrabadi* N.M., Quality-Aware Multimodal Biometric Recognition, *ArXiv, abs/2112.05827, 2021*.
12. *Mugalu B.W., Wamala R.C., Serugunda J., & Katumba A.* Face Recognition as a Method of Authentication in a Web-Based System, *ArXiv, abs/2103.15144, 2021*.
13. *Marattukalam F., Abdulla W.H., & Swain A.K*. 2021 N-shot Palm Vein Verification Using Siamese Networks, *2021 International Conference of the Biometrics Special Interest Group (BIOSIG),* pp. 1-5.
14. *Meng Z., Altaf M.U., Juang B.* Active voice authentication, *ArXiv, abs/2004.12071, 2020*.
15. *Stragapede G., Vera-Rodríguez R., Tolosana R., Morales A., Acien A., & Lan G.L*. Mobile Behavioral Biometrics for Passive Authentication, *ArXiv, abs/2203.07300, 2022*.
16. *Fuksis R., Pudzs M., Greitans M.* Palm Vein Biometrics Based on Palm Infrared Imaging and Complex Matched Filtering, *The 12th ACM Workshop on Multimedia and Security, Rome, 2009,* pp. 27.
17. *Chastikova V. A., Zherlitsyn S. A., Volya Y.I.* Analysis of training of deep neural networks with heterogeneous architecture while detecting malicious network traffic, *IOP Conference Series: Materials Science and Engineering, Krasnoyarsk, Russian Federation*: IOP Publishing Ltd, 2021, pp. 12135. DOI 10.1088/1757-899X/1047/1/012135.
18. *Chastikova V.A., Titova A.A., Voylova D.O*. Analiticheskiy obzor metodov identifikatsii lichnosti na osnove biometricheskikh kharakteristik [Analytical review of personal identification methods based on biometric characteristics], *Vestnik Adygeyskogo gosudarstvennogo universiteta. Seriya 4: Estestvenno-matematicheskie i tekhnicheskie nauki* [Bulletin of the Adyghe State University. Series 4: Natural-mathematical and technical sciences], 2022, No. 1 (296), pp. 92-112.

19. *Promyslov V.G., Semenkov K.V., Mengazetdinov N.E.* Issledovanie metodov autentifikatsii operatorov v promyshlennykh sistemakh upravleniya [Research of methods of authentication of operators in industrial control systems], *Problemy upravleniya* [Management Problems], 2022, No. 3, pp. 40-54.
20. *Artamonov V.A., Artamonova E.V.* Iskusstvennyy intellekt i bezopasnost': problemy, zabluzhdeniya, real'nost' i budushchee [Artificial intelligence and security: problems, delusions, reality and future], *Rossiya: tendentsii i perspektivy razvitiya* [Russia: trends and development prospects], 2022, No. 17-1, pp. 585-594.

Статью рекомендовал к опубликованию д.т.н. Л.А. Видовский.

Частикова Вера Аркадьевна – Кубанский государственный технологический университет; e-mail: chastikova_va@mail.ru; г. Краснодар, Россия; тел.: +79184635536; кафедра компьютерных технологий и информационной безопасности; к.т.н.; доцент.

Жерлицын Сергей Анатольевич – e-mail: kpytooooo@gmail.com; тел.: +79181965775; кафедра компьютерных технологий и информационной безопасности; аспирант.

Chastikova Vera Arkadyevna – Kuban State Technological University; e-mail: chastikova_va@mail.ru; Krasnodar, Russia; phone: +79184635536; the department of computer technologies and information security; cand. of eng. sc.; associate professor.

Zherlitsyn Sergey Anatolyevich – e-mail: kpytooooo@gmail.com; phone: +79181965775; the department of computer technologies and information security; graduate student.

УДК 004.021 DOI 10.18522/2311-3103-2022-4-200-212

К.Н. Алексеев, Д.А. Сорокин, А.Л. Леонтьев

МЕТОДИКА СОЗДАНИЯ ТОПОЛОГИЧЕСКИХ ОГРАНИЧЕНИЙ ПРИ ВЫСОКОЙ УТИЛИЗАЦИИ РЕСУРСОВ ПЛИС

Рассмотрена проблема достижения высокой реальной производительности реконфигурируемых вычислительных систем при решении вычислительно трудоёмких задач различных предметных областей. Величину реальной производительности реконфигурируемых систем определяют параметры выполняемых на них программ, основной компонентой которых являются вычислительные структуры обработки данных, реализованные в виде конфигурационных файлов ПЛИС. При этом одним из ключевых параметров любой вычислительной структуры является тактовая частота ее работы, которая непосредственно влияет на её производительность. Однако достижение высоких тактовых частот сопряжено с рядом проблем, которые современные средства САПР не решают. Причина кроется в неоптимальном топологическом размещении функциональных узлов вычислительной структуры на поле примитивов ПЛИС, особенно при высокой утилизации ресурсов. Это приводит к повышенной нагрузке на коммутационную матрицу ПЛИС и, как следствие, связи между примитивами ПЛИС, имеющими функциональную зависимость, оказываются значительно длиннее, чем это допустимо. Кроме того, излишняя длина связей наблюдается при трассировке соединений между примитивами, которые расположены на разных кремниевых кристаллах ПЛИС или же физически разделены встроенными периферийными устройствами. В настоящей статье описывается методика, которая позволяет рационализировать размещение элементов вычислительной структуры на поле примитивов ПЛИС, минимизировать длину трасс между примитивами, а также минимизировать число трасс между физически разделенными топологическими областями ПЛИС. Работоспособность предложенной методики показана на примере решения тестовой задачи «КИХ-фильтр» на реконфигурируемом компьютере «Терциус». Проиллюстрированы основные проблемы при достижении целевой тактовой частоты и описан способ их преодоления. Применение методики позволило увеличить тактовую частоту и тем самым поднять производительность «Терциус» на 25% без переработки функциональной схемы вычислительной структуры задачи. Текущие исследования