БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2021. – № 2 (101). – 154–165

УДК 004.056.53 DOI: 10.17212/2782-2230-2021-2-154-165

МОДЕЛЬ ПРЕОБРАЗОВАТЕЛЯ «БИОМЕТРИЯ-КОД» НА ОСНОВЕ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ АНАЛИЗА ТЕРМОГРАММ ЛИЦА СУБЪЕКТОВ*

П.С. ЛОЖНИКОВ[1], С.С. ЖУМАЖАНОВА[2]

[1] *644050, РФ, г. Омск, пр. Мира, 11, Омский государственный технический университет, д-р техн. наук, заведующий кафедрой комплексной защиты информации. E-mail: lozhnikov@mail.ru*

[2] *644050, РФ, г. Омск, пр. Мира, 11, Омский государственный технический университет, ассистент кафедры комплексной защиты информации. E-mail: samal_shumashanova@mail.ru*

Существующие алгоритмы асимметричного шифрования подразумевают хранение секретного закрытого ключа, авторизованный доступ к которым, как правило, осуществляется при предъявлении пароля. Пароли уязвимы перед методами социальной инженерии и подвержены «человеческому фактору».

Комбинирование биометрических методов защиты с криптографией рассматривается как возможное решение этой проблемы, но любая биометрическая криптосистема должна иметь возможность преодолевать небольшие различия, существующие между двумя разными реализациями одного и того же биометрического параметра. Особенно это актуально для динамической биометрии, когда различия могут быть вызваны изменением психофизиологического состояния субъекта. Решением этих вопросов является внедрение системы на базе преобразователя «биометрия-код», который настраивается на выдачу ключа пользователя при предъявлении его биометрического образа. Ключ при этом заранее генерируется в соответствии с принятыми нормами без использования биометрических образов. В настоящей работе предлагается использовать тепловизионные изображения пользователя для надежной биометрической аутентификации субъекта на основе нейросетевого преобразователя «биометрия-код». Тепловизионные изображения не так давно используются в качестве нового подхода в биометрических системах идентификации личности и являются особым видом биометрических образов, позволяющих решить вопрос как аутентификации субъекта, так и идентификации его психофизиологического состояния. Преимущества тепловидения заключаются в том, что эта технология в настоящее время становится доступной и мобильной. Это позволяет идентифицировать и аутентифицировать пользователя бесконтактным и непрерывным образом.

В настоящей работе проведен эксперимент по верификации образов термограмм 84 субъектов и получены следующие показатели ошибочных решений: EER = 0,85 % для пользователей в состоянии «норма».

* Статья получена 12 мая 2021 г.

Ключевые слова: преобразователь «биометрия-код», термограммы лица, искусственные нейронные сети, криптографический ключ, биометрическая аутентификация, психофизиологическое состояние, тепловизионные изображения, FRR, FAR

ВВЕДЕНИЕ

Биометрические данные обладают большим преимуществом – они уникальны для каждого человека, за счет этого повышают защищенность информационных ресурсов от несанкционированного доступа. Однако главный их недостаток заключается в том, что они неточны и изменяются от реализации к реализации одного и того же пользователя или состояния. Ограничения технологии сбора данных и естественные изменения биометрических данных и условий окружающей среды приводят к вариациям в каждом образце одного и того же биометрического параметра. Например, радужная оболочка считается наиболее точной из биометрических данных, однако между двумя разными изображениями одной и той же радужной оболочки может быть до 30 % различий [1]. Основная задача всех биометрических криптосистем – преодолеть эту вариацию, используя преимущества биометрии для повышения безопасности ключей и паролей.

Тепловизионные изображения не так давно используются в качестве нового подхода в биометрических системах идентификации личности и являются особым видом биометрических образов, позволяющих решить вопрос как аутентификации субъекта, так и идентификации его психофизиологического состояния.

Большая часть исследований в этой области основаны на выделении сосудистой сети субъекта и тепловой сигнатуры как уникального признака для идентификации субъекта, как это реализовано в [2]. Средняя точность идентификации субъектов при использовании такого метода составляет 88,46…90,39 %. Преимущества тепловидения заключаются в том, что эта технология в настоящее время становится доступной и мобильной. Это позволяет идентифицировать и аутентифицировать пользователя бесконтактным и непрерывным образом. Результаты по идентификации личности по рисунку вен кистей рук на данный момент приближаются к 100 % [3].

Такие высокие результаты достигаются в том числе за счет использования алгоритмов на базе глубокого обучения, в частности, сверточных нейронных сетей. В области обработки и анализа изображений, снятых в инфракрасном диапазоне (ИК-изображений), они дают высокие результаты как по точности распознавания, так и по скорости обучения. Рассматриваются теоретические и практические вопросы обучения преобразователей биометрических параметров нейронной сети в ключевой код (нейросетевые преобразователи «биометрия-код», НПБК), позволяющие также безопасно и анонимно хранить биометрический шаблон [4].

В состав НПБК входят специальные предварительно обученные глубокие сети со специальной архитектурой – автокодировщики [5]. Как показано на

рис. 1, автокодировщик состоит из двух компонентов, кодировщика и декодировщика, каждый из которых может иметь одинаковое количество скрытых слоев. Кодировщик учится сжимать входной вектор X до более короткого кода h, в то время как декодировщик учится восстанавливать входной вектор X, распаковывая h. Кодировщик и декодировщик, соответственно, определяются двумя функциями f и h как $f(X) = h$ и $g(h) = X'$. Типичный автокодировщик стремится решить функцию потерь следующим образом:

$$\arg\min_{f,g} \| X - g(f(X)) \|^2 .$$

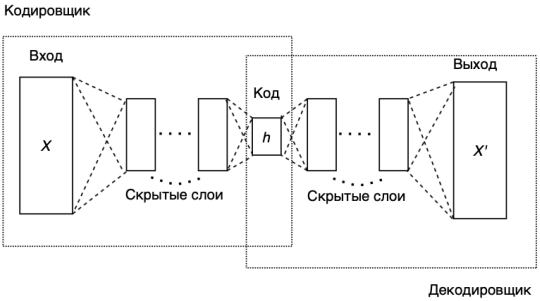


Рис. 1. Стандартная структура автокодировщика

Fig. 1. Standard Autoencoder structure

Важной задачей является защита биометрических образов, ключей и паролей от компрометации при хранении. Для успешной разблокировки криптографического ключа, связанного с биометрическим образом с помощью ПБК, необходимо следующее:

– биометрические данные пользователя;

– открытая дополнительная информация, позволяющая восстановить ключ (secure sketch);

– параметры преобразования для биоключа.

НПБК позволяют избежать разблокировки биоключа и при этом достигают более низких показателей FRR и FAR по сравнению со схемами нечеткого экстрактора [6, 7], не налагая ограничения на длину ключа. Чтобы злоумышленник не смог восстановить исходные данные биометрического образа из компактного описания после обучения НПБК, декодировщик необходимо удалить. НПБК строится персонально для каждого субъекта, при этом формируется искусственная нейронная сеть (ИНС), количество входов кото-

рой равно числу признаков (биометрических параметров), а количество выходов – длине личного ключа. Каждый нейрон последнего слоя генерирует один бит [8, 9].

Надежность обученного ПБК определяется тем, что даже без применения сторонних средств шифрования биометрический эталон пользователя и его личный ключ или пароль скрыты от восстановления из-за невозможности извлечь знания из обученного ПБК (рис. 2).

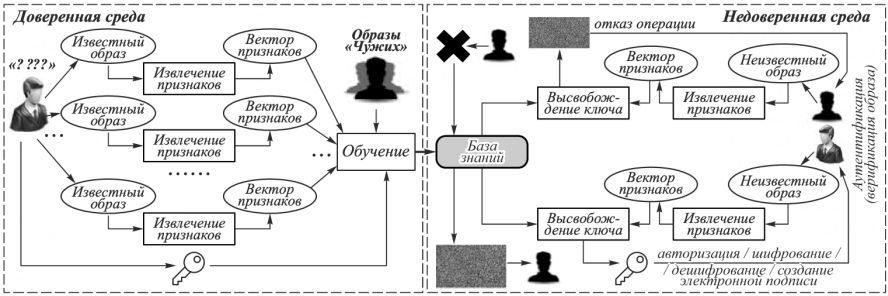


Рис. 2. Общая схема преобразователя «биометрия-код»

Fig. 2. General diagram of the biometrics-to-code converter

Настоящая работа посвящена вопросам генерации ключа на основе термограмм, регистрируемых бесконтактно, и влияния ПФС на результат генерации ключа.

ПОСТРОЕНИЕ НЕЙРОСЕТЕВОГО ПБК ДЛЯ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ ПО ТЕРМОГРАММАМ ЛИЦА С УЧЕТОМ ЕГО ПФС

В соответствии с ГОСТ Р 52633.5–2011 первый НПБК обогащает входные данные, второй – играет роль кодов, исправляющих ошибки. Однако по сравнению с нечеткими экстракторами нейросетевая коррекция ошибочных разрядов ключа обладает гораздо меньшей избыточностью [10]. Искусственный нейрон «широкой» сети базируется на функционале (1) и пороговой функции активации (2), модули весов нейронов первого слоя вычисляются по формуле (3) [10]:

$$y = \sum_{j=1}^{n} \mu_j a_j; \tag{1}$$

$$f(y) = \begin{Bmatrix} 0, y < \mu_0 \\ 1, y \geq \mu_0 \end{Bmatrix}; \quad \mu_j = | m_s(a_j) - m_o(a_j) | \ / \sigma_s(a_j)\sigma_o(a_j); \tag{2}$$

$$\mu_j = |m_s(a_j) - m_o(a_j)| \ / \sigma_s(a_j)\sigma_o(a_j), \quad (3)$$

где a_j – значение *j*-го признака (входа нейрона); $m_o(a_j)$ и $\sigma_o(a_j)$ – математическое ожидание и среднеквадратичное отклонение значений *j*-го признака образа «Свой»; $m_s(a_j)$ и $\sigma_s(a_j)$ – аналогичные показатели образов для образа «Чужие»; μ_0 – порог активации нейрона; *y* – отклик нейрона на образ «Свой» или «Чужой»; *n* – количество входов (размерность) нейрона. Если нейрон настроен на выдачу «единицы» при поступлении образа «Свой», то знак весового коэффициента выбирается исходя из правила: «+» при $m_s(a_j) < m_o(a_j)$, иначе «–». Если нейрон настраивается на ноль, знаки инвертируются. Параметры $m_o(a_j)$, $\sigma_o(a_j)$, $m_s(a_j)$ и $\sigma_s(a_j)$ после обучения удаляются, чтобы не компрометировать эталон. Остаются таблицы связей и весов μ, что не дает непосредственного наблюдения за биометрическими признаками $m_o(a_j)$.

Слои нейронов НПБК являются частично связными. В соответствии с требованиями [11] входы нейронов не должны повторяться – каждый нейрон должен быть связан с уникальным набором признаков. В настоящем исследовании использовались НПБК из 123 нейронов, по 4 входа в каждом (492 / 4 = 123 бит длина ключа).

Количество нейронов последнего слоя равно длине генерируемого ключа.

Проведен вычислительный эксперимент с использованием набора данных термограмм 84 испытуемых, которые находились в следующих ПФС: нормальное, после физической нагрузки, стресс, сонное, 3 стадии алкогольного опьянения. Для ввода субъектов в каждое из заявленных состояний был составлен протокол проведения натурных экспериментов [12–15].

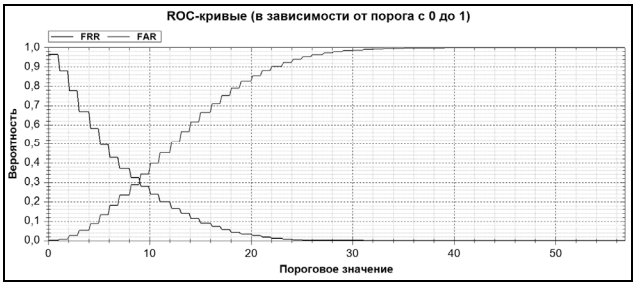
Эксперимент состоял из трех этапов. На первом этапе для обучения НПБК использовалось по 10 примеров термограмм каждого пользователя в нормальном состоянии. Тестирование проводилось на термограммах пользователей, находящихся также в нормальном состоянии, но не вошедших в обучающую выборку.

На втором этапе использовалось 20 обучающих примеров термограмм пользователей в нормальном состоянии. Тестирование проводилось на термограммах пользователей, находящихся в измененных состояниях.

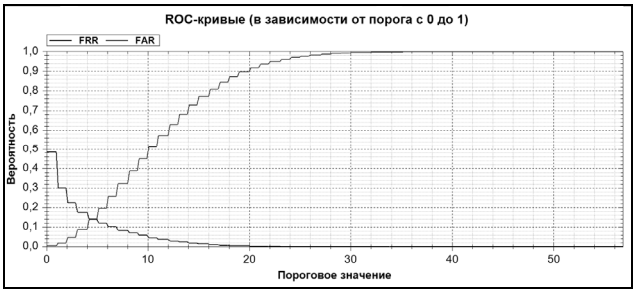
На третьем этапе объем обучающей выборки каждого пользователя составлял 40 примеров: 20 получены в нормальном ПФС, 20 – в состоянии после нагрузки. Тестирование проводилось на термограммах пользователей, соответствующих другим состояниям.

В качестве обучающей выборки «Чужие» во всех случаях использовалось по одному образу на каждого субъекта в нормальном состоянии. Результаты представлены на рис. 3.

а



б



в

Рис. 3. Результаты тестирования НПБК на термографических изображениях лица и шеи субъектов:

а – результаты этапа № 1; *б* – результаты этапа № 2; *в* – результаты этапа № 3

Fig. 3. Results of testing of NNCBC on thermographic images of the face and neck of subjects:

a is results of stage 1; *b* is results of stage 2; *c* is results of stage 3

Ключевыми показателями эффективности биометрической системы являются вероятности ошибок ложного отказа (FRR) и ложного пропуска (FAR). Для сравнения этих показателей обычно используется коэффициент равной вероятности ошибок (EER = FAR = FAR). Из рис. 3 можно сделать вывод, что генерация ключа длиной 123 бита вполне возможно осуществить на основе одной термограммы. Однако ПФС существенно влияет на результат.

ЗАКЛЮЧЕНИЕ

В настоящей работе установлено, что на основе термограммы лица можно сгенерировать криптографический ключ длиной 123 бита. Вероятность ошибок генерации ключа зависит от того, совпадает ли ПФС субъекта на этапе обучения и тестирования НПБК. При совпадении ПФС коэффициент равной вероятности ошибок составил EER = 0,85 %. В случае несовпадения вероятность существенно повышается до EER = 30,84 %.

В настоящей работе предложено следующее: обучение должно проводиться на данных, полученных для различных состояний субъекта (двух, трех) и желательно в разные дни. В этом случае количество ошибок снижается. Причем даже если пользователь обучал систему на данных нормального ПФС, сонного состояния и состояния после физической нагрузки, вероятность ошибочных решений снижается даже для тех состояний, которые не использовались при обучении (стресс, алкогольное опьянение): EER = 14,94 %.

СПИСОК ЛИТЕРАТУРЫ

1. Biometric cryptosystems: issues and challenges / U. Uludag, S. Pankanti, S. Prabhakar, A.K. Jain // Proceedings of the IEEE. – 2004. – Vol. 92 (6). – P. 948–960.

2. Thermal imaging as a biometrics approach to facial signature authentication / A.M. Guzman, M. Goryawala, Jin Wang, A. Barreto, J. Andrian, N. Rishe, M. Adjouadi // IEEE Journal of Biomedical and Health Informatics. – 2013. – Vol. 17 (1). – P. 214–222.

3. VPID: Towards vein pattern identification using thermal imaging / S. Faltaous, J. Liebers, Y. Abdelrahman, F. Alt, S. Schneegass // i-com. De Gruyter Oldenbourg. – 2019. – Vol. 18 (3). – P. 259–270.

4. *Сулавко А. Е., Лыжин А. А.* Модель защищенного нейроиммунного контейнера для задач биометрической аутентификации // Фундаментальные и прикладные исследования молодых ученых: сборник материалов IV Международной научно-практической конференции студентов, аспирантов и моло-

дых ученых / Сибирский государственный автомобильно-дорожный университет. – Омск, 2020. – С. 378–382.

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

6. Fuzzy vault scheme based on fixed-length templates applied to dynamic signature verification / W. Ponce-Hernandez, R. Blanco-Gonzalo, J. Liu-Jimenez, R. Sanchez-Reillo // IEEE Access. – 2020. – Vol. 8. – P. 11152–11164.

7. *Elrefaei L.A., Al-Mohammadi A.M.* Machine vision gait-based biometric cryptosystem using a fuzzy commitment scheme // Journal of King Saud University – Computer and Information Sciences. – 2019. – DOI: 10.1016/j.jksuci.2019.10.011.

8. *Сулавко А.Е.* Высоконадежная двухфакторная биометрическая аутентификация по рукописным и голосовым паролям на основе гибких нейронных сетей // Компьютерная оптика. – 2020. – Т. 44, № 1. – С. 82–91. – DOI: 10.18287/2412-6179-CO-567.

9. *Хайкин С.* Нейронные сети. Полный курс. – 2-е изд. – М.: Вильямс, 2006. – 1103 с.

10. *Ivanov A.I., Kachajkin E.I., Lozhnikov P.S.* A complete statistical model of a handwritten signature as an object of biometric identification // 2016 International Siberian Conference on Control and Communications (SIBCON). – Moscow, Russia, 2016. – P. 1–5. – DOI: 10.1109/SIBCON.2016.7491678.

11. *Akhmetov B.S., Ivanov A.I., Alimseitova Z.K.* Training of neural network biometry-code converters // News of the National Academy of Sciences of the Republic of Kazakhstan. Series of Geology and Technical Sciences. – 2018. – Vol. 1. – P. 61–68.

12. ТС 26.2.002–2020. Системы обработки информации. Криптографическая защита информации. Защита нейросетевых биометрических контейнеров с использованием криптографических алгоритмов / Технический комитет по стандартизации «криптографическая защита информации» ТК 26. – М., 2020.

13. *Жумажанова С.С.* Особенности тепловых паттернов лица и шеи при физическом и ментальном стрессах // Биомедицинская радиоэлектроника. – 2021. – Т. 24, № 1. – С. 13–21. – DOI: 10.18127/j15604136-202101-02.

14. *Белгородцев А.А., Жумажанова С.С., Пасенчук В.А.* О возможности определения степени алкогольного опьянения по термограммам лица субъекта // Приборы и методы измерений, контроля качества и диагностики в промышленности и на транспорте: материалы III всероссийской научно-технической конференции с международным участием. – Омск, 2018. – Р. 373–379.

15. *Жумажанова С.С., Сулавко А.Е., Лукин Д.В.* Анализ термограмм лица и шеи для распознавания состояния сонливости пользователей на основе классификатора Байеса // Вопросы защиты информации. – 2020. – № 2 (129). – С. 24–30.

Ложников Павел Сергеевич, заведующий кафедрой комплексной защиты информации Омского государственного технического университета, доктор технических наук. Основное направление научных исследований – биометрическая защита электронного документооборота. Автор более 60 научных и методических работ. E-mail: lozhnikov@mail.ru

Жумажанова Самал Сагидулловна, ассистент кафедры комплексной защиты информации Омского государственного технического университета. Основное направление научных исследований – дистанционное определение психофизиологического состояния субъектов по термограммам лица на базе сверточных нейронных сетей. E-mail: samal_shumashanova@mail.ru

DOI: 10.17212/2782-2230-2021-2-154-165

Model of the "biometry-code" converter based on artificial neural networks for analysis of facial thermograms*

P.S. Lozhnikov[1], S.S. Zhumazhanova[2]

[1] *Omsk State Technical University, 11 Mira Prospekt, Omsk, 644050, Russian Federation, doctor of technical sciences, head of the Complex Information Protection Department. E-mail: lozhnikov@mail.ru.*
[2] *Omsk State Technical University, 11 Mira Prospekt, Omsk, 644050, Russian Federation, assistant of the Complex Information Protection Department. E-mail: samal_shumashanova@mail.ru*

Existing asymmetric encryption algorithms involve the storage of a secret private key, authorized access to which, as a rule, is carried out upon presentation of a password. Passwords are vulnerable to social engineering and human factors.
Combining biometric security techniques with cryptography is seen as a possible solution to this problem, but any biometric cryptosystem should be able to overcome the small differences that exist between two different implementations of the same biometric parameter. This is especially true for dynamic biometrics, when differences can be caused by a change in the psychophysiological state of the subject. The solution to the problems is the use of a system based on the "biometrics-code" converter, which is configured to issue a user key after presentation of his/her biometric image. In this case, the key is generated in advance in accordance

* *Received 12 May 2021.*

with accepted standards without the use of biometric images. The work presents results on using thermal images of a user for reliable biometric authentication based on a neural network "biometrics-code" converter. Thermal images have recently been used as a new approach in biometric identification systems and are a special type of biometric images that allow us to solve the problem of both the authentication of the subject and the identification of his psychophysiological state. The advantages of thermal imaging are that this technology is now becoming available and mobile, allowing the user to be identified and authenticated in a non-contact and continuous manner. In this paper, an experiment was conducted to verify the images of thermograms of 84 subjects and the following indicators of erroneous decisions were obtained: EER = 0.85 % for users in the "normal"state.

Keywords: “biometrics-code” converter, facial thermograms, artificial neural networks, cryptographic key, biometric authentication, psychophysiological state, thermal imaging images, FRR, FAR

REFERENCES

1. Uludag U., Pankanti S., Prabhakar S., Jain A.K. Biometric cryptosystems: issues and challenges. *Proceedings of the IEEE*, 2004, vol. 92 (6), pp. 948–960.

2. Guzman A.M., Goryawala M., Jin Wang, Barreto A., Andrian J., Rishe N., Adjouadi M. Thermal imaging as a biometrics approach to facial signature authentication. *IEEE Journal of Biomedical and Health Informatics*, 2013, vol. 17 (1), pp. 214–222.

3. Faltaous S., Liebers J., Abdelrahman Y., Alt F., Schneegass S. VPID: towards vein pattern identification using thermal imaging. *i-com. De Gruyter Oldenbourg*, 2019, vol. 18 (3), pp. 259–270.

4. Sulavko A.E., Lyzhin A.A. [Model of protected neuro-immune container for biometric authentication tasks]. *Fundamental'nye i prikladnye issledovaniya molodykh uchenykh* [Fundamental and Applied Research of Young Scientists]. Collection of Materials of the IV International Scientific and Practical Conference of Students, Postgraduates and Young Scientists. Siberian State Automobile and Highway University. Omsk, 2020, pp. 378–382. (In Russian).

5. Akhmetov B.S., Ivanov A.I., Funtikov V.A., Bezyaev A.V., Malygina E.A. *Tekhnologiya ispol'zovaniya bol'shikh neironnykh setei dlya preobrazovaniya nechetkikh biometricheskikh dannykh v kod klyucha dostupa* [Application of large neural networks for fuzzy biometric data conversion into access key code]. Almaty, LEM Publ., 2014. 144 p.

6. Ponce-Hernandez W., Blanco-Gonzalo R., Liu-Jimenez J., Sanchez-Reillo R. Fuzzy vault scheme based on fixed-length templates applied to dynamic signature verification. *IEEE Access*, 2020, vol. 8, pp. 11152–11164.

7. Elrefaei L.A., Al-Mohammadi A.M. Machine vision gait-based biometric cryptosystem using a fuzzy commitment scheme. *Journal of King Saud University – Computer and Information Sciences*, 2019. DOI: 10.1016/j.jksuci.2019.10.011.

8. Sulavko A.E. Vysokonadezhnaya dvukhfaktornaya biometricheskaya autentifikatsiya po rukopisnym i golosovym parolyam na osnove gibkikh neironnykh setei [Highly reliable two-factor biometric authentication based on handwritten and voice passwords using flexible neural networks]. *Komp'yuternaya optika = Computer Optics*, 2020, vol. 44, no. 1, pp. 82–91. DOI: 10.18287/2412-6179-CO-567. (In Russian).

9. Haykin S. Neural networks. Upple Saddle River, Prentice Hall, 1999 (Russ. ed.: Khaikin S. *Neironnye seti. Polnyi kurs*. 2nd ed. Moscow, Williams Publ., 2006. 1104 p.).

10. Ivanov A.I., Kachajkin E.I., Lozhnikov P.S. A complete statistical model of a handwritten signature as an object of biometric identification. *2016 International Siberian Conference on Control and Communications (SIBCON)*, Moscow, Russia, 2016, pp. 1–5. DOI: 10.1109/SIBCON.2016.7491678.

11. Akhmetov B.S., Ivanov A.I., Alimseitova Z.K. Training of neural network biometry-code converters. *News of the National Academy of Sciences of the Republic of Kazakhstan, Series of Geology and Technical Sciences*, 2018, vol. 1, pp. 61–68.

12. TS 26.2.002–2020. *Sistemy obrabotki informatsii. Kriptograficheskaya zashchita informatsii. Zashchita neirosetevykh biometricheskikh konteinerov s ispol'zovaniem kriptograficheskikh algoritmov* [Technical Specification 26.2.002–2020. Information Processing Systems. Cryptographic protection. Data sheet. Protection of neural network biometric containers using cryptographic algorithms]. Technical Committee 26. Moscow, 2020.

13. Zhumazhanova S.S. Osobennosti teplovykh patternov litsa i shei pri fizicheskom i mental'nom stressakh [Difference of thermal patterns of the face and neck regions in states of physical and mental stresses]. *Biomeditsinskaya radioelektronika = Biomedical Radioelectronics*, 2021, vol. 24, no. 1, pp. 13–21. DOI: 10.18127/j15604136-202101-02.

14. Belgorodtsev A.A., Zhumazhanova S.S., Pasenchuk V.A. [On the possibility of subject alcohol intoxication level identification by analysis of face thermograms]. *Pribory i metody izmerenii, kontrolya kachestva i diagnostiki v promyshlennosti i na transporte*: materialy III vserossiiskoi nauchno-tekhnicheskoi konferentsii s mezhdunarodnym uchastiem [Instruments and methods of measurements, quality control and diagnostics in industry and transport: materials of the III All-Russian scientific and technical conference with international participation]. Omsk, 2018, pp. 373–379. (In Russian).

15. Zhumazhanova S.S., Sulavko A.E., Lukin D.V. Analiz termogramm litsa i shei dlya raspoznavaniya sostoyaniya sonlivosti pol'zovatelei na osnove klassifikatora Baiesa [Analysis of face and neck thermograms for users' drowsiness recogni-

tion based on the Bayesian classifier]. *Voprosy zashchity informatsii = Information Security Questions*, 2020, no. 2 (129), pp. 24–30.

Для цитирования:

Ложников П.С., Жумажанова С.С. Модель преобразователя «биометрия-код» на основе искусственных нейронных сетей для анализа термограмм лица субъектов // Безопасность цифровых технологий. – 2021. – № 2 (101). – С. 154–165. – DOI: 10.17212/2782-2230-2021-2-154-165.

For citation:

Lozhnikov P.S., Zhumazhanova S.S. Model' preobrazovatelya "biometriya-kod" na osnove iskusstvennykh neironnykh setei dlya analiza termogramm litsa sub"ektov [Model of the "biometry-code" converter based on artificial neural networks for analysis of facial thermograms]. *Bezopasnost' tsifrovykh tekhnologii = Digital technology security*, 2021, no. 2 (101), pp. 154–165. DOI: 10.17212/2782-2230-2021-2-154-165.