УДК 004.8, 004.032.26
doi:10.21685/2072-3059-2021-3-5

Искусственный интеллект в защищенном исполнении: преимущества замены классических искусственных нейронов на нейроны среднего геометрического и среднего гармонического

В. С. Лукин[1], А. И. Иванов[2], К. А. Перфилов[3]

[1]Пензенский государственный университет, Пенза, Россия
[2]Пензенский научно-исследовательский электротехнический институт, Пенза, Россия
[3]УМВД России по Пензенской области, Пенза, Россия

[1]ibst@pnzgu.ru, [2]ivan@pniei.penza.ru, [3]kperfilov@yandex.ru

Аннотация. *Актуальность и цели.* Ответственные приложения искусственного интеллекта должны быть выполнены в защищенном исполнении. Одним из направлений создания таких приложений является использование больших искусственных нейронных сетей, например, состоящих из персептронов автоматически обученных по ГОСТ Р 52633.5. Целью работы является замещение классических персептронов на искусственные нейроны среднего геометрического и среднего гармонического. *Материалы и методы*. Персептроны выполняют обогащение биометрических данных через их накапливание в линейном пространстве, т.е. их можно рассматривать как искусственные нейроны среднего арифметического. Искусственные хи-квадрат нейроны и нейроны Махалонобиса накапливают данные в пространстве среднего квадратического отклонения. Рассматривается переход к иным классам искусственных нейронов путем формальной замены пространства накопления данных на среднее геометрическое и среднее гармоническое. *Результаты.* Преимущество нейронов среднего геометрического и среднего гармонического в том, что их программная реализация не требует предварительного вычисления первых статистических моментов малых выборок биометрических данных. Последнее снимает проблему сокрытия статистических моментов образа «Свой» через шифрование таблиц связей и весовых коэффициентов сети искусственных нейронов. *Выводы.* Применение искусственных нейронов среднего геометрического и среднего гармонического является перспективным направлением создания нейросетевых решающих правил искусственного интеллекта в защищенном от извлечения знаний исполнении.

Ключевые слова: искусственные нейроны, нейроны среднего гармонического, нейроны среднего геометрического, защита искусственного интеллекта

Финансирование: исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ), проект №19.

Для цитирования: Лукин В. С., Иванов А. И., Перфилов К. А. Искусственный интеллект в защищенном исполнении: преимущества замены классических искусственных нейронов на нейроны среднего геометрического и среднего гармонического // Известия высших учебных заведений. Поволжский регион. Технические науки. 2021. № 3. С. 43–52. doi:10.21685/2072-3059-2021-3-5

Secure-design artificial intelligence: the advantages of replacing classical artificial neurons with neurons of geometric mean and harmonic mean

V.S. Lukin[1], A.I. Ivanov[2], K.A. Perfilov[3]

[1]Penza State University, Penza, Russia
[2]Penza Scientific Research Electrotechnical Institute, Penza, Russia
[3]Administration of the Ministry of Internal Affairs
of the Russian Federation in Penza region, Penza, Russia
[1]ibst@pnzgu.ru, [2]ivan@pniei.penza.ru, [3]kperfilov@yandex.ru

Abstract. *Background.* Responsible artificial intelligence applications must run in a secure execution. One of the directions for creating such applications is the use of large artificial neural networks, for example, consisting of perceptrons automatically trained in accordance with State Standart R 52633.5. The purpose of the work is to replace classical perceptrons with artificial neurons of the geometric mean and harmonic mean. *Materials and methods*. Perceptrons enrich biometric data through their accumulation in linear space, that is, they can be considered as artificial neurons of the arithmetic mean. Artificial chi-square neurons and Mahalonobis neurons accumulate data in the space of the standard deviation. The transition to other classes of artificial neurons by formal replacement of the data accumulation space with the geometric mean and harmonic mean is considered. *Results.* The advantage of the geometric mean and harmonic mean neurons is that their software implementation does not require preliminary calculation of the first statistical moments of small samples of biometric data. The latter removes the problem of hiding the statistical moments of the "Friend" image through encryption of the tables' connections and weight coefficients of the artificial neurons network. *Conclusions.* The use of artificial neurons of the geometric mean and harmonic mean is a promising direction for creating neural network decision rules of artificial intelligence in a performance protected from knowledge extraction.

Keywords: artificial neurons, harmonic mean neurons, geometric mean neurons, artificial intelligence protection

Acknowledgments: the research was financed by the Ministry of Education and Science (grant IB), project No.19.

For citation: Lukin V.S., Ivanov A.I., Perfilov K.A. Secure-design artificial intelligence: the advantages of replacing classical artificial neurons with neurons of geometric mean and harmonic mean. *Izvestiya vysshikh uchebnykh zavedeniy. Povolzhskiy region. Tekhnicheskie nauki = University proceedings. Volga region. Engineering sciences.* 2021;(3):43–52. (In Russ.). doi:10.21685/2072-3059-2021-3-5

Введение

На сегодня в России действует национальный стандарт по быстрому, абсолютно устойчивому автоматическому обучению сетей персептронов ГОСТ Р 52633.5–2011, разработанный ФБГОУ ВО «Пензенский государственный университет» и АО «Пензенский научно-исследовательский электротехнический институт» в рамках НИР «Биометрия» в 2010 г. Персептроны фактически выполняют обогащение относительно бедных биометрических данных через их усреднение (через их накопление в линейном пространстве):

$$\begin{cases} y^1 \leftarrow \sum_{i=1}^{16} \dfrac{E(x_i) - x_i}{\sigma(x_i)}, \\ z(y^1) \leftarrow \text{"0"} \ \ if \ \ y^1 \le k, \\ z(y^1) \leftarrow \text{"1"} \ \ if \ \ y^1 > k, \end{cases} \quad (1)$$

где i – номер входа персептрона; $E(x_i)$ – математическое ожидание i-го биометрического параметра; $\sigma(x_i)$ – стандартное отклонение i-го биометриче-

ского параметра; $z(y^1)$ – квантователь данных на выходе сумматора искусственного нейрона; k – порог принятия решения при квантовании выходных данных накапливающего сумматора.

Все данные, приводимые в статье, читатель может проверить самостоятельно, если получать 416 биометрических параметра с использованием среды моделирования «БиоНейроАвтограф» [1, 2]. В формуле (1) указано суммирование по 16 входным биопараметрам у одного персептрона, обучаемого алгоритмом ГОСТ Р 52633.5–2011. Шестнадцати входов у нейрона достаточно, чтобы гарантированно обучать на биометрических данных с уровнем качества, характерным для динамики рукописного почерка любого человека. Вводить данные пользователь может, применяя манипулятор «мышь», через чувствительный экран ноутбука или через графический планшет, работающий в режиме манипулятора «мышь».

К сожалению, из нейросети могут быть извлечены знания о криптографическом ключе [3–5]. В связи с этим таблицы связей и таблицы весовых коэффициентов нейронов обученной сети нуждаются в криптографической защите [6]. По технической спецификации [6] защищаемые шифрованием таблиц искусственные нейроны не должны иметь общих связей. То есть число нейронов в сети должно быть 416 / 16 = 26. Длина ключа шифрования и биометрико-нейросетевой аутентификации в 26 бит существенно выше длины ключа, которую обеспечивают так называемые «нечеткие экстракторы», активно продвигаемые США, Канадой и странами Евросоюза [7–9].

Проведенные в Пензенском государственном университете исследования показали, что длину криптографического ключа можно увеличить от трех до четырех раз, если перейти от нейронов с накоплением данных в линейном пространстве (1) к нейронам с накоплением данных в квадратичном пространстве [10–12]:

$$\begin{cases} y^2 \leftarrow \sum\limits_{i=1}^{5} \left\{ \dfrac{E(x_i) - x_i}{\sigma(x_i)} \right\}^2, \\ z(y^2) \leftarrow \text{"0"} \ \ if \ \ y^2 \le k, \\ z(y^2) \leftarrow \text{"1"} \ \ if \ \ y^2 > k. \end{cases} \qquad (2)$$

В этом случае длина криптографического ключа биометрико-нейросетевой аутентификации должна составить от 78 до 104 бит. Этого уже вполне достаточно для большинства приложений биометрии, однако шифрование и вычисление криптографических хэш-функций трудно реализуемы в массовых доверенных контроллерах низкой стоимости, низкого потребления, низкой разрядности.

Перспектива отказа от криптографии за счет перехода к использованию нейронов среднего геометрического

Следует отметить, что записи преобразования данных (1) и (2) в явной форме содержат значения математических ожиданий $E(x_i)$ и стандартных отклонений $\sigma(x_i)$, контролируемых биометрических параметров. Знания о значениях этих двух статистических моментов образа «Свой» компромети-

руют тайну этого образа. Для того чтобы скрыть компрометирующую информацию, приходится шифровать таблицы связей и весовых коэффициентов нейронов по соответствующей технической спецификации [6].

Крайне важным является то, что переход от нейронов среднего арифметического (1) и от нейронов среднего квадратичного (2) к нейронам среднего геометрического снимает проблему использования статистических моментов в явной форме:

$$\begin{cases} x \leftarrow \mathrm{sort}(x), \\ \tilde{x}_i \leftarrow x_i - x_0 + 1, \\ sg \leftarrow \sqrt[5]{\prod_{i=1}^{5} \tilde{x}_i}, \\ z(sg) \leftarrow "0"\, if\ sg \le k, \\ z(sg) \leftarrow "1"\, if\ sg > k. \end{cases} \quad (3)$$

Так как в нейронах среднего геометрического (3) отсутствуют статистические моменты тайного образа «Свой», необходимость в классическом шифровании таблиц обученных нейронов [13–17] отпадает. Как результат, в качестве доверенной вычислительной среды (одноразовой или многоразовой) могут использоваться недорогие, мало потребляющие, мало разрядные процессоры RFID токенов, RFID меток, RFID карт.

Перспектива отказа от криптографии за счет перехода к использованию нейронов среднего гармонического

Еще одним классом перспективных нейронов являются искусственные нейроны среднего гармонического [17, 18]:

$$\begin{cases} x \leftarrow \mathrm{sort}(x), \\ \tilde{x}_i \leftarrow x_i - x_0 + 1, \\ sga \leftarrow 5 \cdot \sqrt[5]{\prod_{i=1}^{5} \tilde{x}_i} \Big/ \sum_{i=1}^{5} \tilde{x}_i, \\ z(sga) \leftarrow "0"\, if\ sga \le k, \\ z(sga) \leftarrow "1"\, if\ sga > k. \end{cases} \quad (4)$$

В преобразованиях (4) не используются значения математических ожиданий $E(x_i)$ и стандартных отклонений $\sigma(x_i)$. Как следствие, данные таблиц обученных искусственных нейронов среднего гармонического не требуют их защиты классическим шифрованием.

Возможность перехода к использованию полиномов, собранных из искусственных нейронов среднего геометрического и среднего гармонического

При криптографическом анализе технической спецификации [6] в ряде публикаций [19, 20] показаны угрозы использования нейронов среднего арифметического (1) с общими связями. Видимо, такие же угрозы появятся и для нейронов среднего квадратического отклонения (2). Положение карди-

нальным образом меняется при переходе к использованию нейронов среднего гармонического и среднего геометрического в паре. Для этих двух типов нейронов допустимо полное повторение их входных данных. Поясним этот тезис на рис. 1 и 2.

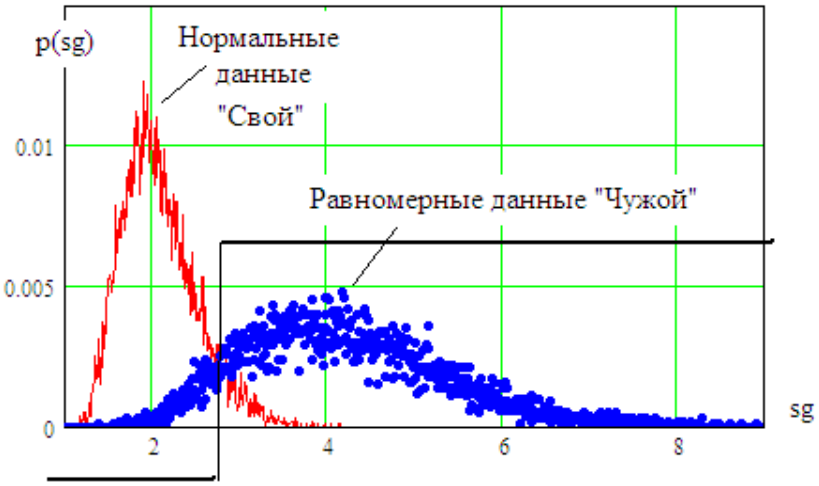

Рис. 1. Плотности вероятности появления различных состояний нейрона среднего геометрического с 5 входами, обученного различать малые выборки с нормальным и равномерным распределениями

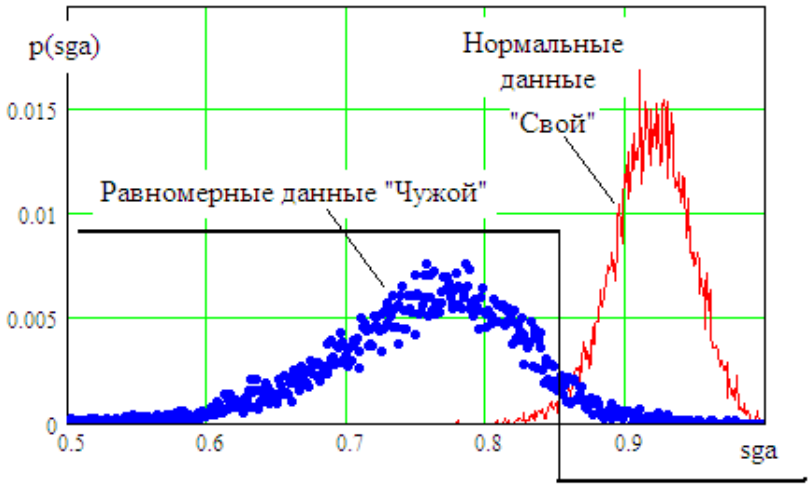

Рис. 2. Плотности вероятности появления различных состояний нейрона среднего гармонического с 5 входами, обученного различать малые выборки с нормальным и равномерным распределениями

На рис. 1 представлены плотности вероятности выходных состояний нейрона среднего геометрического (3), обученного распознавать малую выборку из 5 опытов с нормальным распределением и такую же малую выборку с равномерным распределением данных. При этом выходной квантователь

нейрона имеет порог срабатывания, при котором вероятности ошибок первого и второго рода практически совпадают $P_1 \approx P_2 \approx P_{EE} \approx 0{,}081$.

На рис. 2 представлены плотности вероятности выходных состояний нейрона среднего гармонического (4), обученного распознавать малую выборку из 5 опытов с нормальным распределением и такую же малую выборку с равномерным распределением данных. При этом выходной квантователь нейрона имеет порог срабатывания, при котором вероятности ошибок первого и второго рода практически совпадают $P_1 \approx P_2 \approx P_{EE} \approx 0{,}031$. Последнее означает, что мощность нейрона среднего гармонического более чем в 2 раза выше мощности нейрона среднего геометрического 0,081 / 0,031 ≈ 2,61.

Еще одним важнейшим фактором является то, что выходные состояния двух рассматриваемых нейронов имеют не полную корреляцию corr(sg,sga) ≈ ≈ –0,52. Совместная обработка одной и той же малой выборки двумя нейронами (полиномом из двух нейронов) должна давать результат более надежный, чем даст обработка каждым нейроном отдельно [21].

Получается, что запрет на использование нескольких нейронов, анализирующих одни и те же данные в разных нелинейных многомерных пространствах, может быть полностью снят, если многомерные пространства накопления данных (обогащения данных) взаимно ортогональны [4]. Если же многомерные пространства нейросетевого полинома ортогональны не полностью, то запрет иметь общие входные связи [18, 19] значительно ослабляется.

Если мы частично ослабим запрет наличия общих связей у нейронов и допустим наличие одной обшей связи у нейронов с 5 входами, то таких нейронов окажется 416 / 4 = 104. То есть мы получаем длину криптографического ключа в 104 бита. Если мы допустим наличие двух общих связей, то длина ключа увеличивается до 138 бит. Этого вполне достаточно практически для любых приложений биометрико-нейросетевой аутентификации.

Список литературы

1. Иванов А. И., Захаров О. С. Среда моделирования «БиоНейроАвтограф» [Программный продукт создан лабораторией биометрических и нейросетевых технологий, размещен с 2009 г. на сайте АО «ПНИЭИ»]. URL: http://пниэи.рф/activity/science/noc/bioneuroautograph.zip
2. Иванов А. И. Автоматическое обучение больших искусственных нейронных сетей в биометрических приложениях : учеб. пособие. Пенза, 2013. 30 с. URL: http://пниэи.рф/activity/science/noc/tm_IvanovAI.pdf
3. Язов Ю. К., Волчихин В. И. [и др.]. Нейросетевая защита персональных биометрических данных. М. : Радиотехника, 2012. 157 с.
4. Иванов А. И., Куприянов Е. Н. Защита искусственного интеллекта: ортогонализация статистико-нейросетевого анализа малых выборок биометрических данных : препринт. Пенза : Изд-во ПГУ, 2020. 72 с.
5. Волчихин В. И., Иванов А. И. Нейросетевая молекула: решение обратной задачи биометрии через программную поддержку квантовой суперпозиции на выходах сети искусственных нейронов // Вестник Мордовского университета. 2017. Т. 27, № 4. С. 518–523.
6. Техническая спецификация (проект, публичное обсуждение членами ТК 26 заканчивается в 2020 году) «Криптографическая защита информации. Защита нейросетевых биометрических контейнеров с использованием криптографических алгоритмов». Пенза, 2020.
7. Dodis Y., Reyzin L., Smith A. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy // Proc. EUROCRYPT, 2004. April 13. P. 523–540.

8. Monrose F., Reiter M., Li Q., Wetzel S. Cryptographic key generation from voice // Proc. IEEE Symp. on Security and Privacy, 2001. P. 202–213.
9. Ramírez-Ruiz J., Pfeiffer C., Nolazco-Flores J. Cryptographic Keys Generation Using FingerCodes // Advances in Artificial Intelligence. IBERAMIA-SBIA, 2006. P. 178–187.
10. Волчихин В. И., Иванов А. И., Малыгина Е. А., Юнин А. П. Соотношение мощности нейронов с линейным и квадратичным обогатителями биометрических данных // Известия высших учебных заведений. Поволжский регион. Технические науки. 2018. № 1 (45). С. 17–25.
11. Малыгина Е. А. Биометрико-нейросетевая аутентификация: перспективы применения сетей квадратичных нейронов с многоуровневым квантованием биометрических данных : препринт. Пенза : Изд-во ПГУ, 2020. 114 с.
12. Иванов А. И., Безяев А. В., Малыгина Е. А., Серикова Ю. И. Второй национальный стандарт России по быстрому автоматическому обучению больших искусственных нейронных сетей на малых выборках биометрических данных // Безопасность информационных технологий : сб. науч. ст. по материалам I Всерос. науч.-техн. конф. Пенза, 2019. С. 174–177.
13. Перфилов К. А. Критерий среднего геометрического, используемый для проверки достоверности статистических гипотез распределения биометрических данных // Безопасность информационных технологий : тр. науч.-техн. конф. кластера пензенских предприятий. Пенза, 2014. Т. 9. С. 92–93.
14. Ахметов Б. С., Иванов А. И., Перфилов К. А. Использование среднего геометрического, ожидаемой и наблюдаемой функций вероятности как статистического критерия оценки качества биометрических данных. // Труды Международного симпозиума Надежность и качество. 2015. Т. 2. С. 281–283.
15. Перфилов К. А., Иванов А. И., Проценко Е. Д. Расширение многообразия статистических критериев, используемых при проверке гипотез распределения значений биометрических данных // Европейский союз ученых. 2015. № 4–5 (11). С. 9–12.
16. Иванов А. И., Перфилов К. А., Малыгина Е. А. Многомерный статистический анализ качества биометрических данных на предельно малых выборках с использованием критериев среднего геометрического, вычисленного для анализируемых функций вероятности // Измерение. Мониторинг. Управление. Контроль. 2016. № 2 (16). С. 58–66.
17. Иванов А. И., Банных А. Г., Куприянов Е. Н. Коллекция искусственных нейронов эквивалентных статистическим критериям для их совместного применения при проверке гипотезы нормальности малых выборок биометрических данных // Безопасность информационных технологий : сб. науч. ст. по материалам I Всерос. науч.-техн. конф. Пенза, 2019. С. 163–172.
18. Иванов А. И., Перфилов К. А., Лукин В. С. Нейросетевое обобщение семейства статистических критериев среднего геометрического и среднего гармонического для прецизионного анализа малых выборок биометрических данных // Информационно-управляющие телекоммуникационные системы, средства поражения и их техническое обеспечение : сб. науч. ст. Всерос. науч.-техн. конф. / под общ. ред. В. С. Безяева. Пенза : НПП «Рубин», 2019. С. 50–63.
19. Marshalko G. B. On the security of a neural network-based biometric authentication scheme // Математические вопросы криптографии. 2014. Т. 5. С. 87–98.
20. Bogdanov D. S., Mironkin V. O. Data recovering for a neural network-based biometric authentication scheme. // CTCrypt. Preproceedings, 2018. P. 262–273. URL: https://ctcrypt.ru/files/2018/23_Bogdanov.pdf
21. Безяев А. В. Биометрико-нейросетевая аутентификация: обнаружение и исправление ошибок в длинных кодах без накладных расходов на избыточность : препринт. Пенза : Изд-во ПГУ, 2020. 40 с.

References

1. Ivanov A.I., Zakharov O.S. *Sreda modelirovaniya «BioNeyroAvtograf» [Programmnyy produkt sozdan laboratoriey biometricheskikh i neyrosetevykh tekhnologiy, razmeshchen s 2009 g. na sayte AO «PNIEI»] = Modeling environment "BioNeuroAutograph" [The software product was created by the laboratory of biometric and neural network technologies, posted in 2009 on the website of JSC "PNEI"]*. (In Russ.). Available at: http://pniei.rf/activity/science/noc/bioneuroautograph.zip
2. Ivanov A.I. *Avtomaticheskoe obuchenie bol'shikh iskusstvennykh neyronnykh setey v biometricheskikh prilozheniyakh: ucheb. posobie = Automatic training of large artificial neural networks in biometric applications: textbook*. Penza, 2013:30. (In Russ.). Available at: http://pniei.rf/activity/science/noc/tm_IvanovAI.pdf
3. Yazov Yu.K., Volchikhin V.I. [et al.]. *Neyrosetevaya zashchita personal'nykh biometricheskikh dannykh = Neural network protection of personal biometric data*. Moscow: Radiotekhnika, 2012:157. (In Russ.)
4. Ivanov A.I., Kupriyanov E.N. *Zashchita iskusstvennogo intellekta: ortogonalizatsiya statistiko-neyrosetevogo analiza malykh vyborok biometricheskikh dannykh: preprint = Artificial intelligence protection: orthogonalization of statistics-neural network analysis of small samples of biometric data: preprint*. Penza: Izd-vo PGU, 2020:72. (In Russ.)
5. Volchikhin V.I., Ivanov A.I. Neural network molecule: solving the inverse problem of biometrics through software support of quantum superposition at the outputs of a network of artificial neurons. *Vestnik Mordovskogo universiteta = Bulletin of Mordovian University*. 2017;27(4):518–523. (In Russ.)
6. *Tekhnicheskaya spetsifikatsiya (proekt, publichnoe obsuzhdenie chlenami TK 26 zakanchivaetsya v 2020 godu) «Kriptograficheskaya zashchita informatsii. Zashchita neyrosetevykh biometricheskikh konteynerov s ispol'zovaniem kriptograficheskikh algoritmov» = Technical specification (draft, public discussion by TC 26 members ends in 2020) "Cryptographic information protection. Protection of neural network biometric containers using cryptographic algorithms"*. Penza, 2020. (In Russ.)
7. Dodis Y., Reyzin L., Smith A. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy. *Proc. EUROCRYPT*. 2004;April 13:523–540.
8. Monrose F., Reiter M., Li Q., Wetzel S. Cryptographic key generation from voice. *Proc. IEEE Symp. on Security and Privacy*. 2001:202–213.
9. Ramírez-Ruiz J., Pfeiffer C., Nolazco-Flores J. Cryptographic Keys Generation Using FingerCodes. *Advances in Artificial Intelligence*. IBERAMIA-SBIA, 2006:178–187.
10. Volchikhin V.I., Ivanov A.I., Malygina E.A., Yunin A.P. The ratio of neurons' power with linear and quadratic biometric data enrichers. *Izvestiya vysshikh uchebnykh zavedeniy. Povolzhskiy region. Tekhnicheskie nauki = University proceedings. Volga region. Engineering sciences*. 2018;(1):17–25. (In Russ.)
11. Malygina E.A. *Biometriko-neyrosetevaya autentifikatsiya: perspektivy primeneniya setey kvadratichnykh neyronov s mnogourovnevym kvantovaniem biometricheskikh dannykh: preprint = Biometrical neural network authentication: prospects for the application of quadratic neuron networks with multilevel quantization of biometric data: preprint.* Penza: Izd-vo PGU, 2020:114. (In Russ.)
12. Ivanov A.I., Bezyaev A.V., Malygina E.A., Serikova Yu.I. The second national standard of Russia for fast automatic training of large artificial neural networks on small samples of biometric data. *Bezopasnost' informatsionnykh tekhnologiy: sb. nauch. st. po materialam I Vseros. nauch.-tekhn. konf. = Information technology security: proceedings of the 1st All-Russian scientific and engineering conference*. Penza, 2019:174–177. (In Russ.)
13. Perfilov K.A. A geometric mean criterion used to test the reliability of statistical hypotheses of the distribution of biometric data. *Bezopasnost' informatsionnykh tekhnologiy: tr. nauch.-tekhn. konf. klastera penzenskikh predpriyatiy = Information Technology Security: proceedings of scientific and technical conference cluster of Penza enterprises*. Penza, 2014;9:92–93. (In Russ.)

14. Akhmetov B.S., Ivanov A.I., Perfilov K.A. Using the geometric mean, expected and observed probability functions as a statistical criterion for assessing the quality of biometric data. *Trudy Mezhdunarodnogo simpoziuma Nadezhnost' i kachestvo = Proceedings of the International symposium Reliability and Quality*. Penza, 2015;2:281–283. (In Russ.)
15. Perfilov K.A., Ivanov A.I., Protsenko E.D. Expanding the variety of statistical criteria used to test the hypotheses of the biometric data values distribution. *Evropeyskiy soyuz uchenykh = European union of scientists*. 2015;(4–5):9–12. (In Russ.)
16. Ivanov A.I., Perfilov K.A., Malygina E.A. Multivariate statistical analysis of the quality of biometric data on extremely small samples using the geometric mean criteria calculated for the analyzed probability functions. *Izmerenie. Monitoring. Upravlenie. Kontrol' = Measurement. Monitoring. Administration. Control*. 2016;(2):58–66. (In Russ.)
17. Ivanov A.I., Bannykh A.G., Kupriyanov E.N. A collection of artificial neurons equivalent to statistical criteria for their combined use in testing the hypothesis of normality of small samples of biometric data. *Bezopasnost' informatsionnykh tekhnologiy: sb. nauch. st. po materialam I Vseros. nauch.-tekhn. konf. = Information technology security: proceedings of the 1st All-Russian scientific and engineering conference*. Penza, 2019:163–172. (In Russ.)
18. Ivanov A.I., Perfilov K.A, Lukin V.S. Neural network generalization of a family of statistical criteria for geometric mean and harmonic mean for precision analysis of small samples of biometric data. *Informatsionno-upravlyayushchie telekommunikatsionnye sistemy, sredstva porazheniya i ikh tekhnicheskoe obespechenie: sb. nauch. st. Vseros. nauch.-tekhn. konf. = Information and administration telecommunication systems, weapons and their technical support: proceedings of the All-Russian scientific and engineering conference*. Penza: NPP «Rubin», 2019:50–63. (In Russ.)
19. Marshalko G.B. On the security of a neural network-based biometric authentication scheme. *Matematicheskie voprosy kriptografii = Mathematical questions of cryptography*. 2014;5:87–98.
20. Bogdanov D.S., Mironkin V.O. Data recovering for a neural network-based biometric authentication scheme. *CTCrypt. Preproceedings*. 2018:262–273. Available at: https://ctcrypt.ru/files/2018/23_Bogdanov.pdf
21. Bezyaev A.V. *Biometriko-neyrosetevaya autentifikatsiya: obnaruzhenie i ispravlenie oshibok v dlinnykh kodakh bez nakladnykh raskhodov na izbytochnost': preprint = Biometrical neural network authentication: detecting and correcting errors in long codes without the overhead of redundancy: preprint*. Penza: Izd-vo PGU, 2020:40. (In Russ.)

Информация об авторах / Information about the authors

Виталий Сергеевич Лукин
младший научный сотрудник регионального учебно-научного центра «Информационная безопасность», Пензенский государственный университет (Россия, г. Пенза, ул. Красная, 40)

E-mail: ibst@pnzgu.ru

Vitaliy S. Lukin
Junior researcher, Regional Training and Research Center of "Information security", Penza State University (40 Krasnaya street, Penza, Russia)

Александр Иванович Иванов
доктор технических наук, доцент, научный консультант, Пензенский научно-исследовательский электротехнический институт (Россия, г. Пенза, ул. Советская, 9)

E-mail: ivan@pniei.penza.ru

Aleksandr I. Ivanov
Doctor of engineering sciences, associate professor, scientific adviser, Penza Scientific Research Electrotechnical Institute (9 Sovetskaya street, Penza, Russia)

Константин Александрович Перфилов
главный специалист Центра
информационных технологий связи
и защиты информации, УМВД России
по Пензенской области (Россия, г. Пенза,
ул. Пушкина, 159)
E-mail: perfilov58@gmail.com

Konstantin A. Perfilov
Principal specialist of the Center
of information technologies
in communication and data protection,
Administration of the Ministry of Internal
Affairs of the Russian Federation in Penza
region (159 Pushkina street, Penza, Russia)

Авторы заявляют об отсутствии конфликта интересов / The authors declare no conflicts of interests.

Поступила в редакцию / Received 17.01.2021

Поступила после рецензирования и доработки / Revised 16.05.2021

Принята к публикации / Accepted 02.10.2021