УДК 519.24; 53; 57.017
DOI 10.21685/2072-3059-2018-1-2

В. И. Волчихин, А. И. Иванов, Е. А. Малыгина, А. П. Юнин

СООТНОШЕНИЕ МОЩНОСТИ НЕЙРОНОВ С ЛИНЕЙНЫМ И КВАДРАТИЧНЫМ ОБОГАТИТЕЛЯМИ БИОМЕТРИЧЕСКИХ ДАННЫХ

Аннотация.

Актуальность и цели. Целью работы является сопоставительная оценка мощностей обычных нейронов с линейным суммированием и нейронов с квадратичным суммированием нормированных и центрированных биометрических данных.

Материалы и методы. Обучение обычных нейронов преобразователя биометрии в код абсолютно устойчиво для клона алгоритмов ветви ГОСТ Р 52633.5–2011. Такой же устойчивостью обладают алгоритмы обучения радиально-базисных нейронов. В плане устойчивости нет разницы между обучением нейронов с линейным и квадратичным обогащением данных.

Результаты. Показано, что вероятности ошибок первого и второго рода при обработке биометрических данных обычными нейронами намного больше, чем при обработке радиально-базисными нейронами. При этом наклон линии роста мощности квадратичных нейронов в зависимости от размерности задачи имеет наклон в несколько раз более крутой, чем для линейных нейронов. Наблюдается очень быстрый рост мощности квадратичных нейронов с ростом числа входов у них.

Выводы. Высокая мощность квадратичных нейронов делает их крайне перспективными для применения в нейросетевых преобразователей биометрии. Необходимо направить усилия на то, чтобы разработать специальные меры, устраняющие недостаток квадратичных нейронов, хранящих открыто математическое ожидание и стандартное отклонение персональных биометрических параметров.

Ключевые слова: нейросетевой преобразователь биометрия-код, биометрические данные, большая размерность данных.

V. I. Volchikhin, A. I. Ivanov, E. A. Malygina, A. P. Yunin

CORRELATION OF NEURON POWER WITH LINEAR AND SQUARE COMPARISON OF BIOMETRIC DATA

Abstract.

Background. The goal of the research is comparative assessment of capacity of conventional neurons with linear summation and neurons with the quadratic sum of standardized and centered biometric data.

Materials and methods. Training of conventional neurons converter biometrics in code is absolutely resistant to clone branch algorithms (state standart GOST R 52633.5-2011). Algorithms for training radial-basic neurons have the same stability. In terms of stability, there is no difference between training neurons with linear and quadratic enrichment of data.

Results It is shown that the probabilities of errors of the first and second kind in the processing of biometric data by ordinary neurons are much greater than in the treatment of radial-basic neurons. The slope of the power growth line of quadratic

neurons, depending on the dimension of the problem, has a slope several times steeper than for linear neurons. There is a very rapid increase in the power of quadratic neurons with an increase in the number of entries they have.

Conclusions. High power quadratic neurons makes them extremely promising for application in neural network converters biometrics. Efforts need to be directed to develop special measures to eliminate the disadvantage of quadratic neurons store open mathematical expectation and standard deviation of personal biometric parameters.

Key words: neuronet converter «biometry-code», biometric data, large dimension of data.

Общие положения нейросетевого преобразования биометрии в код

В настоящее время гражданская активность перемещается в сферу цифровой экономики. Защита цифровой экономики России невозможна без активного использования отечественной криптографии при доступе к облачным сервисам. К сожалению, люди не могут запоминать длинные криптографические ключи и длинные пароли доступа к собственным информационным ресурсам. Эту проблему призвана решить биометрия.

В США, Канаде, Евросоюзе развивается технология так называемых «нечетких» экстракторов [1–3]. Технология сводится к тому, что из биометрического образа извлекаются его параметры, далее их значения квантуются. Полученный Биокод может содержать от 20 до 30 % ошибок. Для устранения ошибок используют маскирование наиболее нестабильных бит Биокода, оставшиеся ошибки обнаруживаются и исправляются классическими самокорректирующимися кодами, обладающими примерно 20-кратной избыточностью. То есть длина Биокода оказывается примерно в 20 раз меньше числа биометрических параметров, извлеченных из образа. Как правило, Биокоды на выходе «нечетких» экстракторов оказываются недопустимо короткими для того, чтобы далее использовать полноценную криптографию.

Российские специалисты по информационной безопасности идут иным путем. В России создается, стандартизуется и поддерживается технология нейросетевого преобразования биометрических данных в код заранее полученного криптографического ключа [4, 5]. Основной проблемой применения искусственных нейронных сетей является то, что они очень медленно учатся и для их обучения [6] необходимы огромные обучающие выборки, содержащие порядка 100 000 примеров биометрических образов. Медленное обучение и большие выборки обучающих примеров для обучения «глубоких» нейронных сетей [6] необходимы из-за того, что итерационный алгоритм «обратного распространения ошибки» имеет экспоненциальную вычислительную сложность.

Технический тупик экспоненциальной вычислительной сложности обучения «глубоких» нейронных сетей обходится переходом к применению однослойных искусственных нейронных сетей с большим числом выходов. Для этого типа искусственных нейронных сетей вычислительная сложность обучения оказывается линейной [7], что позволяет их обучать на выборке из 20 примеров образа «Свой». При этом время обучения оказывается незначительным (от 0,5 до 0,05 с) даже при использовании дешевых процессоров низкой производительности.

Основная идея быстрых стандартизованных алгоритмов обучения сводится к тому, что обучение линейной части нейрона (сумматора) и нелинейной части нейрона (квантователя) разделены. Декомпозиция задачи на две простых подзадачи (линейную свертку в пространстве входных состояний и нелинейное преобразование выходных данных свертки [8]) всегда приводит к значительному упрощению вычислений. Этот подход к декомпозиции задачи обучения иллюстрируется рис. 1.

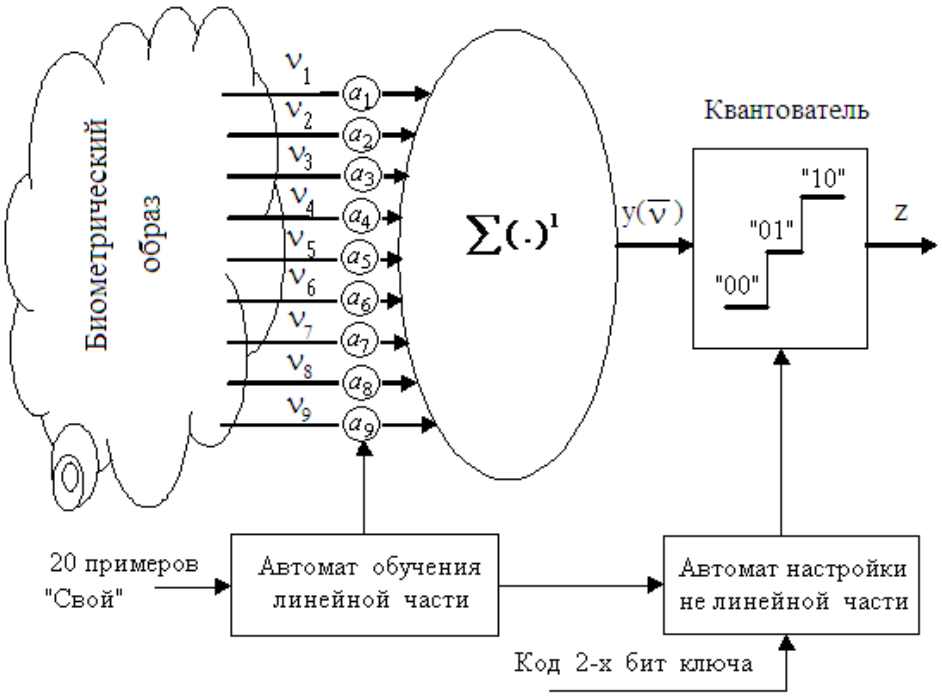

Рис. 1. Декомпозиция задачи обучения на две более простых подзадачи

В частности, в такой декомпозиции задачи построен алгоритм обучения, регламентированный ГОСТ Р 52633.5 [7]. Отличие от структуры рис. 1 от алгоритма [7] состоит только в типе использованного квантователя. ГОСТ Р 52633.5 [7] ориентирован на использование двухуровневого (бинарного) квантователя, который проще троичного квантователя, отображенного на рис. 1.

Троичный квантователь (рис. 1) выгоден тем, что позволяет существенно улучшить уровень защищенности нейросетевого преобразователя [9], так как значительно усложняет реализацию атаки Г. Б. Маршалко [10], построенной на поиске общих входных связей нейронов.

Прозрачная парадигма разделения задачи обучения нейронной сети на две составляющих (линейную и нелинейную) дает очень хорошие результаты по сокращению размеров обучающей выборки и сведению задачи до линейной вычислительной сложности. Тем не менее этот конструктивный прием не является универсальным, вполне могут существовать и другие варианты декомпозиции задачи, приводящие к близким или даже более качественным результатам.

Цель статьи – показ еще одного варианта эффективной декомпозиции обучения. По мнению авторов, линейные свертки по пространству биометрических параметров могут быть заменены на свертки по квадратичному пространству (на квадратичные функционалы). При этом для биометрических данных наблюдается значительное приращение качества принятия решений.

Оценка мощности линейных сверток, обогащающих биометрические данные вокруг центра многомерного образа «Свой»

Алгоритм обучения ГОСТ Р 52633.5 [7] ориентирован на обогащение биометрических данных по отношению к центру образов «Все Чужие». Однако этот же алгоритм можно сориентировать на обогащение данных вокруг центра образов «Свой». В этом случае весовые коэффициенты сумматора нейрона легко выражаются через математическое ожидание и стандартное отклонение параметров образа «Свой». При этом отклик на *j*-й пример образа «Свой» будет описываться следующим уравнением:

$$y_j(\overline{v}) = \sum_{i=1}^{20} \left\{ \frac{E(v_i) - v_{i,j}}{\sigma(v_i)} \right\}^1, \qquad (1)$$

где $E(.)$ – оператор вычисления математического ожидания; $\sigma(.)$ – оператор вычисления стандартного отклонения.

Типичное распределение данных на выходе сумматора с 20 входами для примеров образа «Свой» приведено на рис. 2.

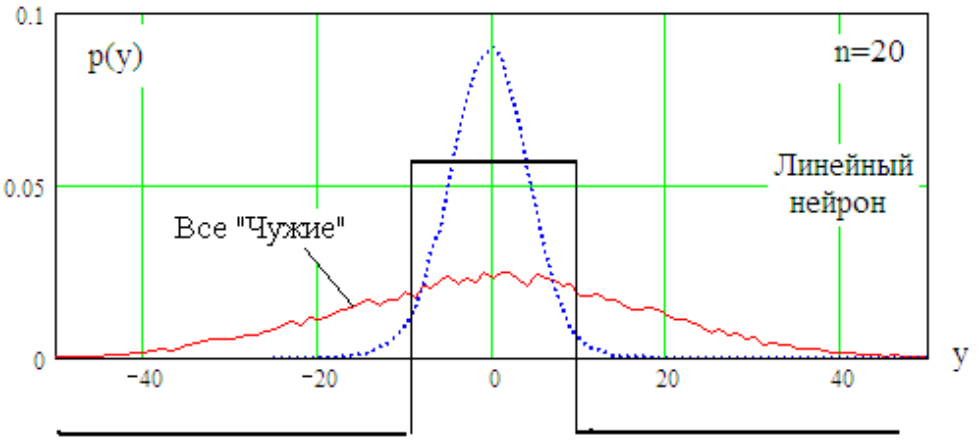

Рис. 2. Распределение данных образа «Свой» (пунктирная линия) и образов «Чужие» на выходе сумматора с 20 входами

Если же подавать на входы обученного сумматора вектор данных образа «Чужой», на выходе получится отклик с иными статистическими параметрами:

$$y_j(\overline{\xi}) = \sum_{i=1}^{20} \left\{ \frac{E(v_i) - \xi_{i,j}}{\sigma(v_i)} \right\}^1. \qquad (2)$$

Из рис. 2 видно, то данные образов «Свой» и данные образов «Чужие» достаточно хорошо разделимы двухпороговым квантователем с двумя выходными состояниями. Очевидно, что при квантовании данных всегда будут возникать с вероятностью P_1 ошибки первого рода (отказ в доступе «Своему»), а также с вероятностью P_2 ошибки второго рода (пропуск «Чужого»). Всегда можно подобрать пороги квантования таким образом, чтобы вероятности первого и второго рода оказались одинаковыми:

$$P_{EE} = P_1 = P_2 . \quad (3)$$

Показатель (3) может быть использован для сравнения качества различных типов нейронов, находящихся в одинаковых условиях.

Оценка мощности сверток квадратичных функционалов, обогащающих биометрические данные вокруг центра многомерного образа «Свой»

Очевидно, что от линейных сверток в пространстве входных данных (1), (2) легко можно перейти к квадратичным сверткам:

$$y_j(\bar{v}) = \sum_{i=1}^{20} \left\{ \frac{E(v_i) - v_{i,j}}{\sigma(\nu_i)} \right\}^2 , \quad (4)$$

$$y_j(\bar{\xi}) = \sum_{i=1}^{20} \left\{ \frac{E(v_i) - \xi_{i,j}}{\sigma(\nu_i)} \right\}^2 . \quad (5)$$

$p(y)$

При этом распределения выходных данных обученного сумматора коренным образом меняются так, как показано на рис. 3.

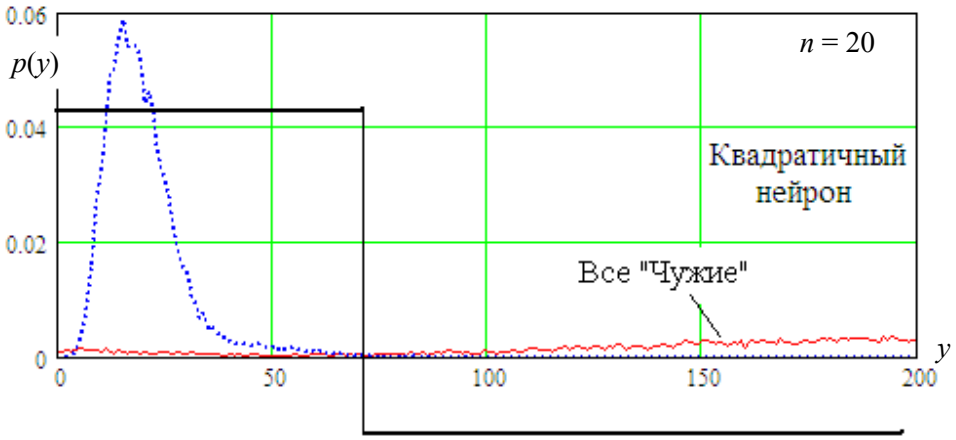

Рис. 3. Распределения выходных состояний сумматора квадратичного нейрона

Для того чтобы получить численное соотношение мощностей линейных и квадратичных нейронов, необходимо сравнить между собой их вероятности ошибок первого и второго рода в точке их совпадения. Это сделано для одних и тех же данных при условии монотонного увеличения числа входов у линейного и квадратичного накопителя. Результаты сравнения приведены на рис. 4.

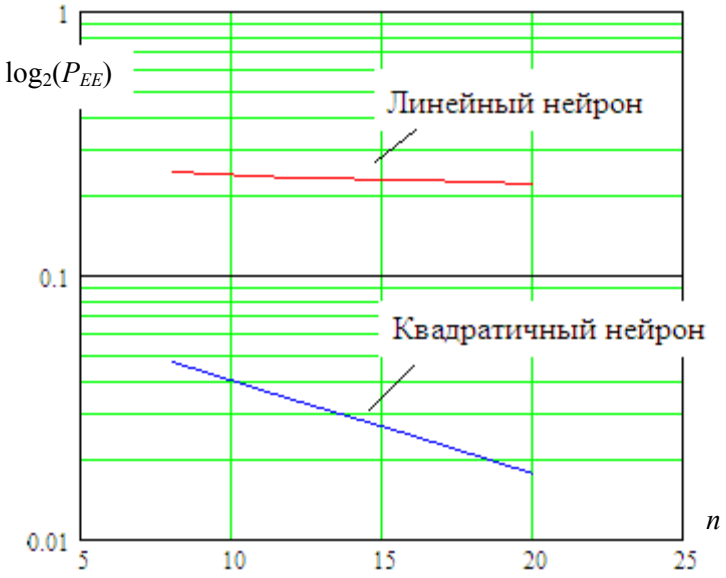

Рис. 4. Снижение вероятностей ошибок линейного и квадратичного нейронов в зависимости от числа входов

Из рис. 4 видно, что мощность квадратичных нейронов намного выше, чем у линейных нейронов. В этом контексте создание нового типа нейросетевых преобразователей биометрия-код путем замены в них линейных обогатителей информации на квадратичные обогатители является перспективным направлением исследований. Можно показать, что линия роста мощности стандартизованного алгоритма обучения [7] всегда будет находиться между линей линейного нейрона (рис. 4) и линией квадратичного нейрона (рис. 4). Более того, один из квадратичных нейронов (нейрон Крамера – фон Мизеса) уже создан [11] и его применение в нейросетевых преобразователях показало результаты лучше, чем у нейросетевых преобразователей с линейным обогащением биометрических данных. Еще более перспективным является использование нейронов среднего геометрического [12, 13], так как мощность статистического критерия среднего геометрического оказывается намного выше классического критерия хи-квадрат.

Заключение

Зарубежные «нечеткие» экстракторы [1–3] дают слишком короткие Биокоды, которые не могут обеспечить серьезную гарантированную защиту данных. Переход к применению нейросетевых преобразователей с линейным обогащением данных [4, 5, 7] решает проблему связывания биометрии с длинным кодом личного высокостойкого ключа. Нейроны преобразователя биометрия-код заранее обучаются обогащать биометрические данные конкретного образа «Свой» и потому лучше работают, чем универсальные избыточные коды с обнаружением и исправлением ошибок. Платить за это приходится повторением входных связей у нескольких нейронов преобразователя, что дает повод для организации атаки Г. Б. Маршалко [10] на нейросетевую защиту.

В свою очередь противодействие атакам Маршалко [10] может быть организовано за счет снижения числа входов у нейронов (повышения мощности нейронов) и за счет увеличения числа выходных состояний у квантователя каждого из нейронов [11]. И тот и другой путь, видимо, должен быть оформлен в виде некоторых рекомендаций или спецификаций. Еще лучше, если будет разработан национальный стандарт по автоматическому обучению сети квадратичных форм, который будет действовать параллельно с уже принятым стандартом [7].

Библиографический список

1. **Dodis, Y.** Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy / Y. Dodis, L. Reyzin, A. Smith // Proc. EUROCRYPT. – 2004. – April 13. – P. 523–540.
2. **Monrose, F.** Cryptographic key generation from voice / F. Monrose, M. Reiter, Q. Li, S. Wetzel // Proc. IEEE Symp. on Security and Privacy, 2001. – P. 202–213.
3. Hao, F. Crypto with Biometrics Effectively / F. Hao, R. Anderson, J. Daugman // IEEE transactions on computers. – 2006. – Vol. 55, № 9. – P. 1073–1074.
4. Нейросетевая защита персональных биометрических данных / Ю. К. Язов, В. И. Волчихин, А. И. Иванов, В. А. Фунтиков, И. Г. Назаров. – М. : Радиотехника, 2012. – 157 с.
5. **Иванов, А. И.** Биометрическая идентификация личности по динамике подсознательных движений : монография / А. И. Иванов. – Пенза : Изд-во ПГУ, 2000. – 178 с.
6. **Гудфеллоу, Я.** Глубокое обучение / Я. Гудфеллоу, И. Бенджио, А. Курвиль. – М. : ДМК Пресс, 2017. – 652 с.
7. ГОСТ Р 52633.5–2011. Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа. – М., 2011.
8. **Иванов, А. И.** Нейросетевые технологии биометрической аутентификации пользователей открытых систем : автореф. дис. … д-ра техн. наук: 05.13.01 «Системный анализ, управление и обработка информации» / А. И. Иванов. – Пенза, 2002. – 34 с.
9. **Волчихин В. И.** Перспективы использования искусственных нейронных сетей с многоуровневыми квантователями в технологии биометрико-нейросетевой аутентификации / В. И. Волчихин, А. И. Иванов, В. А. Фунтиков, Е. А. Малыгина // Известия высших учебных заведений. Поволжский регион. Технические науки. – 2013. – № 4 (28). – С. 86–96.
10. **Marshalko, G. B.** On the security of a neural network-based biometric authentication scheme / G. B. Marshalko // Математические вопросы криптографии. – 2014. – Т. 5, № 2. – С. 87–98.
11. **Волчихин, В. И.** Абсолютно устойчивый алгоритм автоматического обучения сетей вероятностных нейронов «Крамера – фон Мизеса» на малых выборках биометрических данных / В. И. Волчихин, А. И. Иванов, С. Е. Вятчанин, Е. А. Малыгина // Известия высших учебных заведений. Поволжский регион. Технические науки. – 2017. – № 2 (42). – С. 55–65.
12. **Иванов, А. И.** Оценка соотношения мощностей семейства статистических критериев «среднего геометрического» на малых выборках биометрических данных / А. И. Иванов, К. А. Перфилов // Современные охранные технологии и средства обеспечения комплексной безопасности объектов : сб. материалов XI Всерос. НПК. – Пенза ; Заречный, 2016. – С. 223–229.
13. **Иванов, А. И.** Оценка качества малых выборок биометрических данных с использованием дифференциального варианта статистического критерия среднего

геометрического / А. И. Иванов, К. А. Перфилов, Е. А. Малыгина // Вестник Сибирского государственного аэрокосмического университета им. академика М. Ф. Решетнева. – 2016. – № 4 (17). – С. 864–871.

References

1. Dodis Y., Reyzin L., Smith A. *Proc. EUROCRYPT*. 2004, April 13, pp. 523–540.
2. Monrose F., Reiter M., Li Q., Wetzel S. *Proc. IEEE Symp. on Security and Privacy*. 2001, pp. 202–213.
3. Hao F., Anderson R., Daugman J. *IEEE transactions on computers*. 2006, vol. 55, no. 9, pp. 1073–1074.
4. Yazov Yu. K., Volchikhin V. I., Ivanov A. I., Funtikov V. A., Nazarov I. G. *Neyrosetevaya zashchita personal'nykh biometricheskikh dannykh* [Neural network protection of personal biometric data]. Moscow: Radiotekhnika, 2012, 157 p.
5. Ivanov A. I. *Biometricheskaya identifikatsiya lichnosti po dinamike podsoznatel'nykh dvizheniy: monografiya* [Biometric identification of a person by the dynamics of subconscious movements: monograph]. Penza: Izd-vo PGU, 2000, 178 p.
6. Gudfellou Ya., Bendzhio I., Kurvil' A. *Glubokoe obuchenie* [In-depth traning]. Moscow: DMK Press, 2017, 652 p.
7. *GOST R 52633.5–2011. Zashchita informatsii. Tekhnika zashchity informatsii. Avtomaticheskoe obuchenie neyrosetevykh preobrazovateley biometriya-kod dostupa* [State Standard GOST R 52633.5-2011. Information protection. Information protection technique. Automatic learning of neural network "biometrics-access code" converters]. Moscow, 2011.
8. Ivanov A. I. *Neyrosetevye tekhnologii biometricheskoy autentifikatsii pol'zovateley otkrytykh sistem: avtoref. dis. d-ra tekhn. nauk: 05.13.01 «Sistemnyy analiz, upravlenie i obrabotka informatsii»* [Neural network technologies for biometric authentication of open systems users: author's abstract of dissertation to apply for the degree of the candidate of medical sciences: 05.13.01 «System analysis, management and information processing»]. Penza, 2002, 34 p.
9. Volchikhin V. I., Ivanov A. I., Funtikov V. A., Malygina E. A. *Izvestiya vysshikh uchebnykh zavedeniy. Povolzhskiy region. Tekhnicheskie nauki* [University proceedings. Volga region. Engineering sciences]. 2013, no. 4 (28), pp. 86–96.
10. Marshalko G. B. *Matematicheskie voprosy kriptografii* [Mathematical problems of cryptography]. 2014, vol. 5, no. 2, pp. 87–98.
11. Volchikhin V. I., Ivanov A. I., Vyatchanin S. E., Malygina E. A. *Izvestiya vysshikh uchebnykh zavedeniy. Povolzhskiy region. Tekhnicheskie nauki* [University proceedings. Volga region. Engineering sciences]. 2017, no. 2 (42), pp. 55–65.
12. Ivanov A. I., Perfilov K. A. *Sovremennye okhrannye tekhnologii i sredstva obespecheniya kompleksnoy bezopasnosti ob"ektov: sb. materialov XI Vseros. NPK* [Modern security technologies and facilities for providing complex security of facilities: proceedings of XI All-Russian scientific and practical conference]. Penza; Zarechnyy, 2016, pp. 223–229.
13. Ivanov A. I., Perfilov K. A., Malygina E. A. *Vestnik Sibirskogo gosudarstvennogo aerokosmicheskogo universiteta im. akademika M. F. Reshetneva* [Bulletin of Siberian State Aerospace University]. 2016, no. 4 (17), pp. 864–871.

Волчихин Владимир Иванович
доктор технических наук, профессор, президент Пензенского государственного университета (Россия, г. Пенза, ул. Красная, 40)

E-mail: president@pnzgu.ru

Volchikhin Vladimir Ivanovich
Doctor of engineering sciences, professor, the President of Penza State University (40 Krasnaya street, Penza, Russia)

Иванов Александр Иванович
доктор технических наук, доцент, начальник лаборатории биометрических и нейросетевых технологий, Пензенский научно-исследовательский электротехнический институт (Россия, г. Пенза, ул. Советская, 9)

E-mail: ivan@pniei.penza.ru

Ivanov Aleksandr Ivanovich
Doctor of engineering sciences, associate professor, head of the laboratory of biometric and neural network technologies, Penza Research Institute of Electrical Engineering (9 Sovetskaya street, Penza, Russia)

Малыгина Елена Александровна
кандидат технических наук, научный сотрудник, межотраслевая лаборатория тестирования биометрических устройств и технологии, Пензенский государственный университет (Россия, г. Пенза, ул. Красная, 40)

E-mail: mal890@yandex.ru

Malygina Elena Aleksandrovna
Candidate of engineering sciences, research worker, the interindustrial testing laboratory of biometric devices and technologies, Penza State University (40 Krasnaya street, Penza, Russia)

Юнин Алексей Петрович
ведущий специалист, Пензенский научно-исследовательский электротехнический институт (Россия, г. Пенза, ул. Советская, 9)

E-mail: alexey_82@mail.ru

Yunin Aleksey Petrovich
Lead expert, Penza Research Institute of Electrical Engineering (9 Sovetskaya street, Penza, Russia)

УДК 519.24; 53; 57.017

Волчихин, В. И.

Соотношение мощности нейронов с линейным и квадратичным обогатителями биометрических данных / В. И. Волчихин, А. И. Иванов, Е. А. Малыгина, А. П. Юнин // Известия высших учебных заведений. Поволжский регион. Технические науки. – 2018. – № 1 (45). – С. 17–25. – DOI 10.21685/2072-3059-2018-1-2.