

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004. 093.1

DOI: 10.21822/2073-6185-2023-50-4-75-84



Оригинальная статья /Original article

**К вопросу обеспечения защищенного доступа к информационным системам
с применением биометрической аутентификации на основе нечеткого образа**

личности пользователя и нейросетевых преобразований

О.И. Бокова¹, С.В. Канавин², Н.С. Хохлов², И.В. Гилев², Л.А. Лекарь³

¹ООО «Каскад»,

¹115230, г. Москва, Каширское шоссе, 17 к. 5 стр. 3, Россия,

²Воронежский институт МВД России,

²394065, г. Воронеж, пр-т. Патриотов, 53, Россия,

³Академия управления МВД России,

³125171, г. Москва, ул. Зои и Александра Космодемьянских ул., 8, Россия

Резюме. Цель. В современных условиях для доступа к информационным системам применяются технологии криптографической аутентификации личности, основанные на обработке биометрической информации и преобразовании биометрических образов пользователя в его персональный код доступа. Актуальным направлением исследований является применение нейросетевых технологий при организации защищенного доступа к информационным системам. Средства биометрической аутентификации могут быть отнесены к высоконадежным, только если в их состав введены криптографические механизмы аутентификации, работающие совместно с биометрическими механизмами аутентификации через преобразование биометрических образов в однозначный криптографический код доступа. В этом случае совокупность биометрических идентификаторов личности пользователя формируют его нечеткий образ, который используется в дальнейшем при проведении аутентификации. Целью исследования является разработка алгоритма обеспечения защищенного доступа к информационным системам с применением биометрической аутентификации на основе нечеткого образа личности пользователя и нейросетевых преобразований. **Метод.** Разработка алгоритма основана на использовании методов нечеткой логики и аппарата нейронных сетей. **Результат.** В работе выявлены особенности биометрической идентификации личности пользователя информационных систем. Предложен алгоритм обеспечения защищенного доступа к информационным системам с применением биометрической аутентификации на основе нечеткого образа личности пользователя и нейросетевых преобразований. **Вывод.** На основе двухэтапной аутентификации личности пользователя реализован защищенный доступ к информационным системам зарегистрированных пользователей. Приведен листинг программного кода на языке Python для создания и обучения нейронной сети классификатора биоидентификаторов. Материалы статьи представляют практическую ценность для специалистов в области обеспечения защищенного доступа к информационным системам с применением искусственного интеллекта.

Ключевые слова: информационная безопасность; биометрические механизмы аутентификации; биометрические идентификаторы; нейросетевая система преобразования, криптографический ключ, нейросетевая система преобразования биометрических идентификаторов

Для цитирования: О.И. Бокова, С.В. Канавин, Н.С. Хохлов, И.В. Гилев, Л.А. Лекарь. К вопросу обеспечения защищенного доступа к информационным системам с применением биометрической аутентификации на основе нечеткого образа личности пользователя и нейросетевых преобразований. Вестник Дагестанского государственного технического университета. Технические науки. 2023; 50(4):75-84. DOI:10.21822/2073-6185-2023-50-4-75-84

On the issue of ensuring secure access to information systems using biometric authentication based on a fuzzy image of the user's identity and neural network transformations

O.I. Bokova¹, S.V. Kanavin², N.S. Khokhlov², I.V. Gilev², L.A. Lekar³

¹LLC «Cascade»,

¹17 Kashirskoe highway, k. 5 building 3, Moscow 115230, Russia,

²Voronezh Institute of the Ministry of Internal Affairs of Russia,

²53 Patriotov Ave., Voronezh 394065, Russia,

³Academy of Management of the Ministry of Internal Affairs of Russia,

³8 Zoe and Alexandra Kosmodemyanskikh St., Moscow 125171, Russia

Abstract. Objective. In modern conditions, cryptographic personal authentication technologies are used to access information systems, based on processing biometric information and converting the user's biometric images into his personal access code. A current area of research is the use of neural network technologies in organizing secure access to information systems. Biometric authentication tools can be classified as highly reliable only if they include cryptographic authentication mechanisms that work together with biometric authentication mechanisms through the conversion of biometric images into a unique cryptographic access code; in this case, a set of biometric identifiers of the user's identity form his fuzzy image, which is used later during authentication. The purpose of the study is to develop an algorithm for providing secure access to information systems using biometric authentication based on a fuzzy image of the user's identity and neural network transformations. **Method.** The development of the algorithm is based on the use of fuzzy logic methods and neural networks. **Result.** The work reveals the features of biometric identification of the user of information systems. An algorithm is proposed for providing secure access to information systems using biometric authentication based on a fuzzy image of the user's personality and neural network transformations. **Conclusions.** Based on two-step authentication of the user's identity, secure access to the information systems of registered users is implemented. A listing of the program code in Python for creating and training a neural network of a biointentifier classifier is provided. The materials of the article are of practical value for specialists in the field of providing secure access to information systems using artificial intelligence.

Keywords: information security; biometric authentication mechanisms; biometric identifiers; neural network transformation system, cryptographic key, neural network transformation system for biometric identifiers

For citation: O.I. Bokova, S.V. Kanavin, N.S. Khokhlov, I.V. Gilev, L.A. Lekar. On the issue of ensuring secure access to information systems using biometric authentication based on a fuzzy image of the user's identity and neural network transformations. Herald of Daghestan State Technical University. Technical Sciences. 2023; 50(4):75-84. DOI:10.21822/2073-6185-2023-50-4-75-84

Введение. В соответствии с определением из ГОСТ Р-58833-2020 под термином аутентификация понимаются действия по проверке подлинности субъекта и/или объекта доступа, а также проверки принадлежности субъекту доступа и/или объекту доступа предъявленного идентификатора доступа и аутентификационной информации. В качестве идентификатора доступа или аутентификационной информации при входе в информационную систему могут применяться биометрические персональные данные – сведения которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность. Согласно приведенной терминологии, системе необходимо убедиться в предоставлении пользователем данных.

Воспроизводство любых заранее заданных кодов (ключей, паролей, слов и т.д.) возможно из биометрических данных без их сохранения. На настоящий момент апробированы или имеют перспективы широкого практического использования в соответствии с ГОСТ Р-52633.0-2006 следующие биометрические механизмы:

– анализ кровеносных сосудов глазного дна;

- анализ радужной оболочки глаза;
- двухмерный и трехмерный анализы геометрических особенностей лица в видимом и инфракрасном спектрах света;
- анализ особенностей геометрии ушных раковин;
- анализ особенностей голоса;
- анализ особенностей папиллярных рисунков пальцев;
- анализ геометрии ладони, включая рисунки складок кожи ладони и папиллярные рисунки различных фрагментов кожи ладони;
- анализ рисунка кровеносных сосудов, складок кожи тыльной стороны ладони и т.д.

С учетом результатов анализа мирового рынка биометрических систем следует отметить ежегодный рост практики применения биометрических систем в разных отраслях науки и техники. Приведенная на рис. 1 диаграмма использования биометрических данных показывает рост таких идентификационных признаков как двухмерный и трехмерный анализы геометрических особенностей лица, анализ радужной оболочки глаза.

В 2016 году Techportal.ru опубликовал прогноз развития структуры биометрических идентификационных признаков на 2020 год по сравнению с 2014 годом. Из приведенной на рис. 1 диаграммы можно сделать выводы о том, что кроме идентификации личности по отпечаткам пальцев все большее распространение получают системы, использующие в качестве биометрических идентификаторов лицо, радужную оболочку глаз, голос, вены и др.

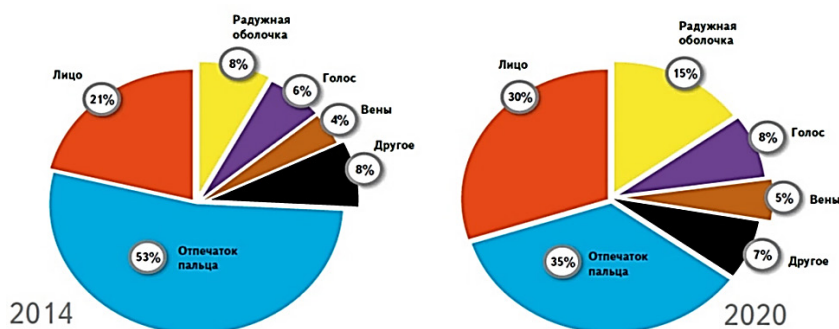


Рис. 1. Диаграмма статистики использования биометрических данных

Fig. 1. Diagram of statistics on the use of biometric data

Каждый из перечисленных выше механизмов биометрической аутентификации способен давать свой уникальный биометрический образ легального пользователя – образ «Свой». Биометрический образ злоумышленника, пытающегося преодолеть биометрическую защиту, формирует образ «Чужой». Важным для систем с биометрической аутентификацией является то, чтобы биометрические данные не должны сохраняться. Воспроизводство любых заранее заданных кодов (ключей, паролей, слов и т.д.) осуществляется из биометрических данных без их сохранения.

Вопросам обеспечения биометрической многофакторной аутентификации посвящены научные работы [1-6]. С.А. Мишин рассматривает применение искусственного интеллекта для ведения базы данных элементов внешности человека [1]. Т.И. Лапина и др. для управления доступом к информационным ресурсам в информационных системах рассматривает подход многофакторной аутентификации и анализа биометрических данных [2-4]. Е.А. Сулавко и др. для комплексирования независимых биометрических признаков при распознавании субъектов применяет подход на основе сетей квадратичных форм, персептронов и меры хи-модуль [3]. В работе [6] уделено внимание проекту третьего национального стандарта России по быстрому автоматическому обучению больших сетей корреляционных нейронов на малых обучающих выборках биометрических данных. Проведенный анализ работ показывает, что представленные в них способы управления доступом к информационным системам, технологии, модели, методы аутентификации используются для решения прикладных задач в своих предметных областях. Вопросы обеспечения комплексной безопасности информации отражены не в полном объеме и требуют более детальной проработки.

С учетом проведенного сравнительного анализа существующих технологий аутентификации по факторам аутентификации можно выделить следующие недостатки. При аутентификации паролями или токенами недостатком будет являться отсутствие связи с физиологическими особенностями оператора. Для биометрических факторов аутентификации недостатком будет выступать возможность сохранения биометрической информации в базах данных и в случае их кражи последствия нейтрализовать невозможно [7]. К другим недостаткам аутентификации можно отнести тот факт, что она проводится только при входе в систему и отвлекает оператора от выполнения своих функций.

Для совершенствования процедуры аутентификации при входе в информационную систему можно рассмотреть следующие варианты: использовать сложные пароли, которые практически невозможно запомнить; воспроизводить сложные пароли с помощью биометрических данных оператора в сочетании с простыми паролями, например с PIN – кодом; воспроизводить сложные пароли без отвлечения оператора с помощью с помощью биометрических данных оператора по двум биометрическим параметрам: лицо и вены. Сканер вен встраивать в мышку. В качестве примеров реализации информационных систем, где используется биометрическая идентификация, можно привести следующие:

- программные библиотеки для аутентификации по лицу, работающие под ОС Windows, Linux, Android, iOS;
- приложение «Биосейф» под ОС Android;
- национальная система платежных карт (НСПК) «МИР»;
- приложение «Электронный кошелек» под Android и iOS;
- библиотеки для внедрения в приложение «Сбербанк онлайн» и другие приложения;
- библиотеки для внедрения в приложение «Персональный медицинский помощник» и в другие медицинские системы.

Рассмотрим возможные области применения защищенного доступа к информационным системам с применением биометрической аутентификации и нейросетевых преобразований в интересах МВД России. Развитие данного направления позволит усовершенствовать процедуру аутентификации пользователей при входе в систему как непосредственно, так и дистанционно в момент управления процессом.

В этом случае процедура аутентификации может носить неотвлекающий характер и может проводиться по лицу или венам. Электронные удостоверения личности сотрудников для аутентификации не требуют физических носителей. Документы хранятся в центре обработки данных или в персональных мобильных устройствах. Биометрические данные и ключи шифрования нигде не хранятся. Также биометрическая идентификация может применяться в сфере электронной подписи. В этом случае имеется непосредственная связь электронной подписи с физиологическими особенностями владельца и отсутствует сам физический носитель ключа. Даная технология и ее реализация будет приведена далее.

Постановка задачи. Целью исследования является разработка алгоритма обеспечения защищенного доступа к информационным системам с применением биометрической аутентификации на основе нечеткого образа личности пользователя и нейросетевых преобразований.

Методы исследования. Технология Биометрия – Нейронные сети – Криптография (БНК) в настоящее время применяется для обеспечения защищенного доступа к информационным системам с применением биометрической аутентификации. Объектом защиты в случае применения технологии БНК являются номера связей и весовые коэффициенты искусственной нейронной сети преобразователя «биометрия – код», хранимые в нейросетевом биометрическом контейнере [8]. После того как нейронная сеть преобразователя «биометрия – код» обучена в соответствии с ГОСТ Р 52633. 5, каждый ее нейрон может быть представлен двумя таблицами (таблицей связей и таблицей весовых коэффициентов) [9]. Эта ситуация отображена на рис. 2.

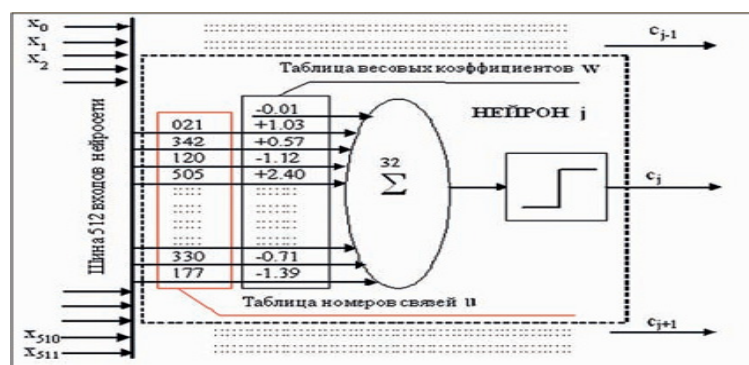


Рис. 2. Пример фрагмента структуры искусственной нейронной сети

Fig. 2. Example of a fragment of the structure of an artificial neural network

Описание технологии приведено в технической спецификации ТК 26 «Защита нейросетевых биометрических контейнеров с использованием криптографических алгоритмов» и регламентируется серией документов ГОСТ Р 52633. Меры противодействия атакам по извлечению ключа из биометрического контейнера рассмотрены в технической спецификации №ТС 26.2.002-2020 технического комитета ТК 26 («Криптографическая защита информации»). В этом же документе приведена методика оценки стойкости нейронной сети к атакам извлечения ключа. Следует отметить, что методика не позволяет рассчитать требуемую стойкость, она позволяет оценить лишь нижнюю границу стойкости. Реальные показатели стойкости всегда будут выше указанных граничных значений.

Процедура оценки стойкости занимает несколько секунд и осуществляется сразу после обучения нейронной сети. Результат оценки сообщается оператору – владельцу биометрических данных для принятия решения [10]. Если по мнению владельца стойкость недостаточна, то он должен либо отказаться от использования технологии, либо принять меры по увеличению стойкости – дополнительно использовать жесты, пароль, токен и т.д. [11, 12]. Принцип работы «широкой» нейронной сети приведен на рис. 3.

«Широкая» нейронная сеть реализует формулу: $A+B=C$, где A – персональные биометрические признаки владельца пароля $\pm \Delta$, Δ – нестабильность биометрических данных B – контейнер – коэффициенты нейронной сети C – пароль или ключ шифрования секретов. В базе данных хранится только слагаемое B .



Рис. 3. Принцип работы «широкой» нейронной сети

Fig. 3. Operating principle of a «wide» neural network

По сути, B – это половина пароля. Вторая половина – это биометрические данные владельца. Зная только B , нельзя вычислить ни C , ни A . Классификация по персональным биометрическим признакам «Свой» – «Чужой» приведена на рис. 4.



Рис. 4. Классификация по персональным биометрическим признакам «Свой» – «Чужой»

Fig. 4. Classification according to personal biometric characteristics «Own» – «Alien»

Обучение «широкой» нейронной сети является сложным процессом, но с правильным подходом и методами можно достичь хороших результатов. Алгоритм обучения «широкой» нейронной сети приведен на рис. 5.



Рис. 5. Обучение «широкой» нейронной сети

Fig. 5. Training a «wide» neural network

Обсуждение результатов. Рассмотренный алгоритм аутентификации при использовании биоидентификаторов не лишен недостатков, один из которых выражается в избыточности выполняемых вычислительных операций за счет вычисления криптографических ключей и определения на их основании близости образов. Авторами предлагается не вычислять сумму S для каждого предъявляемого образа, а осуществлять проверку на подлинность с применением в составе системы дополнительной нейронной сети, классифицирующей образы на «Свой» – «Чужой» на основе вычисления нечеткого образа личности пользователя. Если образ классифицирован как «Чужой» для него нет необходимости вычислять сумму S . В этом случае будет реализована двухэтапная аутентификация, что позволит обеспечить защищенный доступ к информационным системам зарегистрированных пользователей. Подробнее данный алгоритм будет рассмотрен в следующем разделе

Алгоритм обеспечения защищенного доступа к информационным системам с применением биометрической аутентификации на основе нечеткого образа личности пользователя и нейросетевых преобразований. Авторами предлагается в качестве первого

этапа работы алгоритма аутентификации составление нечёткого образа личности на основе следующих биоидентификаторов:

1. «Геометрических особенностей лица»;
2. «Особенностей геометрии ушных раковин»;
3. «Особенностей голоса»;
4. «Особенности папиллярных рисунков пальцев».

Пример составления нечеткого образа лица представлен на рис. 6.



Рис. 6. Пример анализа биоидентификатора «Геометрические особенности лица»

Fig. 6. Example of analysis of the bioidentifier «Geometric facial features»

Рис. 6 иллюстрирует пример составления нечеткого образа с учетом геометрии лица. Нечеткий образ каждого человека будет иметь свое уникальное расположение точек на овале лица, а также характеризоваться определенным расстоянием между ними. По аналогии с нечетким образом человека по особенностям лица составляются его образы и по другим трем идентификаторам. Общий нечеткий образ личности составляется из суммы ее четырех биоидентификаторов. Пример общего образа личности приведен на рис. 7.



Рис. 7. Пример нечеткого образа личности

Fig. 7. Example of a fuzzy personality image

Для создания нейронной сети, осуществляющей классификацию биоидентификаторов на соответствие образу возможно разделить на следующие этапы:

1. Сбор данных. Сбор достаточного количества примеров биоидентификаторов, которые нужно классифицировать. Например, для отпечатков пальцев, понадобятся изображения отпечатков пальцев разных людей.

2. Подготовка данных. Обработка данных для удобства работы с ними. Например, для изображений отпечатков пальцев, можно применить методы обработки изображений, чтобы нормализовать размеры и улучшить качество изображений.

3. Создание модели нейронной сети. Определение архитектуры нейронной сети. В зависимости от типа биоидентификатора, вы можете использовать различные архитектуры нейронных сетей, такие как сверточные нейронные сети (CNN) для изображений или рекуррентные нейронные сети (RNN) для голосовых данных.

4. Обучение модели. Используйте подготовленные данные для обучения нейронной сети. Разделите данные на обучающую и тестовую выборки. Затем обучите модель на обучающей выборке, настраивая веса и параметры сети с помощью метода обратного распространения ошибки.

5. Оценка модели. После обучения оцените производительность модели на тестовой выборке. Используйте метрики, такие как точность, полноту, F1-меру и матрицу ошибок,

чтобы измерить качество классификации.

6. Тестирование модели. После успешной оценки модели, протестируйте ее на новых данных, чтобы убедиться в ее работоспособности.

7. Настройка и улучшение. В случае неудовлетворительных результатов можно провести дополнительные итерации обучения, изменить архитектуру сети или внести другие изменения для улучшения производительности модели.

Соответствие предъявленного идентификатора личности определяется на основании нечетких оценок, выставляемых каждому из составляющих образа нейронной сетью. На основании данных оценок нейронная сеть принимает решение о соответствии идентификаторов нечеткому образу личности и соответствия самого образа, основанного на суммарной оценке совокупности трех идентификаторов, при этом характеризуя их следующими состояниями: соответствует полностью, не соответствует или соответствует частично. При этом показатель стабильности биометрического параметра вычисляется по формуле $A(v_i) = \frac{v_{\text{Чужой}}(v_i)}{v_{\text{Свой}}(v_i)}$ где $v_{\text{Чужой}}(v_i)$ – стандартное отклонение i -го биометрического параметра множества образов «Чужой»; $v_{\text{Свой}}(v_i)$ – стандартное отклонение i -го биометрического параметра множества образов «Свой».

Следует отметить, что решения принимаются нейронной сетью на основе нечетких правил и основанных на них базы знаний. Пример определения принадлежности идентификатора представлен на рис. 8.

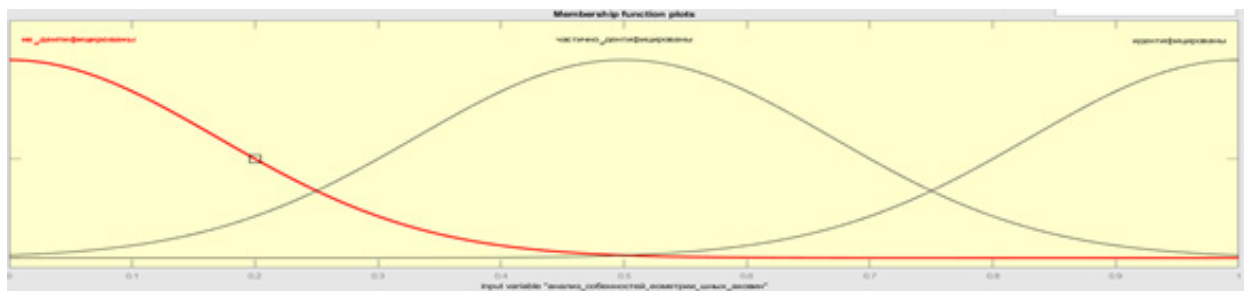


Рис. 8. Пример нечеткого идентификатора личности «Особенностей геометрии ушных раковин»

Fig. 8. Example of a fuzzy personal identifier «Features of the geometry of the auricles»

Ниже приведен листинг программного кода на языке Python для создания и обучения нейронной сети классификатора биоидентификаторов с использованием библиотеки TensorFlow:

```
``python
import tensorflow as tf
from tensorflow.keras import layers
# Загрузка и предобработка данных
# Пример загрузки и предобработки данных отпечатков пальцев
# Загрузка данных
train_data, train_labels = load_fingerprint_data('train_data.csv')
test_data, test_labels = load_fingerprint_data('test_data.csv')
# Предобработка данных
train_data = preprocess_fingerprint_data(train_data)
test_data = preprocess_fingerprint_data(test_data)
# Определение архитектуры нейронной сети
model = tf.keras.Sequential([
    layers.Dense(64, activation='relu', input_shape=(input_size,)),
    layers.Dense(64, activation='relu'),
    layers.Dense(num_classes, activation='softmax')
])
# Компиляция модели
model.compile(optimizer='adam',
              loss=tf.keras.losses.SparseCategoricalCrossentropy(from_logits=True),
              metrics=['accuracy'])
# Обучение модели
```



```
model.fit(train_data, train_labels, epochs=10, batch_size=32, validation_data=(test_data, test_labels))
# Оценка модели
test_loss, test_acc = model.evaluate(test_data, test_labels, verbose=2)
print('Test accuracy:', test_acc)
# Прогнозирование классов для новых данных
predictions = model.predict(new_data)
```

В приведенном программном коде реализована полносвязная нейронная сеть с двумя скрытыми слоями, активацией ReLU и выходным слоем с функцией активации softmax для классификации. Модель компилируется с оптимизатором Adam и функцией потерь SparseCategoricalCrossentropy. Модель обучается на обучающих данных в течение 10 эпох с размером пакета 32. После обучения модель оценивается на тестовых данных и определяется точность классификации на тестовом наборе биоидентификаторов личности. Далее работа алгоритма производится в соответствии с рассмотренными ранее шагами. Примерами применения таких систем являются доступ к различного рода базам данных, оперативное управление при принятии важных решений, а также системы управления вооружением, что сокращает временные и материальные затраты на сбор информации, при этом обеспечивается оперативность проверки и установления личности гражданина.

Вывод. В работе выявлены особенности биометрической идентификации личности пользователя информационных систем. Предложен алгоритм обеспечения защищенного доступа к информационным системам с применением биометрической аутентификации на основе нечеткого образа личности пользователя и нейросетевых преобразований.

Авторами предлагается не вычислять сумму C для каждого предъявляемого образа, а осуществлять проверку на подлинность с применением в составе системы дополнительной нейронной сети, классифицирующей образы на «Свой» – «Чужой» на основе вычисления нечеткого образа личности пользователя. Если образ классифицирован как «Чужой» для него нет необходимости вычислять сумму C .

В этом случае будет реализована двухэтапная аутентификация, что позволит обеспечить защищенный доступ к информационным системам зарегистрированных пользователей. Приведен пример программного кода на языке Python для создания и обучения нейронной сети классификатора биоидентификаторов с использованием библиотеки TensorFlow. Материалы статьи представляют практическую ценность для специалистов в области обеспечения защищенного доступа к информационным системам с применением искусственного интеллекта.

Библиографический список:

1. Рутковская Д. Нейронные сети, генетические алгоритмы и нечеткие системы / Д. Рутковская, М. Иванов А.И., Фунтиков В.А., Ефимов О.В. Нейросетевая защита биометрических данных пользователя, а также его личного криптографического ключа при локальной и дистанционной аутентификации. Вопросы защиты информации. 2008. – С. 25–27.
2. Чуйков А.В., Вульфин А.М., Васильев В.И. Нейросетевая система преобразования биометрических признаков пользователя в криптографический ключ. Доклады ТУСУР. 2018. – С. 35–41.
3. Волчихин В.И., Иванов А.И., Фунтиков В.А., Малыгина Е.А. Перспективы использования искусственных нейронных сетей с многоуровневыми квантователями в технологии биометрико-нейросетевой аутентификации. Известия высших заведений. Поволжский регион. 2013. – С. 86–96.
4. Мишин С.А., Мишин А.В. Применение технологий искусственного интеллекта для ведения базы данных элементов внешности человека. Вестник Воронежского института МВД России. 2022. – С. 87–96.
5. Лапина Т.И., Димов Э.М., Петрик Е.А., Лапин Д.В. Управление доступом к информационным ресурсам в информационных системах. Моделирование, оптимизация и информационные технологии. 2018; 6(4). DOI:10.26102/2310-6018/2018.23.4.039 URL:https://moit.vivt.ru/wp-content/uploads/2018/10/LapinaSoavtors_4_18_3.pdf.
6. Сулавко А.Е., Еременко А.В., Толкачева Е.В., Борисов Р.В. Комплексирование независимых биометрических признаков при распознавании субъектов на основе сетей квадратичных форм, персептронов и меры хи-модуль. Информационно-управляющие системы. 2017. – С.50–62.
7. Исмагилов Р.Ф., Лушников Н.Д., Исмагилова А.С. Конструирование модели обучающей нейронной сети для биометрической многофакторной аутентификации пользователя информационной системы. Вопросы защиты информации. 2023. – С.19–23.
8. Иванов А.И., Сулавко А.Е. Проект третьего национального стандарта России по быстрому автоматическому обучению больших сетей корреляционных нейронов на малых обучающих выборках биометрических данных. Вопросы кибербезопасности. 2021. – С.84–93.

9. Еременко А.В., Сулавко А.Е., Толкачева Е.В., Левитская Е.А. Метод защиты текстовых документов на электронных и бумажных носителях на основе скрытого биометрического идентификатора субъекта, получаемого из подписи. *Инфокоммуникационные технологии*. 2016. – С.628–634.
10. Метод многофакторной аутентификации: обеспечение информационной безопасности в инновационных системах Лазарев А.И., Заенчковский А.Э., Халин В.Г., Масютин С.А. *Экономика и предпринимательство*. 2022. – С.1086–1090.
11. Хорев П.Б. Многофакторная аутентификация пользователей при удаленном доступе к информационным системам *Информационно-технологический вестник*. –2022. – С.20–25.
12. Silasai, O.; Khowfa, W. The Study on Using Biometric Authentication on Mobile Device. *NU Int. J. Sci.* 2020. – pp.90–110.

References

1. Rutkovskaya D. Neural networks, genetic algorithms and fuzzy systems / D. Rutkovskaya, M. Ivanov A.I., Funtikov V.A., Efimov O.V. Neural network protection of the user's biometric data, as well as his personal cryptographic key during local and remote authentication. *Information security issues*. 2008; 25–27. (In Russ)
2. Chuikov A.V., Vulfin A.M., Vasiliev V.I. A neural network system for converting user biometric characteristics into a cryptographic key. *TUSUR reports*. 2018; 35–41. (In Russ)
3. Volchikhin V.I., Ivanov A.I., Funtikov V.A., Malygina E.A. Prospects for the use of artificial neural networks with multi-level quantizers in biometric-neural network authentication technology. *News of higher institutions. Volga region*. 2013; 86–96. (In Russ)
4. Mishin S.A., Mishin A.V. Application of artificial intelligence technologies to maintain a database of elements of human appearance. *Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia*. 2022; 87–96. (In Russ)
5. Lapina T.I., Dimov E.M., Petrik E.A., Lapin D.V. Controlling access to information resources in information systems. *Modeling, optimization and information technology*. 2018;6(4). DOI: 10.26102/2310-6018/2018.23.4.039 7. URL: https://moit.vivt.ru/wp-content/uploads/2018/10/LapinaSoavtors_4_18_3.pdf. (In Russ)
6. Sulavko A.E., Eremenko A.V., Tolkacheva E.V., Borisov R.V. Integration of independent biometric features in subject recognition based on networks of quadratic forms, perceptrons and chi-modulus measures. *Information and control systems*. 2017; 50–62. (In Russ)
7. Ismagilov R.F., Lushnikov N.D., Ismagilova A.S. Construction of a training neural network model for biometric multi-factor authentication of an information system user. *Information security issues*. 2023;19–23. (In Russ)
8. Ivanov A.I., Sulavko A.E. Project of the third Russian national standard for fast automatic training of large networks of correlation neurons on small training samples of biometric data. *Cybersecurity issues*. 2021;84–93. (In Russ)
9. Eremenko A.V., Sulavko A.E., Tolkacheva E.V., Levitskaya E.A. A method for protecting text documents on electronic and paper media based on a hidden biometric identifier of a subject obtained from a signature. *Infocommunication technologies*. 2016; 628–634. (In Russ)
10. Multi-factor authentication method: ensuring information security in innovative systems Lazarev A.I., Zaenchkovsky A.E., Khalin V.G., Masyutin S.A. *Economics and entrepreneurship*. 2022;1086–1090. (In Russ)
11. Khorev P.B. Multi-factor user authentication for remote access to information systems *Information and Technology Bulletin*. 2022; 20–25. (In Russ)
12. Silasai, O.; Khowfa, W. The Study on Using Biometric Authentication on Mobile Device. *NU Int. J. Sci.* 2020; 90–110.

Сведения об авторах:

Бокова Оксана Игоревна, доктор технических наук, профессор, o.i.bokova@gmail.com.

Канавин Сергей Владимирович, кандидат технических наук, доцент, доцент кафедры инфокоммуникационных систем и технологий, sergejj-kanavin@rambler.ru; ORCID: 0000-0003-0575-2773

Хохлов Николай Степанович, доктор технических наук, профессор, профессор кафедры инфокоммуникационных систем и технологий, nikolayhohlov@rambler.ru.

Гилев Игорь Владимирович, преподаватель кафедры инфокоммуникационных систем и технологий, gileviv@bk.ru.

Лекарь Людмила Антоновна, кандидат технических наук, доцент кафедры информационных технологий, antonna47@bk.ru.

Information about authors:

Oksana I. Bokova, Dr. Sci. (Eng.), Prof., o.i.bokova@gmail.com.

Sergey V. Kanavin, Cand. Sci. (Eng.), Assoc. Prof., Assoc. Prof., of the Department of Infocommunication Systems and Technologies, sergejj-kanavin@rambler.ru; ORCID: 0000-0003-0575-2773

Nikolay S. Khokhlov, Dr. Sci. (Eng.), Prof., Prof., of the Department of Infocommunication Systems and Technologies, nikolayhohlov@rambler.ru.

Igor V. Gilev, Lecturer, Department of infocommunication systems and technologies, gileviv@bk.ru.

Lyudmila A. Lekar, Cand. Sci. (Eng.), Assoc. Prof., Department of Information Technologies, antonna47@bk.ru.

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/ Received 18.10.2023.

Одобрена после рецензирования / Reviced 01.11.2023.

Принята в печать /Accepted for publication 01.11.2023.