УДК 004.93

ПРОГРАММНЫЙ МОДУЛЬ ХЭШИРОВАНИЯ БИОМЕТРИЧЕСКИХ ДАННЫХ ПОЛЬЗОВАТЕЛЯ

© **А. С. Исмагилова, Н. Д. Лушников**

Уфимский университет науки и технологий,
450076, г. Уфа, ул. Заки Валиди, 32
E-mail: ismagilovaas@yandex.ru, luschnikovnikita@yandex.ru

Рассмотрены особенности автоматизированной реализации хэширования биометрических персональных данных, информационных ресурсов пользователя, информационной системы в целом. Основой созданной математической модели является искусственная нейронная сеть, предназначенная для хэширования биометрических образов в папке администратора учётной записи с применением математических методов. Объект исследования — информационные системы. Предмет исследования — средства защиты информации с использованием биометрической многофакторной аутентификации.

Ключевые слова: информационные системы, нейронные сети, защита информации, программный комплекс.

DOI: 10.15372/AUT20230403

Введение. В настоящее время большая часть сфер деятельности взаимосвязана с цифровизацией и защитой информации. Программные решения, представленные на рынке для хэширования данных, соответствуют требуемому уровню криптостойкости в силу более длительного анализа алгоритма хэширования и его программной реализации. В том числе к характеристикам криптостойкости системы можно отнести такой аспект, как возможность взлома криптосистемы и несанкционированного чтения данных. Но в будущем при развитии информационных систем и повышении производительной мощности автоматизированных рабочих мест, которые с большей долей вероятности будут представлены в виде квантовых компьютеров в обозримом будущем, этого требования может оказаться недостаточно. На настоящий момент уже существуют нейроморфные процессоры (Intel) и, согласно актуальным данным Национального исследовательского центра «Курчатовский институт» и Санкт-Петербургского государственного электротехнического университета (ЛЭТИ) им. В. И. Ульянова, нейроморфные компьютеры. Именно поэтому необходимо разработать тот программный продукт, который будет соответствовать основным критериям защиты информационных ресурсов пользователей девайсов от несанкционированных действий злоумышленников. В работе [1], к примеру, рассмотрены подходы к распознаванию спуфинг-атак, дана оценка их устойчивости к изменению условий записи информации.

Цель исследования — повышение эффективности криптографических решений, необходимых для защиты биометрических персональных данных пользователей информационной системы.

Структура модели хэширования. Программный модуль предназначен для кодирования биометрических персональных данных, которые являются неотъемлемой частью программного комплекса авторизации пользователей информационной системы (рис. 1). Данный софт реализован на языке программирования Python 3.8 с применением таких библиотек, как hashlib, cryptography, binascii, itertools, numpy и struct, для генерации и вывода ключей. Для получения ключа необходимо пройти этапы распознавания личности по голосу (коэффициенты LPC, PLP, MFCC, CQCC, SCF) и по изображению с использованием локальных бинарных паттернов (LBP). В результате как голос, так и изображение

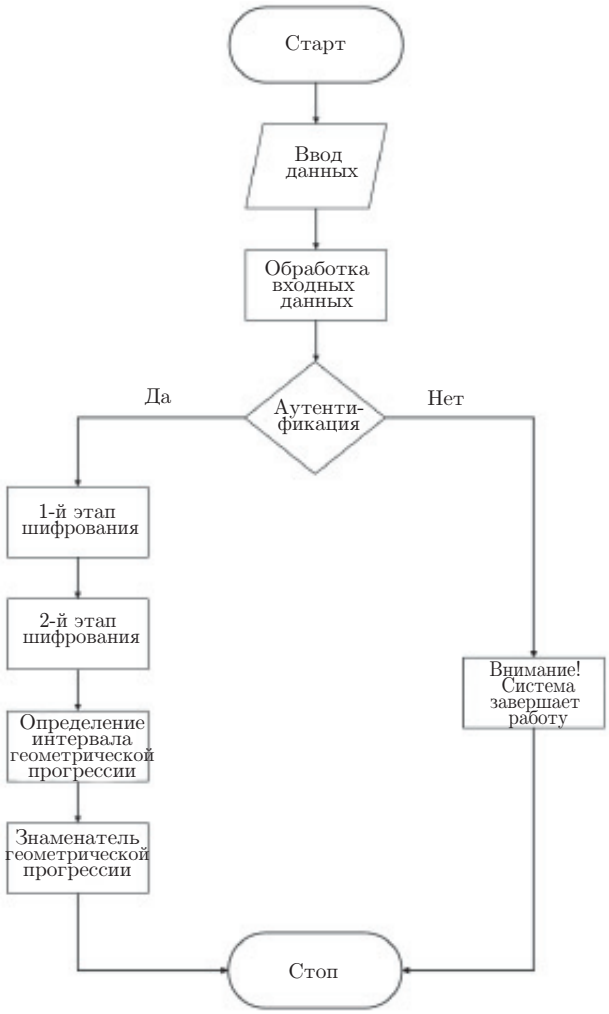

Рис. 1. Архитектура программного модуля хэширования биометрических персональных данных пользователя системы

пользователей информационной системы будут представлены в цифровом виде. Численное значение, полученное при суммировании элементов массива, в виде которых интерпретированы голос и изображение пользователей информационной системы, будет представлено в виде 9 октетов (перевод из восьмеричной системы счисления в двоичную). Полученные октеты далее преобразуются в хэш-код, который является результатом действия алгоритма хэширования и сохраняется в виде файла log.txt в целевой папке администратора учётной записи (рис. 2). Далее представлен процесс хэширования биометрических персональных данных.

На начальном этапе следует определить знаменатель геометрической прогрессии. Под знаменателем геометрической прогрессии подразумевается выбранный интервал. В данном случае интервал будет увеличиваться по формуле

$$q^n = (q^{n-1})^2, \tag{1}$$

где $n = 2, 3, \ldots, N$, q^n — знаменатель геометрической прогрессии, выбранный пользователем устройства.

Необходимо выбрать значение интервала геометрической прогрессии [2]. Интервал

Рис. 2. Процесс генерации файла log.txt

будет вычисляться по следующей формуле:

$$b_n = b^{n-1} \times q^n, \tag{2}$$

где $n = 2, 3, \ldots, N$, b_n — интервал геометрической прогрессии.

Шаги хэширования представлены в виде экспоненциальной функции [3]

$$x = \sum \frac{1}{b_n}, \tag{3}$$

где x — шаг хэширования биометрических персональных данных, $b_n > 1$.

Биометрические персональные данные в цифровом виде будут интерпретированы следующим образом:

$$y = a^{\exp(x)}, \tag{4}$$

где y — результат хэширования биометрических персональных данных, a — биометрические данные в цифровом виде, $\exp(x)$ — экспоненциальная функция.

При разработке программного модуля хэширования биометрических персональных данных используется асимметричное шифрование, которое подразумевает применение открытого и закрытого ключа. В результате цифровые данные будут закодированы на протяжении заданного количества циклов пользователями информационной системы в файле конфигурации программного обеспечения. Криптографическим ключом являются биометрические персональные данные, представленные в цифровом виде.

Модель хэширования реализована с помощью искусственной нейронной сети. Нейронная сеть представляет собой многослойный персептрон. На вход нейронной сети будут подаваться биометрические образы пользователя системы в цифровом виде. Разработанная структура нейронной сети имеет ряд преимуществ (рис. 3) [4]:

1. Нейроны входного слоя состоят из биометрических персональных данных (коэффициенты линейного предсказания LPC, перцепционные коэффициенты линейного предсказания (PLP), мел-кепстральные коэффициенты (MFCC), констант Q-кепстральные коэффициенты (CQCC), частота спектрального центроида (SCF) и локальные бинарные паттерны (LBP)), представленных в виде числового массива, которые необходимы для повышения точности при обработке данных в процессе обучения искусственной нейронной сети.

2. Вычисления производятся для каждого нейрона в независимости от входных данных. Время работы сети будет зависеть только от её архитектуры.

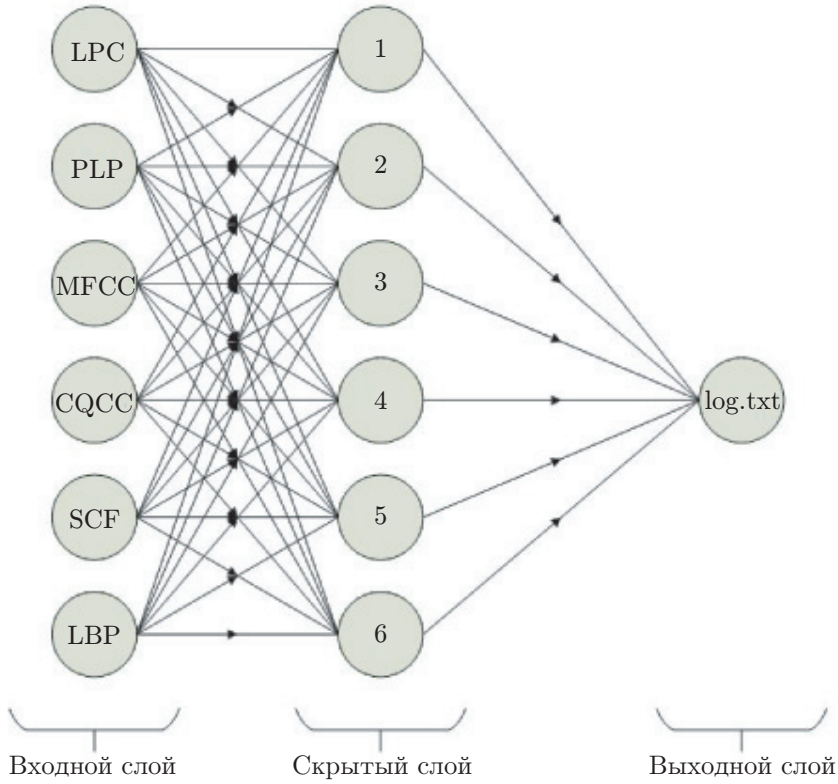

Рис. 3. Схема функционирования нейронной сети программного модуля хэширования биометрических персональных данных

3. По весам сети невозможно определить секретный ключ и даже сам алгоритм хэширования.

Для передачи сигналов на скрытый слой нейронной сети применяется функция активации для того, чтобы на выходе значения принимали вид в диапазоне $[0, 1]$ [5]

$$f(x) = \frac{1}{1 + \mathrm{e}^{-x}}. \tag{5}$$

Входные данные программного модуля хэширования. Метод обратного распространения ошибки. Разработанный в данной работе программный модуль является частью программного комплекса многофакторной биометрической аутентификации (рис. 4) [6]. В совокупности представлено две архитектуры нейронных сетей. В основе математической модели многофакторной аутентификации заложено распознавание личности по голосу, изображению и видео. Первая архитектура нейронной сети на входе получает основные индивидуальные характеристики. После подбора весовых коэффициентов и активации скрытого слоя на выходе получается результат, который будет подаваться на вход архитектуры нейронной сети программного модуля хэширования.

В рамках обучения нейронной сети многофакторной биометрической аутентификации необходимо определиться с параметрами входного слоя. Входной слой будет состоять из:

1) номера пользователей учётных записей;
2) коэффициентов линейного предсказания (LPC);
3) перцепционных коэффициентов линейного предсказания (PLP);
4) мел-кепстральных коэффициентов (MFCC);
5) констант Q-кепстральных коэффициентов (CQCC);

6) частот спектрального центроида (SCF).

Построение признаков PLP и MFCC начинается с процедуры разбиения входного сигнала на временны́е окна, называемые кадрами, с фиксированным шагом смещения. Далее применяются следующие преобразования:

1. Предварительная фильтрация.

Цель данного шага заключается в уменьшении негативных эффектов, возникающих во время обработки звукового сигнала. Как правило, применяется фильтр с конечной импульсной характеристикой (КИХ-фильтр) следующего вида [7]:

$$y_t = x_t - bx_{t-1}, \tag{6}$$

где x_t — входной звуковой сигнал; y_t — звуковой сигнал после фильтрации; $b > 1$ — коэффициент фильтрации; $t = 1, 2, \ldots, T$ — номер кадра.

2. Дискретное преобразование Фурье (ДПФ) [8]

$$F_k = \sum_{t=0}^{T-1} w_t y_t \exp\Big(-\frac{2\pi i}{T}\, kt\Big), \qquad k = 0, \ldots, \frac{T}{2}, \tag{7}$$

где T — количество отсчётов в кадре, w_t — весовая оконная функция, k — индекс частоты.

Весовая оконная функция применяется с целью уменьшения краевых эффектов, возникающих в результате разбиения сигнала на кадры. Наиболее распространёнными оконными функциями являются:

окно Хэмминга [9]

$$w_t^{hamm} = 0{,}54 - 0{,}46\cos\Big(\frac{2\pi t}{T-1}\Big), \qquad k = 0, \ldots, T-1 \tag{8}$$

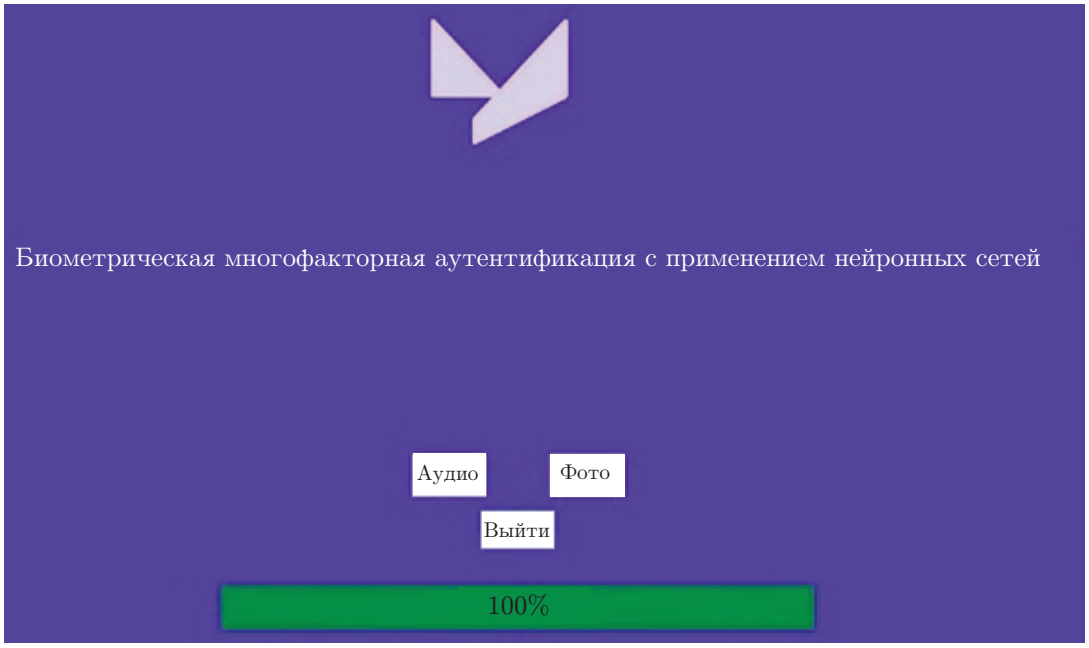

Рис. 4. Пользовательский интерфейс программного комплекса авторизации пользователей информационной системы по биометрическим персональным данным

и окно Хана [9]

$$w_t^{hann} = 0{,}5\Big(1 - \cos\Big(\frac{2\pi t}{T-1}\Big)\Big), \qquad k = 0, \ldots, T-1. \tag{9}$$

Для нахождения PLP используется автокорреляционный метод, который минимизирует ошибку сигнала на всём временно́м промежутке, после чего вычисляется ошибка предсказания. В результате мы находим автокорреляционные коэффициенты, которые и будут являться коэффициентами линейного предсказания [10].

Одним из наиболее продуктивных методов извлечения признаков голоса является константа Q-кепстральных коэффициентов (CQCC). Постоянное Q-преобразование (CQT) даёт более высокое разрешение в области низких частот и большее временно́е разрешение в области высоких частот. Коэффициенты CQCC извлекаются по формуле [11]

$$\mathrm{CQCC}[p] = \sum_{l=1}^{L} \log\,|X^{CQ}[l]|^2 \cos\Big(\frac{p\pi(l-1/2)}{L}\Big), \qquad 0 \leqslant p < L, \tag{10}$$

где $X^{CQ}[l]$ — временной сигнал, $p = 0, 1, \ldots, L-1$ и l — пересчитанные частотные значения.

Частота спектрального центроида (SCF) представляет собой средневзвешенную частоту для данного поддиапазона, а весовые коэффициенты — нормированную энергию каждого частотного компонента в этом поддиапазоне. Частота спектрального центроида определяется следующим образом [12]:

$$F_k = \sum_{f=l_k}^{u_k} f|S[f]\omega_k[f]| \Big/ \sum_{f=l_k}^{u_k} |S[f]\omega_k[f]|, \tag{11}$$

где u и l — верхняя и нижняя граничные частоты поддиапазона; $S[f]$ — спектр фрейма, разделённого на k поддиапазонов; ω_k — частотный отклик фильтра.

Весовые коэффициенты (SCF) вычисляются по формуле [12]

$$M_k = \sum_{f=l_k}^{u_k} f|S[f]\omega_k[f]| \Big/ \sum_{f=l_k}^{u_k} f. \tag{12}$$

Для создания конфигурации файла весов авторы использовали комбинированный метод подбора, который состоит из:

1) классического алгоритма обратного распространения ошибки (метод градиентного спуска);

2) импорта необходимых компонентов из библиотеки keras;

3) коррекции весовых коэффициентов.

Для повышения точности работы обученной искусственной нейронной сети часть весовых коэффициентов скрытого и выходного слоёв подбиралась эмпирическим методом. Весовые коэффициенты корректировались после автоматического подбора (библиотека keras) для повышения точности работы искусственной нейронной сети [13]. Так как архитектура нейронной сети представляет собой многослойный персептрон, необходимо активировать нейроны скрытого слоя таким образом, чтобы на выходном слое получить наиболее высокие показатели точности при обучении нейронной сети. Поэтому некоторые из коэффициентов входного и скрытого слоёв были подобраны самостоятельно.

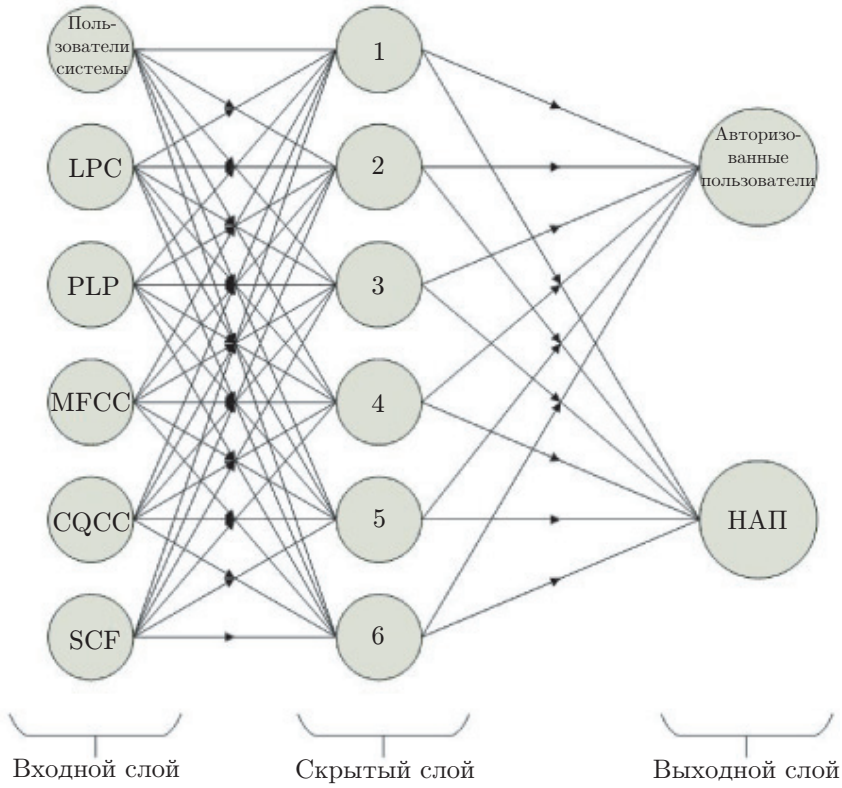

Рис. 5. Архитектура нейронной сети распознавания личности

Обучающая выборка сформирована способом кроссвалидации, который исключает возможность пересечения тестовых и тренировочных наборов. Количество классов обучающей выборки должно быть не менее двух. В каждом наборе формируются модели, отражающие основные метрики нейронной сети. Итоговый результат получается в виде усреднённого значения всех наборов (test, train, val).

Амплитуда спектрального центроида представляет собой амплитуду в положении частоты спектрального центроида, которая также будет нести информацию, касающуюся формант. Данные вычисления необходимы для распознавания голоса пользователей информационной системы [14].

Для достижения цели искусственно была подобрана конфигурация весов как на скрытом слое, так и на выходном. Определившись с входными параметрами, архитектура нейронной сети примет вид как рис. 5.

Следует обратить внимание, что на входе задействованы сами пользователи b, представленные ранее индивидуальные характеристики голоса (LPC, PLP, MFCC, CQCC, SCF). В ходе программной реализации будут обработаны три звукозаписи с временны́ми промежутками 5, 8 и 12 с (1, 2 и 3 соответственно) (см. рис. 3). На выходе программный комплекс определяет авторизованных и неавторизованных пользователей (НАП) системы. На входной слой будут подаваться основные показатели после обработки более 1000 образов из собранной базы данных биометрических элементов.

Экспериментальная часть. Качество и вычислительная сложность обучения нейронной сети. Входной слой нейронной сети состоит из более 1000 биометрических образов сформированной авторами Dataset (папка с изображениями и аудиофрагментами пользователей информационной системы).

Вычисления точности и качества работы обучающей нейронной сети были реализо-

ваны с применением функции потерь. С помощью метода градиентного спуска с частной производной для подсчёта функции ошибки используется следующая формула [15]:

$$\frac{\partial L}{\partial w_i} = \frac{\partial\,(y - y^*)}{\partial w_i} = 2(y - y^*)\,\frac{\partial\,(y - y^*)}{\partial w_i} = 2(y - y^*)\,\frac{\partial y}{\partial w_i}, \tag{13}$$

где w_i — i-й вес, y — выход, y^* — правильное значение выхода, $\partial L/\partial w_i = \nabla L(\vec{w})$ — градиент функции ошибки, Δy — ошибка предсказания, $f'(z)$ — значение производной функции f в точке $z = \sum_{i=1}^{n+1} x_i^* w_i$.

В процессе обучения вес увеличивается по формуле [16]

$$\Delta w_i = -2\alpha \Delta y f'(z) x_i^*, \tag{14}$$

где Δy — ошибка предсказания, $\Delta y = y - y^*$ — величина ошибки предсказания, α — коэффициент скорости обучения.

Dataset обучающей выборки разделён на три папки: test (тестовый набор), train (тренировочный набор) и val (валидационный набор). При прохождении обучения искусственной нейронной сети точность работы (accuracy) составляет 89 % после первой эпохи и 92 % процента после пятидесятой эпохи. Точность обучения валидационного набора (val_accuracy) составляет 89,9 % после первой эпохи и 92 % после пятидесятой эпохи. Соответственно показатели потерь (loss) равны 11 % после первой эпохи и 8 % после пятидесятой эпохи. Потери валидационного набора (val_loss) почти идентичны: 10,1 % после первой эпохи и 8 % после пятидесятой эпохи обучения искусственной нейронной сети.

Таким образом, исходя из представленных показателей искусственной нейронной сети, уровень точности обучения имеет положительную динамику и расположенность к достижению максимальных показателей при увеличении входных параметров (от 89 к 92 %).

Заключение. В ходе исследования была обучена искусственная нейронная сеть для функционирования криптографического программного модуля хэширования данных пользователей информационной системы, а также подобрана конфигурация весовых коэффициентов. Проведена апробация работы программного модуля на персональном компьютере с использованием массива биометрических образов. Результатом исследования является разработанный программный модуль хэширования биометрических персональных данных с обучаемой нейронной сетью. Данный программный модуль предоставляет пользователю устройства необходимый уровень защищённости информационных ресурсов посредством применения биометрических персональных данных и генерации более 1 000 000 ключей с 9 октетами.

Данный результат исследования может применяться в работе автоматизированных рабочих мест предприятия. В совокупности с нейронными сетями и искусственным интеллектом данный программный модуль является дополнением к существующим средствам защиты информации пользователей системы. Основным показателем работы программы является криптостойкость, которая определяется количеством вычислительных операций. Уровень криптостойкости данной программы оценивается в 256 бит (длина открытого и закрытого ключей). Таким же уровнем криптостойкости обладает AES-256. С учётом количества генерируемых ключей, применения циклов, геометрической прогрессии и экспоненциальной функции при возникновении криптографических атак дешифровать результаты данного программного обеспечения не получится за короткий временной промежуток. Для этого понадобится подключить огромное количество циклов, которые могут оказаться неприемлемыми в рамках производительности вычислительной машины.

Финансирование. Исследование выполнено при поддержке ФГБОУ ВО «Московский технический университет связи и информатики» (проект № 40469-20/2022-к).

СПИСОК ЛИТЕРАТУРЫ

1. **Пакулич Д. В., Алямкин С. А.** Использование свёрточных нейронных сетей для обнаружения подмены лица его изображением // Автометрия. 2021. **57**, № 4. С. 91–97. DOI: 10.15372/AUT20210411.
2. **Исмагилова А. С., Лушников Н. Д.** Многофункциональное ПО для защиты учётных записей пользователей с использованием биометрических технологий // Защита информации. Инсайд. 2021. № 2 (98). С. 28–31.
3. **Гуртова К. С.** Метод защиты информации цифровых документов с помощью невидимых цифровых меток и его реализация // Современные информационные технологии и ИТ-образование. 2022. № 1. С. 152–166.
4. **Акилин Г. А., Грицкевич Е. В.** Особенности имитационного моделирования информационных систем, использующих биометрическую идентификацию по лицу // Сб. ст. по мат-лам междунар. науч. конгресса «Интерэкспо Гео-Сибирь». 2019. С. 61–65.
5. **Хайкин С.** Нейронные сети. Полный курс. М.: Вильямс, 2006. 1104 с.
6. **Свидетельство** о государственной регистрации программы для ЭВМ № 2021614672 РФ. Аутентификация учётных записей пользователей с помощью биометрических технологий: № 2021613387 / Н. Д. Лушников, А. С. Исмагилова; Заявл. 15.03.2021; Опубл. 29.03.2021. Заявитель ФГБОУВО «Башкирский государственный университет».
7. **Крейнделин В. Б., Легков Н. А.** Защита аутентификационных данных сайтов и WEB-приложений // Телекоммуникации и информационные технологии. 2022. № 1. С. 6–10.
8. **Robert J., Marks II.** Handbook of Fourier Analysis & Its Applications. Oxford: Oxford University Press, 2009. P. 744.
9. **Слюсар В. И.** Современные тренды радиорелейной связи // Технологии и средства связи. 2014. № 4. С. 32–36.
10. **Крылова И. Ю., Рудакова О. С.** Биометрические технологии как механизм обеспечения информационной безопасности в цифровой экономике // Молодой учёный. 2018. № 45 (231). С. 74–79.
11. **Todisco M., Delgado H., Evans N.** A new feature for automatic speaker verification anti-spoofing: Constant Q cepstral coefficients // Proc. of the Odyssey 2016: Speaker and Language Recognition Workshop. Bilbao, Spain, 21-24 June, 2016. P. 283–290.
12. **Судьенкова А. В.** Обзор методов извлечения акустических признаков речи в задаче распознавания диктора // Сб. науч. тр. НГТУ. 2019. № 3-4(96). С. 139–164.
13. **Лушников Н. Д., Исмагилова А. С.** Обучение и создание весов нейронной сети с применением категориальной кросс-энтропии // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сб. мат. V Всеросс. мол. науч.-практ. конф. Уфа: Башкирский гос. ун-тет, 2022. С. 30–32. DOI: 10.33184/itokbco-2022-05-20.6.
14. **Гасников А. В.** Современные численные методы оптимизации. Метод универсального градиентного спуска: Учебное пособие. М.: МФТИ, 2018. 291 с.
15. **Гафаров Ф. М., Галимянов А. Ф.** Искусственные нейронные сети и приложения: Учеб. пособие. Казань: Изд-во Казан. ун-та, 2018. 121 с.
16. **Караваев Д. А.** Вейвлет-подобная архитектура комплекснозначной свёрточной нейронной сети для синтеза комплексных сигналов // Вестн. кибернетики. 2020. № 2. С. 20–31.

Поступила в редакцию 27.03.2023
После доработки 01.06.2023
Принята к публикации 22.06.2023