УДК 004.032.26

Особенности разработанной системы защиты информации с применением биометрических технологий

Исмагилова А. С., Лушников Н. Д.

Башкирский государственный университет

Аннотация: В статье рассмотрено применение метода синтеза параметров сверточной нейронной сети, представленной в виде уникальных идентификаторов пользователя персонального компьютера. Для полноценной защиты информационных ресурсов авторами реализовано обучение тренировочной модели с помощью категориальной кросс-энтропии. Основной целью исследования является изучение новых аспектов математического моделирования системы защиты информации. Задача данного исследования – программная реализация математической модели многофакторной аутентификации с применением биометрических технологий, необходимая для совершенствования комплексной системы защиты информации.

Ключевые слова: математическая модель, система защиты информации, учетная запись, пользователь, безопасность, искусственный интеллект, идентификация, биометрия.

1. Разработка математической модели системы защиты информации

Компании тратят большие суммы денег на кибербезопасность, часто пренебрегая физической защитой. Такие инвестиции не гарантируют абсолютную защиту от несанкционированного доступа. Для оптимизации системы защиты информации и, соответственно, решения представленной проблемы, авторами было принято решение разработать программный комплекс многофакторной аутентификации с применением биометрических технологий.

Ранее использовались отдельные математические алгоритмы, которые на выходе показывали наименьшую точность распознавания образцов базы данных. Такая база данных обладает наименьшим количеством образцов.

В основе программного комплекса реализованы математические модули фотоидентификации, видеоидентификации, аудиоидентификации, а также система шифрования входных биометрических данных пользователя с использованием таких математических методов, как экспоненциальная функция и геометрическая прогрессия [1].

Первым фактором аутентификации пользователя является фотоидентификация, в основе которого заложено формирование массива данных лица пользователя, состоящего из 128 точек.

В целевой папке сохранены файлы изображения пользователя учетной записи. После запуска программного комплекса система видеонаблюдения в течение 5-7 секунд создаст снимок изображения и автоматически сохранит его в целевой папке для дальнейшей сверки. После всех выполненных действий производится расчет евкли-

дова расстояния по исходным данным. В библиотеке dlib рекомендуется использовать граничное значение евклидова расстояния между дескрипторами лиц, равное 0.6 [2].

Далее производится автоматический запуск математического модуля видеоидентификации, в котором необходимо отличить настоящего пользователя от объекта, олицетворяющего его (фото, видео). Точность обработки данных – 99.4%.

Авторам удалось создать и реализовать многопоточный программный комплекс для одновременного воспроизведения нескольких математических модулей.

Стоит обратить внимание на модуль аудиоидентификации, примененный впервые в области защиты информации. Данное решение дополнено считыванием аудиообразцов целевой папки с помощью евклидова расстояния по 12 характеристикам голоса. Сохраненные в целевой папке аудиофайлы автоматически обрабатываются. Результат обработки данных также представлен в виде двух изображений показателей голоса по каждому параметру мощности [3].

Параметры аудиоидентификации вычисляются по формуле (1):

$$f_n = f_0 \cdot 2^{n/12},$$

где f_n – частота голосового фрагмента, которая удалена от тона на n полутонов, f_0 – частота голосового фрагмента, которая используется в качестве стандартизированных данных, n – количество полутонов.

В результате реализации программного комплекса владельцу учетной записи будет предоставлен доступ. Другому пользователю, который осуществил запуск операционной системы, в доступе будет отказано при несовпадении всех биометрических показателей. При несоответствии одного биометрического параметра пользователю системы будет предоставлена возможность дважды ввести логин и пароль с использованием голосового помощника (рис 1). Данный инструмент разработан с выводом результатов во вкладку браузера (тестирование поиска информации) [4].

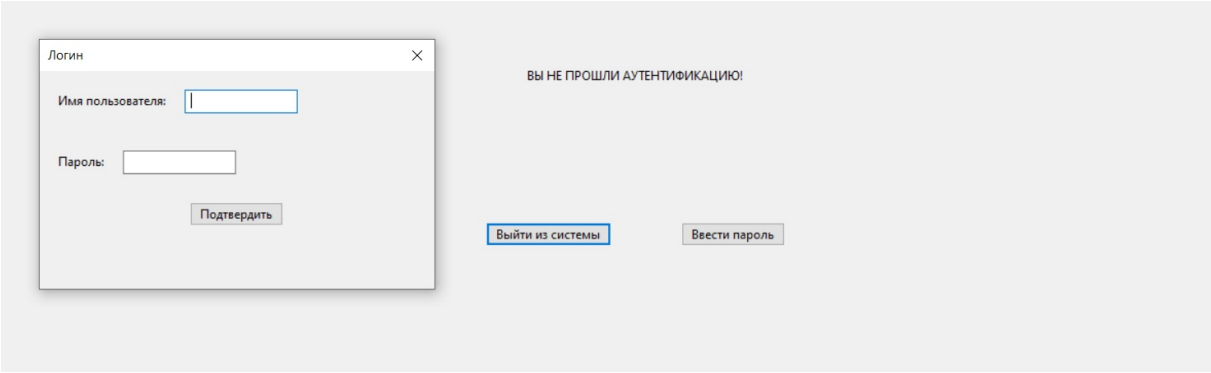

Рис. 1. Форма прохождения аутентификации с помощью голосового помощника.

Главным достоинством математической модели является высокая точность обработки входных данных и синхронизированная работа программных модулей. В основе софта заложен сохраненный файл весов обучающей нейронной сети [5].

Недостатком математической модели является время обработки данных программного модуля распознавания пользователя по голосу. Это обусловлено качеством и корректностью работы программы во время представления голосового об-

разца в виде массива вещественных чисел. Конфигурацию данного параметра пользователь может выбрать самостоятельно [6].

2. Особенности системы защиты информации биометрических данных пользователя

Данный программный комплекс направлен на предоставление максимального уровня защищенности пользователя учетной записи. В связи с этим возникает не менее актуальная проблема: хранение и доступность биометрических данных пользователя.

В настоящее время основными задачами криптографии являются обеспечение конфиденциальности, целостности, аутентификации, невозможности отказа, неотслеживаемости. В отличие от организационных и других способов защиты информации, под криптографическими понимаются такие, которые используют математические методы преобразования защищаемой информации. Криптография с открытым ключом значительно расширила класс задач, решаемых с помощью криптографических методов [7]. В результате появилась потребность как в интерактивных, многофазовых обменах данными, так и в протоколе аутентификации, который помогает обеспечить контроля доступа к данным. Протоколы аутентификации, построенные на основе протоколов с нулевым разглашением знания, используют два ключа (секретный и открытый). Когда говорится о том, что протокол аутентификации построен на основе протокола с нулевым разглашением секрета, то имеется ввиду, что в ходе протокола не происходит никакой утечки данных. Специальный набор символов в шифровании предназначен для обеспечения целостности и аутентификации источника данных [8].

Зашифрованные данные могут подвергаться как целенаправленным искажениям злоумышленников, так и искажениям, причиной которых может являться низкий уровень криптостойкости. Искажения могут привести к потере части или даже всех данных, так как расшифрование искаженных зашифрованных данных может привести к непредсказуемым результатам. В данном программном комплексе рассмотрены, изучены и применены шифры, которые не распространяют искажения при расшифровании [9].

Аутентификация пользователя может быть выполнена следующим образом:

1. Запрос на ввод идентификатора со стороны системы защиты.
2. Ввод пользователем своего идентификатора (имени).
3. Запрос на ввод пароля со стороны системы защиты.
4. Ввод пользователем пароля $password$.
5. Вычисление системой защиты значения односторонней функции y, соответствующей значению аргумента $x = password$.
6. Сравнение системой защиты значения $f(password)$ со значением образа (s) пароля, соответствующего пользователю с идентификатором имени.

Если $f(password) = s$, то система защиты предоставляет пользователю права доступа (полномочия), соответствующие идентификатору (bvtyb). В противном в журнале событий операционной системы регистрируется событие попытки несанкционированного доступа и персональное устройство автоматически выключается. Зная образ s, вычислительно невозможно определить пароль $password$. Если в системе защиты предусмотрены механизмы противодействия перехвату пароля с помощью программных или аппаратных закладок, а также через побочные электромагнитные

излучения и наводки (ПЭМИН), акустический и оптический канал, то данный способ аутентификации пользователей обеспечивает высокую надежность защиты от несанкционированного доступа [10].

Для предоставления доступа ограниченному кругу лиц к целевой папке, содержимое файлов необходимо зашифровать. Шифр должен обладать соответствующим уровнем криптостойкости.

Биометрические данные можно представить следующим образом (2):

$$y_i = x_i + d \pmod{n}, \quad i = 1, 2, ..., l,$$

где y_i – зашифрованные данные, x_i – изначально представленные биометрические данные, n – количество произведенных итераций, i – порядковый номер.

Тогда процесс расшифрования будет реализован с помощью (3):

$$x_i = y_i + n - d \pmod{n}, \quad i = 1, 2, ..., l,$$

где x_i – изначально представленные биометрические данные, y_i – зашифрованные данные, n – количество произведенных итераций, i – порядковый номер.

Для того, чтобы система защиты могла идентифицировать легального пользователя учетной записи, в памяти персонального устройства хранятся образы паролей, вычисленные по специальному криптографическому алгоритму [11].

Представленные решения шифрования данных являются наиболее упрощенными средствами шифрования. Существуют шифры, в которых используется целый набор символов шифртекста (4):

$$\varphi_i = A \Rightarrow B_i, i = 1, 2, ..., s$$

где φ_i – результат шифрования данных, A, B – лица, которым предоставлен доступ к данным, s – количество произведенных итераций, i – порядковый номер.

Тогда открытый текст $x_1...x_s x_{s+1}...x_{2s}...$ в процессе шифрования преобразуется в шифртекст (5):

$$\varphi_i(x_i)...\varphi_s(x_s)\varphi_1(x_{s+1})...\varphi_s(x_{2s})$$

где φ_i, φ_s – результат шифрования данных, A, B – лица, которым предоставлен доступ к данным, s – количество произведенных итераций, i – порядковый номер.

Таким образом, в ходе исследования были рассмотрены, изучены, а также применены аналитические данные голосового образца, евклидово расстояние, шифрование и криптостойкость. Были проведены апробационные работы на персональном компьютере. Результатом исследования является созданный авторами программный комплекс системы защиты информации. Данное решение предоставляет пользователю операционной системы устройства необходимый уровень защищенности информационных ресурсов [12].

В совокупности использование программного обеспечения и обученной нейронной сети позволяет автоматизировать процессы во многих областях [13].

Представленный авторами результат шифрования является необходимым компонентом для программного комплекса многофакторной аутентификации. В совокупности с нейронными сетями и искусственным интеллектом, данный программный модуль представляет собой новый инструмент в области криптографии.

В дальнейшем авторами будут заложены такие математические методы, как геометрическая прогрессия и экспоненциальная функция [14].

Представленный программный продукт является удобным помощником для пользователя любой системы. Данное программное решение является универсальным продуктом при наличии собственного устройства, использовании сайтов, образовательных модулей и систем контроля, управления доступом. Помимо этого, стоит отметить, что интегрированный в программный код голосовой помощник является хорошим гидом абсолютно для всех пользователей, включая людей с ограниченными возможностями (особенно касается слабовидящих людей) [15].

Литература

1. Акилин Г.А., Грицкевич Е.В. Особенности имитационного моделирования информационных систем, использующих биометрическую идентификацию по лицу // Сборник статей по материалам международного научного конгресса «Интерэкспо Гео-Сибирь». 2019. С. 61-65.
2. Гринчук О.В., Цурков В.И. Обучение мультимодальной нейронной сети для определения подлинности изображений // Известия Российской академии наук. Теория и системы управления. 2020. № 4. С. 103-109.
3. Девицына С.Н., Елецкая Т.А., Балабанова Т.Н., Гахова Н.Н. Разработка интеллектуальной системы биометрической идентификации пользователя // Научные ведомости. Серия: Экономика. Информатика. 2019. Т. 46, №1. С. 148-160.
4. Исмагилова А.С. Многофункциональное ПО для защиты учетных записей пользователей с использованием биометрических технологий / А.С. Исмагилова, Н.Д. Лушников // Защита информации. Инсайд. 2021. № 2 (98). С. 28-31.
5. Караваев Д.А. Вейвлет-подобная архитектура комплекснозначной сверточной нейронной сети для синтеза комплексных сигналов // Вестник кибернетики. 2020. № 2. С. 20-31.
6. Кручинина Е.В. Видеоидентификация – ключ в мире адресных услуг // Системы безопасности. 2016. №6. С. 110-111.
7. Крылова И.Ю., Рудакова О.С. Биометрические технологии как механизм обеспечения информационной безопасности в цифровой экономике // Молодой ученый. 2018. № 45 (231). С. 74-79.
8. Мамаев В. Многофакторная биометрическая идентификация // Системы безопасности. 2017. №5. С. 78-79.
9. Немков Р.М. Исследование сверточной нейронной сети, обученной с помощью метода применения нестандартных рецептивных полей при распознавании изображений // Известия Южного федерального университета. 2015. № 7 (168). С. 79-90.
10. Осовский С. Нейронные сети для обработки информации: учебное пособие / С. Осовский. М., Телеком, 2017. 448 с.
11. Пчеловодова Н. Российский биометрический рынок в 2019-2022 годах. Результаты масштабного исследования J'son & Partners Consulting // Системы безопасности. 2019. №2. С. 88-91.

12. Свидетельство о государственной регистрации программы для ЭВМ № 2020660303. Управление доступом при помощи нейронных сетей. 2020 / Исмагилова А.С., Лушников Н.Д. - Башкирский государственный университет.

13. Свидетельство о государственной регистрации программы для ЭВМ № 2021614672. Аутентификация учетных записей пользователей с помощью биометрических технологий. 2021 / Исмагилова А.С., Лушников Н.Д. - Башкирский государственный университет.

14. Четырбок П.В., Шостак М.А. Обучение модульной нейронной сети для многозадачного искусственного интеллекта // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2021. № 4. С. 70-74.

15. Чупакова А.О., Гудин С.В. Разработка и обучение модели искусственной нейронной сети для создания систем поддержки принятия решений // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2020. № 3. С. 61-73.

MSC 68T10 90-04 90-10

Learning neural network for multi-factor authentication using biometric technologies

A. S. Ismagilova, N. D. Lushnikov

Bashkir State University

Abstract: The article considers and applies a method for synthesizing the parameters of convolutional neural network represented in the form of unique personal computer user identifiers. For full-fledged protection of information resources the authors have implemented training of the training model using categorical cross-entropy. The main purpose of the study is to explore new aspects of mathematical modeling of the information protection system. The task of this study is the software implementation of the mathematical model of multifactor authentication using biometric technology, which is necessary to improve the integrated information security system.

Keywords: mathematical model, information protection system, account, user, security, artificial intelligence, identification, biometrics.

References

1. G.A. Akilin, E.V. Gritskevich, Osobennosti imitacionnogo modelirovaniya informacionnyh sistem, ispol'zuyuschih biometricheskuyu identifikaciyu po licu, *Sbornik statej po materialam mezhdunarodnogo nauchnogo kongressa «Interekspo Geo-Sibir'*, 2019, P. 61-65.

2. O.V. Grinchuk, V.I. Tsurkov, Obuchenie mul'timodal'noj nejronnoj seti dlya opredeleniya podlinnosti izobrazhenij, *Izvestiya Rossijskoj akademii nauk. Teoriya i sistemy upravleniya*, 2020, № 4, P. 103-109.

3. S.N. Devitsyna, T.A. Eletskaya, T.N. Balabanova, N.N. Gakhova, Razrabotka intellektual'noj sistemy biometricheskoj identifikacii pol'zovatelya, *Nauchnye vedomosti. Seriya: Ekonomika. Informatika*, 2019, 46, № 1, P. 148-160.

4. A.S. Ismagilova, N.D. Lushnikov, Mnogofunkcional'noe PO dlya zaschity uchetnyh zapisej pol'zovatelej s ispol'zovaniem biometricheskih tehnologij, *Zaschita informacii. Insajd*, 2021, № 2 (98), P. 28-31.

5. D.A. Karavaev, Vejvlet-podobnaya arhitektura kompleksnoznachnoj svertochnoj nejronnoj seti dlya sinteza kompleksnyh signalov, *Vestnik kibernetiki*, 2020, № 2, P. 20-31.

6. E.V. Kruchinina, Videoidentifikaciya – klyuch v mire adresnyh uslug, *Sistemy bezopasnosti*, 2016, № 6, P. 110-111.

7. I.Y. Krylova, O.S. Rudakova, Biometricheskie tehnologii kak mehanizm obespecheniya informacionnoj bezopasnosti v cifrovoj ekonomike, *Molodoj uchenyj*, 2018, № 45 (231), P. 74-79.

8. V. Mamaev, Mnogofaktornaya biometricheskaya identifikaciya, *Sistemy bezopasnosti*, 2017, № 5, P. 78-79.

9. R.M. Nemkov, Issledovanie svertochnoj nejronnoj seti, obuchennoj s pomosch'yu metoda primeneniya nestandartnyh receptivnyh polej pri raspoznavanii izobrazhenij, *Izvestiya Yuzhnogo federal'nogo universiteta*, 2015, № 7 (168), P 79-90.

10. S. Osovsky, Nejronnye seti dlya obrabotki informacii: uchebnoe posobie, M., Telekom, 2017, 448 p.

11. N. Pchelovodova, Rossijskij biometricheskij rynok v 2019-2022 godah. Rezul'taty masshtabnogo issledovaniya J'Son & Partners Consulting, *Sistemy bezopasnosti*, 2019, № 2, P. 88-91.

12. Svidetel'stvo o gosudarstvennoy registratsii programmy dlya EVM № 2020660303. Upravleniye dostupom pri pomoshchi neyronnykh setey. 2020 / A.S. Ismagilova, N.D. Lushnikov - Bashkirskiy gosudarstvennyy universitet.

13. Svidetel'stvo o gosudarstvennoy registratsii programmy dlya EVM № 2021614672. Autentifikatsiya uchetnykh zapisey pol'zovateley s pomoshch'yu biometricheskikh tekhnologiy. 2021 / A.S. Ismagilova, N.D. Lushnikov - Bashkirskiy gosudarstvennyy universitet.

14. P.V. Chetyrbok, M.A. Shostak, Obuchenie modul'noj nejronnoj seti dlya mnogozadachnogo iskusstvennogo intellekta, *Vestnik Adygejskogo gosudarstvennogo universiteta. Seriya 4: Estestvenno-matematicheskie i tehnicheskie nauki*, 2021, № 4, P. 70-74.

15. A.O. Chupakova, S.V. Gudin, Razrabotka i obuchenie modeli iskusstvennoj nejronnoj seti dlya sozdaniya sistem podderzhki prinyatiya reshenij, *Vestnik Astrahanskogo gosudarstvennogo tehnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naya tehnika i informatika*, 2020, № 3, P. 61-73.