УДК 004.001

ДВУХФАКТОРНАЯ БИОМЕТРИЧЕСКАЯ СИСТЕМА АУТЕНТИФИКАЦИИ[1]

Статья поступила в редакцию 29.07.2021, в окончательном варианте – 14.10.2021.

Рассохин Данила Константинович, Кубанский государственный университет, 350040, Российская Федерация, г. Краснодар, ул. Ставропольская, 149.

студент, e-mail: danilarassokhin@gmail.com

Лукащик Елена Павловна, Кубанский государственный университет, 350040, Российская Федерация, г. Краснодар, ул. Ставропольская, 149,

кандидат физико-математических наук, доцент, e-mail: lep_9091@mail.ru

Целью работы является разработка специализированного сервиса для аутентификации пользователей на основе их биометрических данных – уникальных физиологических или поведенческих особенностей человека. Такой способ расширенной аутентификации может быть использован в системах, где безопасность данных имеет особое значение, например в финансовых системах. В статье рассмотрены некоторые виды биометрических данных, используемые в современных системах защиты: голос и отпечатки пальцев, а также методы их сбора и обработки. Проанализированы биометрические системы, рассмотрены их преимущества и недостатки. Такие системы представляются самыми удобными для пользователя, так как не требуют дополнительного запоминания каких-либо данных или владения физическими предметами. Однако биометрические системы являются гораздо более затратными для владельцев данных систем. Отмечены также имеющие место риски взлома активов биометрических данных. Учитывая аппаратную мощность и наличие интерфейсного программного обеспечения, а также широкую аудиторию пользователей современных мобильных устройств, предложен мобильный вариант сервиса двухфакторной биометрической аутентификации. Распознавание отпечатков пальцев выполняется с помощью стандартных средств ОС Android – Biometric API. Для распознавания голоса использован метод, основанный на коэффициентах линейного предсказания (LPC). Разработан специальный протокол аутентификации пользователей сторонних приложений через данный сервис. С целью предотвращения компрометации биометрических данных используется метод шифрования на основе диофантовых уравнений.

Ключевые слова: безопасность, аутентификации, биометрия, распознавание голоса, распознавание отпечатков пальца, двухфакторная аутентификация, диофантовы уравнения

TWO-FACTOR BIOMETRIC AUTHENTICATION SYSTEM

The article was received by the editorial board on 29.07.2021in the final version – 14.10.2021.

Rassokhin Danila K., Kuban State University, 149, Stavropolskay St., Krasnodar, 350040, Russian Federation,

student, e-mail: danilarassokhin@gmail.com

Lukashchik Elena P., Kuban State University, 149, Stavropolskay St., Krasnodar, 350040, Russian Federation.

Cand. Sci. (Physics and Mathematics), Associate Professor, e-mail: lep_9091@mail.ru

The aim of the work is to develop a specialized service for two-factor authentication of users based on their biometric data namely unique physiological or behavioral person characteristics. This extended authentication method can be used in systems where data security is of particular importance, for example, in financial systems. Some types of biometric data used in modern security systems are discussed in the article namely voice and fingerprints, as well as methods for collecting and processing them. Biometric systems are analyzed, their advantages and disadvantages are considered. Such systems seem to be the most convenient for the user since they do not require additional memorization of any data or possession of physical objects. However, biometric systems are much more expensive for the owners of these systems. The risks of hacking biometric data assets were also noted. Considering the hardware power and availability of interface software, as well as a wide audience of users of modern mobile devices, a mobile version of the two-factor biometric authentication service has been proposed. Fingerprint recognition is performed using standard Android OS tools – Biometric API. A method based on Linear Prediction Coefficients (LPC) is used for voice recognition. To apply of this service for authenticating of users by third-party applications special protocol has been developed. To prevent compromise of biometric data, an encryption method based on Diophantine equations is used.

Keywords: information security, authentication, biometric, speaker recognition, fingerprint recognition, two-factor authentication, Diophantine equations

[1] Работа поддержана грантом РФФИ № 19-01-00596 «Теоретико-численные и алгоритмические аспекты разработки математических моделей систем защиты информации, содержащих диофантовы трудности».

Graphical annotation (Графическая аннотация)

Введение. Характерные для традиционных систем защиты проблемы паролей, использование которых сопряжено с рисками информационной безопасности, эффективно решают современные технологии биометрических методов защиты информации. Биометрические системы приспособлены под идентификацию личности без возможности передачи ключа и являются более удобными с точки зрения пользователя. Биометрические данные, уникальные для каждого человека, гарантируют надёжность проверки.

Внедрение биометрических систем распознавания в деятельность современного человека может упростить процессы получения доступа к информации, так как многие современные устройства, например смартфоны, могут производить сбор биометрических данных без дополнительного оборудования, что делает такие системы более удобными для конечных пользователей. В дополнение к традиционным методам защиты они помогают автоматизировать процессы поведенческого анализа и обнаруживать нелегальных пользователей.

В последние годы по данным специалистов Comparitech [3] во многих странах, в особенности в Китае, Пакистане, Малайзии, США и Индии, очень активно ведётся сбор биометрических данных. Так в системе биометрических данных Индии зарегистрировано больше 80 % населения страны, биометрические данные используются во всех сферах – от финансов до образования и государственных услуг.

Несмотря на указанные преимущества, биометрическим системам присущи и недостатки. Во-первых, биометрическая информация, как и любая другая, уязвима. Информационные системы то и дело подвергаются хакерским атакам, и часть информации попадает в руки злоумышленников. Правоохранительным органам не всегда удается должным образом организовать контроль ее безопасности. Так в последнее время замечен ряд случаев утечки биометрических данных в Китае [5]. И уникальность биометрических данных из достоинства превращается в недостаток: при их компрометации злоумышленник получает доступ ко всем активам с биометрической аутентификацией. Во-вторых, биометрические системы бывают также и технологически несовершенны. Наличие указанных уязвимостей, а также отсутствие надёжных систем безопасности приводит к тому, что большинство компаний – потенциальных заказчиков пока ещё не готово к масштабному переходу на биометрию. Широкое применение подобных систем в настоящее время сопряжено с высоким уровнем риска.

Рост числа внутренних и внешних рисков постоянно выдвигает перед разработчиками биометрических систем требование по обеспечению надлежащего уровня защищенности. Рынок биометрии остро нуждается в новых решениях, повышающих доверие к своим продуктам.

Для обеспечения должного уровня безопасности в последнее время все больше систем защиты переходят на многофакторную аутентификацию, где для доказательства аутентификации используется несколько различных и взаимодополняемых механизмов доказательства права на доступ. Для предотвращения взлома баз биометрических сигнатур необходимо для шифрования биометрических данных использовать алгоритмы, устойчивые к квантовым вычислениям. Высокую криптостойкость, например, имеют криптоалгоритмы, основанные на теории диофантовых уравнений [7].

Основные понятия биометрической аутентификации. Аутентификация (authentication) – процедура проверки принадлежности субъекту доступа предъявленного им идентификатора. Биометрический метод аутентификации использует биометрические данные пользователя – уникальные физиологические или поведенческие особенности человека. Данный способ является самым удобным для пользователя, так как для аутентификации нет необходимости запоминать какую-либо информацию или владеть определенным объектом. Человек сам становится «ключом» к информации. Однако у такого способа есть существенная проблема: оборудование для биометрической аутентификации должно иметь достаточно высокую точность определения, чтобы различать людей со схожими данными.

Все биометрические данные можно разделить на два класса:

- статические – физиологические особенности, которые не подвержены изменениям в течение длительного периода времени;
- динамические – поведенческие характеристики, основанные на особенностях движения человека. Для обозначения этого класса биометрии часто используется термин «behaviometrics».

Примеры статических биометрических данных: отпечатки пальцев или рисунок папиллярных линий; радужная оболочка глаза; сетчатка глаза; рисунок вен; лицо; геометрия руки; ДНК.

К динамическим, например, можно отнести следующие данные: почерк и динамика подписи; голос и ритм речи; распознавание жестов; динамика нажатия клавиш; походка.

Биометрические системы могут работать в двух режимах [13]:

- верификация, основанная на биометрическом параметре и на уникальном идентификаторе, который выделяет конкретного человека (сравнение один к одному).
- идентификация, основанная на биометрических измерениях. При этом измеренные параметры сравниваются со всеми записями из базы зарегистрированных пользователей, а не с одной из них, выбранной на основании какого-то идентификатора (сравнение один ко многим).

Многофакторная аутентификация. Многофакторная аутентификация – расширенная аутентификация, метод контроля доступа, в котором пользователю для получения доступа к информации необходимо предъявить более одного фактора аутентификации. Каждый фактор аутентификации охватывает ряд элементов, используемых для аутентификации или проверки личности лица до предоставления доступа.

Способы аутентификации могут быть сгруппированы в три основные категории [1]:

1. Факторы *знания* – это то, что пользователь знает, например, пароль, PIN-код, ответ на секретный вопрос и т.д.
2. Факторы *свойства* – это то, что является частью нас, например, отпечаток пальца, подпись, голос и т.д.
3. Факторы *владения* – это то, что у пользователя есть, например, бесконтактная идентификационная карта, сотовый телефон, физический ключ и т.д.

Сочетание нескольких типов механизмов аутентификации позволяет повысить и уровень безопасности, и эффективность работы систем безопасности, так как количество возможных ошибок, в целом присущих биометрическим системам, снижается.

Многофакторная аутентификация не стандартизирована. Существуют различные формы её реализации. Наиболее распространена двухфакторная аутентификация. Двухфакторная аутентификация – это метод идентификации пользователя в каком-либо сервисе при помощи запроса аутентификационных данных двух разных типов, что обеспечивает двухслойную, а значит, более эффективную защиту аккаунта от несанкционированного проникновения.

Для повышения надежности и эффективности в системах контроля доступа все чаще применяют биометрический способ идентификации. В данной работе представляется вариант системы двухфакторной аутентификации с двумя биометрическими факторами, применяется механизм аутентификации в виде свойства. Для получения биометрических сигнатур пользователя используются технологии распознавания отпечатков пальцев и голоса человека [6], основные положения которых представлены ниже.

Распознавание отпечатков пальцев. Технология распознавания по отпечаткам пальцев является одной из самых распространенных биометрических технологий в мире. Немецкий анатом И. К. Майер в 1788 г. [2] открыл уникальность отпечатков пальцев. Долгое время отпечатки пальцев являлись универсальным источником биометрических характеристик. Многолетний опыт применения биометрических систем на основе отпечатков пальцев подтверждает удобство их использования и высокую надежность.

Компактность современных сканеров отпечатков пальцев позволяет внедрять их в различные устройства ввода. Благодаря встроенным в смартфоны сканерам можно разблокировать мобильное устройство, оплатить покупки в интернете. В ближайшем будущем планируется внедрить подобные технологии и в другие устройства общего пользования, например в банкоматы и даже в метрополитене для замены билетов. Широко используются отпечатки пальцев в криминалистике для поиска и идентификации преступников. Ряд стран требуют сдачи отпечатков пальцев при оформлении визы, например страны Шенгенского соглашения. В России биометрические заграничные паспорта содержат записанные на микросхему отпечатки пальцев. В последнее время разрабатывается методика использования отпечатков пальцев для дерматоглифических исследований (способ тестирования организма человека, основанный на изучении признаков узоров на коже ладонной стороны кистей и стоп).

Распознавание голоса. Использование биометрии по голосу человека сложнее и интереснее чем использование большинства биометрических признаков. Технология распознавания голоса

попадает в сферы и физиологических, и поведенческих биометрических данных. С физиологической точки зрения такие системы распознают форму голосового тракта человека, включая нос, рот и гортань, определяют производимый звук. С поведенческой точки зрения они фиксируют то, как человек что-либо говорит – вариации движений, тон, темп, акцент и т.д., что также является уникальным для каждого человека. Объединение данных физической и поведенческой биометрии создаёт точную голосовую подпись.

Однако, поскольку голос человека может меняться в зависимости от возраста, эмоционального состояния, здоровья, гормонального фона и целого ряда других факторов, метод не является абсолютно точным.

Голосовая идентификация одна из самых притягательных для идентификации, но существующие на данный момент проблемы необходимо учитывать при внедрении в работающие бизнесы. Распознавание голоса эффективно используется как дополнительный метод в многофакторных системах.

Практическая реализация. Стремительное распространение мобильных технологий значительно расширило аудиторию пользователей мобильных устройств, что стимулирует развитие рынка мобильных приложений различного предназначения. При разработке мобильных приложений мощность современных мобильных платформ и API-интерфейсов позволяет использовать все возможности аппаратного обеспечения. В данной работе для мобильных платформ предлагается вариант системы аутентификации, использующей статические и динамические характеристики человека (распознавание голоса и отпечатков пальцев). Разработанная биометрическая система представляет собой клиент-серверное мобильное приложение для двухфакторной аутентификации пользователя через специальный протокол (рис. 1).

Биометрическая идентификация представляет собой процесс сравнения и определения сходства между представленными пользователем биометрическими данными и соответствующего этим данным цифрового эталона, отражающего уникальные биометрические характеристики этого пользователя [4]. Эталонная модель биометрических характеристик человека предварительно формируется на основе одного или несколько биометрических образцов и сохраняется в базе данных. Для работы с базой биометрических данных в предложенном сервисе аутентификации используется СУБД PostgreSQL. Информация о пользователях и их биометрические цифровые сигнатуры в базе данных хранятся в зашифрованном виде. Для шифрования данных используется алгоритм SOLDEEA, основанный на линейных диофантовых уравнениях [12]. Согласно работам К. Шеннона [11], криптографические схемы, содержащие диофантовы трудности, наиболее устойчивы к взлому, что положительно скажется на безопасности биометрических данных и повысит уровень доверия пользователей к биометрическим системам аутентификации.

Серверное приложение сервиса, написанное на языке Java, обеспечивает доступ к биометрическим данным пользователей, авторизацию пользователей в сервисе, а также распознавание отпечатков пальцев и голоса. Сервис предоставляет возможность интеграции двухфакторной аутентификации в сторонних приложениях.

Рисунок 1 – Структура системы

Серверное приложение делится на 2 основные части:

- интерфейс для сторонних приложений позволяет сторонним приложениям взаимодействовать с сервисом и производить аутентификацию;
- интерфейс для пользователей позволяет пользователям взаимодействовать с сервисом: добавлять биометрическую сигнатуру определенного вида, подтверждать аутентификацию.

Чтобы настроить аутентификацию, администратору стороннего приложения необходимо зарегистрировать в сервисе свое приложение (так называемый проект). Для этого администратор должен указать название, описание своего приложения и домен, которые в дальнейшем будет видеть пользователь при аутентификации с помощью мобильного сервиса. Это нужно для того, чтобы пользователь мог определить приложение, в котором он хочет произвести аутентификацию. После создания проекта администратор получает от сервера сервиса секретный ключ проекта, который в дальнейшем используется для создания запросов на аутентификацию.

Клиентское приложение написано на языке Java для операционной системы Android. Оно предоставляет базовый функционал для пользователей сервиса:

- авторизация/регистрация;
- добавление/удаление биометрических данных;
- аутентификация в сторонних приложениях.

Протокол для аутентификации пользователя в стороннем приложении выглядит следующим образом (рис. 2):

- стороннее приложение отправляет сервису запрос на авторизацию, в котором передает секретный ключ, уникальный для каждого приложения, и идентификатор пользователя в сервисе;
- сервис возвращает стороннему приложению код авторизации;
- стороннее приложение показывает код авторизации пользователю;
- пользователь вводит данный код в мобильном приложении-аутентификаторе;
- пользователь выбирает способ и выполняет аутентификацию;
- при успешной аутентификации сервис отправляет пользователю код аутентификации;
- пользователь вводит код аутентификации в стороннем приложении;
- стороннее приложение проверяет код аутентификации.

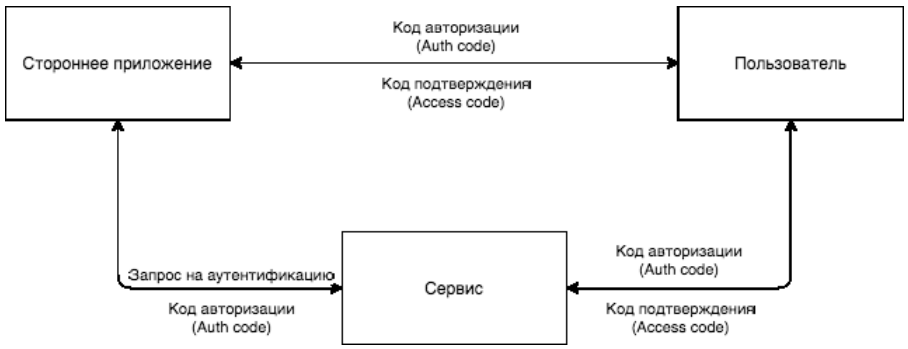

Рисунок 2 – Протокол аутентификации

После отправки запроса на аутентификацию пользователя стороннее приложение получает код авторизации, для генерации которого используется алгоритм создания одноразовых паролей для защищенной односторонней аутентификации TOTP **(*Time-based One-Time Password Algorithm*)**.

$$AuthCode = TOTP(ProjectSecret + UserID, AuthTime),$$
$$ProjectSecret - \text{секретный ключ проекта},$$
$$AuthTime - \text{время действия кода},$$
$$UserID - \text{идентификатор пользователя в системе}$$

Данный код позволяет одновременно идентифицировать запрос на авторизацию и установить ограничение по времени для запроса.

После этого стороннее приложение должно принять от пользователя код-подтверждение, который генерируется сервисом при успешной аутентификации:

$$AccessCode = TOTP(ProjectSecret + UserToken, AuthTime),$$
$$ProjectSecret - \text{секретный ключ проекта},$$
$$AuthTime - \text{время действия кода},$$
$$UserToken - \text{специальный токен пользователя в сервисе}.$$

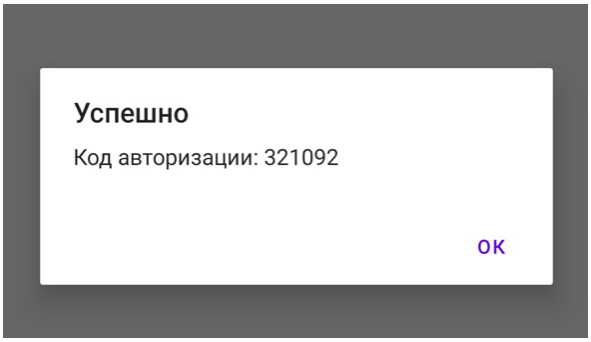

Рисунок 3 – Экран успешной аутентификации

Полученный от пользователя код подтверждения можно проверить путем отправки сторонним приложением соответствующего запроса сервису.

Реализованный в системе метод распознавания по голосу позволяет подключать для идентификации личности человека уникальные характеристики его голоса. Для записи аудио с микрофона устройства используется стандартный интерфейс ОС Android – AudioRecord. В процессе записи голос сохраняется в виде аудио файла в формате WAV (рис. 4).

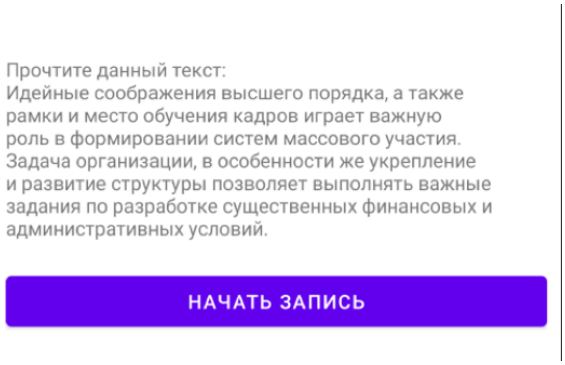

Рисунок 4 – Стартовое окно аутентификации по голосу

Распознавание говорящего производится с помощью библиотеки Recognito [9] на сервере. Для преобразования аудио файла в цифровой код используется алгоритм линейного предсказания LPC (Linear Prediction Coefficients). Коэффициенты линейного предсказания отражают главные голосовые характеристики человека, необходимые для принятия решения о личности диктора: голосовой источник, резонансные частоты речевого тракта и их затуханий, а также динамика управления артикуляцией [10]. На рисунке 5 показаны этапы получения цифровой сигнатуры голоса:

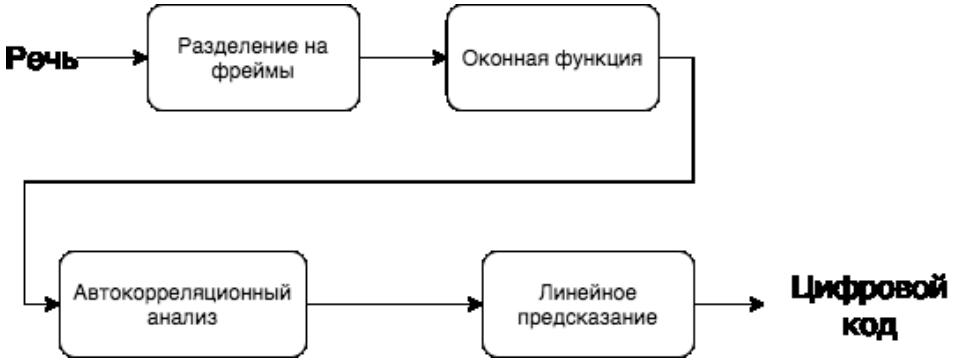

Рисунок 5 – Схема получения цифровой сигнатуры голоса

Полный алгоритм аутентификации пользователя по голосу в сервисе:

- получение на вход аудиофайла;
- создание цифровой сигнатуры из полученного аудиофайла;

- извлечение для данного пользователя из базы данных существующей эталонной сигнатуры голоса пользователя;
- сравнение полученного образца с эталонным и сигнатурами, созданными на основе других голосов и различного шума, на основе результатов сравнения считается отношение правдоподобия, которое показывает вероятность, того, что полученный образец близок к эталонному.
- аутентификация считается успешной, если результат отношения правдоподобия для полученного образца превысил определенную отметку (0–100). В данной реализации отметка равна 90.

Цифровая сигнатура хранится в базе и используется для аутентификации в виде массива десятичных чисел, отражающих характеристики голоса (рис. 6).

Сигнатуры	
1	3[illegible]
2	1[illegible]
3	1[illegible]

Рисунок 6 – Пример хранения отпечатка голоса в зашифрованном виде

Для аутентификации по отпечатку пальца приложение использует стандартные возможности ОС Android – Biometric API (Automated Biometric Identification System). После считывания сканером уникальный рисунок трансформируется в цифровой биометрический шаблон. Затем интерфейс сохраняет необходимые для распознавания данные в специальное защищенное хранилище – Android Keystore. Система гарантирует безопасность данных в этом хранилище от несанкционированного доступа. Приложение использует 3 класс безопасности, что не позволяет пользователю использовать пароль устройства или другие методы вместо отпечатка пальцев.

Последовательность действий сервиса при использовании для аутентификации отпечатков пальцев:

- пользователь включает аутентификацию по отпечаткам пальцев в приложении;
- сервис генерирует случайную строку и отправляет ее пользователю, строка сохраняется в базе данных сервиса;
- приложение шифрует полученную строку специальным ключом, зашифрованная строка сохраняется в памяти приложения, а ключ для дешифрования – в специальное хранилище;
- при аутентификации пользователь использует отпечаток пальца, и приложение получает доступ к ключу дешифрования, после чего сохраненная в памяти приложения строка расшифровывается и отправляется на сервер для проверки.

Цифровая сигнатура отпечатков пальцев представляется в виде строки, состоящей из английских букв и цифр.

Оценка работы. Для определения эффективности представленного сервиса аутентификации используем F-меру (F-measure) [14], применяемую для оценки точности алгоритмов распознавания:

$$F_\beta = (\beta^2 + 1) \cdot \frac{Precision \cdot Recall}{\beta^2 \cdot Precision + Recall},$$
$$0 < F_\beta < 1.$$

Данная метрика учитывает и объединяет в себе меру точности и полноты алгоритма.

Расчет точности произведем на основе выборки из 100 различных пользователей.

Для начала вычислим количество ошибок первого и второго рода, т.е. количество ложноотрицательных и ложноположительных результатов, а также количество истинно положительных и истинно отрицательных результатов. Получим следующую таблицу.

Таблица – Результаты распознавания

Верная гипотеза / результат распознавания	**Верно**	**Неверно**
Верно	51 (верно принятых TP)	11 (неверно принятых, ошибки второго рода FP)
Неверно	18 (неверно отвергнутых, ошибки первого рода FN)	20 (верно отвергнутых TN)

Точность (*Precision*) вычислим по формуле:

$$Precision = \frac{TP}{TP + FP}.$$

В нашем случае имеем:

$$Precision = \frac{51}{51 + 11} \approx 0{,}82.$$

Далее вычислим полноту (*Recall*) по формуле:

$$Recall = \frac{TP}{TP + FN}.$$

Получим следующее значение:

$$Recall = \frac{51}{51 + 18} \approx 0{,}74.$$

F-мера вычисляется на основе значений полноты и точности. Чтобы добавить одной из этих величин определенный вес, то есть увеличить значимость при оценке, используется параметр β:

$$\begin{cases} 0 < \beta < 1, \text{если важна точность} \\ \beta > 1, \text{если важна полнота} \end{cases}.$$

В нашем случае большее значение имеет точность, поэтому выберем параметр $\beta = 0{,}5$.

Вычислим F-меру:

$$F_2 = (0{,}5^2 + 1) \cdot \frac{0{,}82 \cdot 0{,}74}{0{,}5^2 \cdot 0{,}82 + 0{,}74} \approx 0{,}79.$$

Таким образом, точность реализованного в сервисе биометрической аутентификации алгоритма составляет ~79 %.

Применением более точных алгоритмов можно улучшить точность распознавания голоса. Например, коэффициенты линейного предсказания (LPC) заменить на мел-частотные кепстральные коэффициенты (MFCC), а при создании сигнатуры голоса использовать модель смеси Гауссовых распределений (GMM) [15].

Заключение. Проверка личности используется как в простых системах для усиленной аутентификации, так и для подтверждения личности пользователя в различных критически важных операциях. Представленный мобильный сервис разработан с целью обеспечения проверки личности по требованию любого стороннего приложения, где требуются высокие стандарты безопасности.

Реализация сервиса под мобильные платформы выполнена с целью улучшить удобство его использования для широкой аудитории пользователей. Согласно проведенному аналитической компанией Pew Research Center [8] социальному опросу более 60 % взрослого населения пользуются смартфонами. Описанный в работе сервис устанавливается как приложение на смартфонах под операционную систему Android. При помощи разработанного специализированного протокола любое стороннее приложение может обратиться к сервису для дополнительной проверки права доступа.

Использование современных биометрических технологий защиты информации в данном сервисе гарантирует надёжность проверки вследствие уникальности биометрических данных.

Дополнительное сочетание в системе двухфакторной аутентификации нескольких механизмов биометрического доказательства права положительно сказывается как на уровне безопасности, так и на эффективности процесса аутентификации.

Шифрование конфиденциальной информации криптографическим методом, основанным на диофантовых уравнениях, направлено на уменьшение риска несанкционированного доступа к биометрическим данным в сервисе. Известно, что в общей постановке задача решения диофантовых уравнений в целых числах алгоритмически неразрешима, что приводит к высокой криптостойкости подобных алгоритмов шифрования.

Библиографический список

1. Петруненков, А. Эра биометрики / А. Петруненков // Директор информационной службы. – 2003. – № 12. – 24 дек.

2. История биометрии: от древности до начала XX века. – Режим доступа: https://worldvision.com.uk, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 13.02.2021).

3. Biometric data collection by country. – Режим доступа: https://www.comparitech.com, свободный. – Заглавие с экрана. Яз. англ. (дата обращения: 24.01.2021).

4. Jain, A. K. An introduction to biometric recognition / A. K. Jain, Arun Ross & Salil Prabhakar // IEEE Transactions on Circuits and Systems for Video Technology. – 2004. – Vol. 14t (1). – P. 4–20.

5. Kaspersky reports surge in cyber-attacks on selfies and others biometry // Biometric technology today. January 2020. – Режим доступа: https://www.biometricstoday.com, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 15.03.2021).

6. Ometov, Aleksandr. Multi-Factor Authentication: A Survey / Aleksandr Ometov, Sergey Bezzateev, Niko Mäkitalo, Sergey Andreev, Tommi Mikkonen, Yevgeni Koucheryavy. – 2018.

7. Quantized Convolutional Neural Networks for Mobile Devices. – Режим доступа: https://arxiv.org/abs/1512.06473, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 24.02.2021).

8. Osipyan, V. O. Development of information security system mathematical models by the solutions of the multigrade Diophantine equation systems / V. O. Osipyan, K. I. Litvinov, R. Kh. Bagdasaryan, E. P. Lukashchik, S. G. Sinitsa, A. S. Zhuk. – ACM Press, 2019. – P. 1–8.

9. Recognito: Text Independent Speaker Recognition in Java. – Режим доступа: https://github.com /amaurycrickx/recognito, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 16.02.2021).

10. Sabur, Ajibola Alim. Some Commonly Used Speech Feature Extraction / Sabur Ajibola Alim and Nahrul Khair Alang Rashid // Algorithms From Natural to Artificial Intelligence – Algorithms and Applications. – 2018.

11. Shor, P. Algorithms for Quantum Computation: Discrete Logarithms and Factoring / P. Shor // Foundations of Computer Science : Proceedings of the 35th Annual Symposium – IEEE, 1994. – P. 124–134.

12. SOLDEEA – Encryption algorithm based on system of linear diophantine equations. – Режим доступа: https://github.com/CrissNamon/soldeea, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 12.04.2021).

13. Sushil, Phadke. The Importance of a Biometric Authentication System / Sushil Phadke // The SIJ Transactions on Computer Science Engineering & its Applications (CSEA). – 2013.

14. Yutaka, Sasaki. The truth of the F-measure / Yutaka, Sasaki // School of Computer Science. – University of Manchester, 2007.

15. G. Suvarna, Kumar. Speaker recognition using GMM / G. Suvarna, Kumar // International Journal of Engineering Science and Technology. – 2010. – Vol. 2 (6). – P. 2428–2436.

References

1. Petrunenkov, A. Era biometriki [The Era of Biometrics]. *Direktor informatsionnoy sluzhby* [Director of Information Services], 2003, no. 12, December 24.

2. *Istoriya biometrii: ot drevnosti do nachala XX veka* [The history of biometrics: from antiquity to the beginning of the XX-th century]. Available at: https://worldvision.com. uk (accessed 13.02.2021).

3. *Biometric data collection by country*. Available at: https://www.comparitech.com (accessed 24.01.2021).

4. Jain, A. K. Ross, Arun, Prabhakar, Salil. An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 2004, vol. 14 (1), p. 4–20.

5. Kaspersky reports surge in cyber-attacks on selfies and others biometry. *Biometric technology today. January 2020*. Available at: https://www.biometricstoday.com (accessed 15.03.2021).

6. Ometov, Aleksandr, Bezzateev, Sergey, Mäkitalo, Niko, Andreev, Sergey, Mikkonen, Tommi, Koucheryavy, Yevgeni. *Multi-Factor Authentication: A Survey*, 2018.

7. Osipyan, V. O., Litvinov, K. I., Bagdasaryan, R. Kh., Lukashchik, E. P., Sinitsa, S. G., Zhuk, A. S. *Development of information security system mathematical models by the solutions of the multigrade Diophantine equation systems.* ACM Press, 2019, pp.1–8.

8. *Quantized Convolutional Neural Networks for Mobile Devices.* Available at: https://arxiv.org/abs/1512.06473 (accessed 24.02.2021).

9. *Recognito: Text Independent Speaker Recognition in Java.* Available at: https://github.com/amaurycrickx/recognito (accessed 16.02.2021).

10. Sabur, Ajibola Alim, Nahrul, Khair Alang Rashid. Some Commonly Used Speech Feature Extraction. *Algorithms From Natural to Artificial Intelligence – Algorithms and Applications*, 2018.

11. Shor, P. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. *Foundations of Computer Science : Proceedings of the 35th Annual Symposium on – IEEE*, 1994, pp. 124–134.

12. *SOLDEEA – Encryption algorithm based on system of linear diophantine equations*. Available at: https://github.com/CrissNamon/soldeea (accessed 12.04.2021).

13. Sushil, Phadke. The Importance of a Biometric Authentication System. *The SIJ Transactions on Computer Science Engineering & its Applications (CSEA)*, 2013.

14. Yutaka, Sasaki. The truth of the F-measure. *School of Computer Science*. University of Manchester, 2007.

15. G. Suvarna, Kumar. Speaker recognition using GMM. *International Journal of Engineering Science and Technology*, 2010, vol. 2 (6), pp. 2428–2436.