МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

ФГБОУ ВО «ПЯТИГОРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

«Социотехнические и гуманитарные аспекты информационной безопасности»

27-28 апреля 2022 г.

Материалы
III Всероссийской научно-практической конференции

Пятигорск 2022

УДК 004.056
ББК 32.97
С 693

Печатается по решению
редакционно-издательского совета
ФГБОУ ВО «Пятигорский
государственный университет»

«Социотехнические и гуманитарные аспекты информационной безопасности». Материалы III Всероссийской научно-практической конференции. Пятигорск: ПГУ, 2022. – 196 с.

Сборник содержит статьи по материалам докладов участников Всероссийской научно-практической конференции «Социотехнические и гуманитарные аспекты информационной безопасности».

Сборник адресован специалистам в сфере информационной безопасности, информационных технологий, гуманитарных наук, научно-педагогическим работникам. Материалы сборника могут применяться в научно-исследовательской и образовательной деятельности учебных заведений всех уровней образования.

Рецензенты: доктор технических наук, профессор **А.Б. Чернышев;** доктор психологических наук, профессор **С.В. Хребина.**

Материалы публикуются в редакции авторов

СОДЕРЖАНИЕ

М.С. Дедюрина, А.Д. Петухов,
г. Королёв, ГБОУ ВО МО «Технологического университета им. дважды Героя Советского Союза, летчика-космонавта А. А. Леонова»

БИОМЕТРИЧЕСКИЕ СИСТЕМЫ ИДЕНТИФИКАЦИИ. ТЕНДЕНЦИИ ИХ РАЗВИТИЯ В СОВРЕМЕННОМ МИРЕ

Аннотация: *В данной статье рассмотрен вопрос тенденций и развития биометрических систем идентификации. Уже сейчас технологии биометрические технологии внедряются во всех странах мира для защиты важной информации, а также в современных системах обеспечения безопасности. Назревшая необходимость использования более точных технологий идентификации человека для создания более высокой степени обеспечения конфиденциальности информации говорит об актуальности использования биометрических программных интерфейсов. Описываются мировые тенденции, а так же сферы, которые могут быть защищены данными технологиями. Кроме того, описывается, какие существуют типы систем биометрических данных.*

Ключевые слова: *информационная безопасность, биометрические системы идентификации, тенденции развития, биометрия.*

Annotation: *This article discusses the issue of trends and development of biometric identification systems. Biometric technologies are already being implemented in all countries of the world to protect important information, as well as in modern security systems. The urgent need to use more accurate human identification technologies to create a higher degree of ensuring the confidentiality of information indicates the relevance of using biometric software interfaces. Global trends are described, as well as areas that can be protected by these technologies. In addition, it describes what types of biometric data systems exist.*

Key words: *information security, biometric identification systems, development trends, biometrics*

История биометрии на государственном уровне началась с США, ведь инициатором внедрения биометрических идентификаторов (паспортов) были именно они: в 2002 г. Конгресс США принял Закон о защите государственных границ, в соответствии с которым граждане 27 стран мира, которые имели соглашения с США о безвизовом режиме, могли беспрепятственно въезжать на территорию США сроком до 90 дней только при условии наличия у них биометрических документов. С 2004 г. в США введена система снятия отпечатков пальцев и фотографирования всех прибывающих в Америку иностранцев (115 аэропортов, 14 морских портов, биометрическая база данных более чем на 5 млн человек). США участвуют в обмене биометрическими данными с многими странами

мира (Германия, Нидерланды, Финляндия, Испания, Греция, Южная Корея, Бельгия, Хорватия). Более 80 стран мира (включая Афганистан, Бахрейн, Кувейт, Оман, Катар, Саудовскую Аравию и ОАЭ) используют программы электронных паспортов, в которых содержатся биометрические данные. Многие страны в обязательном порядке заносят биометрические данные иммигрантов при въезде в страну.

В нашей стране так же используются биометрические данные, как пример, с 2015 г. в Российской Федерации выдается паспорт гражданина Российской Федерации нового образца с биометрическими данными (3D-фотография и отпечатки двух пальцев рук), удостоверяющий его личность за пределами территории Российской Федерации [6]. С конца 2017 г. выдаются водительские удостоверения нового образца, которые также содержат сведения о биометрических данных (отпечатки пальцев и изображение лица), а также разрабатывается удостоверение личности нового поколения с набором биометрических данных. Российские банки также активно используют биометрические данные в своей деятельности. Крупные банки уже применяют голосовые технологии в call-центрах, технологии распознавания изображения лица при повторном обращении клиента в отделение банка и в процессе кредитования, сканирование отпечатков пальца для входа в мобильное приложение (на определенных моделях мобильных телефонов) и для доступа к банковским ячейкам. Примером является банк ВТБ24, в 2017 г. они запустили пилот по подтверждению личности с использованием фотографии своих клиентов, а также их голоса. Около одной тысячи подписчиков мобильного приложения банка оставили записи голосов и фотографии, с которыми сравнивались селфи и разговоры при идентификации. В ВТБ планируют использовать технологию для подтверждения переводов на крупные суммы с мобильных телефонов. Злоумышленнику не поможет даже видеозапись клиента, так как его попросят произнести уникальную комбинацию цифр [4].

Основой на законодательном уровне для биометрических систем идентификации и безопасности в Российской Федерации являются: Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных», ст. 11, Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», ст. 14.1, а так же ГОСТ ISO/IEC 2382-37-2016 Информационные технологии. Словарь. Часть 37. Биометрия (принят протоколом МГС №93-П от 22 ноября 2016 г.), ГОСТ Р ИСО/МЭК 19794-2-2013 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца — контрольные точки, и др. [1, 2].

Биометрические технологии основаны на идентификации человека по уникальным, присущим только ему биологическим признакам. Выделяют два типа систем биометрических данных:

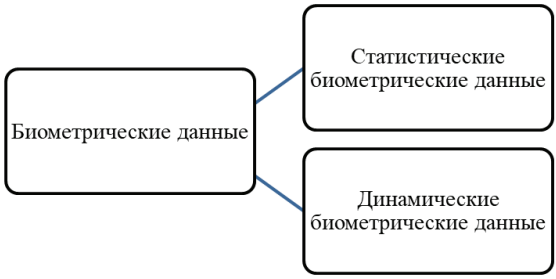

Рисунок 1- Виды биометрических данных

Первая группа биометрических данных (статистические) представляют собой уникальные набор признаков, которые присуще человеку от рождения (ДНК, отпечатки пальцев, геометрия руки, радужная оболочка глаза и иное).

Вторая группа биометрических данных – динамические. Данная группа представляет собой характеристики, приобретённые со временем или способные меняться с возрастом или под внешним воздействием (динамика воспроизведения подписи, походка, динамика набора текста, голос и иное).

Идентификация с использованием любых типов биометрических данных состоит из следующих этапов:

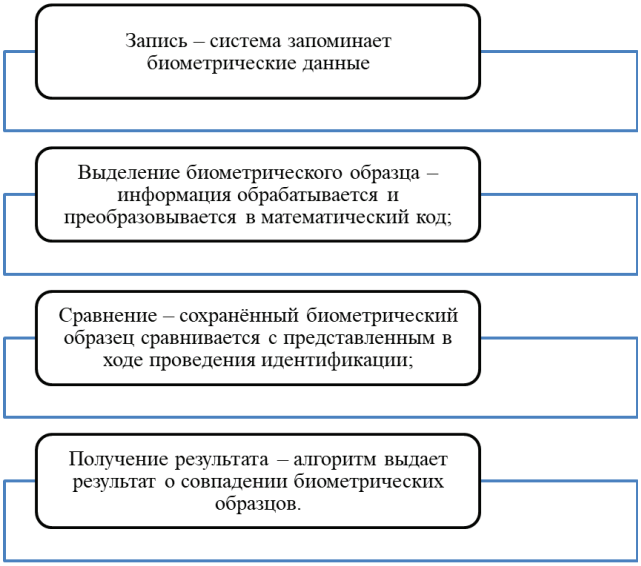

Рисунок 2- Этапы обработки биометрических данных

Заключение о совпадении/несовпадении идентификаторов может затем транслироваться другим системам (контроля доступа, защиты информации и т. д), которые далее действуют на основе полученной информации.

Диапазон проблем, решение которых может быть найдено с данных технологий, чрезвычайно широк:

- предотвратить проникновение злоумышленников на охраняемые территории и в помещения за счет подделки, кражи документов, карт, паролей;
- ограничить доступ к информации и обеспечить персональную ответственность за ее сохранность;
- обеспечить допуск к ответственным объектам только сертифицированных специалистов;
- процесс распознавания, благодаря интуитивности программного и аппаратного интерфейса, понятен и доступен людям любого возраста и не знает языковых барьеров;
- избежать накладных расходов, связанных с эксплуатацией систем контроля доступа (карты, ключи);
- исключить неудобства, связанные с утерей, порчей или элементарным забыванием ключей, карт, паролей;
- организовать учет доступа и посещаемости сотрудников [3].

Одна из самых важных характеристик систем защиты информации, основанных на биометрических технологиях, является высокая *надежность*, то есть способность системы достоверно различать биометрические характеристики, принадлежащие разным людям, и надежно находить совпадения. В биометрии эти параметры называются ошибкой первого рода (*False Reject Rate*, *FRR*) и ошибкой второго рода (*False* Accept *Rate*, *FAR*). Первое число характеризует *вероятность* отказа доступа человеку, имеющему *доступ*, второе – *вероятность* ложного совпадения биометрических характеристик двух людей. Подделать папиллярный узор пальца человека или радужную оболочку глаза очень сложно. Так что возникновение «ошибок второго рода» (то есть предоставление доступа человеку, не имеющему на это право) практически исключено. Однако, под воздействием некоторых факторов биологические особенности, по которым производится *идентификация* личности, могут изменяться. Например, человек может простудиться, в результате чего его голос поменяется до неузнаваемости. Поэтому частота появлений «ошибок первого рода» (отказ в доступе человеку, имеющему на это право) в биометрических системах достаточно велика. Система тем лучше, чем меньше *значение FRR* при одинаковых значениях *FAR*. Иногда используется и сравнительная характеристика EER (*Equal Error Rate*), определяющая точку, в которой графи-

ки *FRR* и *FAR* пересекаются. Но она далеко не всегда репрезентативна. При использовании биометрических систем, особенно системы распознавания по лицу, даже при введении корректных биометрических характеристик не всегда решение об аутентификации верно. Это связано с рядом особенностей и, в первую *очередь*, с тем, что многие биометрические характеристики могут изменяться. Существует определенная степень вероятности ошибки системы. Причем при использовании различных технологий ошибка может существенно различаться.

Не только *FAR* и *FRR* определяют качество биометрической системы. Если бы это было только так, то лидирующей технологией было бы *распознавание* людей по ДНК, для которой *FAR* и *FRR* стремятся к нулю. Но ведь очевидно, что эта технология не применима на сегодняшнем этапе развития человечества. Поэтому важной характеристикой является *устойчивость* к муляжу, скорость работы и *стоимость* системы. Не стоит забывать и то, что биометрическая характеристика человека может изменяться со временем, так что если она неустойчива – это существенный минус. Также важным фактором для пользователей биометрических технологий в системах безопасности является простота использования. Человек, характеристики которого сканируются, не должен при этом испытывать никаких неудобств. В этом плане наиболее интересным методом является, безусловно, технология распознавания по лицу. Правда, в этом случае возникают иные проблемы, связанные в первую *очередь*, с точностью работы системы [5].

Обычно биометрическая система состоит из двух модулей: *модуль* регистрации и *модуль* идентификации.

Модуль регистрации «обучает» систему идентифицировать конкретного человека. На этапе регистрации видеокамера или иные датчики сканируют человека для того, чтобы создать цифровое *представление* его облика. В результате сканирования чего формируются несколько изображений. В идеальном случае, эти изображения будут иметь слегка различные ракурсы и выражения лица, что позволит получить более точные данные. Специальный программный *модуль* обрабатывает это *представление* и определяет характерные особенности личности, затем создает *шаблон*. Существуют некоторые части лица, которые практически не изменяются с течением времени, это, например, верхние очертания глазниц, области окружающие скулы, и края рта. Большинство алгоритмов, разработанных для биометрических технологий, позволяют учитывать возможные изменения в прическе человека, так как они не используют для анализа области лица выше границы роста волос. *Шаблон* изображения каждого пользователя хранится в базе данных биометрической системы.

Модуль идентификации получает от видеокамеры изображение человека и преобразует его в тот же цифровой формат, в котором хранит-

ся *шаблон*. Полученные данные сравниваются с хранимым в базе данных шаблоном для того, чтобы определить, соответствуют ли эти изображения друг другу. Степень подобия, требуемая для проверки, представляет собой некий порог, который может быть отрегулирован для различного типа персонала, мощности *PC*, времени суток и ряда иных факторов.

Идентификация может выполняться в виде верификации, аутентификации или распознавания. При верификации подтверждается идентичность полученных данных и шаблона, хранимого в базе данных. *Аутентификация* - подтверждает соответствие изображения, получаемого от видеокамеры одному из шаблонов, хранящихся в базе данных. При распознавании, если полученные характеристики и один из хранимых шаблонов оказываются одинаковыми, то система идентифицирует человека с соответствующим шаблоном [8].

Объем мирового рынка биометрических систем на конец 2016 г., по данным международной консалтинговой компании J'son & Partners, оценивается на уровне 14,45 млрд долларов США. Согласно прогнозу, на ближайшие 6 лет показатель среднегодового темпа роста (CAGR) рынка биометрических технологий составит 18,6%, а прогнозируемый объем рынка к 2022 г. вырастет до 40,2 млрд долларов США.

Рисунок 3 – Объем рынка биометрических систем

На мировом рынке биометрических систем активно применяются технологии, основанные на распознавании и использовании следующих биометрических данных:

1. отпечатки пальцев (составляют более 50% всего объема рынка);

2. изображение лица (21,6%);
3. изображение радужной оболочки глаза (10,2%);
4. голос (4%);
5. рисунок вен (3%).
6. геометрия ладони, ДНК и иное (около 7%).

При этом, в соответствии с прогнозами, рынок технологий идентификации по отпечаткам пальцев в 2022 г. будет расти медленнее средних темпов роста всего рынка биометрических технологий, в результате чего данный сегмент сократит свою долю.

Самыми быстрорастущими сегментами в ближайшие 5-7 лет станут технологии идентификации по рисунку вен ладони, голосу и изображению радужной оболочки глаза.

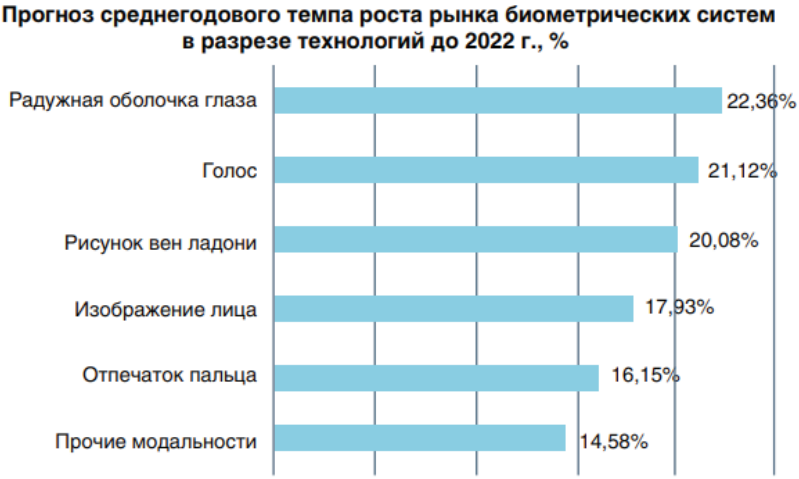

Рисунок 4 – Прогноз темпа роста биометрических систем

В настоящее время в мире продолжается поиск новых форм использования биометрических технологий: наблюдается тенденция перехода от их использования в традиционных системах государственной безопасности в сферу коммерческого и пользовательского применения.

По словам эксперта Рината Анисимова из компании «Smart Security», цитирую: «Распознавание походки. По сравнению с другими биометрическими модальностями, такими как лицо, радужная оболочка, отпечаток ладони и отпечаток пальца, идентификация человека по походке может успешно применяться для распознавания личности на расстоянии до 50 м даже при помощи видео низкого разрешения. На мой взгляд, идентификация по походке в сочетании с традиционной технологией портретной идентификации сыграет заметную роль в решении столь значимой

проблемы, как общественная безопасность. Например, такое сочетание может эффективно обеспечивать безопасность в аэропортах, стадионах».

В соответствии с международной классификацией можно выделить следующие ключевые сегменты рынка биометрических технологий по отраслям применения:

• государственный сектор: электронные документы, содержащие биометрические данные (e-passports, e-ID, электронные водительские удостоверения), национальные биометрические программы, а также системы национальной безопасности (за исключением систем, которые используются на транспорте и в иммиграционном контроле);

• путешествия и миграция: e-Visas , e-Gates , ABC-Kiosks и иное (все биометрические системы, используемые на объектах транспортной инфраструктуры и в иммиграционном контроле);

• финансовый сектор: финансы, банки, платежные системы и страхование;

• здравоохранение: как государственный, так и частный сектора;

• корпоративное использование: информационная безопасность (виртуальный контроль доступа), физический контроль доступа, учет рабочего времени в крупных организациях и иное.

Первоочередным фактором развития биометрических технологий в мире являются инициативы государств, направленные на обеспечение национальной безопасности. Практически во всех развитых странах биометрия активно используется в иммиграционном контроле: биометрические паспорта (в настоящее время используются в большинстве стран мира), оформление виз, идентификация беженцев, идентификация пассажиров и иное.

Многие страны в обязательном порядке заносят биометрические данные иммигрантов при въезде в страну. Крупнейшей в мире системой биометрической идентификации в настоящее время является Aadhaar (Индия). По состоянию на конец января 2018 г., в системе зарегистрировано более 1,19 млрд человек, что составляет свыше 99% граждан Индии в возрасте 18 лет и старше. Система реализована в рамках государственной программы Unique Identification Authority of India (UIDAI) [5].

Aadhaar представляет собой систему идентификации, запись в которой является удостоверением личности гражданина, состоящим из 12-значного уникального идентификационного номера (ID-card), выданным всем жителям Индии на основе их биометрических данных (фотография, 10 шаблонов папиллярных узоров пальцев рук, 2 шаблона радужной оболочки глаза) и персональных данных (дата рождения, Ф.И.О., пол, адрес, номер телефона и адрес электронной почты).

В некоторых странах мира для участия в выборах требуется сдать биометрические данные. Таким образом, крупнейшими сегментами мирового рынка биометрических систем является государственный сектор,

включая сферу миграции, а также сегмент путешествий. Третьим крупным рынком для биометрических систем является финансовый сектор, доля которого оценивается на уровне 15%. Доля сегмента здравоохранения составляет 9%. Доля Retail оценивается на уровне 5%. При этом наблюдается высокий темп роста использования биометрии в коммерческом сегменте. По прогнозам агентства FindBiometrics, рынок биометрических систем в ближайшие 5-7 лет будет более активно развиваться именно в коммерческом сегменте.

Из всех моделей многофакторной аутентификации наиболее распространенной (и традиционной) является двухфакторная аутентификация (например, пин-код или одноразовый пароль плюс биометрические технологии), которая используется в онлайн-банкинге, банкоматах, доступу к банковским ячейкам.

Решения трехфакторной аутентификации включают в себя смарт-карты с пин-кодом и биометрическими технологиями, смарт-карты с двумя технологиями биометрического распознавания, пин-код плюс два вида биометрических факторов. Такие решения используются в сферах, требующих высокой конфиденциальности, например, при обеспечении доступа к банковским сейфам, хранилищам секретных данных.

Четырех- и пятифакторная аутентификация строится на комбинации смарт-карты с пин-кодом и несколькими видами биометрического распознавания (лицо, отпечатки пальцев, радужная оболочка, голос). Такие системы применяются в сложных и дорогих проектах повышенной секретности. Например, Швейцарский банк «Pictet & Cie» для доступа к особой категории банковских ячеек использует четырёхфакторную идентификацию: флеш-накопитель (ключ) с пин-кодом, идентификация по радужной оболочке глаза и трехмерному изображению лица [7].

В данной статье были затронуты темы актуальности и перспектив использования биометрических технологий как в частном секторе, так и на государственном уровне. Также был проведен анализ рынка биометрических программных интерфейсов и более подробный анализ некоторых систем. На основании этого был сделан вывод о том, что данная отрасль активно развивается и дает возможность повысить уровень качества своих систем безопасности как внутренне, так и внешне, предоставляя гражданам не только возможность легкого доступа, например, к их банковским счетам, но и надежную охрану их персональных данных.

Библиографический список:

1. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных», ст. 11: с изменениями, вступившими в силу с 01.07.2020 [Электронный ресурс] // Правовая справочно-консультационная система URL: http://kodeks.systecs.ru/zakon/fz-152/glava2/st11.html (дата обращения: 27.02.2022)
2. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, инфор-

мационных технологиях и о защите информации», ст. 14.1: текст с изменениями и дополнениями на 2022 г. [Электронный ресурс] // Гарант: информационно-правовое обеспечение. URL: https://base.garant.ru/12148555/ (дата обращения: 28.02.2022)
3. ГОСТ ISO/IEC 2382-37-2016 Информационные технологии. Словарь. Часть 37. Биометрия (принят протоколом МГС №93-П от 22 ноября 2016 г.) // Гарант: информационно-правовое обеспечение. URL: https://base.garant.ru/71965400/ (дата обращения: 01.03.2022)
4. Статья ЦБРФ "ОБЗОР МЕЖДУНАРОДНОГО РЫНКА БИОМЕТРИЧЕСКИХ ТЕХНОЛОГИЙ И ИХ ПРИМЕНЕНИЕ В ФИНАНСОВОМ СЕКТОРЕ", 2018 г., [Электронный ресурс] // https://cbr.ru/Content/Document/File/36012/rev_bio.pdf (дата обращения: 03.03.2022)
5. Информационная безопасность в банках, 2020 [Электронный ресурс] // TADVISER: Государство, бизнес, IT. URL: http://www.tadviser.ru/index.php/ (дата обращения: 6.03.2022)
6. Биометрический рынок России: прогноз на 2015 год и перспективу / ООО «Биолинк Солюшенс». – М., 2014 – 17с. (дата обращения: 04.03.2022)
7. Перспективные технологии обеспечения ИБ, 2020 [Электронный ресурс] // IB-BANK.RU: отраслевой портал. URL: https://ib-bank.ru/bisjournal/news/12908 (дата обращения 20.04.2020)
8. НОУ ИНТУИТ, Биометрические системы информационной безопасности, Лекция 4. [Электронный ресурс] // URL: https://intuit.ru/studies/courses/10620/1104/lecture/24041

Е.А. Дербин
Москва, МГТУ им. Н.Э. Баумана

ПРОТИВОДЕЙСТВИЕ РАСПРОСТРАНЕНИЮ МИЛИТАРИСТСКОГО НАЦИЗМА (ФАШИЗМА) В ОБЩЕСТВЕННОМ СОЗНАНИИ КАК НЕЙТРАЛИЗАЦИЯ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИИ

Победа советского народа в Великой Отечественной войне памятна нам не только ощущением причастности к ней через подвиг наших предков или образом Победного знамени, развевающимся над рейхстагом. Любой здравомыслящий человек связан с Победой своей памятью о зверином оскале врага – носителя идеологии гитлеровского фашизма[1] и гер-

[1] Фашизм – обобщенное название крайне правых политических движений, идеологий и соответствующая им форма правления диктаторского типа, характерным признаком которых называют милитаристский национализм.