https://gospodarkainnowacje.pl

GOSPODARKA I INNOWACJE

LABORATORIUM WIEDZY Artur Borcuch

Volume: 42 | 2023

Economy and Innovation
ISSN: 2545-0573

For more information contact: editor@gospodarkainnowacje.pl

ПЕРСПЕКТИВЫ БИОМЕТРИИ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Жураев Дилшодбек Махсутали угли

Ассистент кафедры информационных технологий, Наманганский инженерно-технологический институт

ARTICLEINFO.

Ключевые слова: биометрические системы, идентификация, аутентификация, биометрические персональные данные, информационная безопасность.

Аннотация

В статье рассматривается использование биометрических систем в информационных системах с акцентом на обеспечение информационной безопасности. Анализируются потенциальные риски, которые могут оказать влияние на безопасность данных, а также предлагаются методы их снижения.

Для контроля доступа к информационным системам (ИС) далеко не последнюю роль играют процессы идентификации и аутентификации пользователей, которые позволяют определить пользователя по идентификатору и проверить его подлинность. И если в наиболее распространенном случае эти системы основаны на связке логин и пароль, т.е. пользователь должен запомнить эту комбинацию, то в последние годы возрастает популярность систем, использующих биометрические данные человека, которые всегда с нами и их невозможно забыть и потерять, что дает определенные удобства для пользователей, так как не требуется ничего запоминать или предъявлять каких-либо документов удостоверяющих личность. В данной статье речь пойдет о биометрических системах с точки зрения вопроса информационной безопасности, будут рассмотрены вопросы регулирования этого направления законодательством РФ, основные угрозы присущие этим системам и способы их минимизации. Биометрические системы и принципы их функционирования основаны на науке о биометрии и биометрических данных. Под наукой о биометрии подразумеваются способы автоматизированного распознавания человека по уникальным физическим или/и пси распознавание) и аутентификацию (она же верификация) и эти понятия, как может показаться на первый взгляд, далеко не одно и тоже. Под биометрической идентификацией (распознаванием) понимается база данных, в которой хранятся все полученные образцы какого-либо признака всех индивидов, для которых требуется предоставить доступ, и при сравнении с каждым из которых можно определить является ли заявитель тем, чей признак есть в базе или нет. Биометрическая аутентификация (верификация) представляет собой сам процесс сравнения признака из БД с предъявляемым для подтверждения истинности и принятия соответствующего решения о предоставления доступа к ИС. Биометрические данные можно разделить на три группы. Ниже представлена схема-классификация, на которой отображено деление на эти три группы и подвиды-представители технологий биометрии, которые относятся к этим группам (рис. 1). Под схемой дано краткое описание этих технологий: Физиологические характеристики: 1) Отпечатки пальцев: теория об их уникальности была выдвинута еще в 1877 году. В наши дни этот признак является одним из самых распространенных и хорошо изученных, практически в каждом

современном смартфоне есть датчик отпечатка пальца. 2) Геометрия кисти руки: для такого признака измеряется профиль руки, т.е. объем кисти и пальцев их длина, а также неровности ладони и расположение складок кожи на сгибах фаланг пальцев. 3) Радужная оболочка глаза: чтобы произвести распознавание используется видео захват с камеры с помощью программных средств выделяется область зрачка и самой радужной оболочки глаза. Далее полученное круговое изображение конвертируют в чернобелый прямоугольный формат iris code (подобие QR-кода). 4) Сетчатка глаза: метод основан на распознавании по уникальному рисунку сосудов и капилляров на сетчатке глаза. Сложен с технической точки зрения, может произойти отказ в распознавании в случае изменения рисунка от действия болезни или не правильном положении головы при сканировании. 5) Рисунок вен: бесконтактный способ распознавания, основан на способности гемоглобина крови поглощать инфракрасное излучение. В результате работы такого датчика, получают изображение, где рисунок вен выделен более темным цветом. 6) Лицо: данный вид технологии распознавания делится на два подвида: 2D и 3D распознавание. В основе двухмерного распознавания лежат плоские двухмерные изображения, лица на этих изображениях можно с помощью алгоритмов представить в виде графов со взвешенными вершинами и ребрами. Трехмерное распознавание представляет собой 3D сканирование лица с помощью специальных сканеров. Психологические характеристики: 1) Почерк и анализ рукописной подписи: применяют теорию нейронных сетей. На сегодняшний день это одна из самых лучших технологий для распознавания графических образов.

Рис. 1. Классификация средств биометрии

Использование искусственного интеллекта (ИИ) для распознавания биометрических данных имеет многочисленные перспективы и преимущества в различных отраслях. Вот некоторые из ключевых перспектив:

1. Повышенная безопасность:
- Точность: алгоритмы искусственного интеллекта могут повысить точность систем биометрического распознавания, снижая вероятность ложноположительных или ложноотрицательных результатов.
- Мультимодальная биометрия: искусственный интеллект позволяет интегрировать несколько биометрических методов (например, отпечатки пальцев, распознавание лиц, распознавание голоса) для более надежной и безопасной аутентификации.

2. Улучшенный пользовательский интерфейс:
- Удобство. Биометрическое распознавание на основе искусственного интеллекта обеспечивает удобство и удобство работы пользователя, устраняя необходимость в паролях или традиционных методах идентификации.
- Скорость: алгоритмы искусственного интеллекта могут быстро обрабатывать

биометрические данные, обеспечивая быструю аутентификацию и доступ.

3. Предотвращение мошенничества:
- Методы защиты от спуфинга: искусственный интеллект может использоваться для реализации передовых методов защиты от спуфинга для обнаружения и предотвращения мошеннических попыток обойти биометрические системы безопасности с использованием поддельных отпечатков пальцев, масок или других средств.
- Непрерывная аутентификация: ИИ обеспечивает непрерывный мониторинг биометрических функций во время взаимодействия с пользователем, обеспечивая дополнительный уровень безопасности от кражи личных данных.

4. Широкий спектр применения:
- Мобильные устройства: биометрическое распознавание на основе искусственного интеллекта все чаще используется в смартфонах и других мобильных устройствах для разблокировки, платежей и безопасного доступа.
- Финансовые транзакции: ИИ повышает безопасность финансовых транзакций за счет использования методов биометрической аутентификации, снижая риск несанкционированного доступа.

5. Здравоохранение и медицинское применение:
- Идентификация пациентов. ИИ может улучшить идентификацию пациентов в медицинских учреждениях с помощью биометрических данных, обеспечивая точный и безопасный доступ к медицинским записям.
- Мониторинг и оповещения. Биометрический мониторинг с помощью искусственного интеллекта можно использовать для обнаружения аномальных закономерностей или несанкционированного доступа к медицинским устройствам.

6. Кастомизация и адаптируемость:
- Адаптация машинного обучения. Системы искусственного интеллекта могут со временем адаптироваться и совершенствоваться посредством машинного обучения, что позволяет постоянно повышать точность биометрического распознавания.
- Профили пользователей: ИИ может создавать и постоянно обновлять профили пользователей на основе меняющихся биометрических характеристик.

7. Юридические и судебные применения:
- Идентификация преступников. Биометрическое распознавание на основе искусственного интеллекта имеет важное значение в криминалистических приложениях для идентификации преступников, помогая правоохранительным органам более эффективно раскрывать дела.
- Наблюдение: ИИ может анализировать большие объемы биометрических данных в режиме реального времени из систем наблюдения, помогая идентифицировать и отслеживать людей.

8. Проблемы конфиденциальности:
- Шифрование и защита: ИИ может использоваться для реализации надежных методов шифрования и мер защиты конфиденциальности для решения проблем, связанных с хранением и использованием биометрических данных.

Хотя перспективы многообещающие, крайне важно учитывать этические соображения, проблемы конфиденциальности и потенциальные предвзятости в алгоритмах ИИ, чтобы обеспечить ответственное и безопасное развертывание систем биометрического распознавания. Кроме того, должна быть создана нормативная база, регулирующая использование ИИ при обработке конфиденциальных биометрических данных.

Конкретно для этой задачи используют обучение нейронной сети с учителем. 2) Голос и ритм речи: голоса людей сильно отличаются и это обусловлено как физиологическими отличиями (в

росте, весе, поле, возрасте, размере рта), так и психологическими (в громкости, скорости, высоте, в особенности дыхания). Современные системы распознавания учитывают все эти факторы, разбивают запись голоса на «голосовые отпечатки» и далее производят их оцифровку и сравнение. 3) Скорость и особенность печати на клавиатуре: основными отличительными характеристиками клавиатурного ввода является период удержания клавиши нажатой и время паузы между нажатиями клавиш. Этот метод сложно применить по отношению к малоопытным пользователям, т.к. их клавиатурный почерк еще недостаточно полностью сформирован. В случае обычного пользователя на эти характеристики может повлиять психологическое состояние (усталость, возбужденность или внешние отвлекающие факторы). 4) Походка: каждый человек передвигает свое тело в пространстве уникально, так как он не просто переставляет ноги, хотя их тоже можно переставлять по разному (например, человек может быть пожизненно хромым или переставлять ноги с разной скоростью), но и дополнительно совершает различные движения, одними из таких движений являются взмахи руками с разной интенсивностью. Это дает возможность для каждого индивида выделить паттерны-образцы походки и на их основе распознать человека. К биохимическим характеристикам на данный момент времени можно отнести только один способ распознавания – ДНК (он же генетическая дактилоскопия). В любом биоматериале человека есть ДНК и по ее отличительным особенностям, выявляемым при анализе, можно однозначно определить индивида. С каждым годом популярность технологий распознавания растет как на российском рынке, так и на зарубежном и в связи с тем, что не существует абсолютно неуязвимых технологий эта сфера входит в интересы специалистов по информационной безопасности. Согласно исследованиям J'son & Partners Consulting, основанным на опросе 15 ключевых вендоров и 26 интервью с крупными заказчиками, к 2020 году прогнозируется рост объема мирового рынка биометрического распознавания до $40 млрд [5] (рис. 2). Уже сейчас практически все новые модели смартфонов и ноутбуков бизнес-класса оснащаются биометрическими датчиками. Например, в продукции Apple для массмаркета это технологии TouchID и FaceID, у Microsoft это WindowsHello. Если говорить о более серьезных отраслях таких как банки и бизнес системы, то биометрия начинает успешно внедряться и там. Например, начиная с лета 2018 года в России заработала Единая Биометрическая Система (далее ЕБС), оператором которой является «Ростелеком» и которая уже используется некоторыми крупными банками мира [5]. Как уже сказано не существует систем, которые не могли бы быть полностью неуязвимыми. Одним из векторов защиты от нарушения информационной безопасности может является соблюдение законодательства ИБ в данной сфере. Первым делом стоит понимать, что биометрические признаки всех трех групп относятся к персональным данным.

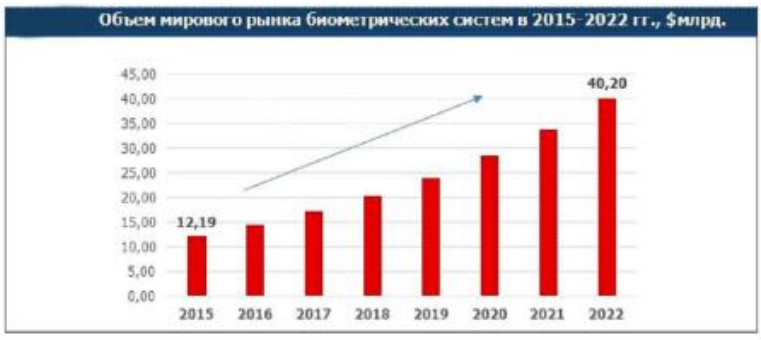

Рис. 2. Прогноз роста рынка биометрических технологий

С надежностью датчиков связаны следующие вероятностные понятия: 1. Ошибки первого рода (FRR – False Rejection Rate) – вероятность ложного отказа пользователю для которого должен быть предоставлен доступ. 2. Ошибки второго рода (FAR – False Acceptance Rate) – вероятность ошибочного предоставления доступа злоумышленнику. Отношение этих вероятностей показывает эффективность системы распознавания. Современные датчики и системы имеют

низкие показатели возникновения ошибок и высокую скорость при распознавании.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р ИСО/МЭК 19784-1-2007. – Электрон. текстовые дан. – Режим доступа: http:// docs.cntd.ru/document/gost-r-iso-mek-19784-1-2007 (дата обращения: 07.11.2019). – Загл. с экрана.
2. ГОСТ Р ИСО/МЭК 19795-1-2007. – Электрон. текстовые дан. – Режим доступа: http:// docs.cntd.ru/document/1200067413 (дата обращения: 07.11.2019). – Загл. с экрана.
3. ГОСТ ISO/IEC 2382-37-2016 Информационные технологии (ИТ). Словарь. Часть 37. Биометрия. – Электрон. текстовые дан. – Режим доступа: http://docs.cntd.ru/document/1200144206 (дата обращения: 23.10.2019). – Загл. с экрана.
4. Методические рекомендации по нейтрализации банками угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации. – Электрон. текстовые дан. – Режим доступа: http://www.cbr.ru/ content/document/file/62907/4mr.pdf (дата обращения: 07.11.2019). – Загл. с экрана.
5. Мировой рынок биометрических систем, 2015–2022 гг. – Электрон. текстовые дан. – Режим доступа: http://json.tv/ict_telecom_analytics_view/ mirovoy-rynok-biometricheskih-sistem-2015-2022-gg20170119025618 (дата обращения: 23.10.2019). – Загл. с экрана.
6. Обучение нейросети с учителем, без учителя, с подкреплением – в чем отличие? Какой алгоритм лучше? – Электрон. текстовые дан. – Режим доступа: https://neurohive.io/ru/osnovy-datascience/obuchenie-s-uchitelem-bez-uchitelja-s
7. ЦБ решил обязать банки оказывать услуги с использованием биометрии клиентов. – Электрон. текстовые дан. – Режим доступа: https:// www.interfax.ru/business/662298 (дата обращения: 07.11.2019). – Загл. с экрана.
8. Эксперты нашли способ обхода биометрической аутентификации по сосудам. – Электрон. текстовые дан. – Режим доступа: https:// www.securitylab.ru/news/497290.php (дата обращения: 23.10.2019). – Загл. с экрана.
9. Major Breach Found in Biometrics System Used by Banks, UK Police and Defence Firms. – Electronic text data. – Mode of access: https:// www.theguardian.com/technology/2019/aug/14/ majorbreach-found-in-biometrics-system-used-by-banks-ukpolice-and-defence-firms (accessed 23 October 2019).
10. The 2017 IARPA Face Recognition Prize Challenge (FRPC). – Electronic text data. – Mode of access: https://www.nist.gov/sites/default/files/ documents/2017/11/22/nistir_8197.pdf (accessed 23 October 2019).