

# БИОМЕТРИЧЕСКАЯ АУТЕНТИФИКАЦИЯ КАК СРЕДСТВО ЗАЩИТЫ ИНФОРМАЦИИ В СОВРЕМЕННОМ МИРЕ

Д. А. Горбачёва<sup>1)</sup>, Т. А. Онисько<sup>2)</sup>

<sup>1)</sup> *Белорусский государственный университет, пр. Независимости, 4, 2203030, Беларусь, fееebsee@gmail.com*

<sup>2)</sup> *Белорусский государственный университет, пр. Независимости, 4, 2203030, Беларусь, tayonisko@gmail.com*  
*Научный руководитель – Н. И. Шандора*

В современном мире вопрос защиты личных данных становится все актуальнее с каждым годом из-за растущей угрозы подмены и изменений правил защиты баз данных. Сегодня одним из самых лучших способов защиты от несанкционированного доступа к электронным данным является использование биометрических методов идентификации, которые разрабатываются для обеспечения высокого уровня безопасности, при этом оставаясь простыми и удобными в использовании.

**Ключевые слова:** биометрическая аутентификация; информационная безопасность; сканер.

Понятие «биометрика» происходит из греческих слов «bíos» и «metron», что в переводе означает «жизнь» и «мера». Таким образом, биометрика – система, идентифицирующая людей по уникальным признакам, таким как лицо, глазная сетчатка, радужная оболочка глаза, отпечатки пальцев и т.д. Такой способ защиты находит применение в следующих случаях: контроль доступа, онлайн просмотр доступа, предотвращение мошенничества, способ оплаты, аутентификация пользователя.

Биометрическая система состоит из двух этапов: регистрация и распознавание. Этап регистрации включает в себя предварительную обработку полученных данных и извлечение их характерных черт. Эти черты сохраняются в виде шаблонов в базе данных. Во время идентификации после процесса извлечения характеристик следует процесс принятия решения путем сравнения полученных данных с сохраненными шаблонами. Этот процесс регулируется путём использования порогового значения  $t$ . Если при сравнении полученных данных с шаблонами результат превышает  $t$ , это означает, что они принадлежат одному и тому же лицу. В противном случае они соответствуют разным лицам [1].

Современная биометрическая аутентификация опирается на два подхода:

- Статистический метод,
- Динамический метод.

Статистический метод аутентификации является основным на всемирном рынке биометрической защиты. Этот метод основан на распознавании физических характеристик человека, которые не меняются на протяжении всей жизни. К таким характеристикам относятся отпечатки пальцев, особенности глазной сетчатки и радужной оболочки глаза, геометрия лица и кисти руки, а также фрагменты генетического материала.

В статистический метод входят:

#### 1. Дактилоскопия.

Дактилоскопия – метод идентификации личности, основанный на уникальном рисунке папиллярных линий кожи на пальцах и ладонях, который является индивидуальным для каждого человека.

На сегодняшний день использование сканера отпечатка пальца является самым распространённым биометрическим методом в силу легкости его использования. Главным устройством этого метода является небольшой по размеру и относительно недорогой сканер. Идентификация осуществляется быстро за счёт того, что системе достаточно обнаружить совпадения в крупных участках папиллярного рисунка, а также проанализировать такие особенности, как разветвления, разрывы и другие искажения линий (минуции).

В зависимости от принципа работы, сканеры делятся на три типа: оптические сканеры, полупроводниковые сканеры, ультразвуковые сканеры.

#### 2. Аутентификация по сетчатке глаза.

Сканеры сетчатки глаза обладают большими габаритами и большей стоимостью, чем сканеры отпечатков пальцев. В основе технологии такого метода лежит неповторимость кровеносных сосудов на сетчатке глаза, что подразумевает высокую надёжность и невозможность обмана сканера. Сбои при распознавании сетчатки очень малы – один на миллион случаев.

#### 3. Аутентификация по радужной оболочке.

Данный биометрический метод основывается на том, что структуру радужной оболочки глаза очень трудно воспроизвести, что является надёжным источником для идентификации. Специальные камеры используются для захвата рисунка радужной оболочки с расстояния от 10 до 40 см, а затем программное обеспечение оцифровывает одну из записей и преобразовывает его в упрощённую версию, из которой происходит отбор 200 характерных точек и их данные заносятся в шаблон.

#### 4. Аутентификация по геометрии руки.

Метод биометрической аутентификации по геометрии руки основывается на измерении конкретных характеристик человеческой кисти, таких как длина, толщина, изгибы пальцев, общая структура ладони, ее ширина и толщина и т.д. Собрав эту информация, система строит 3D-модель кисти.

Достоинствами данного метода являются:

- Ни влажность, ни загрязненность ладони не влияют на аутентификацию.

- Может быть использовано изображение низкого качества.

- Алгоритм сравнения полученных данных с шаблоном очень прост.

Однако, в связи с тем, что вероятность ошибки при распознавании составляет 0,1%, при ушибах и прочих повреждениях руки аутентификацию пройти не удастся. Устройства аутентификации по геометрии руки могут иметь разнообразную конфигурацию и возможности – одни сканируют лишь два пальца, другие делают снимок всей кисти, а некоторые новейшие модели с помощью инфракрасной камеры сканируют вены и выполняют аутентификацию по их изображению.

#### 5. Аутентификация по геометрии лица.

Метод биометрической аутентификация по геометрии лица предполагает фотографирование и сканирование лица. Программа выделяет до 45 специфических характеристик (например, форму и размеры носа, глаз, бровей, губ и т.д.), что позволяет создать уникальный шаблон для распознавания личности пользователя.

В настоящее время существует 2 вида распознавания: двухмерное (2D) и трехмерное (3D).

Двухмерное распознавание существует уже очень давно и в большинстве случаев используется в криминалистике. Трехмерное распознавание является новым методом, надёжность которого пока не определена. Сама процедура сканирования занимает 30 секунд. Системы выделяют черты лица, такие как контур глаз, губ, бровей, носа и т.д., и определяет расстояние между ними. Шаблон состоит из формы черепа, высоты и ширины скул, надбровных дуг и других особенностей. Всего используется 12–40 специфических характеристик.

Динамический метод аутентификации основан на поведенческих данных человека, таких как голос, подпись, клавиатурный почерк.

В динамический метод входят:

##### 1. Распознавание голоса.

Метод распознавания голоса основан на характеристиках голоса, таких как тональность, интонация, модуляция и произношение звуков речи. Присутствует небольшой процент ошибок, вызванный изменчивостью голоса. На голос может повлиять болезнь, психическое состояние, а также возраст человека. Из-за этого, данный метод не рекомендуется для объектов повышенной безопасности, но эта технология активно применяется в голосовых помощниках.

##### 2. Клавиатурный почерк.

Метод распознавания клавиатурного почерка основан на характеристиках поведения пользователя при вводе текста, таких как скорость ввода, интервалы между нажатиями клавиш, ошибки при вводе и другие параметры. Аутентификация по клавиатурному почерку может осуществляться через ввод известной фразы или случайно сгенерированной фразы. Процесс включает режим обучения, где система формирует шаблон показателей пользователя на основе многократного ввода определённого слова, и режим самой аутентификации. Преимуществами данного метода являются удобство использования, возможность аутентификации без специального оборудования и скрытая аутентификация.

### 3. Подпись.

Метод аутентификации по подписи основан на анализе визуальных характеристик и динамических характеристик написания подписи. Образец подписи формируется с учетом требуемого уровня защиты и содержит информацию о координатах пера, угле наклона и нажатии. Однако, этот метод также зависит от самочувствия человека, подобно методу распознавания клавиатурного почерка [2].

Комбинированные решения биометрической аутентификации объединяют несколько биометрических технологий в одном устройстве. Они считаются наиболее надежными, так как подделать несколько биометрических показателей сложнее, чем один. Популярными комбинациями являются проверка радужной оболочки и отпечаток пальца или отпечаток и геометрия руки.

В заключение, применение и безопасность каждой биометрической техники аутентификации различны и зависят от цели и контекста использования. Биометрия представляет будущее аутентификации, обеспечивая удобство, экономичность и высокий уровень безопасности. Однако необходимо учитывать потенциальные проблемы, такие как подделка и компрометация или изменение биометрических данных, а также правовые вопросы.

### **Библиографические ссылки**

1. Challenges and opportunities in biometric security: A survey [Electronic resource]. URL: <https://sci-hub.se/10.1080/19393555.2021.1873464> (date of access: 09.05.2024).
2. Trends in Biometric Authentication: A review [Electronic resource]. URL: [https://journals.ekb.eg/article\\_320990\\_e4e226d840fa356725ba5bd699e0b61f.pdf](https://journals.ekb.eg/article_320990_e4e226d840fa356725ba5bd699e0b61f.pdf) (date of access: 09.05.2024).