*Д. В. Соколов*

# ПОНЯТИЕ «БИОМЕТРИЯ». БИОМЕТРИЧЕСКИЕ АУТЕНТИФИКАЦИОННЫЕ ПРОТОКОЛЫ

Биометрия — это комплекс постоянно развивающихся технологий, которые дали начало новой перспективной науке [1]. В том же источнике дано другое, более точное, определение: биометрия — это наука об идентификации или верификации личности по физиологическим или поведенческим отличительным характеристикам. Исследования в области биометрии начались полтора века назад с методов сравнения отпечатков пальцев, основанных на идеях англичанина Уильяма Гершеля, выдвинувшего в 1877 г. гипотезу о неизменности папиллярного рисунка ладонных поверхностей кожи человека.

Различают два вида биометрических параметров:

1. *Физиологические* — являются физическими характеристиками человека, которые измеряются в определенный момент времени (отпечатки пальцев, сетчатка глаза и т. д.);

2. *Поведенческие* — представляют собой последовательность действий и длятся в течение определенного периода времени (подпись, голос, походка и т. д.).

Биометрические параметры обладают рядом свойств, которые описаны Кларком:

1. *Всеобщность:* каждый человек имеет биометрические характеристики;

2. *Уникальность:* для биометрии нет двух людей, обладающих одинаковыми биометрическими свойствами;

3. *Постоянство:* биометрические характеристики стабильны во времени;

4. *Измеряемость*: биометрические характеристики измеряемы каким-либо физическим считывающим устройством;

5. *Приемлемость:* общество в целом не должно возражать против измерения и сбора биометрических параметров [2].

Комбинация этих свойств определяет эффективность аутентификационных систем [3]. Любой метод биометрической аутентификации — результат компромиссов, так как нет биометрических параметров, которые абсолютно удовлетворяют любому их этих требований. Как нет и тех, которые сочетали бы в себе все эти свойства одновременно, особенно если учитывать пятое свойство.

На данный момент существует шесть наиболее разработанных биометрических параметров: лицо, отпечатки пальцев, геометрия руки, радужная оболочка (не путать с сетчаткой глаза — это разные способы аутентификации), подпись, голос. Биометрические параметры, которые используются реже: ДНК, форма ушей, запах, сетчатка глаза, кожное отражение, термограмма, походка, клавиатурный почерк.

В биометрии различают два аутентификационных метода:

1. *Верификация* — основана на биометрическом параметре и уникальном идентификаторе конкретного человека. Измеренные параметры сравниваются с одной записью из базы данных зарегистрированных пользователей, выбранной на основании идентификатора, и принимается решение о принятии или отказе. Следовательно, верификационные системы совершают одно сопоставление 1:1.

2. *Идентификация* — основана исключительно на биометрических измерениях, и ее можно рассматривать как «чистую» биометрическую аутентификацию. Измеренные параметры сравниваются один за другим со всеми записями из базы зарегистрированных пользователей для определения, есть ли в ней шаблоны, имеющие сходство с вводимым образцом биометрического параметра объекта. Базы данных содержат биометрические образцы или репрезентации

биометрических образцов, называемые *шаблонами*, которые могут содержать репрезентации нескольких биометрических образцов. Системы совершают множество сопоставлений: каждый из биометрических образцов сопоставляется с каждой записью из базы данных, сопоставление 1: m. В итоге может быть найдено несколько кандидатов, имеющих сходство с объектом.

Существует два вида идентификации:

*а) положительная* — система определяет, зарегистрирована ли данная личность в базе данных;

*б) отрицательная* — в этом случае система проверяет *отсутствие* объекта в некоторой отрицательной базе данных. Это может быть, например, база данных разыскиваемых преступников. Отрицательная идентификация еще называется *сортировкой*, так как входящие объекты сортируются относительно базы данных.

Существует две возможные конфигурации базы данных:

1. *Централизованная* — хранит биометрическую информацию всех зарегистрированных объектов, пользователь предоставляет идентификационный знак, после чего система может найти в базе данных соответствующий биометрический шаблон для дальнейшего сравнения с биометрическим образцом объекта;

2. *Распределенная* — хранит биометрическую информацию в распределенном виде, например, смарт-карта. Объект предоставляет системе один биометрический шаблон, записанный на носителе. Биометрическая система сравнивает этот шаблон с биометрическим образцом, предоставленным человеком.

На практике многие системы используют базы данных обоих типов (распределенная — ежедневной оффлайновой верификации, централизованная — онлайновой верификации).

Любую биометрическую аутентификационную систему можно представить как систему распознавания образцов, состоящую из подсистем регистрации и аутентификации (рис. 1).

Задача регистрационного модуля — зафиксировать параметры объекта и сохранить их в базе данных. Задача аутентификационного модуля — распознать объект и идентифицировать либо верифицировать личность.

Существует два вида регистрации:

1. *Положительная* — регистрация для верификации и положительной идентификации. Цель такой регистрации — создать базу данных легитимных объектов.

2. *Отрицательная* — регистрация для негативной идентификации — представляет собой данные об объектах, которые не допускаются к каким-либо приложениям (базы данных являются централизованными).

В биометрических системах могут возникнуть ошибки: *ложное отрицание*, т. е. отказ в доступе подлинному пользователю (коэффициент ложного отказа доступа); *ложное признание*, т. е. разрешение доступа злоумышленнику (коэффициент ложного доступа). Данные ошибки не могут быть измерены, их можно подсчитать только приблизительно.

Основные требования, предъявляемые к биометрическим системам, следующие: скорость вычисления; масштабируемость; обработка исключительных случаев; стоимость системы; безопасность; точность. В процессе разработки учитываются многие факторы, в числе которых: методика измерений биометрических параметров; методы эффективного поиска в базе данных; определение набора неизменных признаков и признаков, доступных для автоматического сопоставления; определение показателей для сопоставления двух образцов, которые выразили бы сходство между ними; сведение к минимуму частоты исключительных случаев.

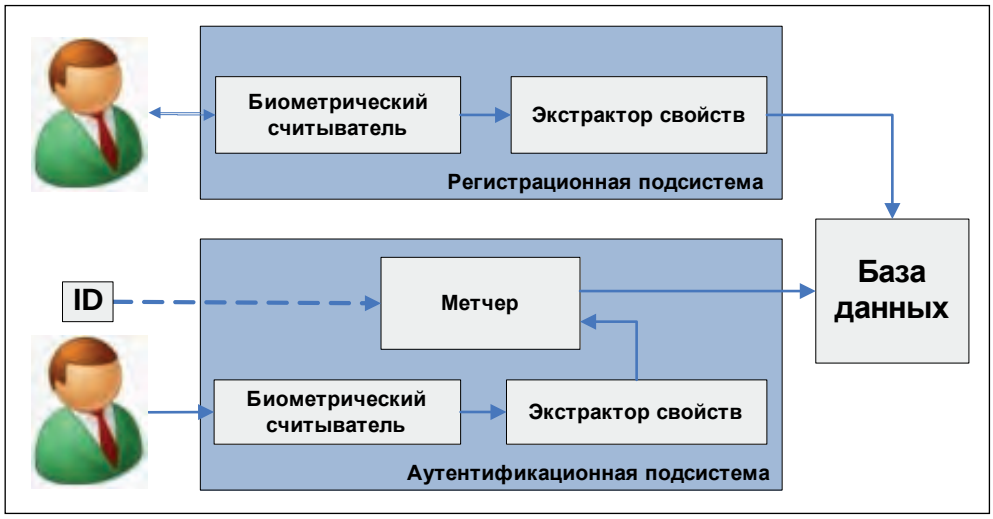


*Рис. 1. Система распознавания образцов*

Существует три основных метода авторизации объектов, описанных Миллером в [4]: $P$ — по собственности, $K$ — по знаниям, $B$ — по биометрическому параметру. Примеры методов аутентификации с их положительными и отрицательными свойствами: *то, что имею* $(P)$ — ИН пользователя, кредитные карты, бейджи, ключи (можно обменять, сделать дубликат, потерять или может быть украдено); *то, что знаю* $(K)$ — пароль, ПИН, девичья фамилия матери, личная информация (большинство паролей несложно угадать, можно передать другим или забыть); *уникальные характеристики пользователя* $(B)$ — отпечатки пальцев, лицо, радужная оболочка, запись голоса (невозможно передать другим, отказ от авторства маловероятен, очень сложно подделать, нельзя потерять или украсть).

*(номер счета, пароль)* = *(Собственность, Знания)* = $(P, K)$, вероятно, является наиболее распространенным аутентификационным методом. При использовании собственности и знаний происходит сравнение информации, при этом пользователь не связывается с установленной «личностью». Но личность, определяемая по владению собственностью $P$, связывается с анонимным паролем $K$, а не с реально зарегистрированным человеком.

Аутентификационный биометрический метод $B$ обеспечивает дополнительную защиту благодаря сложности замены биометрических параметров, поэтому метод установления подлинности пользователей является более надежным и заслуживает доверия.

Так как биометрические параметры являются неотъемлемыми свойствами человека, их очень тяжело подделать или обменяться ими без его ведома, а измениться они могут только в случае серьезной травмы, некоторых болезней или разрушения тканей. Поэтому биометрические идентификаторы могут подтвердить личность пользователя в аутентификационном протоколе, что не способны сделать методы, в которых используются собственность и знания. При комбинировании метода $B$ с методом $P$ и (или) $K$ получаются дополнительные биометрические методы.

*Протокол* — это определенная последовательность шагов двух и более сторон, которые собираются решить какую-либо задачу. Порядок шагов очень важен, поэтому протокол регулирует поведение двух сторон.

*Аутентификационный протокол* — это (автоматизированный) процесс принятия решения, действительно ли удостоверяющие данные объекта являются достаточными для подтверждения его личности, чтобы разрешить ему доступ на основе этих удостоверяющих данных или других признаков. Аутентификационный протокол должен иметь характеристики: установлен заблаговременно, взаимно согласован, недвусмыслен, детален. Любой аутентификационный протокол, в котором

используются различные методы (и различные биометрические идентификаторы), может быть определен и выполнен на основе представленных удостоверяющих данных.

Ряд признаков $T = \{x_1, x_2, \ldots x_n \mid x_i \in (P, K, B)\}$ — это только часть аутентификационного протокола. Кроме них необходим набор правил, который определит аутентификационный протокол $A_\rho$, использующий T как точно установленную последовательность шагов и правил поведения. Чем больше в протоколе будет аутентификационных методов (особенно $B$), тем достовернее будет аутентификация. Примером аутентификационного протокола является система Гальтона—Генри (методика опубликована в июне 1900 г., через год введена в Скотланд-Ярде) — метод ручной классификации отпечатков пальцев на основе 10 карточек, адаптирована для автоматизированных систем.

В дополнение к ряду признаков $T = \{P, K, B\}$ и правилам работы с ними $A_\rho(T)$ аутентификационный протокол требует наличия возможности сопоставления. Биометрические образцы $B$ можно только сравнивать при помощи техник распознавания, так как две машинные репрезентации, полученные из двух образцов биометрических параметров β, никогда не будут одинаковыми из-за присутствия шума. Биометрический шаблон — это машинная репрезентация биометрического образца $B$ в терминах свойств (например, отпечатки пальцев, расстояние между глазами, длина пальцев).

Стандартный биометрический метчер — это устройство, выполняющее сравнение двух биометрических параметров. Он выполняет простой протокол для определения идентичности двух реальных биометрических параметров $\beta_1$ и $\beta_2$ и решает вопрос, принадлежат ли они одному объекту $d$. Биометрический метчер вычисляет *величину* $s$, которая выражает степень сходства $s(B_1, B_2)$ между шаблонами, полученными из биометрических образцов $B_1 = f(\beta_1)$ и $B_2 = f(\beta_2)$:

$s = s(B_1, B_2) = s(f(\beta_1), f(\beta_2))$.

Биометрическая часть аутентификационного протокола использует величину $s$ для принятия решения, основываясь на пороговой величине $T$:

если $s > T$, значит, $\beta_1$ и $\beta_2$ совпадают,

если $s \leq T$, значит, $\beta_1$ и $\beta_2$ не совпадают.

Из вышесказанного вытекают три главных аспекта разработки биометрической системы:

- получение биометрических образцов или сигналов $B = f(\beta)$;
- функция сходства между двумя шаблонами $s = s(B_1, B_2)$;
- пороговая величина принятия решения или сходства T.

Основные статистические методы, применяемые при анализе биометрических данных, рассмотрены в книге [5].

Существуют различные варианты использования биометрических технологий:

1. *Автоматическая положительная идентификация*. Для аутентификационного протокола системе требуется представление только биометрического параметра. Объект $d$ предоставляет параметр β, сенсор снимает с него образец $f(\beta)$, из этого образца получается биометрический шаблон $B$, далее определяется сходство $s_i = s(B, B_i)$ между шаблонами $B$ и $B_i$ согласно записям в базе данных. Если $s_i > T$, то $d = d_i$, а если $s_i \leq T$, то $d \neq d_i$. Этому критерию может удовлетворять множество $d_i \in M$, и тогда система выдаст список кандидатов $C = \{d_a, d_b, \ldots\}$.

2. *Отбор*. Это отрицательная идентификация, показывающая, что человек не входит в список «интересующих» людей.

3. *Верификация*. Объект $d$ предъявляет идентификационный номер $m$ и биометрический параметр β для получения образца $f(\beta)$. Экстрактор свойств вычисляет биометрический шаблон $B$, шаблон $B_i$, связанный с $i$, извлекается из базы данных $M$. Тогда биометрический метчер подсчитывает значение $s = s(B, B_i)$: если $s > T$, то $d = d_i$ и объект допускается к приложению; если наоборот, то $d \neq d_i$ и объект получает отказ.

4. *Целостность личности*. Спустя некоторое время работы может возникнуть необходимость перепроверить аутентификационные данные, которые предоставил пользователь, чтобы удостовериться, что в системе работает тот же человек. Например, проверка происходит в процессе визуального наблюдения, когда система следит за перемещением человека в пространстве. Пока система наблюдает за человеком, она может утверждать, что это один и тот же объект. Таким образом, любая выполненная аутентификация человека распространяется на весь период отслеживания.

5. *Верификация с помощью человека*. Метод заключается в том, что проверяющим выступает человек, аутентификационными данными являются ($P$, $B$). В этом случае точность зависит от конкретного человека, от его утомленности, отношения к работе, условий работы, состояния здоровья и т. д. В среднем количество ошибок составляет 1 на 1000 [1]. Наверное, самый распространенный пример — это аутентификация по «лицу» и «подписи»: паспорт с фотографией, кредитная карта с подписью.

Из вышесказанного видно, что разница между биометрическими и другими идентификаторами — это понятие степени сходства, основа технологии сравнения. Аутентификационный протокол, использующий пароль, всегда выдает точный, двойной результат: истина или ложь. Биометрия же использует теорию вероятности и статистические методы для анализа вероятности сходства. Это выражается в коэффициентах ошибок.

Способность сравнивать различные виды идентификаторов из $T = \{P, K, B\}$ является одной из проблем биометрической аутентификации. Чтобы принять решение о сходстве признаков, необходимо интегрировать отдельные результаты сопоставления метчеров. Возможность объединения нескольких биометрических параметров является объектом повышенного внимания исследователей. В этом случае запрашиваемые удостоверяющие данные T могут включать в себя разные биометрические параметры, т. е. $\{B_1, B_2\}$, где, например, $B_1$ — палец, а $B_2$ — лицо.

Слабое место биометрических технологий — вероятность обмануть аутентификационную систему при помощи подражания, когда биометрическая информация представляется в отсутствие ее владельца. Например, могут сниматься латентные отпечатки пальцев или совершаться насильственные действия для их снятия (отрезание пальцев). Опасения насильственных действий над личностью препятствуют распространению биометрических технологий. Хотя снять латентные отпечатки пальцев, это, по сути, то же самое, что подсмотреть вводимый пароль. Но использовать чужие биометрические параметры гораздо сложнее, чем подсмотренный пароль.

В качестве заключения необходимо отметить, что биометрия не является независимой наукой. Все актуальные направления биометрии изначально появились в рамках других дисциплин. Обработка сигналов и изображений, распознавание речи, компьютерное зрение, теория распознавания патеров — все это связано с развитием биометрии. Биометрические технологии имеют как технические и прикладные, так и социально-правовые аспекты. А при разработке и внедрении учитываются вопросы эргономики и безопасности, точности и скорости распознавания данных, стоимости системы и администрирования.

## СПИСОК ЛИТЕРАТУРЫ:

1. *Болл Р. М., Коннен Дж. Х., Панканти Ш., Ратха Н. К., Сеньор Э. У.* Руководство по биометрии. М.: Техносфера, 2007.
2. *Clarke R.* Human identification in information systems: Management challenges and public policy issues // Information Technology & People. December 1994. № 7 (4). P. 6–37.
3. *Jain A. K., Bolle R. M. and Pankanti S.* (Eds.). Biometrics: Personal Identification in Networked Society. Boston, MA: Kluwer Academic Publishers, 1999.
4. *Miller B.* Vital signs of identity // IEEE Spectrum. February 1994. Vol. 31. № 2. P. 22–30.
5. *Глотов Н. В., Животовский Л. А., Хованов Н. В., Хромов-Борисов Н. Н.* Биометрия. Л.: ЛГУ, 1982.