

УДК 004

СОВРЕМЕННЫЕ СПОСОБЫ БИОМЕТРИЧЕСКОЙ
АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ

Закурдаев А.Д., студент гр. ИЭэ 49-23, 1 курс
Научный руководитель: Агуреев И.А.,
старший преподаватель кафедры безопасности и информационных
технологий, Национальный исследовательский университет «МЭИ»,
г. Москва

Аутентификация (процедура проверки подлинности пользователя) может проводиться различными способами, в том числе при помощи биометрии, использующей при создании различных автоматических систем разграничения доступа уникальные биометрические признаки, присущие конкретному человеку. Основной принцип функционирования систем биометрической аутентификации - сопоставление набора уникальных индивидуальных характеристик пользователя с образцом, внесенным в базу.

Биометрические характеристики личности традиционно делят на физические (статические, основанные на уникальных физиологических характеристиках человека, присущих ему от рождения до смерти) и поведенческие (динамические, основанные на воспроизведении движений в процессе повторения какого-либо действия).

Статическая биометрическая аутентификация пользователя может проводиться с использованием следующих методов:

	Способ (метод) аутентификации	Достоинства	Недостатки	Оборудование
1	По отпечаткам пальцев (дактилоскопия)	Возможность создания электронной базы образцов для правоохранительных органов. Сканер имеет небольшие размеры, дешев, быстрая процедура проведения сканирования и распознавания. Можно использовать в быту – на компьютере или смартфоне.	При недостаточном контакте пальца со сканером может быть сбой, нельзя применять к людям с некоторыми физическими недостатками. Кроме того, можно обмануть систему с помощью муляжа или мертвого пальца. Контактный метод, не подходит для аутентификации в многопользовательском режиме (из-за соображений гигиены).	Sherlock, СОП 1 и СОП 2 («Интек»)
2	По сетчатке глаза	Обмануть сканер практически невозможно, потому что рисунок кровеносных	Сканеры имеют большие размеры и дороги. Если имеются заболевания глаза (например, ката-	HBOX (EyeLock)

		сосудов глазного дна не повторяется даже у близнецов.	ракта), нельзя использовать. Нельзя использовать для быстрой аутентификации большого количества людей.	
3	По радужной оболочке	При сканировании обоих глаз очень надежный способ. Считывающая камера находится на расстоянии до одного метра от глаз, процесс распознавания быстрее.	Стоимость дороже, чем сканер сетчатки глаза.	Iris Access, «Взор»
4	По геометрической форме руки	Сканер руки удобен и распознавание не отнимает много времени. Можно использовать шаблон низкого качества, на распознавание не влияют температура, влажность, чистота рук.	Форма руки человека не уникальна, необходимо использовать многофакторную аутентификацию. Способ не подходит для обеспечения безопасности на объекты высокой степени секретности, есть вероятность ошибки.	HandKey II
5	По геометрической форме лица	Аутентификация при помощи трехмерного изображения достаточно надежна, процедура сканирования занимает до 30 секунд.	Аутентификация при помощи двухмерного изображения используется в криминалистике, не исключены ошибки.	Blink Identify, «Face-Интеллект», PERCo-Web, ПАК «Визирь»
6	По термограмме лица	Лицо сканируется при помощи инфракрасного света и отображается температурная карта лица, которая является уникальной. Расстояние сканирования – 10 метров, что комфортно для человека. Не влияет старение, пластические операции, можно распознавать близнецов.	Качество получаемых термограмм низкое, метод не получил широкого распространения.	Estone FSAC-80
7	По рисунку вен (васкулярная аутентификация ладони)	Быстрое сканирование, бесконтактное, возможно в общественных местах. Под воздействием специального сенсора кровь в венах проявляется в виде индивидуального узора. Высокий уровень точности.	Не получила широкого распространения.	FingoPay, M2SYS Bio-Plugin, Palm Jet

8	По фрагментам генетического кода (ДНК)	Единственная форма биометрии, которая позволяет отслеживать родственные связи, высока точность измерений.	Дорогой метод, используется в основном в судебной медицине. Однояйцевые близнецы имеют одну и ту же ДНК.	Не используется в гаджетах из-за проблем со сбором материала
9	По форме ушной раковины	Измеряют акустику уха при помощи специальных наушников и неслышимых звуковых волн, дешевый способ. Высокая точность - 99,6%	Не получила широкого распространения	В разработке
10	По запаху тела / химическому составу пота	Состав аминокислот в нашем поте уникален, однако точность аутентификации составляет 85 %	Не получила широкого распространения	В разработке
11	Индивидуальная биоакустическая подпись	Звуковые волны от передатчика через пальцы проникают в тело человека и создают микровибрации уникального спектра, точность – 97 %.	Не получила широкого распространения	В разработке
12	Передача цифрового сигнала через тело человека	Система биометрии состоит из приёмника и передатчика, в качестве способа связи используется электромагнитное поле малой мощности. Передатчик в виде наручного браслета создает низкочастотное магнитное поле, которое проходит через тело человека по пути к приемнику, перехватить такой сигнал, в отличие от NFS, невозможно.	Не получила широкого распространения	В разработке

Динамическая биометрическая аутентификация может проводиться с использованием следующих методов:

	Способ аутентификации	Достоинства	Недостатки	Оборудование
1	По голосу	Дешевый способ, возможно использовать как скрытый метод аутентификации.	Голос можно записать, голос человека меняется во время болезни, в зависимости от психического состояния и возраста. Данный метод не следует	Ar-morVox, IDVoice,

			использовать на объектах критической инфраструктуры.	
2	По биометрической (верификация подписи)	Электронный документ имеет такую же юридическую силу, как и бумажный. Максимально точную верификацию подписи дает использование специальных световых перьев.	В России доверяют бумажным документам или подписанным электронно-цифровой подписью. Метод также зависит от психофизического состояния человека.	SIGNificant Biometric Server
3	По клавиатурному почерку	Подходит для аутентификации удаленных пользователей, дешевый способ. Дает возможность наиболее полного сокрытия факта применения системы контроля, а также возможность реализации системы контроля только программными средствами; хорошая сочетаемость методов идентификации и аутентификации субъекта доступа по парольной фразе, введенной с клавиатуры.	Надежность зависит от длины вводимой фразы, ошибки возможны в случае с учетом возрастных факторов, а также состояния здоровья пользователя (моторика зависит от состояния человека).	TypingDNA
4	По походке	Идеально подходит для массового наблюдения за толпой, быстро позволяет идентифицировать человека, даже на большом расстоянии.	Не получила широкого распространения.	SFootBD, Watrrix
5	По движению губ	Биометрические датчики фиксируют активность мышц вокруг рта, создавая шаблон движения.	Не получила широкого распространения	Lip password

При осуществлении процесса биометрической аутентификации может возникнуть ряд проблем: ошибочный отказ или допуск (из-за неполного совпадения считанной характеристики с эталонной); использование внешнего записывающего устройства; угроза атак подделки считываемых данных и др.

Эффективность биометрической аутентификационной системы характеризуется двумя параметрами: коэффициентом ошибочных отказов (система не подтверждает личность пользователя) и коэффициентом ошибочных подтверждений (подтверждение личности незаконного пользователя). Ни один из вышеперечисленных методов (если использовать его изолированно), не дает абсолютно надёжной аутентификации пользователя. Наиболее надежна **мультимодальная биометрическая аутентификация** (например, единая биометрическая система от Ростелекома) – сочетание нескольких методов (можно считывать радужную оболочку одного глаза или двух, сочетать сканирование

радужной оболочки глаза и отпечатков). «Максимально надежными считают комбинации «радужная оболочка+палец» или «палец+рука». Хотя в последнее время популярность набирают системы типа «лицо+голос». Это связано с широким распространением коммуникационных средств, которые сочетают в себе модальности аудио и видео» [3, с. 1352]. В связи с пандемией стали очень востребованы методы бесконтактной аутентификации (например, в России наиболее популярна биометрическая аутентификация по лицу, в Европе продолжает лидировать дактилоскопия).

Кроме того, «для защиты компьютерных систем от несанкционированного доступа часто применяется комбинация из двух систем: биометрической и контактной на базе смарт-карт или USB-ключей» [1, с. 210]. В настоящее время активно используют нейросетевые модели в процессе биометрической аутентификации (например, при аутентификации пользователей по клавиатурному почерку, по отпечаткам пальцев и др.) [5], [6].

Применение биометрических параметров при идентификации субъектов доступа автоматизированных систем для обеспечения надежной защиты информации ограниченного распространения, составляющей государственную тайну, до настоящего времени не получило надлежащего нормативно-правового обеспечения, поэтому использование биометрических признаков личности системами разграничения доступа допускается только в автоматизированных системах, обрабатывающих и хранящих персональные данные, сведения, составляющие коммерческую или служебную тайну, и другие виды конфиденциальной информации.

В нашей стране началось активная разработка не только надежных методов биометрической аутентификации, но и правовых основ работы с биометрическими данными. Нормативной базой, регламентирующей процесс биометрической аутентификации личности, являются ФЗ № 152 от 27.07.2006 «О персональных данных», ФЗ № 572 от 29.12.2022 «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных». В данных документах к биометрическим персональным данным относят физиологические и биологические особенности человека, на основании которых можно установить личность субъекта персональных данных. Перечень конкретных биометрических персональных данных в ФЗ № 152 отсутствует, но Роскомнадзор в своих разъяснениях уточняет, что к подобным сведениям относятся «дактилоскопические данные, радужная оболочка глаз, анализы ДНК, рост, вес и другие данные, а также иные физиологические или биологические характеристики человека, в том числе изображение человека (фотография и видеозапись)» [4, с. 48]. Получать и обрабатывать такие данные оператор может только с письменного согласия субъекта персональных биометрических данных.

В 2018 году на портале «Госуслуги» начала действовать Единая система идентификации и аутентификации Российской Федерации (ЕСИА). С января 2022 года разработанная в России единая биометрическая система (ЕБС) приобрела статус государственной информационной системы, оператором которой является компания «Ростелеком» (все организации, собирающие биометрические данные, должны были до 20 сентября 2023 года передать их в ЕБС,

организации накопили свыше 75 млн. образцов, причем половину из них собрал Сбербанк).

Методы аутентификации личности постоянно совершенствуются, несомненным преимуществом использования биометрической аутентификации перед другими методами является непосредственная идентификация самого пользователя, а не представляющего его технического устройства или криптографической записи (пароля). Биометрическая аутентификация является одной из самых удобных, надежных и трудно фальсифицируемых. Однако, если злоумышленник похитит образцы биометрических данных пользователя, то изменить их (например, в отличие от пароля пользователя, нельзя), поэтому в настоящее время активно разрабатывается так называемая технология *отменяемой биометрии* - т.е. направленное и неоднократное искажение биометрического образца по специальному алгоритму при регистрации пользователя и его последующих идентификациях, что делает восстановление оригинала (в случае его похищения злоумышленниками) невозможным. Повысить уровень надежности биометрической аутентификации личности можно не только при помощи двух-трехфакторной аутентификации, не следует забывать, что биометрическая аутентификация – один из факторов MFA (многофакторная аутентификация), дающей гарантированно надежный результат.

Список литературы:

1. Беликова, Н. В. Аспекты биометрической аутентификации, используемой в современных информационных системах / Н. В. Беликова, А. В. Беликов // Инновации в современной науке : Материалы III Международного зимнего симпозиума, Таганрог, 26 февраля 2014 года / Научный редактор: Г.Ф. Гребенщиков. – Таганрог: ООО "Издательство "Спутник+", 2014. – С. 209-214.
2. Бронникова, Н. И. Правовые основы работы с биометрическими данными / Н. И. Бронникова // Современные тренды управления и цифровая экономика: от регионального развития к глобальному экономическому росту : сборник статей V Международной научно-практической конференции, Екатеринбург, 10 августа 2023 года / Институт цифровой экономики и права. – Екатеринбург: Общество с ограниченной ответственностью "Институт Цифровой Экономики и Права", 2023. – С. 250-255.
3. Ибрагимов, Р. И. Биометрические системы аутентификации / Р. И. Ибрагимов, С. В. Чичахова // Инновации. Наука. Образование. – 2021. – № 32. – С. 1339-1352.
4. Полуянова, Е. В. Нормативное регулирование использования биометрических персональных данных в Российской Федерации / Е. В. Полуянова, С. Д. Ковалев // Вестник Томского института повышения квалификации работников ФСИН России. – 2020. – № 3(5). – С. 45-51.
5. Сатыбалдиев, Н. Э. Применение нейросетевых технологий для биометрической идентификации в системах безопасности / Н. Э. Сатыбалдиев,

Ж. Ж. Ахметова // Вестник Казахской академии транспорта и коммуникаций им. М. Тынышпаева. – 2019. – № 2(109). – С. 163-168.

6. Силантьев, И. О. Нейросетевые модели биометрической идентификация и аутентификация пользователей по отпечаткам / И. О. Силантьев // Технические науки - от теории к практике. – 2014. – № 36. – С. 43-47.

7. Черняев, С. В. Биометрическая идентификация в современном российском законодательстве / С. В. Черняев // Труды Оренбургского института (филиала) Московской государственной юридической академии. – 2021. – № 4(50). – С. 55-58.