Рынок средств биометрической аутентификации: преимущества и особенности

Александр ЖАРИКОВ,
руководитель группы аналитиков, VisionLabs

С каждым годом повсеместное использование биометрических технологий только набирает обороты. Согласно прогнозам MarketsandMarkets [1], к 2024 г. объем мирового рынка таких систем вырастет до 65,3 млрд долл. Несмотря на то что государственные инициативы по-прежнему остаются ключевым драйвером роста, ожидается, что доля мирового рынка будет смещаться в сторону активного использования в коммерческих и потребительских сегментах. Давайте рассмотрим преимущества применения биометрических технологий и выделим наиболее перспективные.

Многообразие биометрических характеристик

Если говорить в общем, то биометрическая аутентификация – это определение личности человека по его уникальным физиологическим и поведенческим характеристикам. Всего на сегодняшний день насчитывается более 25 биометрических модальностей, которые могут быть применены в качестве средств аутентификации.

Физиологические биометрические характеристики человек получает при рождении, большинство из них неизменны в течение всей жизни. Собрать эти данные не составляет труда, а результаты идентификации с их использованием не зависят от психофизического состояния человека. Поведенческие биометрические характеристики основаны на индивидуальных особенностях движений, из-за чего сбор таких данных занимает какое-то время и должен повторяться на регулярной основе.

Однако более 80% существующих модальностей почти не применяются на практике. Ключевой фактор, препятствующий развитию и распространению, – незрелость технологий и, как следствие:

- высокая стоимость разработки и внедрения;
- низкая инвестиционная привлекательность;
- отсутствие экспертизы и справедливой оценки потенциальной емкости рынка;
- недостаточная точность и надежность модальностей;
- аппаратная зависимость;
- ограничения технологии и сценариев применения модальностей;
- возникновение рисков, не присущих иным средствам аутентификации;
- неготовность законодательства и внутренних регламентов безопасности организаций.

Биометрия повсеместно

Биометрия нашла применение практически в каждой сфере «умного» города. При омниканальной коммуникации распространение получили преимущественно физиологические модальности: отпечаток пальца, радужная оболочка глаза, рисунок вен, лицо и голос – их доля на рынке биометрических систем, по разным оценкам, составляет от 74 до 89%.

Один из главных трендов сейчас – аутентификация в дистанционных каналах, которая позволила реализовать принцип «финансового супермаркета» при продаже услуг и обеспечила их доступность и распространенность среди потребителей. Пандемия коронавирусной инфекции только усилила этот тренд. Так, по данным Федеральной налоговой службы (ФНС), на конец августа 2020 г. зарегистрировано более 1 млн самозанятых граждан,

применяющих налог на профессиональный доход, – из них более 50% были зарегистрированы с применением биометрии [3]. В сервис «Сбер ID», используемый для аутентификации и автозаполнения данных на сайтах партнеров (например, mos.ru), в III квартале 2020 г. к существующим (пара «логин-пароль», QR-код и пуш-уведомление) был добавлен еще один способ аутентификации – по биометрии, в качестве модальности используется лицо. В октябре текущего года Национальный банк Республики Казахстан (НБРК) запустил сервис удаленной биометрической идентификации – аналог российской Единой биометрической системы (ЕБС). В целом возможность дистанционного подтверждения финансово значимых операций приводит не только к повышению удовлетворенности и увеличению базы клиентов, но и к сокращению операционных издержек и доли мошеннических операций (фрода). В период массового перехода на дистанционный режим работы и учебы вырос спрос на интеграцию с существующими и создание новых специализированных решений для учета рабочего времени и контроля сотрудников при удаленной работе с использованием биометрии.

Также наблюдается устойчивый рост использования биометрических средств в устройствах самообслуживания, банкоматах, системах управления очередями и POS-оборудовании. В 2017 г. подтверждение платежей с помощью биометрии было запущено платежной системой Alipay (компания Alibaba) в Китае. В 2018 г. возможность применения отпечатков пальца и лица для подтверждения оплаты анонсировали Mastercard [4] и другие платежные системы. А уже начиная с 2019 г. подобные решения заработали повсеместно: например, в России в июле текущего года Visa совместно со «Сбербанком» запустила пилотный проект оплаты по лицу [5].

Кроме того, широкое распространение получило применение

Биометрические характеристики человека

биометрических технологий в системах контроля и управления доступом (СКУД). Интеграция позволяет снизить риски спуфинг-атак и компрометации данных, повысить пропускную способность, сократить время реагирования на инциденты и оптимизировать расходы на персонал. В период пандемии обнаружились и другие, ранее неочевидные выгоды. Например, использование некоторых из модальностей (лицо, радужная оболочка или сетчатка глаза) обеспечивает полностью бесконтактный способ взаимодействия с турникетами. А простая интеграция с тепловизионными камерами позволяет реализовать термоконтроль на объекте и снизить риск распространения инфекций.

Оценка биометрических систем

Для сравнения различных биометрических технологий по точности принято их оценивать по следующим показателям:

- ошибки первого рода – количество ложноотрицательных (False Negatives Rate – FNR или False Rejection Rate – FRR) исходов от общего количества запросов;
- ошибки второго рода – количество ложноположительных (False Positives Rate – FPR или False Acceptance Rate – FAR) исходов от общего количества запросов.

При биометрической аутентификации ошибочный пропуск «чужого» (FAR) существеннее и опаснее ошибочного отказа «своему» (FRR), так как это может привести не только к репутационным, но и к финансовым потерям. Помимо точности принято оценивать быстродействие, стоимость, безопасность, масштабируемость и удобство использования решения. В таблице 1 представлено сравнение технологий распознавания по перечисленным критериям.

Доминирующая технология

Благодаря адаптивности к различным точкам аутентификации и невысоким требованиям к условиям и аппаратному обеспечению распознавание лиц имеет темпы среднегодового прироста объема рынка более высокие по сравнению с остальными биометрическими технологиями, а на российском рынке доля лицевой биометрии

Таблица 1. Сравнение биометрических технологий и модальностей

Модальность / Критерий	Лицо (2D)	Голос	Отпечаток пальца	Радужная оболочка глаза	Рисунок вен
Точность	FRR=0.025 при FAR=0.001	FRR=0.03 при FAR=0.01	FRR=0.006 при FAR=0.00001	FRR=0.00016 при FAR=0.0000001	FRR=0.0001 при FAR=0.000008
Быстродействие	низкая скорость (<1 с.)	средняя скорость	низкая скорость (<1 с.)	средняя скорость (~2 с.)	средняя скорость
Стоимость **• Сенсор/сканер** **• ПО**	• низкая: от 1,5 тыс. руб. (web-камера без IR/Depth модуля); • приобретается отдельно, стоимость зависит от кол-ва шаблонов в базе.	• низкая: от 0,3 тыс. руб. (подойдет любой микрофон); • приобретается отдельно, стоимость зависит от кол-ва шаблонов в базе.	• средняя от 4,5 тыс. руб.; • поставляется вместе с сенсором (наиболее распространенная модель).	• высокая от 100 тыс. руб.; • поставляется вместе с сенсором (наиболее распространенная модель).	• высокая 50–100 тыс. руб.; • поставляется вместе с сенсором (наиболее распространенная модель).
Безопасность	• чувствительность к условиям окружающей среды и положению субъекта; • высокая зависимость от качества изображений, используемых в качестве эталонов; • снижение эффективности при изменении выражения лица; • невысокая уникальность признака (фальсификация возможна).	• чувствительность к условиям окружающей среды; • чувствительность к состоянию субъекта идентификации; • необходимость близкого расположения микрофона к субъекту идентификации; • невысокая уникальность признака (фальсификация возможна).	• высокие показатели надежности; • фальсификация возможна, зависит от типа сканнера.	• высокие показатели надежности; • фальсификация безуспешна.	• устойчивость к подделке или краже; • небольшой практический опыт применения; • высокая уникальность признака (фальсификация невозможна).
Масштабируемость	• отсутствие необходимости в специализированном оборудовании; • возможность удаленной идентификации; • возможность идентификации в потоке; • наилучшая адаптивность к точкам аутентификации (банкомат, СКУД, смартфон, Web-сайт, клиент-банк, Call Center и др.).	• отсутствие необходимости в специализированном оборудовании; • возможность удаленной идентификации; • зависимость от языка и/или языковой группы; • хорошая адаптивность к точкам аутентификации (банкомат, СКУД, смартфон, Web-сайт, клиент-банк, Call Center и др.).	• невысокая стоимость сканера; • широкое распространение; • хорошая адаптивность к точкам аутентификации (банкомат, СКУД, смартфон, Web-сайт, клиент-банк, Call Center и др.).	• невозможность идентификации в потоке; • ограниченность применения для удаленной идентификации.	• большой размер сканера; • невозможность идентификации в потоке; • ограниченность применения для удаленной идентификации; • зависимость от вендора.
Преимущества и недостатки технологии	'+' бесконтактная технология; '+' стабильность к изменениям психофизического состояния человека; '–' чувствительность к изменениям условий съёмки.	'+' бесконтактная технология; '–' чувствительность к изменениям психофизического состояния человека.	'+' простота использования; '–' чувствительность к изменениям окружающей среды и состоянию кожи.	'–' риск повреждения радужной оболочки глаза.	'+' стабильность к изменениям окружающей среды и состоянию кожи.

уже составляет около 50% всего объема рынка.

Задача биометрической аутентификации по лицу является комплексной и включает целый набор различных подзадач:

- обнаружение (детекция) лиц на изображении;
- обнаружение ключевых точек лица и определение положения (углов наклона и поворота) головы;
- компенсация поворота плоскости изображения и центрирование изображения на основе положения глаз;
- опциональная оценка атрибутов (пол, возраст, направление взгляда, этническая принадлежность или раса, эмоции и пр.) обнаруженного лица;
- оценка качества изображения лица по параметрам (размытость, неравномерная освещенность, наличие бликов и др.);
- опционально выбор лучшего кадра для распознавания из нескольких;
- проверка на живое лицо;
- извлечение биометрического шаблона из изображения лица;
- сравнение биометрических шаблонов и определение результата по пороговым значениям.

Для решения большинства из подзадач используются сверточные нейронные сети, причем для каждой – отдельный алгоритм или даже набор алгоритмов. Биометрический шаблон (дескриптор), извлекаемый из изображения, уникален, а сама операция необратима. Получить исходное изображение из биометрического шаблона невозможно, что обеспечивает защищенность системы.

Для оценки эффективности биометрической системы помимо точности необходимо обращать внимание на размер биометрических шаблонов, скорость их извлечения и сопоставления с другими шаблонами. Эти показатели напрямую не влияют на качество распознавания, однако не менее важны для работы под нагрузкой, с большим объемом данных – полномасштабные сервисы распознавания лиц должны работать надежно при выполнении тысяч одновременных запросов на аутентификацию и осуществлении поиска в базе данных на миллионы лиц.

Таблица 2. Лучшие результаты в разных категориях тестов NIST			
Скорость извлечения биометрического шаблона			
10 мс, размер биометрического шаблона: 1036 Кб			Ayonix (ayonix-0), Япония
Скорость поиска биометрического шаблона по базе ⩽6 млн шаблонов			
менее 1 мс			FarBar Inc (f8-001), Тайвань
Точность верификации без маски			
Тип изображения	**FAR**	**FRR**	**Разработчик (алгоритм), страна**
Visa	⩽0.000001	0.0025	VisionLabs (visionlabs-009), Россия
Mugshot	⩽0.00001	0.0026	VisionLabs (visionlabs-009), Россия
Mugshot DT⩾12yrs	⩽0.00001	0.0027	SenseTime (sensetime-003), Китай
VisaBorder	⩽0.000001	0.0035	VisionLabs (visionlabs-009), Россия
Border	⩽0.000001	0.0064	VisionLabs (visionlabs-009), Россия
Wild	⩽0.00001	0.0293	ercacat-001
Child Exp	⩽0.01	0.2467	Paravision (paravision-004), США
Точность верификации в маске			
VisaBorder	⩽0.00001	0.0237	DeepGlint (deepglint-002), Китай
Точность идентификации по базе 1.6 млн. биометрических шаблонов			
Mugshot	⩽0.003	0.0015	SenseTime (sensetime_004), Китай
Webcam	⩽0.003	0.0105	SenseTime (sensetime_003), Китай
Profile	⩽0.003	0.0850	SenseTime (sensetime_004), Китай
Visa Border	⩽0.003	0.0047	SenseTime (sensetime_004), Китай
«Точность идентификации по базе 3 млн биометрических шаблонов лиц с разницей в возрасте более 12 лет»			
Mugshot DT⩾12yrs	⩽0.003	0.0112	SenseTime (sensetime_003), Китай

Отраслевым исследованием в настоящий момент является тестирование NIST Face Recognition Vendor Test Ongoing, проводимое ежегодно Национальным институтом стандартов и технологий на больших закрытых наборах данных. В табл. 2 представлены лучшие результаты тестов NIST [7–9] – точность верификации и скорость алгоритмов покрывает сформировавшиеся потребности. Однако использовать биометрию в качестве единственного фактора подтверждения подлинности личности не рекомендуется.

Перспективы развития

Глобально на рынке биометрии сохраняется несколько устойчивых трендов: проникновение биометрических сенсоров на рынок смартфонов, вытеснение карточных систем на рынке СКУД и постоянное расширение рынка Интернета вещей. В последнем направлении с развитием 5G ожидается взрывной рост, который затронет и рынок биометрических технологий, применяемых в таких устройствах. Например, «умные» устройства для дома и автомобиля уже сейчас используют распознавание жестов, аутентификацию по лицу или голосу, а замки – по отпечатку пальца. В целом среди принципов применения средств биометрической аутентификации можно наблюдать переход к мультивендорным, многофакторным, мультимодальным решениям.

Пандемия коронавирусной инфекции дала дополнительный толчок распространению биометрических технологий и развитию инициатив в сфере биометрии, а также возможности оцифровать и оценить эффект от внедрения биометрических технологий. Существующие нормативно-правовые акты позволяют использовать биометрию в сферах госуслуг, финансов, образования и др.

Однако в период изоляции также обнаружилось, что регуляторные ограничения и обособленность массивов биометрических шаблонов, накопленных разными организациями, не позволяют выполнять значимые операции. Поэтому для развития рынка средств биометрической аутентификации в России уже в ближайшее время будут внесены изменения в федеральные законы «Об электронной подписи» № 63 от 06.04.2011, «О персональных данных» № 152 от 27.07.2006, а также в национальные стандарты, разработанные в рамках подкомитета Росстандарта ТК-098 «Биометрия и биомониторинг», в соответствии с «Программой национальной стандартизации на 2020 г.». ■

Ссылки

1. *https://www.marketsandmarkets.com/Market-Reports/next-generation-biometric-technologies-market-697.html*
2. *https://ict.moscow/presentation/kiberbezopasnost-proryvnykh-tekhnologii/*
3. *https://news.rambler.ru/other/44976090-bolee-polumilliona-chelovek-poluchili-status-samozanyatyy-po-biometrii-litsa-c-pomoschyu-platformy-visionlabs/*
4. *https://newsroom.mastercard.com/ru/press-releases/mastercard-определяет-будущее-подтверждение/*
5. *https://www.sberbank.ru/ru/person/promo/bio_visa*
6. *https://www.kommersant.ru/doc/4407532*
7. *https://pages.nist.gov/frvt/html/frvt11.html*
8. *https://pages.nist.gov/frvt/html/frvt1N.html*
9. *https://pages.nist.gov/frvt/html/frvt_facemask.html*