Биометрические технологии - это новый этап в развитии систем безопасности, которые используются во всем мире. Эти технологии позволяют идентифицировать человека по его уникальным физическим и поведенческим характеристикам, таким как отпечатки пальцев, голос, лицо, сетчатка глаза, а также распознавание походки или письма. Использование биометрических технологий позволяет создавать более безопасные и удобные способы аутентификации личности.

Биометрическая идентификация решает сегодня целый ряд конкретных отраслевых задач как в области безопасности, так и в сфере маркетинга. Применение биометрии повышает уровень безопасности и дает возможность перестроить процессы взаимодействия с клиентами. Например, можно автоматически выделять категории посетителей, требующих особого внимания, выявлять нежелательных посетителей или «нарушителей» и оповещать персонал или охрану. Это помогает, с одной стороны, обеспечить дополнительную безопасность и снизить риски, а с другой - повысить уровень обслуживания клиентов. Не меньшее значение такая идентификация имеет и для маркетингового анализа. Алгоритм может оценивать пол и возраст посетителей, фиксировать повторные визиты, выделять целевые аудитории, оценивать эффективность рекламных кампаний, показатели лояльности и т. п. [3] На сегодняшний день, выделяют два типа систем биометрических данных: статические биометрические данные, то есть уникальные признаки, полученные человеком от рождения (ДНК, отпечатки пальцев, геометрия руки, радужная оболочка глаза и иное), и динамические биометрические данные – характеристики, приобретенные со временем или способные меняться с возрастом или под внешним воздействием (динамика воспроизведения подписи, походка, динамика набора текста, голос и иное). На мировом рынке биометрических систем активно применяются технологии, основанные на распознавании и использовании следующих биометрических данных.

В соответствии с международной классификацией можно выделить следующие ключевые сегменты рынка биометрических технологий по отраслям применения: -государственный сектор: электронные документы, содержащие биометрические данные (e-passports, e-ID, электронные водительские удостоверения), национальные биометрические программы, а также системы национальной безопасности (за исключением систем, которые используются на транспорте и в иммиграционном контроле); -путешествия и миграция: e-Visas, e-Gates, ABC-Kiosks и т.п. (все биометрические системы, используемые на объектах транспортной инфраструктуры и в иммиграционном контроле); -финансовый сектор: финансы, банки, платежные системы и страхование; -здравоохранение: как государственный, так и частный сектора; -ритейл: системы мониторинга покупателей; -корпоративное использование: информационная безопасность (виртуальный контроль доступа), физический контроль доступа, учет рабочего времени в крупных организациях и т.д. Таким образом, крупнейшими сегментами мирового рынка биометрических систем является государственный сектор, включая сферу миграции, а также сегмент путешествий. Третьим крупным рынком для биометрических систем является финансовый сектор, доля которого оценивается на уровне 15,0%. Доля сегмента здравоохранения составляет 9,0%. Доля Retail оценивается на уровне 5,0%.

FAR (False Acceptance Rate) и FRR(False Rejection Rate). Первое число характеризует вероятность ложного совпадения биометрических характеристик двух людей. Второе – вероятность отказа доступа человеку, имеющего допуск. Система тем лучше, чем меньше значение FRR при одинаковых значениях FAR. Иногда используется и сравнительная характеристика EER, определяющая точку в которой графики FRR и FAR пересекаются. Но она далеко не всегда репрезентативна. Подробнее можно посмотреть, например, [тут](http://support.bioid.com/sdk/docs/About_EER.htm).  
Можно отметить следующее: если в характеристиках системы не даны FAR и FRR по открытым биометрическим базам — то что бы производители не заявляли о её характеристиках, эта система скорее всего недееспособна или сильно слабее конкурентов.  
Но не только FAR и FRR определяют качество биометрической системы. Если бы это было только так, то лидирующей технологией было бы распознавание людей по ДНК, для которой FAR и FRR стремятся к нулю. Но ведь очевидно, что эта технология не применима на сегодняшнем этапе развития человечества! «Устойчивость к подделке» – это эмпирическая характеристика, обобщающая то, насколько легко обмануть биометрический идентификатор. «Устойчивость к окружающей среде» – характеристика, эмпирически оценивающая устойчивость работы системы при различных внешних условиях, таких как изменение освещения или температуры помещения. «Простота использования» показывает насколько сложно воспользоваться биометрическим сканером, возможна ли идентификация «на ходу». Важной характеристикой является «Скорость работы», и «Стоимость системы». Не стоит забывать и то, что биометрическая характеристика человека может изменяться со временем, так что если она неустойчива– это существенный минус.  
Обилие биометрических методов поражает. Основными методами, использующими статические биометрические характеристики человека, являются идентификация по папиллярному рисунку на пальцах, радужной оболочке, геометрии лица, сетчатке глаза, рисунку вен руки, геометрии рук. Также существует семейство методов, использующих динамические характеристики: идентификация по голосу, динамике рукописного подчерка, сердечному ритму, походке. Ниже представлено распределение биометрического рынка пару лет назад. В каждом втором источнике эти данные колеблются на 15-20 процентов, так что это всего лишь оценочное представление.

Применение биометрических технологий повлечет за собой цифровизацию других секторов экономики. В медицине биометрические технологии используются для того, чтобы осуществлять мониторинг, идентификацию пациентов, а также они нашли свое применение в национальных программах идентификации носителей ВИЧ по отпечаткам пальцев, которая, например, действует в Африке. По прогнозам объем осуществляющихся транзакций с мобильных устройств при помощи биометрии к 2023 году может превысить $2 трлн. Наиболее быстро будет возрастать количество удаленных транзакций (более 48 миллиардов к 2023 году, или 57% от общего числа). В офисах биометрия начинает вытеснять PIN-коды, магнитные карты и пароли, идентифицирующие сотрудников, биометрические технологии осуществляют контроль за дисциплиной работников. Показателен пример парламента Аргентины, где при помощи биометрии было зафиксированы факты прогулов работы сотрудниками компаний. В фитнес клубах также активно применяется идентификация клиентов по изображению лица. Tractica делает прогноз, что рынок биометрических технологий будет демонстрировать уверенный рост до 2025 г. на 22,9% каждый год и составит более 15 млрд долларов. Исследователи компании Frost & Sullivan прогнозируют, что к тому моменту времени каждый третий новый автомобиль будет оснащен биометрией, что повысит уровень безопасности на трансопрте. Использование цифровых технологий позволяет исключить посредников между исполнителем и его клиентами, что положительно влияет на время исполнения операций и производительность [11]. Цифровые устройства также будут использовать биометрические решения. Голосовое управление освещением и температурой уже активно применяется в «умных» домах. Потребительская электроника (например, смартфоны или планшеты) оснащаются сканерами отпечатков пальцев. Получат распространение такие надежные идентификаторы личности, как 3D-модель лица, радужная оболочка глаза и рисунок вен