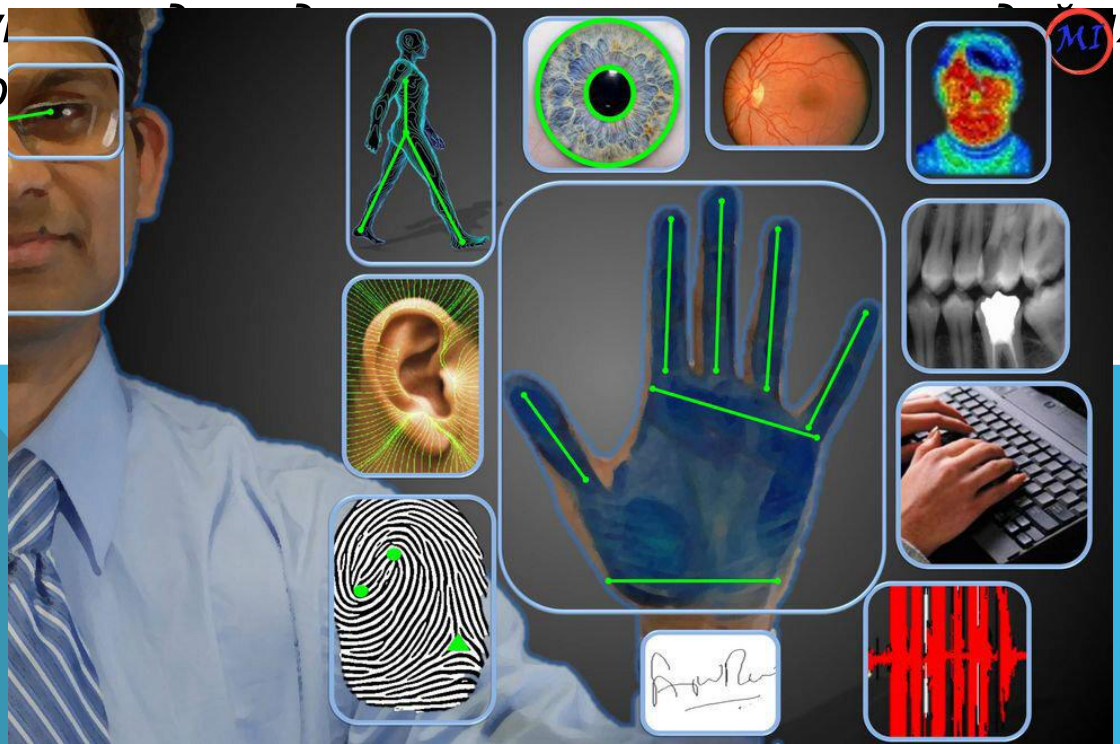
УСТРОЙСТВА ДЛЯ ОПОЗНАВАНИЯ И ИДЕНТИФИКАЦИИ ЛИЧНОСТИ.

БИОМЕТРИЧЕСКАЯ ИДЕНТИФИКАЦИЯ

Биометрическая аутентификация — процесс доказательства и проверки подлинности через предъявление пользователем своего биометрического образа и путем преобразования этого образа в соответствии с заранее определенным протоколом аутентификации. Биометрические системы аутентификации — системы аутентификации, использу… …х биометр…



БИОМЕТРИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Сравнительная характеристика биометрических систем	Отпечаток пальца 	Голос 	Радужная оболочка 	Лицо 
Надежность верификации	96,7-98%	99,14%-99,9%	95,4%-95,9%	95,9%
Ошибка регистрации	4%	2%	7%	0,1%
Вероятность «допуска чужого»	2,5%	0,75%	6%	4%
Вероятность «отказа своему»	0,1%	0,75%	0,001%	10%
Стоимость системы	Высокая	Низкая	Очень высокая	Высокая

(из материалов доклада Dan Miller, Senior Analist, Opus Reserch на конференции VoiceBioCon 2007)

биометрия

научная дисциплина, изучающая способы измерения различных биологических параметров человека для

верификации

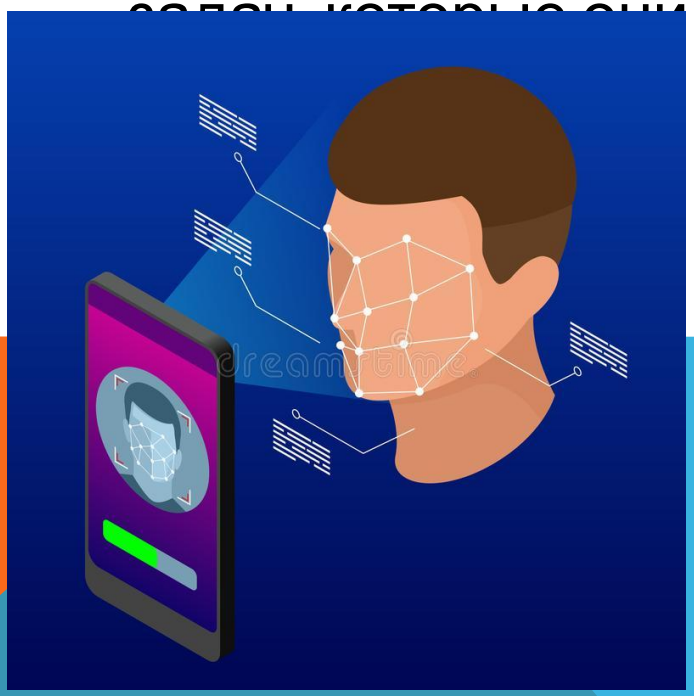
установления сходства или различия между людьми

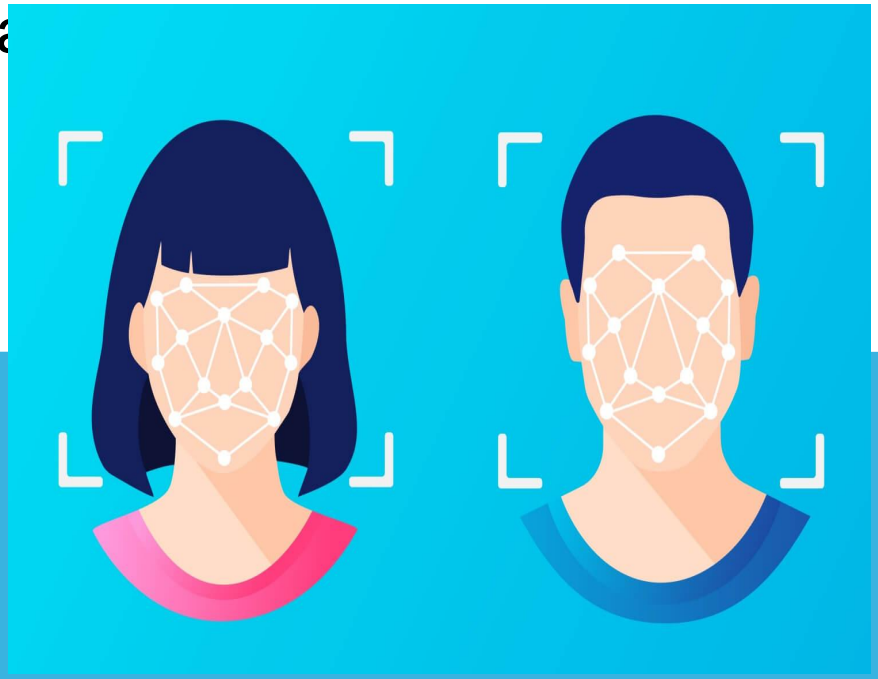
идентификации

выделения одного конкретного человека из множества других людей

ЛИЦО (FACIAL RECOGNITION, СЕЛФИ)

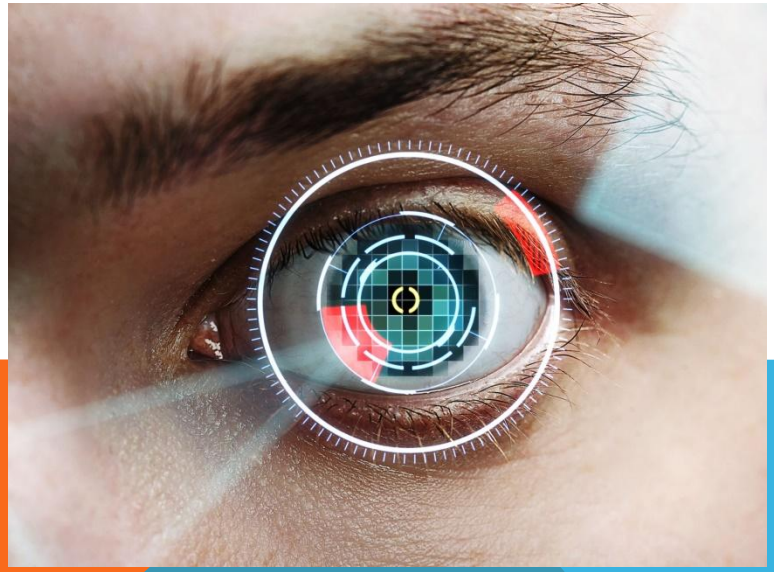
Распознавание лиц - это автоматическая локализация человеческого лица на изображении или видео и, при необходимости, идентификация личности человека на основе имеющихся баз данных. Интерес к этим системам очень велик в связи с широким кругом





ИДЕНТИФИКАЦИЯ ПО РАДУЖНОЙ ОБОЛОЧКЕ ГЛАЗА

Биометрия по радужной оболочке глаз – быстрый, бесконтактный, безопасный и исключительно точный способ идентификации, обеспечивающий решение широкого круга задач заказчиков различных отраслей.



ОТПЕЧАТКИ ПАЛЬЦЕВ

Отпечатки пальцев представляют собой рельефные линии, так называемые папиллярные узоры, строение которых обусловлено рядами гребешковых выступов кожи, разделенных бороздками. Эти линии образуют сложные кожные узоры (дуговые, петлевые, завитковые), которые обладают следующими свойствами:

- индивидуальность (различная совокупность папиллярных линий, образующих рисунок узора по их местоположению, конфигурации, взаиморасположению, неповторимая в другом узоре);
- относительная устойчивость (неизменность внешнего строения узора, возникающего в период внутриутробного развития человека и сохраняющегося в течение всей его жизни);
- восстанавливаемость (при поверхностном нарушении кожного покрова папиллярные линии восстанавливаются в прежнем виде).

Существует несколько алгоритмов распознавания отпечатков пальцев. Наиболее распространенным является алгоритм, основанный на выделении деталей. Обычно в отпечатке присутствует от 30 до 40 мелких деталей. Каждая из них характеризуется своим положением — координатами, типом (разветвление, окончание или дельта) и

ДЕТАЛИ ПАПИЛЛЯРНОГО УЗОРА ВТОРОГО УРОВНЯ

1 — фрагмент папиллярной линии;

2 — начало папиллярной линии;

3 — глазок;

4 — разветвление папиллярной линии;

5 — крючок;

6 — мостик;

7 — островок;

8 — папиллярная точка;

9 — окончание папиллярной линии;

10 — слияние папиллярной линии;

11 — тонкие межпапиллярные линии

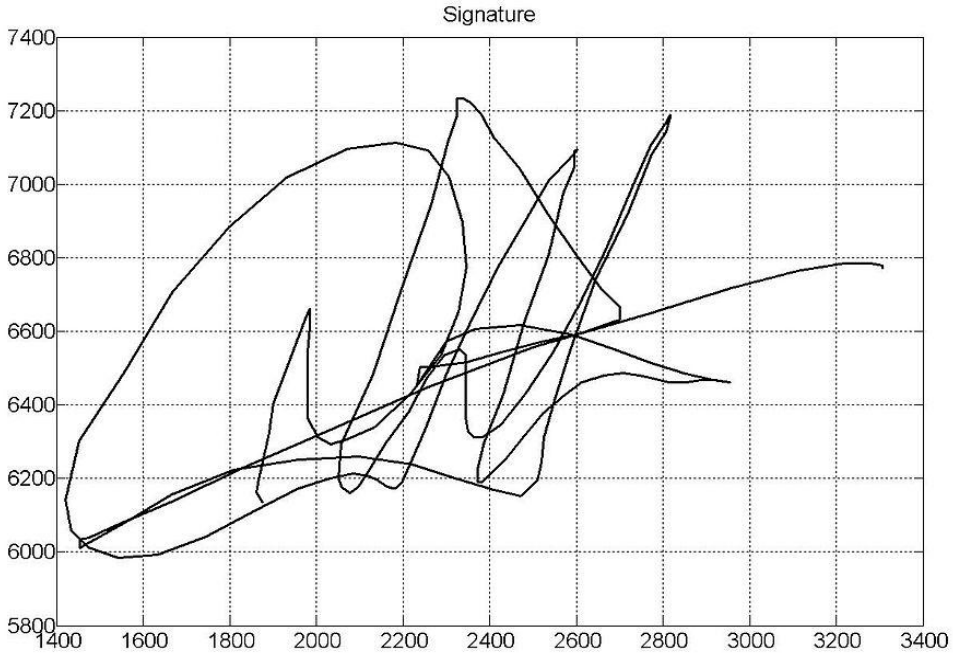
ГОЛОСОВАЯ БИОМЕТРИЯ

Голосовая биометрия — одна из технологий, которая развивается очень быстро и позволяет разным компаниям использовать ее решения для идентификации заказчиков. В биометрической системе для определения или подтверждения личности используют индивидуальные поведенческие, психологические и некоторые другие характеристики. Имеется множество биометрических измерений, включая сканирование радужной оболочки глаза, отпечатков пальцев, распознавание лица, голоса, подписи и т. д. Голосовая биометрия позволяет, исследуя голосовые характеристики человека, идентифицировать клиента. Она представляет собой относительно простой и экономичный способ

ВЕРИФИКА́ЦИЯ ПО́ДПИСИ

Верифика́ция по́дписи — биометрическая технология, использующая подпись для идентификации личности.

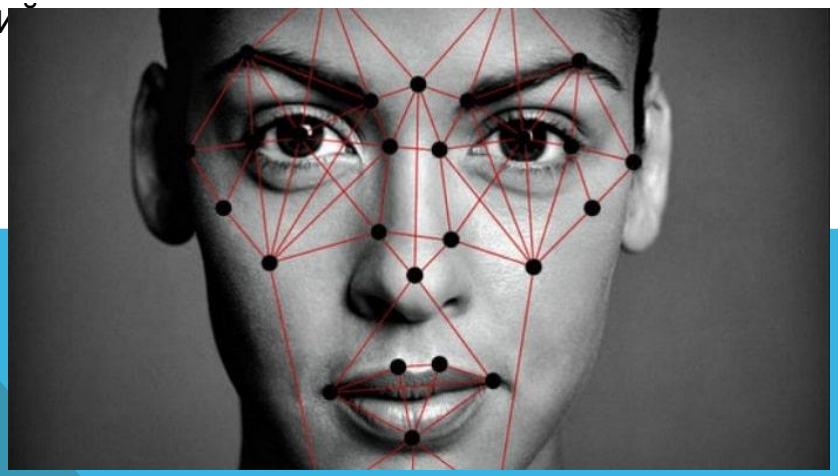
Верификация подписи может быть применима в областях, требующих автоматизацию документооборота, например, банковское или судебное дело. Алгоритмы распознавания подписи опираются на алгоритмы распознавания образов или математические методы анализа кривых, так как подпись может быть представлена набором точек. Поэтому в задаче верификации часто используется разложение в ряды или аппроксимация кривыми.



2D – РАСПОЗНАВАНИЕ ЛИЦ

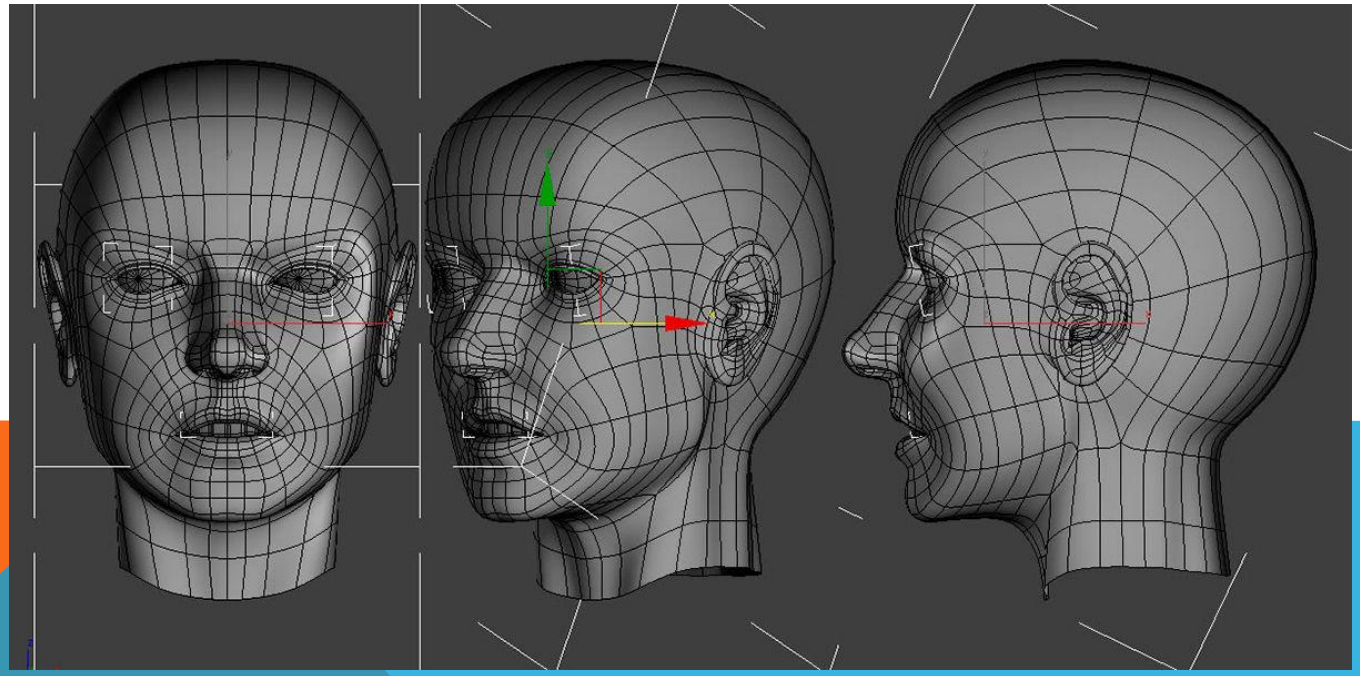
Сегодня наибольшее распространение получило программное обеспечение, основанное на двумерном анализе изображения. Большинство выпускаемой продукции в мире поддерживают именно 2D технологию. При определенном программном обеспечении 2D изображения преобразуются в 3D, и обрабатываются уже методами, предусмотренными для трехмерных изображений. Но все по порядку.

Распространению 2D распознавания способствует наличие в мире огромных баз уже наработанных и поддерживающих определенную структуру, которая хорошо задокументирована и практически готова к применению. Так же базы постоянно обновляются и совершенствуются алгоритмы выборки из них. Существуют общедоступные и коммерческие реализации баз изображений.



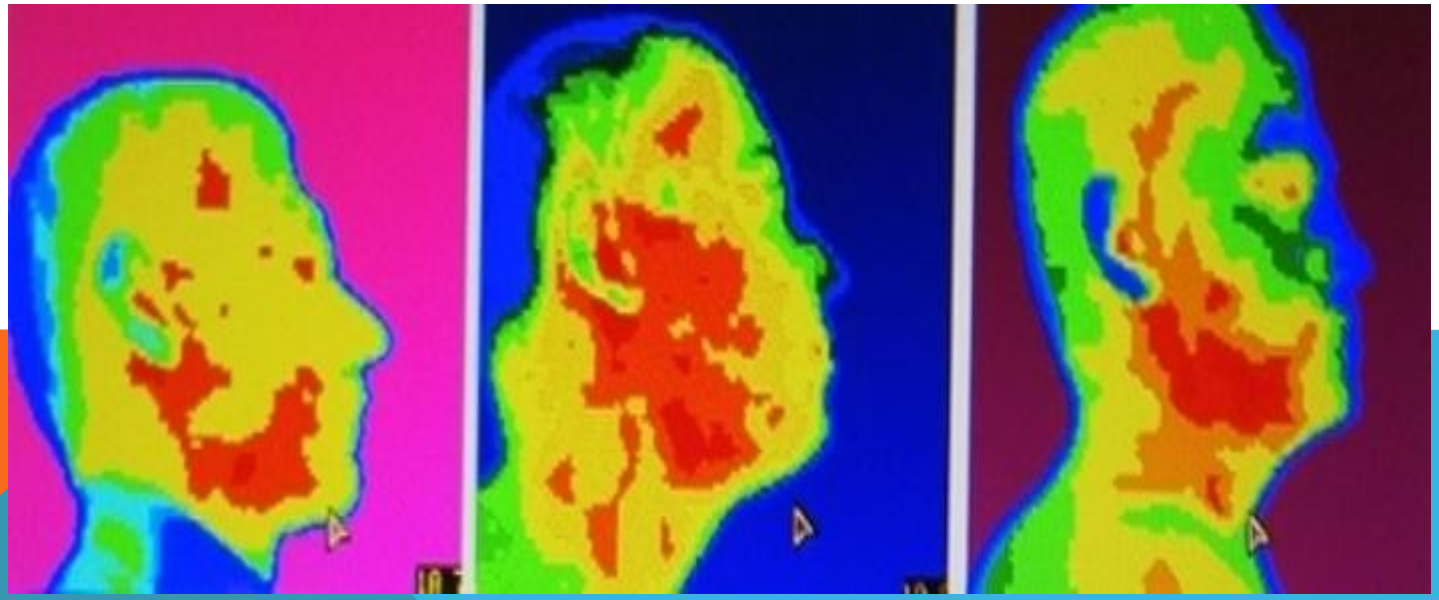
3D – РАСПОЗНАВАНИЕ ЛИЦ

Такое распознавание содержит более низкий процент ошибок, но реализация его многократно сложнее. 3D – маски для анализа получить довольно сложно. Для успешного сканирования лица необходимо оборудование с точками наблюдения из разных ракурсов и позиций. То есть за высоким процентом точности распознавания в 3D кроется дороговизна оборудования. Так как говорилось выше проще всего 2D – изображения преобразовывать в 3D с помощью соответствующего программного обеспечения.



РАСПОЗНАВАНИЕ ЛИЦ ПО ТЕПЛОВОМУ ИЗЛУЧЕНИЮ

Довольно перспективная технология, но сейчас есть только опытные образцы реализации. Если коротко, то определенные участки оголенного тела (лицо) довольно четко отдают тепло внешней среде, связано это с расположением кровеносных сосудов к поверхности кожи. И разные участки с разным тепловым излучением легко сопоставить друг другу, это будет являться качеством идентификации. При таком анализе достаточно не эффективно скрытие методами изменения внешности (изменение прически, накладные элементы, макияж, очки и аксессуары). Но как говорилась, технология в промышленных масштабах еще не реализована.



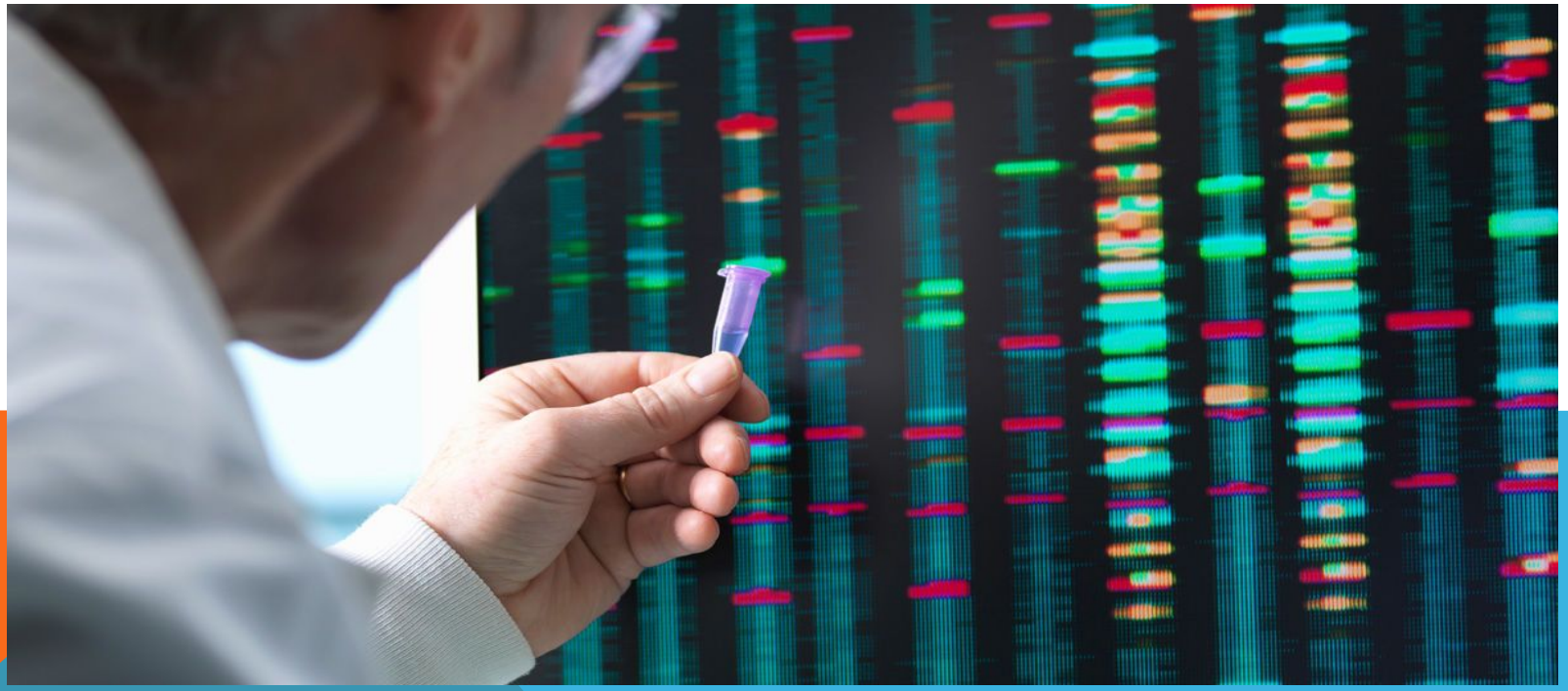
АУТЕНТИФИКАЦИЯ ПО СЕРДЕЧНОМУ РИТМУ И ГЕОМЕТРИИ СЕРДЦА

Биометрия сердечного ритма — перспективный и довольно новый метод, использующий уникальность работы сердца каждого из нас. Для него важны следующие параметры: частота, ритмичность, наполнение, напряжение, амплитуда колебаний и скорость пульса. А для снятия показаний достаточно специального браслета.

Анализ геометрии сердца — новая технология, появившаяся в 2017 году. Сейчас находится в стадии разработки. Для нее используется низкоуровневый допплеровский радар, сканирующий сердце каждые 8 секунд и определяющий форму, размер и ритм его сокращений. Уже сейчас в гаджетах доступны датчик пульса и функция ЭКГ. Возможно, в будущем они усовершенствуются до новой технологии, доступной в компактных устройствах.

АУТЕНТИФИКАЦИЯ ПО ДНК

Анализ ДНК — метод дорогой и сложный, но очень перспективный. Широко используется в медицине и криминалистике, позволяя находить преступников по следам, оставленным на месте преступления. Метод также позволяет установить родственников по неидентифицированному образцу ДНК. В гаджетах пока не используется из-за сложностей со сбором материала и его анализом, однако в будущем, вполне возможно, станет одним из важнейших методов идентификации пользователя.

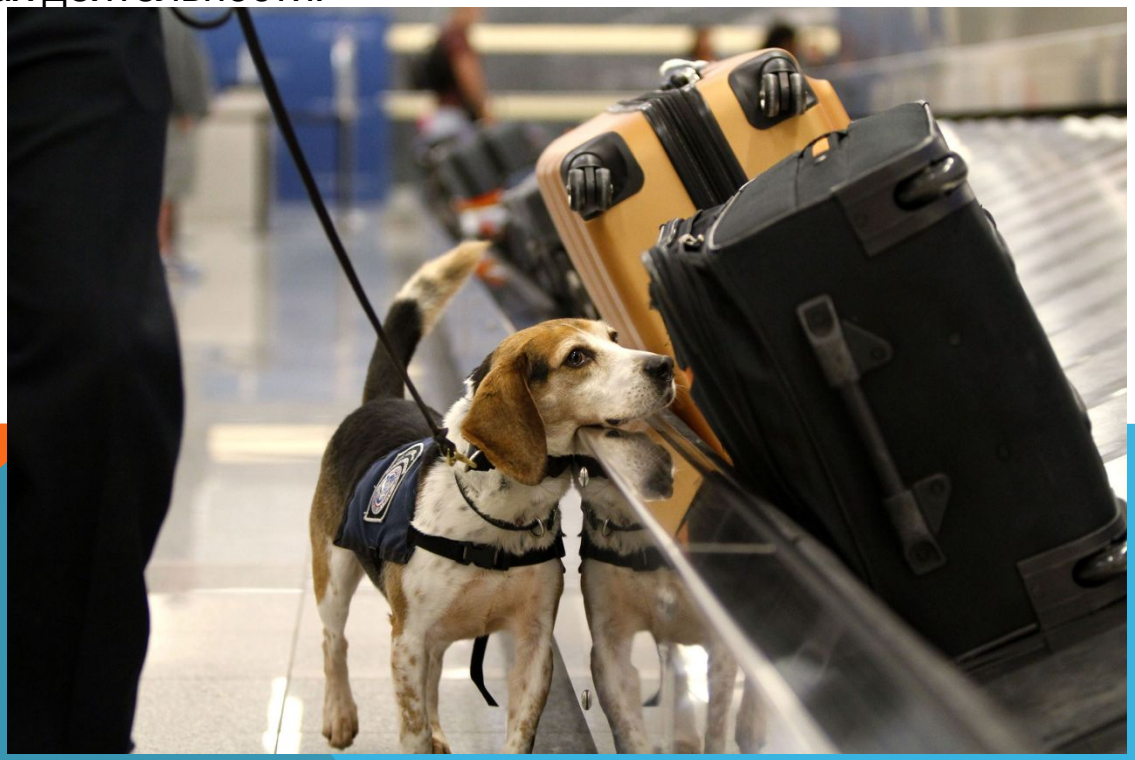


АУТЕНТИФИКАЦИЯ ПО ХИМИЧЕСКОМУ СОСТАВУ ПОТА

Новейший метод биометрии, находящийся в разработке с 2017 года. Он использует уникальный химический состав пота у каждого человека. Если метод найдет применение на практике, то для разблокировки, например, смартфона, надо будет лишь коснуться датчика, анализирующего состав аминокислот пота на коже.

АУТЕНТИФИКАЦИЯ ПО ЗАПАХУ

Еще один перспективный метод биометрии, который также пока находится на стадии разработки. Он использует уникальность запаха каждого человека. Анализ может производиться бесконтактно, а при необходимости — и незаметно от человека. Собак с их чувствительным обонянием используют для поиска людей очень давно. Если ученым удастся создать электронный «собачий нос», то, помимо идентификации людей или поиска взрывчатых или наркотических веществ, его смогут применить и в других сферах деятельности.



АРГУМЕНТЫ СТОРОННИКОВ И ПРОТИВНИКОВ БИОМЕТРИИ

Биометрия стала широко применяться совсем недавно, но уже вызывает в обществе бурные дискуссии. Ее противники упоминают «большого брата» и пугают миром, где будет невозможно спрятаться от всевидящего ока. Но такие аргументы от людей, пользующихся смартфонами на ОС Android, сервисами Google, соцсетями и ПК с Windows 10, выглядят уже не слишком серьезно.

Дальше всех пошло китайское приложение WeChat, которое аккумулировало практически всю возможную информацию о пользователе в одной базе. Несмотря на то, что оно открыто собирает огромное количество данных, приложением добровольно пользуются миллионы людей: через него заказывают товары, оплачивают коммунальные услуги, транспорт, записываются к врачу, оформляют документы, берут кредиты, подписываются на блогеров, организации и новости, общаются с друзьями. В результате WeChat знает, во сколько просыпается каждый пользователь, с кем он чаще всего общается и куда ходит, на каких остановках транспорта бывает ежедневно, сколько готов потратить на ту или иную статью расхода, какие у него любимые бренды и многое другое.

Понятно, что доступ к такой информации следует надежно защищать. Общество уже выбрало биометрическую аутентификацию как средство, которое заменит нам привычные, но не слишком надежные средства, такие как логин и пароль, на уникальный ключ, который невозможно забыть или потерять.

В обществе, где будут работать надежные средства биометрии, жить очень комфортно. Двери подъезда и ква а. Машина заведет двигатель, толь окупка в магазине пройдут, только ты.

БЛАГОДАРЮ ЗА ВНИМАНИЕ