### ****Биометрические автоматизированные информационные системы****

### ****Вступление****

Первый вариант данной статьи появился еще в 2005 году. За прошедшие 3 года в мире **биометрических технологий** произошли существенные изменения, связанные с тем, что началось широкомасштабное внедрение **биометрических систем**. Теперь мы сталкиваемся с **биометрией** самым непосредственным образом – например, при получении заграничного паспорта.

Изменилась и ситуация со стандартизацией, которая была одной из основных проблем несколько лет назад: усилиями отечественных специалистов подготовлены основные стандарты в области **биометрии**, часть из них уже действует, хотя работа пока и не до конца завершена. Российские специалисты участвуют и в процессе международной стандартизации.

С другой стороны, существенно развились сами **биометрические технологии**, причем мы можем констатировать, что отставание России в технологическом плане также остается в прошлом. Отечественные компании в настоящий момент предлагают конкурентоспособные на мировом уровне решения.

### ****Предыстория биометрии****

**Биометрические методы** распознавания применяются человечеством на протяжении всей его истории. Действительно, чаще всего мы узнаем знакомых людей именно с их помощью – по лицу, голосу или походке.

Начиная с XIX века, **биометрические технологии**, в первую очередь дактилоскопические, применяются в криминалистике, а с конца прошлого века, в связи с развитием техники, возникла возможность формализовать алгоритмы распознавания человека по его внешнему виду или особенностям поведения и применять для этого автоматизированные системы.

**Биометрические технологии** в настоящее время переживают период бурного развития. Во многом этот рост связан с решениями правительств ведущих государств об их применении в паспортно-визовых документах, что направило в эту область крупные финансовые и материальные ресурсы. Наличествует и огромный интерес общества к данным технологиям.

Слово «**биометрия**» часто встречается нам в различных новостях на телевидении, в газетах и на радио. К сожалению, использующие это понятие люди не всегда точно представляют, о чем говорят. В данной статье сделана попытка разъяснить азы **биометрических технологий**, рассказать о том, как они работают, где могут и где не могут применяться.

### ****Определения****

Сначала несколько определений:

Под **биометрикой** понимают область науки, изучающую методы измерения физических характеристик и поведенческих черт человека для последующей **идентификации** и аутентификации личности.

**Биометрической характеристикой человека** (БХЧ) называется его измеренная физическая характеристика или персональная поведенческая черта, в процессе сравнения которой с аналогичной ранее зарегистрированной **биометрической характеристики человека** реализуется процедура **идентификации**. Основными источниками **биометрической характеристики человека** являются отпечатки пальцев, радужная оболочка и сетчатка глаз, голос, лицо, манера работы на клавиатуре компьютера, подпись, походка и др.

Методы и технические средства **идентификации** и аутентификации личности на основе **биометрической характеристики человека** получили название **биометрических технологий** (БТ).

### ****Виды биометрических технологий****

Для **биометрической идентификации** можно применять различные характеристики и черты человека (рис. 1). Укрупнено **биометрические характеристики человека** подразделяют на статические, связанные с его физическими характеристиками, например, отпечатком пальца или формой уха, и динамические (или поведенческие), связанные с особенностями выполнения человеком каких-либо действий, например, походка.

Наиболее развитыми на данный момент технологиями являются распознавание по отпечатку пальца, радужной оболочке глаза и двумерному (плоскому, как на фотографии) изображению лица. Причем дактилоскопическая **идентификация** в настоящий момент по применимости и доступности с финансовой точки зрения превосходит все другие технологии в несколько раз.

### ****Как работают биометрические технологии****

**Биометрия** решает вопросы **верификации** и **идентификации**. В первом случае задача состоит в том, чтобы убедиться, что полученная биометрическая характеристика соответствует ранее взятой. **Верификация** (или сравнение 1 к 1) используется для проверки того, что субъект является именно тем, за кого себя выдает. Решение принимается на основании степени похожести характеристик.

**Идентификация** (или сравнение 1 к N) решает вопрос поиска для получаемой биометрической характеристики наиболее подходящей из ранее взятых. В простейшем случае это последовательное осуществление сравнений полученной характеристики со всеми имеющимися. При этом в качестве результата будет выбрана наиболее похожая ранее взятая характеристика (**идентификация** выполнена) или не будет вообще никакого результата, если степень похожести оказалась меньше заданной для всех сравнений.

Рассмотрим, как работают **биометрические технологии** на примере распознавания по отпечатку пальца. Для распознавания необходимо получить (с помощью специальных ридеров) изображение папиллярного узора одного или нескольких пальцев. Далее это изображение обрабатывается, и в процессе обработки находятся его характерные особенности, такие как разветвление линий, окончание линии или пересечение линий. Для каждой особенности, помимо ее типа, запоминаются относительное расположение и другие параметры, например, для точки окончания – направление линии. Совокупность данных особенностей и их характеристик образует шаблон **биометрической** характеристики.

При **идентификации** или **верификации** используется сравнение получаемого шаблона с ранее полученными. При определенном уровне соответствия делается вывод об идентичности шаблонов и, соответственно, происходит **верификация** или **идентификация** представленного пальца.

Аналогичным образом происходит распознавание и для других **биометрических характеристик человека**. Естественно, при этом используются другие особенности характеристик, например, для лица – это расположение и относительные размеры носа, скул и т.д. Причем в связи с тем, что фотографии могут быть разного размера, для их сравнения необходимо масштабирование, для которого в качестве «масштабного коэффициента» применяется расстояние между зрачками глаз.
Оценка эффективности **биометрических технологий**, помимо стоимостных показателей и удобства использования, основывается на использовании двух вероятностных параметров – ошибка ложного отказа (FRR – False Reject Rate) и ошибка ложного пропуска (FAR – False Accept Rate). Ошибка ложного отказа возникает в случае, если система не опознала **биометрический** признак, который соответствует имеющемуся в ней шаблону, а ошибка ложного пропуска – в случае, если система неверно сопоставила предъявленный ей признак с не соответствующим ему на самом деле шаблоном. Как понятно, ошибка ложного пропуска более опасна с точки **безопасности**, а ошибка ложного отказа приводит к уменьшению удобства пользования системой, которая иногда не распознает человека с первого раза.

Эти две вероятности взаимосвязаны, попытка уменьшения одной приводит к увеличению второй, поэтому на практике в зависимости от требований к системе выбирается определенный компромисс. Типичные значения данных вероятностей для дактилоскопических систем составляют 0,1 ё 1% для FRR и 10–3 ё 10–7% для FAR.

### ****Проблемы биометрических технологий****

Не все радужно в области **биометрических технологий**. Укажем несколько из существующих на данных момент проблем, отметив, что они, все же, постепенно разрешаются:

Дороговизна. Эта проблема актуальна для новых **биометрических технологий**, как, впрочем, и для всех новых технологий вообще. Для дактилоскопических систем можно считать ее почти решенной.

Неуниверсальность. Данная проблема связана с тем, что некоторые характеристики плохо выражены у отдельных людей. Известно, что примерно у 2% людей папиллярные узоры находятся в таком состоянии, что с трудом поддаются автоматическому распознаванию. Данная проблема возникает и при попытке применения **биометрических технологий** для людей, имеющих физические недостатки (ампутации рук или пальцев, шрамы на лице, проблемы с глазами и т.д.). В этом случае (в отличие от ошибок первого и второго рода – FAR и FRR) говорят о так называемой «ошибке третьего рода» – отказе системы принимать **биометрическую** характеристику. Путем решения этой проблемы является комплексность подхода, использующего сразу несколько **биометрических** характеристик, что позволяет на порядок снизить количество людей, **биометрическая идентификация** которых невозможна. Другим путем решения данной проблемы является использование **биометрической идентификации** совместно с другими методами (например, с аутентификацией по смарт-карте).

Относительно комплексного применения нескольких **биометрических технологий** следует сказать еще несколько слов. Помимо решения проблемы ошибки третьего рода, такое применение позволяет существенно улучшить и характеристики, связанные с ложным отказом и ложным допуском. Именно поэтому данное направление, называемое **мультибиометрической идентификацией**, является одним из наиболее перспективных в области **биометрии**.

Чувствительность к обману. Проблема, наиболее выраженная для традиционных технологий (палец, лицо), что связано с их давним появлением. Существуют и успешно применяются различные методы борьбы с этой проблемой, основанные на различных физических характеристиках муляжей и живых тканей. Например, для отпечатков пальцев может применяться методика измерения пульса или электропроводности.
Отсутствие стандартов. По сравнению с 2005 годом, когда появился первый вариант данной статьи, положение существенно улучшилось. Приняты или находятся на выходе стандарты, касающиеся данных отпечатка пальца, двумерного изображения лица, **биометрического** программного интерфейса, тестирования **биометрических технологий** и обмена **биометрическими** данными.

Отсутствие нормативной базы. Последнее по месту, но не по значению. Наоборот, проблема отсутствия нормативной базы является в настоящий момент наиболее важной: получение и использование **биометрических** характеристик может регулироваться только на основе федерального законодательства. Существующие в настоящий момент законы («О персональных данных», «О государственной дактилоскопической регистрации в Российской Федерации» и пр.) требуют серьезных дополнений и корректировок, без которых, с одной стороны, не будут защищены права человека, а с другой – не могут нормально развиваться **биометрические технологии**.

### ****Области применения**** биометрических технологий

**Биометрические технологии** решают вопросы **идентификации** человека, область их применения – это различные системы, где требуется такая **идентификация**.

В первую очередь следует упомянуть системы доступа к информации, где у **биометрических технологий** есть существенное преимущество перед остальными методами. В отличие от пароля (того, что знает человек и может сообщить кому-то еще) или от различных карт и ключей (того, что принадлежит человеку и может быть им утеряно или скопировано), **биометрические** характеристики однозначно **идентифицируют** именно самого человека. Такие же преимущества есть и при применении **биометрических технологий** в области физического доступа в различных **системах контроля доступа**.

Именно исходя из вышеуказанных преимуществ **биометрических технологий** и было принято решение об их использование в паспортно-визовых документах.

Традиционно **биометрия** применяется в криминалистике, причем объемы информации, с которыми приходится иметь дело, измеряются миллионами записей, и есть даже специальный термин для обозначения таких систем – АДИС (**автоматизированная дактилоскопическая идентификационная система**).

**Биометрические технологии** также применяются и в других сферах, например, для поиска разыскиваемых субъектов в потоке людей по внешнему виду. Особый интерес вызывает применение **биометрии** в области медицины.

### ****Перспективы**** биометрических технологий

Как уже отмечалось, в настоящий момент совершенствование **биометрических технологий** происходит ускоренными темпами. В первую очередь это приводит к тому, что повышается надежность и снижается стоимость для традиционных технологий: распознавания по отпечатку пальца, лицу и радужной оболочке глаза.

Наряду со старыми технологиями появляются и новые. Ряд из них – особенно распознавание по трехмерному образу лица – имеют значительный потенциал и способны в будущем серьезно изменить положение дел на **биометрическом** рынке.

И, конечно, основным событием в области **биометрии** является уже начавшееся массовое внедрение данных технологий для паспортно-визовых документов. Данное событие приводит не только к технологическим изменениям и совершенствованию имеющихся на рынке систем и устройств, в будущем оно значительно изменит сам образ жизни людей. Я считаю, что это будут изменения к лучшему, так как они позволят повысить безопасность как отдельных людей, так и общества в целом.