Современные методы биометрической идентификации

К современным методам аутентификации относится проверка подлинности на основе биометрических показателей. При биометрической аутентификации, секретными данными пользователя могут служить, как глазная сетчатка, так и отпечаток пальца. Эти биометрические образы являются уникальными для каждого пользователя, что обеспечивает высокий уровень защиты доступа к информации. Согласно предварительно установленным протоколам, биометрические образцы пользователя регистрируются в базе данных.

Современная биометрическая аутентификация основывается на двух методах:

- ***статический метод аутентификации — распознает физические параметры человека, которыми он обладает на протяжении всей жизни: от своего рождения и до самой смерти (отпечатки пальцев, отличительные характеристики радужной оболочки глаза, рисунок глазной сетчатки, термограмма, геометрия лица, геометрия кисти руки и даже фрагмент генетического кода);***
- ***динамический метод — анализирует характерный черты, особенности поведения пользователя, которые демонстрируются в момент выполнения какого либо обычного повседневного действия (подпись, клавиатурный почерк, голос и другое).***

Основным на всемирном рынке биометрической защиты, всегда являлся статический метод. Динамическая аутентификация и комбинированные системы защиты информации занимали, всего лишь, 20 % рынка. Однако, в последние годы, наблюдается

активное развитие динамических методов защиты. Особенный интерес сетевых технологий представляют методы клавиатурного почерка и аутентификации по подписи.

В связи с довольно быстрым развитием современных биометрических технологий, появляется критически важная проблема — определение общих стандартов надежности биометрических систем защиты. Большим авторитетом среди специалистов пользуются средства, имеющие сертификаты качества, которые выдает Международная ассоциация по компьютерной безопасности ICSA (International Computer Security Association).

Статический метод биометрической аутентификации и его разновидности

Дактилоскопия — наиболее популярная технология биометрической аутентификации, основанная на сканировании и распознавании отпечатков пальцев.

Данный метод активно поддерживается правоохранительными органами, с целью привлечения в свои архивы электронных образцов. Также, метод сканирования отпечатков пальцев легок в использовании и надежен универсальностью данных. Главным устройством этого метода биометрической аутентификации есть сканер, который сам по себе имеет небольшие размеры и является относительно недорогим в цене. Такая аутентификация осуществляется достаточно быстро за счет того, что система не требует распознавания каждой линии узора и сравнения её с исходными образцами, находящимися в базе. Системе достаточно определить совпадения в масштабных блоках и проанализировать раздвоения, разрывы и прочие искажения линий (минуции).

Уникальность каждого отпечатка позволяет использовать данный метод биометрической аутентификации как в криминалистике, в процессах серьезных бизнес-операций, так и в быту. В последнее время появилось множество ноутбуков со встроенным сканером отпечатков пальцев, клавиатур, компьютерных мышей, а также смартфонов для аутентификации пользователя.

Есть и минусы в этой, казалось бы, неоспоримой и не поддельной, аутентификации. Из-за использования сложных алгоритмов распознавания мельчайших папиллярных линий, система аутентификации может демонстрировать сбои при недостаточном контакте пальца со сканером. Обмануть средство аутентификации и саму систему защиты можно и с помощью муляжа (очень качественно выполненного) или мертвого пальца.

По принципу работы, используемые для аутентификации сканеры, делятся на три вида:

- ***оптические сканеры, функционирующие на технологии отражения, или по принципу просвета. Из всех видов, оптическое сканирование не способно распознать муляж, однако, благодаря своей стоимости и простоте, именно оптические сканеры наиболее популярны;***
- ***полупроводниковые сканеры — подразделяются на радиочастотные, емкостные, термочувствительные и чувствительные к давлению сканеры. Тепловые (термосканеры) и радиочастнотные сканеры лучше всех способны распознать настоящий отпечаток и не допустить аутентификацию по муляжу пальца. Полупроводниковые сканеры считаются более надежными, нежели оптические;***
- ***ультразвуковые сканеры. Данный вид устройств является самым сложным и дорогим. С помощью ультразвуковых сканеров можно совершать аутентификацию не только по отпечаткам пальцев, но и по некоторым другим биометрическим параметрам, таким как частота пульса и пр.***

Аутентификация по сетчатке глаза. Данный метод стали использовать еще в 50-х годах прошлого столетия. В то время, как раз, была изучена и определена уникальность рисунка кровеносных сосудов глазного дна.

Сканеры сетчатки глаза имеют довольно большие габариты и более высокую цену, нежели сканеры отпечатков пальцев. Однако, надежность такого вида аутентификации гораздо выше дактилоскопии, что и оправдывает вложения. Особенности рисунка кровеносных сосудов глазного дна таковы, что он не повторяется даже у близнецов. Поэтому, такая аутентификация имеет максимальную защиту. Обмануть сканер сетчатки глаза, практически невозможно. Сбои при распознавании глазного рисунка незначительно малы — примерно, один на миллион случаев. Если, у

пользователя нет серьезных глазных заболеваний (например, катаракта), он может уверенно использовать систему аутентификации по сетчатке глаза для защиты доступа к всевозможным хранилищам, приватных кабинетов и сверхсекретных объектов.

Сканирование сетчатки глаза предусматривает использование инфракрасного низкоинтенсивного излучения, которое направляется к кровеносным сосудам глазного дна через зрачок. Сигнал отображает несколько сотен характерных точек, которые записываются в шаблон. Самые современные сканеры вместо инфракрасного света направляют лазер мягкого действия.

Для прохождения данной аутентификации, человек должен максимально приблизить к сканеру лицо (глаз должен быть не далее 1,5 см от устройства), зафиксировать его в одном положении и направить взгляд на дисплей сканера, на специальную метку. Около сканера, в таком положении, приходится находиться приблизительно минуту. Именно столько много времени требуется сканеру для осуществления операции сканирования, после чего, системе понадобится еще несколько секунд для сравнения полученного образца с установленным шаблоном. Длительное нахождение в одном положении и фиксация взгляда на вспышку света и являются самыми большими недостатками использования данного вида аутентификации. Плюс, из-за относительно долгого сканирования сетчатки и обработки результатов, данное устройство невозможно устанавливать для аутентификации большого количества людей (например, проходной).

Аутентификация по радужной оболочке глаза. Данный метод аутентификации основан на распознавании уникальных особенностей радужной оболочки глаза.

Схожий на сеть, сложный рисунок подвижной диафрагмы между задней и передней камерами глаза — это и есть уникальная радужная оболочка. Данный рисунок человеку дается еще до его рождения и особо не изменяется в течении всей жизни. Надежности аутентификации методом сканирования радужной оболочки глаза способствует различие левого и правого глаз человека. Такая технология, практически, исключает ошибки и сбои при аутентификации.

Однако, сложно назвать устройства, считывающие рисунок радужной оболочки — сканерами. Это, скорее всего, специализированная камера, которая делает 30 снимков в секунду. Затем оцифровывается одна из записей и преобразовывается в упрощенную

форму, из которой отбираются около 200 характерных точек и информация по ним записывается в шаблон. Это куда более надежно, чем сканирование отпечатков пальцев — для формирования таких шаблонов используются всего лишь 60-70 характерных точек.

Данный вид аутентификации предполагает дополнительную защиту от поддельных глаз — в некоторых моделях устройств, для определения «жизни» глаза, изменяется поток света, направленный в него и система отслеживает реакцию и определяет изменяется ли размер зрачка.

Данные сканеры уже широко используются, к примеру, в аэропортах многих стран для аутентификации сотрудников во время пересечения зон ограниченного доступа, а также, неплохо зарекомендовали себя в Англии, Германии, США и Японии во время экспериментального использования с банкоматами. Следует отметить, что при аутентификации по радужной оболочке глаза, в отличие от сканирования сетчатки, считывающая камера может находиться от 10 см до 1 метра от глаза и процесс сканирования и распознавания проходит намного быстрее. Данные сканеры стоят дороже, нежели вышеуказанные средства биометрической аутентификации, но, в последнее время и они становятся все более доступными.

Аутентификация по геометрии руки — данный метод биометрической аутентификации предполагает измерение определенных параметров человеческой кисти, например: длина, толщина и изгибы пальцев, общая структура кисти, расстояние между суставами, ширина и толщина ладони.

Руки человека не являются уникальными, поэтому для надежности данного вида аутентификации необходимо комбинировать распознавание сразу по нескольким параметрам.

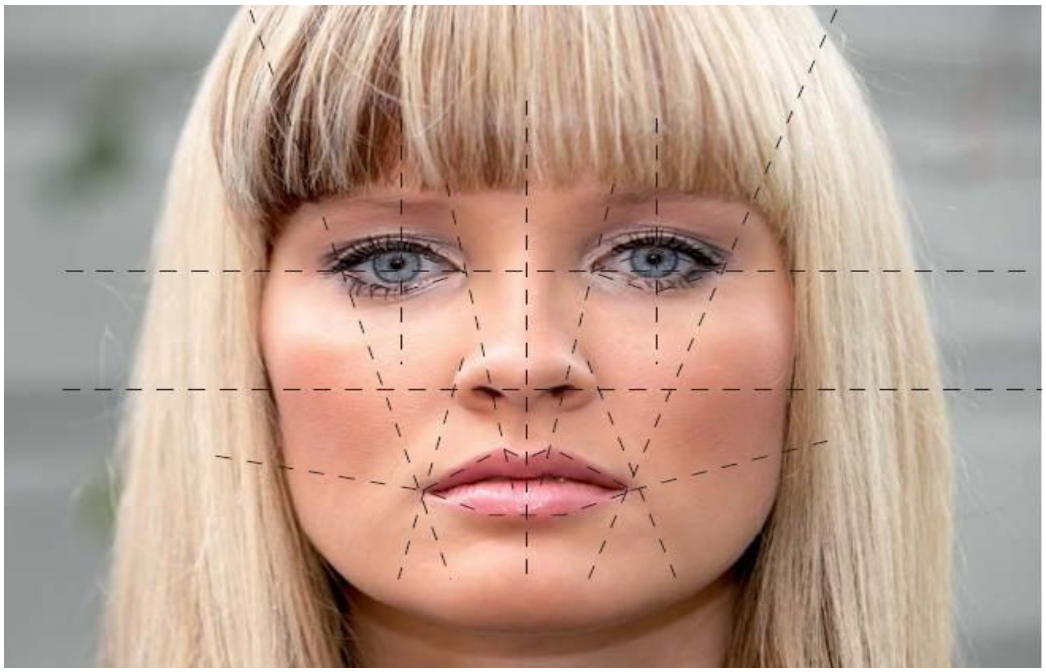
Вероятность ошибок при распознавании геометрии кисти составляет около 0,1%, а это значит, что при ушибе, артрите и прочих заболеваниях и повреждениях кисти, скорее всего, пройти аутентификацию не удастся. Так что, данный метод биометрической аутентификации не подходит для обеспечения безопасности объектов высокой степени секретности.

Однако, данный метод нашел широкое распространение, благодаря тому, что он удобен для пользователей по целому ряду причин. Одной из немаловажных таких причин является то, что устройство для распознания параметров руки не принуждает пользователя к дискомфорту и не отнимает много времени (весь процесс аутентификации осуществляется за несколько секунд). Следующей причиной популярности аутентификации по геометрии руки можно назвать тот факт, что ни температура, ни загрязненность, ни влажность кисти не влияют на процедуру аутентификации. Также, удобен данный метод и тем, что для распознавания кисти можно использовать изображение низкого качества — размер шаблона, хранящегося в базе всего 9 байт. Процедура сравнения кисти пользователя с установленным шаблоном очень проста и легко может быть автоматизирована.

Устройства данного вида биометрической аутентификации могут иметь разный внешний вид и функционал — одни сканируют лишь два пальца, другие делают снимок всей руки, а некоторые современные устройства при помощи инфракрасной камеры сканируют вены и по их изображению осуществляют аутентификацию.

Данный метод впервые был использован в начале 70-х годов прошлого века. Сегодня подобные устройства можно встретить в аэропортах и различных предприятиях, где необходимо формировать достоверные сведения о присутствии того, или иного человека, учета рабочего времени и прочих процедур контроля.

Аутентификация по геометрии лица. Этот биометрический метод аутентификации является одним из «трёх больших биометрик» наряду с распознаванием по радужной оболочке и сканированию отпечатков пальцев.



Данный метод аутентификации подразделяется на двухмерное и трехмерное распознавание. Двухмерное (2D) распознавание лица используется уже очень давно, в основном, в криминалистике. Но, с каждым годом данный метод усовершенствуется, повышая, этим самым, уровень своей надежности. Однако, до совершенства двухмерному методу распознавания лица еще далеко — вероятность ложных срабатываний при данной аутентификации варьируется от 0,1 до 1 %. Еще выше частота ошибок непризнания.

Куда больше надежд возлагают на новейший метод — трехмерное (3D) распознавание лиц. Оценки надежности данного метода пока не выведены, так как он является относительно молодым. Разработкой систем трехмерного распознавания лиц занимаются около десяти ведущих мировых ИТ-компаний, в том числе и из России. Большинство таких разработчиков предоставляют на рынок сканеры вместе с программным обеспечением. И только некоторые работают над созданием и выпуском сканеров.

При трёхмерном распознавании лиц используется множество сложных алгоритмов, эффективность которых зависит от условий их применения. Процедура сканирования составляет около 20-30 секунд. В этот момент лицо может быть повернуто относительно камеры, что принуждает систему компенсировать движения и формировать проекции лица с четким выделением черт лица, таких как контуры бровей, глаз, носа, губ и др. Затем система определяет расстояние между ними. В основном, шаблон составляется из таких неизменных характеристик, как глубина глазных впадин, форма черепа, надбровных дуг, высота и ширина скул и прочих ярко выраженных особенностей, благодаря которым впоследствии система сможет распознать лицо даже при наличии бороды, очков, шрамов, головного убора и прочего. Всего для построения шаблона используется от 12 до 40 особенностей лица и головы пользователя.

Международный подкомитет по стандартизации в области биометрии (IS0/IEC JTC1/SC37 Biometrics) в последнее время занимается разработкой единого формата сведений для распознавания человеческих лиц на основе двух- и трехмерных изображений. Скорее всего, два данных метода объединят вы один биометрический метод аутентификации.

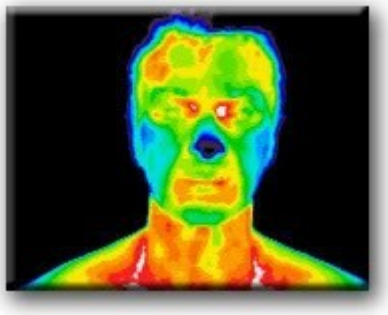
Термография лица. Данный биометрический метод аутентификации выражается в установлении человека по его кровеносным сосудам.

Лицо пользователя сканируется при помощи инфракрасного света и формируется термограмма — температурная карта лица, являющаяся достаточно уникальной. Данный метод по своей надежности сравним с методом аутентификации по отпечаткам пальцев. Сканирование лица при данной аутентификации можно производить с десятиметрового расстояния. Этот метод способен распознать близнецов (в отличии от распознавания по геометрии лица), людей, перенесших пластические операции, использующих маски, а также он эффективен не смотря на температуру тела и старение организма.

Однако, данный метод не распространен широко, возможно, из-за невысокого качества получаемых термограмм лиц.

Динамические методы биометрической аутентификации

Метод распознавания голоса. Биометрический метод аутентификации пользователя по голосу является наиболее доступным для реализации.



Данный метод позволяет произвести идентификацию и аутентификацию личности при помощи лишь одного микрофона, который подключен к записывающему устройству. Использование данного метода бывает полезным в судебных случаях, когда единственной уликой против подозреваемого служит запись телефонного разговора. Метод распознавания голоса является очень удобным — пользователю достаточно лишь произнести слово, без совершения каких-либо дополнительных действий. И, наконец, огромным преимуществом данного метода является право осуществления скрытой аутентификации. Пользователь не всегда может быть осведомлен о включении дополнительной проверки, а значит, злоумышленникам будет еще сложнее получить доступ.

Формирование персонального шаблона производится по многим характеристикам голоса. Это может быть тональность голоса, интонация, модуляция, отличительные особенности произношения некоторых звуков речи и другое. Если система аутентификации должным образом проанализировала все голосовые характеристики, то вероятность аутентификации постороннего лица никчемно мала. Однако, в 1-3 % случаев, система может дать отказ и настоящему обладателю ранее определенного голоса. Дело в том, что голос человека может меняться во время болезни (например, простуды), в зависимости от психического состояния, возраста и т.п. Поэтому, биометрический метод голосовой аутентификации нежелательно использовать на объектах повышенной безопасности. Он может быть использован для доступа в компьютерные классы, бизнес-центры, лаборатории и подобного уровня безопасности объекты. Также, технология распознавание голоса может применяться не только в качестве аутентификации и идентификации, но и как незаменимый помощник при голосовом вводе данных

Метод распознавания клавиатурного почерка — является одним из перспективных методов биометрической аутентификации сегодняшнего дня. Клавиатурный почерк представляет собой биометрическую характеристику поведения каждого пользователя, а именно — скорость ввода, время удержания клавиш, интервалы между нажатиями на них, частота образования ошибок при вводе, число перекрытий между клавишами, использование функциональных клавиш и комбинаций, уровень аримичности при наборе и др.

Данная технология является универсальной, однако, лучше всего, распознавание клавиатурного почерка подходит для аутентификации удаленных пользователей. Разработкой алгоритмов распознавания клавиатурного почерка активно занимаются как зарубежные, так и российские ИТ-компании.

Аутентификация по клавиатурному почерку пользователя имеет два способа:

- ***ввод известной фразы (пароля);***
- ***ввод неизвестной фразы (генерируется случайным образом).***

Оба способа аутентификации предполагают два режима: режим обучения и режим самой аутентификации. Режим обучения заключается в многократном вводе пользователем кодового слова (фразы, пароля). В процессе повторного набора, система определяет характерные особенности ввода текста и формирует шаблон показателей пользователя. Надежность такого вида аутентификации зависит от длины вводимой пользователем фразы.

Среди преимуществ данного метода аутентификации следует отметить удобство пользования, возможность осуществления процедуры аутентификации без специального оборудования, а также возможность скрытой аутентификации. Минусом данного метода, как и в случае с распознаванием голоса, можно назвать зависимость отказа системы от возрастных факторов и состояния здоровья пользователя. Ведь, моторика, куда сильнее, нежели голос, зависит от состояния человека. Даже простая человеческая усталость может повлиять на прохождение аутентификации. Смена клавиатуры, также может быть причиной отказа системы — пользователь способен не сразу адаптироваться к новому устройству ввода и поэтому, при вводе проверочной фразы, клавиатурный почерк может не соответствовать шаблону. В частности, это влияет на темп ввода. Хотя, исследователи предлагают повысить эффективность данного метода за счет использования ритма. Искусственное добавление ритма (например, ввод пользователем слова под какую-то знакомую мелодию) обеспечивает устойчивость клавиатурного почерка и более надежную защиту от злоумышленников.

Верификация подписи. В связи с популярностью и массовому использованию различных устройств с сенсорным экраном, биометрический метод аутентификации по подписи становится очень востребованным.

Максимально точную верификацию подписи обеспечивает использование специальных световых перьев. Во многих странах электронные документы, подписанные биометрической подписью, имеют такую же юридическую силу, что и бумажные носители. Это позволяет осуществлять документооборот значительно быстрее и беспрепятственно. В России, к сожалению, доверие оказывает лишь бумажный подписанный документ, или электронный документ, на который наложена официально зарегистрированная электронная цифровая подпись (ЭЦП). Но, ЭЦП легко передать другому лицу, что не сделаешь с биометрической подписью. Поэтому, верификация по биометрической подписи является более надежной.

Биометрический метод аутентификации по подписи имеет два способа:

- ***на основе анализа визуальных характеристик подписи. Данным способом предполагается сравнение двух изображений подписи на соответствие идентичности — это может осуществляться как системой, так и человеком;***
- ***способ компьютерного анализа динамических характеристик написания подписи. Аутентификация таким способом происходит после тщательного исследования сведений о самой подписи, а также о статистических и периодических характеристиках ее написания.***

Формирование шаблона подписи осуществляется в зависимости от требуемого уровня защиты. Всего, одна подпись анализируется пол 100-200 характерным точкам. Если же, подпись ставится с использованием светового пера, то помимо координат пера, учитывается и угол его наклона, нажатие пера. Угол наклона пера исчисляется относительно планшета и по часовой стрелке.

Данный метод биометрической аутентификации, как и распознавание клавиатурного почерка, имеют общую проблему — зависимость от психофизического состояния человека.

Комбинированные решения биометрической аутентификации
Мультимодальная, или комбинированная система биометрической аутентификации — это устройство, в котором объединены сразу несколько биометрических технологий. Комбинированные решения по праву считаются наиболее надежными в плане защиты информации с помощью биометрических показателей пользователя, ведь подделать сразу несколько показателей гораздо сложнее, нежели один признак, что

является, практически, не под силу злоумышленникам. Максимально надежными считаются 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, например, мобильные телефоны со встроенными камерами, ноутбуки, видеодомофоны и прочее.

Комбинированные системы биометрической аутентификации значительно эжффективнее мономодальных решений. Это подтверждает множество исследований, в том числе опыт одного банка, который установил сперва систему аутентификации пользователей по лицу (частота ошибок за счет низкого качества камер 7 %), затем по голосу (частота ошибок 5% из-за фоновых шумов), а после, комбинировав эти два метода, достигли почти 100 % эффективности.

Биометрические системы могут быть объединены различными способами: параллельно, последовательно или согласно иерархии. Главным критерием при выборе способа объединения систем должна служить минимализация соотношения количества возможных ошибок ко времени одной аутентификации.

Помимо комбинированных систем аутентификации, можно использовать и многофакторные системы. В системах с многофакторной аутентификацией, биометрические данные пользователя используются вместе с паролем или электронным ключом.

Защита биометрических данных
Биометрическая система аутентификации, как и многие другие системы защиты, в любой момент может быть подвергнута нападению злоумышленников. Соответственно, начиная с 2011 года, международная стандартизация в области информационных технологий предусматривает мероприятия по защите биометрических данных — стандарт IS0/IEC 24745:2011. В российском законодательстве защиту биометрических данных регламентирует Федеральный закон «О персональных данных», с последними изменениями в 2011 году.

Наиболее распространенным направлением в области современных биометрических методов аутентификации является разработка стратегии защиты, хранящихся в базах данных биометрических шаблонов. Среди самых популярных киберпреступлений дня сегодняшнего во всем мире считается «кража личности». Утечка шаблонов из базы данных делает преступления более опасными, так как восстанавливать биометрические данные злоумышленнику проще за счет обратного инжиниринга шаблона. Поскольку биометрические характеристики неотъемлемы от своего носителя, похищенный шаблон нельзя заменить нескомпроментированным новым, в отличии от пароля. Опасность кражи шаблона еще заключается в том, что помимо доступа к защищенным данным, злоумышленник может заполучить секретную информацию о человеке, или организовать за ним тайную слежку.

Защита биометрических шаблонов базируется на трех основных требованиях:

- *необратимость — данное требование ориентировано на сохранение шаблона таким образом, чтобы злоумышленнику было невозможно восстановить вычислительным путем биометрические характеристики из образца, или создать физические подделки биометрических черт;*
- *различимость — точность системы биометрической аутентификации не должна быть нарушена схемой защиты шаблона;*
- *отменяемость — возможность формирования нескольких защищенных шаблонов из одних биометрических данных. Данное свойство предоставляет биометрической системе*

возможность отзывать биометрические шаблоны и выдавать новые при компрометации данных, а также предотвращает сопоставление сведений между базами данных, сохраняя этим самым приватность данных пользователя.

Оптимизируя надежную защиту шаблона, главной задачей является нахождение приемлемого взаимопонимания между этими требованиями. Защита биометрических шаблонов строится на двух принципах: биометрические криптосистемы и трансформация биометрических черт. Последние изменения в законодательстве запрещают оператору биометрической системы самостоятельно, без присутствия человека, менять его персональные данные. Соответственно, приемлемыми становятся системы, хранящие биометрические данные в зашифрованном виде. Шифровать эти сведения можно двумя методами: с помощью обычного ключа и шифрование при помощи ключа биометрического — доступ к данным предоставляется исключительно в присутствии владельца биометрических показателей. В обычной криптографии ключ расшифровки и зашифрованный шаблон представляют собой две абсолютно разные единицы. Шаблон может считаться защищенным в том случае, если защищен ключ. В биометрическом ключе происходит одновременная инкапсуляция шаблона криптографического ключа. В процессе шифрования подобным способом, в биометрической системе хранится лишь частичная информация из шаблона. Ее называют защищенным эскизом — secure sketch. На основании защищенного эскиза и другого биометрического образца, схожего на представленный при регистрации, восстанавливается оригинальный шаблон.

ИТ-специалисты, занимающиеся исследованиями схем защиты биометрических шаблонов, обозначили два главных метода создания защищенного эскиза:

- *нечеткое обязательство (fuzzy commitment);*
- *нечеткий сейф (fuzzy vault).*

Первый метод годится для защиты биометрических шаблонов, имеющих вид двоичных строк определенной длины. А второй может быть полезным для защиты шаблонов, которые представляют собой наборы точек.

Внедрение криптографических и биометрических технологий положительное влияет на разработку инновационных решений для обеспечения информационной безопасности. Особенно перспективной является многофакторная биометрическая криптография, объединившая в себе технологии пороговой криптографии с разделением секрета, многофакторной биометрии и методы преобразования нечетких биометрических признаков в основные последовательности.

Невозможно сформировать однозначный вывод, какой из современных биометрических методов аутентификации, или комбинированных методов является наиболее эффективным для тех, или иных коммерческих из расчета соотношения цены и надежности. Определенно видно, что для множества коммерческих задач использовать сложные комбинированные системы не представляется логичным. Но, вовсе не рассматривать такие системы, тоже не верно. Комбинированную систему аутентификации можно задействовать с учетом требуемого в данный момент уровня безопасности с возможностью активации дополнительных методов в дальнейшем.