## 6. Задачи идентификации, аутентификации, авторизации, методы их реализации. Методы биометрической аутентификации пользователей

Идентификация призвана каждому пользователю (группе пользователей) сопоставить соответствующую ему разграничительную политику доступа на защищаемом объекте.

Для этого пользователь должен себя идентифицировать – указать своё «имя» (идентификатор). Таким образом, проверяется, относится ли регистрирующийся пользователь к пользователям, идентифицируемым системой. И в соответствии с введённым идентификатором пользователю будут сопоставлены соответствующие права доступа.

Аутентификация предназначена для контроля процедуры идентификации. Для этого пользователь должен ввести пароль. Правильность вводимого пароля подтверждает однозначное соответствие между регистрирующимся пользователем и идентифицированным пользователем.

В общем случае, идентифицируются и аутентифицируются не только пользователи, но и другие субъекты доступа к ресурсам.

Совокупность выполнения процедур идентификации и аутентификации принято называть процедурой авторизации. Иногда не требуется идентифицировать пользователя, а достаточно только выполнения процедуры аутентификации. Например, это происходит когда требуется подтвердить текущего (уже зарегистрированного) пользователя при выполнении каких-либо действий, требующих дополнительной защиты. В свою очередь, не всегда требуется осуществлять контроль идентификации, то есть в некоторых случаях аутентификация может не производиться.

Процедура авторизации имеет ключевое значение при защите компьютерной информации, т.к. вся разграничительная политика доступа к ресурсам реализуется относительно идентификаторов пользователей. То есть, войдя в систему с чужим идентификатором, злоумышленник получает права доступа к ресурсу того пользователя, идентификатор которого был им предъявлен при входе в систему.

Чтобы исключить работу с системой незаконных пользователей, необходима процедура распознавания системой каждого законного пользователя (или групп пользователей). Для этого в защищенном месте система обязана хранить информацию, по которой можно опознать пользователя, а пользователь при входе в систему, при выполнении определенных действий, при доступе к ресурсам обязан себя идентифицировать, т. е. указать идентификатор, присвоенный ему в данной системе. Получив идентификатор, система проводит его аутентификацию, т. е. проверяет его содержательность (подлинность) - принадлежность к множеству идентификаторов. Если бы идентификация не дополнялась аутентификацией, то сама идентификация теряла бы всякий смысл. Обычно устанавливается ограничение на число попыток предъявления некорректного идентификатора.

**Аутентификация пользователя может быть основана на следующих принципах:**

- на предъявлении пользователем пароля;
- на предъявлении пользователем доказательств, что он обладает секретной ключевой информацией;
- на ответах на некоторые тестовые вопросы;
- на предъявлении пользователем некоторых неизменных признаков, неразрывно связанных с ним;
- на предоставлении доказательств того, что он находится в определенном месте в определенное время;
- на установлении подлинности пользователя некоторой третьей, доверенной стороной.

Процедуры аутентификации должны быть устойчивы к подлогу, подбору и подделке. После распознавания пользователя система должна выяснить, какие права предоставлены этому пользователю, какую информацию он может использовать и каким образом (читать, записывать, модифицировать или удалять), какие программы может выполнять, какие ресурсы ему доступны, а также другие вопросы подобного рода. Этот процесс называется авторизацией. Таким образом, вход пользователя в систему состоит из идентификации,

аутентификации и авторизации. В процессе дальнейшей работы иногда может появиться необходимость дополнительной авторизации в отношении каких-либо действий.

Существуют различные механизмы реализации разграничения доступа. Например, каждому ресурсу (или компоненту) системы может быть поставлен в соответствие список управления доступом, в котором указаны идентификаторы всех пользователей, которым разрешен доступ к данному ресурсу, а также определено, какой именно доступ разрешен.

При обращении пользователя к конкретному ресурсу система проверяет наличие у данного ресурса списка управления доступом и, если он существует, проверяет, разрешено ли этому пользователю работать с данным ресурсом в запрошенном режиме.

Другим примером реализации механизма авторизации пользователя является профиль пользователя - список, ставящий в соответствие всем идентификаторам пользователей перечень объектов, к которым разрешен доступ данному пользователю, с указанием типа доступа.

Может быть организована системная структура данных, так называемая матрица доступа, которая представляет собой таблицу, столбцы которой соответствуют идентификаторам всех системных ресурсов, а строки - идентификаторам всех зарегистрированных пользователей. На пересечении i-го столбца j-й строки таблицы администратор системы указывает разрешенный тип доступа владельца i-го идентификатора j-му ресурсу.

Доступ к механизмам авторизации должны иметь только специальные системные программы, обеспечивающие безопасность системы, а также строго ограниченный круг пользователей, отвечающих за безопасность системы.

Рассматриваемые механизмы должны быть тщательно защищены от случайного или преднамеренного доступа неавторизованных пользователей. Многие атаки на информационные системы нацелены именно на вывод из строя или обход средств разграничения доступа.

Аналогичные действия осуществляются в системе и при аутентификации других субъектов взаимодействия (претендентов), например прикладных процессов или программ, с системой (верификатором). В отличие от аутентификации субъекта взаимодействия, процедура аутентификации объекта, устанавливая подлинность электронной почты, банковского счета и т. п., проверяет факт принадлежности данного объекта владельцу указанного идентификатора.

**Требования к идентификации и аутентификации**

**Формализованные требования к данным механизмам защиты состоят в следующем:**

- Должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов
- Система защиты должна требовать от пользователей идентифицировать себя при запросах на доступ.
- Система защиты должна подвергать проверке подлинность идентификации — осуществлять аутентификацию. Для этого она должна располагать необходимыми данными для идентификации и аутентификации.
- Система защиты должна препятствовать доступу к защищаемым ресурсам не идентифицированных пользователей и пользователей, подлинность идентификации которых при аутентификации не подтвердилась (для 5 класса защищенности по классификации СВТ).

Кроме ограничения «...паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов...» данные требования никак не формализуют подходы к реализации механизмов парольной защиты. Кроме того, данные требования не определяют, каким образом должны быть реализованы механизмы парольной защиты, а также не накладывают дополнительных ограничений, связанных с повышением стойкости пароля к

подбору. В частности, они не регламентируют использование внешних носителей парольной информации — дискет, смарт-карт и т.д.

**Дополнительные требования:**

Существует целая группа угроз, связанная с некорректностью реализации процедуры авторизации в современных ОС, а также с наличием ошибок в реализации соответствующих механизмов защиты. Это обусловливает целесообразность рассмотрения механизмов авторизации с целью их добавочной защиты. Кроме того, механизмы идентификации и аутентификации являются важнейшими для противодействия НСД к информации, а значит, следует рассматривать возможные варианты их резервирования.

Кроме того, в рамках декларируемого системного подхода к проектированию системы защиты, при разработке механизмов авторизации следует рассматривать как явные, так и скрытые угрозы преодоления защиты.

***Авторизация в контексте количества и вида зарегистрированных пользователей***

Кого следует воспринимать в качестве потенциального злоумышленника:

1. **В системе зарегистрирован один пользователь**

Данный пользователь является и прикладным пользователем, и администратором безопасности. Здесь источником потенциальной угрозы является только сторонний сотрудник предприятия, а вся задача защиты сводится к контролю доступа в компьютер (либо в систему), т.е. к парольной защите.

2. **В системе зарегистрированы администратор безопасности и один прикладной пользователь**

Общий случай функционирования системы с одним прикладным пользователем — это наличие в системе администратора безопасности и только одного прикладного пользователя. В задачи администратора безопасности здесь входит ограничение прав прикладного пользователя по доступу к системным (администратора безопасности) и иным ресурсам компьютера. В частности, может ограничиваться набор задач, разрешенных для решения на компьютере, набор устройств, которые могут быть подключены к компьютеру (например, внешний модем, принтер и т.д.), способ сохранения обрабатываемых данных (например, на дискетах только в шифрованном виде) и т.д.

В данном случае потенциальным злоумышленником в части несанкционированного использования ресурсов защищаемого объекта может являться как сторонний сотрудник предприятия, так и собственно прикладной пользователь. Заметим, что прикладной пользователь здесь может выступать в роли сознательного нарушителя, либо стать «инструментом» в роли стороннего нарушителя, например, запустив по чьей-либо просьбе какую-нибудь программу).

3. **В системе зарегистрированы администратор безопасности и несколько прикладных пользователей**

Кроме администратора безопасности, в системе может быть заведено несколько прикладных пользователей. При этом ресурсами защищаемого компьютера могут пользоваться несколько сотрудников, решая различные задачи. Ввиду этого информационные и иные ресурсы защищаемого объекта должны между ними разграничиваться.

В данном случае к потенциальным нарушителям добавляется санкционированный прикладной пользователь, целью которого может служить НСД к информации, хранимой на защищаемом объекте другим пользователем.

**Рекомендации по построению авторизации, исходя из вида и количества зарегистрированных пользователей**

Наиболее простой в реализации защитой является защита от стороннего сотрудника. В этом случае все мероприятия по защите возлагаются на использование механизма парольного входа.

Простота состоит в том, что, как увидим далее, в этом случае следует оказывать противодействие только явным угрозам преодоления парольной защиты, от которых защититься не представляет большого труда.

Однако основной угрозой служат преднамеренные или неумышленные действия санкционированного пользователя, который обладает возможностью осуществления скрытой атаки на защищаемый ресурс (например, запустив какую-либо программу собственной разработки).

Механизмы идентификации и аутентификации должны предусматривать противодействие всем потенциальным злоумышленникам, т.е. как сторонним по отношению к защищаемому объекту, так и санкционированным пользователям, зарегистрированным на компьютере. При этом речь идет о прикладных пользователях, т.к. осуществить какую-либо защиту от НСД к информации от администратора безопасности невозможно, даже включая применение механизмов криптографической защиты (он сумеет снять информацию до момента ее поступления в драйвер шифрования).

**С учетом сказанного можем сделать следующие выводы:**

1. На защищаемом объекте, как правило, зарегистрированы, по крайней мере, два пользователя — прикладной пользователь и администратор безопасности. Поэтому в качестве потенциального злоумышленника при реализации механизмов парольной защиты в общем случае следует рассматривать не только стороннее по отношению к защищаемому объекту лицо, но и санкционированного пользователя, который преднамеренно либо неумышленно может осуществить атаку на механизм парольной защиты.

2. Рассматривая атаки на парольную защиту следует учитывать, что по сравнению со сторонним лицом, которое может характеризоваться явными угрозами парольной защите, защита от атак санкционированного пользователя качественно сложнее, т.к. им могут быть реализованы скрытые угрозы.

## МЕТОДЫ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

В настоящее время существует множество методов биометрической аутентификации, которые делятся на две группы, рассмотренные ниже:

### 1. Статические методы

Статические методы биометрической аутентификации основываются на физиологической (статической) характеристике человека, то есть уникальной характеристике, данной ему от рождения и неотъемлемой от него. Рассмотрим их ниже:

#### 1.1. Аутентификация по отпечатку пальца.

Все существующие на сегодняшний день сканеры отпечатков пальцев по используемым ими физическим принципам можно выделить в три группы:

- - оптические;
- - кремниевые (или полупроводниковые);
- - ультразвуковые.

В основе работы оптических сканеров лежит оптический метод получения изображения. По видам используемых технологий можно выделить следующие группы оптических сканеров.

**FTIR-сканеры** - устройства, в которых используется эффект нарушенного полного внутреннего отражения (Frustrated Total Internal Reflection, FTIR).

Существуют модификации описанного сканера, в которых каждый полупроводниковый элемент в матрице сканера выступает в роли одной пластины конденсатора, а палец - в роли другой. При приложении пальца к сенсору между каждым чувствительным элементом и выступом-впадиной папиллярного узора образуется некая емкость, величина которой определяется расстоянием между поверхностью пальца и элементом. Матрица этих емкостей преобразуется в изображение отпечатка пальца.

**Чувствительные к давлению сканеры (pressure scanners)** - в этих устройствах используются сенсоры, состоящие из матрицы пьезоэлементов.

Данные типы сканеров являются самыми распространенными. Во всех приведенных полупроводниковых сканерах используются матрица чувствительных микроэлементов (тип которых определяется способом реализации) и преобразователь их сигналов в цифровую форму. Таким образом, обобщенно схему работы приведенных полупроводниковых сканеров можно продемонстрировать следующим образом.

**Радиочастотные сканеры (RF-Field scanners)** -- в таких сканерах используется матрица элементов, каждый из которых работает как маленькая антенна.

**Из достоинств можно выделить следующие:**

- Пользователю не нужно запоминать логин-пароль. В некоторых случаях это позволяет избавиться от шпаргалок на мониторе или под клавиатурой. Если же сканер встроен в мышь, то можно проводить незаметную идентификацию довольно часто.
- Малая вероятность подделки (соотношение цена/надёжность очень высоко).
- Малые размеры сканеров (можно сделать размером со щель 1x10мм и даже меньше) позволяют размещать их в мобильных устройствах.

Сейчас люди используют смартфоны и флешки для хранения конфиденциальной информации - сканер отпечатков оказывается неплохой защитой (если использовать разумно). В случае со смартфонами можно обеспечить защиту от несанкционированного использования в случае "гоп-стопа".

**Из недостатков возможно выделить следующие:**

- Пользователи считают, что их отпечатки пальцев могут использоваться в криминалистике (впрочем, иногда это так и есть).
- В случае сильного ожога или множественных порезов, идентификация пользователя становится невозможной.
- Зависимость от чистоты пальца.
- Для сухой кожи качество распознавания ниже.

### 1.2. Аутентификация по радужной оболочке глаза.

Считается, что технология аутентификации по радужной оболочке глаза произошла от еще одной очень известной технологии - аутентификации по сетчатке глаза.

Ученые провели ряд исследований, которые показали, что сетчатка глаза человека может меняться со временем, в то время как радужная оболочка глаза остается неизменной. Невозможно найти два абсолютно идентичных рисунка радужной оболочки глаза, даже у близнецов. Очки и контактные линзы, даже цветные, никак не повлияют на процесс получения изображения.

Также нужно отметить, что произведенные операции на глазах, удаление катаракты или вживление имплантатов роговицы не изменяют характеристики радужной оболочки, ее невозможно изменить или модифицировать. Слепой человек также может быть идентифицирован при помощи радужной оболочки глаза. Пока у глаза есть радужная оболочка, ее хозяина можно идентифицировать, что проиллюстрировано на рисунке 2.

Камера может быть установлена на расстоянии от 10 см до 1 метра, в зависимости от сканирующего оборудования. Термин «сканирование» может быть обманчивым, так как в процессе получения изображения проходит не сканирование, а простое фотографирование.

Радужная оболочка по текстуре напоминает сеть с большим количеством окружающих кругов и рисунков, которые могут быть измерены компьютером. Программа сканирования радужной оболочки глаза использует около 260 точек привязки для создания образца. Для сравнения, лучшие системы идентификации по отпечаткам пальцев используют 60-70 точек.

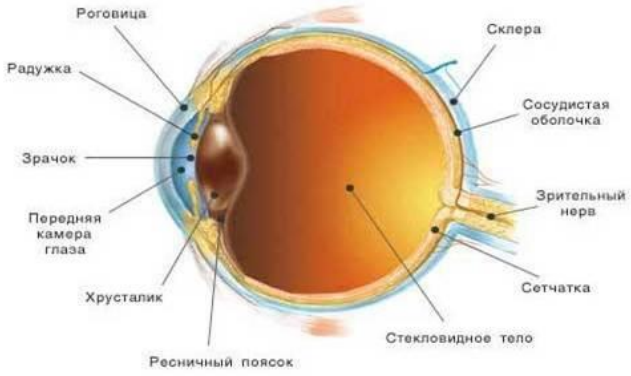


Рисунок 2 - Строение глаза, анализ участков

Стоимость всегда была самым большим сдерживающим моментом перед внедрением технологии, но сейчас системы идентификации по радужной оболочке становятся более

доступными для различных компаний. Сторонники технологии заявляют о том, что распознавание радужной оболочки глаза очень скоро станет общепринятой технологией идентификации в различных областях.

**1.3. Аутентификация по геометрии руки.**

В биометрике в целях идентификации человека большое распространение получил метод аутентификации по геометрии руки. Ключевыми признаками здесь являются размер, форма руки, а также определенные информационные знаки на тыльной стороне руки.

Существует два основных подхода к использованию геометрических характеристик кисти руки. Первый из этих подходов основан чисто на геометрических характеристиках руки. Второй же вводит еще и образцовые характеристики руки (образы на сгибах между фалангами пальцев и узоры кровеносных сосудов проиллюстрированы на рисунке 3).

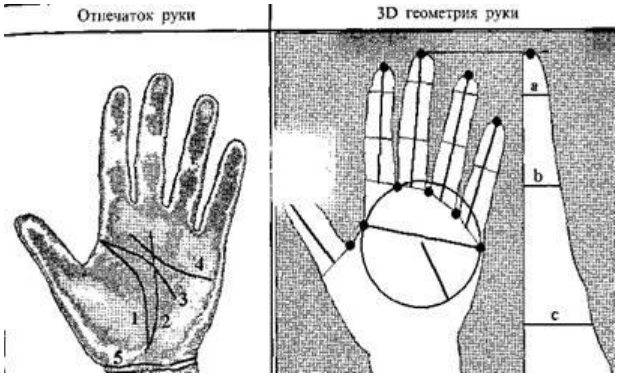


Рисунок 3 - Образы сгибов между фалангами пальцев и узоры кровеносных сосудов

**Основными геометрическими признаками являются:** ширина ладони, радиус вписанной в ладонь окружности, длины пальцев, ширина пальцев, высота кисти руки в трёх местах.

Все эти признаки объединяются в так называемый вектор значений. Метод идентификации по вектору значений достаточно прост. В начале с пользователя снимают несколько силуэтов его руки.

Для каждого из этих силуэтов формируется свой вектор значений. На основе нескольких векторов значений создается специальный класс. Далее все признаки в классе усредняются, и получаются признаки эталонного образа (или, говорят, находится центр класса). В процессе работы исходные образы могут модифицироваться.

При сравнении нового образа с эталоном, в случае успеха он может быть помещен в класс исходных признаков. Сравнивать же между собой два образа можно по нескольким критериям. Наиболее очевидный из них - наименьшее расстояние от исследуемого образа до эталона.

Более сложный метод - снимать четыре характеристики, три из которых - характерные размеры, а четвертая - полутоновое изображение складок кожи на сгибе между фалангами. Такой метод сильно затрудняет обман прибора. Стоит отметить, что в принципе более подробной информации по используемым характеристикам и алгоритмах сравнения найти не удастся, потому что компании, занимающиеся распознаванием по руке, не разглашают эту информации из соображений защиты от обмана их устройств.

В заключении стоит отметить, что метод идентификации по геометрии руки, построенный с использованием полутонового изображения обладает высокой надежностью. Кроме того, сканеры геометрии рук не выдвигают никаких требований к характеристикам рук (чистоте, температуре рук) и не наводят пользователей на мысли о криминалистике, как в случае сканеров отпечатков пальцев.

**Достоинства метода:**

- «Ключ» всегда с пользователем.
- Не предъявляются требования к чистоте, влажности, температуре рук.
- Пользователь не стесняется "криминалистического" уклона технологии.

**Недостатки метода:**

- Громоздкость устройств (за некоторым исключением).

- Невысокая сложность изготовления муляжа для устройств первого типа (использующих только геометрические характеристики).

**1.4. Аутентификация по геометрии лица.**

Система распознавания по лицу - наиболее древний и распространенный способ идентификации. Именно такой процедуре подвергается каждый, кто пересекает границу. При этом пограничник сверяет фото на паспорте с лицом владельца паспорта и принимает решение, его это паспорт или нет.

Примерно такую же процедуру выполняет компьютер, но с той лишь разницей, что фото уже находится в его памяти. Привлекательность данного метода основана на том, что он наиболее близок к тому, как мы идентифицируем друг друга.

Развитие данного направления обусловлено быстрым ростом мультимедийных видео технологий, благодаря которым можно увидеть все больше видеокамер, установленных дома и на рабочих местах.

**2. Существенный импульс**

**Существенный импульс** — это направление получило с повсеместным распространением технологии видеоконференций Internet/intranet.

Ориентация на стандартные видеокамеры персональных компьютеров делает этот класс биометрических систем сравнительно дешевым. Тем не менее, идентификация человека по геометрии лица представляет собой достаточно сложную (с математической точки зрения) задачу.

Хотя лицо человека - уникальный параметр, но достаточно динамичный; человек может улыбаться, отпускать бороду и усы, надевать очки - все это добавляет трудности в процедуре идентификации и требует достаточно мощной и дорогой аппаратуры, что соответственно влияет на степень распространенности данного метода.

Алгоритм функционирования системы опознавания достаточно прост. Изображение лица считывается обычной видеокамерой и анализируется. Программное обеспечение сравнивает введенный портрет с хранящимся в памяти эталоном. Некоторые системы дополнительно архивируют вводимые изображения для возможного в будущем разбора конфликтных ситуаций.

Весьма важно также то, что биометрические системы этого класса потенциально способны выполнять непрерывную идентификацию (аутентификацию) пользователя компьютера в течение всего сеанса его работы.

Большинство алгоритмов позволяет компенсировать наличие очков, шляпы и бороды у исследуемого индивида. Было бы наивно предполагать, что с помощью подобных систем можно получить очень точный результат. Несмотря на это, в некоторых странах они довольно успешно используются для верификации кассиров и пользователей депозитных сейфов.

Основными проблемами, с которыми сталкиваются разработчики данного класса биометрических систем, являются изменение освещенности, вариации положения головы пользователя, выделение информативной части портрета (гашение фона). С этими проблемами удается справиться, автоматически выделяя на лице особые точки и затем измеряя расстояния между ними. На лице выделяют контуры глаз, бровей, носа, подбородка. Расстояния между характерными точками этих контуров образуют весьма компактный эталон конкретного лица, легко поддающийся масштабированию.

Задача оконтуривания характерных деталей лица легко может быть решена для плоских двухмерных изображений с фронтальной подсветкой, но такие биометрические системы можно обмануть плоскими изображениями лица-оригинала. Для двухмерных систем изготовление муляжа-фотографии - это не сложная техническая задача.

Существенные технические трудности при изготовлении муляжа возникают при использовании трехмерных биометрических систем, способных по перепадам яркости отраженного света восстанавливать трехмерное изображение лица. Такие системы способны компенсировать неопределенность расположения источника освещенности по отношению к идентифицируемому лицу, а также неопределенность положения лица по отношению к

видеокамере. Обмануть системы этого класса можно только объемной маской, точно воспроизводящей оригинал.

**Данный метод обладает существенным преимуществом:** для хранения данных об одном образце идентификационного кода (одном лице) требуется совсем немного памяти. А все потому, что, как выяснилось, человеческое лицо можно поделить на относительно небольшое количество «блоков», неизменных у всех людей. Этих блоков больше, чем известных нам частей лица, но современная техника научилась выделять их и строить на их основе модели, руководствуясь взаимным расположением блоков.

Технология идентификации геометрии лица может использоваться, в частности, для такой экзотической цели, как слежение. Алгоритм позволяет выделять изображение лица на некотором расстоянии и на любом фоне, даже состоящем из других лиц, чтобы затем сравнить его с хранящимся в памяти эталонным кодом.

Система была испытана для выявления преступников на чемпионате США по американскому футболу. Факт применения этой системы скрывали до конца чемпионата, и зрители пришли в негодование от такого посягательства на демократические свободы. Технология состояла в преобразовании фотографии лица в математическое выражение, описывающее геометрию его черт. Система переводила изображение в 84-разрядный файл, называемый face print. Затем файлы, полученные при помощи видеокамер во время матчей, сравнивались с face print известных преступников.

Хотя несанкционированное применение такой технологии, равно как и сама технология, подверглись осуждению со стороны общественности, правоохранительные органы ряда городов уже выделили средства для ее развертывания.

Программа One-on-One, используя камеру, распознает лица и обеспечивает «ненавязчивый» контроль над пользователем. При инсталляции системы пользователь должен зарегистрировать свое лицо в базе данных. В результате этой процедуры One-onOne создаст цифровой шаблон (подпись), связанный с изображением лица. При дальнейшем использовании системы она будет проверять, совпадает ли изображение лица (вернее -- шаблон) пользователя с хранящимся в базе.

Наличие косметики не влияет на работу системы распознавания, которая распознает людей даже в тех случаях, когда они решили отказаться от очков.

One-on-One не сохраняет изображение лица. Поэтому компьютерный взломщик не может реконструировать изображение по учетной записи в базе данных.

**NVisage** - это наиболее продвинутая разработка Cambridge Neurodynamics. Уникальность продукта заключается в том, что он ориентирован на распознавание трехмерных объектов, в то время как в большинстве современных устройств используется только двухмерная техника.

Более надежной разновидностью описываемого метода является идентификация по «тепловому портрету» лица или тела человека в инфракрасном диапазоне. Этот метод, в отличие от обычного, оптического, не зависит от изменений лица человека (например, появления бороды), так как тепловая картина лица меняется крайне редко.

Недавно появилось сообщение об устройствах Technology Recognition Systems (США), в которых происходит распознавание лица в инфракрасном свете. Данная технология основана на том, что термограмма лица человека (тепловая картинка, созданная излучением тепла кровеносными сосудами лица) уникальна для каждого человека и, следовательно, может быть использована в качестве биокода для систем контроля допуска.

Данная термограмма является более стабильным кодом, чем геометрия лица, поскольку не зависит от времени и изменений внешности человека.