Содержание

Введение

Для идентификации личности современные электронные систем контроля и управления доступом (СКУД) используют устройства нескольких типов. Наиболее распространенными являются:

- кодонаборные устройства ПИН-кода (кнопочные клавиатуры);
- считыватели бесконтактных смарт-карт (интерфейс Виганда);
- считыватели проксимити-карт;
- считыватели ключа «тач-мемори»;
- считыватели штрих-кодов;
- биометрические считыватели.

В настоящее время самое широкое распространение получили всевозможные считыватели карт. Они имеют свои неоспоримые преимущества и удобства в использовании, однако при этом в автоматизированном пункте доступа контролируется «проход карточки, а не человека». В то же время карточка может быть потеряна или украдена злоумышленниками. Все это снижает возможность использования СКУД, основанных исключительно на считывателях карт, в приложениях с высокими требованиями к уровню безопасности. Несравненно более высокий уровень безопасности обеспечивают всевозможные биометрические устройства контроля доступа, использующие в качестве идентифицирующего признака биометрические параметры человека, которые однозначно предоставляют доступ только определенному человеку - носителю кода. Но на сегодняшний день подобные устройства все еще остаются достаточно дорогими и сложными, и поэтому находят свое применение только в особо важных пунктах доступа.

Цель работы рассмотреть принципы работы и использования биометрических средств иденфикации личности.

1. Классификация и основные характеристики биометрических средств идентификации личности

Достоинства биометрических идентификаторов на основе уникальных биологических, физиологических особенностей человека, однозначно удостоверяющих личность, привели к интенсивному развитию соответствующих средств. В биометрических идентификаторах используются статические методы, основанные на физиологических характеристиках человека, т. е. на уникальных характеристиках, данных ему от рождения (рисунки папиллярных линий пальцев, радужной оболочки глаз, капилляров сетчатки глаз, тепловое изображение лица, геометрия руки, ДНК), и динамические методы (почерк и динамика подписи, голос и особенности речи, ритм работы на клавиатуре). Предполагается использовать такие уникальные статические методы, как идентификация по подноггевому слою кожи, по объему указанных для сканирования пальцев, форме уха, запаху тела, и динамические методы -идентификация по движению губ при воспроизведении кодового слова, по динамике поворота ключа в дверном замке и т. д. Классификация современных биометрических средств идентификации показана на рис. 1.

Биометрические идентификаторы хорошо работают только тогда, когда оператор может проверить две вещи: во-первых, что биометрические данные получены от конкретного лица именно во время проверки, а во-вторых, что эти данные совпадают с образцом, хранящимся в картотеке. Биометрические характеристики являются уникальными идентификаторами, но вопрос их надежного хранения и защиты от перехвата по-прежнему остается открытым

Биометрические идентификаторы обеспечивают очень высокие показатели: вероятность несанкционированного доступа - 0,1 - 0,0001 %, вероятность ложного задержания - доли процентов, время идентификации - единицы секунд, но имеют более высокую стоимость по сравнению со

средствами атрибутной идентификации. Качественные результаты сравнения различных биометрических технологий по точности идентификации и затратам указаны на рис. 2. Известны разработки СКУД, основанные на считывании и сравнении конфигураций сетки вен на запястье, образцов запаха, преобразованных в цифровой вид, анализе носящего уникальный характер акустического отклика среднего уха человека при облучении его специфическими акустическими импульсами и т. д.

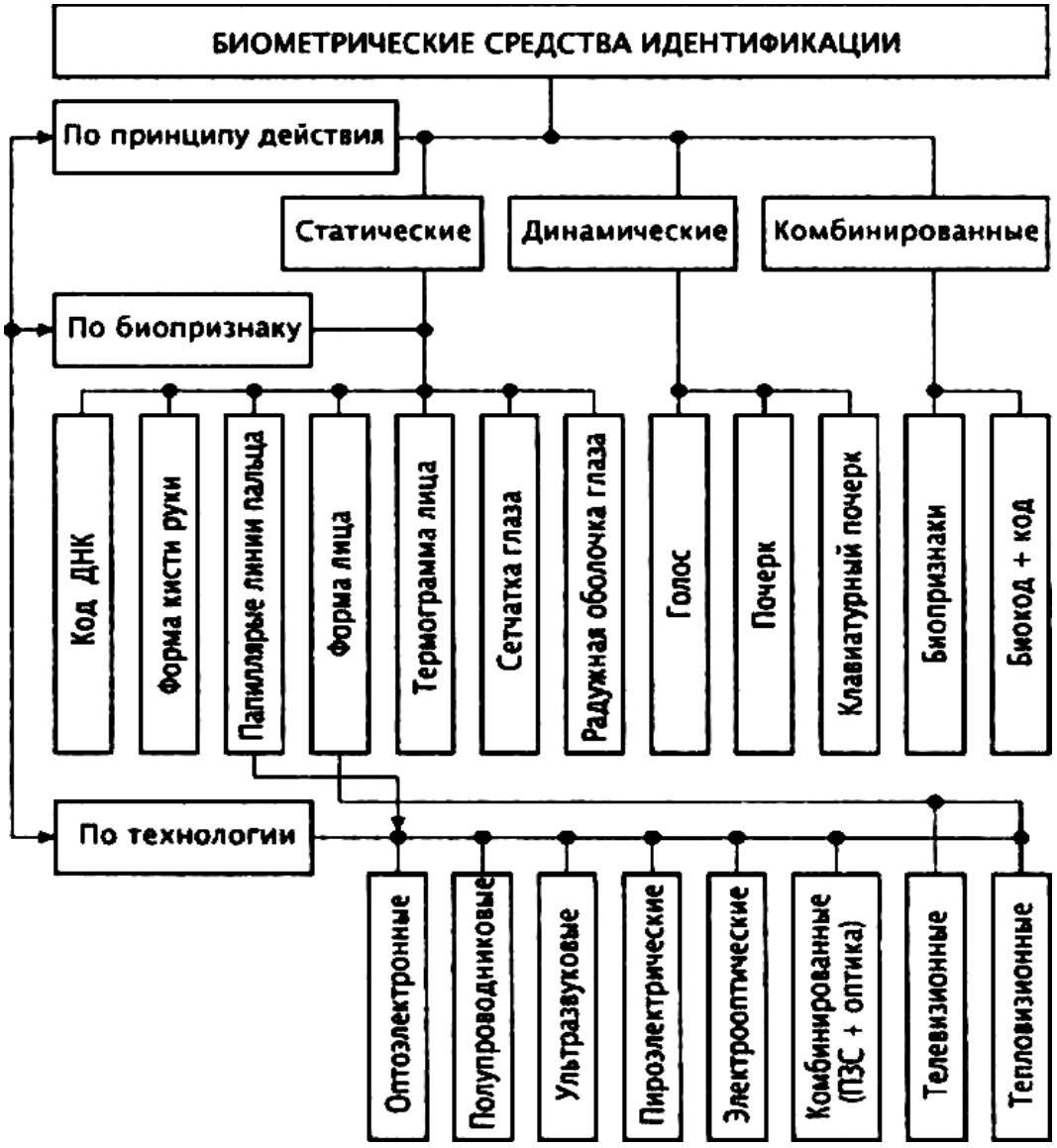

Рис. 1. Классификация современных биометрических средств идентификации

Тенденция значительного улучшения характеристик биометрических идентификаторов и снижения их стоимости приведет к широкому применению биометрических идентификаторов в различных системах контроля и управления доступом. В настоящее время структура этого рынка представля-

тся следующим образом: верификация голоса - 11 %, распознавание лица -15 %, сканирование радужной оболочки глаза - 34 %, сканирование отпечатков пальцев - 34 %, геометрия руки - 25 %, верификация подписи - 3 %.

Любая биометрическая технология применяется поэтапно:

- сканирование объекта;
- извлечение индивидуальной информации;
- формирование шаблона;
- сравнение текущего шаблона с базой данных.

Методика биометрической аутентификации заключается в следующем. Пользователь, обращаясь с запросом к СКУД на доступ, прежде всего, идентифицирует себя с помощью идентификационной карточки, пластикового ключа или личного идентификационного номера. Система по предъявленному пользователем идентификатору находит в своей памяти личный файл (эталон) пользователя, в котором вместе с номером хранятся данные его биометрии, предварительно зафиксированные во время процедуры регистрации пользователя. После этого пользователь предъявляет системе для считывания обусловленный носитель биометрических параметров. Сопоставив полученные и зарегистрированные данные, система принимает решение о предоставлении или запрещении доступа.

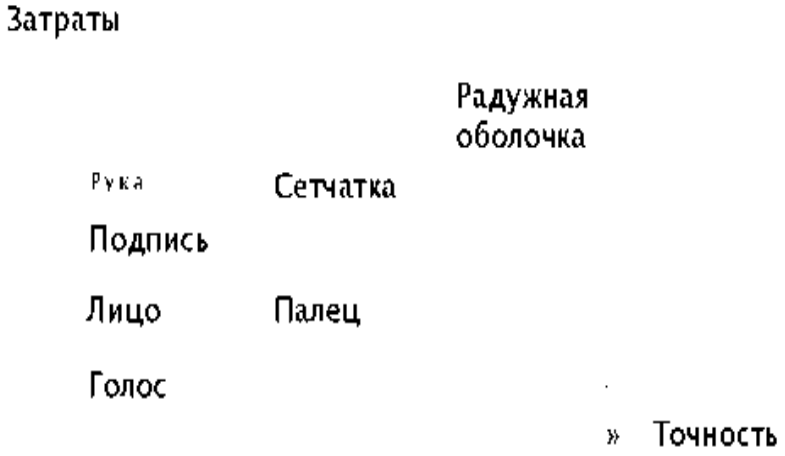

Рис. 2. Сравнение методов биометрической идентификации

Таким образом, наряду с измерителями биометрических характеристик СКУД должны быть оборудованы соответствующими считывателями идентификационных карточек или пластиковых ключей (или цифровой клавиатурой).

Основные биометрические средства защиты информации, предоставляемые сегодня российским рынком обеспечения безопасности, приведены в табл. 1, технические характеристики некоторых биометрических систем представлены в табл. 2.

Таблица 1. Современные биометрические средства защиты информации

Наименование	Производитель	Биопризнак	Примечание
SACcat	SAC Technologies	Рисунок кожи пальца	Приставка к компьютеру
TouchLock, TouchSafe, TouchNet	Identix	Рисунок кожи пальца	СКУД объекта
Eye Dentification System 7,5	Eyedentify	Рисунок сетчатки глаза	СКУД объекта (моноблок)
Ibex 10	Eyedentify	Рисунок сетчатки глаза	СКУД объекта (порт, камера)
eriprint 2000	Biometric Identification	Рисунок кожи пальца	СКУД универсал
ID3D-R Handkey	Recognition Systems	Рисунок ладони руки	СКУД универсал
HandKey	Escape	Рисунок ладони руки	СКУД универсал
ICAM 2001	Eyedentify	Рисунок сетчатки глаза	СКУД универсал
Secure Touch	Biometric Access Corp.	Рисунок кожи пальца	Приставка к компьютеру
BioMouse	American Biometric Corp	Рисунок кожи пальца	Приставка к компьютеру
Fingerprint Identification Unit	Sony	Рисунок кожи пальца	Приставка к компьютеру
Secure Keyboard Scanner	National Registry Inc.	Рисунок кожи пальца	Приставка к компьютеру
Рубеж	НПФ «Кристалл»	Динамика подписи, спектр голоса	Приставка к компьютеру
Дакточип Delsy	Элсис, НПП Электрон (Россия), Опак (Белоруссия), P&P (Германия)	Рисунок кожи пальца	Приставка к компьютеру
BioLink U-Match Mouse, Мышь SFM-2000A	BioLink Technologies	Рисунок кожи пальца	Стандартная мышь со встроенным сканером отпечатка пальца

Биометрическая система защиты компьютерной информации Дакто	ОАО «Черниговский завод радиоприборов»	Биологически активные точки и папиллярные линии кожи	Отдельный блок
Биометрическая система контроля Iris Access 3000	LG Electronics, Inc	Рисунок радужной оболочки глаза	Интеграция со считывателем карт

Говоря о точности автоматической аутентификации, принято выделять два типа ошибок Ошибки 1-го рода («ложная тревога») связаны с запрещением доступа законному пользователю. Ошибки 1-го рода («пропуск цели»)- предоставление доступа незаконному пользователю. Причина возникновения ошибок состоит в том, что при измерениях биометрических характеристик существует определенный разброс значений. В биометрии совершенно невероятно, чтобы образцы и вновь полученные характеристики давали полное совпадение. Это справедливо для всех биометрических характеристик, включая отпечатки пальцев, сканирование сетчатки глаза или опознание подписи. Например, пальцы руки не всегда могут быть помещены в одно и то же положение, под тем же самым углом или с тем же самым давлением. И так каждый раз при проверке.

Таким образом, биометрический процесс (под ним здесь понимается автоматизация оценки биометрических характеристик) констатирует уровень надежности, который гарантирует система в выявлении истинности проверяемого лица. Процесс не заявляет, что предъявленные характеристики являются точной копией образцов, а говорит о том, что вероятность того, что пользователь именно то лицо, за которое себя выдает, составляет величину X %. Всегда ожидается (предполагается), что автоматический процесс должен обеспечить вероятность правильного распознавания равную пли очень близкую к 100 %. Таким образом, намек на то, что здесь могут быть элементы ошибки, заставляет некоторых думать, что биометрия не может играть существенной роли в организации входного контроля. Анализ

показывает, что хотя ни одна система аутентификации не обеспечивает 100 %-ной надежности и что биометрический процесс не дает точного совпадения характеристик, все же он дает чрезвычайно высокий уровень точности. Некоторые зарубежные охранные структуры к разработчикам (производителям) СКУД применяют априори заданные требования, при выполнении которых последние могут рассчитывать на продажу своих систем.

Уровень надежности, дозволенный для системы контроля доступа, может быть совершенно различным, однако уровень ложных отказов истинным пользователям не вызывает какого-либо беспокойства, в то время как уровень фальшивых доступов фактически должен быть доведен до нуля

Таблица 2. Технические характеристики некоторых биометрических систем

Модель	Принцип действия	Вероятность ложного задержания,	Вероятность ложного допуска, %	Время идентификации, с
Eye Dentify	Параметры глаза	0,001	0,4	1,5-4
Iriscan	Параметры зрачка	0,00078	0,00068	2
Identix	Отпечаток пальца	0,0001	1,0	0,5
Startek BioMet	Отпечаток пальца	0,0001	1,0	1
Partners Recog-nition	Геометрия руки	0,1	0,1	1
Systems	Геометрия руки	0,1	0,1	1
«Кордон»	Отпечаток пальца	0,0001	1,0	1
DS-100	Отпечаток пальца	0,001	-	1-3
TouchSafe Per-sonal(8)	Отпечаток пальца	2	0,001	1
Eyedentify ICAM 2001 (Eyedentify)	Параметры сетчатки глаза	0,4	0,0001	1,5-4
Iriscan (Iriscan)	Параметры радужной оболочки глаза		0,00078	2
FingerScan	Отпечаток пальца	1,0	0,0001	0,5

(Identix)				
TouchSafe (Identix)	Отпечаток пальца	2,0	0,001	1
TouchNet (Identix)	Отпечаток пальца	1,0	0,001	3
Startek	Отпечаток пальца	1,0	0,0001	1
1D3D-R ND-KEY (Recognition Systems)	Геометрия руки	0,1	0,1	1
U.areU. (Digital Persona)	Отпечаток пальца	3,0	0,01	1
Fill (Sony, I/O Software)	Отпечаток пальца	0,1	1,0	0,3
BioMause (ABC)	Отпечаток пальца	-	0,2	1
Кордон (Россия)	Отпечаток пальца	1,0	0,0001	1
DS-100 (Россия)	Отпечаток пальца	-	0,001	1... 3
BioMet	Геометрия руки	0,1	0,1	1
Veriprint 2100 (Biometric ID)	Отпечаток пальца	0,001	0,01	1

Поскольку уровень надежности при сравнении может в конечном итоге регулироваться с тем, чтобы удовлетворить запросы конкретного потребителя, чрезвычайно важно этому пользователю реально представлять себе, чего данная система способна достигнуть. Наибольшую степень озабоченности вносит то, что фирмы-производители часто задают степени точности: скажем, 0,01% (т. е. 1 ошибка на 10 000 случаев аутентификации).

Можно получить статистические доказательства, позволяющие компьютеру сделать соответствующие расчеты, подтверждающие приведенные цифры, однако большинство пользователей не совсем доверяют этим результатам. Тем не менее реальная картина не столь мрачна, как

кажется на первый взгляд. Большинство биометрических методов чрезвычайно точны. Так, результаты работы в г. Ньюхема в 1998 г. комплексной системы видеонаблюдения, дающей возможность идентификации преступников, впечатляют: уровень нападения на граждан снизился на 21%, нанесение ущерба имуществу граждан сократилось на 26 %, а уровень краж имел беспрецедентное снижение на целых 39 %.

Заметное оживление на рынке биометрических систем произошло после появления довольно мощных и в то же время недорогих 16-битовых микропроцессоров и создания эффективных алгоритмов обработки биометрической информации В настоящее время биометрические терминалы разрабатываются и предлагаются к продаже в основном фирмами США, небольшим количеством фирм в Англии, России, Украины, есть информация о работах в этом направлении в Японии и во Франции.

2. Биометрические технологии будущего

Спектр технологий, которые могут использоваться в системах безопасности, постоянно расширяется. В настоящее время ряд биометрических технологий находится в стадии разработки, причем некоторые из них считаются весьма перспективными. К ним относятся технологии на основе:

1) термограммы лица в инфракрасном диапазоне излучения;
2) характеристик ДНК;
3) клавиатурного почерка;
4) анализ структуры кожи и эпителия на пальцах на основе цифровой ультразвуковой информации (спектроскопия кожи);
5) анализ отпечатков ладоней;
6) анализ формы ушной раковины;
7) анализ характеристик походки человека;
8) анализ индивидуальных запахов человека;

9) распознавание по уровню солености кожи;

10) распознавание по расположению вен.

Технология построения и анализа термограммы является одним из последних достижений в области биометрии. Как обнаружили ученые, использование инфракрасных камер дает уникальную картину объектов, находящихся под кожей лица. Разные плотности кости, жира и кровеносных сосудов строго индивидуальны и определяют термографическую картину лица пользователя. Термограмма лица является уникальной, вследствие чего можно уверенно различать даже абсолютно похожих близнецов. Из дополнительных свойств этого подхода можно отметить его инвариантность по отношению к любым косметическим или косметологическим изменениям, включая пластическую хирургию, изменения макияжа и т. п., а также скрытность процедуры регистрации.

Технология, построенная на анализе характеристик ДНК (метод геномной идентификации) является, по всей видимости, хотя и самой продолжительной, но и наиболее перспективной из систем идентификации. Метод основан на том, что в ДНК человека имеются полиморфные локусы (локус -положение хромосомы (в гене или аллели), часто имеющие 8-10 аллелей. Определение набора этих аллелей для нескольких полиморфных локусов у конкретного индивида позволяет получить своего рода геномную карту, характерную только для этого человека. Точность данного метода .определяется характером и количеством анализируемых полиморфных локусов и на сегодняшний день позволяет достичь уровня 1 ошибки на 1 млн человек.

Динамику ударов по клавиатуре компьютера (клавиатурный почерк) при печатании текста анализирует способ (ритм) печатания пользователем той или иной фразы. Существуют два типа распознавания клавиатурного почерка. Первый предназначена для аутентификации пользователя при попытке получения доступа к вычислительным ресурсам. Второй осуществляет мониторинговый контроль уже после предоставления доступа

и блокирует систему, если за компьютером начал работать не тот человек, которому доступ был предоставлен первоначально. Ритм работы на клавиатуре, как показали исследования ряда фирм и организаций, является достаточно индивидуальной характеристикой пользователя и вполне пригоден для его идентификации и аутентификации. Для измерения ритма оцениваются промежутки времени либо между ударами при печатании символов, расположенных в определенной последовательности, либо между моментом удара по клавише и моментом ее отпускания при печатании каждого символа в этой последовательности. Хотя второй способ считается более эффективным, наилучший результат достигается совместным использованием обоих способов. Отличительной особенностью этого метода является его дешевизна, так как для анализа информации не требуется никакого оборудования, кроме клавиатуры. В литературе описаны 4 математических подхода к решению задачи распознавания клавиатурного почерка пользователя ЭВМ: статистический, вероятностно-статистический (на базе теории распознавания образов) и нечеткой логики (на основе нейросетевых алгоритмов).

Следует отметить, что в настоящий момент данная технология находится в стадии разработки, и поэтому сложно оценить степень ее надежности, особенно с учетом высоких требований, предъявляемых к системам безопасности.

Для идентификации человека по руке используют несколько биометрических параметров - это геометрическая форма кисти руки или пальцев, расположение подкожных кровеносных сосудов ладони, узор линий на ладони. Технология анализа отпечатков ладоней стала развиваться сравнительно недавно, но уже имеет определенные достижения. Причиной развития этой технологии послужил тот факт, что устройства для распознавания отпечатков пальцев имеют недостаток - им нужны только чистые руки, а отпечаток грязного пальца система может и не распознать. Поэтому ряд компаний-разработчиков (например, в Великобритании)

сосредоточились на технологии, анализирующей не рисунок линий на коже, а очертание ладони, которое также имеет индивидуальный характер. Аналогичная система, работающая с отпечатками пальцев, успешно используется британскими полицейскими уже три года. Но одних лишь отпечатков пальцев, как утверждают криминалисты, часто оказывается недостаточно. До 20 % следов, оставляемых на месте преступления - это отпечатки ладоней. Однако их анализ традиционными средствами достаточно трудоемок. Компьютеризация этого процесса позволит использовать отпечатки ладоней более широко и приведет к существенному увеличению раскрываемости преступлений. Следует отметить, что устройства сканирования ладони, как правило, имеют высокую стоимость, и поэтому оснастить ими большое число рабочих мест не так уж и просто.

Технология анализа формы ушной раковины является одной из самых последних подходов в биометрической идентификации человека. С помощью даже недорогой Web-камеры можно получать довольно надежные образцы для сравнения и идентификации. Этот способ недостаточно изучен, в научно-технической литературе достоверная информация о текущем состоянии дел отсутствует.

В настоящее время ведутся разработки систем «электронного носа», реализующих процесс распознавания по запаху. Наличие генетического влияния на запах тела позволяют считать эту характеристику перспективной для использования в целях биометрической аутентификации личности. Как правило, «электронный нос» представляет собой комплексную систему, состоящую из трех функциональных узлов, работающих в режиме периодического восприятия пахучих веществ: системы пробоотбора и пробоподготовки, линейки или матрицы сенсоров с заданными свойствами и блока процессорной обработки сигналов матрицы сенсоров. Этой технологии, как и технологии анализа формы ушной раковины, еще предстоит пройти долгий путь развития, прежде чем она станет удовлетворять биометрическим требованиям.

Заключение

В заключение хочется отметить, что обойтись без биометрической идентификации, если необходимо получить позитивные, надежные и неопровержимые результаты проверки, невозможно. Ожидается, что в самом ближайшем будущем пароли и ПИН-коды уступят место новым, более надежным средствам авторизации и аутентификации.

Список использованной литературы

1. Абалмазов Э. И. Энциклопедия безопасности. Справочник каталог, 1997.
2. Абрамов А. М., Никулин О. Ю, Петрушин А. И. Системы управления доступом. М.: «Оберег-РБ», 2018.
3. Барсуков В. С. Интегральная защита информации // Системы безопасности, 2022. №5, 6.
4. Гинце А. Новые технологии в СКУД // Системы безопасности, 2020.
5. Горлицин И. Контроль и управление доступом - просто и надежно КТЦ «Охранные системы», 2022.
6. Злотник Е. Touch Memory - новый электронный идентификатор // Монитор, 2021. №6 С. 26-31.