

# Сравнительный анализ методов биометрической идентификации личности

А.Г. САБАНОВ, С. Г. СМОЛИНА

**Аннотация.** Рассматривается достоверность идентификации личности при доступе к корпоративным сетям и информационным системам общего пользования. Анализируется достоверность идентификации, выполненной с использованием различных технологий, в том числе с применением биометрии. Приводится обзор наиболее известных способов и технических решений биометрической идентификации. Показано, что достоверность биометрической идентификации личности с применением наиболее используемых технологий сравнима с достоверностью применения традиционных идентификаторов. Выработаны рекомендации по применению определенных технологий биометрической идентификации для небольших систем. Для систем с большим числом зарегистрированных пользователей применимость биометрии вызывает сомнения из-за невысокой точности идентификации и большой стоимости. Для широкого класса систем биометрическая идентификация пригодна к использованию как усиление защиты или в качестве специальных устройств, работающих на территории контролируемого периметра (как часть системы контроля и управления доступом).

**Ключевые слова:** биометрия, идентификация, анализ, метод.

## Введение

В связи с интенсификацией информатизации российского общества, переходом к облачным вычислениям и вовлечением в эти процессы федеральных и муниципальных государственных органов, предприятий, организаций и граждан весьма актуальными становятся вопросы достоверной идентификации и аутентификации (ИА) участников электронного взаимодействия. Развитие и модернизация информационных систем (ИС), содержащих открытую информацию и информацию ограниченного доступа различного уровня, а также необходимость их более тесного взаимодействия ставит одной из первоочередных задачу организации защищённого авторизованного доступа пользователей к информационным ресурсам, в том числе содержащим конфиденциальную информацию. Согласно Федеральному закону [1] информация о состоянии здоровья гражданина является одной из самых чувствительных к разглашению видов конфиденциальной информации. Управление доступом пользователей невозможно без корректного решения задач ИА [2]. Развитие системы государственных и муниципальных услуг, электронной торговли, дистанционного банковского обслуживания и образования, а также электронного здравоохранения (e-Health) требует создания и практического применения надёжных методов определения сторон удалённого электронного взаимодействия (УЭВ), позволяющих с

определённой долей уверенности говорить о достоверности идентификации личности, как правило, выступающей одной из сторон УЭВ. Одним из самых интенсивно развиваемых в последние годы методов ИА личности являются идентификация по биометрическим характеристикам. Биометрия привлекает разработчиков тем, что пользователю не надо запоминать или записывать идентификационную и аутентификационную информацию. За последние два десятилетия разработано несколько десятков методов идентификации. В маркетинговых материалах производители приводят весьма привлекательные данные по точности идентификации, однако на практике эти данные оказываются завышенными. В данной работе рассматривается достоверность некоторых самых применяемых методов идентификации, приводится обзор и краткий анализ наиболее используемых биометрических способов идентификации.

## Проблема достоверности идентификации личности в современных условиях

*Под достоверностью идентификации (ДИ) будем понимать полноту и точность идентификационной информации о пользователе. ДИ обратно пропорциональна вероятности возникновения ошибок при возникновении в ИС идентификационной и аутентификационной информации, а также во время их хранения, передачи и обработки в ИС. Другими словами,*

ДИ определяется надёжностью [13-15] и безошибочностью процесса идентификации личности.

Вопросам достоверности идентификации сторон взаимодействия пока не уделялось должное внимание, возможно из-за того, что только сейчас к множеству закрытых ранее корпоративных систем начали предъявлять требования Web-доступа и обмена с другими ИС. Число внешних пользователей многих ИС интенсивно растёт, например, ИС ФНС России уже содержит более 30 млн. внешних пользователей, и потенциал роста ещё не исчерпан. Основной проблемой при этом является определение технологий, механизмов и средств идентификации (ТМСИ), позволяющих с определенной степенью уверенности доверять результатам идентификации как для небольших ИС, так и для ИСОП (ИС общего пользования – в терминах Федерального закона №63 – ФЗ). Задача осложняется тем, что отечественная нормативная база не содержит требований к безопасности, надёжности и качеству (БНК) выполнения процессов идентификации и аутентификации [3]. Вопросы выбора тех или иных ТМСИ отдают на откуп владельцам информационных систем. Требуется найти критерии выбора, отвечающие запросам БНК и охватывающие все существующие и перспективные решения на рынке.

В качестве одного из возможных подходов к решению задачи рассматривается использование для идентификации участников УЭВ сертификатов ключа проверки электронной подписи (СКПЭП), прямым назначением которого является в числе прочих и функция идентификации владельца. Однако исследование достоверности идентификации  $D$  личности владельца СКПЭП, приведенное в работе [4], показало слишком низкие значения достоверности, рассчитываемые по формуле:

$$D = 1 - \prod_{i=1}^k p_i,$$

где  $p_i$  – вероятность отсутствия ошибки идентификации при предъявлении  $i$ -го идентификатора. Согласно существующим требованиям СКПЭП физического лица содержит в обязательном порядке ФИО и страховой номер индивидуального лицевого счета СНИЛС (2 идентификатора, из них только СНИЛС обеспечивает уникальность), что явно недостаточно для однозначной идентификации владельца СКПЭП в ИСОП; с идентификацией владельца СКПЭП – сотрудника юридического лица дело обстоит немного лучше, но не решает проблему уникальности владельца при его идентификации по заданным полям СКПЭП, поскольку точность идентификации при этом не превышает  $10^{-4}$  [4]. Для ИС общего пользования, где порядок числа пользователей составляет

$10^5 - 10^7$ , необходимо иметь надежные механизмы идентификации, обеспечивающие точность идентификации порядка  $10^{-8}$ . При увеличении числа пользователей порядок точности оценивается как  $10^{-n-1}$ , где  $n$  – количество пользователей системы. Чтобы определить пригодность предлагаемых рынком методов биометрической идентификации в качестве самостоятельного идентификатора (в сравнении с использованием СНИЛС, ИНН и других идентификаторов, находящихся в государственных реестрах) рассмотрим общее решение задачи достоверности идентификации.

Результаты идентификации (сравнения предъявленного значения идентификатора с занесённым в базу данных при регистрации пользователя значением) по своей природе должны являться предметом изучения с помощью теории вероятности. Поэтому предлагается введение уровней доверия к результатам идентификации (априори вероятностная характеристика) и аутентификации (надёжность и качество которой тоже является вероятностной характеристикой). Для упрощения задачи можно ввести 2 уровня идентификации: упрощённая (в соответствии с Федеральным законом №115-ФЗ) и стандартная, и 3 уровня аутентификации: простая, усиленная и строгая. Такой подход согласуется с исследованием процессов и результатов ИА, проведенных на основе анализа рисков идентификации и аутентификации [5] и анализа надёжности [6].

Следует различать ДИ при первичном обращении субъекта (регистрации нового пользователя) в ИС и ДИ при вторичных (чаще всего повторных) обращениях.

При этом следует учитывать, что ДИ личности при первичном обращении заявителя зависит от следующих аспектов:

- качество идентификации – отличие одного субъекта от другого путём сравнения предъявленных идентификаторов с данными, занесёнными в базу при регистрации;
- в процессе идентификации имеются ошибки первого (злоумышленник идентифицирован как легальный user) и второго рода (легальный пользователь не идентифицирован);
- необходимость введения уровней доверия к результатам сравнения в зависимости от числа идентификаторов и, главное, от надёжности и безопасности механизмов сравнения;
- необходимость протоколирования результатов процессов подтверждения совпадения идентификаторов из государственных баз данных для разбора конфликтных ситуаций.

При вторичной идентификации (повторных обращениях к ресурсам ИС) процесс идентифи-

кации сводится к процедуре сравнения предъявленных претендентом идентификаторов с занесёнными ранее данными в информационную базу при регистрации. В простейшем случае это может быть один идентификатор (например, логин), в более сложных схемах идентификации это может быть последовательная процедура предъявления заданного системой количества идентификаторов. Например, при первичном обращении гражданина РФ к portalу госуслуг, как минимум, необходимо предъявить номер паспорта и СНИЛС.

Одной из актуальных проблем является недостаточность регулирования процесса первичной идентификации заявителя, обращающегося впервые за СКПЭП квалифицированной электронной подписи (КЭП) в удостоверяющий центр (УЦ). Объективная необходимость вовлечения в процесс информатизации государственных и муниципальных услуг, с одной стороны, и положения №115-ФЗ о возможности проведения упрощённой идентификации для мало рискованных операций – с другой, допускают возможность облегчённой идентификации пользователей единого портала государственных услуг (ЕПГУ) с последующим повышением уровня достоверности идентификации при дальнейших обращениях. В зависимости от уровня рисков операций, производимых пользователем СКП КЭП, выделим способы идентификации, начиная с упрощённой (по номеру мобильного телефона, адресу электронной почты), стандартной идентификации (предъявление СКП, выданного недоверенным

УЦ, или личная явка заявителя в центр регистрации УЦ) и усиленной идентификации (рис. 1). Личная явка заявителя в центр регистрации в отличие от скана паспорта, высланного по электронной почте, может значительно повысить ДИ путем проверки ИНН и СНИЛС, а также сличения фотографии в паспорте с лицом предъявителя; при этом в случае проверки паспорта на подлинность с помощью процедур, принятых в ряде крупных банков и федеральных структур, ДИ может подняться на более высокий уровень.

Достоверность аутентификации также важна как для управления доступом пользователя к прикладному программному обеспечению, которое вызывает процедуру электронной подписи, так и для организации процедуры волеизъявления владельца средством электронной подписи (ЭП) в момент подписания документа или сообщения.

Предлагаемые выше простые уровни аутентификации могут также быть разбиты на подуровни достоверности в зависимости от используемых технологий и механизмов аутентификации. По сути, эти уровни также связаны с рисками авторизации злоумышленника под именем легального пользователя. Применяемый в западных нормативных актах и стандартах (обязательных к исполнению в отличие от российских) термин «идентификация» включает в себя как идентификацию, так и аутентификацию.

Пример оценки достоверности идентификации в терминах такого обобщённого подхода ил-

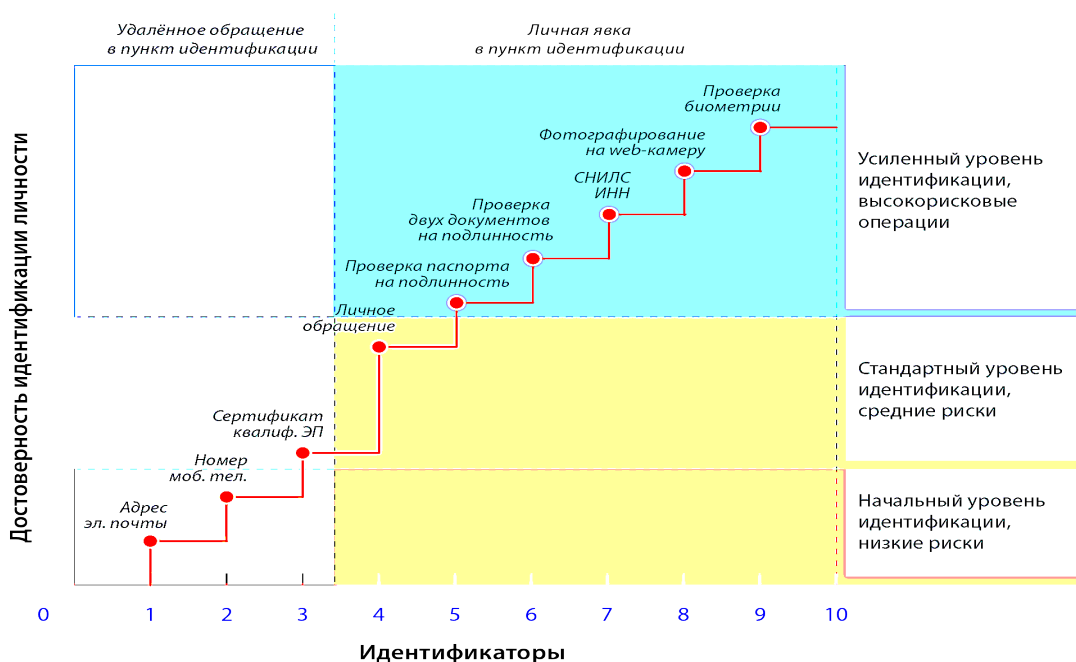


Рис. 1. Достоверность идентификации в зависимости от уровня рисков предполагаемых операций при первичном обращении

люстрируется на рис. 2. Поясним некоторые точки, изображенные на данном рисунке.

Так, предоставление паспортных данных в удалённом режиме (скана страниц паспорта) может служить основанием для проведения упрощённой идентификации в терминах №315-ФЗ. Заметим, что предъявление уже не скана, а самого паспорта при личной явке и проверка его подлинности, описанная выше, существенно повышает уровень идентификации (рис.1). Если при проверке паспорта на пункте идентификации задавались бы вопросы, ответ на которые знает только его владелец, то это была бы не идентификация, а аутентификация владельца.

Следующей точкой является предоставление заявителем его биометрической информации. Применение биометрии оправдано тем, что в отличие от возможности качественной подделки паспорта или украденных данных ИНН и СНИЛС антропологические данные в ряде случаев подделать сложнее. Достоверность идентификации в таких случаях зависит от механизма и применяемых технологий, используемых в процессе идентификации. Например, при точности метода анализа ДНК, оцениваемого как  $10^{-10}$ , совокупная точность идентификации личности путем поиска и экспертного анализа сопоставляемых образцов в базе данных находится в пределах  $10^{-5}$ - $10^{-4}$  [15,16].

В случае отсутствия более точных данных можно использовать биометрические данные, содержащиеся в новых заграничных паспортах. При всех плюсах и минусах использование биометри-

ческих характеристик является мировым трендом. Полученные тем или иным способом биометрические данные заявителя могут в дальнейшем использоваться не только для его идентификации, но, например, для разблокирования токена, содержащего ключевой материал для сертификатов доступа и сертификата ключа проверки электронной подписи.

Верхняя точка, помеченная знаком X.509\* (рис. 2) отличается от точки X.509 тем, что в данном случае применяется устройство SSCD (SecireSignatureCreationDevice – устройство безопасной генерации криптографических ключей электронной подписи) с не извлекаемым закрытым ключом. В данном случае достоверность идентификации и аутентификации владельца такого устройства выше, чем в случае применения устройств для хранения ключевых контейнеров (точка X.509), где вероятность подмены ключевого материала больше. Чтобы определить место биометрии в ряду известных и широко применяемых технологий, воспользуемся классификацией средств идентификации и аутентификации с точки зрения применяемых технологий, представленной на рис. 3 [7].

Несмотря на обилие международных нормативных документов, регулирующих процессы ИА [3], вопросы достоверности идентификации личности по биометрическим признакам до конца не изучены. Обычно при сравнении методов идентификации рассматривают только точность самой технологии идентификации (опираясь на значения, заявленные производителем). В отличие от такого

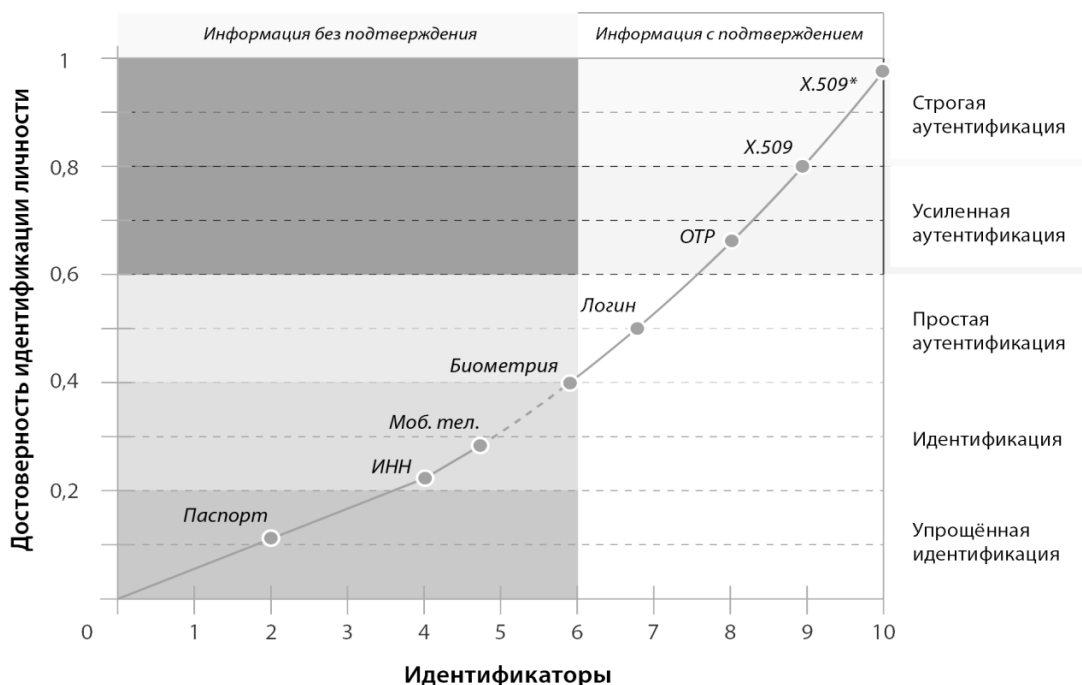


Рис. 2. Уровни идентификации и аутентификации личности

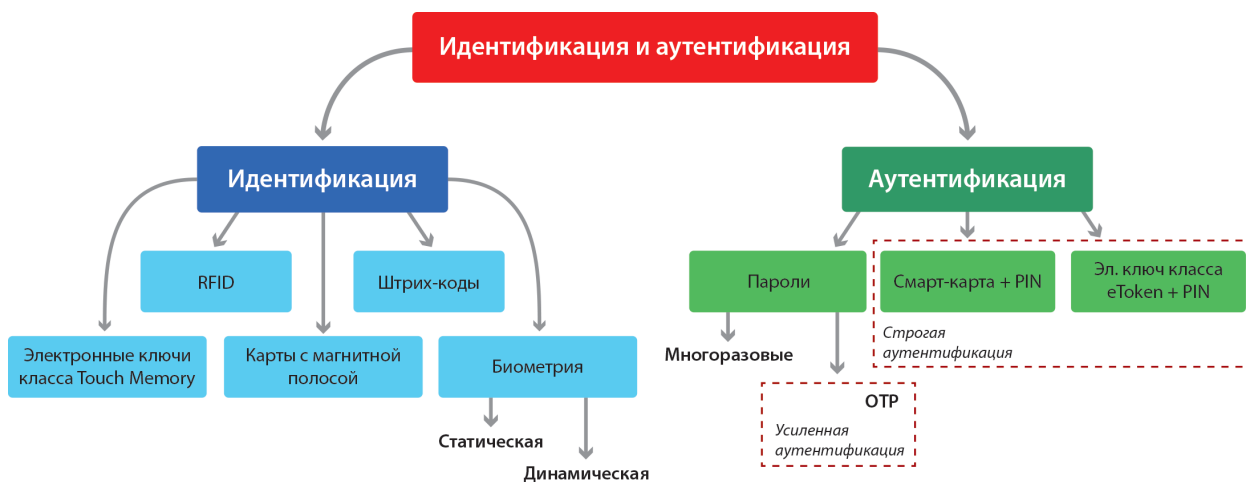


Рис. 3. Классификация средств ИА с точки зрения применяемых технологий

подхода в данной работе процедура идентификации рассматривается в виде процесса принятия решения класса «да/нет» с учётом возможных погрешностей и ошибок, как при первичной регистрации идентификаторов объектов, так и непосредственно в процессе идентификации.

Все биометрические методы основаны на вероятностных и статистических методах. Надёжность методов может оцениваться несколькими способами, в наиболее распространённом подходе в качестве основных характеристик можно принять ошибки первого и второго рода. **Ошибка первого рода** (FRR – False Rejection Rate) – это вероятность ложного отказа в доступе пользователю, имеющему право доступа. **Ошибка второго рода** (FAR – False Acceptance Rate) – это вероятность ложного доступа, когда система ошибочно опознает чужого как своего. Одним из критериев работы системы может являться подход, заключающийся в следующем: система тем лучше, чем меньше значение FRR при одинаковых значениях FAR. Иногда используется сравнительная характеристика EER, определяющая точку пересечения графиков FRR и FAR.

Основными методами, использующими статические биометрические характеристики человека, являются идентификация по папиллярному рисунку на пальцах, по радужной оболочке, геометрии лица, сетчатке глаза, рисунку вен руки, геометрии рук. Также существует семейство методов, использующих динамические характеристики: идентификация по голосу, динамике рукописного подчёрка, сердечному ритму, походке. Распределение рынка биометрии представлено на рис.4.

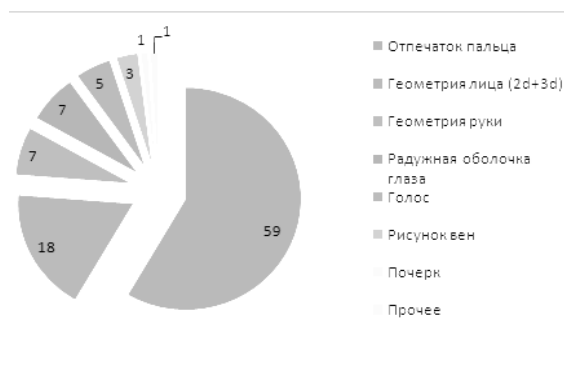


Рис. 4. Технологии идентификации (%), 2006г.[11].

На рис. 5 представлен объём рынка биометрических технологий с 2002 по 2007 гг.

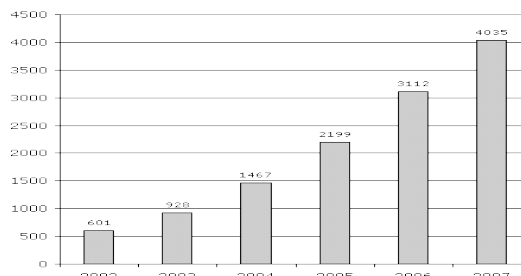


Рис. 5. Объём рынка биометрических технологий по данным International Biometric Group в период с 2002 по 2007 гг. (в млн. долл.) [11].

В данной работе рассматриваются только те характеристики, которые применимы в системах контроля и управления доступом (СКУД), как правило, это статические характеристики. Из динами-



ческих характеристик на момент написания текста только распознавание по голосу имеет статистическую значимость (FAR~0,1%, FRR~6% в идеальных условиях). В таблице 1 приведены основные методы идентификации по статическим характеристикам. [7, 9, 11,16,17,19].

В таблице 2 приведены технические характеристики биометрических систем.

### Классификация и основные характеристики средств идентификации личности



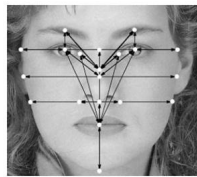
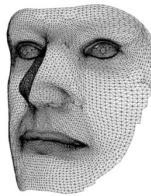
В работах[16,17] представлены несколько эмпирических характеристик, позволяющих оценить качество системы:



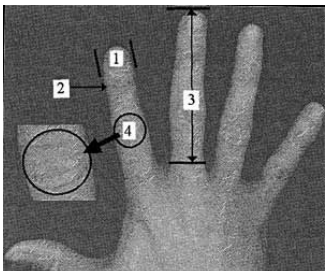
- устойчивость к подделке – эмпирическая характеристика, обобщающая то, насколько легко обмануть биометрический идентификатор;
- устойчивость к окружающей среде – характеристика, эмпирически оценивающая устойчивость работы системы при различных внешних условиях, таких как изменение освещения или температуры;
- простота использования – показывает, насколько сложно воспользоваться биометрическим сканером, возможна ли идентификация «на ходу»;
- скорость работы;
- стоимость системы.

В таблице 3 приведены экспертные оценки (по 10-бальной шкале) характеристик, которыми

**Таблица 1.**

Основные методы идентификации по статическим характеристикам.

Биометрические сканеры	Дактилоскопия (распознавание отпечатков пальцев)	Радужная оболочка	Распознавание по лицу	
Объект метода			 2-D -распознавание	
Методика	Уникальность для каждого человека рисунка папиллярных узоров на пальцах	Выделение изображения радужной оболочки глаза с помощью нескольких снимков	 3-D -распознавание	
Статистические характеристики метода(средние)	FAR	FRR	FAR	FRR
	0,10%	0,30%	0,10%	0,065%
	0,01%	0,40%	0,01%	0,070%
	0,0010%	0,60%	0,0010%	0,115%
	0,0001%	0,90%	0,0001%	0,150%
Преимущества метода	Низкая стоимость сканирующих устройств, простота процедуры	Надёжность алгоритма, защита объекта от повреждений и подделок	Отсутствие необходимости контакта со сканирующим устройством. Низкая чувствительность к внешним факторам (появление очков, бороды) Высокий уровень надежности	
Недостатки метода	Высокая степень отказа, зависимость от внешних воздействий (порез, ожог), возможность подделки	Высокая цена, низкая доступность готовых решений	Дороговизна оборудования. Изменения мимики ухудшают статистическую надежность метода	

Основные производители	SecBayometric Inc. DigitalPersona Inc. BioLink Сонда СмартЛок	LG Electronics, Panasonic, OKI. Iris Access 2200, BM-ET500, OKI IrisPass,	Geometrix, Inc. Artec Group Cognitec Systems GmbH Bioscrypt Identity Solutions Genex Technologies
Биометрические сканеры	Распознавание по венам руки	Идентификация по капиллярам сетчатки глаз	Геометрия рук
Объект метода			
Методика	Инфракрасная камера делает снимки внешней или внутренней стороны руки	Рисунок капилляров на поверхности сетчатки глаза	Оценивается более 90 характеристик, включая размеры ладони (три измерения), длину и ширину пальцев, очертания суставов и т.п.
Статистические характеристики метода (средние)	FAR=0,0008% FRR=0,0100%	FAR=0,001% FRR= 0,400%.	Нет достоверных данных
Преимущества метода	Отсутствие необходимости контактировать со сканирующим устройством. Высокая достоверность	Высокий уровень статистической надёжности	
Недостатки метода	Недопустима засветка сканера солнечными лучами и лучами галогеновых ламп. Некоторые возрастные заболевания	Сложная при использовании, долгое время обработки, высокая стоимость системы	
Основные производители		Eye Identify	Recognition Systems, BioMet Partners, Escape

должны обладать системы: устойчивость к подделке, устойчивость к окружающей среде, простота использования, стоимость, скорость, стабильность биометрического признака во времени.

Соотношение FAR и FRR (таблица 4) определяет эффективность системы и широту её использования. Заметим, что для радужной оболочки можно увеличить точность системы практически без увеличения времени процедуры квадратично, усложнив ее, сканируя два глаза, для дактилоскопического метода – путём комбинирования нескольких пальцев и распознаванию по венам, путём комбинирования двух рук, но при увеличении времени, затрачиваемого при работе с человеком.

Обобщив приведенные результаты, можно заключить, что для средних и больших предприятий, а также для объектов с максимальным требованием к безопасности рекомендуется использовать радужную оболочку в качестве средства биометрического доступа. Для объектов с количеством персонала до нескольких сотен человек оптимальным будет доступ по отпечаткам пальцев. Для ИС с большим количеством пользователей создание систем доступа на основе биометрии не оправдано экономически. Для таких систем можно использовать биометрические характеристики из федеральной базы данных (например, паспорта нового типа) в качестве дополнительного фактора.

Таблица 2.

Технические характеристики некоторых биометрических систем[13]

Модель	Принцип действия	Вероятность ложного задержания, %	Вероятность ложного допуска, %	Время идентификации, с
Eye Dentry	Параметры глаза	0,001	0,4	1,5-4
Iriscan	Параметры зрачка	0,00078	0,00068	2
Eyedentry CAM 2001	Параметры сетчатки глаза	0,4	0,0001	1,5-4
BioMet, 1D3D-R NDKEY(Recognition Systems)	Геометрия Руки	0,1	0,1	1
Identix, Startek BioMet	Отпечаток пальца	0,0001	1,0	0,5-1
FingerScan (Identix) Startek	Отпечаток пальца	1,0	0,0001	0,5-1
Кордон (Россия)	Отпечаток пальца	1,0	0,0001	1
Veriprint 2100(Biometric ID)	Отпечаток пальца	0,001	0,01	1

### Угрозы безопасности для биометрической идентификации

Рассмотрим наиболее известные угрозы безопасности для биометрической идентификации:

1. Угроза кражи биометрической информации с сервиса авторизации. Парится специальными методами, но гораздо более сложными, чем хеширование. Пока не появится рабочий и недорогой аналог хеширования биометрической информации, возможна ее кража. В настоящее время даже пароли часто хранятся в базе с недостаточно стойкими хешами.

2. Перехват биометрической информации, передаваемой по сети. Парится шифрованием канала связи. В отличие от пароля здесь необходимо

полноценное шифрование с проверкой подлинности с помощью электронной подписи.

3. Чтение биометрической информации с физически или программно (если возможно) взломанного устройства аутентификации. Парится с помощью мер физической и программной защиты устройств.

4. Кража биометрической информации «с человека» или с носителя информации. Если имеется необходимый доступ к мебели, посуде, которой касался человек, и т.п., то можно украсть отпечатки пальцев. Записывая речь человека, можно синтезировать звуки, который система биометрической идентификации посчитает похожими (считывание можно делать без ведома человека). Уже есть системы чте-

Таблица 3.

Оценка эмпирических характеристик систем биометрической идентификации.

Эмпирические характеристики	Устойчивость к подделке	Устойчивость к окружающей среде	Простота использования	Стоимость системы	Скорость работы	Стабильность признака времени
Радужная оболочка	10	9	8	7	9	10
Дактилоскопия	6	9	9	10	10	9
Лицо 2D/3D	4/9	6/8	6/10	10/5	10/7	8/10
Вены рук	10	7	9	7	8	7
Сетчатка	10	10	6	3	6	9



Таблица 4.

Соотношение FAR и FRR для систем биометрической идентификации

FRR \ FAR	0,1%	0,01%	0,001%	0,0001%	0,00001%
Радужная оболочка	0,07%	0,07%	0,12%	0,15%	0,16%
Дактилоскопия	0,30%	0,40%	0,60%	0,90%	Нет данных
Лицо 2D/3D	2,5%	5%(2D) / 0,1%(3D)	6%	9%(2D)	Нет данных
Вены рук	Нет достоверных данных				
Сетчатка	Нет достоверных данных				

ния текста вслух, при соответствующей доработке их можно использовать для фальсификации. Лучше дело обстоит с рисунком сосудов сетчатки и радужки: здесь считать информацию сложнее. Угроза парируется лишь более сложными системами аутентификации, которые смогут различить подделку. Однако парирование не такое уж и надёжное.

5. Считывание биометрической информации с помощью методов социальной инженерии или поддельных устройств. Трудно парировать. Во втором случае рекомендуется оснащать устройства чипами, имеющими сертификат с ИА информацией в защищенной памяти чипа. Тогда перед использованием проводится взаимная аутентификация устройства с сервером ИС.

6. Получение биометрической информации насильно: подделка или отрезание пальца, копирование отпечатков насильно и т.п. В отличие от пароля, человек не сможет сообщить аварийный пароль, блокирующий доступ к аккаунту (хотя сейчас только некоторые СКУД оборудованы аварийными пин-кодами на случай захвата сотрудника злоумышленниками). Как бы ни старался человек, изменить свою биометрическую информацию он вряд ли сможет. Однако, в отличие от пароля, который можно узнать в одном месте, а ввести в другом или удалённо, биометрическая идентификация требует человека для ввода биометрической информации (исключая отрезанные пальцы или системы подделки голоса). Таким образом, злоумышленнику будет сложнее скрытно заставить человека пройти идентификацию, чем при парольной защите, но только в случае, если считывающие устройства расположены на территории контролируемой зоны, специально оснащены шлюзами и охраняются. В противном случае угроза вообще никак не парируется.

### Перспективные биометрические технологии

Спектр технологий, которые могут использоваться в системах безопасности, постоянно расширяется. Ряд биометрических технологий находится

в стадии разработки, некоторые из них считаются весьма перспективными. К ним относятся технологии на основе термограммы лица в инфракрасном диапазоне излучения, характеристик ДНК, клавиатурного почерка, анализа структуры кожи и эпителия на пальцах на основе цифровой ультразвуковой информации (спектроскопия кожи), анализа отпечатков ладоней, формы ушной раковины, характеристик походки человека, индивидуальных запахов человека, распознавания по расположению вен. Оценки качества работы ряда перспективных систем приводятся в [17], а обоснованность принятия вариативного решения (идентификация личности по анализу ДНК) приводится в [18].

### Заключение

Рассмотренный подход к анализу идентификации позволяет оценить достоверность и надёжность различных методов биометрии в сравнении с другими методами идентификации. Как показано в работе, применение биометрии не решит проблем надёжности идентификации для систем с большим количеством пользователей, но может повысить достоверность идентификации субъектов при организации доступа к системам с числом пользователей, измеряемым сотнями, а также к критически важным системам как часть системы контроля и управления физическим доступом или в качестве дополнительного фактора аутентификации.

Проведенный анализ позволяет заключить, что промышленная готовность, надёжность и функциональная устойчивость работы средств биометрической идентификации в целом пока не слишком высока, а достоверность идентификации одного порядка с широко применяемыми в качестве идентификаторов СНИЛС, ИНН и т.д. Для систем с большим числом зарегистрированных пользователей применимость биометрии вызывает сомнения из-за невысокой точности идентификации и большой стоимости. Для широкого класса систем биометрическая идентификация пригодна

к использованию как усиление защиты (третий фактор аутентификации) или в качестве устройств, работающих на территории контролируемой зоны в специально отведённых зонах (как часть СКУД).

### Литература

1. *Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных».*
2. *Грушо А.А., Применко Э.А., Тимонина Е.Е.* Теоретические основы компьютерной безопасности – М.: Академия, 2009. – 272с.
3. *Сабанов А.Г.* Обзор иностранной нормативной базы по идентификации и аутентификации // Инсайд. Защита информации. 2013. №4(52). С.82-88.
4. *Сабанов А.Г.* О проблеме достоверности идентификации пользователя при удаленном электронном взаимодействии. // Доклады Томского государственного университета систем управления и радиоэлектроники, №2(32) июнь. 2014. С.180-184.
5. *Сабанов А.Г.* Анализ рисков аутентификации при удаленном электронном взаимодействии. Материалы 23-й Научно-технической конференции «Методы и технические средства обеспечения безопасности информации. 30 июня – 3 июля. Санкт-Петербург. Репино. С 53-53.
6. *Сабанов А.Г.* Методы исследования надежности удаленной аутентификации // Электросвязь. 2012. №10. С.20-24.
7. *Аутентификация.* Теория и практика. Под ред. проф., д.т.н. Шелупанова. М.: Горячая линия-Телеком, 2009,- 552 с.
8. *Постановление Правительства РФ от 28 ноября 2011г. № 977 «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме».*
9. *Смирнова Г.Н., Сорокин А.А., Тельнов Ю.Ф.* Проектирование экономических информационных систем/ Под ред. Ю.Ф. Тельнова. Московский государственный университет экономики, статистики и информатики. – М.: МЭСИ. 2004. – 452с.
10. *Громов Ю.Ю., Драчёв В.О.* и др. Моделирование процесса возникновения ошибок в информационных системах // Вестник Воронежского института ФСИН России. 2011. №1. С.32-36.
11. *Литвиненко В., Чакчир С.* Биометрия / Алгоритм безопасности. 2006. №3. См. также: <http://www.algorithm.org/arch/arch.php?id=21&a=208>
12. *Сабанов А.Г.* Методика идентификации рисков процессов аутентификации // Доклады Томского государственного университета систем управления и радиоэлектроники. 2013. №4 (30). С.136-141.
13. *Громов Ю.Ю., Иванова О.Г.* и др. Надёжность информационных систем / Тамбов: Изд-во ГОУ ВПО ТГТУ. 2010. – 158с.
14. *Шубинский И.Б.* Структурная надёжность информационных систем. Методы анализа / Ульяновск: Областная типография «Печатный двор», 2012. – 216 с.
15. *Шубинский И.Б.* Функциональная надёжность информационных систем. Методы анализа / Ульяновск: Областная типография «Печатный двор», 2012. – 296 с. <http://habrahabr.ru/post/126144/>
16. *S.Soviany, H.Jurian* A Hierarchical Data Fusion and Classification Model for Biometric Identification Systems. <http://www.agir.ro/buletine/1577.pdf>
17. *Перепечина И.О.* Проблема категорического экспертного вывода в судебной ДНК-идентификации и разработка подхода к его решению. <http://www.k-press.ru/bh/2003/2/perepechina/perepechina.asp>].
18. *Сабанов А.Г.* Обзор технологий идентификации и аутентификации // Документальная электросвязь. 2006. №17. С.23-27.

**Сабанов Алексей Геннадьевич.** Доцент МГТУ им. Н.Э. Баумана. Окончил в 1980 г. МФТИ. Количество печатных работ: более 300. Область научных интересов: методы математического моделирования, теория вероятностей, теория функциональной надежности. E-mail: [asabanov@mail.ru](mailto:asabanov@mail.ru)

**Смолина Светлана Георгиевна.** С.н.с. ИСА ФИЦ ИУ РАН. Окончила в 1979 г. МФТИ. Количество печатных работ: 52. Область научных интересов: методы математического моделирования, системный анализ. E-mail: [smolinas@mail.ru](mailto:smolinas@mail.ru)