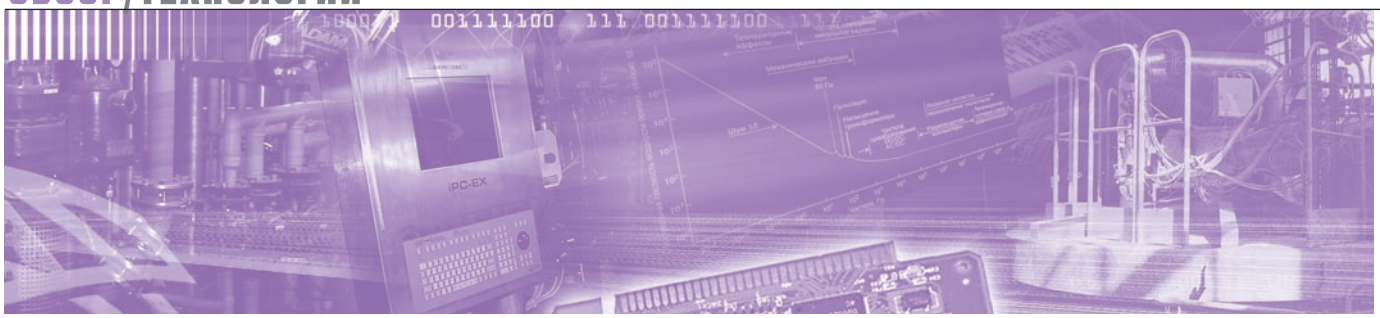

Никита Якубов

# Преимущества биометрических методов идентификации человека

**Системы биометрической идентификации человека давно стали повседневной реальностью. Тем не менее они всё ещё далеки от совершенства, и специалисты постоянно трудятся над повышением надёжности их работы и снижением стоимости. В статье описаны преимущества различных биометрических методов идентификации по сравнению с привычными RFID-картами и пин-кодами. На примере оборудования BioSmart компании «Прософт-Биометрикс» будут проиллюстрированы преимущества достаточно нового, набирающего всё большую популярность метода, основанного на уникальном рисунке подкожных вен ладони.**

Биометрические системы используют для идентификации человека такие его уникальные характеристики, как отпечатки пальцев или рисунок вен ладони, узор радужной оболочки глаза и некоторые другие. В этой статье мы приведём сравнение наиболее популярных методов идентификации, рассмотрим их плюсы и минусы.

Технологии биометрической аутентификации давно перестали ограничиваться в применении дорогостоящими системами СКУД (система контроля и управления доступом). В последние несколько лет практически все мы стали применять их ежедневно – почти все современные телефоны оснащены сканерами отпечатков пальцев, в последних моделях его даже научились скрывать под экраном смартфона, что делает его использование абсолютно незаметным для пользователя (рис. 1).

Помимо привычных для всех нас сканеров отпечатков пальцев второй по распространённости технологией является распознавание лица. В последнее время она разделилась на две ветви – 2D- и 3D-анализ. Обе они набирают популярность: 3D-сканеры, как и сканеры отпечатков пальцев, стали появляться в некоторых последних моделях смартфонов, а 2D-сканирование стало активно развиваться на фоне бурного ажиотажа вокруг нейронных сетей и машинного зрения. К слову, 2D-сканирование появилось в смартфонах довольно давно, но тогда эти системы легко можно было обмануть обычной фо-

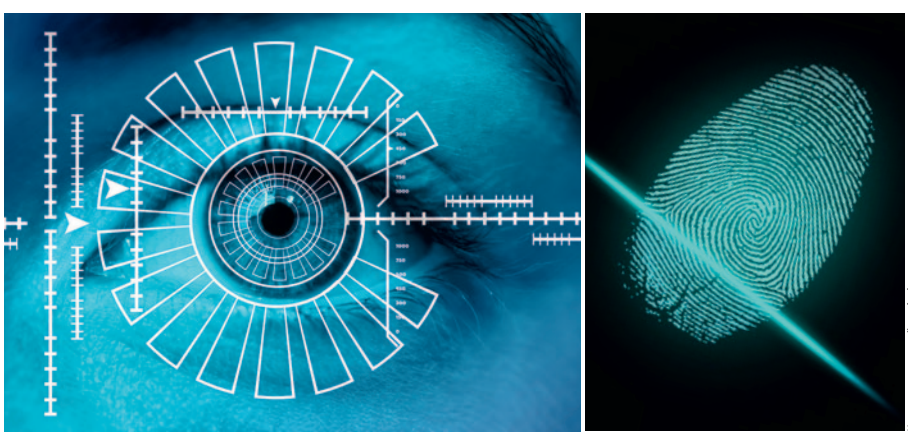

Иллюстрация с сайта pixabay.com

**Рис. 1. За биометрической идентификацией – будущее**

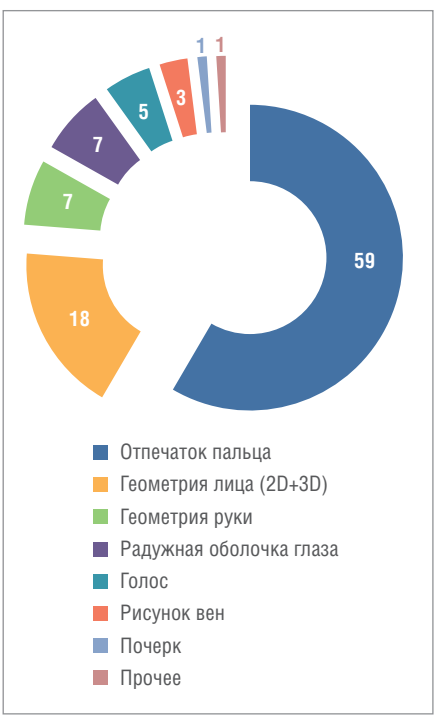


**Рис. 2. Распространённость методов биометрической идентификации**

тографией. Сейчас же система распознавания 2D с применением нейронных сетей и машинного зрения позиционируется как бюджетное решение, которое невозможно обмануть при помощи фотографии или видео, но многие всё же относятся к ней скептически.

Следующим по популярности методом биометрической идентификации является сканирование радужной оболочки глаза. На одном уровне с ним находится метод, основанный на использовании геометрии руки, но он в последнее время сдаёт позиции ввиду возможности фальсификации и появления более современного метода на основе уникального рисунка вен ладони. Все описанные методы используют статические биометрические характеристики. Помимо них существуют и динамические – голос, почерк, походка и т.д. Они менее распространены, хотя в последнее время к идентификации по голосу проявляется всё больший интерес, но его рассматривают в качестве второго фактора в дополнение к одной из статических биометрических характеристик. Более подробно процентное соотношение методов представлено на рис. 2 [1].

## Сравнительный анализ основных методов биометрической идентификации

Главными для оценки любой биометрической системы являются два параметра:

- **FAR** (False Acceptance Rate) – коэффициент ложного пропуска, то есть процент возникновения ситуаций, когда система разрешает доступ пользователю, не зарегистрированному в системе;
- **FRR** (False Rejection Rate) – коэффициент ложного отказа, то есть отказ в доступе настоящему пользователю системы.

*Таблица 1*

**Значения FAR и FRR для основных методов биометрической идентификации**

| Методы идентификации, используемые биометрической СКУД | FAR | FRR |
|---|---|---|
| Отпечаток пальца | 0,001% | 0,6% |
| Распознавание лица 2D | 0,1% | 2,5% |
| Распознавание лица 3D | 0,0005% | 0,1% |
| Радужная оболочка глаза | 0,00001% | 0,016% |
| Сетчатка глаза | 0,0001% | 0,4% |
| Рисунок вен | 0,0008% | 0,01% |

Обе характеристики получают расчётным путём на основе методов математической статистики. Чем ниже эти показатели, тем точнее распознавание объекта. В табл. 1 представлены средние значения FAR и FRR для самых популярных на сегодняшний день методов биометрической идентификации.

Но для построения эффективной системы контроля доступа недостаточно отличных показателей FAR и FRR. Например, сложно представить СКУД на основе анализа ДНК, хотя при таком методе аутентификации указанные коэффициенты стремятся к нулю, зато растёт время идентификации, увеличивается влияние человеческого фактора, неоправданно увеличивается стоимость системы.

Таким образом, для должного анализа биометрической системы контроля доступа необходимо использовать несколько эмпирических характеристик, позволяющих оценить качество системы. В первую очередь, к таким данным нужно отнести возможность подделки биометрических данных для идентификации в системе и способы повышения уровня безопасности. Во-вторых, стабильность биометрических факторов: их неизменность со временем и независимость от условий окружающей среды (температура, освещение и т.д.). В-третьих, скорость аутентификации, возможность быстрого бесконтактного снятия биометрических данных для идентификации. И, конечно, стоимость реализации биометрической СКУД на основе рассматриваемого метода и доступность составляющих [2].

## Преимущества биометрии перед традиционными RFID-картами и пин-кодами

До появления биометрических методов идентификации, впрочем, как и сейчас, СКУД по большей части основывались на RFID-картах разных форматов и пин-кодах. Если же говорить о различных Интернет-ресурсах и компьютерных системах в принципе, то сейчас, как и ранее, преобладают сочетания логина и пароля. Разумеется, RFID-карты, как и методы онлайн-аутентификации, за последнее время значительно эволюционировали. Появились новые форматы RFID-карт с защищёнными областями чтения и записи, подделать которые довольно трудно, а порой и вовсе невозможно. Для онлайн-ресурсов активно вводится двух-, и даже трёхфакторная аутентификация. Но всё же, каким бы ни было развитие, не исключены кражи карты или телефона, который зачастую используется для двухфакторной идентификации (SMS-коды подтверждения).

Большинство работающих на данный момент СКУД используют устаревшие типы карт, подделать которые не составит труда даже при минимальном бюджете. То есть пользователи подобных систем находятся в ещё большей зоне риска – ведь для создания клона карты её оригинал нужен лишь на непродолжительное время, её не обязательно красть, что довольно быстро обнаружит владелец. Но карты не только крадут или клонируют, иногда их просто забывают в другой сумке или в кармане, и это создаёт проблемы владельцу с доступом в помещение. Применяя СКУД с биометрической идентификацией, пользователь не столкнётся с проблемой забытой, украденной или скопированной карты, ведь палец или ладонь всегда при себе.

## Метод идентификации по рисунку вен ладони

Как упоминалось в начале статьи, в последнее время все бóльшую популярность набирает метод идентификации по уникальным особенностям рисунка вен ладоней. Данная система имеет общие черты со СКУД по отпечаткам пальцев, но всё же обладает некоторыми неоспоримыми преимуществами:

- не зависит от влажности или загрязнения ладони (мокрые или грязные пальцы отсканировать проблематично, порой просто невозможно);
- система успешно работает вне зависимости от сезона (рисунок кожи на пальцах может меняться в разное время года или после порезов);
- является более гигиеничным методом считывания, так как нет необходимости в контакте ладони со считывателем;
- рисунок вен ладони невозможно подделать в отличие от отпечатков пальцев, которые успешно клонируются различного рода слепками.

На последнем пункте хотелось бы остановиться подробней. Невозможность подделки рисунка вен ладони с целью обмана сканера обусловлена принципом его работы (рис. 3).

Большая часть рисунка находится глубоко под кожей и не видна на поверхности, поэтому считывание происходит в инфракрасном (ИК) спектре. Восстановленный гемоглобин крови поглощает ИК-излучение, поэтому со-

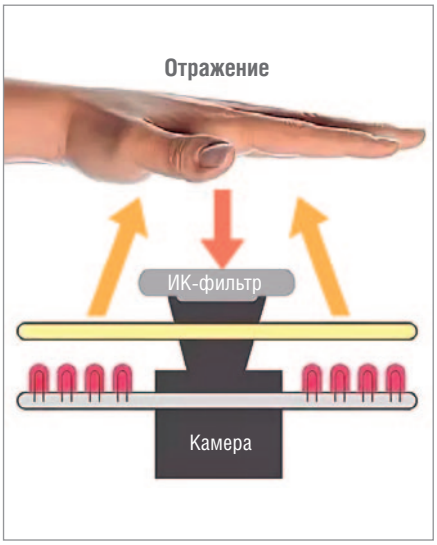


**Рис. 3. Принцип работы сканера рисунка вен ладони**

**Рис. 4. Комбинированный считыватель DCR-PV-XX**

суды ладони отражают излучение меньшей интенсивности в ИК-спектре. Проходя через ИК-фильтр камеры, полученное отражение представляет картину кровеносных сосудов, которая в последующем преобразуется в математический шаблон.

Последние технологии в сканерах отпечатков пальцев, конечно, частично отсекают подделки. Это и сканеры на основе ёмкостной технологии, и подсветка оптических считывателей в двух различных спектрах, и фиксация пульса. Но всё же сложность венозного рисунка многократно превышает сложность рисунка отпечатка пальцев, что, в свою очередь, даёт лучшие значения FAR и FRR. Все эти преимущества в совокупности с ценой, сопоставимой с решениями на основе отпечатков пальцев, поддерживающими защиту от подделок, склоняют чашу весов в сторону решений по рисунку вен ладони. Эту статистику подтверждает и компания «Прософт-Биометрикс», предлагающая решения как по технологии отпечатков пальцев, так и по рисунку вен ладони под торговой маркой BioSmart.

Сама по себе система аутентификации по рисунку вен ладони является довольно защищённой, но компания «Прософт-Биометрикс» в некоторых своих решениях смогла обезопасить её ещё больше.

## Интеграционное решение для банковской сферы DCR-PV-XX

Специально для применения в банковской сфере была создана особая версия настольного сканера рисунка вен ладоней DCR-PV-XX (рис. 4). Считыватель BioSmart DCR-PV-XX позволяет записывать шаблон рисунка вен ладони пользователя на карту формата Mifare DESFire и производить идентификацию пользователя по записанному ра-

нее шаблону. Запись шаблона производится в защищённую область карты, а сам шаблон не хранится на сервере или в терминале, что обеспечивает ещё большую защиту системы. Считыватель предназначен для интеграции в сторонние системы. Для связи используется закрытый протокол, что позволяет применять данное изделие для аутентификации также и в системах Интернет-банкинга. Характеристики считывателя BioSmart DCR-PV-XX представлены в табл. 2.

Ключевые особенности решения:

- запись шаблона рисунка вен ладони на карту;
- проверка наличия шаблона на карте;
- проверка соответствия шаблона на карте ладони пользователя;
- передача сообщений о соответствии/несоответствии ладони пользователя в стороннее ПО.

*Таблица 2*

**Характеристики считывателя BioSmart DCR-PV-XX**

| | |
|---|---|
| **Сканер вен ладоней** | Оптический, инфракрасный |
| **Встроенный считыватель RFID-карт** | Да |
| **Дальность считывания карт** | До 50 мм |
| **Интерфейс связи с ПК** | Ethernet (IEEE 802.3u, 100Base-TX) |
| **Web-интерфейс** | Да |
| **Поддержка PoE** | IEEE 802.3af class 3 |
| **Относительная влажность воздуха при эксплуатации** | Не более 90% |
| **Диапазон рабочих температур** | 0…+50°C |
| **Исполнение** | Настольное |
| **Габаритные размеры (В×Ш×Г)** | 195×115×120 мм |
| **Масса** | Нетто 370 г, брутто 570 г |
| **Гарантия** | 5 лет |

## Высоконадёжное биометрическое решение BioSmart Mobile ID

Также компания «Прософт-Биометрикс» представила перспективную технологию мобильной идентификации Mobile ID. Она позволяет организовать контроль доступа с использованием персональных данных и биометрических шаблонов, хранящихся на телефоне пользователя в зашифрованном виде. Решение соответствует требованиям европейского закона GDPR (General Data Protection Regulation – генеральный регламент о защите персональных данных) о безопасном хранении персональных биометрических данных и может использоваться в различных секторах экономики. Таким образом, BioSmart Mobile ID открывает новые пути для высоконадёжных биометрических решений.

BioSmart Mobile ID – это решение, основанное на сервисе LEGIC Connect и технологии распознавания рисунка вен ладони Biosmart. Оно позволяет организовать сложную биометрическую систе-

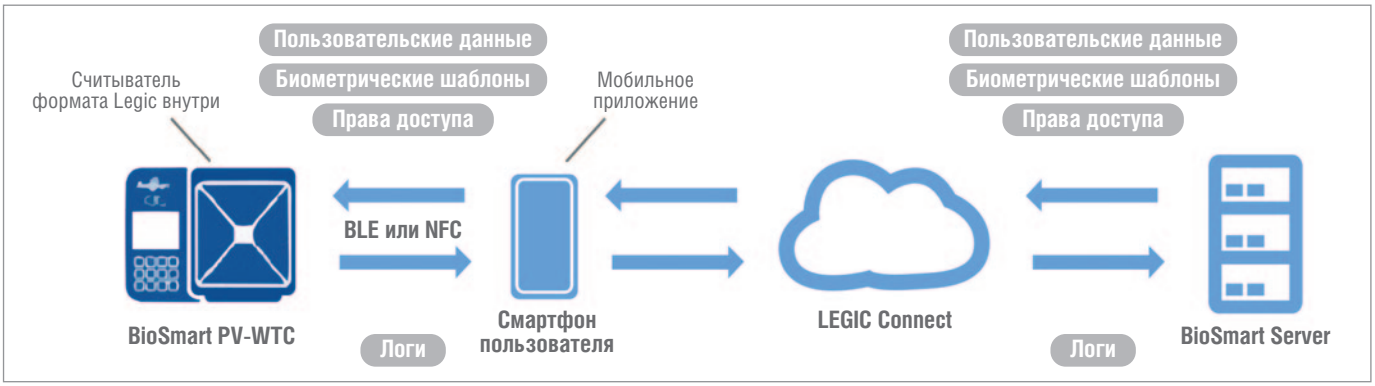


**Рис. 5. Схема решения BioSmart Mobile ID**

му контроля доступа (Access Control System – ACS), в которой все личные данные пользователя, включая биометрические шаблоны, хранятся на его мобильном устройстве.

Система состоит из четырёх основных компонентов: сервера BioSmart, сервиса LEGIC Connect, пользовательского смартфона и терминала BioSmart PV-WTC (рис. 5).

1. Сервер BioSmart предназначен для регистрации пользователей, регистрации их в службе LEGIC Connect и управления системой.
2. LEGIC Connect предоставляет наборы ключей для пользовательских данных и передаёт данные между сервером и пользовательскими устройствами.
3. Пользовательский смартфон используется в качестве платформы для мобильного приложения BioSmart, которое хранит биометрические шаблоны, права доступа и учётные данные в виде файлов NEON.
4. BioSmart PV-WTC со встроенной микросхемой LEGIC серии 6000 считывает данные с ближайших устройств через Bluetooth с низким энергопотреблением (BLE) или ближнюю связь (NFC).

Во время регистрации в программе BioSmart Studio v5 на сервере BioSmart пользователь также может быть зарегистрирован в службе LEGIC Connect. Пользовательские данные, права доступа и биометрические шаблоны будут отправлены через LEGIC Connect в виде зашифрованных файлов NEON в мобильное приложение на пользовательском смартфоне. Когда телефон пользователя приближается к точке доступа, оснащённой терминалом BioSmart PV-WTC, файлы NEON с пользовательскими данными, правами доступа и биометрическими шаблонами будут считываться терминалом через BLE и временно сохраняться в его памяти. Как только данные загружены, пользователь может получить доступ,

*Таблица 3*

**Характеристики терминала BioSmart PV-WTC**

| | |
|---|---|
| **Максимальное количество пользователей (идентификация по RFID-картам)** | 1 000 000 |
| **Максимальное количество ладоней** | 300 000 |
| **Время идентификации по венам ладони (1:1000)** | Не более 2 с |
| **Вероятность ошибочного предоставления доступа FAR** | 0,00008% |
| **Максимальное количество хранимых событий** | 10 000 000 |
| **Сканер вен ладони** | Оптический, инфракрасный |
| **Встроенный считыватель карт (опционально)** | EM-Marin, Mifare, HID Prox, HID iClass, Legic |
| **Экран** | TFT 3,5 разрешение 320×240 |
| **Клавиатура** | Сенсорная, 12 кнопок |
| **Web-интерфейс для конфигурации** | Да |
| **Поддержка блока управления реле (БУР) BioSmart** | Есть |
| **Wiegand-выход** | 26–40 бит |
| **Количество дискретных входов** | 1 |
| **Бортовое реле** | 12 В, 1 А постоянного тока |
| **Параметры электропитания** | 12 В±15%, 1 А постоянного тока |
| **Поддержка PoE** | IEEE 802.3af class 3 |
| **Диапазон рабочих температур** | 0…+50°С |
| **Габаритные размеры (В×Ш×Г)** | 220×155×140 мм |
| **Масса** | Нетто 840 г, брутто 1230 г |
| **Исполнение** | Накладной пластиковый корпус |
| **Гарантия** | 5 лет |
| **Интерфейс для связи с компьютером** | Ethernet (IEEE 802.3, 10Base-T, IEEE 802.3u, 100Base-TX) |

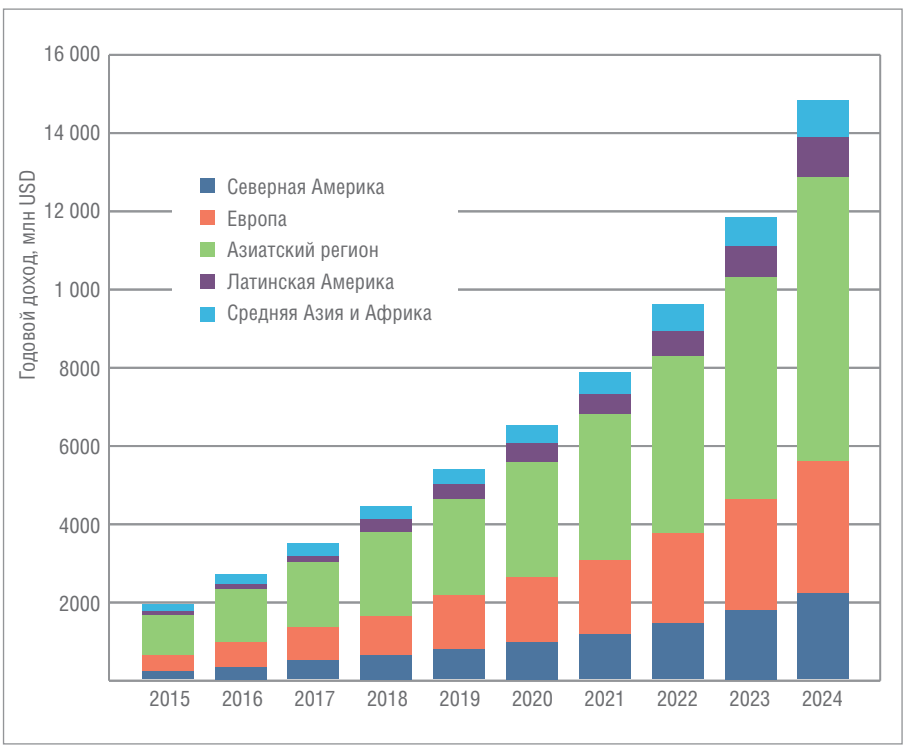


**Рис. 6. Годовой доход от биометрии по регионам, 2015–2024 гг.**

представив ладонь. С характеристиками терминала PV-WTC, входящего в состав решения BioSmart Mobile ID, можно ознакомиться в табл. 3.

Пользовательский мобильный телефон также может применяться в качестве инструмента конфигурации для BioSmart PV-WTC. Он может хранить файлы NEON с настройками, режимами работы и данными журнала с терминала.

Основные преимущества решения:

- защита пользовательских биометрических данных, предоставляемых LEGIC;
- база данных состоит только из идентификатора пользователя (UID) и прав доступа;
- производительность не зависит от количества пользователей;
- двухфакторная аутентификация (телефон + ладонь);
- неограниченное количество точек доступа, которые могут быть изолированы друг от друга.

## Заключение

Биометрические методы идентификации всё более плотно входят в нашу повседневную жизнь, и основным локомотивом при этом являются смартфоны. Пока что важнейшей областью их применения остаётся потребительская электроника, но в последнее время всё же наметился прогресс в замене старых карточных СКУД на биометрические. При этом в коммерческом секторе, а иногда и в государственных структурах, предпочтение отдаётся методу идентификации по рисунку вен ладони. На рис. 6 приведены данные о годовом доходе от биометрии на мировом рынке по регионам, основанные на статистике, а также оценивающие перспективы его развития [3].●

## Литература

1. Мальцев А. Современные биометрические методы идентификации [Электронный ресурс] // Режим доступа : https://habrahabr.ru/post/126144/.
2. Биометрическая идентификация [Электронный ресурс] // Режим доступа : http://www.techportal.ru/glossary/biometricheskaya_identifikaciya.html.
3. Титов А. Биометрия от «А» до «Я» полное руководство биометрической идентификации и аутентификации [Электронный ресурс] // Режим доступа : https://securityrussia.com/blog/biometriya.html.

**Автор – сотрудник фирмы ПРОСОФТ**
**Телефон: (495) 234-0636**
**E-mail: info@prosoft.ru**