**ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ**
**INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS**

УДК 004. 57.087.1
DOI: 10.21822/2073-6185-2023-50-3-46 -56

Оригинальная статья/Original article

# Использование биометрических данных для защиты информации

**К.Н. Власов[1], О.В. Толстых[1], О.В. Исаев[2]**
[1]Воронежский институт МВД России,
[1]394065, г. Воронеж, пр. Патриотов, 53, Россия,
[2]Воронежский институт ФСИН России,
[1]394072, г. Воронеж, ул. Иркутская 1А, Россия

**Резюме. Цель.** Актуальной задачей является оценка системы защиты доступа к информации с минимизацией ошибок, на основе использования биометрических данных человека. Необходимо оценить и сравнить методы и решения биометрической аутентификации, возможности их комбинирования. **Метод.** Метод оценки и сравнения способов и решений биометрической аутентификации основывается на практическом опыте и нормативно-технической документации по использованию биометрических данных в целях защиты информации. Необходимо усложнить возможность несанкционированного доступа к информации. Вместе с тем, совершенствование системы не должно ухудшать комфорт легитимного пользователя при попытке доступа. Остаются задачи уменьшения времени входа и упрощения системы. **Результат.** Проведена оценка методов и решений биометрической аутентификации и предложено решение по разработке систем биометрической аутентификации для защиты от несанкционированного доступа, ключевыми критериями в которых выбраны сложность взлома, комфорт пользователя, время входа и упрощение системы. **Вывод.** Оптимальным решением в разработке систем биометрической аутентификации будет использование многофакторной аутентификацией с использованием динамических параметров субъекта доступа. Современную систему биометрической аутентификации следует устанавливать с учетом требуемого на данный момент уровня безопасности.

**Ключевые слова:** биометрия, биометрические данные, защита информации, аутентификация, подлинность личности, индивидуальные характеристики личности.

**Для цитирования:** К.Н. Власов, О.В. Толстых, О.В. Исаев. Использование биометрических данных для защиты информации. Вестник Дагестанского государственного технического университета. Технические науки. 2023; 50(3):46-56. DOI:10.21822/2073-6185-2023-50-3-46-56

# Using biometric data to protect information

**K.N. Vlasov[1], O.V. Tolstykh[1], O.V. Isaev[2]**
[1]Voronezh Institute of the Ministry of Internal Affairs of Russia,
[1]53 Patriotov St., Voronezh 394065, Russia,
[2]Voronezh Institute of the Federal Penitentiary Service of Russia,
[2]1A Irkutskaya St., Voronezh 394072, Russia

**Abstract. Objective.** An urgent task is to evaluate the system for protecting access to information while minimizing errors, based on the use of human biometric data. It is necessary to evaluate and compare methods and solutions of biometric authentication, and the possibility of combining them. **Method.** The method for assessing and comparing biometric authentication methods and solutions is based on practical experience and regulatory and technical documentation on the use of biometric data for information security purposes. It is necessary to complicate the possibility of unauthorized access to information. At the same time, improving the system should not worsen the comfort of a legitimate user when trying to access. The remaining tasks are to reduce

entry time and simplify the system. **Result.** An assessment of biometric authentication methods and solutions was carried out and a solution was proposed for the development of biometric authentication systems to protect against unauthorized access, the key criteria in which were the complexity of hacking, user comfort, login time and simplification of the system**. Conclusion.** The optimal solution in the development of biometric authentication systems would be to use multi-factor authentication using dynamic parameters of the access subject. A modern biometric authentication system should be installed taking into account the level of security required at the time.

**Keywords:** biometrics, biometric data, information security, authentication, identity authenticity, individual characteristics of a person.

**For citation:** K.N. Vlasov, O.V. Tolstykh, O.V. Isaev. The use of biometric data to protect information. Herald of Daghestan State Technical University. Technical Science. 2023; 50 (3): 46-56. DOI: 10.21822 /2073-6185-2023-50-3-46-56

**Введение.** В современном мире не так трудно представить биометрические системы защиты. Появились, развиваются и используются средства доступа в информационные системы, идентификация и аутентификация пользователей и др. Есть возможность по отпечатку пальца разблокировать смартфон, голосовой помощник Siri у IPhone может узнать своего владельца по голосу. Именно процесс проверки подлинности субъекта доступа по предъявлению им своих биометрических данных называется биометрической аутентификацией. Если говорить о биометрических данных, как о средстве обеспечения безопасности, то использование такой системы защиты помогает бороться с терроризмом, кибертерроризмом и рядом других угроз. Большая стоимость биометрических систем защиты заставляет задуматься о внедрении их в повседневную жизнь человека в полном объеме. К тому же, неуязвимость таких систем куда ниже, чем о ней заявляют. Но биометрические технологии, в частности определение личности человека по биометрическим данным, стали развиваться очень быстро за последние десятки лет.

**Постановка задачи.** В России пока только происходит развитие в направлении биометрических систем идентификации и аутентификации, но решительные шаги уже сделаны. Большое количество российских компаний пытается сейчас развивать биометрические технологии. В частности, это касается защиты информации от несанкционированного доступа в системы различных ведомств. Поэтому актуальной задачей остается разработка технологий, которые способны быстро и эффективно разграничить доступ. К таким технологиям будет относится биометрическая аутентификация. Она характеризуется не только контролем доступа, но и контролем функционального состояния пользователя, а также простой внедрения и реализации.

**Методы исследования.** Метод оценки и сравнения способов и решений биометрической аутентификации основывается на практическом опыте и нормативно-технической документации по использованию биометрических данных в целях защиты информации.

**Обсуждение результатов.** Летом 2018 года Банк России и ПАО «Ростелеком» пустили в ход Единую биометрическую систему, благодаря чему, гражданам стало проще пользоваться услугами банков из-за удаленной идентификации.

Работа такой системы руководствуется Федеральным законом от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», а также Постановлением Правительства РФ от 16 июня 2022 г. №1089 «Об утверждении Положения о единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица».

В России на фоне пандемии COVID-19 наибольшее распространение получили

системы биометрической идентификации и аутентификации. Пандемия создала направление на дистанционные и бесконтактные технологии. Так в 2021 на всех станциях метро Москвы была запущена технология FacePay – платежная система, при помощи которой граждане могут оплачивать свои билеты около турникетов, оснащенных «умными камерами». Система может идентифицировать лица, даже которые закрыты медицинскими масками, но не более чем на 60%. Поэтому прогресс в области развития биометрических механизмов идентификации и аутентификации не стоит на месте.

Стоит отметить и статистические данные развития рынка биометрии в России по сравнению с мировым рынком. Эксперты утверждают, что темпы роста российских биометрических технологий опережают темпы роста мирового рынка в 1,5 раза. График сравнения предоставлен на рис. 1.

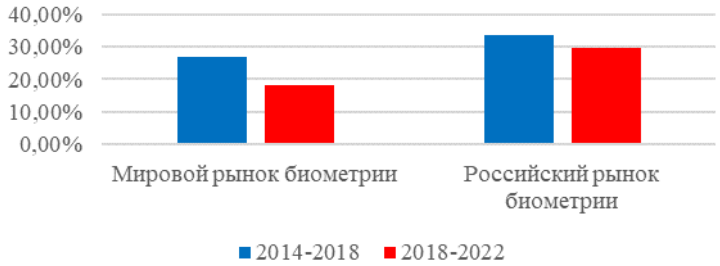


**Рис. 1. Темпы увеличения мирового и отечественного рынков биометрии**
**Fig. 1. The growth rates of the global and domestic biometrics markets**

За последние восемь лет доля России на рынке биометрии существенно увеличилась, что говорит о сохранении тенденции роста по сравнению с 2014 годом в 1,8 раз (рис. 2).

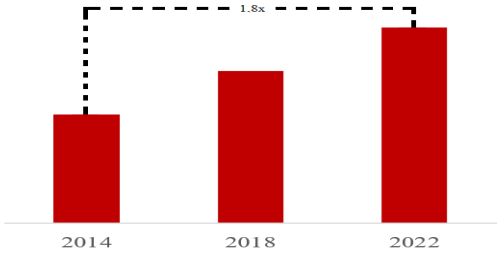


**Рис.2. Доля России в общемировом рынке биометрии**
**Fig.2. Russia's share in the global biometrics market**

К концу 2022 года был подписан закон о единой системе биометрических данных. Развитие биометрии в России стало настолько быстрым, отчего в законодательстве стали появляться пробелы, в частности это касается сбора и хранения биометрических данных. Федеральный закон от 29 декабря 2022 года №572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» устанавливает разработку видов биометрии таких как изображение лица и образец голоса. Однако существующие механизмы предусматривают более широкий спектр возможностей анализа биометрических характеристик, которые не указываются в данном законе, но в дальнейшем могут быть использованы в государственных организациях. Исходя из ГОСТ Р 52633.0-2006. «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации», нам известно, что в значительной степени используют следующие биометрические механизмы:

- анализ кровеносных сосудов глазного дна и радужной оболочки глаза;
- двухмерный и трехмерный анализы геометрических особенностей лица в видимом и инфракрасном спектрах света;
- анализ особенностей геометрии ушных раковин и особенностей голоса;
- анализ особенностей папиллярных рисунков пальцев;

- анализ геометрии ладони, включая рисунки складок кожи ладони и папиллярные рисунки различных фрагментов кожи ладони;
- анализ рисунка кровеносных сосудов, складок кожи тыльной стороны ладони;
- анализ рукописного почерка и клавиатурного почерка;
- анализ геометрических соотношений частей тела;
- анализ особенностей походки.

Таким образом, отличительные характеристики на основе анализа биометрических механизмов можно классифицировать на статические и динамические, которые характеризуются рядом свойств. Для определения качества работы биометрической системы руководствуются следующей нормативной документацией:

- ГОСТ Р ИСО/МЭК 19795-1–2007 «Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура»;
- ГОСТ Р ИСО/МЭК 19795-2–2008 «Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 2. Методы проведения технологического и сценарного испытаний»;
- ГОСТ Р ИСО/МЭК ТО 19795-3–2009 «Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 3. Особенности проведения испытаний при различных биометрических модальностях»;
- ГОСТ Р ИСО/МЭК 19795-4–2011 «Информационные технологии. Биометрия. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 4. Испытания на совместимость»;
- ГОСТ Р ИСО/МЭК 19795-6–2015 «Информационные технологии. Биометрия. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 6. Методология проведения оперативных испытаний».

Говоря о биометрии в качестве средства аутентификации, стоит отметить что такое средство способно принимать высоконадежное решение, которое включает в себя преобразование биометрических данных в векторы биометрических параметров огромной размерности, криптографическую аутентификацию, а также преобразователь «биометрия-код». Несомненно, инструменты биометрической аутентификации высокой надежности проходят тестирования для доверия, которые подтверждаются сертификационными документами. Такие тестирования закреплены в следующих нормативных документах:

- ГОСТ Р 52633.1–2009. Защита информации. Техника защиты информации. Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации;
- ГОСТ Р 52633.2–2010. Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации;
- ГОСТ Р 52633.3–2011. Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора.

Говоря о биометрии, подразумевая ее как способ защиты информации, мы можем назвать ее наукой, позволяющей проводить процесс идентификации и аутентификации личности по анатомическим или поведенческим отличительным характеристикам.

Биометрическая аутентификация – это процесс доказательства и контроль подлинности идентификатора, предъявленного субъектом доступа. Методы биометрической аутентификации подразделяют на такие виды, как статические и динамические (рис. 3). Статические биометрические характеристики человек приобретает к своему рождению. Лишь малая часть из них будет меняться в течение жизни. Большинство характеристик, которые неизменны, могут с успехом использоваться для аутентификации личности человека. Статическими их называют потому что при измерении таких характеристик, они не будут изменяться и к тому же они независимы по времени. Но бывают ошибки, например, относительное смещение аутентификатора и измерителя. Поэтому, чтобы зарегистрировать личность, измерения проводят не один раз. Это

способствует нейтрализации ошибок.

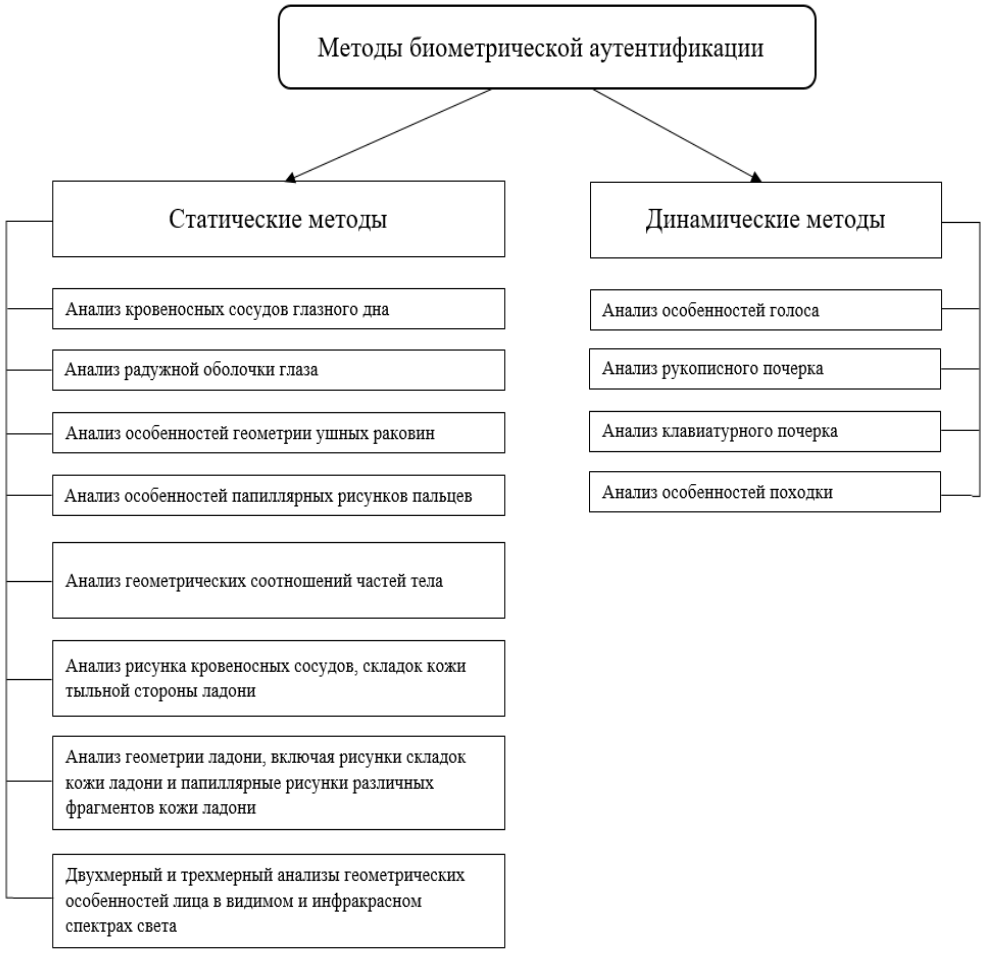


**Рис. 3. Методы биометрической аутентификация**
**Fig. 3. Biometric authentication methods**

Несомненно, у статического метода биометрической аутентификации присутствуют свои преимущества и недостатки. К положительным характеристикам статического вида стоит отнести: удобство снятия характеристик; сжатость машинных наборов высокого качества (эталонов) биометрических характеристик; для прохождения различных процедур персоналом требуется небольшое количество затрат; возможность использования систем биометрической аутентификации при больших потоках людей; психофизическое состояние человека не влияет на результат.

Недостатки статических методов: биометрические признаки открыты, поэтому существует вероятность их фальсификации; оборудование дорогостоящее, так как используются технологии высокого качества; значительное количество людей, негативно относящихся к обработке своих биометрических данных.

Индивидуальные подсознательные движения, заученные человеком, могут успешно использоваться в динамических методах аутентификации. Такие характеристики зависимы во времени. Это учитывается, когда данные измеряются, обрабатываются и хранятся. Для получения поведенческих характеристик следует проходить специальную процедуру, обусловленную динамических характером:

1. Так как характеристики зависимы от времени, то нужно проводить измерение в определенный отрезок времени.
2. Данные при измерениях могут быть разные, поэтому следует при регистрации личности проводить измерения ни один раз. Это способствует получению усредненного образа.

Как и со статическими методами обращается внимание на преимущества и недостатки.

Во-первых, низкая стоимость биометрических систем для считывания динамических характеристик говорит о том, что не обязательно использование дорогостоящего оборудования. Такие системы могут быть реализованы на клавиатуре, микрофоне, графических планшетах и т.д. Затраты при создании системы будут зависеть от разработки программного обеспечения для считывания характеристик.

Во-вторых, эталон биометрических характеристик личности хранится только у самого субъекта доступа в тайне. Дополнительно эталон возможно сменить, например, при изменении парольной фразы. Сравнивая виды методов биометрической аутентификации, статические характеристики даны человеку раз и навсегда, поэтому нет возможности их изменить или же хранить в тайне.

Говоря о недостатках динамических параметров, отметим, что работа биометрической системы зависит от психофизического состояния человека (заболевания, стрессовое состояние и т.п.). Но в некоторых случаях использование зависимости от психофизического состояние может быть использовано с пользой. К примеру, допуск людей к деятельности, где цена ошибки очень велика. Ведь отклонение психофизического состояния человека от нормы могут привести человека к неправомерным поступкам. Положительным эффектом может использоваться выявление таких людей, так как даже легальный пользователь склонен к совершению правонарушений. Чтобы достоверно оценить и сравнить использование биометрических методов аутентификации и их комбинаций, необходимо разобраться в каждом конкретном методе.

Статические методы характеризуют восемь параметров: кровеносные сосуды глазного дна; радужная оболочка глаза; двухмерная и трехмерная геометрические особенности лица в видимом и инфракрасном спектрах света; особенности геометрии ушных раковин; особенности папиллярных рисунков пальцев; геометрия ладони, включая рисунки складок кожи ладони и папиллярные рисунки различных фрагментов кожи ладони; рисунок кровеносных сосудов, складок кожи тыльной стороны ладони; соотношения частей тела в геометрии. Применять его следует исходя из зависимостей поставленных целей и задач. Учтём, что наиболее популярным остается анализ геометрии лица. Менее популярным является анализ сосудов глазного дна. Для наглядности, данные биометрической аутентификации по статическим признакам приведем в сравнительной табл. 1.

**Таблица 1. Соотношение характеристик различных методов биометрической аутентификации по статическим характеристикам**

**Table 1. The ratio of the characteristics of various methods of biometric authentication by static characteristics**

| | Сетчатка | Радужная оболочка | Геометрия лица | Геометрия ушных раковин | Отпечаток пальца | Ладонь | Тыльная сторона ладони | Геометрия соотношения частей тела |
|---|---|---|---|---|---|---|---|---|
| Неизменность характеристики | Высокая | Высокая | Средняя | Средняя | Средняя | Высокая | Высокая | Низкая |
| Чувствительность к влиянию внешних факторов | Высокая | Средняя | Средняя | Средняя | Высокая | Средняя | Средняя | Средняя |
| Скорость аутентификации | Низкая | Высокая | Высокая | Высокая | Высокая | Высокая | Высокая | Высокая |
| Комфорт пользователя | Низкий | Высокий | Высокий | Высокий | Средний | Средний | Средний | Высокий |
| Стоимость | Высокая | Высокая | Низкая | Низкая | Низкая | Средняя | Средняя | Низкая |
| Вероятность фальсификации | Невозможна | Возможна | Возможна | Возможна | Возможна | Возможна | Возможна | Возможна |

Второй метод биометрической аутентификации пользователя – динамический. К нему относят следующие параметры: клавиатурный почерк; рукописный почерк; особенности голоса; особенности походки. Неизменность характеристик для всех видов остается низкой, так как динамические методы характеризуются поведением человека при аутентификации, которое не может быть неизменным. Сравнивая динамические способы биометрической аутентификации, составим характеристику для каждого и приведем её в табл. 2.

**Таблица 2. Соотношение характеристик различных методов биометрической аутентификации по динамическим характеристикам**
**Table 2. The ratio of the characteristics of various methods of biometric authentication by dynamic characteristics**

| | Голос | Рукописный почерк | Клавиатурный почерк | Походка |
|---|---|---|---|---|
| Чувствительность к влиянию внешних факторов | Высокая | Высокая | Высокая | Высокая |
| Скорость аутентификации | Средняя | Высокая | Высокая | Высокая |
| Комфорт пользователя | Высокий | Высокий | Высокий | Высокий |
| Стоимость | Низкая | Низкая | Средняя | Высокая |
| Вероятность фальсификации | Возможна | Невозможна | Невозможна | Невозможна |

Исходя из описания методов биометрической аутентификации по динамическим характеристикам, можно сделать вывод о том, что при использовании систем аутентификации с данными технологиями стоит учитывать поставленные задачи.

Нет особого требования устанавливать дорогостоящее оборудование, если информация и доступ к ней не относятся к высоким классам защиты. К тому же использование данных методов ориентируется на программном обеспечении, которое в свою очередь может быть разработано самой компанией или организацией, где используется биометрическая аутентификация. К перспективному признаку относится клавиатурный почерк пользователя. Характеристики анализа клавиатурного почерка в биометрической аутентификации являются наиболее оптимальными для защиты информации в различных сферах деятельности человека. Если понимать, как использовать биометрическую аутентификацию в целях защиты систем от несанкционированного доступа и сохранении информации секретной, то, определенно, решение будет заключаться в подключении сразу нескольких методов. Такой выбор считается более надежным, так как для попытки фальсификации для каждого показателя в системе правонарушитель должен подделать несколько характеристик. Объединение в системе биометрической аутентификации нескольких показателей называется комбинированным решением или мультимодальным. Такое решение для систем повышает надежность защиты информации. Способы объединения представлены на рис. 4.


**Рис. 4. Способы объединения нескольких признаков для биометрической аутентификации**
**Fig. 4. Ways to combine several marks for biometric authentication**

Следует учесть критерий, когда выбор способа объединения систем в конечном итоге вынужден сводить к минимуму пропорциональность количества вероятных ошибок ко вре-

мени одной проверки подлинности. Исследования банков приводит статистику, где показывается, что использование комбинированных решений в системах биометрической аутентификации намного эффективнее одиночных. Сравнив использование технологий аутентификации по лицу, далее по голосу, а в конечном итоге скомбинировав эти методы, получили вывод об эффективности в 93%, 95%, почти 100% соответственно.

Однако использование большего количества считывателей параметров в системе не всегда приводит к лучшему результату. Это связано с появлением ошибок первого и второго рода. Ошибки первого рода выражаются, когда система принимает «своего» за «чужого». Появляется так называемый «ложный отказ». И ошибки второго рода, когда, наоборот, происходит возникновение «ложного доступа», система принимает «чужого» за «своего». Большое количество методов биометрической аутентификации может привести к частому появлению ошибок первого рода. Вероятности ложного доступа и ложного отказа представлены на рис. 5.

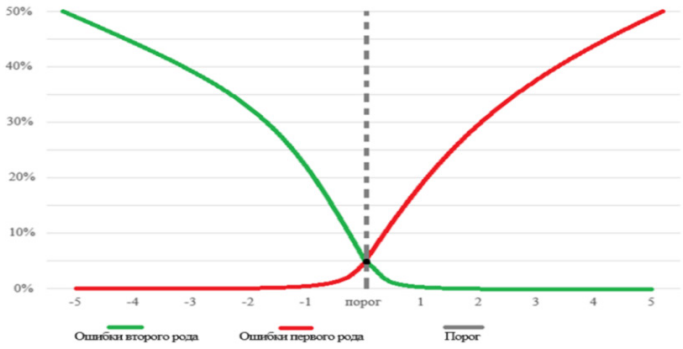


**Рис. 5. График вероятности ошибок первого рода и ошибок второго рода**
**Fig. 5. Graph of probability of errors of the first kind and errors of the second kind**

Общий процент эффективности будет снижаться при увеличении числа используемых методов. Если вероятность верного решения одного метода умножится с вероятностью другого, тогда вырастет вероятность ошибки первого рода. Существуют и многофакторные системы аутентификации, когда использование биометрии сочетается с использованием пароля или электронного ключа. Такое решение отличается меньшими затратами на считыватели биометрических характеристик.

Например, если использовать электронный ключ для доступа к информации, при этом система биометрической аутентификации будет узнавать вас по лицу, то защита информации не только будет более защищена, но и вероятность ошибок снизится.

По данным исследований больше пользователей выбирают двухфакторную аутентификацию по принципу «пароль + клавиатурный почерк» (рис. 6).


**Рис. 6. Диаграмма, характеризующая предпочтения пользователей в биометрии**
**Fig. 6. Diagram describing user preferences in biometrics**

Стоит согласиться с мнением большинства. Низкая стоимость биометрической системы, при этом ее высокие надежность, скорость и комфорт составляют значительное

доверие. При этом пароль, составленный пользователем, позволяет иметь доступ только правомерному субъекту доступа. Использование такого метода очень удобно, поскольку он позволяет сократить время аутентификации до времени обычного ввода парольной фразы, при этом система скрытно определит, что точно ли легитимный пользователь вводит пароль и выведет решение о правомерности доступа к информации.

**Вывод.** Таким образом, исходя из целей систем безопасности, в которые включены технологии биометрической аутентификации, мы полагаем, что необходимо усложнить возможность несанкционированного доступа к информации. Вместе с тем, совершенствование системы не должно ухудшать комфорт легитимного пользователя при попытке доступа. Остаются задачи уменьшения времени входа и упрощения системы.

Если поставленные задачи решены, то система биометрической аутентификации будет иметь лучшие показатели для субъектов доступа. Учтем и то, что с совершенствованием технологий для защиты информации, появляются и технологии для совершения атак злоумышленниками. Поэтому решение при использовании систем биометрической аутентификации должно включать реагирование на попытку взлома.

Исследование всех параметров, на которые стоит всмотреться, показывает, что оптимальным решением в разработке систем биометрической аутентификации будет использование многофакторной аутентификацией с использованием динамических параметров субъекта доступа. Поведенческие характеристики человека практически невозможно фальсифицировать, при этом низкая стоимость оборудования по сравнению с оборудованием для считывания статических характеристик выделяет в лучшую сторону метод динамической биометрии. К тому же вероятность ошибок по сравнению с комбинированными решениями ниже. Также комбинированные решения требуют больше времени для считывания биометрических характеристик человека, а это усложняет систему.

Пользователям, компаниям и организациям сложно сделать однозначный вывод о том, какое решение для систем биометрической аутентификации использовать для контроля доступа к информации из расчета соотношения цены и качества. Высокая стоимость комбинированных решений, слабая стойкость к фальсификации систем аутентификации по одному биометрическому показателю заставляют задуматься о выборе. Стоит учитывать какую информацию необходимо защищать. Иногда защищаемая информация требует самой сложной защиты, и тогда отпадает вопрос о затратах на необходимое оборудование.

Современную систему биометрической аутентификации следует устанавливать с учетом требуемого на данный момент уровня безопасности. К тому же, не стоит забывать о включении новых методов в будущем. Ведь прогресс не стоит на месте, и развитие биометрии как в мире, так и в России показывает на появление вероятности использования своего образа для подтверждения своей же личности. Возможно в скором времени нам больше не нужно использовать ключи, паспорта, водительские удостоверения, карты.

**Библиографический список:**

1. Об информации, информационных технологиях и о защите информации. Федеральный закон от 27.07.2006г., №149-Ф [Электронный ресурс]. Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_61798/
2. О персональных данных. Федеральный закон от 27.07.2006 г. № 152-ФЗ / [Электронный ресурс]. Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_61801/
3. Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации. Федеральный закон от 29.12.2022 г. № 572-ФЗ / [Электронный ресурс]. Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_436110/
4. Об утверждении Положения о единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица. Постановление Правительства Р от 16 июня 2022 г. № 1089 / [Электрон.ресурс]. Режим доступа: https://www.garant.ru/products/ipo/prime/doc/404747823/
5. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения // М.: Федеральное

агентство по техническому регулированию и метрологии. 2008. – 7 с / [Электронный ресурс]. Режим доступа: https://docs.cntd.ru/document/1200058320

6. ГОСТ Р 52633.0-2006. Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации. 2007. – 19с / [Электронный ресурс]. Режим доступа: https://docs.cntd.ru/document/1200048922
7. ГОСТ Р 52633.1–2009. Защита информации. Техника защиты информации. Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации. 2010. – 19с / [Электронный ресурс]. Режим доступа: https://docs.cntd.ru/document/1200079555
8. ГОСТ Р 52633.2–2010. Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации. 2018. – 18с / [Электронный ресурс]. Режим доступа: https://docs.cntd.ru/document/1200081163
9. ГОСТ Р 52633.3–2011. Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора. 2018. – 11с / [Электронный ресурс]. Режим доступа: https://docs.cntd.ru/document/1200088765
10. ГОСТ Р ИСО/МЭК 19795-1–2007. Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура. 2019. – 50с / [Электронный ресурс]. Режим доступа: https://docs.cntd.ru/document/1200067413
11. ГОСТ Р ИСО/МЭК 19795-2–2008. Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 2. Методы проведения технологического и сценарного испытаний. 2009. – 42с / [Электронный ресурс]. Режим доступа: https://docs.cntd.ru/document/1200073050
12. ГОСТ Р ИСО/МЭК ТО 19795-3–2009. Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 3. Особенности проведения испытаний при различных биометрических модальностях. 2010. – 23с / [Электронный ресурс]. Режим доступа: https://docs.cntd.ru/document/1200075111
13. ГОСТ Р ИСО/МЭК 19795-4–2011. Информационные технологии. Биометрия. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 4. Испытания на совместимость. 2012. – 49с / [Электронный ресурс]. Режим доступа: https://docs.cntd.ru/document/1200087807
14. ГОСТ Р ИСО/МЭК 19795-6–2015. Информационные технологии. Биометрия. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 6. Методология проведения оперативных испытаний. 2016. –27с / [Электронный ресурс]. Режим доступа: https://docs.cntd.ru/document/1200122961
15. ФСТЭК РФ. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения.
16. Брюхомицкий Ю.А. Биометрические технологии идентификации личности; Южный федеральный университет. – Ростов-на-Дону : Издательство Южного федерального университета, 2017. – 263 с.
17. Иванов А. И. Нейросетевые алгоритмы биометрической идентификации личности М. : Радиотехника, 2004. – 143 с.
18. Мартынова Л. Е. Исследование и сравнительный анализ методов аутентификации.// Молодой ученый. – 2016. – № 19. – С. 90–93.
19. Биометрические системы / Журнал для руководителей и специалистов в области безопасности Secutek // Системы безопасности – 2019. – №2. – С. 126.
20. Фэйспасс. Журнал для руководителей и специалистов в области безопасности Secutek // Системы безопасности – 2022. – №3. – С. 134.
21. Размещение биометрии в единой биометрической системе (ЕБС) / Журнал «Информационная безопасность» // Информационная безопасность itsec – 2022. – №4. – С. 56.

**References**

1. On Information, Information Technologies and Information Protection Federal law No 149-FL dated 27.07.2006/ [Electron. Res.] Access mode: https://www.consultant.ru/document/cons_doc_LAW_61798/ (In Russ).
2. On Personal Data Federal law No 152-FL dated 27.07.2006 / [Electronic resource]. Access mode: https://www.consultant.ru/document/cons_doc_LAW_61801/(In Russ).
3. On the Identification and (or) Authentication of Individuals Using Biometric Personal Data, on Amendments to Certain Legislative Acts of the Russian Federation and Invalidation of Certain Provisions of Legislative Acts of the Russian Federation. Federal Law No 572-FL dated 29.12.2022 / [Electronic resource]. Access mode: https://www.consultant.ru/document/cons_doc_LAW_436110/ (In Russ).
4. On Approval of the Regulations on the Unified Personal Data Information System that Ensures the Processing, including Collection and Storage, of Biometric Personal Data, their Verification and Transmission of information on the Degree of their Compliance with the Provided Biometric Personal data of an Individual.

Decree of the Government of the Russian Federation No 1089 dated 16.06.2022 / [Electronic resource]. Access mode: https://www.garant.ru/products/ipo/prime/doc/404747823/ (In Russ).
5. GOST R 50922-2006. Information protection. Basic terms and definitions // Moscow: Federal Agency for Technical Regulation and Metrology. 2008;7./[Electronic resource].Access mode: https://docs.cntd.ru/document/1200058320 (In Russ).
6. GOST R 52633.0-2006. Information protection. Information security techniques. Requirements for highly reliable biometric authentication tools. 2007;19/[Electronic resource].Access mode: https://docs.cntd.ru/document/1200048922 (In Russ).
7. GOST R 52633.1–2009. Information protection. Information security techniques. Requirements for the formation of databases of natural biometric images intended for testing highly reliable biometric authentication tools. 2010; 19. [Electron. Res.]. Access mode: https://docs.cntd.ru/document/1200079555 (In Russ).
8. GOST R 52633.2–2010. Information protection. Information security techniques. Requirements for the formation of synthetic biometric images intended for testing highly reliable biometric authentication tools. 2018; 18. / [Electronic resource]. Access mode: https://docs.cntd.ru/document/1200081163 (In Russ).
9. GOST R 52633.3–2011. Information protection. Information security techniques. Testing the resistance of highly reliable biometric protection tools to selection attacks. 2018; 11. / [Electronic resource]. Access mode: https://docs.cntd.ru/document/1200088765 (In Russ).
10. GOST R ISO/IEC 19795-1-2007. Automatic identification. Biometric identification. Operational tests and test reports in biometrics. Part 1. Principles and structure. 2019; 50. / [Electronic resource]. Access mode: https://docs.cntd.ru/document/1200067413 (In Russ).
11. GOST R ISO/IEC 19795-2-2008. Automatic identification. Biometric identification. Operational tests and test reports in biometrics. Part 2. Methods of technological and scenario testing. 2009; 42. / [Electronic resource]. Access mode: https://docs.cntd.ru/document/1200073050 (In Russ).
12. GOST R ISO/IEC TO 19795-3-2009. Automatic identification. Biometric identification. Operational tests and test reports in biometrics. Part 3. Features of testing with various biometric modalities. 2010; 23. / [Electronic resource]. Access mode: https://docs.cntd.ru/document/1200075111 (In Russ).
13. GOST R ISO/IEC 19795-4-2011. Information technology. Biometrics. Operational tests and test reports in biometrics. Part 4.Compatibility tests. 2012;49./[Electronic resource].Access mode: https://docs.cntd.ru/document/1200087807 (In Russ).
14. GOST R ISO/IEC 19795-6-2015. Information technology. Biometrics. Operational tests and test reports in biometrics. Part 6. Methodology of operational tests. 2016; 27[Electronic resource]. Access mode: https://docs.cntd.ru/document/1200122961 (In Russ).
15. FSTEC of the Russian Federation. Guidance document. Protection against unauthorized access to information. Terms and definitions. (In Russ).
16. Bryukhomitsky Y.A. Biometric technologies of identity identification; Southern Federal University. Rostov-on-Don : Southern Federal University Press, 2017; 263. (In Russ).
17. Ivanov A. I. Neural network algorithms of biometric identification of personality. Moscow: Radio Engineering, 2004; 143. (In Russ).
18. Martynova L. E. Research and comparative analysis of authentication methods. *Young Scientist*. 2016;19: 90-93. (In Russ).
19. Biometric systems / Journal for managers and security specialists Secutek. *Security systems*. 2019; 2:126. (In Russ).
20. Facepass. *Journal for managers and security specialists Secutek*. *Security systems*. 2022; 3: 134. (In Russ).
21. Placement of biometrics in the unified biometric system (UBS). *Journal "Information Security"* Information security itsec 2022;4: 56. (In Russ).

**Сведения об авторах:**

Власов Константин Николаевич, командир отделения; vlasikko@yandex.ru

Толстых Ольга Владимировна, кандидат технических наук, доцент кафедры радиотехнических систем и комплексов охранного мониторинга; tov48@mail.ru

Исаев Олег Викторович, кандидат технических наук, доцент, старший преподаватель кафедры технических комплексов охраны и связи; olegisaev71@mail.ru

**Information about authors:**

Konstantin N. Vlasov, Section Commander; vlasikko@gmail.com

Olga V. Tolstykh, Cand. Sci. (Eng), Assoc Prof., Department of Radio Engineering Systems and Security Monitoring Complexes; tov48@mail.ru

Oleg V. Isaev, Cand. Sci. (Eng), Assoc Prof., Senior teacher of the Department of technical complexes of safety and communication; olegisaev71@mail.ru

**Конфликт интересов/Conflict of interest.**

**Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.**

**Поступила в редакцию/Received** 06.06.2023.

**Одобрена после рецензирования/ Reviced** 12.07.2023.

**Принята в печать/Accepted for publication** 12.07.2023.