АБИСС

Регуляторика биометрических технологий

Информационные партнеры

АИС
АКАДЕМИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

Листок
Бюрократической
Защиты
Информации

Биометрия и нормативная база: Поиск ответов

Алексей Лазарев,

Руководитель департамента защиты киберфизических систем,
Компания «Актив»

О чем поговорим?

01 Аутентификация и идентификация: проблема трактовки определений. Нужны ли универсальные базовые формулировки?

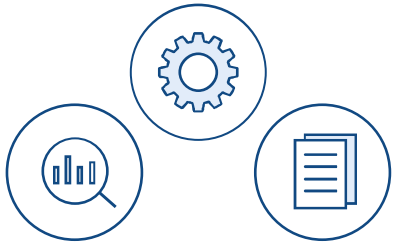
02 Биометрический фактор:
можно ли его использовать как единственный?

03 Биометрический модальности: что выбрать?

04 Биометрическое распознавание и установление личности: ищем подводные камни.

ГОСТ Р 58833-2020

Идентификация



Действия по присвоению субъектам и объектам доступа идентификаторов и/или по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Авторизация

Проверка, подтверждение и предоставление прав логического доступа при осуществлении субъектами доступа логического доступа

ГОСТ Р 58833-2020

Аутентификация

Действия по проверке подлинности субъекта доступа и/или объекта доступа,
а также по проверке принадлежности субъекту доступа и/или объекту доступа предъявленного идентификатора доступа
и аутентификационной информации

Верификация

Процесс проверки информации путём сопоставления предоставленной информации с ранее подтвержденной информацией

Применительно к биометрии

- **Биометрическая идентификация** — преобразование совокупности примеров биометрических образов человека, позволяющее описать их стационарную и случайную составляющие, например, в виде математического ожидания и дисперсий контролируемых параметров или, например, в виде параметров обученной сети искусственных нейронов. **(ГОСТ Р 52633.0—2006)**

- **Биометрическая идентификация** — процесс поиска по базе данных биометрических регистраций, направленный на поиск и возврат идентификатора(ов) биометрического контрольного шаблона, связанного с одним индивидом. **(ГОСТ ISO-IEC 2382-37-2016)**

- **Идентификация** — функция биометрической системы, которая выполняет поиск «один ко многим» для получения списка кандидатов. **(ГОСТ Р ИСО/МЭК 19794-1-2015)**

- **Биометрическая аутентификация** — аутентификация пользователя, осуществляемая путем предъявления им своего биометрического образа. **(ГОСТ Р 52633.0—2006)**

Применительно к биометрии

- **Аутентификация** — действие, доказывающее или показывающее бесспорное происхождение или достоверность. **(ГОСТ ISO/IEC 2382-37—2016)**

- **Верификация** — функция биометрической системы, выполняющая сравнение запросного образца с указанным шаблоном, хранящимся в системе, в режиме «один к одному» и возвращающая результат в виде индекса совпадения или решения о совпадении. **(ГОСТ ISO/IEC 24713-1— 2013)**

- **Биометрическая верификация** — процесс подтверждения биометрического заявления при сравнении. **(ГОСТ ISO/IEC 2382-37—2016)**

- **Биометрическое распознавание** — автоматическое распознавание индивидов, основанное на их поведенческих и биологических характеристиках. Биометрическое распознавание включает в себя биометрическую верификацию и биометрическую идентификацию. Использование термина «аутентификация» в качестве синонима термина «биометрическая верификация» или термина «биометрическая идентификация» неприемлемо. Предпочтительнее использование термина «биометрическое распознавание». **(ГОСТ ISO/IEC 2382-37—2016)**

Как трактует законодательство?

- **Идентификатор** - уникальное обозначение сведений о лице, необходимое для определения такого лица.

- **Идентификация** - совокупность мероприятий по **установлению сведений** о лице и их **проверке**, осуществляемых в соответствии с федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами, и **сопоставлению данных сведений с идентификатором**.

- **Аутентификация** - совокупность мероприятий **по проверке лица на принадлежность ему идентификаторов** посредством сопоставления их со сведениями о лице, которыми располагает лицо, проводящее аутентификацию, и **установлению правомерности владения** лицом идентификаторами посредством использования аутентифицирующих признаков в рамках процедуры аутентификации, в результате чего лицо считается установленным.

Биометрический фактор

01

6.5…

- биометрический фактор: субъекту доступа должен быть свойственен определенный признак (характеристика), информация о котором (которой) используется при аутентификации.

02

6.7

Биометрический фактор должен использоваться **только совместно с другими факторами**, в том числе для подтверждения фактора владения. При этом применение биометрического фактора в качестве единственного фактора при однофакторной аутентификации не допускается.

Критерии отбора модальностей для биометрической идентификации

- Проведены исследования, подтверждающие эффективность
- Методика описана в стандарте

~FAR	0,1%	0,0008%	0,001%	0,1%	1%
~FRR	2,5%	0,01%	0,6%	1%	4%

ГОСТ Р ИСО/МЭК 19794-5-2013

ЕБС

ГОСТ Р 58668.8-2019
ИСО/МЭК 19794-9:2011

ГОСТ Р ИСО/МЭК 19794-2-2013

ГОСТ Р 58298-2018
ИСО/МЭК 19794-4:2011

ГОСТ Р 58668.11–2019
ИСО/МЭК 19794-13:2018)

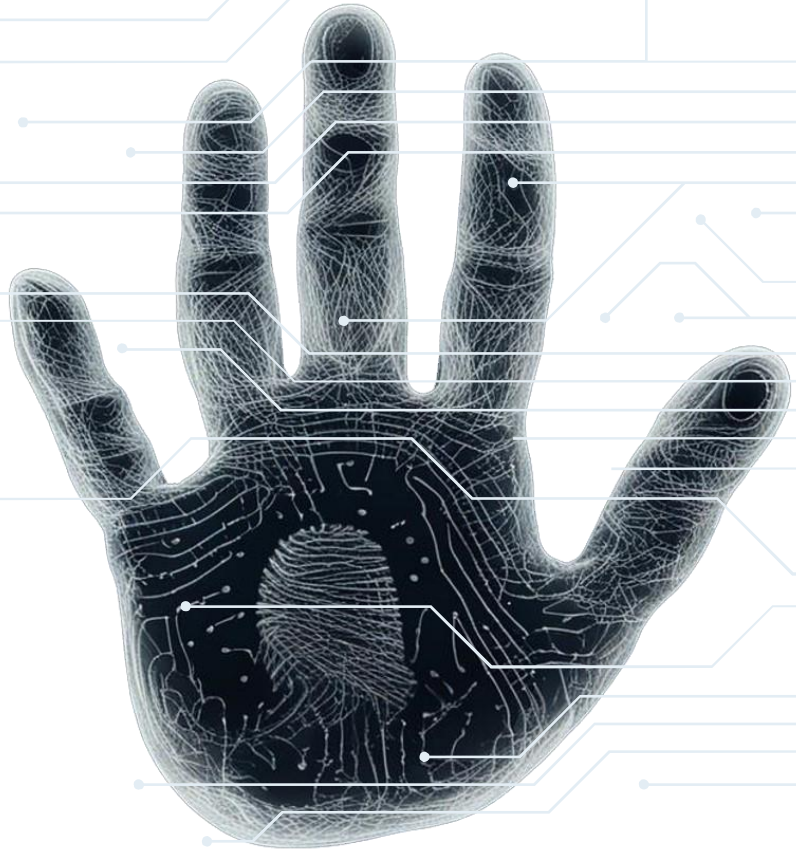
ЕБС

Перспективная модальность — новые возможности

- Быстро
- Скрытно (ИК – камера)
- Бесконтактно
- Высокая степень индивидуальности = хороший FAR/FRR
- Сложно подменить
- ГОСТ Р ИСО/МЭК 19794-9-2015

  ГОСТ Р 58668.8-2019 (ИСО/МЭК 19794-9:2011)

  ГОСТ Р ИСО/МЭК 29109-9-2017



Биометрические персональные данные

- **Биометрические персональные данные** — это «сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно **установить его личность** и которые используются оператором для **установления личности** субъекта персональных данных

(152 ФЗ)

- В ЕБС размещаются и обрабатываются биометрические персональные данные следующих видов:
1) **изображение лица человека**, полученное с помощью фотовидеоустройств;
2) **запись голоса человека**, полученная с помощью звукозаписывающих устройств.

(572 ФЗ)

Установление личности= определение субъекта?

Установление личности - **процедура**, которая должно соблюдаться при совершении правовых действий в отношении субъекта;

Установление личности гражданина будет осуществляться нотариусом на основании получения им с использованием единой информационной системы нотариата:
- информации о результатах проверки соответствия **представленных биометрических персональных данных физического лица его биометрическим персональным данным, содержащимся в единой биометрической системе**, а также информации о степени взаимного соответствия указанных биометрических персональных данных, достаточной для проведения идентификации;
- сведений о гражданине РФ, содержащихся в единой системе идентификации и аутентификации:
  - фамилии, имени, отчества (при наличии),
  - даты рождения,
  - адреса места жительства (регистрации),
  - реквизитов основного документа, удостоверяющего личность,
  - страхового номера индивидуального лицевого счёта.

Приказ Минюста России от 30.09.2020 № 228

Биометрия и нормативная база: Поиск ответов

LAZAREV@rutoken.ru
info@rutoken.ru

www.abiss.ru
www.aktiv.consulting

+7 495 925-77-90
+7 905 729-34-26

Алексей Лазарев,

Руководитель департамента защиты киберфизических систем,
Компания «Актив»

RTM GROUP

Типовые ошибки
При защите биометрии

Кобец Дмитрий,

Заместитель директора технического департамента RTM Group

Нормативные нарушения

01 Нет периодической оценки по ГОСТ

02 Нет периодической оценки защиты ПДн

03 Персонал не знает порядок защиты

Сетевое взаимодействие

Отсутствие сетевой изоляции сегмента	АРМ сбора «воткнут» в общий неуправляемый коммутатор
Сетевая изоляция «глухая»	Нет доступа к корпоративным СЗИ
Отсутствие СЗИ в сегменте	Сегмент и так полностью изолирован и достаточно защищён. При этом реальная причина — сегмент изолирован и СЗИ там пользоваться не удобно.

Применение СЗИ

01 Отсутствие актуальных обновлений (см. предыдущий пункт)

02 Локальные СЗИ без централизованного управления

Игнорирование способов утечек

Размещение мест сбора в общем зале	Отсутствие шумоизоляции помещений сбора	Возможности доступа третьих лиц в места сбора	Работа из-под одной неперсонифицированной УЗ

RTM GROUP

Типовые ошибки при защите биометрии

info@rtmtech.ru

https://rtmtech.ru

+7 (495) 197-64-95

Кобец Дмитрий,

Заместитель директора технического департамента RTM Group

Спасибо за внимание!

АБИСС