ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 58624.1— 2019 (ИСО/МЭК 30107-1:2016)

Информационные технологии

БИОМЕТРИЯ

Обнаружение атаки на биометрическое предъявление

Часть 1

Структура

(ISO/IEC 30107-1:2016, Information technology — Biometric presentation attack detection — Part 1: Framework, MOD)

Издание официальное

Москва
Стандартинформ
2019

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Акционерным обществом «Всероссийский научно-исследовательский институт сертификации» (АО «ВНИИС») и Некоммерческим партнерством «Русское общество содействия развитию биометрических технологий, систем и коммуникаций» (Некоммерческое партнерство «Русское биометрическое общество») на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4, при консультативной поддержке Федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)» (МГТУ им. Н.Э. Баумана)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 098 «Биометрия и биомониторинг»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 31 октября 2019 г. № 850-ст

4 Настоящий стандарт является модифицированным по отношению к международному стандарту ИСО/МЭК 30107-1:2016 «Информационные технологии. Обнаружение атаки на биометрическое предъявление. Часть 1. Структура» (ISO/IEC 30107-1:2016 «Information technology — Biometric presentation attack detection — Part 1: Framework», MOD) путем изменения отдельных фраз (слов, значений показателей, ссылок), которые выделены в тексте курсивом. Внесение указанных технических отклонений направлено на учет потребностей национальной экономики Российской Федерации.

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5—2012 (пункт 3.5).

Сведения о соответствии ссылочных межгосударственных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте, приведены в дополнительном приложении ДА.

Сопоставление структуры настоящего стандарта со структурой примененного в нем международного стандарта приведено в дополнительном приложении ДБ

5 ВВЕДЕН ВПЕРВЫЕ

6 Некоторые элементы настоящего стандарта могут быть объектами патентных прав. Международная организация по стандартизации (ИСО) и Международная электротехническая комиссия (МЭК) не несут ответственности за установление подлинности каких-либо или всех таких патентных прав

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© ISO, 2016 — Все права сохраняются
© Стандартинформ, оформление, 2019

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Обозначения и сокращения 3
5 Атаки на биометрическое предъявление 3
5.1 Общие положения 3
5.2 Инструменты атаки на биометрическое предъявление 3
6 Структура методов обнаружения атаки на биометрическое предъявление 4
6.1 Типы методов обнаружения атаки на биометрическое предъявление 4
6.2 Метод «запрос-ответ» 5
6.3 Процесс обнаружения атаки на биометрическое предъявление 6
6.4 Подсистема обнаружения атаки на биометрическое предъявление в структуре биометрической системы 7
7 Противодействие атакам самозванца на биометрическое предъявление в биометрической системе 9
Приложение ДА (справочное) Сведения о соответствии ссылочных межгосударственных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте 10
Приложение ДБ (справочное) Сопоставление структуры настоящего стандарта со структурой примененного в нем международного стандарта 10
Библиография 11

Введение

Биометрические технологии часто используются в системах безопасности для распознавания индивидов на основе их биологических и поведенческих характеристик. С помощью биометрических систем безопасности могут совершаться попытки распознавания субъектов сбора биометрических данных, субъектов — нарушителей сбора биометрических данных или субъектов, биометрические данные которых отсутствуют в системе.

С самого начала применения биометрических технологий отмечалась возможность взлома распознавания со стороны субъектов — нарушителей сбора биометрических данных, а также необходимость принятия мер для обнаружения и пресечения попыток взлома распознавания или атак на биометрическое предъявление. Область применения серии национальных стандартов *«Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление»* ограничена методами автоматического обнаружения атак на биометрическое предъявление, осуществляемыми субъектами сбора биометрических данных в процессе биометрического предъявления и сбора соответствующих биометрических характеристик. Данные автоматические методы называются методами обнаружения атаки на биометрическое предъявление (ОАБП).

Вероятность взлома биометрических систем в процессе сбора данных индивидами, имитирующими субъектов сбора биометрических данных, ограничила возможность использования биометрии в приложениях, которые не контролируются оператором биометрической системы, например такие, как удаленный сбор биометрических данных с использованием ненадежных сетей. В автономных приложениях, например таких, как удаленная аутентификация с использованием открытых сетей, для снижения риска атак могут применяться методы автоматического обнаружения атак на биометрическое предъявление. Применение стандартов, рекомендации и методы независимой оценки могут повысить безопасность биометрических систем, включая биометрические системы распознавания, обеспечивающие безопасность онлайн-транзакций, вне зависимости от того, контролируется ли процесс сбора биометрических данных оператором или нет.

Как и методы биометрического распознавания, методы ОАБП подвержены ложноположительным и ложноотрицательным результатам. В случае ложноположительного результата система ошибочно классифицирует надлежащее биометрическое предъявление как атаку, тем самым снижая эффективность системы, а в случае ложноотрицательного результата система ошибочно классифицирует атаку на биометрическое предъявление как надлежащее биометрическое предъявление, в результате чего происходит нарушение безопасности. Поэтому решение об использовании биометрической системой конкретного метода ОАБП будет зависеть от ее применения и компромисса между уровнями безопасности и эффективности.

Настоящий стандарт устанавливает термины и структуру ОАБП с целью обнаружения, классификации и детального описания атак на биометрическое предъявление для последующего принятия решения о сравнении и определения эксплуатационных характеристик системы. Однако метод ОАБП, определенный в настоящем стандарте, не представляется в качестве общепринятого.

В *ГОСТ Р 58624.2 (ИСО/МЭК 30107-2:2017)* установлены требования к формату обмена данными и результатами работы методов ОАБП. В *ГОСТ Р 58624.3 (ИСО/МЭК 30107-3:2017)* определены принципы и методы оценки эффективности работы методов ОАБП.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

БИОМЕТРИЯ

Обнаружение атаки на биометрическое предъявление

Часть 1

Структура

Information technology. Biometrics. Biometric presentation attack detection. Part 1. Framework

Дата введения — 2020—06—01

1 Область применения

Настоящий стандарт устанавливает термины и определения, используемые для описания, а также структуру методов обнаружения атак на биометрическое предъявление (ОАБП) с целью обнаружения, классификации и детального описания атак на биометрическое предъявление для последующего принятия решения о сравнении и определения эксплуатационных характеристик системы.

В область применения настоящего стандарта не входят:

- стандартизация конкретных методов ОАБП;
- подробная информация о мерах предотвращения атак (то есть методах защиты от спуфинга), алгоритмах или биометрических сканерах;
- комплексная оценка безопасности или уязвимости на системном уровне.

Атаки, рассмотренные в серии национальных стандартов *«Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление»*, направлены на биометрический сканер во время биометрического предъявления и сбора биометрических данных.

Настоящий стандарт не распространяется на другие типы атак.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ ISO/IEC 2382-37 Информационные технологии. Словарь. Часть 37. Биометрия

ГОСТ ISO/IEC 19794-1 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 1. Структура

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую ссылку этого стандарта с учетом всех внесенных в данную версию изменений. Если изменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

Издание официальное

3 Термины и определения

В настоящем стандарте применены термины по *ГОСТ ISO/IEC 2382-37* и *ГОСТ ISO/IEC 19794-1*, а также следующие термины с соответствующими определениями:

3.1 **артефакт** (artefact)**:** Искусственный объект или представление с копией биометрических характеристик или синтезированными биометрическими данными.

3.2

витальность (liveness): Свойство или состояние живого индивида, подтверждаемое анатомическими характеристиками, непроизвольными реакциями, физиологическими функциями, произвольными реакциями или поведенческими характеристиками индивида.

[1], [2].

Примеры

1 Поглощение света кожей и кровью является анатомическими характеристиками частей тела.

2 Реакция радужной оболочки глаза на свет и пульсирование кровотока являются непроизвольными реакциями (называемыми также физиологическими функциями).

3 Сжимание пальцев рук при идентификации по геометрии контура кисти руки и биометрическое предъявление в ответ на прямую команду являются произвольными реакциями (называемыми также поведенческими характеристиками субъекта).

3.3

обнаружение витальности (liveness detection): Измерение и анализ анатомических характеристик, непроизвольных или произвольных реакций индивида с целью определения того, что биометрический образец получен от живого индивида.

[1], [2]

Примечание — Обнаружение витальности входит в число методов ОАБП.

3.4 **надлежащее биометрическое предъявление** (normal presentation): Взаимодействие субъекта сбора биометрических данных и подсистемы сбора биометрических данных в соответствии с политикой биометрической системы.

Примечание — Термин «надлежащий» аналогичен термину «стандартный», когда речь идет о «надлежащем биометрическом предъявлении». Любое биометрическое предъявление, не являющееся атакой, считается «надлежащим биометрическим предъявлением».

3.5 **атака на биометрическое предъявление** (presentation attack): Биометрическое предъявление подсистеме сбора биометрических данных с целью вмешательства в работу биометрической системы.

Примечания

1 Атака на биометрическое предъявление может быть реализована множеством методов, например путем использования артефакта, повреждения, воспроизведения и так далее.

2 Атаки на биометрическое предъявление могут иметь ряд целей, например имитация или не распознавание биометрической системой.

3 Биометрические системы не могут отличить атаку на биометрическое предъявление с целью вмешательства в работу системы и ненадлежащее биометрическое предъявление.

3.6 **обнаружение атаки на биометрическое предъявление;** ОАБП (presentation attack detection; PAD): Автоматическое обнаружение атаки на биометрическое предъявление.

Примечание — ОАБП не позволяет определить намерения субъекта. Попытка обнаружить атаку в процессе сбора биометрических данных или в полученном биометрическом образце может оказаться невозможной.

3.7 **инструмент атаки на биометрическое предъявление;** ИАБП (presentation attack instrument; PAI): Биометрическая характеристика или объект, используемые для атаки на биометрическое предъявление.

Примечание — Помимо артефактов ИАБП включает в себя биометрические характеристики, полученные от мертвого индивида, и измененные биометрические характеристики (например, измененные отпечатки пальцев), которые используются для атаки.

4 Обозначения и сокращения

В настоящем стандарте использованы следующие обозначения и сокращения:
ОАБП — обнаружение атаки на биометрическое предъявление;
ИАБП — инструмент атаки на биометрическое предъявление.

5 Атаки на биометрическое предъявление

5.1 Общие положения

Атаки на биометрическую систему могут осуществляться любым субъектом в любой точке биометрической системы. Настоящий стандарт посвящен биометрическим атакам на подсистему сбора биометрических данных субъектами сбора биометрических данных, пытающимися вмешаться в работу биометрической системы. Атаки, проводимые другими субъектами и в других точках системы, в настоящем стандарте не рассмотрены. В настоящем стандарте не определены методы защиты подсистемы сбора биометрических данных, включая биометрический сканер, от модификации, замены или извлечения, а также методы защиты каналов связи между подсистемой сбора биометрических данных и другими подсистемами.

Атаки на биометрическое предъявление могут выполняться двумя типами субъектов — нарушителей сбора биометрических данных: самозванцем, то есть субъектом — нарушителем сбора биометрических данных, который намеревается быть распознанным как другой индивид, или укрывателем личности, который намеревается избежать совпадения с любым биометрическим контрольным шаблоном, хранящимся в биометрической системе.

Самозванцы могут совершать атаки двумя разными способами. В первом случае субъект-нарушитель намеревается быть распознанным как определенный индивид, известный биометрической системе. Во втором случае субъект-нарушитель пытается быть распознан как любой индивид, известный биометрической системе.

Укрыватель личности, наоборот, будет пытаться скрыть свои собственные биометрические характеристики путем подделки биометрических характеристик, известных биометрической системе субъектов, например с использованием артефакта или с помощью маскировки или изменения собственных биометрических характеристик.

5.2 Инструменты атаки на биометрическое предъявление

Объектом или характеристикой, используемой для атаки на биометрическое предъявление, является ИАБП. Атаки на биометрический сканер с использованием ИАБП делятся на две категории: искусственно созданные или на основе человеческих характеристик. Существует третья категория ИАБП — на основе животных или растений.

В настоящем разделе, и в частности в таблице 1, используются термины «совместимый» и «несовместимый», но они не влияют на кодирование ОАБП, поскольку их значение связано с взаимодействием субъекта и биометрического сканера, которое трудно объективно измерить и которое, следовательно, не может быть закодировано. Примером такого несовместимого взаимодействия является размещение пальца боковой поверхностью на рабочей поверхности биометрического сканера отпечатков пальцев вместо подушечки пальца.

Обнаруженная атака может быть вызвана проблемами общедоступности или удобства использования биометрического сканера, а не попыткой атаковать биометрическую систему.

На рисунке 1 показаны категории ИАБП и соответствующие им типы.

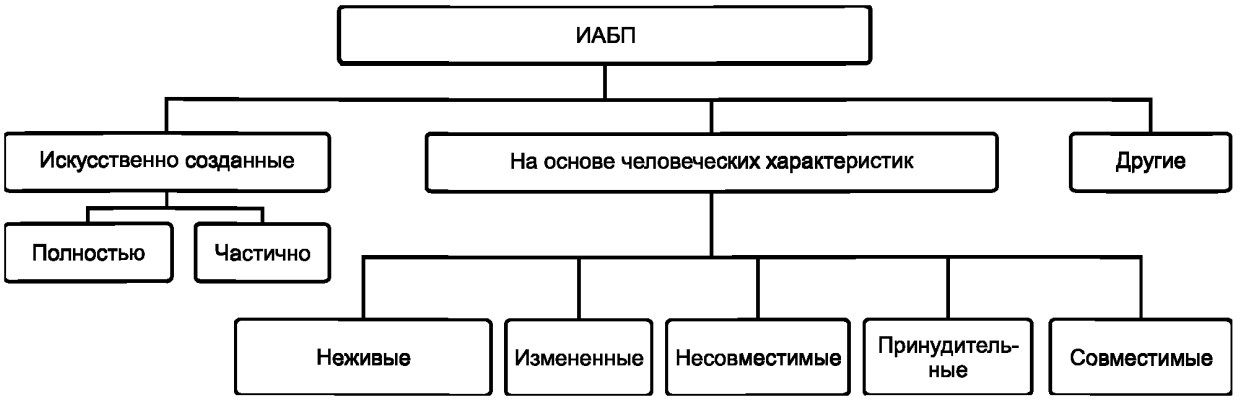


Рисунок 1 — Типы атак на биометрическое предъявление

В таблице 1 приведены примеры каждого конкретного типа ИАБП, представленного на рисунке 1 на третьем уровне. С помощью прилагательного из второй графы таблицы 1, за которым следует слово из первой графы таблицы 1, можно описать конкретный ИАБП. Например, Часть тела, полученная от трупа, является примером «неживого ИАБП на основе человеческих характеристик».

Таблица 1 — Примеры искусственно созданных ИАБП и ИАБП на основе человеческих характеристик

Искусственно созданные ИАБП	Полностью	Желатиновый поддельный палец, видеозапись лица
	Частично	Нанесение клея на палец, солнцезащитные очки, маскирующие контактные линзы, макияж
ИАБП на основе человеческих характеристик	Неживые	Часть трупа, отрезанный палец или рука
	Измененные	Нанесение увечий, операция по пересадке участков кожи между пальцами рук и/или пальцами ног
	Несовместимые	Изменение выражения лица/проведение пластических операций лица, размещение пальца на рабочей поверхности биометрического сканера отпечатков пальцев кончиком или боковой стороной
	Принудительные[a]	Субъект в бессознательном состоянии, принуждение субъекта к выполнению необходимых действий
	Совместимые	Попытка самозванца без затрачивания усилий

[a] Предполагается, что невозможно обнаружить все случаи принудительного биометрического предъявления. Некоторые модальности позволяют определять показатели принуждения, такие как напряжение в голосе, высокая частота пульса или выражение эмоции на лице (страх).

6 Структура методов обнаружения атаки на биометрическое предъявление

6.1 Типы методов обнаружения атаки на биометрическое предъявление

Как показано в таблице 2, методы ОАБП делятся на две категории: методы на основе данных, полученных с помощью подсистемы сбора биометрических данных, и методы на основе мер обеспечения безопасности на системном уровне. Не существует взаимно-однозначного соответствия между методами ОАБП и типами ИАБП (см. рисунок 2).

Таблица 2 — Примеры методов ОАБП

Обнаружение атак через подсистему сбора биометрических данных	Обнаружение артефактов	Обнаружение характерных особенностей, указывающих на использование артефакта. Например, электрическое сопротивление пальца на биометрическом сканере находится за пределами типичного диапазона; изображения поверхностного и подкожного отпечатков пальца существенно отличаются
	Обнаружение витальности	Определение приведено в 3.3. Примеры приведены в 6.2.1 и 6.2.2
	Обнаружение изменений	Обнаружение характерных особенностей, указывающих на попытки изменения биометрического признака. Например, определение наличия шрама на отпечатке пальца
	Обнаружение несоответствия	Обнаружение отклонений, которые не должны наблюдаться при надлежащем биометрическом предъявлении. Например, обнаружение несоответствия уровня освещенности нормальным условиям эксплуатации
	Обнаружение принуждения	Например, анализ напряжения в голосе или наличие эмоций
	Обнаружение искажений	Обнаружение того, что биометрические признаки были частично или полностью скрыты. Например, обнаружение аксессуара (шарфа или шляпы), закрывающего часть лица
Обнаружение атак на системном уровне	Счетчик обнаружения неудачных попыток	Например, обнаружение последовательности однотипных неудачных попыток
	Определение места атаки	Например, обнаружение местоположения или времени биометрического предъявления, недопустимого или нехарактерного для субъекта сравнения
	Определение времени атаки	
	Видеонаблюдение	Например, обнаружение атаки оператором (человеком или системой видеоаналитики)

6.2 Метод «запрос-ответ»

Метод обнаружения атак «запрос-ответ» широко используется в системах распознавания, основанных как на биометрических, так и на небиометрических характеристиках. В настоящем подразделе представлена структура метода обнаружения атаки «запрос-ответ» общего вида, а также реализация данного метода для обнаружения атак на биометрические системы и для определения живого индивида.

В данном контексте под запросом подразумевается целенаправленное действие, которое приводит к ожидаемому ответу при наличии целевого условия.

6.2.1 Обнаружение витальности с использованием метода «запрос-ответ»

Метод «запрос-ответ» может использоваться для определения того, получено ли биометрическое предъявление субъекта от живого субъекта сбора биометрических данных. Например, ожидается, что изменения в интенсивности видимого света (запрос) приведут к изменениям размера зрачка (ожидаемый ответ в случае предъявления радужной оболочки глаза живого человека).

В таблице 3 представлена структура всех компонентов метода «запрос-ответ» для обнаружения витальности биометрического образца. Метод, представленный в последней графе таблицы 3, в отличие от двух других методов не может использоваться при первом взаимодействии субъекта с биометрической системой или для обнаружения витальности во время процесса биометрической регистрации.

Таблица 3 — Обнаружение витальности с использованием метода «запрос-ответ»

Метод	Непроизвольные реакции	Произвольные реакции	Сочетание того, что знает субъект, и того, что является частью субъекта
Запрос	Целенаправленный импульс, предназначенный для известных биометрических характеристик	Подсказки (звуковые, визуальные и т. д.), направленные на выполнение конкретного действия, результат которого должен быть получен биометрической системой	Указания по биометрическому предъявлению с использованием ранее зарегистрированной информации
Ответ	Естественные, непроизвольные реакции, не контролируемые субъектом	Реакции, основанные на восприятии субъекта, и произвольные реакции, контролируемые субъектом	Реакции, основанные на восприятии субъекта и биометрической регистрации индивида
Примеры	Изменение размера зрачка в зависимости от изменения интенсивности света	Изменение угла наклона головы в ответ на просьбу повернуть голову. Окклюзия радужной оболочки левого глаза в ответ на просьбу закрыть левый глаз	Порядок пальцев (выбранный случайным образом системой) определяет правильный порядок процесса биометрического предъявления и сравнения пальцев. Порядок цифр определяет правильный порядок произнесения и сравнения цифр

6.2.2 Обнаружение витальности без использования метода «запрос-ответ»

Обнаружение витальности без использования метода «запрос-ответ» называется проверкой посредством невключенного наблюдения за витальностью (или «пассивным» обнаружением витальности). В этом случае обнаружение витальности проводится на основе данных, полученных биометрическим сканером за определенный период времени без использования целенаправленного импульса. Примеры методов пассивного обнаружения витальности:

- потоотделение пальцев (за определенное время),
- малые движения радужной оболочки глаза/частота движений (за короткое время),
- измерение пульса (за определенное время),
- мультиспектральное освещение (анализ коэффициентов поглощения света кровью или кожей).

6.2.3 Метод «запрос-ответ» для небиометрического распознавания

Некоторые методы аутентификации, не основанные на биометрических характеристиках индивида, используют метод «запрос-ответ» для повышения уровня безопасности системы, как правило, с помощью многофакторной аутентификации (без использования биометрических характеристик для распознавания). В этом случае запрос может представлять собой попытку аутентификации устройства или идентификационной карты на основе цифровых сертификатов или запроса ответа на контрольный вопрос (секретный).

6.3 Процесс обнаружения атаки на биометрическое предъявление

Процесс ОАБП может быть представлен в виде этапов, аналогичных этапам процесса биометрического распознавания:

1) сбор необработанных данных субъекта подсистемой сбора биометрических данных для ОАБП;

Примечание — Устройства сбора данных ОАБП могут отличаться от биометрических сканеров, а сбор биометрических данных и данных ОАБП может расходиться во времени, что может привести к уязвимости системы.

2) извлечение признаков из данных ОАБП;

3) сравнение полученных признаков ОАБП с установленными критериями;

4) возвращение результата сравнения (обнаруженная атака, отсутствие атаки, оценка и т. д.). Эти данные отдельно или в сочетании с другими данными будут учитываться при принятии окончательного решения биометрической системы о принятии или отклонении биометрического образца.

Этапы процесса ОАБП должны выполняться в приведенном выше порядке, но они не обязательно должны быть непрерывными во времени и пространстве.

Критерии принятия решения, используемые на третьем этапе процесса ОАБП, могут быть общими для всех субъектов или индивидуальными для каждого субъекта. Например, для обнаружения атаки на биометрическое предъявление на основе непроизвольных реакций, физиологических функций, произвольных реакций или поведенческих характеристик субъекта могут использоваться критерии ОАБП, общие для всех субъектов, в случае невысокой точности их измерения. При использовании критериев ОАБП, измеренных с высокой точностью, они могут быть индивидуальными для каждого субъекта.

Следовательно, процесс регистрации критериев необходим в тех случаях, когда они являются индивидуальными для каждого субъекта.

6.4 Подсистема обнаружения атаки на биометрическое предъявление в структуре биометрической системы

6.4.1 Подсистема обнаружения атаки на биометрическое предъявление в структуре биометрической системы общего вида

Хотя в область применения настоящего стандарта входят только атаки в точке сбора биометрических данных, процесс ОАБП может быть выполнен в любой точке системы и в любом процессе, выполняемом системой.

На рисунке 2 показана одна из возможных реализаций подсистемы ОАБП в структуре биометрической системы общего вида. Существует несколько способов включения подсистемы ОАБП (и ее отдельных процессов) в структуру биометрической системы общего вида. Процесс обнаружения атаки на биометрическое предъявление может быть выполнен после (или во время) процесса сбора биометрических данных и/или после процесса обработки сигнала, как показано пунктирными линиями на рисунке 2. Процесс ОАБП может также быть выполнен после работы подсистемы сравнения или подсистемы принятия решений (данная реализация не показана на рисунке 2) или в нескольких точках системы. Кроме того, в системе может быть реализовано аппаратное, временное или функциональное распараллеливание процесса сбора биометрических данных с целью распознавания личности и процесса обнаружения атаки на биометрическое предъявление. В 6.4.2 и 6.4.3 представлены дополнительные сведения о возможных реализациях процесса ОАБП в различных точках биометрической системы.

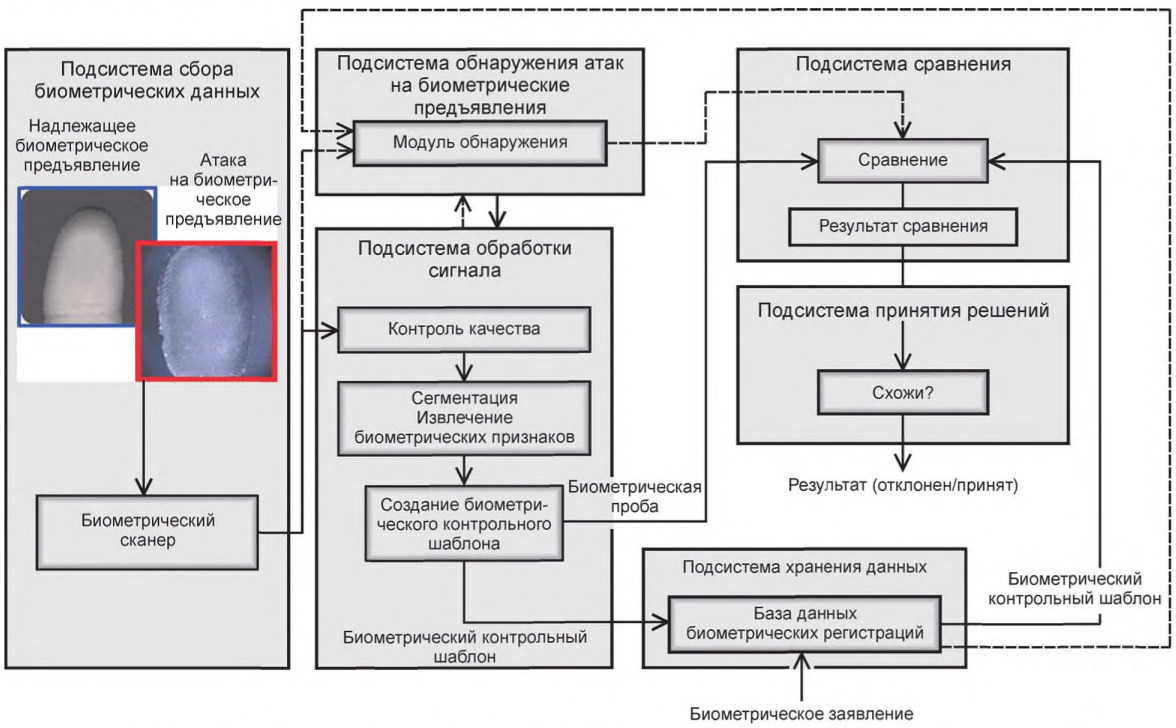


Рисунок 2 — Структура биометрической системы общего вида с подсистемой обнаружения атак на биометрическое предъявление

На рисунке 3 приведены дополнительные сведения о компонентах подсистемы ОАБП. В некоторых реализациях подсистемы ОАБП может не быть блока извлечения признаков ОАБП, но блок сравнения ОАБП и хранимые критерии ОАБП являются обязательными компонентами подсистемы. Критерии ОАБП могут быть общими для всех субъектов или индивидуальными для каждого субъекта.

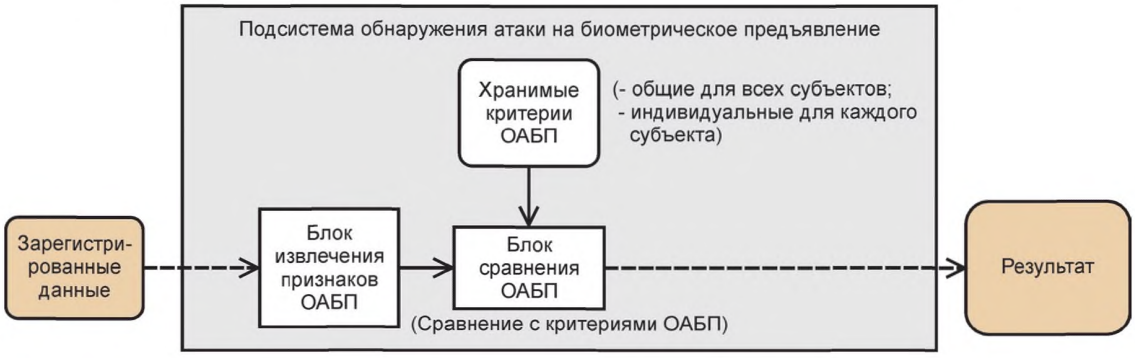


Рисунок 3 — Компоненты подсистемы обнаружения атак на биометрическое предъявление общего вида

6.4.2 Обработка данных ОАБП относительно других биометрических подсистем

Сбор и обработку данных ОАБП и данных биометрического образца следует разделять во времени и пространстве. Оба типа данных могут существовать одновременно или существовать в отсутствие другого. Процесс ОАБП может выполняться биометрической системой одновременно, до или после процесса работы любой из ее подсистем. Компоненты подсистемы ОАБП могут быть реализованы в качестве отдельной подсистемы, между процессами работы нескольких подсистем и/или одновременно с ними. Результат ОАБП может зависеть от множества полученных биометрических образцов и не обязательно является простым двоичным индикатором.

Примеры

1 Биометрический сканер может создавать данные биометрического образца и данные ОАБП для каждого события сбора данных. В зависимости от конструкции биометрической системы биометрический сканер может выводить данные биометрического образца независимо от результата процесса ОАБП или только в том случае, если подсистема ОАБП не обнаружила атаки. При создании данных ОАБП без получения биометрического образца результатом ОАБП будет являться простой двоичный индикатор обнаруженной атаки.

2 Полученные данные ОАБП могут быть проанализированы в процессе обработки сигнала после получения биометрического образца. В этом случае биометрический образец, биометрические признаки или биометрическая модель, полученные из подсистемы обработки сигнала, могут сопровождаться показателем ОАБП, определенным в процессе обработки сигнала.

3 Процесс сбора данных ОАБП и процесс их анализа могут разделяться во времени. В этом случае сигнал запуска обработки данных ОАБП хранится с биометрическим образцом, биометрическими признаками или биометрической моделью.

Примечание — Так как система не всегда может контролировать процесс сбора данных в режиме реального времени, видеонаблюдение и аналогичные способы записи могут стать эффективным механизмом обнаружения атаки и анализа процесса(ов) биометрического предъявления и условий биометрического предъявления, как, например, обнаружения кражи средств из автоматических кассовых машин с использованием незаконно созданных дубликатов карт. Это могло бы повысить эффективность используемого метода обнаружения атаки (успешного или нет) или принуждения субъекта. Данный механизм позволяет получить дополнительные биометрические образцы для ретроспективного анализа (например, изображения лица, полученные с кадров видеонаблюдения за автоматическими кассовыми машинами, доступ к которым осуществляется с помощью отпечатка пальца), что могло бы усилить фактор сдерживания атак на такие системы. Описанные решения используются в настоящее время для предотвращения и обнаружения ненадлежащего использования систем и могут применяться в качестве рекомендаций при реализации биометрических систем.

6.4.3 Влияние реализации ОАБП на обмен данными

Компоненты подсистемы ОАБП могут быть реализованы в различных точках системы (клиентской или серверной части системы, интерфейсной или прикладной части, мобильном устройстве или в

программном обеспечении приложения/облаке). Продукты, поддерживающие ОАБП, могут представлять собой различные устройства и быть реализованы в различных точках системы.

Ниже приведены возможные подходы к ОАБП, некоторые из которых не связаны с процессом обмена данными (или не зависят от него).

Процесс ОАБП может выполняться на биометрическом сканере. При использовании устройства, имеющего достаточную вычислительную мощность для выполнения процесса ОАБП, может не требоваться передача результата ОАБП из устройства (например, передача на компьютер базы данных, сервер или приложение). Вывод данных биометрического образца или предоставление прав доступа (или невыполнение указанных действий) может быть достаточным показателем результата процесса ОАБП.

С другой стороны, даже если все компоненты подсистемы ОАБП реализованы в биометрическом сканере, приложения с уязвимостями высокой степени риска могут направить запрос на получение информации о взаимодействии с биометрическим сканером, данных о неудавшихся попытках и надежности биометрического образца на основании доступных данных ОАБП (например, необработанных данных или оценок).

Данные ОАБП могут быть получены доверенным устройством и переданы на сервер или в приложение (запущенное программное обеспечение, созданное другим разработчиком) с целью принятия решения по утверждению личности и правах доступа. В зависимости от приложения данные ОАБП, включенные в процесс обмена данными, могут представлять собой необработанные данные, передаваемые в том виде, в котором они были получены, или показатели и данные, извлеченные локальным устройством из биометрического образца.

7 Противодействие атакам самозванца на биометрическое предъявление в биометрической системе

Для проведения успешной атаки самозванца на биометрическое предъявление в биометрической системе:

I) биометрический образец для проведения атаки на биометрическое предъявление должен быть получен подсистемой сбора биометрических данных;

II) биометрический образец для проведения атаки на биометрическое предъявление должен быть успешно обработан для получения биометрического шаблона или биометрической пробы;

III) решение о сравнении биометрической пробы или биометрического шаблона, полученных в процессе атаки на биометрическое предъявление, и биометрического контрольного шаблона должно быть положительным;

IV) проведение атаки должно быть реализовано при соблюдении мер безопасности на системном уровне;

V) подсистема ОАБП, при ее наличии в системе, не должна классифицировать предъявленный биометрический образец как попытку атаки.

Атака на биометрическое предъявление может быть предотвращена на любом из этих этапов в зависимости от типа биометрической системы и сложности атаки. Например (в соответствии с порядком этапов проведения атаки, представленным выше):

I) может быть получен отказ в биометрической регистрации артефакта благодаря особенностям конструкции биометрического сканера и свойств, которые он контролирует при получении биометрических образцов, например при предъявлении силиконового поддельного отпечатка пальца емкостному сканеру отпечатков пальцев;

II) подсистема обработки сигнала может отклонить биометрический образец, полученный с использованием артефакта, ввиду неудовлетворительного качества;

III) результат сравнения может не превышать установленный порог принятия решений ввиду использования для сравнения печатной копии истинного биометрического образца низкого качества;

IV) предъявление головы манекена в натуральную величину, вероятно, будет замечено оператором системы.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных межгосударственных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте

Таблица ДА.1

Обозначение ссылочного межгосударственного стандарта	Степень соответствия	Обозначение и наименование ссылочного международного стандарта
ГОСТ ISO/IEC 2382-37—2016	IDT	ISO/IEC 2382-37:2017 «Информационные технологии. Словарь. Часть 37. Биометрия»
ГОСТ ISO/IEC 19794-1—2015	IDT	ISO/IEC 19794-1:2011 «Информационные технологии. Форматы обмена биометрическими данными. Часть 1. Структура»
Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов: - IDT — идентичные стандарты.		

Приложение ДБ
(справочное)

Сопоставление структуры настоящего стандарта со структурой примененного в нем международного стандарта

Таблица ДБ.1

Структура настоящего стандарта	Структура международного стандарта ИСО/МЭК 30107-1:2016
Приложение ДА Сведения о соответствии ссылочных межгосударственных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте	—
Приложение ДБ Сопоставление структуры настоящего стандарта со структурой примененного в нем международного стандарта	—
Примечание — Сопоставление структуры стандартов приведено начиная с приложения ДА, так как предыдущие разделы стандартов идентичны.	

Библиография

[1] Костылев *Н.М.*, Горевой *А.В. Модуль обнаружения витальности лица по спектральным характеристикам отражения кожи человека // Инженерный журнал: Наука и инновации — 2013. — Вып. 9. — http://engjournal.ru/catalog/pribor/optica/925.html*

[2] *Калиновский И.А., Лаврентьева Г.М. Обнаружение спуфинг-атак на систему лицевой биометрии // Computer Vision. — 2018. — С. 204—207, — http://*gost.e-ecolog.ru

УДК 004.93'1:006.354

ОКС 35.240.15;
01.080.50

Ключевые слова: информационные технологии, биометрия, обнаружение атаки, биометрическое предъявление, структура

БЗ 11—2019/74

Редактор *Н.А. Аргунова*
Технический редактор *И.Е. Черепкова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 05.11.2019. Подписано в печать 21.11.2019. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 1,86. Уч.-изд. л. 1,68.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru