ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 58624.3— 2019 (ИСО/МЭК 30107-3:2017)

Информационные технологии

БИОМЕТРИЯ

Обнаружение атаки на биометрическое предъявление

Часть 3

Испытания и протоколы испытаний

(ISO/IEC 30107-3:2017, Information technology — Biometric presentation attack detection — Part 3: Testing and reporting, 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 20 ноября 2019 г. № 1197-ст

4 Настоящий стандарт является модифицированным по отношению к международному стандарту ИСО/МЭК 30107-3:2017 «Информационные технологии. Обнаружение атаки на биометрическое предъявление. Часть 3. Испытания и протоколы испытаний» (ISO/IEC 30107-3:2017 «Information technology — Biometric presentation attack detection — Part 3: Testing and reporting», 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 национальных и 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, 2017 — 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
3.1 Элементы атаки . . . 2
3.2 Метрики . . . 3
4 Сокращения . . . 4
5 Соответствие . . . 5
6 Общие положения обнаружения атаки на биометрическое предъявление . . . 5
7 Уровни оценки методов обнаружения атаки на биометрическое предъявление . . . 6
7.1 Общие положения . . . 6
7.2 Общие принципы оценки методов обнаружения атаки на биометрическое предъявление . . . 6
7.3 Оценка подсистемы обнаружения атаки на биометрическое предъявление . . . 7
7.4 Оценка подсистемы сбора биометрических данных . . . 7
7.5 Оценка полнокомплектной биометрической системы . . . 8
8 Свойства артефактов . . . 8
8.1 Свойства инструментов атаки на биометрическое предъявление при атаках самозванца . . . 8
8.2 Свойства инструментов атаки на биометрическое предъявление при атаках укрывателя личности . . . 10
8.3 Свойства синтезированных биометрических образцов с нестандартными характеристиками . . . 10
9 Аспекты несогласованных попыток сбора биометрических характеристик . . . 11
9.1 Методы биометрического предъявления . . . 11
9.2 Методы оценки . . . 11
10 Создание и использование артефактов при оценке методов обнаружения атаки на биометрическое предъявление . . . 11
10.1 Общие положения . . . 11
10.2 Создание и подготовка артефактов . . . 11
10.3 Использование артефактов . . . 12
10.4 Итерационные испытания по определению эффективных артефактов . . . 13
11 Факторы оценки различных процессов . . . 13
11.1 Общие положения . . . 13
11.2 Оценка процесса биометрической регистрации . . . 13
11.3 Оценка процесса биометрической верификации . . . 14
11.4 Оценка процесса биометрической идентификации . . . 14
11.5 Оценка методов обнаружения атаки на биометрическое предъявление в автономном режиме . . . 14
12 Метрики оценки биометрических систем с методами обнаружения атак на биометрическое предъявление . . . 15
12.1 Общие положения . . . 15
12.2 Метрики оценки подсистемы обнаружения атаки на биометрическое предъявление . . . 15

12.3 Метрики оценки подсистем сбора биометрических данных 17
12.4 Метрики оценки полнокомплектных биометрических систем 18
Приложение А (справочное) Классификация типов атак. 20
Приложение В (справочное) Примеры видов артефактов, используемых в оценке подсистем обнаружения атаки на биометрическое предъявление для биометрических сканеров отпечатков пальцев 24
Приложение ДА (справочное) Сведения о соответствии ссылочных национальных и межгосударственных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте 25
Приложение ДБ (справочное) Сопоставление структуры настоящего стандарта со структурой примененного в нем международного стандарта 26
Библиография 27

Введение

Предъявление артефакта или биометрической характеристики индивида подсистеме сбора биометрических данных с целью нарушения намеченной политики биометрической системы называется атакой на биометрическое предъявление. *Область применения серии стандартов ГОСТ Р 58624 ограничена методами автоматического обнаружения атак на биометрическое предъявление, осуществляемыми субъектами сбора биометрических данных в процессе биометрического предъявления и сбора соответствующих биометрических характеристик.* Данные методы называются методами обнаружения атаки на биометрическое предъявление (ОАБП).

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 уровнем безопасности и эффективности.

Настоящий стандарт устанавливает:

- термины, относящиеся к испытаниям ОАБП и протоколам испытаний;
- принципы и методы оценки эксплуатационных характеристик методов ОАБП, включая метрики.

Настоящий стандарт предназначен для разработчиков методов ОАБП и/или для испытательных лабораторий, планирующих проводить оценки эффективности методов ОАБП.

Терминология и методы эксплуатационных испытаний, а также методология статистического анализа в биометрии регламентированы *в серии стандартов ГОСТ Р ИСО/МЭК 19795-1—2007.* В качестве эксплуатационных характеристик биометрических систем используются такие метрики, как вероятность ложного допуска, ВЛД*, вероятность ложного недопуска, ВЛНД** и вероятность отказа биометрической регистрации, ВОБР***. Терминология и методы эксплуатационных испытаний, а также методология статистического анализа в биометрии лишь частично применимы к оценке методов ОАБП ввиду значительных фундаментальных различий между концепцией эксплуатационных испытаний в биометрии и концепцией испытаний методов ОАБП. Фундаментальные различия заключаются в следующем:

а) статистическая значимость.

В биометрических эксплуатационных испытаниях применяют статистически значимое количество субъектов, представляющих целевую группу пользователей. Вероятности ошибок не будут значительно отличаться при существенном увеличении числа участников или привлечении другой группы субъектов. Как правило, при проведении большего числа измерений увеличивается точность вероятностей ошибок.

В испытаниях ОАБП многие биометрические модальности могут подвергаться атакам большого или неопределенного числа видов потенциальных инструментов атаки на биометрическое предъявление (ИАБП). В таких случаях сложно или даже невозможно построить исчерпывающую модель всех возможных ИАБП. Следовательно, невозможно найти репрезентативный набор видов ИАБП для оценки, поэтому измеренные вероятности ошибок одного набора ИАБП не могут считаться применимыми к другому набору.

Виды ИАБП представляют собой источник систематических изменений в испытаниях. Различные ИАБП могут иметь значимо различные вероятности ошибок. Кроме того, в пределах любого вида ИАБП будут наблюдаться случайные различия между экземплярами серии ИАБП. Число биометрических предъявлений, необходимых для статистически значимых испытаний, будет линейно масштабироваться с учетом числа видов ИАБП. В пределах каждого вида ИАБП неопределенность, связанная с оценкой вероятности ошибок ИАБП, будет зависеть от числа испытуемых артефактов и числа индивидов.

Пример — В дактилоскопии известно много потенциальных материалов для создания артефактов, и при атаке возможно использование любого из этих материалов или сочетания материалов, с помощью которых можно предъявить характеристики отпечатка пальца биометрическому сканеру. Поскольку такие свойства артефакта, как продолжительность эксплуатации, толщина, влажность,

* false accept rate, FAR.

** false reject rate, FRR.

*** failure-to-enrol rate, FTE.

температура, скорость смешивания и технология производства, могут оказать значительное влияние на результат метода ОАБП, легко определить десятки тысяч видов ИАБП с использованием существующих материалов. Для корректного статистического анализа потребуются сотни тысяч биометрических предъявлений, и даже в этом случае вероятности ошибок не могут быть перенесены на следующий набор новых материалов;

b) сравнимость результатов испытаний по всем системам.

В эксплуатационных испытаниях биометрических систем для сравнения различных биометрических систем или разных конфигураций могут быть использованы вероятности ошибок, рассчитанные на основе одной и той же выборки биометрических образцов на конкретном приложении. Общепринятыми являются понятия «лучше» и «хуже».

В то же время при использовании вероятностей ошибок для сравнения методов ОАБП такой термин, как «лучше», может в значительной степени зависеть от конкретного приложения.

Пример — В сценарии испытаний с 10 видами ИАБП (представляемых 100 раз) система 1 обнаруживает 90 % предъявлений атаки, а система 2 — 85 %. Система 1 фиксирует все предъявления девяти видов ИАБП, но не все предъявления 10-го вида ИАБП. Система 2 обнаруживает 85 % всех видов ИАБП. Какая система лучше? С точки зрения безопасности система 1 хуже, чем система 2, так как обнаружение уязвимости 10-го вида ИАБП сориентирует злоумышленника постоянно использовать этот метод для обмана устройства сбора биометрических данных. Однако если злоумышленники лишены возможности применять 10-й вид ИАБП, то система 1 будет лучше, чем система 2, поскольку отдельные вероятности ошибок показывают, что можно обмануть систему 2 всеми видами ИАБП;

c) согласованность.

Многие эксплуатационные испытания биометрических систем относятся к приложениям, когда поведение субъектов является согласованным, например при контроле доступа. Ошибки вследствие неправильной работы являются скорее следствием нехватки знаний, опыта или руководства, а не намерения. Несогласованность поведения значительной части группы не является частью соответствующей «биометрической модели» и сделает вероятности ошибок практически бесполезными для эксплуатационных испытаний биометрических систем.

Испытания ОАБП включают субъекты, поведение которых не является согласованным. Злоумышленники попытаются найти и использовать любую уязвимость биометрической системы, обходя или воздействуя на ее предполагаемое функционирование. Типы атак на биометрическое предъявление, определяемые опытом и знаниями экспериментатора, могут значительно изменить вероятностные характеристики успешности атак. Следовательно, сложно определить процедуры испытания, которые измеряют вероятности ошибок в виде, характеризующем согласованное поведение;

d) автоматические испытания.

В эксплуатационных испытаниях биометрических систем часто возможны испытания алгоритмов сравнения с использованием баз данных с устройств или датчиков похожего качества. Производительность может быть измерена в технологических испытаниях с использованием ранее собранной выборки образцов в соответствии с *ГОСТ Р ИСО/МЭК 19795-1*.

При испытаниях ОАБП может быть недостаточно данных биометрического сканера (например, цифровых изображений отпечатков пальцев). Биометрические системы с методами ОАБП часто содержат дополнительные датчики для обнаружения специфических свойств биометрической характеристики. Следовательно, база данных, собранная ранее для конкретной биометрической системы или конфигурации, может не подходить для другой биометрической системы или конфигурации. Даже незначительные изменения в оборудовании или программном обеспечении могут сделать предыдущие измерения непригодными. Нецелесообразно хранить многовариантные синхронизированные сигналы ОАБП и воспроизводить их в автоматических испытаниях, поэтому в автоматическом режиме часто испытания не задействованы при проведении испытаний и оценке методов ОАБП;

e) качество и производительность.

В эксплуатационных испытаниях биометрических систем производительность, как правило, напрямую зависит от качества биометрических данных. Использование образцов низкого качества приводит к высоким вероятностям ошибок, а применение образцов высокого качества — к снижению вероятностей ошибок. Следовательно, показатели качества часто используются при повышении эксплуатационных характеристик (в зависимости от приложения).

Несмотря на то что при испытаниях ОАБП низкое качество биометрических данных может привести к неудовлетворительному результату артефакта, основания предполагать определенный уровень качества артефактов отсутствуют. Образцы артефактов могут демонстрировать качество лучшее, чем образцы биометрических характеристик человека. При отсутствии модели навыка злоумышленника корректным (по крайней мере, в оценке безопасности) будет предполагать сценарий «наихудшего случая», когда злоумышленник всегда использует наилучшее возможное качество. В этом случае можно определить гарантированную минимальную вероятность обнаружения для конкретного набора испытаний, уменьшая при этом число необходимых испытаний. Затем проводят балльную оценку потенциала нападения успешных артефактов (усилия и опыт для необходимого качества).

На основе различий, приведенных в перечислениях а)—е), могут быть сделаны следующие общие примечания относительно вероятностей ошибок и метрик, относящихся к методам ОАБП:

- виды ОАБП должны быть проанализированы и оценены по отдельности;
- вероятность ошибок классификации предъявлений атаки, отличная от 0 %, демонстрирует только то, что ОАБП может быть успешным. Другой экспериментатор может обеспечить более высокую или более низкую вероятность ошибок классификации предъявлений атаки. Кроме того, обучение определению соответствующих материалов и параметров предъявления может повысить вероятность ошибки классификации предъявления атаки для этого вида ИАБП. Опыт и знания экспериментатора, а также наличие необходимых ресурсов являются важными факторами при проведении испытаний ОАБП и учитываются в процессе сравнения или анализа производительности;
- вероятности ошибок для методов ОАБП определены конкретным контекстом метода ОАБП, набором видов ИАБП, приложением, методом испытаний и экспериментатором. Вероятности ошибок для методов ОАБП не обязательно как сопоставимы с аналогичными испытаниями, так и воспроизводимы в разных испытательных лабораториях.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

БИОМЕТРИЯ

Обнаружение атаки на биометрическое предъявление

Часть 3

Испытания и протоколы испытаний

Information technology. Biometrics. Biometric presentation attack detection.
Part 3. Testing and reporting

Дата введения — 2020—06—01

1 Область применения

Настоящий стандарт определяет:

- принципы и методы оценки эксплуатационных характеристик методов ОАБП;
- протоколы результатов испытаний методов ОАБП;
- классификацию известных типов атак (см. приложение А).

Настоящий стандарт не определяет:

- конкретные методы ОАБП;
- детальную информацию о методах противодействия (то есть о методах защиты от спуфинга), алгоритмах или датчиках;
- общую оценку безопасности или уязвимости биометрической системы.

Атаки, рассмотренные в серии стандартов ГОСТ Р 58624, 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

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 58624.1—2019 (ИСО/МЭК 30107-1:2016) Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. 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,

Издание официальное

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.

3 Термины и определения

В настоящем стандарте применены термины по *ГОСТ ISO/IEC 2382-37, ГОСТ ISO/IEC 19794-1* и *ГОСТ Р (ИСО/МЭК 30107-1:2016)*, а также следующие термины с соответствующими определениями:

3.1 Элементы атаки

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

Примечание — Предъявление атаки может быть одной попыткой, транзакцией с несколькими попытками или другим типом взаимодействия с подсистемой сбора биометрических данных.

3.1.2 **подлинное биометрическое предъявление** (bona fide presentation): Взаимодействие субъекта сбора биометрических данных и подсистемы сбора биометрических данных в соответствии с политикой биометрической системы.

Примечания

1 В отношении биометрического предъявления «подлинное» соответствует «нормальному» или «обычному».

2 Подлинные биометрические предъявления могут включать те, в которых пользователь имеет низкий уровень подготовки или навыков. Подлинные биометрические предъявления включают множество достоверных предъявлений для подсистемы сбора биометрических данных.

3.1.3 **тип атаки** (attack type): Элементы и свойства атаки на биометрическое предъявление, в том числе вид инструментов атаки на биометрическое предъявление, атака укрывателя или самозванца, степень контроля и способ взаимодействия с биометрическим сканером.

3.1.4 **подход к испытаниям** (test approach): Совокупность принципов и факторов, учитываемых в оценке обнаружения атаки на биометрическое предъявление.

Примечания

1 Элементы подхода к испытаниям представлены в разделах от 7 до 11.

2 Подход к испытаниям относится ко всем процессам, факторам и аспектам, учитываемым в ходе проведения оценки.

3.1.5 **объект испытания; ОИ** (item under test; IUT): Реализация, являющаяся объектом утверждения испытаний или контрольным примером.

Примечание — Термин «объект испытания/ОИ» является эквивалентом термина «ОО/объект оценки» (TOE/target of evaluation) *в серии стандартов ГОСТ Р ИСО/МЭК 15408.*

3.1.6 **вид инструментов атаки на биометрическое предъявление** (PAI species): Класс инструментов атаки на биометрическое предъявление, созданных одинаковым методом производства и использующих разные биометрические характеристики.

Примеры

1 Видом ИАБП является набор поддельных отпечатков пальцев, изготовленных одинаковым способом из одинаковых материалов, но с разными узорами папиллярных гребней.

2 Видом ИАБП является определенный тип изменений, вносимых в отпечатки пальцев нескольких субъектов сбора биометрических данных.

Примечания

1 Для обозначения того, как сделать вид ИАБП, часто используют термин «инструкция».

2 Инструменты атаки на биометрическое предъявление одного вида могут иметь разные вероятности успешных попыток ввиду изменчивости производственного процесса.

3.1.7 **комплект инструментов атаки на биометрическое предъявление** (PAI series): Инструменты атаки на биометрическое предъявление, созданные одинаковым способом производства в одинаковых условиях и использующие один источник биометрических характеристик.

Пример — Набор поддельных отпечатков пальцев, изготовленных одинаковым способом из одинаковых материалов с одинаковыми узорами папиллярных линий.

Примечание — В зависимости от целей испытаний в оценке могут быть использованы комплекты ИАБП из одного или нескольких источников. Несмотря на то что испытания с комплектами из нескольких источников биометрических данных могут демонстрировать общность вида ИАБП, может наблюдаться изменчивость, связанная с индивидуальными характеристиками человека.

3.1.8 **объект оценки;** ОО (target of evaluation, TOE): Продукт информационных технологий*, являющийся предметом оценки.

Примечание — Термин «объект оценки/ОО» является эквивалентом термина «ОИ/объект испытания» (IUT/item under test) *в серии стандартов ГОСТ Р ИСО/МЭК 15408*.

3.1.9 **потенциал нападения** (attack potential): Мера возможности атаковать объект оценки с учетом знаний, профессиональных навыков, ресурсов и мотивации злоумышленника.

3.2 Метрики

3.2.1 **вероятность ошибки классификации предъявления при атаке;** ВОКПА (attack presentation classification error rate, APCER): Доля предъявлений при атаке одним видом инструментов атаки на биометрическое предъявление, которые некорректно классифицируют как подлинные биометрические предъявления в конкретном сценарии.

3.2.2 **вероятность ошибки классификации подлинных биометрических предъявлений;** ВОКПБП (bona fide presentation classification error rate, BPCER): Доля подлинных биометрических предъявлений, которые некорректно классифицируют как предъявления атаки в конкретном сценарии.

3.2.3 **вероятность отсутствия ответа на предъявление артефакта;** ВООПА (attack presentation non-response rate, APNRR): Доля предъявлений артефакта одного вида инструментов атаки на биометрическое предъявление, которые вызывают отсутствие ответа со стороны подсистемы ОАБП или подсистемы сбора биометрических данных.

Пример — Биометрическая система отпечатков пальцев может не проводить регистрацию или не реагировать на предъявление атаки ввиду недостаточной реалистичности ИАБП.

3.2.4 **вероятность отсутствия ответа на подлинное биометрическое предъявление;** ВООПБП (bona fide presentation non-response rate, BPNRR): Доля подлинных биометрических предъявлений, которые вызывают отсутствие ответа со стороны подсистемы обнаружения атаки на биометрическое предъявление или подсистемы сбора биометрических данных.

3.2.5 **вероятность получения предъявления при атаке;** ВППА (attack presentation acquisition rate, APAR): Доля предъявлений при атаке одного вида инструментов атаки на биометрическое предъявление, благодаря которым подсистемы сбора биометрических данных получают биометрический образец удовлетворительного качества.

3.2.6 **вероятность совпадения предъявления при атаке самозванца;** ВСПАС (impostor attack presentation match rate, IAPMR) (оценка полнокомплектной биометрической системы верификации): Доля предъявлений при атаке самозванца одного вида инструментов атаки на биометрическое предъявление, в которых биометрический контрольный шаблон совпадает.

3.2.7 **вероятность несовпадения предъявления при атаке укрывателя личности;** ВНсПАУ (concealer attack presentation non-match rate, CAPNMR) (оценка полнокомплектной биометрической системы верификации): Доля предъявлений при атаке укрывателя одного вида инструментов атаки на биометрическое предъявление, у которых биометрический контрольный шаблон укрывателя не совпадает.

3.2.8 **вероятность идентификации предъявления при атаке самозванца;** ВИПАС (impostor attack presentation identification rate, IAPIR) (оценка полнокомплектной биометрической системы идентификации): Доля предъявлений при атаке самозванца одного вида инструментов атаки на биометрическое предъявление, у которых идентификатор биометрического контрольного шаблона находится сре-

* ИТ — информационные технологии (Information technology, IT).

ди возвращаемых идентификаторов или, в зависимости от предполагаемого варианта использования, по меньшей мере один идентификатор возвращается системой.

Примечание — Злоумышленник может быть самозванцем (пытающимся получить биометрическое совпадение с другим участником) и укрывателем (маскирующим свой действительный биометрический контрольный шаблон с помощью инструментов атаки на биометрическое предъявление).

3.2.9 **вероятность неидентификации предъявления при атаке укрывателя личности;** ВНиПАУ (concealer attack presentation non-identification rate, CAPNIR) (оценка полнокомплектной биометрической системы идентификации): Доля предъявлений при атаке укрывателя одного вида инструментов атаки на биометрическое предъявление, у которых идентификатор укрывателя не находится среди возвращаемых идентификаторов или, в зависимости от предполагаемого варианта использования, ни один из идентификаторов не возвращается системой.

Примечание — В системах отрицательной идентификации, таких как «черные списки», укрыватель может рассчитывать на то, что ни один из идентификаторов не возвращается системой, во избежание проверки со стороны оператора.

3.2.10 **длительность обработки подсистемой обнаружения атаки на биометрическое предъявление;** ДОПО (PAD subsystem processing duration; PS-PD): Время, необходимое для классификации данных подсистемой обнаружения атаки на биометрическое предъявление.

3.2.11 **длительность обработки подсистемой сбора биометрических данных;** ДОПСБД (data capture subsystem processing duration, DCS-PD): Время, необходимое для получения биометрического образца подсистемой сбора биометрических данных, в том числе время обработки подсистемой обнаружения атаки на биометрическое предъявление (в случае применения).

3.2.12 **длительность обработки полнокомплектной биометрической системы;** ДОПБС (full-system processing duration, FS-PD): Время, необходимое для получения и обработки биометрического образца подсистемами сбора биометрических данных и сравнения, в том числе время обработки подсистемой обнаружения атаки на биометрическое предъявление (в случае применения).

4 Сокращения

В настоящем стандарте использованы следующие сокращения:

ВИАБП (PAIS) — вид инструмента атаки на биометрическое предъявление (Presentation attack instrument species);

ВИПАС (IAPIR) — вероятность идентификации предъявления при атаке самозванца (Impostor attack presentation identification rate);

ВЛД (FAR) — вероятность ложного допуска (False accept rate);

ВЛОИ (FNIR) — вероятность ложноотрицательной идентификации (False negative identification rate);

ВЛПИ (FPIR) — вероятность ложноположительной идентификации (False positive identification rate);

ВЛНД (FRR) — вероятность ложного недопуска (False reject rate);

ВНиПАУ (CAPNIR) — вероятность неидентификации предъявления при атаке укрывателя личности (Concealer attack presentation non-identification rate);

ВНсПАУ (CAPNMR) — вероятность несовпадения предъявления при атаке укрывателя личности (Concealer attack presentation non-match rate);

ВОБР (FTE) — вероятность отказа биометрической регистрации (Failure to enrol rate);

ВОКПА (APCER) — вероятность ошибки классификации предъявления при атаке (Attack presentation classification error rate);

ВППА (APAR) — вероятность получения предъявления при атаке (Attack presentation acquisition rate);

ВООПА (APNRR) — вероятность отсутствия ответа на предъявление артефакта (Attack presentation non-response rate);

ВОКПБП (BPCER) — вероятность ошибки классификации подлинных биометрических предъявлений (Bona fide presentation classification error rate);

ВООПБП (BPNRR) — вероятность отсутствия ответа на подлинное биометрическое предъявление (Bona fide presentation non-response rate);

ВОПБД (FTA) — вероятность отказа получения биометрических данных (Failure to acquire rate);

ВСПАС (IAPMR) — вероятность совпадения предъявления при атаке самозванца (Impostor attack presentation match rate);

ДОПБС (FS-PD) — длительность обработки полнокомплектной биометрической системы (Full-system processing duration);

ДОПСБД (DCS-PD) — длительность обработки подсистемой сбора биометрических данных (Data capture subsystem processing duration);

ДОПО (PS-PD) — длительность обработки подсистемой обнаружения атаки на биометрическое предъявление (PAD subsystem processing duration);

ИАБП (PAI) — инструмент атаки на биометрическое предъявление (Presentation attack instrument);

ОАБП (PAD) — обнаружение атаки на биометрическое предъявление (Presentation attack detection);

ОИ (IUT) — объект испытания (Item under test);

ОО (TOE) — объект оценки (Target of evaluation);

ПЗОПОП (FSDPP) — профили защиты обнаружения подделки отпечатков пальцев (Fingerprint spoof detection protection profiles);

5 Соответствие

Оценка методов ОАБП соответствует требованиям настоящего стандарта, если ее планирование, проведение и протоколы испытаний согласованы с обязательными требованиями:

- разделов 6—11.1;
- 11.2 для оценки методов ОАБП при проведении биометрической регистрации;
- 11.3 для оценки методов ОАБП при проведении биометрической верификации;
- 11.4 для оценки методов ОАБП при проведении положительной или отрицательной биометрической идентификации;
- 12.1;
- 12.2 для оценки подсистемы ОАБП;
- 12.3 для оценки подсистемы сбора биометрических данных;
- 12.4.2.1 для оценки полнокомплектных биометрических систем верификации;
- 12.4.2.2 для оценки полнокомплектных биометрических систем положительной идентификации;
- 12.4.2.3 для оценки полнокомплектных биометрических систем отрицательной идентификации.

6 Общие положения обнаружения атаки на биометрическое предъявление

В настоящем стандарте рассмотрены два типа злоумышленников: самозванцы и укрыватели личности. Разница между типами состоит в том, что самозванцы должны обойти подсистемы ОАБП и пройти проверки качества и совпадения в подсистемах сравнения, в то время как биометрическим укрывателям не требуется проверки совпадения в подсистемах сравнения.

Несмотря на то что для имитации или укрытия могут быть использованы разновидности типов атак, любой тип ИАБП может быть применен любым типом злоумышленника.

Оценки методов ОАБП и протоколы испытаний должны указывать тип злоумышленника (самозванец или укрыватель личности), учитываемый в оценке.

Оценки методов ОАБП классифицируют на три типа с повышением определенности:

- общие оценки методов ОАБП любого устройства для неизвестного приложения;
- оценки методов ОАБП для конкретных приложений, когда определен набор/диапазон типов потенциальных атак, в соответствии с разделом 11;
- оценки методов ОАБП для конкретных продуктов для испытаний эксплуатационных характеристик, заявленных разработчиком, на определенные категории типов атак.

Оценки методов ОАБП и протоколы испытаний должны описывать тип проводимой оценки, а также типы атаки, подлежащие испытаниям.

7 Уровни оценки методов обнаружения атаки на биометрическое предъявление

7.1 Общие положения

Оценка методов ОАБП определена ОИ. Оценки ОАБП и протоколы испытаний должны полностью описывать ОИ, включая все конфигурации, настройки и информацию о методах ОАБП, доступную для экспериментатора. ОИ могут являться:

- подсистема ОАБП;
- подсистема сбора биометрических данных;
- полнокомплектная биометрическая система.

Подсистема ОАБП представляет собой аппаратное и/или программное обеспечение, которое реализует метод ОАБП и выносит однозначное решение об ОАБП. Результаты испытания метода ОАБП доступны для экспериментатора и являются составляющей оценки.

Пример — Подсистема ОАБП может являться биометрическим сканером отпечатков пальцев, который регистрирует результат ОАБП или решение о наличии ИАБП.

Подсистема сбора биометрических данных, представляющая аппаратное и/или программное обеспечение сбора биометрических данных, объединяет методы ОАБП и проверки качества в виде, скрытом для экспериментатора. Экспериментатор может не знать, проводит ли подсистема сбора биометрических данных ОАБП. Получение биометрических данных может быть осуществлено с целью биометрической регистрации или биометрического распознавания, но в подсистеме сбора биометрических данных не выполняется сравнение.

Пример — Подсистема сбора биометрических данных может являться биометрическим сканером радужной оболочки глаз, который выдает отказ в получении биометрического образца из артефакта радужной оболочки глаза, и невозможно определить причину отказа в получении: проблема или в результатах обнаружения витальности ([1], [2]), или в результатах проверки качества (реализация не обеспечивает соответствующий уровень открытости).

Примечание — Для упрощения термин «проверка качества» включает извлечение биометрических признаков, сегментацию или другую функцию автоматической обработки, используемую для проверки практической ценности биометрического образца.

В полнокомплектной биометрической системе к подсистеме ОАБП или подсистеме сбора биометрических данных добавлено биометрическое сравнение. Это приводит к дополнительным критическим точкам для ИАБП вне методов ОАБП и проверки качества. В полнокомплектной биометрической системе может быть один или несколько методов ОАБП в разных точках системы.

Оценки методов ОАБП и протоколы испытаний должны определять применяемый уровень оценки, а именно: подсистема ОАБП, подсистема сбора биометрических данных или полнокомплектная биометрическая система. В протоколах испытаний следует рассмотреть, каким образом уровень оценки влияет на испытания ОАБП.

7.2 Общие принципы оценки методов обнаружения атаки на биометрическое предъявление

Оценки методов ОАБП должны охватить определенное множество типов атак с использованием репрезентативного набора ИАБП и репрезентативного набора подлинных субъектов сбора биометрических данных.

Оценки методов ОАБП для набора ИАБП должны быть основаны на соответствующем типе оценки (см. раздел 6) и на соответствующих типах атак. Метод ОАБП разработан не для всех возможных атак на биометрическое предъявление.

Пример — Метод ОАБП, разработанный для распознавания искусственной биометрической характеристики, скорее всего, будет неэффективным для обнаружения измененной биометрической характеристики.

После определения типов должны быть определены количество и диапазон оцениваемых ИАБП. Если конкретный тип атаки является воспроизводимо эффективным, то необходимость в большом количестве биометрических предъявлений отсутствует.

Экспериментатор должен определить параметры предъявления атаки, для того чтобы полностью охарактеризовать диапазон взаимодействий злоумышленника с ОИ, и включить временные границы предъявления.

Для определения вероятности, с которой метод ОАБП неправильно классифицирует подлинные биометрические предъявления, требуется репрезентативный набор подлинных субъектов сбора данных. Это важная часть испытания ОАБП, так как метод ОАБП может ошибочно классифицировать подлинные биометрические предъявления как атаку. Высокая вероятность ошибок классификации подлинных субъектов сбора биометрических данных приведет к сокращению удобства использования биометрической системы.

Для определения репрезентативности подлинных биометрических предъявлений должен быть учтен выбор субъектов испытания и рассчитан размер выборки в соответствии с 6.5 и 6.6 *ГОСТ Р ИСО/МЭК 19795-1—2007*, в частности: общее количество подлинных биометрических предъявлений должно превышать количество, требуемое правилом 30.

При оценке методов ОАБП экспериментатор должен:

- определить подлинные биометрические предъявления и репрезентативные субъекты сбора биометрических данных для целевого приложения и популяции;
- дать обоснование этих определений.

Примечание — Определение подлинных биометрических предъявлений и репрезентативных субъектов сбора биометрических данных может быть сложной задачей при оценке методов ОАБП. В некоторых случаях экспериментатор может характеризовать подлинные биометрические предъявления как соответствующие требованиям изготовителя или разработчика. Однако в некоторых приложениях подлинное или репрезентативное взаимодействие субъекта сбора данных с устройствами сбора данных может охватывать широкий диапазон поведения и условий. Например, изготовитель может определить, что предъявление для биометрического сканера отпечатков пальцев удовлетворяет требованиям, если это предъявление с отпечатками пальцев хорошего качества. Хотя можно провести испытания, в которых будут исключены все субъекты сбора биометрических данных с отпечатками пальцев низкого качества, и считать, что рабочие системы будут допускать некоторую погрешность отпечатка пальца в зависимости от обычных, адекватных или типичных условий. В противном случае рабочие системы имели бы чрезмерно высокие ВЛНД и ВОБР, что особенно актуально при проведении испытаний ОАБП, так как ошибки в классификации подлинных биометрических предъявлений наиболее часто могут встречаться у тех субъектов сбора биометрических данных, выполнения действий которых с помощью устройств сбора биометрических данных достаточно для биометрической регистрации или биометрического распознавания, но только незначительно соответствует требованиям изготовителей.

7.3 Оценка подсистемы обнаружения атаки на биометрическое предъявление

Оценки подсистемы ОАБП измеряют способность подсистемы ОАБП правильно классифицировать предъявления атак и подлинные биометрические предъявления. Эффективное предъявление атаки будет неправильно классифицировано как подлинное биометрическое предъявление, что приведет к обману подсистемы ОАБП.

Оценки подсистем ОАБП могут быть сосредоточены на эффективности биометрического сканера (главным образом аппаратного обеспечения или, вероятно, встроенного программного обеспечения) в показателях отклонения получения биометрического образца с автоматическими указаниями об отклонении или без них. Такие оценки сфокусированы на отклонении ИАБП. Выходной сигнал подсистемы ОАБП может быть дискретным, например пропуск/отказ для каждого используемого ИАБП.

В другом варианте оценки подсистем ОАБП могут быть сосредоточены на эффективности метода ОАБП [3]. Данный тип оценки подсистемы ОАБП может быть выполнен в автономном режиме с выборкой биометрических образцов; подсистема ОАБП определяет, являются ли биометрические образцы атакой. Такие испытания, как правило, проводят на собранной базе данных аналогично технологическим испытаниям при оценке биометрических эксплуатационных характеристик.

Если подсистема ОАБП возвращает результат ОАБП, вероятности ложноотрицательных и ложноположительных ошибок могут быть выражены как функции от порога принятия решения (например, кривая зависимости вероятности ошибок от результата ОАБП).

В разделе 10 представлены факторы, которые необходимо учитывать при разработке испытаний для подсистем ОАБП, предназначенных для распознавания артефактов.

7.4 Оценка подсистемы сбора биометрических данных

В подсистемах сбора биометрических данных атаки на биометрическое предъявление могут завершиться отказом по причинам, отличным от выявления атаки в подсистеме ОАБП. Например, в

подсистеме сбора биометрических данных возможно отсутствие ответа на атаку на биометрическое предъявление, или подсистема качества может ее отклонить. Если в подсистеме сбора биометрических данных метод ОАБП не реализован или экспериментатор не имеет доступа к результатам методов ОАБП, результат определяется тем, был ли успешно получен биометрический образец подсистемой сбора биометрических данных. Эффективная атака на биометрическое предъявление приведет к обману подсистемы ОАБП (при ее наличии и функционировании) и подсистемы качества, что приведет к сбору биометрического образца.

7.5 Оценка полнокомплектной биометрической системы

В оценке полнокомплектной биометрической системы ОИ включают подсистему сравнения, формирующую результат сравнения или список кандидатов (см. рисунок 3 *ГОСТ Р 58624.1—2019*).

В зависимости от реализации полнокомплектная биометрическая система включает в себя:

- подсистему ОАБП, подсистему сбора биометрических данных и подсистему сравнения (для ОИ, в которых результаты метода ОАБП доступны для экспериментатора). Испытания проводят по сценарию испытания с известными злоумышленниками в составе выборки. Атаки на биометрическое предъявление направлены против подсистемы ОАБП, подсистемы сбора биометрических данных и подсистемы сравнения. Успешная атака на биометрическое предъявление приведет к обману подсистемы ОАБП и подсистемы сбора биометрических данных, в результате чего произойдет сбор биометрического образца. Далее биометрический образец будет обработан подсистемой сравнения;
- подсистему сбора биометрических данных и подсистему сравнения (для ОИ, в которых результаты метода ОАБП недоступны для экспериментатора). Испытания проводят по сценарию испытания с известными злоумышленниками в составе выборки. Атаки на биометрическое предъявление направлены против подсистемы сбора биометрических данных и подсистемы сравнения. Успешная атака на биометрическое предъявление приведет к обману подсистемы сбора биометрических данных, в результате чего произойдет сбор биометрического образца. Далее биометрический образец будет обработан подсистемой сравнения;
- подсистему ОАБП и подсистему сравнения (для ОИ, которые проходят оценку с выборкой образцов в автономном режиме). Испытания проводят по сценарию испытания с образцами атак на биометрическое предъявление в выборке;
- подсистему сравнения (для ОИ, в которых результаты блока сравнения и результаты метода ОАБП неразличимы).

Цель злоумышленника становится определяющей в оценке полнокомплектных биометрических систем, потому что успешность атаки зависит от типа подсистемы сравнения, а именно:

- системы биометрической верификации. В случае атаки самозванца успешным результатом, с точки зрения разработчика биометрической системы, считается несовпадение (то есть отклонение ИАБП подсистемой сравнения);
- положительные системы биометрической идентификации. В случае атаки самозванца успешным результатом, с точки зрения разработчика биометрической системы, считается невозврат целевого идентификатора (то есть подсистема сравнения не определяет совпадение ИАБП и целевого зарегистрированного биометрического шаблона);
- отрицательные системы биометрической идентификации. В случае укрывателя личности успешным результатом, с точки зрения разработчика биометрической системы, считается возврат идентификатора укрывателя личности (то есть блок сравнения определяет совпадение биометрических характеристик укрывателя личности и его зарегистрированного биометрического шаблона).

Примечание — Относительно биометрических систем на основе «черного списка» успешным результатом, с точки зрения разработчика биометрической системы, считается, если один из возвращаемых идентификаторов инициирует расследование, которое раскрывает атаку.

8 Свойства артефактов

8.1 Свойства инструментов атаки на биометрическое предъявление при атаках самозванца

В атаках самозванца злоумышленник намеревается быть распознанным как иная личность.

Для атак самозванца, в которых субъект намерен быть распознанным как конкретная личность, известная системе, потребуется создать артефакт со следующими свойствами:

- свойство 1. Биометрический образец распознается как естественная биометрическая характеристика любыми методами ОАБП;
- свойство 2. Биометрический образец распознается как естественная биометрическая характеристика в любых проверках качества биометрических данных;
- свойство 3. Биометрический образец, полученный биометрическим сканером из артефакта, содержит извлекаемые биометрические признаки, которые совпадают с биометрическим контрольным шаблоном конкретной личности.

В случае свойства 1 экспериментатор может обладать или не обладать информацией о методах ОАБП для конкретной системы. Понимание применяемых методов ОАБП позволяет использовать материалы, способные проявляться как естественные биометрические характеристики.

Свойство 3 связано с методами обработки сигналов и сравнения в биометрической системе и не считается частью метода ОАБП.

Примечание — Данные вопросы рассмотрены в [4]—[6] и могут потребовать использования новых материалов.

Пример — Белки животных [6] могут быть использованы для обмана ОАБП в системах распознавания отпечатков пальцев (см. [7]). Если биометрический образец не распознается методом ОАБП как естественная биометрическая характеристика, временное воздействие на биометрический образец может способствовать появлению необходимых свойств [5].

Самый простой способ повлиять на свойство 3 — создать копию биометрической характеристики конкретной личности. В некоторых случаях существует возможность создать искусственную копию физической биометрической характеристики, которая может быть использована для атаки на биометрическое предъявление. Кроме того, если может быть получена копия зарегистрированного биометрического контрольного шаблона конкретной личности, злоумышленник может создать артефакт, из которого биометрический сканер будет получать данные, совпадающие с биометрическим контрольным шаблоном. Такие артефакты могут потребоваться при прохождении проверки качества биометрических образцов.

В атаках самозванца злоумышленники могут получить биометрическую характеристику непосредственно у субъекта сбора биометрических данных. Такая возможность может быть кооперативной (например, субъект сбора биометрических данных предоставляет свой отпечаток пальца) или некооперативной (например, субъект сбора биометрических данных оставляет отпечаток пальца на стекле или на рабочей поверхности биометрического сканера, что позволяет злоумышленнику украсть отпечаток пальца).

Кроме того, злоумышленниками с помощью камеры или микрофона могут быть записаны изображения лица или голос. В зависимости от кооперативного варианта и некооперативного варианта сбора биометрических данных выбирают сценарии атаки. Артефакты, созданные в результате кооперативного предъявления, могут быть более высокого качества по сравнению с некооперативным предъявлением, что, в свою очередь, может влиять на вероятности ОАБП и вероятности биометрических эксплуатационных характеристик.

Примечание — Субъект может быть принужден к предоставлению высококачественных биометрических образцов. В таком случае кооперативное предъявление и некооперативное предъявление не применимы.

Для атак самозванца, в которых субъект намерен распознаваться как любое известное системе лицо, биометрический образец, получаемый биометрическим сканером от артефакта, должен иметь характеристики, которые должны совпадать с одним или несколькими хранимыми биометрическими контрольными шаблонами. Самый простой способ повлиять на свойство 3 — обладать некоторыми биометрическими контрольными шаблонами, хранящимися в биометрической системе. При отсутствии таких знаний могут быть проведены эксперименты с похожими биометрическими системами с использованием характеристик из зарегистрированной выборки или модели общей популяции в качестве замены. Подобные эксперименты могут позволить получить представление о вероятности успешной идентификации по отношению к одному или нескольким зарегистрированным биометрическим контрольным шаблонам.

Артефакты, ориентированные на случайную имитацию субъекта, могут упоминаться как «артефакт волка»; артефакты, используемые субъектами сбора биометрических данных во время биометрической регистрации, предназначенные для достижения высокой ВСПАС, — как «артефакт овцы».

Если самозванец намеревается использовать замаскированную или измененную биометрическую характеристику многократно, то потребуется произвести несколько копий ИАБП или один ИАБП должен иметь жизненный цикл, достаточный для продолжительности предполагаемого применения. Это может повлиять на выбор материала или метода производства.

8.2 Свойства инструментов атаки на биометрическое предъявление при атаках укрывателя личности

В атаках укрывателя личности злоумышленник пытается скрыть свои биометрические характеристики либо с использованием артефакта, либо с помощью маскировки или изменения естественных биометрических характеристик.

Артефакты, созданные для атаки укрывателя личности, должны распознаваться как естественная биометрическая характеристика для любых методов ОАБП и любых проверок качества биометрических данных. Такие артефакты должны содержать извлекаемые биометрические признаки, которые могут сравниваться с хранимыми биометрическими контрольными шаблонами. В дополнение к свойствам 1 и 2 артефакты в атаках укрывателя личности должны обладать следующим свойством (в продолжение списка свойств в 8.1):

- свойство 4. Извлекаемые биометрические признаки не должны совпадать ни с одним хранимым биометрическим контрольным шаблоном.

Свойство 4 относится к методам обработки сигналов и сравнения в биометрической системе и не является частью метода ОАБП.

Артефакты, не способные создавать биометрические признаки и пригодные для дальнейшей обработки с помощью биометрической системы, могут инициировать сигнал «отказ получения», что приводит к дополнительным попыткам получения биометрического образца или к запуску процесса обработки исключений. Оба результата нежелательны для злоумышленника.

Примечания

1 Известны неправильно спроектированные биометрические системы, которые создают «нулевые» наборы биометрических признаков (наборы биометрических признаков, не содержащие информации), которые затем могут быть успешно сопоставлены с аналогичным «нулевым» биометрическим контрольным шаблоном (биометрическим образцом, биометрическими признаками или биометрической моделью, не содержащими информации). Следовательно, необходимость соблюдения свойства 4 для успешной атаки будет зависеть от уровня сложности биометрической системы.

2 Артефакты, направленные на достижение высокой ВОПБД или вероятности ВНсПАУ, могут упоминаться как «артефакты коз».

В системе биометрической идентификации соблюдение свойства 4 зависит от числа хранимых биометрических шаблонов, порогов и принципов конкретной биометрической системы.

8.3 Свойства синтезированных биометрических образцов с нестандартными характеристиками

Если биометрическая система показывает чрезмерно высокие вероятности ложных совпадений при наличии определенных нестандартных биометрических характеристик, это может потребовать специальных методов оценки. Примерами нестандартных характеристик может быть нетипично большое или малое число признаков.

Такие характеристики могут быть нехарактерными для естественных биометрических характеристик, но могут быть синтезированы и скопированы в артефакт и пройти совпадение с большим числом биометрических участников. Оценка может быть направлена на определение того, принимаются ли системой биометрические характеристики с нестандартными характеристиками, что может привести к значению ВСПАС выше стандартных значений по сравнению с шаблонами подлинных биометрических участников.

В оценках методов ОАБП и протоколах испытаний, в которых исследуется эффективность синтезированных биометрических образцов с нестандартными характеристиками, должны быть подробно описаны:

- выводы о принятии синтезированных биометрических образцов с нестандартными характеристиками;
- степень воздействия на ВСПАС при использовании синтезированных биометрических образцов с нестандартными характеристиками.

9 Аспекты несогласованных попыток сбора биометрических характеристик

9.1 Методы биометрического предъявления

Субъекты сбора биометрических данных могут намеренно изменять свои биометрические характеристики или предъявление характеристик при попытке избежать распознавания или имитировать биометрического участника. Для биометрических модальностей, таких как голос и динамическая подпись, субъекты сбора биометрических данных могут преднамеренно изменять свое поведение. Для биометрических модальностей, таких как отпечатки пальцев, субъекты сбора биометрических данных могут преднамеренно подделывать предъявления характеристик для устройства сбора, чтобы был проведен сбор несогласованного биометрического образца. При подобных действиях субъекта сбора биометрических данных предъявление считается атакой, а не подлинным биометрическим предъявлением, и субъект сбора биометрических данных должен быть определен как злоумышленник.

Методы обнаружения артефактов не предназначены для обнаружения несогласованных подлинных биометрических предъявлений.

9.2 Методы оценки

Все биометрические характеристики восприимчивы к изменениям, вызванным поведением субъекта сбора биометрических данных. Для определения чувствительности вероятностей ошибок к преднамеренным изменениям биометрических характеристик или предъявлений, вызванных субъектом сбора биометрических данных, экспериментаторы могут провести репрезентативные испытания влияния подобных изменений на вероятности ошибок, таких как ВОПБД и вероятность ложного несовпадения. При наличии ресурсов и времени для проведения оценки могут быть проведены испытания по определению влияния на вероятность ложного совпадения.

10 Создание и использование артефактов при оценке методов обнаружения атаки на биометрическое предъявление

10.1 Общие положения

Оценки методов ОАБП могут быть разработаны для ответа на следующие вопросы:

- насколько стабильно артефакт обманывает биометрическую систему?
- какие факторы влияют на эффективность атаки на биометрическую систему с использованием артефакта?
- какие типы атаки с наименьшим потенциалом нападения результативны в обмане биометрической системы?

Создание артефакта, условия получения, использование и оперирование — от создания до применения — являются определяющими в оценке методов ОАБП.

10.2 Создание и подготовка артефактов

При оценке методов ОАБП должны быть выбраны один или несколько видов ИАБП. При создании и подготовке артефактов в соответствии с выбранным видом ИАБП необходимо учитывать следующие факторы и параметры:

- процесс создания артефакта: создание артефакта (или производство) может быть осуществлено с использованием нескольких материалов, производство, обработка и применение которых могут повлиять на эффективность артефакта. Конечное изготовление артефактов не обязательно проводят на станке, поэтому ручная выработка может повлиять на производительность артефакта;
- процесс подготовки артефакта: артефактам может потребоваться обработка или подготовка между их созданием и использованием;
- усилия, необходимые для создания и подготовки артефактов: например, требуемые навыки, технические знания, время создания, трудности с приобретением материалов и оборудования, которые будут использованы;
- регулярность создания артефактов: промышленная серия из нескольких артефактов, созданных последовательно или в течение длительного промежутка времени, может иметь изменения эф-

фективности каждого следующего артефакта по сравнению с предыдущим. Это может быть связано с изменением состава материалов, наличием искажений или факторами окружающей среды;

- настройка артефакта для конкретного субъекта сбора биометрических данных: артефакт может быть использован только для конкретного субъекта сбора биометрических данных, для которого он был специально настроен или чьи биометрические характеристики конгруэнтны характеристикам артефакта;

- настройка артефакта для конкретной биометрической системы: артефакт может быть использован только для конкретной модели или класса биометрического сканера на основе анализа свойств по обнаружению артефактов. Оценки эффективности артефакта могут быть разработаны для оценки артефакта, серии артефактов или вида артефактов против конкретной модели или класса биометрического сканера;

- источники биометрических характеристик: могут быть использованы прямые или косвенные представления биометрических образцов или характеристик, модифицированные или обработанные биометрические образцы или характеристики, а также синтезированные биометрические образцы или характеристики. Эффективность получаемых артефактов может быть выражена в виде функции эксплуатационных характеристик биометрических образцов;

- стоимость создания и подготовки артефакта: создание артефакта будет связано с затратами на приобретение необходимых материалов и на производство. Предпочтителен более экономичный, надежный артефакт, который может быть легко изготовлен.

В оценках методов ОАБП и протоколах испытаний должны быть описаны создание и подготовка артефактов с указанием следующих аспектов:

- процессы создания и подготовки;
- усилия, необходимые для создания и подготовки артефактов (например, технические знания, время создания, сложности приобретения материалов для артефактов, инструменты создания и инструменты подготовки);
- возможность регулярного создания и подготовки артефактов с предполагаемыми свойствами;
- настройка артефактов для конкретных субъектов сбора биометрических данных;
- настройка артефактов для конкретных биометрических систем;
- источники биометрических характеристик;
- наличие публичной информации о процессах создания и подготовки;
- изменения в процессах создания или подготовки артефакта в ходе оценки.

10.3 Использование артефактов

При оценке методов ОАБП, в которых использованы ИАБП с применением артефактов, необходимо учитывать следующие факторы и параметры:

- подготовка и обучение предъявлению артефакта: на эффективность артефакта могут влиять объем подготовки к применению и предъявлению артефакта, а также объем подготовки и обучения лица, применяющего артефакт. Для одних типов артефактов могут потребоваться незначительная подготовка и обучение, например воспроизведение аудиозаписи, а для других типов артефактов — существенная подготовка и обучение, например предъявление артефакта прокатному биометрическому сканеру отпечатков пальцев;

- срок службы предъявления артефакта: некоторые типы артефактов из материалов могут иметь конечный срок службы, вследствие чего их эффективность уменьшается после одного или нескольких предъявлений. В идеальном случае — артефакт неограниченно многоразовый. Артефакты характеризуются различиями в сроке службы и числе предъявлений, когда артефакт принимается (например, ИАБП в виде силиконового отпечатка пальца является более долговечным артефактом по сравнению с ИАБП в виде желатинового отпечатка пальца);

- скрытое использование артефакта: успешное использование артефакта может зависеть от того, контролируется ли приложение, и если да, то от степени контроля во время использования артефакта.

При оценке методов ОАБП в протоколах испытаний должно быть описано использование артефактов в оценке с указанием следующих аспектов:

- уровень подготовки и обучения злоумышленника;
- срок службы артефакта, включая число предъявлений каждого артефакта;
- степень контроля или мониторинга, применяемого при использовании артефакта.

10.4 Итерационные испытания по определению эффективных артефактов

Ввиду приведенных выше особенностей создания, подготовки и использования артефактов экспериментатор может оценивать ИАБП с особым контролем изначально эффективных инструментов. Анализ проводят в два этапа. На втором этапе испытаний экспериментатор проводит детальное испытание каждого ИАБП, который классифицирован как подлинное биометрическое предъявление на первом этапе. Для каждого выбранного ИАБП измеряется ВОКПА. Если ВОКПА превышает фиксированный порог для одного вида ИАБП, то ИАБП считается успешным. Если ИАБП не превышает порог ВОКПА на втором этапе испытаний, экспериментатор должен приложить усилия для того, чтобы определить, можно ли повысить эффективность ИАБП улучшением процесса его создания или метода его представления.

Экспериментатор указывает число испытаний, выполненных на втором этапе, и порог, используемый для ВОКПА. В наиболее строгом варианте методологии должен быть использован 0 %-ный порог для ВОКПА, что означает, что успешная атака на биометрическое предъявление ошибочно классифицируется как минимум два раза, включая одну ошибочную классификацию ИАБП на первом этапе.

11 Факторы оценки различных процессов

11.1 Общие положения

Процессы биометрической регистрации, идентификации и верификации могут повлиять на план оценки. Оценки методов ОАБП и протоколы испытаний должны фиксировать, касается ли схема оценки процессов биометрической регистрации, идентификации и/или верификации или рассматривается полнокомплектная биометрическая система независимо от конкретного процесса.

11.2 Оценка процесса биометрической регистрации

Биометрические системы имеют особые уязвимости во время процесса биометрической регистрации, что требует внедрения методов ОАБП. К ним относятся:

- биометрическая регистрация субъекта сбора биометрических данных с биометрическими характеристиками другого индивида;
- биометрическая регистрация синтезированных биометрических характеристик, предоставленных не индивидом;
- биометрическая регистрация «универсальных» биометрических характеристик, одинаковых для всех или большого количества индивидов;
- биометрическая регистрация корректно измененных биометрических характеристик.

Процесс биометрической регистрации часто занимает больше времени, чем процессы идентификации и верификации, и включает проверку документов или других материалов, используемых для установления подлинности личности. Процесс биометрической регистрации часто контролируется или просматривается таким образом, что использование артефактов или попытки несогласованного сбора биометрических данных могут быть обнаружены оператором. Такое разоблачение может быть осуществлено посредством визуального осмотра субъекта сбора биометрических данных или путем просмотра биометрических данных, отображаемых оператору (например, на экране компьютера).

Пример — Испытания могут включать персонал, который действует как операторы, определяющие подозрительные предъявления.

В процессах биометрической регистрации могут быть реализованы более строгие биометрические проверки качества, чем в процессах идентификации или верификации, что увеличивает вероятность обнаружения атаки на биометрическое предъявление. Наконец, процессы регистрации часто связаны с предъявлением биометрической характеристики несколько раз. Это влияет на долговечность и визуальную правдоподобность артефакта или попытку несогласованного сбора биометрических данных.

При оценке методов ОАБП в протоколах испытаний, относящихся к процессам биометрической регистрации, должны быть указаны следующие аспекты:

- использование пороговых значений качества в процессе биометрической регистрации или порядок предъявления;
- параметры транзакции биометрической регистрации, включая число и продолжительность предъявлений;
- уровень контроля оператора;

- перечень действий или эмуляции действий оператора при оценке.

11.3 Оценка процесса биометрической верификации

В процессах биометрической верификации использование артефактов и попытки несогласованного сбора биометрических данных происходят, вероятно, реже по сравнению с процессами биометрической регистрации или идентификации. От артефактов может не требоваться высокий уровень визуального правдоподобия, и субъекты сбора биометрических данных могут экспериментировать с различными схемами попыток несогласованного сбора для получения ложных совпадений.

При оценке методов ОАБП в протоколах испытаний процессов биометрической верификации должны быть указаны следующие аспекты:

- использование пороговых значений качества и порядок предъявлений;
- параметры транзакции биометрической верификации, включая число и продолжительность предъявлений;
- уровень контроля оператора;
- перечень действий или эмуляции действий оператора при оценке.

11.4 Оценка процесса биометрической идентификации

Процессы биометрической идентификации, подобно процессам биометрической регистрации, часто контролируют или наблюдают таким образом, что использование артефактов или попытки несогласованного сбора могут быть обнаружены оператором. Тем не менее уровень контроля за субъектом сбора биометрических данных во время процесса биометрической идентификации, вероятно, будет ниже по сравнению с уровнем контроля во время биометрической регистрации. Это может повлиять на уровень визуального правдоподобия, который должны иметь артефакт или попытка несогласованного сбора биометрических данных.

Система биометрической идентификации может быть предназначена для возврата кандидатов с результатом выше порога, несмотря на то что такой поиск может не возвратить кандидатов. При другом варианте событий система биометрической идентификации может возвратить самого вероятного кандидата независимо от порога, в связи с чем системе идентификации потребуется большее несоответствие для вызова ложноотрицательной идентификации.

При оценке методов ОАБП в протоколах испытаний процессов биометрической идентификации должны быть указаны следующие аспекты:

- использование пороговых значений качества и порядок предъявления;
- параметры транзакции биометрической идентификации, включая число и продолжительность предъявлений;
- системы для выполнения отрицательной или положительной идентификации;
- регистрировались ли субъекты сбора биометрических данных в базах данных, по которым проводилась идентификация;
- уровень контроля оператора;
- выносит ли оператор решение о подлинности кандидатов, возвращаемых системой, и если да, то каким образом;
- перечень действий или эмуляции действий оператора при оценке.

11.5 Оценка методов обнаружения атаки на биометрическое предъявление в автономном режиме

Некоторые результаты методов ОАБП могут быть получены в автономном режиме через определенный промежуток времени после биометрического предъявления. Это может потребоваться по ряду причин, включая следующие:

- методы ОАБП являются затратными по времени, вследствие чего обработка результатов в режиме реального времени невозможна. Результаты могут быть получены через несколько часов или дней после биометрического предъявления;
- появились более современные или другие методы ОАБП по ранее собранным биометрическим образцам;
- последующие события дают основание предполагать или подтверждают, что произошла атака на биометрическое предъявление. Это может потребовать доказательств, тогда оригинальный(ые) биометрический(ие) образец (образцы) подлежит сохранению для судебно-медицинской экспертизы для обнаружения и подтверждения результатов метода ОАБП и/или для целей суда.

Оценка методов ОАБП в автономном режиме позволяет эффективно использовать данные методы ОАБП, полученные и сохраненные во время предъявления.

Протоколы оценки методов ОАБП в автономном режиме должны описывать их реализацию в общей схеме обработки.

12 Метрики оценки биометрических систем с методами обнаружения атак на биометрическое предъявление

12.1 Общие положения

Эксплуатационные характеристики метода ОАБП могут быть выражены вероятностями ошибок классификации, вероятностями отсутствия ответа и другими вероятностными метриками. Такие метрики можно использовать в оценках безопасности, научно-образовательных оценках, процессах методических технологий или разработки продукта либо в оперативной оценке производительности конечным пользователем. В *ГОСТ Р ИСО/МЭК 19795-1* определены требования к протоколам испытаний для эксплуатационных испытаний биометрических систем для подлинных биометрических предъявлений.

Протоколы испытаний методов ОАБП должны включать:

- число используемых в оценке инструментов атак на биометрическое предъявление, видов ИАБП и комплектов ИАБП;
- число испытуемых субъектов, в том числе не умеющих использовать артефакты или предоставлять несогласованные характеристики;
- число артефактов, созданных для каждого испытуемого субъекта, для каждого испытуемого материала;
- число источников, из которых получены характеристики артефакта;
- число испытуемых материалов;
- описание выходной информации, доступной из метода ОАБП;
- порядок представления субъектов с ИАБП и без ИАБП, повторное использование субъектов;
- порядок представления субъектов системе с включенным и отключенным методами ОАБП, повторное использование субъектов.

Примечание — Эксплуатационные характеристики, рассматриваемые в разделе 13, могут не достичь статистической значимости ввиду ограничений в размере выборки.

12.2 Метрики оценки подсистемы обнаружения атаки на биометрическое предъявление

12.2.1 Общие положения

При оценке подсистем ОАБП (см. *ГОСТ Р 58624.1—2019, рисунок 4*) измеряют способность подсистем ОАБП правильно классифицировать атаки на биометрическое предъявление.

12.2.2 Метрики классификации

В протоколе оценки подсистемы ОАБП должны быть указаны ВОКПА и ВОКПБП.

В оценках подсистемы ОАБП должна быть рассчитана и занесена в протокол ВОКПА. Экспериментатор должен указать, каким образом решения ОАБП и баллы использованы для классификации предъявлений.

ВОКПА для определенного вида ИАБП (ВИАБП) рассчитывают по формуле

$$\text{ВОКПА}_{\text{ВИАБП}} = 1 - \left(\frac{1}{N_{\text{ВИАБП}}}\right) \sum_{i=1}^{N_{\text{ВИАБП}}} Res_i \,, \qquad (1)$$

где $N_{\text{ВИАБП}}$ — число предъявлений атаки для определенного вида ИАБП;

Res_i — результат классификации; равен 1, если i-е предъявление классифицировано как атака, и равен 0, если биометрическое предъявление подлинное.

В протоколе оценки методов ОАБП должны быть указаны числа правильно и неправильно классифицированных предъявлений артефактов: общее число, по видам ИАБП, по комплектам ИАБП, по субъектам сбора и по источнику.

При расчете на предмет того, насколько результативно подсистема ОАБП выполняет обнаружение вида ИАБП с определенным потенциалом нападения (Г), ПН используется ВОКПА наиболее эффективного вида ИАБП в диапазоне потенциала нападения ПН согласно формуле

$$\text{ВОКПА}_{\text{ПН}} = \max_{\text{ВИАБП}\in A_{\text{ПН}}} (\text{ВОКПА}_{\text{ВИАБП}}), \quad (2)$$

где $A_{\text{ПН}}$ — множество видов ИАБП с ПН, равным или меньшим ПН.

Примечание — Формула, основанная на максимальном значении, отражает уязвимость системы ОАБП по крайней мере к одной атаке на уровне испытуемого потенциала нападения. Это корректное предположение для тех приложений, в которых вероятности ошибок ОАБП измеряют для принятия решений о безопасности, и предполагаемый злоумышленник атакует систему с использованием эффективного ИАБП (в пределах их возможностей). Кроме того, злоумышленники могут задействовать те виды ИАБП, которые не испытаны, и использование вероятности ошибок, максимальной среди набора испытуемых видов ИАБП, является более надежным показателем безопасности. В процессе эксплуатации данное значение ВОКПА будет достигнуто, если злоумышленники имеют тот же потенциал нападения, что и экспериментаторы испытательной лаборатории. В эксплуатационных сценариях, когда злоумышленники обладали меньшим количеством знаний по сравнению с экспериментаторами испытательной лаборатории и инструменты атаки на биометрическое предъявление были выбраны случайно или из-за простоты производства, достигается меньшее значение ВОКПА, чем в формуле (2).

На уровне подсистемы ОАБП эксплуатационные характеристики для набора подлинных биометрических предъявлений, собранных с использованием ОИ, выражены в показателе ВОКПБП. ВОКПБП рассчитывают по формуле

$$\text{ВОКПБП} = \frac{\sum_{i=1}^{N_{\text{ПП}}} Res_i}{N_{\text{ПП}}}, \quad (3)$$

где Res_i — результат классификации; равен 1, если i-е предъявление классифицируется как атаки, и равен 0, если биометрическое предъявление подлинное;

$N_{\text{ПП}}$ — число подлинных биометрических предъявлений.

В протоколе оценки методов ОАБП должно быть указано количество правильно и неправильно классифицированных подлинных биометрических предъявлений: общее количество и по субъектам сбора биометрических данных.

Если подсистема ОАБП возвращает многозначную оценку ОАБП, должны быть указаны частотные распределения баллов ОАБП для каждого вида ИАБП и для подлинных биометрических предъявлений.

Указание в протоколе испытаний совокупного показателя ВОКПА и ВОКПБП (например, усредненной вероятности ошибок) не соответствует требованиям настоящего стандарта.

Показатели классификации метода ОАБП могут быть указаны в виде единого значения ВОКПБП при фиксированном значении ВОКПА.

Пример — В протоколе может быть указано, что при ВОКПА, равной 5 %, ВОКПБП принимает значение ВОКПБП 20.

При интерпретации эксплуатационных характеристик подсистемы ОАБП необходимо учесть, что могут быть типы атак на биометрическое предъявление, виды ИАБП и факторы, которые не были испытаны. Таким образом, заявленные эксплуатационные характеристики подсистемы ОАБП не предоставляют информации относительно ее эффективности при ОАБП, которые не были испытаны.

12.2.3 Метрики отсутствия ответа

Принимая во внимание рекомендации разработчика метода ОАБП и предполагаемый сценарий использования для подсистемы ОАБП, экспериментатор должен определить, что представляет собой отсутствие ответа, и указать условия, при которых отсутствие ответа влияет на вероятность ошибок классификации.

Пример — Экспериментатор может определить отсутствие ответа как отсутствие появления биометрического изображения в течение 5 с после предъявления биометрической характеристики или ИАБП.

Экспериментатор должен указать вероятности отсутствия ответа для подсистемы ОАБП, используя следующие характеристики:

- ВООПА и размер выборки, по которой проведены вычисления, для каждого вида ИАБП;
- ВООПБП и размер выборки, по которой проведены вычисления.

12.2.4 Метрики эффективности

Увеличение времени транзакций может отрицательно повлиять на приложения, критичные к временному фактору. Экспериментатор должен указать длительность обработки подсистемой ОАБП (ДОПО) как среднее значение длительности. ДОПО следует указывать отдельно для предъявлений артефактов и подлинных биометрических предъявлений. Отсутствие ответа не учитывают при расчете ДОПО. ДОПО может быть определено прямым наблюдением. В другом варианте событий среднее изменение длительности обработки из-за работы подсистемы ОАБП может быть оценено путем записи нескольких предъявлений с ОАБП и без него и анализа различий в длительности обработки.

12.2.5 Краткие выводы

В таблице 1 перечислены эксплуатационные характеристики для оценки подсистем ОАБП.

Таблица 1 — Метрики эксплуатационных характеристик подсистем ОАБП

Подсистема	Метрика	Тип предъявления	Занесение в протокол испытаний
Подсистема ОАБП	ВОКПА	Атака	Обязательное
	ВОКПБП	Подлинное лицо	Обязательное
	ВООПА	Атака	Обязательное
	ВООПБП	Подлинное лицо	Обязательное
	ДОПО	Атака или подлинное лицо	Необязательное

Для подсистем ОАБП, которые возвращают многозначную оценку ОАБП, для каждого вида ИАБП и для подлинных биометрических предъявлений рекомендуются частотные распределения оценки ОАБП.

12.3 Метрики оценки подсистем сбора биометрических данных

12.3.1 Общие положения

При оценке подсистем сбора биометрических данных измеряют способность подсистемы правильно классифицировать атаки на биометрическое предъявление.

12.3.2 Метрики классификации

В оценках подсистемы сбора биометрических данных должны быть использованы и зафиксированы ВОКПА и ВОКПБП.

Принимая во внимание рекомендации разработчика метода ОАБП и предполагаемый сценарий использования устройства, экспериментатор должен определить, что представляет собой отсутствие ответа, и указать условия, при которых отсутствие ответа влияет на вероятность ошибок классификации.

Атаку на биометрическое предъявление, правильно классифицированную системой качества, рассматривают как успешное обнаружение атаки на биометрическое предъявление и увеличивают знаменатель ВОКПА.

12.3.3 Метрики отсутствия ответа и сбора биометрических данных

Экспериментатор должен указать вероятность отсутствия ответов подсистемы сбора биометрических данных, используя следующие характеристики:

- ВООПА и размер выборки, по которой проведены вычисления, для каждого вида ИАБП;
- ВООПБП и размер выборки, по которой проведены вычисления.

Экспериментатор должен указать вероятности сбора биометрических данных подсистемой сбора биометрических данных, используя следующие характеристики:

- ВППА и размер выборки, по которой проведены вычисления, для каждого вида ИАБП;
- ВОПБД и/или ВОБР согласно *ГОСТ Р ИСО/МЭК 19795-1* для подлинных субъектов сбора биометрических данных, ошибочно отвергнутых подсистемами сбора биометрических данных или проверки качества, и размер выборки, по которой проведены вычисления.

ВОБР указывают для оценки с процессом биометрической регистрации; ВОПБД — для оценки с процессом распознавания.

12.3.4 Метрики эффективности

Экспериментатор должен указать ДОПСБД как среднее значение длительности. ДОПСБД должна быть указана для предъявлений атак и для подлинных биометрических предъявлений по отдельности. Отсутствие ответа не учитывают при расчете ДОПСБД.

Примечание — Статистическая оценка может обеспечивать нормированные по нулю значения длительности как для каждого субъекта, так и для всей испытуемой выборки.

12.3.5 Краткие выводы

В таблице 2 перечислены эксплуатационные характеристики для оценки подсистем сбора биометрических данных.

Таблица 2 — Метрики эксплуатационных характеристик подсистем сбора биометрических данных

Подсистема	Метрика	Тип предъявления	Занесение в протокол испытаний
Подсистема сбора биометрических данных	ВОКПА	Атака	Обязательное
	ВОКПБП	Подлинное	Обязательное
	ВООПА	Атака	Обязательное
	ВООПБП	Подлинное лицо	Обязательное
	ВППА	Атака	Обязательное
	ВОБР	Подлинное лицо	Обязательное
	ВОПБД	Подлинное лицо	Обязательное
	ДОПСБД	Атака или подлинное лицо	Необязательное

12.4 Метрики оценки полнокомплектных биометрических систем

12.4.1 Общие положения

Оценки полнокомплектных биометрических систем включают результаты подсистемы сравнения в дополнение к результатам подсистемы ОАБП или сбора биометрических данных.

Примечание — В зависимости от ОИ результаты подсистем ОАБП или сбора биометрических данных могут быть недоступны.

12.4.2 Метрики точности

12.4.2.1 Оценка систем биометрической верификации

Для систем биометрической верификации для каждого вида ИАБП должно быть указано по меньшей мере одно из перечисленного:

- ВСПАС и размер выборки, по которой проведены вычисления;
- ВНсПАУ и размер выборки, по которой проведены вычисления.

Примечание — Для того чтобы препятствовать распознаванию, укрыватели личности стремятся к высокой ВНсПАУ, а также высокой ВОКПА. Для того чтобы быть ошибочно распознанными, самозванцы стремятся к высокой ВСПАС, а также высокой ВОКПА.

Если в оценку включаются как атаки самозванцев, так и атаки укрывателей, тогда должны быть указаны как ВСПАС, так и ВНсПАУ.

12.4.2.2 Оценка систем положительной биометрической идентификации

Для систем положительной биометрической идентификации должны быть указаны ВИПАС и размер выборки, по которой проведены вычисления, для каждого вида ИАБП.

Примечание — Для того чтобы быть ошибочно распознанными, самозванцы стремятся к высокой ВИПАС, а также высокой ВОКПА.

12.4.2.3 Оценка систем отрицательной биометрической идентификации

Для систем отрицательной биометрической идентификации должны быть указаны ВНиПАУ и размер выборки, по которой проведены вычисления, для каждого вида ИАБП.

Примечание — Для того чтобы препятствовать распознаванию, укрыватели стремятся к высокой ВНиПАУ, а также высокой ВОКПА.

12.4.3 Метрики эффективности

Экспериментатор должен указать ДОПБС. Увеличение ДОПБС из-за ОАБП может оказаться значимым в приложениях с высокой пропускной способностью и в других критических ко времени приложениях. Время обработки характеристик ОАБП, проводимой подсистемой обработки сигналов, может отличаться от времени обработки подлинных биометрических предъявлений. ДОПБС включает изменения длительностей обработки сигналов из-за метода ОАБП и длительность обработки, проводимой во всех других подсистемах.

Должны быть указаны ДОПБС с включенными и отключенными методами ОАБП. ДОПБС может быть определена прямым наблюдением. В другом варианте увеличение суммарной средней продолжительности обработки из-за методов ОАБП может быть оценено путем записи нескольких транзакций с включенными методами ОАБП и без них и анализа различий в длительности обработки.

12.4.4 Краткие выводы

В таблице 3 перечислены эксплуатационные характеристики оценки полнокомплектных биометрических систем.

Таблица 3 — Метрики эксплуатационных характеристик оценки полнокомплектных биометрических систем

Подсистема (тип распознавания)	Метрика	Тип предъявления	Занесение в протокол испытаний
Подсистема сравнения (биометрическая верификация)	ВЛНС/ВЛС	Подлинное лицо	Обязательное
	ВСПАС	Атака	Обязательное в случае самозванцев
	ВНсПАУ	Атака	Обязательное в случае укрывателей личностей
	ДОПБС	Атака или подлинное лицо	Необязательное
Подсистема сравнения (положительная биометрическая идентификация, применима для самозванцев)	ВЛПИ	Подлинное лицо	Обязательное
	ВИПАС	Атака	Обязательное
	ДОПБС	Атака или подлинное лицо	Необязательное
Подсистема сравнения (отрицательная биометрическая идентификация, применима для укрывателей личностей	ВЛОИ	Подлинное лицо	Обязательное
	ВНиПАУ	Атака	Обязательное
	ДОПБС	Атака или подлинное лицо	Рекомендуемое

Приложение А
(справочное)

Классификация типов атак

А.1 Общие положения

В настоящем приложении представлены классификация и краткое описание известных типов атак на биометрическое предъявление согласно таблице А.1. Целью настоящего приложения является обеспечение структурной оценки мер противодействия атакам. Оценка мер противодействия может быть проведена эмпирически, и может быть получен ответ на вопрос: «Насколько эффективно эта мера противодействия классифицирует атаки?» Оценка мер противодействия на основе известных атак позволяет обосновать заявления о безопасности продукта.

Настоящее приложение не является сборником инструкций по созданию биометрических артефактов. Представлены высокоуровневое описание атак и их классификация, но не следует рассматривать это как исчерпывающий список.

Атаки на биометрическое предъявление подразделяют на две категории: с использованием искусственных ИАБП и с участием человека в ИАБП.

А.2 Использование искусственных инструментов атаки на биометрическое предъявление

А.2.1 Источник биометрических характеристик

Искусственный ИАБП, или артефакт, формируется на основе источника биометрических характеристик (см. таблицу А.1). Биометрические характеристики могут быть записаны или скопированы на искусственные объекты. При таком типе атаки злоумышленник должен иметь доступ к представлению оригинальных биометрических характеристик либо напрямую (совместно или принудительно), либо косвенно на основе следов, изображений или других записей. Предъявление биометрической характеристики ИАБП может быть также синтезировано. Синтезированные данные могут быть сгенерированы несколькими способами:

a) без условия иметь сходство с биометрическими характеристиками человека на основе:
- случайного генерирования элементов биометрических характеристик,
- изменения или объединения существующих биометрических характеристик,
- обратного проектирования методов кодирования без учета сходства с характеристикой субъекта.

Таблица А.1 — Источники биометрических характеристик в атаках на биометрическое предъявление с артефактами

Источник	Описание	Примеры
Сотрудничество	Биометрические характеристики, полученные непосредственно от другого человека с его помощью	Форма лица, форма руки, маска лица
Скрытый	Биометрические характеристики, собранные косвенно со скрытого образца	Скрытый отпечаток пальца, скрытый отпечаток ладони, волосы, кожа, жидкость организма
Запись	Биометрические характеристики, собранные напрямую с индивида на носители информации	Фотография, видеозапись, аудиозапись
Реконструкция из шаблона	Использование информации из шаблона для синтезированной генерации ИАБП	Реконструкция отпечатка пальца [8], реконструкция лица [9] [10], реконструкция радужной оболочки глаза [11]
Имитация	Обработка биометрических характеристик для сходства с биометрическими характеристиками другого индивида с помощью искусственных средств	Преобразование голоса с использованием компьютера
Генерация искусственных шаблонов	Создание ИАБП не на основе биометрических характеристик индивида	Синтезированный отпечаток пальца [12], синтезированная радужная оболочка глаза [6], синтезированное лицо [5], синтезированный голос [13], синтезированный «образец «волка» [14], 3D-скульптура лица

b) с условием иметь сходство с биометрическими характеристиками какого-либо объекта на основе:
- изменения или объединения существующих биометрических характеристик без введения отклонений,
- обратного проектирования методов кодирования с дополнительными ограничениями на результат генерации;

с) с условием иметь сходство с биометрическими характеристиками определенного субъекта с учетом биометрического шаблона на основе обратного проектирования методов кодирования с дополнительными ограничениями на результат генерации.

Атака на биометрическое предъявление с использованием артефакта может не иметь источника биометрической характеристики, особенно если целью является сокрытие личности с помощью маскировки (например, лыжной маски, непрозрачных контактных линз) или создания другой личности (например, макияж, протез), когда не требуются конкретные биометрические характеристики. Генерация синтезированных, но реалистичных биометрических характеристик может быть трудной или невозможной для определенных модальностей, так как для этого требуется набор машинно-программируемых правил, которые определяют характеристики части реального тела человека или реального человеческого поведения.

Процедура создания искусственного ИАБП включает метод производства артефактов, указанный в таблице А.2. По типу использования искусственных биометрических характеристик атаки на биометрическое предъявление можно классифицировать на статические и динамические.

В статических атаках на биометрическое предъявление артефакты используют как статические объекты, которые не эмулируют поведенческие аспекты, связанные с биометрической характеристикой. Статические атаки на биометрическое предъявление включают, но не ограничиваются следующими примерами:

- атака с использованием распечатки 2D. Данная атака состоит из демонстрации распечатки характеристики (например, бумаги, слайда, контактных линз) на входном датчике. Атака является наиболее вероятной для реализации по двум причинам:

- экономичный способ сделать или заказать распечатки (например, лица, радужной оболочки глаз или вен). Если требования к разрешению распечатки (например, при распознавании лиц) отсутствуют, может оказаться достаточным отображать фотографии на экранах смартфонов или портативных компьютерах,

- с появлением цифровой фотографии и обмена социальными изображениями (Flickr, Facebook, Google Photos и др.) фотографии головы человека становятся более легкодоступными и потенциально могут быть использованы для атаки систем распознавания лиц,

- атака с использованием 3D-объекта. Данная атака требует большего количества навыков и, возможно, доступа к дополнительным материалам, которые должны быть хорошо выполнены, так как необходимо сконструировать приблизительный трехмерный прототип. Атаки с использованием 3D-объектов включают, но не ограничиваются следующими примерами:

- форма/муляж: создается негатив биометрической характеристики (форма), который(ую) используют для формирования искусственного воссоздания биометрической характеристики (муляжа), например искусственного пальца или лицевой театральной маски,

- печать на 3D-объекте, например печать конфигурации вены на протезе руки,

- гравировка на 3D-объекте, например отпечаток пальца, гравированный на металле,

- маска: сокрытие биометрических характеристик артефактом частично или полностью, например накладные волосы на лице, лыжная маска, косметика.

В отличие от статических предъявлений динамические атаки на биометрическое предъявление имитируют поведение, связанное с оригинальными биометрическими характеристиками. Динамические атаки на биометрическое предъявление включают, но не ограничиваются следующими примерами:

- видеоатаки с помощью мобильных телефонов, планшетов или ноутбуков. С введением признаков жизнеспособности данные атаки увеличивают вероятность результата атаки. Системы, которые не оказывают противодействия фотографическим атакам, будут функционировать еще хуже в отношении видеоатак. Получение биометрических изображений становится гораздо более простым с появлением публичных сайтов обмена видео и одновременным снижением цен на высококачественные камеры;

- атаки воспроизведения, в которых оригинальная речь субъекта сбора воспроизводится с изменением или без изменения в той же биометрической системе.

Артефакты, указанные в таблице А.2, могут иметь биометрические характеристики из источников, приведенных в таблице А.1, или не иметь биометрических характеристик (например, лыжная маска).

Таблица А.2 — Производство артефактов для атак на биометрическое предъявление

Тип атаки	Артефакт	Описание	Примеры
Статическая физическая репродукция	Муляж (двухэтапный процесс «форма/муляж»)	Формовка — 3D-представление биометрических характеристик	Форма лица, собранная у дублера; форма пальца, собранная с использованием стоматологического материала, формовочного пластика, глины для лепки, печатной монтажной платы [15], печатного слайда

Окончание таблицы А.2

Тип атаки	Артефакт	Описание	Примеры
Статическая физическая репродукция	Муляж (двухэтапный процесс «форма/муляж»)	Отливка — воссоздание из формы	Театральная маска лица, имитация пальца из глины для лепки, желатина [15], [16], силикона [15], латекса, столярного клея, глицерина [7], материалов на основе смолы
	Прямое воспроизведение	2D-печать	Радужная оболочка глаза [17], [18], лицо, отпечаток пальца [18], рисунок вен, рука, напечатанная на слайде или бумаге
		3D-печать	Контактные линзы с напечатанным рисунком, протез руки с нарисованной конфигурацией вен
		Гравировка	Отпечаток пальца, выгравированный на металле
		Рисование — шаблоны и цвета, рисуемые на протезе	Протез окуляра с нарисованным шаблоном радужной оболочки глаза [4], протез руки с нарисованной конфигурацией вен
	Маска	Измененные или сокрытые биометрические характеристики (частично или полностью) с использованием артефакта	Клей на пальце, накладные волосы на голове, косметика, удаляемые импланты, непрозрачные линзы, лыжная маска, карнавальная маска, макияж
Динамическое содержимое	Вычислительное устройство	Ноутбук или планшет для демонстрации изображения или видео	Изображение лица или радужной оболочки глаза, видео лица или радужной оболочки глаза
	Плеер временных рядов	Запись временных рядов	Запись голоса, регистрация ручной подписи с использованием цифрового планшета, регистрация электрофизиологических сигналов (например, ЭЭГ)
Генерация синтезированных шаблонов	—	Создание синтезированных биометрических характеристик, возможно не привязанных к реальному человеку или не похожих на любые биометрические характеристики	Синтезированный отпечаток пальца [12], синтезированная радужная оболочка глаза [6], синтезированное лицо [5], синтезированный голос [13], синтезированный образец «волка» [14], 3D-скульптура лица

А.3 Участие человека (физических характеристик или поведения)

Участие человека в ИАБП для атак на биометрическое предъявление может быть классифицировано следующим образом:

- неодушевленные образцы. В данном типе атаки используют неживые части человеческого тела;
- изменение биометрических характеристик. Данный тип атаки проводится субъектом сбора биометрических данных с использованием образца из модифицированной, но оригинальной биометрической характеристики;
- несогласованная имитация и/или сокрытие биометрических характеристик. Данный тип атаки проводится

субъектом сбора биометрических данных, который стремится быть распознанным как конкретный субъект сбора или как субъект сбора, который не распознается биометрической системой. Злоумышленник может подделывать биометрические характеристики на основе полного или частичного знания об оригинальных биометрических характеристиках;

- принудительное использование биометрических характеристик. В данном типе атаки оригинальные биометрические характеристики (поведения или части тела) использованы под принуждением. Вероятно, это самый сложный тип атаки для автоматического обнаружения ввиду ограниченных возможностей биометрии количественно описать влияние принуждения на части организма и поведение. Хотя конкретная зарегистрированная биометрическая характеристика может быть обозначена индикатором принуждения (например, один конкретный палец), это можно обнаружить только на уровне системы, а не на уровне биометрического сканера. Обнаружение атак данного типа на системном уровне не рассматривается в настоящем стандарте;

- совместимая атака. Данная атака соответствует попытке самозванца с нулевым усилием.

В таблице А.3 описаны и приведены примеры атак на биометрическое предъявление с использованием организма или поведения человека.

Таблица А.3 — Атаки на биометрическое предъявление с участием человека

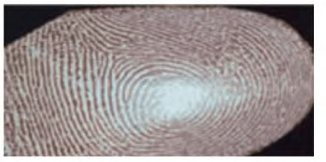
Биометрические характеристики	Изменение	Описание	Примеры
Неживые	—	Использование частей организма человека или трупа	Мертвый палец, мертвая рука, мертвый глаз
Измененные	Повреждение	Разрушение биометрических характеристик	Рубцевание, ампутация, использование кислоты, истирание папиллярного узора
	Хирургическое преобразование	Умышленное преобразование биометрических характеристик	Замена папиллярного узора, коррекция носа, подтяжка лица
	Медикаментозно индуцированное	Временное преобразование биометрических характеристик ввиду лекарств или болезни	Наркотическое расширение или спазм зрачков
Несовместимые	Имитация	Попытка имитировать биометрические характеристики другого человека без использования артефакта	Подражание голосу, поддельная подпись
	Предъявление	Использование попытки несогласованного сбора для преобразования биометрических характеристик	Контроль формы руки, выражение лица/чрезмерность, кончик или сторона пальца, аномальная походка
Принудительные	—	Использование биометрических характеристик под принуждением	Принудительное или бессознательное использование настоящей радужной оболочки глаза или отпечатков пальцев
Совместимые	—	Попытка самозванца с нулевым усилием	Подлинные биометрические предъявления, которые могут пройти сравнение с другим индивидом

Приложение В
(справочное)

Примеры видов артефактов, используемых в оценке подсистем обнаружения атаки на биометрическое предъявление для биометрических сканеров отпечатков пальцев

Согласно 3.1.6 все артефакты определенного вида ИАБП производят одним и тем же способом производства (т. е. инструкцией). Набор ИАБП для оценки биометрических сканеров отпечатков пальцев может включать минимальный набор видов артефактов, представленный в таблице В.1.

Таблица В.1 — Виды артефактов для оценки подсистем ОАБП устройств сбора биометрических данных отпечатков пальцев [19]

Вид артефакта	Описание	Иллюстрация
Силиконовый палец	Матовый или глянцевый	
Палец, полученный лазерной печатью	Обычная 2D-распечатка	
Палец из желатина	Полупрозрачный желатин с глицерином	

Приложение ДА
(справочное)

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

Таблица ДА.1

Обозначение ссылочного национального, межгосударственного стандарта	Степень соответствия	Обозначение и наименование соответствующего международного стандарта
ГОСТ ISO/IEC 2382-37—2016	IDT	ISO/IEC 2382-37:2012 «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»
ГОСТ Р ИСО/МЭК 19795-1—2007	IDT	ISO/IEC 19795-1:2006 «Информационные технологии. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура»
ГОСТ Р 58624.1—2019	MOD	ISO/IEC 30107-1:2016 «Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 1. Структура»
Примечание — В настоящей таблице использованы следующие условные обозначения степени соответствия стандартов: - IDT — идентичные стандарты; - MOD — модифицированные 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 30107-3:2017
Приложение ДА Сведения о соответствии ссылочных национальных и межгосударственных стандартов международным стандартам, использованным в качестве ссылочных в применяемом 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 (за исключением предисловия) идентичны.	

Библиография

[1] *Н.М. Костылев, А.В. Горевой «Модуль обнаружения витальности лица по спектральным характеристикам отражения кожи человека». Инженерный журнал: «Наука и инновации», 2013, вып. 9.* gost.e-ecolog.ru *ru/catalog/pribor/optica/925.html*

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

[3] Marcialis G.L., Lewicke A., Tan B., Coli P., Grimberg D., Congiu A. First International Fingerprint Liveness Detection Competition — LivDet 2009, gost.e-ecolog.ru

[4] Une M., Otsuka A., Imai H. Wolf attack probability: a new security measure in biometric authentication systems. In: Advances in Biometrics, 2007, pp. 396—406

[5] Barral C., & Tria A. Fake fingers in fingerprint recognition: glycerin supersedes gelatin. In: Formal to Practical Security, Vol. 5458, Springer Berlin, Heidelberg, 2009, pp. 57—69

[6] Lefohn A., Budge B., Shirley P., Caruso R., Reinhard E. An ocularist's approach to human iris synthesis. IEEE Comput. Graph. Appl. 2003, pp. 70—75

[7] gost.e-ecolog.ru

[8] Matsumoto T., Matsumoto H., Yamada K., Yoshino S. Impact of Artificial «Gummy» Fingers on Fingerprint Systems, Proc. Of SPIE, Optical Security and Counterfeit Deterrence Techniques IV, Vol. 4677, January 2002, pp. 275—289

[9] Cappelli R., Maio D., Maltoni D., Erol A. «Synthetic fingerprint-image generation», 15th International Conference on Pattern Recognition, Vol. 3, pp. 471—474, 2000

[10] Bunnell H.T., Pennington C., Yarrington D., Gray J. «Automatic personal synthetic voice construction», Ninth European Conference on Speech Communication and Technology, 2005

[11] Adler A. «Can Images be Regenerated from Biometric Templates?», Biometrics Conference, Vol. 1, Sept. 22—24, 2003

[12] Saintourens M., Tramus M.H., Huitric H., Nahas M. «Creation of a synthetic face speaking in real time with a synthetic voice», The ESCA Workshop on Speech Synthesis, 1991

[13] Makthal S., & Ross A. «Synthesis of iris images using Markov random fields», Proc. 13th European Signal Processing Conf, 2005

[14] Zwiesele A., Munde A., Busch C., Daum H. Comparative Study of Biometric Identification Systems, in: 34th Annual 2000 IEEE International Carnahan Conference on Security Technology, Ottawa, pp. 60—63, (2000)

[15] Pacut A., & Czajka A. «Aliveness detection for iris biometrics», 2006 IEEE International Carnahan Conference on Security Technology, 40th Annual Conference, October 17-19, Lexington, Kentucky, IEEE 2006

[16] Thalheim L., Krissler J., Ziegler P.-M. «Body Check Biometric Access Protection Devices and their Programs Put to the Test», gost.e-ecolog.ru course/EDA263/oh10/L03_DL2_Biometric%20access%20protection%20devices.pdf

[17] Fingerprint Spoof Detection Protection Profile (FSDPP) v1.8

[18] Fingerprint Spoof Detection Evaluation Guidance, Version 2.1, 2009-12-18

[19] Stein C., Bouatou V., Busch C. «Video-based Fingerphoto Recognition with Anti-spoofing Techniques with Smartphone Cameras», in Proceedings of the IEEE 12th International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, September 5-6, (2013), available online at gost.e-ecolog.ru Stein-VideoFingerphoto-BIOSIG-2013.pdf

УДК 004.93'1:006.89:006.354 ОКС 35.240.15

Ключевые слова: информационные технологии, атака на биометрическое предъявление, инструмент атаки на биометрическое предъявление, испытания биометрической системы, протоколы испытаний

БЗ 12—2019/110

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

Сдано в набор 25.11.2019. Подписано в печать 27.12.2019. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 4,18. Уч.-изд. л. 3,55.
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