ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 71414.1— 2024 (ИСО/МЭК 19795-1:2021)

Информационные технологии

БИОМЕТРИЯ

Эксплуатационные испытания и протоколы испытаний в биометрии

Часть 1

Принципы и структура

(ISO/IEC 19795-1:2021, Information Technology — Biometric performance testing and reporting — Part 1: Principles and framework, MOD)

Издание официальное

Москва
Российский институт стандартизации
2024

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Некоммерческим партнерством «Русское общество содействия развитию биометрических технологий, систем и коммуникаций» (Некоммерческое партнерство «Русское биометрическое общество») и Федеральным государственным бюджетным учреждением «Российский институт стандартизации» (ФГБУ «Институт стандартизации») на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

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 30 сентября 2024 г. № 1323-ст

4 Настоящий стандарт является модифицированным по отношению к международному стандарту ИСО/МЭК 19795-1:2021 «Информационные технологии. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура» (ISO/IEC 19795-1:2021 «Information technology — Biometric performance testing and reporting — Part 1: Principles and framework», MOD) путем изменения ссылок, исключения отдельных положений, которые дублируются по тексту стандарта, исключения из библиографии информации о документах, ссылки на которые не использованы при изложении настоящего стандарта, дополнения сносок, примечаний и сокращений, которые необходимы для понимания настоящего стандарта и выделены в тексте курсивом.

Внесение указанных технических отклонений направлено на учет целесообразности использования ссылочных национальных стандартов вместо ссылочных международных стандартов. При этом дополнительные ссылки выделены в тексте курсивом.

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 приложении ДА

5 ВЗАМЕН ГОСТ Р ИСО/МЭК 19795-1—2007

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, 2021
© IEC, 2021
© Оформление. ФГБУ «Институт стандартизации», 2024

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

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Сокращения 5
5 Соответствие 5
6 Биометрическая система общего вида 5
7 Планирование испытания 12
8 Сбор данных 18
9 Анализ 26
10 Графическое представление результатов 37
11 Хранение записей 43
12 Протоколы эксплуатационных испытаний 44
Приложение А (справочное) Различия между видами испытаний 49
Приложение В (справочное) Объем испытаний и случайная неопределенность 51
Приложение С (справочное) Факторы, влияющие на эксплуатационные характеристики биометрических систем 57
Приложение D (справочное) Эксплуатационные характеристики алгоритма предварительного отбора 61
Приложение Е (справочное) Идентификационные эксплуатационные характеристики как функция размера базы данных 63
Приложение F (справочное) Алгоритмы получения данных для графиков КОО и ХСС 64
Приложение G (справочное) Интерпретация графика КОО 67
Приложение ДА (справочное) Сведения о соответствии ссылочного межгосударственного стандарта международному стандарту, использованному в качестве ссылочного в примененном международном стандарте 70
Библиография 71

Введение

Настоящий стандарт устанавливает требования к эксплуатационным испытаниям и протоколам испытаний в области биометрии. Эксплуатационные испытания направлены на определение вероятностей появления ошибок и показателей пропускной способности с целью понимания и прогнозирования реальных ошибок и пропускной способности биометрических систем. Вероятности ошибок включают в себя как ложноположительные, так и ложноотрицательные вероятности, а также вероятность отказа биометрической регистрации (ВОР) и вероятность отказа сбора данных (ВОСД) по всей целевой выборке. Показатели пропускной способности устанавливают число пользователей, подвергаемых анализу в единицу времени, зависящее от скорости вычислений и взаимодействия пользователя с биометрической системой. Эти измерения, как правило, применимы ко всем биометрическим системам и устройствам. В настоящем стандарте не установлены технические эксплуатационные испытания, зависящие от конкретной модальности (например, качество изображения биометрического сканера отпечатков пальцев).

Целью настоящего стандарта является установление методов технических эксплуатационных испытаний и требований к подготовке протоколов испытаний, соответствующих передовому международному опыту. Технические эксплуатационные испытания — это одна из форм испытаний в биометрии. Другие виды испытаний, на которые не распространяется настоящий стандарт, включают следующие аспекты:

- надежность, доступность и ремонтопригодность;
- защиту, в том числе уязвимость;
- соответствие;
- безопасность;
- человеческий фактор, в том числе степень принятия пользователем;
- затраты/выгоды;
- соблюдение правил конфиденциальности.

Технические эксплуатационные испытания в биометрии могут быть трех видов: технологическое, сценарное и оперативное. Для каждого вида испытаний требуются отдельный протокол и предоставление результатов разных типов. Другие части серии стандартов под общим наименованием *«Информационные технологии. Биометрия. Эксплуатационные испытания и протоколы испытаний в биометрии»* содержат конкретные рекомендации и устанавливают требования к разработке и использованию разных протоколов испытаний. В настоящем стандарте установлены основные положения и принципы, которые рекомендуется применять в широком диапазоне условий испытаний.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

БИОМЕТРИЯ

Эксплуатационные испытания и протоколы испытаний в биометрии

Часть 1

Принципы и структура

Information technology. Biometrics. Biometric performance testing and reporting. Part 1. Principles and framework

Дата введения — 2025—01—01

1 Область применения

Настоящий стандарт устанавливает:

- общие требования к проведению эксплуатационных испытаний биометрических систем в отношении определения вероятности появления ошибок и пропускной способности, используемых для измерения, прогнозирования и сравнения эксплуатационных характеристик систем, а также для проверки их соответствия установленным эксплуатационным требованиям;
- эксплуатационные характеристики биометрических систем;
- требования к записи данных испытаний и форме представления результатов испытаний;
- требования к протоколам испытаний для того, чтобы:
  - уменьшить систематические ошибки, обусловленные несоответствующими процедурами сбора и анализа данных,
  - более точно оценить результаты эксплуатационных испытаний в соответствии с уровнем затраченных усилий,
  - уточнить область применения результатов испытаний.

Настоящий стандарт распространяется на эмпирические эксплуатационные испытания биометрических систем и алгоритмов на основании анализа результатов сравнения и решений, выдаваемых системой, без детальной информации об алгоритмах системы или о законе распределения биометрических характеристик целевой выборки.

Настоящий стандарт не устанавливает:

- принципы и методы оценки эксплуатационных характеристик методов обнаружения атак на биометрическое предъявление;
- требования к протоколу результатов испытаний методов обнаружения атак на биометрическое предъявление*.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

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

---

* *Требования к испытанию методов обнаружения атак на биометрическое предъявление установлены в ГОСТ Р 58624.3—2019 (ИСО/МЭК 30107-3:2017) «Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 3. Испытания и протоколы испытаний».*

Издание официальное

ГОСТ Р 54411/ISO/IEC TR 24722:2015 Информационные технологии. Биометрия. Мультимодальные и другие мультибиометрические технологии

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен 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*, а также следующие термины с соответствующими определениями:

3.1 **испытуемый субъект** (test subject): Физическое лицо, биометрические персональные данные которого будут регистрироваться или подвергаться сравнению при испытании.

3.2 **испытуемая группа** (test crew): Множество испытуемых субъектов, участвующих в испытании.

3.3 **целевая выборка** (target population): Группа пользователей системы, для которых происходит оценка эксплуатационных характеристик.

3.4 **испытательная лаборатория** (test organization): Организация, в которой проводят испытания.

3.5 **экспериментатор** (experimenter): Ответственное лицо, несущее ответственность за описание, разработку и анализ испытания.

3.6 **администратор испытания** (test administrator): Ответственное лицо, проводящее испытание.

Пример — Персонал, проводящий биометрическую регистрацию или наблюдающий за транзакциями биометрической верификации или идентификации.

3.7 **наблюдатель за испытанием** (test observer): Ответственное лицо, записывающее данные испытания или наблюдающий за испытуемой группой.

3.8 **попытка биометрической регистрации** (enrolment attempt): Последовательность из одной или нескольких попыток сбора биометрических данных с целью получения биометрического контрольного шаблона испытуемого субъекта.

Примечание — Попытка биометрической регистрации может потребовать определенного количества попыток сбора биометрических данных (например, трех отдельных размещений пальца на датчике в течение заданного периода), из которых выбирают биометрический(е) образец(ы) самого высокого качества для дальнейшей обработки.

3.9 **транзакция биометрической регистрации** (enrolment transaction): Одна или несколько попыток биометрической регистрации с целью получения биометрического контрольного шаблона испытуемого субъекта.

Примечание — Если попытка биометрической регистрации не удалась, то дальнейшие попытки биометрической регистрации могут быть выполнены в рамках той же транзакции биометрической регистрации до тех пор, пока попытка не будет результативной или биометрическая регистрация не будет прекращена.

3.10 **транзакция идентификации** (identification transaction): Последовательность из одной или нескольких попыток сбора биометрических данных и биометрического поиска соответствующего контрольного шаблона, который может относиться к данному испытуемому субъекту.

3.11 **эффект канала передачи** (channel effect): Изменение биометрического образца вследствие дискретизации, помех и особенностей амплитудно-частотных характеристик датчика и канала передачи.

3.12 **эффект предъявления** (presentation effect): Изменение биометрического образца вследствие особенностей предъявления биометрических характеристик датчику.

Пример — При биометрическом распознавании лиц такими эффектами являются угол расположения испытуемого субъекта и освещение; при распознавании отпечатков пальцев — поворот пальца и влажность кожи. Во многих случаях различие между изменениями основных биометрических характеристик и эффектом предъявления может быть неявным (например, выражение лица при распознавании лиц или изменение высоты звука в биометрических системах верификации диктора).

3.13 **технологическое испытание** (technology evaluation): Испытание одного или более одного алгоритма распознавания одинаковых биометрических модальностей с использованием существовавшей ранее или специально собранной базы данных биометрических образцов в режиме отложенного задания.

3.14 **сценарное испытание** (scenario evaluation): Испытание, при проведении которого эксплуатационные характеристики системы определяются с помощью прототипа или имитирующего приложения при участии испытуемой группы.

3.15 **оперативное испытание** (operational evaluation): Испытание, в котором эксплуатационные характеристики биометрической системы определяются в специальных условиях эксплуатации по специальной целевой выборке.

3.16 **режим реального времени** (online): Режим испытания, при котором биометрическая регистрация или сравнение выполняется непосредственно после процесса сбора биометрических данных.

3.17 **режим отложенного задания** (offline): Режим испытания, при котором биометрическая регистрация или сравнение выполняются на заранее сохраненных биометрических данных и не связаны с процессом сбора биометрических данных.

Примечание — Сбор базы данных изображений или сигналов для биометрической регистрации и вычисления результатов сравнения в режиме отложенного задания позволяет более эффективно осуществлять контроль того, какие биометрические пробы или биометрические контрольные шаблоны следует использовать для каждой транзакции.

3.18 **испытание на замкнутом множестве** (closed-set test): Испытание, в котором испытуемая группа состоит только из субъектов, зарегистрированных в базе данных.

Примечание — Испытания на замкнутом множестве — это особый вид испытаний для представления эксплуатационных характеристик биометрической системы идентификации в виде графика характеристики совокупного совпадения (ХСС).

3.19 **отказ сбора данных** (failure to acquire): Отказ создания биометрического образца, пригодного для последующего сравнения.

3.20 **вероятность ложного недопуска**; ВЛНД (false reject rate; FRR): Доля биометрических транзакций с подлинными биометрическими заявлениями, которые были ошибочно отклонены, от общего числа биометрических транзакций с подлинными биометрическими заявлениями.

3.21 **вероятность ложного допуска**; ВЛД (false accept rate; FAR): Доля транзакций с ложными биометрическими заявлениями, которые были ошибочно приняты, от общего числа транзакций с ложными биометрическими заявлениями.

3.22 **вероятность ложноотрицательной биометрической идентификации;** ВЛОИ; ВЛОИ (N, R, T) [false-negative identification rate; FNIR; FNIR (N, R, T)]: Доля транзакций биометрической идентификации испытуемых субъектов, зарегистрированных в системе, в результате которых среди возвращаемых идентификаторов отсутствует правильный идентификатор субъекта, от общего числа транзакций биометрической идентификации испытуемых субъектов, зарегистрированных в системе.

Примечание — ВЛОИ может быть выражена как функция от числа зарегистрированных в системе испытуемых субъектов N, а также от параметров процесса биометрической идентификации: ранга R, определяющего количество возвращаемых идентификаторов, и порога принятия решения T, которому должны удовлетворять возвращаемые идентификаторы.

3.23 **вероятность ложноположительной биометрической идентификации;** ВЛПИ; ВЛПИ (N, T) [false-positive identification rate; FPIR; FPIR (N, T)]: Доля транзакций биометрической идентификации незарегистрированных в системе испытуемых субъектов, в результате которых возвращается идентификатор, от общего числа транзакций биометрической идентификации незарегистрированных в системе испытуемых субъектов.

Примечания

1 ВЛПИ может быть выражена как функция от числа зарегистрированных в системе испытуемых субъектов N, а также от порога принятия решения T, которому должны удовлетворять возвращаемые идентификаторы.

2 Для тех систем, которые неизменно возвращают фиксированное число кандидатов без применения порога принятия решения для оценок, ВЛПИ не является значимым показателем.

3.24 **ранг идентификации** (rank): Наименьшее значение *k*, для которого правильный идентификатор испытуемого субъекта находится в первых *k* идентификаторах, возвращенных биометрической системой идентификации.

Примечание — Ранг идентификации зависит от размера регистрационной базы данных и должен быть приведен как «ранг k из n».

3.25 **вероятность истинно положительной идентификации;** ВИПИ; ВИПИ (*N*, *R*, *T*) [true-positive identification rate; TPIR; TPIR (*N*, *R*, *T*)]: Доля транзакций биометрической идентификации зарегистрированных в системе испытуемых субъектов, в которых правильный идентификатор субъекта возвращается в ранге *R* или выше, от общего числа транзакций биометрической идентификации зарегистрированных в системе испытуемых субъектов.

Примечания

1 ВИПИ может быть выражена как функция от числа зарегистрированных в системе испытуемых субъектов *N*, а также от параметров процесса биометрической идентификации: ранга *R*, определяющего количество возвращаемых идентификаторов, и порога принятия решения *T*, которому должны удовлетворять возвращаемые идентификаторы.

2 Сумма ВИПИ (*N*, *R*, *T*) и ВЛОИ (*N*, *R*, *T*) для одного и того же ранга, порога и числа зарегистрированных испытуемых субъектов в системе равна 1.

3.26 **селективность;** СЕЛ (*N*, *R*, *T*) [selectivity; SEL (*N*, *T*)]: Среднее количество возвращаемых кандидатов, удовлетворяющих порогу принятия решения *T*, при непарном поиске.

Примечания

1 Селективность может быть выражена как функция от числа зарегистрированных в системе испытуемых субъектов *N*, а также от параметров процесса биометрической идентификации: ранга *R*, определяющего количество возвращаемых идентификаторов, и порога принятия решения *T*, которому должны удовлетворять возвращаемые идентификаторы.

2 Если ранг *R* равен числу зарегистрированных испытуемых субъектов *N*, то селективность измеряют по всей базе данных.

3.27 **вычислительная нагрузка** (computational workload): Общие вычислительные затраты на одну транзакцию (или набор транзакций) в биометрической системе, включая количество внутренних операций, время выполнения, требования к памяти и т. д.

Примечание — Вычислительная нагрузка зависит от аппаратного обеспечения, на котором работает биометрическая система.

3.28 **компромиссное определение ошибки;** КОО (detection error trade-off; DET): Соотношение между ложноположительными и ложноотрицательными ошибками бинарной классификационной системы при изменении порога принятия решения.

Примечания

1 КОО может быть представлено в виде таблицы КОО или графика КОО.

2 В предыдущей версии настоящего стандарта использовалась кривая рабочей характеристики (РХ). РХ соответствует КОО.

3.29 **график характеристики совокупного совпадения;** график ХСС (cumulative match characteristic plot; CMC plot): Графическое представление результатов испытаний на замкнутом множестве, на котором по оси *X* откладывают значения ранга, а по оси *Y* — вероятность биометрической идентификации при каждом ранге.

3.30 **алгоритм предварительного отбора** (pre-selection algorithm): Алгоритм, позволяющий сократить число необходимых сравнений при идентификационном поиске по регистрационной базе данных.

3.31 **ошибка предварительного отбора** (pre-selection error): Ошибка алгоритма предварительного отбора, заключающаяся в отсутствии соответствующего идентификатора испытуемого субъекта в предварительно отобранной подгруппе кандидатов.

Примечание — В предварительном отборе с использованием исключительной классификации ошибка предварительного отбора возникает в том случае, если зарегистрированный биометрический контрольный шаблон

испытуемого субъекта и последующий биометрический образец той же биометрической характеристики находятся в разных подгруппах.

3.32 **степень проникновения** (penetration rate): Характеристика алгоритма предварительного отбора, являющаяся долей числа предварительно отобранных биометрических контрольных шаблонов от общего числа биометрических контрольных шаблонов.

3.33 ***вероятность ложного несовпадения;*** *ВЛНС (false non-match rate; FNMR): Доля завершенных попыток биометрического парного сравнения, приведших к ложному несовпадению, от общего числа завершенных попыток биометрического парного сравнения.*

3.34 ***вероятность ложного совпадения;*** *ВЛС (false match rate; FMR): Доля завершенных попыток биометрического непарного сравнения, приведших к ложному совпадению, от общего числа завершенных попыток биометрического непарного сравнения.*

3.35 ***вероятность ложноположительной биометрической идентификации;*** *ВЛПИ; ВЛПИ (N, T) [false-positive identification rate; FPIR; FPIR (N, T)]: Доля транзакций биометрической идентификации незарегистрированных в системе испытуемых субъектов, в результате которых возвращается идентификатор, от общего числа транзакций биометрической идентификации незарегистрированных в системе испытуемых субъектов.*

Примечание — ВЛПИ может быть выражена как функция от числа зарегистрированных в системе испытуемых субъектов N, а также от порога принятия решения T, которому должны удовлетворять возвращаемые идентификаторы.

4 Сокращения

В настоящем стандарте применены следующие сокращения:

ВОР — вероятность отказа биометрической регистрации;
ВОСД — вероятность отказа сбора данных;
КПО — комплект программного обеспечения;
ОВЛД — обобщенная вероятность ложного допуска;
ОВЛНД — обобщенная вероятность ложного недопуска;
ПИН — персональный идентификационный код;
ПИП — программный интерфейс приложений;
ПОВО — половина общей вероятности ошибок;
РВО — равная вероятность ошибок;
РОГ — радужная оболочка глаза.

5 Соответствие

Эксплуатационные испытания в биометрии, претендующие на соответствие настоящему стандарту, необходимо планировать, выполнять и представлять их результаты в соответствии со всеми обязательными требованиями, установленными в настоящем стандарте.

6 Биометрическая система общего вида

6.1 Схема концептуального представления биометрической системы общего вида

Из многообразия биометрических приложений и технологий можно сделать некое обобщение биометрических систем. Во всех биометрических системах присутствуют общие элементы. Биометрические образцы испытуемого субъекта регистрируют с помощью биометрических сканеров. Данные с биометрического сканера передают в устройство обработки, которое извлекает отличительные, но повторяющиеся характеристики биометрического образца (его биометрические признаки) и отбрасывает все прочие элементы. Выделенные таким образом биометрические признаки записывают в базу данных в виде биометрического контрольного шаблона. В некоторых случаях биометрический образец (без выделения биометрических признаков) может быть записан в базу данных в виде биометрического контрольного шаблона. Последующий биометрический запрос или биометрическую пробу сравнивают с отдельным биометрическим контрольным шаблоном, с несколькими биометрическими контрольными

шаблонами или со всеми биометрическими контрольными шаблонами, хранящимися в базе данных, для определения соответствия. Решение о подтверждении биометрического заявления выносят на основании оценки степени схожести или различия биометрических признаков пробы и биометрических признаков биометрического контрольного шаблона или шаблонов, с которыми сравнивают данную биометрическую пробу.

На рисунке 1 показаны информационные потоки биометрической системы общего вида, которая состоит из подсистем сбора биометрических данных, обработки сигнала, хранения данных, сравнения и принятия решения. Данная схема показывает процесс биометрической регистрации и работу биометрических систем верификации и идентификации. В следующих разделах настоящего стандарта каждая из перечисленных подсистем описана более подробно. Следует отметить, что в любой реально действующей биометрической системе некоторые из представленных концептуальных компонентов могут отсутствовать или не соответствовать в точности реальным физическим компонентам или программному обеспечению.

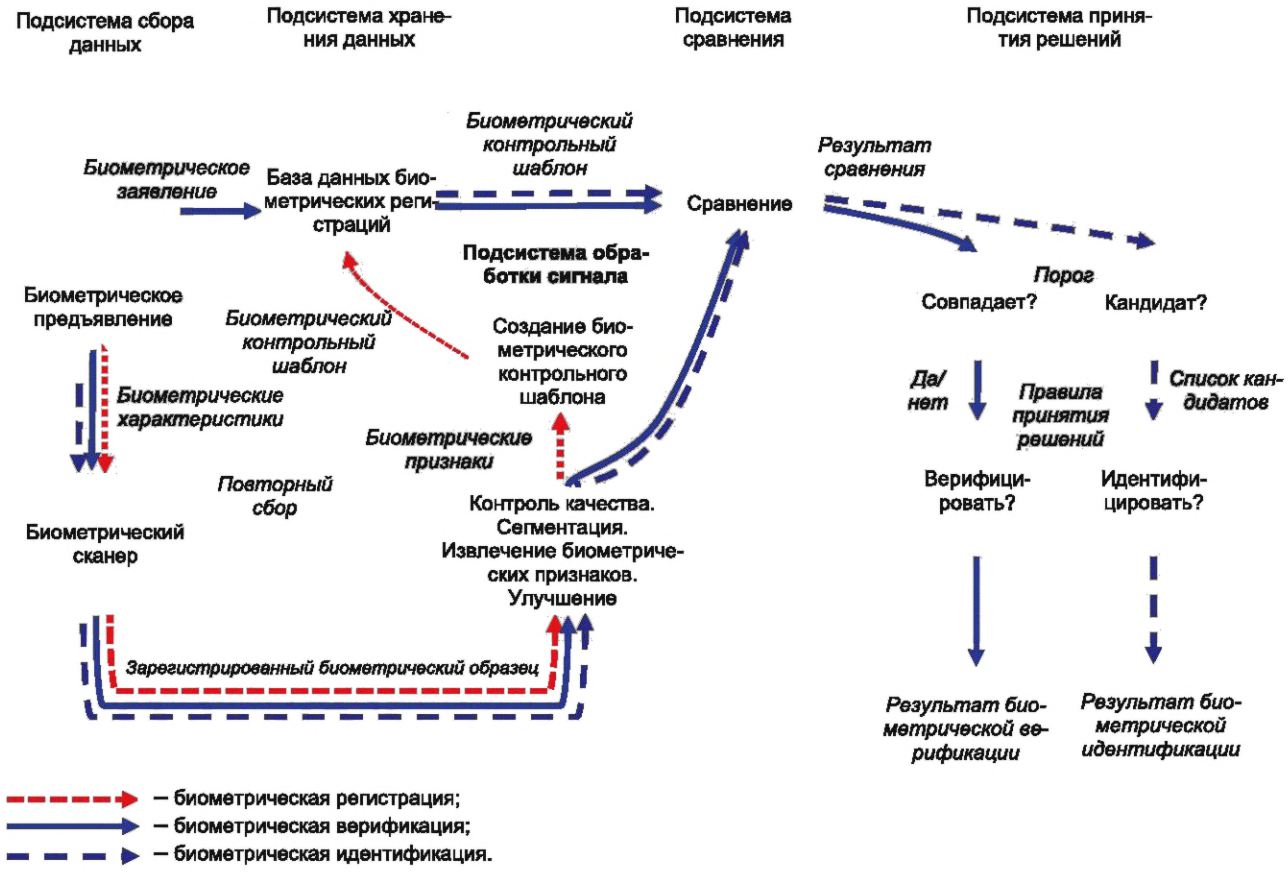

Рисунок 1 — Компоненты биометрической системы общего вида

6.2 Концептуальные компоненты биометрической системы общего вида

6.2.1 Подсистема сбора данных

Подсистема сбора данных получает с биометрического сканера биометрические характеристики испытуемого субъекта в виде изображения или сигнала и выводит изображение/сигнал в виде зарегистрированного биометрического образца.

6.2.2 Подсистема передачи данных

Примечание — На рисунке 1 подсистема передачи данных не приведена.

Подсистема передачи данных, которая не всегда присутствует или явно представлена в биометрической системе, осуществляет передачу биометрических образцов, биометрических признаков, биометрических контрольных шаблонов, результатов сравнения и итоговых результатов между различными подсистемами биометрической системы. Зарегистрированный биометрический образец может

быть подвержен сжатию и/или шифрованию перед передачей и распакован и/или дешифрован перед использованием. В процессе передачи зарегистрированный биометрический образец может изменяться из-за помех в канале передачи данных или из-за потерь при сжатии и распаковке. Данные могут быть переданы с использованием стандартных форматов обмена, а для обеспечения подлинности, целостности и конфиденциальности записанных и передаваемых биометрических персональных данных требуется использовать методы защиты информации в соответствии с требованиями национального законодательства.

6.2.3 Подсистема обработки сигнала

Обработка сигнала включает следующие процессы:

- улучшение, т. е. повышение качества и четкости зарегистрированного биометрического образца;
- сегментацию, т. е. локализацию сигнала, содержащего биометрические характеристики испытуемого субъекта, внутри зарегистрированного биометрического образца;
- извлечение биометрических признаков, т. е. получение повторяющихся и отличительных показателей испытуемого субъекта из зарегистрированного биометрического образца;
- контроль качества, т. е. оценку пригодности биометрических образцов, биометрических признаков, биометрических контрольных шаблонов и возможное влияние других процессов, например: возвращение управления подсистеме сбора данных для последующего сбора биометрических образцов (повторного сбора данных) или изменение параметров сегментации, извлечения биометрических признаков или сравнения.

В процессе биометрической регистрации подсистема обработки сигнала создает биометрический контрольный шаблон. В некоторых случаях для процесса биометрической регистрации от испытуемого субъекта может потребоваться несколько предъявлений биометрических характеристик. В случае, когда биометрический контрольный шаблон содержит только биометрические признаки, его именуют шаблоном. В случае, когда биометрический контрольный шаблон содержит только биометрический образец, извлечение биометрических признаков из биометрического контрольного шаблона происходит непосредственно перед сравнением.

В случае биометрической верификации и идентификации подсистема обработки сигнала создает биометрическую пробу.

Последовательность и итерация вышеупомянутых процессов определены спецификой каждой биометрической системы.

6.2.4 Подсистема хранения данных

Биометрические контрольные шаблоны хранят в регистрационной базе данных, являющейся частью подсистемы хранения данных. Каждый биометрический контрольный шаблон должен быть связан с определенным зарегистрированным испытуемым субъектом или процессом биометрической регистрации. Перед сохранением в регистрационную базу данных биометрические шаблоны могут быть преобразованы в формат обмена. Биометрические контрольные шаблоны допускается хранить на самом устройстве сбора данных, на переносном носителе (например, смарт-карте), локально на персональном компьютере или сервере, в центральной базе данных или в «облаке».

6.2.5 Подсистема сравнения

Подсистема сравнения выполняет сравнение биометрических проб с одним или несколькими биометрическими контрольными шаблонами и передает подсистеме принятия решений результат сравнения. Результаты сравнения определяют степени схожести или различия между сравниваемыми биометрическими пробами и биометрическим(и) контрольным(и) шаблоном(ами). При выполнении биометрической верификации испытуемого субъекта на единственный запрос выдается единственный результат сравнения. При выполнении биометрической идентификации множество или все биометрические контрольные шаблоны могут сравниваться с биометрическими признаками, при этом результат сравнения будет выдаваться на каждое сравнение.

6.2.6 Подсистема принятия решений

Подсистема принятия решений использует результаты сравнения, сформированные в результате одного или нескольких биометрических сравнений, чтобы выдать итоговый результат для транзакции биометрической верификации или идентификации.

В случае биометрической верификации сравнение биометрической пробы и биометрического контрольного шаблона признают успешным (считая, что более высокие результаты соответствуют большему сходству), если результат сравнения превышает установленный порог. Биометрическое заявление может быть подтверждено на основании политики принятия решений, которая может предусматривать несколько попыток биометрической верификации.

В случае биометрической идентификации зарегистрированный биометрический контрольный шаблон является потенциальным кандидатом для испытуемого субъекта (считая, что более высокие результаты соответствуют большему сходству), если результат сравнения превысил установленный порог и/или если результат сравнения является одним из наиболее высоких ранжированных значений, созданных во время сравнения по всей базе данных. Политика принятия решений может потребовать нескольких попыток идентификации перед принятием решения.

Примечание — Концептуально можно рассматривать мультибиометрические системы подобно монобиометрическим системам, считая комплексные зарегистрированные биометрические образцы/шаблоны/показатели за один биометрический образец/шаблон/показатель и позволяя подсистеме принятия решений, при необходимости, оперировать объединением результатов сравнения или объединением на уровне принятия решения (см. *ГОСТ Р 54411*).

6.2.7 Подсистема администрирования

Примечание — На рисунке 1 подсистема администрирования не показана.

Подсистема администрирования управляет общими правилами, реализацией, конфигурацией и работой биометрической системы с учетом законодательных, юридических и общественных ограничений и требований.

В частности, подсистема администрирования выполняет:

a) взаимодействие с испытуемым субъектом, включая обеспечение обратной связи с испытуемым субъектом в процессе и/или после сбора данных и запрос дополнительной информации от испытуемого субъекта;

b) хранение и форматирование биометрических контрольных шаблонов и/или биометрических персональных данных;

c) вынесение окончательного заключения на основе решения и/или результатов сравнения;

d) установку пороговых значений;

e) настройку параметров сбора данных;

f) контроль операционной среды и хранение небиометрических данных;

g) обеспечение соответствующих гарантий конфиденциальности и безопасности данных испытуемого субъекта;

h) взаимодействие с приложением, использующим биометрическую систему.

6.2.8 Интерфейс для внешнего приложения

Примечание — На рисунке 1 интерфейс для внешнего приложения не показан.

Биометрическая система может взаимодействовать с внешними приложениями или системами через интерфейс веб-служб, ПИП, аппаратный интерфейс или интерфейс протоколов.

6.3 Функции биометрической системы общего вида

6.3.1 Биометрическая регистрация

При биометрической регистрации данные, полученные в результате взаимодействия испытуемого субъекта с биометрической системой, обрабатывают и хранят в виде контрольного шаблона биометрической регистрации для данного испытуемого субъекта.

При биометрической регистрации выполняют следующие операции:

a) сбор биометрических образцов;

b) восстановление или улучшение биометрических образцов;

c) сегментацию;

d) извлечение биометрических признаков;

e) контроль качества (по результатам которого биометрический образец или биометрические признаки могут быть отклонены как непригодные для создания биометрического контрольного шаблона и могут потребоваться дополнительные образцы);

f) обнаружение атаки на биометрическое предъявление (в результате которого может быть отклонен биометрический образец или биометрические признаки, непригодные для использования в качестве зарегистрированного биометрического контрольного шаблона);

g) сравнение с существующими биометрическими контрольными шаблонами для того, чтобы убедиться, что испытуемый субъект еще не зарегистрирован (при наличии соответствующих системных требований);

h) создание биометрического контрольного шаблона (для этого могут потребоваться биометрические признаки нескольких образцов) с возможным созданием соответствующего индекса базы данных;

i) хранение (возможно в преобразованном в формат обмена и хранения виде);

j) тестовую биометрическую верификацию или идентификацию для подтверждения пригодности результата биометрической регистрации при дальнейшем использовании;

k) разрешение повторной попытки биометрической регистрации, если результаты первоначальной биометрической регистрации признаны неудовлетворительными (в зависимости от правил биометрической регистрации).

6.3.2 Биометрическая верификация положительного биометрического заявления

В приложениях, таких как контроль доступа, при верификации данные, полученные в результате взаимодействия испытуемого субъекта с системой, обрабатываются с целью подтверждения наличия биометрической регистрации данного субъекта в системе (например, «Я зарегистрирован как субъект *X*»). Следует учитывать, что некоторые биометрические системы позволяют испытуемому субъекту регистрировать несколько биометрических характеристик. Например, в биометрической системе идентификации по РОГ испытуемые субъекты могут зарегистрировать изображения радужных оболочек обоих глаз, а в биометрической системе идентификации по отпечаткам пальцев — другие пальцы, если основной палец окажется травмированным.

Биометрическая верификация положительного биометрического заявления состоит из следующих этапов:

a) сбор биометрических образцов;

b) восстановление или улучшение биометрических образцов;

c) сегментация;

d) извлечение биометрических признаков;

e) контроль качества (по результатам которого биометрический образец или биометрические признаки могут быть отклонены как непригодные для сравнения и может потребоваться сбор дополнительных биометрических образцов);

f) обнаружение атаки на биометрическое предъявление (которое может отклонить биометрический образец/биометрические признаки как непригодные для использования);

g) создание биометрической пробы (что может потребовать биометрические признаки нескольких образцов), возможное преобразование в формат обмена;

h) сравнение биометрической пробы с биометрическим контрольным шаблоном для подтверждения личности с выводом результата сравнения;

i) определение совпадения биометрических признаков пробы и биометрического контрольного шаблона, основанное на превышении результатом сравнения установленного порога (т. е. более высокие результаты сравнения соответствуют большему сходству);

j) принятие решения по биометрической верификации на основании результата сравнения в одной или нескольких попытках согласно правилам принятия решений.

Функция биометрической верификации либо примет, либо отклонит определенное положительное биометрическое заявление. Результат решения биометрической системы верификации считают ошибочным, если принято ложное заявление (ложный допуск) или отклонено истинное заявление (ложный недопуск). В этом приложении ложный допуск происходит, если представленный биометрический образец ошибочно совпал с биометрическим контрольным шаблоном, который не создавался данным испытуемым субъектом. Ложный недопуск происходит, если представленный биометрический образец не совпадает с биометрическим контрольным шаблоном, действительно созданным данным испытуемым субъектом.

Примечание — Биометрическая верификация неопределенного положительного биометрического заявления также реализуема с помощью биометрической системы. В 90-х г. XX в. такие приложения именовали «верификациия без ПИН-кода», так как ни персональный идентификационный код (ПИН-код), ни другой идентификатор не требовался для подтверждения того, что испытуемый субъект действительно зарегистрирован в базе данных. С конца 90-х г. XX в. в этом качестве для контроля допуска использовались системы распознавания РОГ. Процесс идентичен процессу биометрической верификации определенного биометрического заявления по перечислениям a)—g). При этом для биометрической верификации неопределенного биометрического заявления перечисления h)—j) отличаются, а именно:

h) сравнение биометрической пробы со всеми контрольными шаблонами и вывод результата для каждого сравнения;

i) определение совпадения биометрических признаков пробы и какого-либо биометрического контрольного шаблона, основанное на превышении результатом сравнения установленного порога (т. е. более высокие результаты сравнения соответствуют большему сходству);

j) принятие решения на основании результатов сравнения одной или нескольких попыток согласно правилам принятия решений.

6.3.3 Биометрическая идентификация

При биометрической идентификации транзакция испытуемого субъекта обрабатывается с целью сбора биометрической пробы, а в регистрационной базе данных осуществляется поиск с целью возвращения идентификаторов биометрических контрольных шаблонов, схожих с этой пробой. По результатам биометрической идентификации создается список кандидатов. Список кандидатов может быть пустым, содержать только один идентификатор или более. Биометрическую идентификацию считают успешной, если испытуемый субъект прошел биометрическую регистрацию и его идентификатор присутствует в списке кандидатов. Биометрическую идентификацию считают ошибочной, если идентификатор зарегистрированного субъекта отсутствует в списке кандидатов (ложноотрицательная биометрическая идентификация) или в результате обработки запроса от незарегистрированного субъекта создается непустой список кандидатов (ложноположительная биометрическая идентификация).

Биометрическая идентификация состоит из следующих этапов:

a) сбор биометрических образцов;

b) восстановление или улучшение биометрических образцов;

c) сегментация;

d) извлечение биометрических признаков;

e) контроль качества (по результатам которого биометрический образец или биометрические признаки могут быть отклонены как непригодные для сравнения и может потребоваться сбор дополнительных биометрических образцов);

f) обнаружение атаки на биометрическое предъявление (которое может отклонить биометрический образец/биометрические признаки как непригодные для использования);

g) создание биометрической пробы (что может потребовать биометрические признаки нескольких образцов), возможное преобразование в формат обмена;

h) сравнение пробы с отдельными или со всеми биометрическими контрольными шаблонами, имеющимися в регистрационной базе данных, вывод результата сравнения для каждого сравнения;

i) определение потенциальных идентификаторов для данного пользователя, основанное на превышении каким-либо результатом сравнения установленного порога и/или его принадлежности к диапазону максимальных значений, формирование списка кандидатов;

j) принятие решения на основании списка кандидатов из одной или нескольких попыток согласно правилам принятия решений.

6.4 Транзакции биометрической регистрации, верификации и идентификации

Процессы сбора данных для биометрической регистрации, верификации или идентификации состоят из одной или нескольких попыток сбора, разрешенных или требуемых соответствующей политикой принятия решений. Каждая попытка может состоять из одного или нескольких предъявлений биометрических образцов, зависящих от работы датчика, политики оценки качества биометрического образца и других настроек, ограничивающих число предъявлений или время, установленное для проведения попытки.

Примеры

1 Если политика принятия решений для биометрической верификации допускает три попытки, то транзакция может состоять из одной попытки или из двух попыток в случае отклонения первой попытки и, наконец, из трех попыток в случае отклонения двух первых попыток.

2 Процесс биометрической регистрации, как правило, требует многократного предъявления биометрических характеристик регистрируемого пользователя.

3 Некоторые биометрические системы верификации обрабатывают последовательность биометрических образцов за одну попытку, например:

a) сбор биометрических образцов в течение фиксированного периода времени для поиска наиболее подходящего биометрического образца;

b) сбор биометрических образцов до момента достижения соответствия или момента истечения системного времени.

4 Некоторые системы биометрической идентификации собирают несколько образцов от одного субъекта персональных данных и объединяют результаты биометрического поиска по каждому образцу в единый список кандидатов. Типичными случаями являются использование нескольких пальцев при идентификации по отпечаткам пальцев и применение нескольких кадров при распознавании лиц по видео.

На рисунке 2 показана взаимосвязь между биометрическими предъявлениями, попытками и транзакциями.

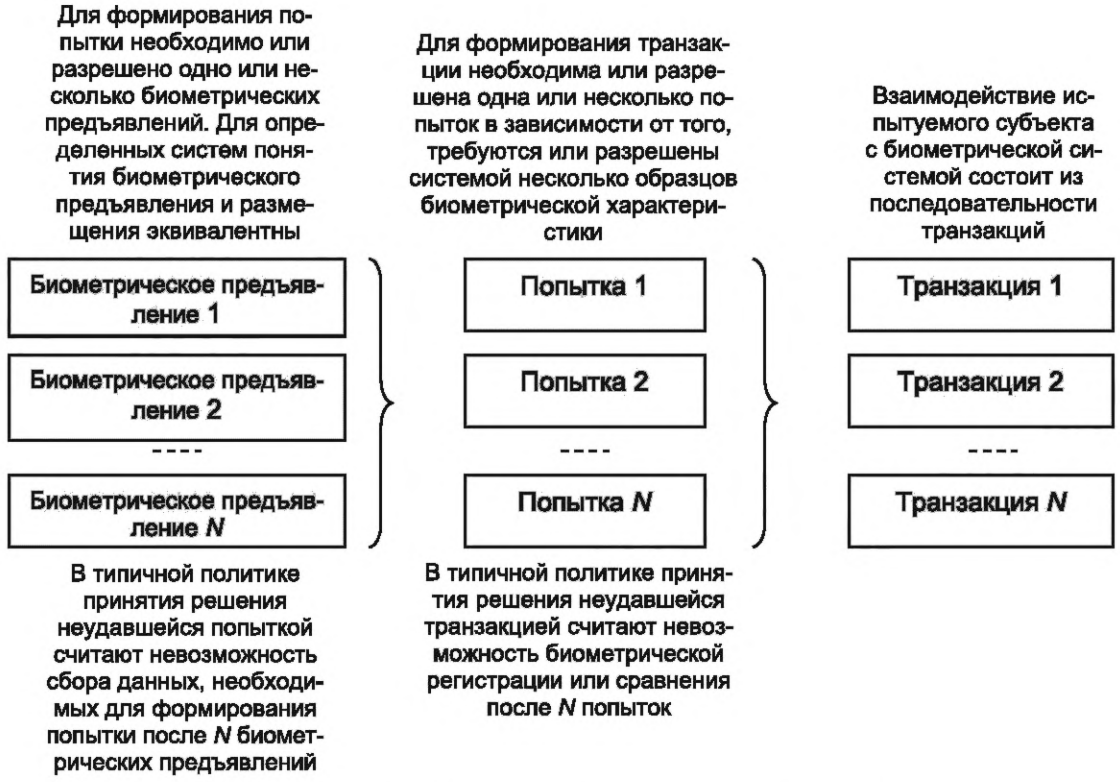

Рисунок 2 — Биометрические предъявления, попытки и транзакции

6.5 Эксплуатационные характеристики

6.5.1 Вероятности появления ошибок

В биометрической системе базовые ошибки включают в себя ошибки сравнения (ложное совпадение и ложное несовпадение) и ошибки создания биометрического контрольного шаблона/биометрической пробы (отказ сбора данных и отказ биометрической регистрации). Базовые ошибки в совокупности образуют ошибки принятия решения в системах биометрической верификации и идентификации. Влияние сочетания данных базовых ошибок на появление ошибок принятия решения зависит от числа необходимых или разрешенных сравнений, от того, является ли истинным или ложным биометрическое заявление, а также от политики принятия решения.

6.5.2 Показатели пропускной способности

6.5.2.1 Показатели пропускной способности определяют количество испытуемых субъектов, подвергаемых анализу в единицу времени, зависящее от скорости вычислений и от взаимодействия пользователя с биометрической системой. Показатели пропускной способности для биометрических систем верификации, например для систем контроля и управления доступом, как правило, определяются скоростью взаимодействия пользователя с системой в процессе предоставления биометрического образца достаточного качества. На показатели пропускной способности для биометрических систем идентификации, например для систем регистрации в программе социального обеспечения, может влиять время вычислительной обработки, необходимое для сравнения зарегистрированного биометрического образца с базой данных контрольных шаблонов. Поэтому, в зависимости от приложения, рекомендуется измерять время взаимодействия испытуемых субъектов с системой, а также время режима

работы вычислительных аппаратных средств в зависимости от количества хранимых биометрических контрольных шаблонов. Кроме того, при эксплуатации действия, необходимые после получения результата от биометрической системы (например, прохождение через ворота, открытие двери, выход со станции), могут повлиять на способность следующего испытуемого субъекта взаимодействовать с системой. Измерение пропускной способности должно учитывать эти дополнительные действия, которые могут варьироваться в зависимости от результата биометрической системы.

Примечание — Фактические экспериментальные измерения быстродействия вычислительной системы приведены в таких руководствах, как [*1*], и не рассмотрены в настоящем стандарте.

6.5.2.2 Для определения скорости взаимодействия испытуемого субъекта с системой необходимо точно установить признаки начала и окончания транзакции. Эти признаки должны быть определены перед началом испытаний и указаны в протоколе испытаний. В протокол испытаний следует также включить краткий список действий, выполняемых испытуемыми субъектами в процессе взаимодействия с биометрической системой.

Пример — Пропускная способность может быть измерена только для процесса сбора биометрических образцов или для транзакций биометрического распознавания, допускающих несколько попыток.

6.5.3 Виды эксплуатационных испытаний

6.5.3.1 Технические эксплуатационные испытания в биометрии могут быть трех видов: технологическое, сценарное и оперативное.

6.5.3.2 В процессе технологического испытания проводят испытание одного или нескольких алгоритмов с использованием базы данных биометрических образцов. Сбор базы данных может быть частью испытания. Также допускается использовать заранее собранную базу данных, доступную экспериментатору. Несмотря на то что для разработки и настройки биометрической системы перед испытанием можно использовать демонстрационные данные, фактическое испытание необходимо проводить на данных, которые ранее не использовались разработчиками алгоритмов. Испытание проводят путем обработки данных в режиме отложенного задания. Вследствие неизменяемости базы данных результаты технологических испытаний являются воспроизводимыми. Тем не менее эксплуатационные характеристики по отношению к этой базе данных будут зависеть как от внешних условий, так и от выборки.

6.5.3.3 В процессе сценарного испытания проводят испытание одной или нескольких полнокомплектных биометрических систем в условиях, моделирующих определенную ситуацию, максимально приближенную к действительности. Каждая испытуемая биометрическая система имеет собственный датчик сбора, в результате чего могут быть небольшие различия в получаемых начальных данных. Следовательно, если сравнивают несколько биометрических систем, необходимо уделить внимание тому, чтобы сбор данных для всех испытуемых систем проходил в одних и тех же условиях окружающей среды и с использованием одной и той же выборки. В зависимости от требований к испытанию обработка данных может быть как в режиме отложенного задания, так и в режиме реального времени. Воспроизводимость результатов испытания обеспечивают тщательным контролем выполнения сценария.

6.5.3.4 Оперативное испытание, как правило, проводят в режиме реального времени для обеспечения согласованности со средой применения (если только испытуемые системы не обрабатывают данные в режиме отложенного задания). Воспроизводимость результатов оперативного испытания может быть ограничена из-за неизвестных и недокументированных различий в условиях эксплуатации. Более того, может быть сложно установить истинную информацию о личностях и поведении испытуемых субъектов, особенно в условиях отсутствия администратора испытания, наблюдателя за испытанием или обслуживающего персонала.

Различия между видами испытаний приведены в приложении А.

7 Планирование испытания

7.1 Общие положения

7.1.1 На первом этапе испытания экспериментатор должен определить:

a) тип испытуемых систем, их применение, условия испытания и выборку;

b) эксплуатационные характеристики, которые необходимо измерить;

c) данные, необходимые для оценки эксплуатационных характеристик (т. е. определить вид испытания: технологическое, сценарное или оперативное).

Вышеуказанные данные являются основой для разработки соответствующего протокола испытания, определяя необходимые средства контроля условий испытаний, выборку испытуемых субъектов и объем испытаний.

Примечание — Вид испытания может быть определен заранее, например: при наличии базы данных испытуемых биометрических образцов для технологического испытания или установленной системы для оперативного испытания. Возможны также условия, при которых все виды испытаний могут быть проведены последовательно, с постепенным сужением вариантов модальности и биометрических систем, рассматриваемых для ввода в эксплуатацию.

7.1.2 Протокол испытания по возможности должен отражать различия биометрических систем и условий их применения, такие как:

a) различия в условиях среды;

b) различия в выборке испытуемых субъектов (например, различия в привыкании субъектов);

c) различия в биометрических модальностях (например, различия в модальностях, находящихся под влиянием различных условий, а также различия между испытаниями преимущественно поведенческой и преимущественно физиологической биометрии);

d) различия в эксплуатационных характеристиках (например, измерение общих эксплуатационных характеристик для биометрической верификации, идентификации на открытом множестве и идентификации на замкнутом множестве проводят разными методами);

e) дополнительные проблемы в установлении истинной информации для биометрических систем идентификации (в которой транзакции биометрической идентификации не сопровождаются определенным биометрическим заявлением).

7.1.3 Настоящий стандарт устанавливает основные принципы проведения оценки эксплуатационных характеристик и требования к оформлению протокола испытаний. Методы и требования к конкретным видам испытаний, биометрическим модальностям и к целевым применениям в настоящем стандарте не рассмотрены.

7.2 Определение информации о системе

При планировании процедур сбора данных экспериментатор должен дать ответы на следующие вопросы о биометрической системе, которая будет подвергнута испытанию:

a) регистрирует ли система информацию о транзакциях? При отрицательном ответе данная информация должна быть записана самим испытуемым субъектом, администратором испытания или наблюдателем за испытанием;

b) сохраняет ли система биометрические образцы или биометрические признаки для каждой транзакции? Это необходимо, если результаты сравнения для собранных в процессе испытания данных определяют в режиме отложенного задания;

c) возвращает ли система информацию о результатах сравнения или только решения о допуске или недопуске? В последнем случае может потребоваться сбор данных при различных настройках порога для создания кривой КОО (см. 8.2.3). Если система возвращает результаты сравнения, то какая информация доступна о параметрах и шкале?

d) предоставил ли изготовитель КПО? Формирование результатов парного и непарного сравнения в режиме отложенного задания потребует использования программных модулей КПО:

1) для создания биометрических контрольных шаблонов из биометрических образцов для регистрации,

2) создания биометрических проб из биометрических образцов для распознавания,

3) определения результатов сравнения между биометрическими пробами и биометрическими контрольными шаблонами;

e) требуются ли модификации системы для проведения испытания? Повлияют ли требуемые модификации на эксплуатационные характеристики системы?

f) создает ли система независимые биометрические контрольные шаблоны? Если биометрические контрольные шаблоны зависимы, то процедуры для сбора или создания попыток непарного сравнения будут различными (см. 8.4.11).

Примечание — Независимый биометрический контрольный шаблон — это шаблон, содержание и состав которого не определены и не могут быть определены содержанием и составом других биометрических контрольных шаблонов;

g) использует ли система алгоритмы, которые адаптируют биометрический контрольный шаблон после успешной биометрической верификации? В этом случае необходимо исходить из количества адаптаций биометрического контрольного шаблона, которые должны произойти до измерения эксплуатационных характеристик, и возможности неблагоприятного влияния попыток непарного сравнения на контрольные шаблоны (см. 8.4.5);

h) какими являются рекомендуемые значения качества изображения и порогов принятия решений о совпадении для целевого применения? Данные настройки влияют на качество представляемых биометрических образцов и вероятности ошибок;

i) установлены ли ожидаемые вероятности ошибок? Данную информацию используют при проверке достаточности объема испытания (см. раздел В.1);

j) какие факторы влияют на эксплуатационные характеристики системы данного типа? Они должны быть контролируемыми или задокументированными (см. 7.3);

k) зависят ли эксплуатационные характеристики от числа зарегистрированных биометрических контрольных шаблонов? Данная зависимость существует у большинства биометрических систем идентификации и у некоторых биометрических систем верификации, которые выполняют регистрацию группы или осуществляют поиск «один ко многим» во время процесса биометрической верификации.

7.3 Контроль факторов, влияющих на эксплуатационные характеристики

7.3.1 Показатели эксплуатационных характеристик биометрической системы могут в значительной степени зависеть от способов ее применения, условий окружающей среды и выборки. Список особенностей выборки, факторов применения, внешних и системных факторов, которые влияют на эксплуатационные характеристики биометрической системы, приведен в приложении С.

7.3.2 Факторы, влияющие на измеряемые эксплуатационные характеристики, должны быть явно или неявно отнесены к одному из следующих четырех классов:

a) контролируемые управляемые факторы, включенные в методику испытания (как независимые переменные), которые можно наблюдать, протоколировать и анализировать;

b) контролируемые неуправляемые факторы (постоянные в течение испытаний), являющиеся частью условий испытания;

c) неконтролируемые факторы — случайные и независимые от испытания факторы;

d) незначительные факторы, эффект от которых не будет учитываться. Без данной категории факторов испытание будет предельно сложным.

До начала сбора данных должно быть установлено, каким образом будет осуществляться контроль данных факторов. Для определения того, какие факторы наиболее существенны, а какие могут быть отнесены к незначительным, может понадобиться провести предварительное испытание биометрических систем. При определении контролируемых факторов может возникнуть противоречие между необходимостью внутренней достоверности (т. е. различия в эксплуатационных характеристиках вызваны только независимыми переменными, зарегистрированными при испытании) и внешней достоверности (т. е. результаты действительно представляют эксплуатационные характеристики при целевом применении).

Пример — При сравнении эксплуатационных характеристик двух биометрических систем необходимо определить, влияет ли квалификация или личность администратора испытания на эксплуатационные характеристики. Контролировать этот фактор можно следующим образом:

a) спланировать эксперимент таким образом, чтобы измерять эксплуатационные характеристики между администраторами испытания дифференциально, так же как и между системами;

b) использовать только одного администратора испытания или регламентировать взаимодействие администратора испытания или испытуемого субъекта для соблюдения единообразия в течение испытания;

c) случайно распределить попытки регистрации между всеми администраторами испытания, тем самым исключая любую систематическую ошибку;

d) при наличии данных о том, что различия между администраторами испытания являются небольшими по сравнению с различиями между системами, данный фактор допускается не учитывать.

7.3.3 При технологическом испытании могут быть учтены особенности применения и выборки, гарантирующие, что испытания будут недостаточно трудными и недостаточно простыми для испытуемых алгоритмов.

7.3.4 Для того чтобы биометрическая система могла быть испытана на репрезентативной выборке в реальных условиях, при сценарном испытании должны быть определены и смоделированы условия реального применения и выборка.

7.3.5 При оперативном испытании условия окружающей среды и выборку определяют в реальных условиях под контролем экспериментатора.

7.3.6 При сценарном и оперативном испытаниях любые изменения устройств и условий испытания для обеспечения оптимальной производительности (включая пороги качества и принятия решений) должны быть выполнены до сбора данных. Более жесткий контроль качества может привести к меньшему количеству ложных совпадений и ложных несовпадений, но более высокой вероятности отказов сбора данных. Порог принятия решения также должен быть установлен соответствующим образом, если решение о сравнении предоставляется испытуемому субъекту в виде положительной или отрицательной обратной связи, которая влияет на его поведение. Разработчики могут дать рекомендации относительно оптимальных условий испытания и компромисса между настройками.

7.3.7 Одним из основных условий при планировании испытания является определение временного интервала между биометрической регистрацией и сбором данных биометрической пробы. Продолжительные временные интервалы, как правило, осложняют сопоставление образцов биометрической пробы и биометрических контрольных шаблонов из-за явления, именуемого как «старение шаблона». Это сопряжено с увеличением вероятностей ошибок, вызванных изменениями биометрических характеристик, связанными со временем их предъявления. Поэтому сбор данных биометрической пробы для попыток парного сравнения должен быть отделен во времени от биометрической регистрации интервалом, соразмерным с целевым применением. Если данный интервал неизвестен, то разделение во времени должно быть настолько продолжительным, насколько это возможно.

Примечание — Иногда прошедшее с момента биометрической регистрации время может являться одним из контролируемых экспериментальных факторов, требующих сбора нескольких биометрических образцов с течением времени. Это позволит провести динамический анализ таких факторов, как привыкание, старение шаблона и стабильность/постоянство биометрических характеристик в течение всего периода эксперимента (см. 9.7.1).

7.4 Отбор испытуемых субъектов

7.4.1 Биометрическая регистрация и биометрическое распознавание требуют входных сигналов или изображений биометрических характеристик. Биометрические образцы должны быть собраны с испытуемой группы с соблюдением требований действующих нормативных документов в области обработки персональных данных, действующих на территории Российской Федерации.

7.4.2 Испытуемая группа не должна включать в себя испытуемых субъектов, биометрические характеристики которых предварительно использовались для разработки или настройки испытуемой биометрической системы.

7.4.3 Испытуемая группа должна быть демографически подобна группе целевого применения, для которой по результатам испытания будут определены эксплуатационные характеристики. В данном случае испытуемые субъекты должны быть выбраны случайным образом из целевой выборки. В других случаях необходимо использовать добровольцев.

7.4.4 Увеличение числа испытуемых субъектов в испытуемой группе за счет добровольцев без введения адекватного контроля может оказать влияние на испытания. Например, люди с ограниченными возможностями могут быть недостаточно представлены в целевой выборке. Может возникнуть необходимость набора добровольцев, чтобы испытуемая группа была максимально репрезентативной и отражала разнообразие потенциальных пользователей. Приближение целевой выборки является значимым вопросом в обеспечении достоверности испытаний.

7.4.5 Биометрическая регистрация и биометрическое распознавание, как правило, состоят из нескольких этапов, которые в зависимости от целевого применения биометрических систем отделены друг от друга днями, неделями, месяцами или годами. Не всегда можно собрать испытуемую группу с постоянным составом на длительный период, поэтому вполне вероятно, что некоторые испытуемые субъекты могут выбыть из группы в период между этапами испытаний.

7.4.6 Испытуемая группа должна быть надлежащим образом проинструктирована, чтобы ее действия и поведение соответствовали целевому применению. Если испытуемым субъектам происходящее представляется рутинным или они устают от установленного порядка испытаний, то они могут начать экспериментировать или становятся менее аккуратными. Поэтому экспериментатор должен учитывать вовлечение испытуемого субъекта в процесс испытания при планировании испытания.

7.4.7 Для скрытых целевых применений испытуемые субъекты должны вести себя так, будто они не имеют представления о сборе биометрического образца в данный момент. Это может быть достигнуто путем пассивного сбора на протяжении длительного периода и использования радиометок, чтобы установить правильный идентификатор испытуемых субъектов без их участия.

7.4.8 Перед испытанием испытуемые субъекты должны быть полностью проинформированы о продолжительности испытания, процедурах сбора, условиях использования и распространения данных испытания, а также о количестве этапов испытания. Независимо от характера использования личных данных, они не подлежат разглашению экспериментатором. Управление данными испытуемых субъектов должно осуществляться с соблюдением требований нормативных документов в области защиты персональных данных, действующих на территории Российской Федерации. В соответствии с этими правилами могут быть предписаны, например, полное раскрытие информации и подписание формы соглашения перед участием в испытании, а также обеспечение анонимности всех полученных данных.

Примечание — Для некоторых видов испытаний, например для оперативного испытания скрытой системы идентификации, информирование испытуемых субъектов, возможно, будет нецелесообразным или может изменить их поведение, что приведет к недостоверности полученных результатов.

7.4.9 При необходимости использования искусственных биометрических образцов или биометрических признаков (включая созданные путем изменения реальных данных) их применение должно быть обосновано и указано в протоколе испытания, в котором также должны быть описаны метод сбора биометрических образцов и условия его применимости. Результаты испытания для искусственных и неискусственных биометрических образцов должны быть указаны в протоколе испытания отдельно, а результаты испытания смешанных искусственных и неискусственных биометрических образцов должны содержать подробности смешения.

Примечание — Использование искусственно синтезированных изображений биометрических характеристик повысило бы внутреннюю достоверность технологических испытаний, так как контролируются все независимые переменные, влияющие на эксплуатационные характеристики. Внешняя достоверность при этом, вероятно, будет снижена.

7.5 Объем испытания

7.5.1 Общие положения

Масштаб испытания с точки зрения числа испытуемых субъектов, образцов и транзакций влияет на точность измерения вероятностей ошибок. Чем больше объем испытания, тем выше точность результатов. Для установления нижних границ количества попыток или транзакций, необходимых для заданного уровня точности, применяют правило трех и правило тридцати (см. раздел В.1). Однако данные правила завышают степень доверия к биометрическим результатам, так как предполагают, что вероятности ошибок являются следствием единственного источника вариации, что неверно в отношении биометрических систем.

Примечание — По мере увеличения объема испытания дисперсия оценки уменьшается, но масштабный коэффициент зависит от источника дисперсии. Например, испытуемые субъекты могут иметь отличающиеся вероятности ошибки [*2*], дающие компоненту дисперсии, которую вычисляют как единицу, разделенную на число испытуемых субъектов, вместо единицы, разделенной на число попыток. Подробное описание данного эффекта приведено в приложении В.

7.5.2 Сбор нескольких транзакций биометрического распознавания для каждого испытуемого субъекта в системе

7.5.2.1 В процессе испытания допускается использовать несколько транзакций от каждого испытуемого субъекта в системе. Испытания, при которых от каждого испытуемого субъекта необходимо получить несколько транзакций, включают в себя:

- испытание эффектов старения, адаптации и других систематических изменений;
- испытание биометрических систем, использующих обновление биометрического контрольного шаблона;
- определение диапазонов вероятностей ошибок, индивидуальных для каждого испытуемого субъекта;
- испытание, при котором транзакция не полностью определена до проведения испытания, например: при определении влияния числа попыток в транзакции на эксплуатационные характеристики.

Использование нескольких транзакций в каждой системе неуместно в тех испытаниях, в которых предполагается, что испытуемые субъекты не знакомы с устройством или биометрическим приложением.

Примечание — Если стоимость и усилия по организации и регистрации группы испытуемых субъектов не являются существенным условием, то для обеспечения независимости транзакций используют большое число испытуемых субъектов, каждый из которых создает отдельную транзакцию. Десять пар «биометрическая проба — биометрический контрольный шаблон» от каждого из 100 испытуемых субъектов статистически не эквивалентны одной паре «биометрическая проба — биометрический контрольный шаблон» от каждого из 1000 испытуемых субъектов и не обеспечивают такой же уровень достоверности результатов. В зависимости от необходимых стоимости и времени допускается использовать ранее зарегистрированных испытуемых субъектов, а не искать и регистрировать новых. При выполнении транзакции для одновременного проведения дополнительных транзакций требуются незначительные усилия. Несмотря на корреляцию между несколькими транзакциями возможно, что при использовании нескольких транзакций от меньшего числа испытуемых субъектов возникает меньшая неопределенность результатов испытания, чем при испытании аналогичной стоимости с использованием одной транзакции от большего числа испытуемых субъектов.

7.5.2.2 Количество и частота применения испытательных тестовых транзакций, полученных от каждого испытуемого субъекта, должны соответствовать их целевому применению. Использование множественных транзакций непригодно в тех испытаниях, в которых пользователь должен быть незнаком с устройством или биометрическим приложением.

Примечание — Поведение испытуемого субъекта может изменяться с каждой последующей попыткой из-за повышения уровня его осведомленности об устройстве или обратной связи в виде решения о сравнении. Например, первая попытка, которую совершает испытуемый субъект, будет иметь более высокую вероятность отказа, чем следующие попытки. В результате наблюдаемая ВЛНС будет зависеть от структуры попыток каждого испытуемого субъекта, как определено в соответствии с протоколом испытания. Вероятности ошибок оценивают в среднем не только по целевой выборке, но также по попыткам, которые испытуемый субъект может выполнить корректно. В этом случае применяют усреднение по нескольким попыткам. Однако существует вероятность того, что изменение количества и структуры попыток на одного испытуемого субъекта влияет на поведение субъекта в достаточной степени, чтобы значительно изменить измеренные вероятности ошибок.

7.5.3 Требования к объему испытания

При определении уровня достоверности результатов испытания число испытуемых субъектов имеет большее значение, чем число проводимых транзакций, поэтому:

a) группа должна быть настолько большой, насколько это практически осуществимо. Мерой целесообразности могут быть затраты на набор и испытание группы;

b) при необходимости определяют заданный уровень точности и уровень достоверности, необходимый для проведения биометрического эксплуатационного испытания. От каждого испытуемого субъекта должно быть получено достаточное число транзакций, чтобы общее число транзакций превысило значение, определенное исходя из заданного уровня точности и достоверности. Для определения объема испытания может быть использовано правило трех или правило тридцати. При наличии возможности собрать несколько транзакций одного и того же испытуемого субъекта в разные дни или разные образцы испытуемого субъекта (при условии сохранения репрезентативности*) можно уменьшить зависимости между транзакциями одного и того же испытуемого субъекта;

c) после того как данные собраны и проанализированы, должна быть проведена оценка неопределенности измерений эксплуатационных характеристик.

Примечание — В этом случае применяют закон убывающей отдачи, т. е. цель достигнута, если число ошибок, возникающих из-за изменений условий использования или выборки испытуемых субъектов, превышает число ошибок, связанных с численностью группы и объемом испытаний.

7.6 Многократные испытания

7.6.1 Вследствие высокой стоимости процедуры сбора данных допускается проводить несколько испытаний с одним набором данных. Этот метод используют при проведении технологического испытания. Для проведения испытания нескольких алгоритмов сравнения в режиме отложенного задания

* Например, использование мизинца может быть нерепрезентативным для нормального применения биометрической системы отпечатков пальцев, и значения вероятности ошибок будут различными (см. [*3*]). Точно так же использование перевернутой левой руки не будет репрезентативным в биометрической системе, предназначенной для регистрации правой руки.

может быть собрана одна база данных. Таким образом обеспечивается разделение подсистемы сбора данных и подсистемы обработки сигнала. Поскольку данные подсистемы, как правило, не являются абсолютно независимыми, то могут возникнуть проблемы. Например, модуль проверки качества, требующий от подсистемы сбора биометрических данных повторного получения изображения, является частью подсистемы обработки сигнала. Кроме того, на качество изображения влияют различные виды пользовательских интерфейсов, которые управляют процессом сбора биометрических данных. Следовательно, при использовании объективной базы данных технологическое испытание алгоритмов в режиме отложенного задания может дать недостоверные показатели общих эксплуатационных характеристик биометрической системы или сместить результаты в пользу одних систем по отношению к другим.

7.6.2 Сценарные испытания нескольких биометрических систем допускается проводить одновременно при наличии испытуемой группы с использованием нескольких различных устройств или методов на каждом этапе. Данный подход требует осторожности. Например, когда испытуемые субъекты перемещаются от устройства к устройству, привыкание к одному устройству может влиять на взаимодействие субъекта со следующим устройством. Чтобы уравнять данный эффект по всем устройствам, порядок их предъявления каждому испытуемому субъекту должен быть случайным.

8 Сбор данных

8.1 Исключение отказа сбора данных

8.1.1 Полученные биометрические образцы или биометрические признаки заносят в базу данных. Информация о биометрических образцах, биометрических признаках и испытуемых субъектах, которым они принадлежат, является метаданными. База данных и метаданные могут быть повреждены, если будут допущены ошибки в процессе сбора данных. Вероятности ошибок в процессе сбора данных могут превышать вероятности ошибок биометрической системы, поэтому сбору данных следует уделять повышенное внимание, чтобы избежать ошибок в базе данных (неправильно полученный биометрический образец) и в метаданных (неправильно маркированный биометрический образец).

Примеры

1 Возможными причинами ошибок в базе данных являются:

a) данные испытуемых субъектов, использующих систему, неправильные (вне рамок инструкции по эксперименту), например из-за неправильного использования сканера отпечатков пальцев;

b) данные пустого или испорченного изображения, если испытуемый субъект ввел ПИН, но не представил качественного биометрического образца.

2 Возможными причинами ошибок в метаданных являются:

a) испытуемый субъект с неверным ПИН;

b) неверный ввод ПИН;

c) использование нерегламентированной для испытуемого субъекта биометрической характеристики, например: субъект использует средний палец, когда требуется указательный.

8.1.2 При сборе данных следует использовать программное обеспечение, которое минимизирует объем данных, требующих ввода с клавиатуры, не требует присутствия нескольких администраторов или наблюдателей за испытанием для проверки введенных данных, а также имеет встроенное резервирование данных. Администраторы испытания и наблюдатели за испытанием должны знать правила работы с биометрической системой и предотвращать возможные ошибки. Во избежание различной интерпретации понятия «неправильно полученный биометрический образец» должны быть заранее установлены объективные критерии. Любая внештатная ситуация, возникающая при попытке сбора данных и затрагивающая транзакцию, должна быть задокументирована администраторами испытания и/или наблюдателями за испытанием.

8.1.3 Ошибки, допущенные при сборе данных, снижают достоверность результатов испытания. Исправление ошибок в базе данных или метаданных должно быть выполнено с помощью встроенного в систему устройства резервирования сбора данных и не должно быть полностью основано на результатах проверенного биометрического алгоритма. В этом отношении биометрические системы, которые могут сохранять биометрические образцы и/или протоколы транзакций, предоставляют больше возможностей для исправления ошибок, чем системы, в которых все особенности испытания должны быть записаны вручную.

8.1.4 Администраторы испытания и наблюдатели за испытанием не должны вручную отбраковывать или использовать автоматизированный механизм отбраковки собранных биометрических образцов, кроме тех случаев, когда биометрические образцы не соответствуют некоторому формальному предопределенному задокументированному и представленному критерию исключения. Число исключенных таким образом биометрических образцов должно быть отражено в протоколе.

Пример — Исключается биометрический образец отпечатка пальца, если площадь зарегистрированной области пальца менее 0,25 см^2.

8.2 Собранные данные и особенности испытания

8.2.1 Данные, которые могут быть собраны автоматически, зависят от используемой биометрической системы. Биометрические системы должны автоматически записывать все попытки биометрической регистрации, верификации или идентификации, включая параметры требуемой идентичности, результаты сравнения и показатели качества. Это позволит свести к минимуму объем данных, записанных вручную, и вероятность ошибок расшифровки.

Если биометрические системы сохраняют биометрические образцы, то это дает следующие преимущества:

a) если изготовитель предоставил КПО или ПИП, то зарегистрированные биометрические контрольные шаблоны и результаты сравнения могут быть рассчитаны в режиме отложенного задания, что обеспечивает полное перекрестное сравнение биометрических проб с биометрическими контрольными шаблонами для получения большего количества результатов сравнения;

b) собранные биометрические образцы могут быть использованы в нескольких случаях: для проверки модифицированного алгоритма или (если биометрические образцы имеют соответствующий формат) для проверки других алгоритмов при технологическом испытании;

c) потенциальные ошибки в базе данных или метаданных могут быть проконтролированы визуально или при проверке записей транзакций.

8.2.2 Многие биометрические системы в нормальном режиме работы не сохраняют биометрические образцы, биометрические контрольные шаблоны или автоматические записи транзакций. При взаимодействии с изготовителем следует указать, что система должна обеспечивать выполнение функциональных возможностей, но при этом необходимо, чтобы эксплуатационные характеристики системы не были изменены. Например, запись биометрических образцов или биометрических признаков может замедлить работу биометрической системы и повлиять на поведение испытуемого субъекта. Если биометрические образцы или биометрические признаки не могут быть сохранены, то биометрическая регистрация и попытки парного и непарного сравнения должны быть проведены в режиме реального времени и результаты, при необходимости, должны быть зарегистрированы вручную. Для получения достоверных результатов необходимо обеспечить контроль за администраторами испытания и наблюдателями за испытанием.

8.2.3 Некоторые биометрические системы предоставляют решение о совпадении или несовпадении при данных настройках безопасности, но не предоставляют результаты сравнения. Если протокол испытания требует генерации компромиссного определения ошибки, то результаты попыток парного и непарного сравнения должны быть собраны или получены при разных настройках порогов. Изготовитель может сообщить соответствующий диапазон настроек порогов. Выбранные значения порогов (которые могут быть низкими, средними и высокими) будут характеризовать КОО вместо порога принятия решения. В этом случае при испытании в режиме реального времени каждый испытуемый субъект должен совершить требуемое число транзакций при каждой выбранной настройке безопасности.

Протоколы испытаний могут быть оформлены таким образом, что попытки парного сравнения будут отражены в порядке повышения толерантности биометрической системы, останавливаясь при получении совпадения, а попытки непарного сравнения — в порядке снижения толерантности системы, останавливаясь при получении несовпадения. Такое оформление протоколов не соответствует требованиям настоящего стандарта, так как результаты нескольких попыток могут быть ошибочно приняты за результаты изменения порога принятия решения.

8.2.4 План сбора данных должен соответствовать применимым нормативным актам, касающимся защиты данных и конфиденциальности. Для снижения вероятности ошибок и повышения быстродействия в план сбора данных следует включить метод удаления биометрических образцов и биографической информации об испытуемом субъекте по его запросу.

8.3 Биометрическая регистрация

8.3.1 Транзакции биометрической регистрации

8.3.1.1 Каждый испытуемый субъект должен зарегистрироваться в системе только один раз, но в результате биометрической регистрации может быть получено более одного биометрического контрольного шаблона в рамках одной регистрационной записи (например, биометрический контрольный шаблон для каждого отпечатка пальца или для нескольких различных положений лица). В процессе биометрической регистрации допускается проведение нескольких попыток с заранее определенным максимальным количеством попыток или максимальным затраченным временем. Необходимо избегать случайных биометрических регистраций.

8.3.1.2 Рекомендуется проверять работу систем биометрической идентификации, в которых пользователи могут иметь несколько регистрационных записей. В таких случаях количество испытуемых и кратность регистрационных записей с биометрическими контрольными шаблонами должны сообщаться с результатами испытания.

8.3.1.3 С помощью некоторых биометрических модальностей испытуемый субъект может предъявлять различные биометрические характеристики, например до десяти пальцев, левый и правый глаз. Чтобы максимально увеличить количество данных биометрической регистрации и биометрического распознавания, доступных экспериментатору, допускается интерпретировать биометрическую регистрацию различных характеристик одного и того же испытуемого субъекта как отдельные биометрические регистрации. Эта практика должна соответствовать предполагаемому способу функционирования испытуемой системы. Экспериментатор должен задокументировать и включить в протокол информацию о таком использовании. Несколько биометрических регистраций одного и того же испытуемого субъекта в данной системе не считают эквивалентными биометрическим регистрациям различных испытуемых субъектов, например с целью достижения уровня статистической значимости (см. также 8.4.1.3).

8.3.1.4 Во время биометрической регистрации могут быть проведены тренировочные попытки парного сравнения, чтобы удостовериться, что зарегистрированные биометрические образцы имеют достаточно высокое качество для дальнейшего сравнения, и ознакомить испытуемых субъектов с биометрической системой. Количественные результаты таких попыток не допускается регистрировать как часть записи попыток парного сравнения.

8.3.2 Условия биометрической регистрации

8.3.2.1 Условия биометрической регистрации должны соответствовать условиям биометрической регистрации при целевом применении биометрической системы. Таксономия (см. [*4*]) условий окружающей среды при биометрической регистрации определяет применимость результатов испытания. Следует руководствоваться рекомендациями изготовителя биометрической системы и обращать внимание на условия окружающей среды. Такие условия, как фоновый шум в случае верификации диктора или внешнее освещение в случае использования систем распознавания РОГ или лица, могут снизить качество биометрической регистрации, повлиять на вероятности ошибок биометрической регистрации и на результирующие вероятности распознавания. Особое значение для систем с оптическими элементами имеют свет, падающий непосредственно на датчик, и неконтролируемые отражения от биометрической характеристики. Условия освещения должны максимально соответствовать условиям целевой среды применения. Результаты испытаний, полученные в разных условиях окружающей среды, как правило, отличаются между собой.

8.3.2.2 Биометрическую регистрацию следует выполнять в одних и тех же условиях. Большое число попыток сбора данных может быть испорчено из-за изменений в протоколах или оборудовании в процессе длительного сбора данных*. Поэтому необходимо обеспечить такое управление представлением и эффектами канала передачи, чтобы данные эффекты были постоянными или изменялись случайным образом у всех испытуемых субъектов.

8.3.2.3 В процессе испытания администратор испытания может получить дополнительные сведения о системе, которые могут повлиять на последующие биометрические регистрации. Для предотвращения такой ситуации процесс биометрической регистрации и критерии вмешательства адми-

---

* Известным примером является «Большое разделение» в базе данных речи KING (см. [*5*]). Примерно на середине процесса сбора данных оборудование регистрации по неустановленной причине было временно демонтировано. Позже оно было снова установлено в соответствии с монтажной схемой; тем не менее амплитудно-частотные характеристики были немного изменены, что привело к разделению данных и усложнению анализа алгоритмов.

нистратора испытания должны быть определены заранее, кроме того, должно быть предусмотрено соответствующее обучение администратора испытания.

8.3.3 Отказы биометрической регистрации и ошибки предъявления

8.3.3.1 Биометрическая система может не принимать некоторые попытки биометрической регистрации. Модули контроля качества некоторых систем, требующих наличия большого числа биометрических образцов для биометрической регистрации, будут отклонять биометрические образцы, которые значительно изменяются между предъявлениями; другие модули контроля качества отклоняют отдельные низкокачественные биометрические образцы. Если данные модули позволяют настроить критерий принятия решения, то необходимо следовать рекомендациям изготовителя. Требуется обеспечить сохранение всех показателей качества при биометрической регистрации. Рекомендации или корректирующее действие в отношении испытуемых субъектов, совершивших неудачную попытку биометрической регистрации, должны быть определены заранее и указаны в плане испытания.

Примечание — Требования к качеству биометрических образцов установлены в серии стандартов под общим наименованием «Информационные технологии. Биометрия. Качество биометрического образца».

8.3.3.2 Число испытуемых субъектов, которые не смогли зарегистрироваться при выбранном критерии, должно быть зафиксировано и указано в протоколе как BOP. По возможности должны быть зафиксированы и указаны в протоколе причины отказа в биометрической регистрации (например, попытки, которые были предприняты без предъявления биометрических характеристик, а также случаи, когда биометрический образец не был получен, отказы или исключения алгоритма биометрической регистрации, когда система не может успешно выполнить биометрическую верификацию).

8.3.3.3 Проверка качества не должна быть полностью автоматической. Вмешательство администратора испытания требуется в случае несоответствия предъявленных при биометрической регистрации биометрических характеристик некоторым установленным критериям. Например, при биометрической регистрации испытуемые субъекты могут предъявить не тот палец, руку или глаз, зачитать неправильную регистрационную фразу или подписаться другим именем. Эти данные должны быть удалены, но должен быть обеспечен учет таких случаев.

8.3.3.4 Последовательность испытаний биометрического распознавания после биометрической регистрации может выявить неправильно собранные зарегистрированные биометрические контрольные шаблоны (например, получено неправильное положение пальца). Необходимо выполнять редактирование данных с целью удаления таких зарегистрированных биометрических контрольных шаблонов, при этом следует регистрировать влияние подобных изменений на эксплуатационные характеристики.

8.4 Попытки сравнения биометрической верификации (сравнение «один к одному»)

8.4.1 Общие положения

8.4.1.1 План сбора биометрических образцов должен обеспечивать сбор данных, характерных для выбранного сценария, и гарантировать отсутствие повторяющихся биометрических образцов.

8.4.1.2 Биометрические парные сравнения включают в себя испытуемых субъектов, представляющих биометрические образцы для сравнения с их собственными зарегистрированными биометрическими контрольными шаблонами. Биометрические непарные сравнения включают в себя испытуемых субъектов, представляющих биометрические образцы для сравнения с несобственными зарегистрированными биометрическими контрольными шаблонами.

8.4.1.3 Если различные характеристики одного и того же испытуемого субъекта рассматривают как отдельные биометрические регистрации (см. 8.3.1.3), то попытки биометрического непарного сравнения не должны включать в себя сравнение биометрических характеристик одного испытуемого субъекта. Сравнение биометрических характеристик одного испытуемого субъекта не эквивалентно сравнению между испытуемыми субъектами. При сравнении в режиме реального времени испытуемый субъект может ошибочно предъявить неверно зарегистрированную биометрическую характеристику, которая будет расценена как ложное совпадение.

Примеры

1 Отпечатки левого указательного и среднего пальца испытуемого субъекта могут иметь сходство и соответствовать с большей вероятностью, чем отпечатки пальцев разных испытуемых субъектов.

2 Сосудистые русла левой и правой ладоней у испытуемого субъекта имеют различную направленность и могут быть менее схожими, чем сосудистые русла правой ладони у двух разных испытуемых субъектов.

8.4.1.4 Попытки сравнения проводят в режиме реального времени и/или в режиме отложенного задания. Использование режима реального времени или режима отложенного задания для попыток сравнения, как правило, зависит от типа испытания:

- в технологическом испытании попытки сравнения проводят в режиме отложенного задания;
- в сценарном испытании попытки сравнения проводят в режиме реального времени;
- в оперативном испытании попытки сравнения проводят в режиме реального времени.

Иногда системы, тестируемые в сценарном или оперативном испытании, сохраняют собранные биометрические образцы или извлеченные биометрические признаки. В таких случаях сохраненные данные могут быть использованы для создания дополнительных попыток в режиме отложенного задания, результаты которых допускается представлять в протоколе испытания вместе с результатами, полученными в режиме реального времени.

8.4.2 Условия сбора данных

Данные попыток сравнения следует собирать в условиях окружающей среды, как можно более точно соответствующих условиям целевого применения биометрической системы. В течение процесса сбора данных эти условия не должны изменяться. Мотивация испытуемых субъектов и уровень их обучения и осведомленности о биометрической системе должны соответствовать целевому применению конкретной биометрической системы. Попытки непарного сравнения проводят в таких же условиях, как и попытки парного сравнения.

В процессе сбора данных необходимо обеспечить, чтобы эффекты предъявления и канала передачи были постоянными или изменялись случайно во всей выборке испытуемых субъектов. Если данные эффекты остаются постоянными во всей выборке, то те же эффекты предъявления и канала передачи при биометрической регистрации должны быть обеспечены также для сбора данных испытаний. Систематический разброс эффектов предъявления и канала передачи между данными биометрической регистрации и данными испытаний приводит к искажению результатов. Если эффекты предъявления и канала передачи будут изменяться в выборке испытуемых субъектов случайно, то экспериментатор должен проанализировать результаты и сообщить о любой корреляции между ними между сеансами биометрической регистрации и сравнения.

8.4.3 Частота использования

В идеальном случае между биометрической регистрацией и сбором данных попыток сравнения испытуемые субъекты должны использовать биометрическую систему с такой же частотой, как и при целевом применении. Такое использование испытуемой группы может быть нерентабельным. Следует отказаться от любого предварительного применения биометрической системы и предоставить возможность повторного ознакомления с ней непосредственно перед попытками сравнения.

8.4.4 Системы, выполняющие оптимизацию на основе зарегистрированных биометрических контрольных шаблонов

Для тех систем, которые реализуют такие методы, как нормализация результатов сравнения на основе зарегистрированных биометрических контрольных шаблонов для повышения эксплуатационных характеристик сравнения, до проведения попыток парного и непарного сравнения должно быть зарегистрировано достаточное число испытуемых субъектов.

8.4.5 Системы, выполняющие адаптацию биометрических контрольных шаблонов

Испытания биометрических систем, адаптирующих биометрические контрольные шаблоны после успешной биометрической верификации, следует проводить до начала биометрической регистрации и сбора данных попыток парного сравнения. Объем испытания должен быть определен до начала сбора данных и указан в протоколе испытаний.

Адаптация биометрических контрольных шаблонов должна быть отключена во время попыток непарного сравнения. Если это невозможно, то попытки непарного сравнения должны быть отложены до тех пор, пока не будут завершены все попытки парного сравнения.

8.4.6 Процессы для ошибок при вводе данных и неправильном использовании системы

Для предотвращения ошибок при вводе данных и для документирования любых внештатных ситуаций во время сбора данных необходимо обеспечить контроль сбора данных. Ввод путем нажатия клавиш должен быть минимизирован как со стороны испытуемых субъектов, так и со стороны администраторов испытания. Данные могут быть повреждены испытуемыми субъектами, которые намеренно неправильно используют систему. Для предотвращения таких действий персонал, проводящий испытания, должен предпринять соответствующие меры. При этом данные не следует удалять из базы данных до тех пор, пока не будет получено дополнительное подтверждение ненадлежащего использования системы.

8.4.7 Отказы сбора данных

В ряде случаев испытуемые субъекты не могут предоставить системе пригодный биометрический образец, что определяет администратор испытания или модуль контроля качества. Персонал, проводящий испытания, должен зарегистрировать информацию о попытках, закончившихся отказом сбора данных. ВОСД определяется числом таких попыток и зависит от порога качества. Как и при биометрической регистрации, пороги качества должны быть установлены в соответствии с рекомендациями изготовителя.

Примечание — Параметры настройки порога качества (и порога принятия решения) могут влиять на действия испытуемых субъектов: более высокие пороги способствуют более осторожному предъявлению биометрической характеристики; более низкие пороги допускают большую свободу действий. Поэтому база данных может быть не столь независимой от порога, как предполагается.

8.4.8 Добавление данных испытания в базу данных

Все попытки, включая отказы сбора данных, должны быть зафиксированы. Рекомендуется записывать также значения качества для каждого биометрического образца, если они доступны, а при проведении испытания в режиме реального времени — результат(ы) сравнения.

Данные транзакций должны быть добавлены в базу данных независимо от того, действительно ли они соответствуют зарегистрированному биометрическому контрольному шаблону. Программное обеспечение некоторых изготовителей не осуществляет запись данных транзакции, если она не соответствует зарегистрированному биометрическому контрольному шаблону. В этом случае при сборе данных происходит смещение в направлении недооценивания ВЛНС. Поэтому ошибки несовпадения должны быть записаны вручную. Данные должны быть исключены только по заранее установленным причинам, не зависимым от результатов сравнения.

8.4.9 Попытки сравнения в режиме реального времени

Попытки сравнения в режиме реального времени осуществляются при совершении каждым испытуемым субъектом транзакций биометрического распознавания по отношению:

a) к собственным биометрическим контрольным шаблонам в случае попыток парного сравнения;

b) каждому из ранее определенного числа биометрических контрольных шаблонов, отобранных случайным образом из всех предыдущих биометрических регистраций в случае попыток непарного сравнения. Выбор регистрационных шаблонов может быть ограничен одной демографической группой. Случайный выбор должен быть независимым между испытуемыми субъектами. Из-за нестационарного статистического характера данных испытуемых субъектов рекомендуется использовать больше посторонних испытуемых субъектов, каждый из которых испытывает несколько случайно выбранных несобственных шаблонов, вместо того чтобы использовать несколько испытуемых субъектов, испытывающих множество несобственных шаблонов.

Итоговые результаты сравнения записывают вместе с идентификаторами испытуемого субъекта и биометрического контрольного шаблона. Поскольку попытки парного и непарного сравнения проводят одновременно, необходимо соблюдать осторожность, чтобы результаты были отнесены к правильной идентичности.

Если испытуемый субъект осведомлен, что проводится непарное сравнение, то изменение манеры предъявления может привести к нерепрезентативным результатам, особенно если используется биометрическая система, основанная преимущественно на поведенческих характеристиках. Поэтому, чтобы избежать даже подсознательных изменений в предъявлении, рекомендуется не сообщать испытуемому субъекту о том, что проводится парное или непарное сравнение.

Попытки непарного сравнения могут быть проведены до того, как будут зарегистрированы все испытуемые субъекты. Первые зарегистрированные биометрические контрольные шаблоны будут иметь более высокую вероятность непарного сравнения, но это не будет вносить систематическую ошибку при вычислении вероятности ложного совпадения, если испытуемые субъекты зарегистрированы в порядке, который не имеет отношения к качеству их биометрических характеристик.

8.4.10 Попытки сравнения в режиме отложенного задания

Попытки сравнения в режиме отложенного задания получают путем сравнения ранее собранных биометрических признаков с зарегистрированными биометрическими контрольными шаблонами. Ранее собранные биометрические признаки или биометрические пробы могут быть получены от зарегистрированных испытуемых субъектов или от отдельного набора незарегистрированных испытуемых субъектов. При выполнении вычислений в режиме отложенного задания можно использовать метод

полного перекрестного сравнения, при котором каждую биометрическую пробу сравнивают с каждым биометрическим контрольным шаблоном.

Не рекомендуется использовать дополнительные базы данных биометрических образцов или биометрических контрольных шаблонов, собранных при различных (как правило, неизвестных) условиях окружающей среды для различных выборок. Информация о таких базах данных должна быть приведена в протоколе испытания и включать в себя информацию о размере, характеристиках и других значимых факторах.

Попытки сравнения в режиме отложенного задания проводят таким же методом, как и попытки сравнения в режиме реального времени, нижеприведенным образом.

При попытках парного сравнения осуществляют сравнение каждой биометрической пробы с соответствующим парным биометрическим контрольным шаблоном.

При попытках непарного сравнения осуществляют:

- случайный выбор с заменой биометрических образцов и биометрических контрольных шаблонов для попыток непарного сравнения;

- случайный выбор для каждой биометрической пробы, собранной при попытке парного сравнения множества несобственных биометрических контрольных шаблонов из всех зарегистрированных биометрических контрольных шаблонов для сравнения с биометрическими признаками образца (случайный выбор биометрических контрольных шаблонов, являющихся независимыми для каждой биометрической пробы), или

- полное перекрестное сравнение, при котором каждую собранную биометрическую пробу сравнивают с каждым несобственным биометрическим контрольным шаблоном. При наличии N биометрических контрольных шаблонов и M биометрических проб (от одной и той же испытуемой группы) может быть проведено $M(N-1)$ попыток непарного сравнения. Данные попытки непарного сравнения не будут статистически независимыми, но если испытуемые субъекты осуществят такое же количество транзакций, то результаты применения данного метода будут статистически объективными и представлять собой более эффективную технику оценки, чем использование случайно выбранных непарных сравнений (см. *[6]*).

Определение результатов сравнения в режиме отложенного задания проводят с помощью программных модулей, предоставленных изготовителями КПО. Первый модуль создает биометрические контрольные шаблоны из биометрических образцов при биометрической регистрации, второй — биометрические пробы из биометрических образцов при биометрическом распознавании. Данные модули могут быть объединены. Третий модуль возвращает результат сравнения. Некоторые изготовители предоставляют инструменты оценки в режиме отложенного задания, использующие истинную информацию для каждого сравнения, чтобы облегчить анализ результатов. Такие инструменты следует использовать только для проверки результатов, полученных испытательной лабораторией.

Если оценка включает в себя попытки сравнения и в режиме реального времени, и в режиме отложенного задания, то администратор испытания должен обеспечить использование одного и того же алгоритма и одних и тех же настроек параметров (например, одна и та же фоновая модель) в обоих случаях.

8.4.11 Попытки непарного сравнения в режиме отложенного задания с зависимыми биометрическими контрольными шаблонами

Для биометрических систем с зависимыми биометрическими контрольными шаблонами объективные попытки непарного сравнения могут быть получены путем использования метода «вырезания» для создания зарегистрированных биометрических контрольных шаблонов. Метод «вырезания» заключается в биометрической регистрации всей испытуемой группы с единственным пропущенным испытуемым субъектом, и подмножество попыток непарного сравнения осуществляется для пропущенного испытуемого субъекта и всех зарегистрированных биометрических контрольных шаблонов. Процесс биометрической регистрации повторяют для каждого члена испытуемой группы, и в результате формируется полное множество результатов непарного сравнения.

Допускается использовать более простой метод, при котором испытуемую группу случайным образом разделяют на зарегистрированных и незарегистрированных испытуемых субъектов. Попытки парного сравнения основаны на попытках биометрического распознавания, осуществляемых зарегистрированными испытуемыми субъектами, в то время как попытки непарного сравнения основаны на попытках биометрического распознавания, осуществляемых незарегистрированными испытуемыми субъектами. В этом случае данные используют менее эффективно, чем при применении метода «вырезания».

8.4.12 Попытки непарного сравнения в режиме отложенного задания, основанные на сравнении биометрических контрольных шаблонов

Для получения результатов непарного сравнения допускается использовать перекрестное сравнение зарегистрированных биометрических контрольных шаблонов. Данный метод применяют, например, при оперативных испытаниях, когда биометрические образцы или биометрические признаки не сохраняются. Каждый из *N* испытуемых (или зарегистрированных) биометрических контрольных шаблонов сравнивают с оставшимися (*N* – 1) испытуемыми (или зарегистрированными) биометрическими контрольными шаблонами. Перекрестное сравнение биометрических контрольных шаблонов не следует применять, если:

a) биометрическая регистрация и верификация требуют одного и того же действия испытуемого субъекта (например, оба требуют единственного предъявления);

b) биометрическая регистрация и биометрическая верификация используют одни и те же алгоритмы для извлечения и кодирования биометрических признаков образца;

c) пороги качества для биометрической регистрации такие же, как и для биометрической верификации.

При несоблюдении данных требований перекрестное сравнение биометрических контрольных шаблонов может привести к появлению систематической ошибки в результатах непарного сравнения (см. *[4]*). Данное утверждение справедливо как для случая, когда зарегистрированный биометрический контрольный шаблон усреднен, так и для случая, когда он выбран для наиболее соответствующего зарегистрированного биометрического образца. Методы исправления данной систематической ошибки отсутствуют.

8.4.13 Использование биометрических образцов от транзакций сравнения при нескольких попытках сбора данных

Большинство биометрических систем осуществляют сбор и обработку последовательности биометрических образцов, используя одну попытку, например:

a) сбор биометрических образцов за установленный период времени и определение наиболее совпадающего биометрического образца;

b) сбор биометрических образцов до тех пор, пока не будет получено совпадение или пока не истечет установленный период времени;

c) сбор биометрических образцов до тех пор, пока не будет получен один биометрический образец удовлетворительного качества или пока не истечет установленный период времени;

d) сбор второго биометрического образца, если результат сравнения первого биометрического образца близок к порогу принятия решения.

В таких случаях единственный биометрический образец, собранный при попытке парного распознавания, может не подходить как биометрическая проба для попытки непарного сравнения. В случае, указанном в перечислении a), собранным биометрическим образцом будет тот, который в наибольшей степени совпадает с заявленным биометрическим контрольным шаблоном при попытке парного сравнения, а не тот, который в наибольшей степени совпадает с биометрическим контрольным шаблоном при попытке непарного сравнения. Чтобы оценить целесообразность перекрестного сравнения на данных, полученных при попытках парного сравнения, следует ответить на следующие вопросы:

- зависит ли сохраненный биометрический образец от биометрического контрольного шаблона, с которым сравнивается?

- существенно ли этот способ влияет на получаемые результаты сравнения?

Если ответы на оба данных вопроса будут положительными, то должна быть сохранена и использована в анализе в режиме отложенного задания целая последовательность биометрических образцов или попытки непарного сравнения должны быть получены в режиме реального времени.

8.5 Попытки биометрической идентификации (сравнение «один ко многим»)

8.5.1 Общие положения

Попытки биометрической идентификации должны быть собраны и записаны тем же методом, что и попытки биометрической верификации, за исключением того, что регистрируемые результаты попыток биометрической идентификации состоят из списка кандидатов, содержащего ноль, один или более идентификаторов. Рекомендуется возвращать результаты сравнения для каждого кандидата, чтобы обеспечить возможность анализа в диапазоне рабочих порогов. Если биометрическая система определяет показатели качества, то они также должны быть зафиксированы.

Транзакции биометрической идентификации выполняют в режиме отложенного задания и проводят при различных размерах базы данных, чтобы определить зависимость эксплуатационных характеристик биометрической идентификации от размера базы данных.

При биометрической идентификации допускается использовать предварительный отбор для ограничения числа биометрических контрольных шаблонов, сравниваемых с помощью соответствующего алгоритма. Для определения производительности алгоритма предварительного отбора записывают число предварительно отобранных биометрических контрольных шаблонов для каждой попытки биометрической идентификации (см. приложение D).

8.5.2 Испытание биометрической идентификации с незарегистрированными испытуемыми субъектами

В дополнение к зарегистрированным испытуемым субъектам испытание биометрической идентификации должно включать в себя испытуемых субъектов, не зарегистрированных в биометрической системе, для обеспечения значимой оценки ВЛПИ. Эти незарегистрированные испытуемые субъекты не должны быть испытуемыми субъектами, у которых произошел отказ биометрической регистрации. Транзакции идентификации зарегистрированных испытуемых субъектов проводят при тех же условиях.

8.5.3 Использование метода «вырезания» для испытания биометрической идентификации

Если регистрационные и идентификационные биометрические образцы зарегистрированных испытуемых субъектов сохранены, то транзакции биометрической идентификации незарегистрированных испытуемых субъектов могут быть выполнены в режиме отложенного задания методом «вырезания». Для этого регистрируют всю испытуемую группу с единственным пропущенным испытуемым субъектом. Затем система пытается осуществить идентификацию пропущенного испытуемого субъекта в оставшейся испытуемой группе. Данный процесс повторяют для каждого испытуемого субъекта. В этом случае также следует учитывать положения 8.4.11.

9 Анализ

9.1 Общие положения

9.1.1 Если испытуемая группа представляет собой целевую выборку, в которой каждый испытуемый субъект имеет один зарегистрированный биометрический контрольный шаблон и одинаковое число (и структуру) транзакций, то наблюдаемые вероятности ошибок будут наиболее соответствовать действительным вероятностям ошибок.

9.1.2 Если испытуемая группа не представляет собой целевую выборку (например, при избыточном представлении известных проблемных случаев) или транзакции отдельных испытуемых субъектов нетипичны для испытуемой группы в целом (например, отдельный испытуемый субъект выполняет больше или меньше транзакций в отличие от типичного испытуемого субъекта), то скомпенсировать неустойчивость можно путем взвешивания результатов. Если вероятности ошибок оценивают с использованием весовых коэффициентов, то это должно быть зафиксировано в протоколе испытания. При использовании взвешивания по классу испытуемых субъектов наблюдаемые вероятности ошибок класса также должны быть зафиксированы в протоколе испытаний.

Пример — Если испытуемые субъекты проводят разное число попыток биометрической верификации или биометрической идентификации, то ошибки каждого испытуемого субъекта могут быть взвешены в обратной пропорции к числу совершаемых им попыток, так как простая пропорция может сместить ожидаемые вероятности ошибок к «тяжелым» пользователям системы или к тем испытуемым субъектам, которым для допуска нужно выполнить несколько попыток.

9.1.3 Рекомендуется определять вероятности ошибок для каждого отдельного класса группы испытуемых субъектов (например, отдельные вероятности ошибок для мужчин и женщин) или для отдельного вида биометрических характеристик (например, определение вероятности ошибок для каждого положения пальца).

9.1.4 Если ошибки возникают при биометрической регистрации, сборе биометрических образцов, биометрической верификации или биометрической идентификации, их можно классифицировать по причине или стадии процесса биометрической регистрации, сбора или сравнения, а также определить отдельные вероятности ошибок для различных случаев или для различных компонентов процесса.

9.2 Эксплуатационные характеристики биометрической регистрации

9.2.1 Вероятность отказа биометрической регистрации

9.2.1.1 BOP — это доля транзакций биометрической регистрации, для которых система не может создать и сохранить биометрический контрольный шаблон в соответствии с политикой биометрической регистрации, от общего количества транзакций биометрической регистрации. BOP должна включать в себя испытуемые субъекты, которые:

- неспособны предъявить необходимую биометрическую характеристику;
- при биометрической регистрации неспособны предоставить биометрический образец удовлетворительного качества;
- не могут получить подтверждение о совпадении со своим заново созданным биометрическим контрольным шаблоном в процессе подтверждения применимости биометрической регистрации.

Примечания

1 Политика биометрической регистрации, как правило, допускает повторные попытки биометрической регистрации для получения надежного биометрического контрольного шаблона.

2 BOP рекомендуется определять для различных биометрических образцов, например: сообщать о разных значениях BOP для больших, указательных пальцев и т. д.

3 При технологическом испытании анализ основан на предварительно собранной базе данных и сбор биометрического образца не вызывает проблем. Даже в этом случае могут произойти отказы биометрической регистрации, например: когда биометрический образец имеет настолько низкое качество, что извлечь из него биометрические признаки невозможно.

9.2.1.2 BOP для целевой выборки следует определять как долю испытуемых субъектов в испытуемой группе, которые не смогли зарегистрироваться при определенной политике биометрической регистрации, от общего количества испытуемых субъектов в испытуемой группе.

9.2.1.3 BOP зависит от политики регистрации, которая определяет уровень качества биометрического образца для биометрической регистрации, порог принятия решения для подтверждения применимости биометрической регистрации, а также число попыток или время, отведенное на транзакцию биометрической регистрации. Политика биометрической регистрации должна быть описана в протоколе испытаний наряду с наблюдаемой BOP.

Примечание — Более жесткие требования к качеству биометрической регистрации увеличивают BOP, но улучшают эксплуатационные характеристики совпадения.

9.2.1.4 Попытки биометрической регистрации испытуемых субъектов, не способных зарегистрироваться в биометрической системе, не должны вносить вклад в BOCД или вероятности ошибок совпадения. При этом их учитывают в обобщенных вероятностях ошибок допуска.

9.2.2 Продолжительность транзакции биометрической регистрации

Средняя продолжительность транзакции биометрической регистрации должна быть измерена и зафиксирована в протоколе испытания.

При сравнительных сценарных испытаниях может оказаться невозможным установить пороги для допустимого времени или качества биометрического образца согласованным образом для всех технологий биометрической регистрации. В этих случаях один из подходов заключается в том, чтобы рассматривать указанные переменные как контролируемые факторы данной технологии биометрической регистрации и измерять, насколько быстро выполняется сбор биометрического образца. Затем для каждой технологии биометрической регистрации можно рассчитать функцию распределения в зависимости от продолжительности сбора данных, например график зависимости BOP от продолжительности. Таким образом, экспериментатор может фиксировать в протоколе испытания наблюдаемую BOP, не устанавливая и не фиксируя порог качества биометрического образца и допустимую продолжительность сбора биометрического образца по всей системе.

9.3 Эксплуатационные характеристики сбора данных

9.3.1 Вероятность отказа сбора данных

9.3.1.1 BOCД — это доля процессов сбора биометрических данных для попыток биометрической верификации или биометрической идентификации, для которых биометрическая система не может осуществить сбор биометрического образца удовлетворительного качества, от общего количества

процессов сбора данных для попыток биометрической верификации или биометрической идентификации. ВОСД должна включать в себя попытки, при которых:

- биометрическая характеристика не может быть предъявлена (например, из-за временной болезни или раны) или собрана;
- не удается выполнить сегментацию или извлечение биометрических признаков;
- извлеченные биометрические признаки не подходят по порогу проверки качества.

Примечания

1 ВОСД можно определить для каждой транзакции, например: путем определения числа транзакций, в процессе которых ни при одной из предпринятых попыток не был получен биометрический образец удовлетворительного качества для сравнения.

2 При технологическом испытании анализ основан на предварительно собранной базе данных. В этом случае не должно происходить отказов сбора биометрического образца. Тем не менее отказы сбора данных возможны, если биометрический образец имеет слишком низкое качество для извлечения биометрических признаков.

9.3.1.2 ВОСД следует определять как долю попыток (для попыток парного сравнения), которые не могут быть завершены из-за отказов при предъявлении (биометрический образец не собран), сегментации, извлечении биометрических признаков или при контроле качества.

9.3.1.3 ВОСД зависит от порога качества биометрического образца, а также от времени, установленного на сбор биометрического образца, или от допускаемого числа предъявлений. Данные параметры настройки должны быть указаны в протоколе испытаний вместе с наблюдаемой ВОСД.

Примечание — Более жесткий порог качества для сбора биометрических образцов увеличивает ВОСД, но улучшает эксплуатационные характеристики совпадения.

9.3.1.4 Попытки, при которых биометрический образец не был получен или не имеет удовлетворительного качества, не обрабатываются алгоритмом сравнения, а результат сравнения не определяется. Такие отказы сбора данных должны быть исключены при вычислении ВЛС и ВЛНС, но должны быть включены в вычисления ВЛД и ВЛНД. ВОСД, ВЛС и ВЛНС должны быть вычислены при одних и тех же порогах качества.

9.3.2 Продолжительность сбора данных

При сравнительных сценарных испытаниях может оказаться невозможным установить пороги для допустимого времени сбора данных или качества биометрического образца согласованным образом для всех технологий. В этих случаях один из подходов заключается в том, чтобы рассматривать эти переменные как контролируемые факторы данной технологии и измерять, насколько быстро выполняется сбор биометрического образца. Затем для каждой технологии можно рассчитать функцию распределения в зависимости от продолжительности сбора данных, например график зависимости ВОСД от продолжительности. Таким образом, экспериментатор регистрирует в протоколе испытания наблюдаемую вероятность отказов сбора данных, не устанавливая и не фиксируя порог качества биометрического образца и допустимую продолжительность сбора биометрического образца по всей системе.

9.3.3 Другие аспекты эксплуатационных характеристик сбора данных

9.3.3.1 В зависимости от данных, полученных в процессе сбора, можно отдельно проанализировать различные причины отказов, например: отказа сегментации, отказа извлечения биометрических признаков или отказа вследствие неудовлетворительного качества биометрического образца.

9.3.3.2 С помощью соответствующей базы данных, обеспечивающей определенную базовую истинную информацию, можно измерить точность сегментации. Значения точности сегментации будут варьироваться в зависимости от рассматриваемой биометрической модальности.

9.4 Эксплуатационные характеристики сравнения «один к одному»

9.4.1 Вероятность ложного несовпадения

9.4.1.1 ВЛНС — это доля завершенных попыток парного сравнения, при которых парная биометрическая проба и биометрический контрольный шаблон ошибочно признаны несовпадающими, от общего количества завершенных попыток парного сравнения.

9.4.1.2 ВЛНС зависит от порога принятия решения о совпадении и должна быть указана вместе с наблюдаемой ВЛС при том же пороге (или показана в зависимости от ВЛС при том же пороге на графике КОО).

9.4.1.3 При испытаниях, в которых испытуемые субъекты совершили несколько попыток, следует указать, как ВЛНС изменяется в пределах испытуемой группы: путем вычисления вероятности ошибки

для попыток каждого испытуемого субъекта и построения гистограммы, показывающей вероятность ошибки для каждого испытуемого субъекта, упорядочивания испытуемых субъектов по возрастанию значений вероятностей ошибок.

9.4.2 Вероятность ложного совпадения

9.4.2.1 ВЛС — это доля завершенных попыток непарного сравнения, при которых непарная биометрическая проба и биометрический контрольный шаблон ошибочно признаны совпадающими, от общего количества завершенных попыток непарного сравнения.

Примечание — При попытках непарного сравнения биометрические пробы, как правило, получают от испытуемых субъектов, предъявляющих собственные биометрические характеристики, как будто они совершают попытку успешной биометрической верификации с собственным биометрическим контрольным шаблоном без какой-либо попытки подмены. Например, в случае динамической верификации подписи испытуемый субъект скорее поставит собственную подпись, чем подпись, соответствующую непарному биометрическому контрольному шаблону. Если испытуемый субъект может легко воспроизвести свойства требуемой биометрической характеристики, то вторая вероятность непарного сравнения может быть мерой, допускающей определенную степень имитации. Настоящий стандарт не распространяется на методы или уровень навыка, которые используют при подмене.

9.4.2.2 ВЛС зависит от порога принятия решения о совпадении и должна быть указана наряду с наблюдаемой ВЛНС при том же пороге (или показана в зависимости от ВЛНС при том же пороге на графике КОО).

9.4.2.3 Если испытуемый субъект зарегистрирован и его биометрическая регистрация оказывает влияние на биометрические контрольные шаблоны других испытуемых субъектов в системе или если алгоритм сравнения изменяется, используя данный и другие биометрические контрольные шаблоны, то попытки непарного сравнения, использующие данный испытуемый субъект, будут вносить систематическую ошибку, поэтому их не следует применять для оценки ВЛС (см. 8.4.11).

9.4.2.4 Сравнение наследственно идентичных биометрических характеристик (например, между указательным и средним пальцами или у идентичных близнецов) приводит к другому распределению результатов сравнения, чем сравнение различных по происхождению характеристик (см. *[7]—[9]*). В плане испытания должна быть определена политика в отношении того, следует ли включать непарные сравнения, такие как между идентичными близнецами, братьями и сестрами или родителем и ребенком, в ВЛС. Сравнения между двумя биометрическими образцами одного и того же испытуемого субъекта должны быть исключены.

Примечания

1 Частота появления идентичных (монозиготных) близнецов составляет приблизительно три или четыре случая на 1000 родов, и их присутствие в развернутой биометрической системе распознавания лица может увеличить ВЛС по сравнению с ВЛС, измеренной при исключении таких генетически сходных сравнений.

2 Генетические эффекты могут быть распространены не только на идентичных близнецов, но и на семьи и национальность. Например, при биометрическом распознавании лица это может привести к гораздо более высокой ВЛС между испытуемыми субъектами, родившимися в одной стране, чем между испытуемыми субъектами из географически и этнически различных стран.

9.4.2.5 В протоколе испытаний, в которых проводят несколько попыток непарного сравнения на каждый испытуемый субъект или биометрический контрольный шаблон, должно быть указано, как ВЛС изменяется в пределах числа испытуемых субъектов и сохраненных биометрических контрольных шаблонов. Для этого необходимо определить вероятность индивидуальной ошибки ложного совпадения для биометрического контрольного шаблона и для биометрических проб каждого испытуемого субъекта. Чтобы показать вероятность ошибки для каждого испытуемого субъекта, следует построить гистограммы, упорядочивая испытуемые субъекты по возрастанию значений вероятностей ошибок.

Пример — Биометрическая система распознавания лица может пропустить ряд «золотых» лиц, для которых главным образом происходят ложные совпадения. Данную уязвимость системы можно определить по гистограмме, показывающей изменение вероятностей ошибок по испытуемым субъектам.

9.5 Эксплуатационные характеристики биометрической системы верификации

9.5.1 Общие положения

Определение ВЛД и ВЛНД для транзакций с несколькими попытками допускается проводить с помощью кривой КОО. При таком определении не учитывают корреляцию между последовательными попытками и сравнениями в отношении одного и того же испытуемого субъекта, и, следовательно, оно

может быть неточным. Поэтому данные эксплуатационные характеристики рекомендуется получать путем транзакций с несколькими попытками в соответствии с политикой принятия решения.

9.5.2 Вероятность ложного недопуска

9.5.2.1 ВЛНД — это доля транзакций биометрической верификации с истинным биометрическим заявлением, которые были ошибочно отвергнуты, от общего количества транзакций биометрической верификации с истинным биометрическим заявлением. В зависимости от политики принятия решения транзакция может состоять из одной или более попыток.

9.5.2.2 Транзакции биометрической верификации, которые были ошибочно отвергнуты из-за отказа сбора данных и ошибок сравнения, включают в расчет ложного недопуска. Для биометрических систем верификации с положительными биометрическими заявлениями (например, для контроля доступа) допуск потребует успешного сбора биометрических характеристик и решения о совпадении в результате сравнения.

Пример — Если для биометрической системы верификации с положительными биометрическими заявлениями транзакция верификации состоит из единственной попытки, то отказ сбора данных или ложное несовпадение вызовут ложный недопуск, и ВЛНД вычисляют по формуле

$$ВЛНД = ВОСД + ВЛНС(1 – ВОСД). \quad (1)$$

9.5.2.3 ВЛНД зависит от политики принятия решения, порога принятия решения о совпадении и качества биометрического образца. ВЛНД должна быть указана в протоколе испытания вместе с данными параметрами с оценкой ВЛД для тех же параметров (или должна быть построена зависимость ВЛНД от ВЛД при тех же порогах путем построения графика КОО).

9.5.3 Вероятность ложного допуска

9.5.3.1 ВЛД — это доля транзакций с ложным биометрическим заявлением, которые были ошибочно приняты, от общего количества транзакций с ложным биометрическим заявлением. В зависимости от политики принятия решения транзакция может состоять из одной или более попыток.

9.5.3.2 Недопуски из-за отказа сбора данных включают в число транзакций, но не в число ложных допусков. Для биометрических систем верификации с положительными биометрическими заявлениями (например, для контроля доступа) допуск потребует успешного сбора биометрических характеристик и решения о совпадении в результате сравнения.

Пример — Если транзакция верификации с положительным биометрическим заявлением состоит из единственной попытки, то успешный сбор данных и последующее ложное совпадение приведут к ложному допуску, и ВЛД вычисляют по формуле

$$ВЛД = ВЛС(1 – ВОСД). \quad (2)$$

9.5.3.3 ВЛД зависит от политики принятия решения, порога принятия решения о соответствии и порога качества биометрического образца, а также от установленной продолжительности или числа предъявлений. ВЛД должна быть указана в протоколе испытания вместе с данными параметрами с оценкой ВЛНД для тех же параметров (или должна быть построена зависимость ВЛД от ВЛНД при тех же порогах путем построения графика КОО).

9.5.4 Продолжительность транзакции биометрической верификации

9.5.4.1 При сравнительных сценарных испытаниях может оказаться невозможным установить пороги для допустимого времени сбора или качества биометрического образца согласованным образом для всех технологий. В этих случаях один из подходов заключается в том, чтобы рассматривать эти переменные как контролируемые факторы данной технологии и измерять, насколько быстро выполнен сбор биометрического образца. Затем для каждой технологии можно рассчитать функцию распределения в зависимости от продолжительности сбора данных, например график зависимости ВЛНД от продолжительности. Таким образом, экспериментатор регистрирует в протоколе испытания наблюдаемую ВЛНД, не устанавливая и не фиксируя сведения о конфигурации разных систем.

9.5.4.2 Для уменьшения влияния более длительной транзакции из-за недостаточных навыков использования системы или перерывов в процессе испытания среднюю продолжительность успешной транзакции биометрической верификации рассчитывают следующим образом:

a) для каждого испытуемого субъекта определяют среднее значение продолжительности успешных транзакций парной биометрической верификации;

b) затем эти значения усредняют по всем (зарегистрированным) испытуемым субъектам.

9.5.5 Обобщенные вероятности ложного допуска и недопуска

Для сравнения биометрических систем, имеющих различные ВОР, следует использовать обобщенные ВЛД и ВЛНД, которые включают в себя ошибки, возникающие при биометрической регистрации, сборе биометрических образцов и определении совпадения. Метод обобщения должен соответствовать испытанию. Как правило, обобщение должно включать в себя отказы биометрической регистрации как если бы биометрическая регистрация завершилась, но все последующие транзакции биометрической верификации или биометрической идентификации с данным регистрируемым испытуемым субъектом или с его биометрическим контрольным шаблоном были неудачными. Метод обобщения указывают в протоколе испытания.

Примеры

1 Проводят сценарное испытание биометрической системы верификации с положительным биометрическим заявлением, допускающей единственную попытку для транзакции биометрической верификации. Испытуемые субъекты, которые не могут быть зарегистрированы, не принимают дальнейшего участия в испытании. Протокол испытаний включает проведение полного перекрестного сравнения между биометрическими пробами и биометрическими контрольными шаблонами всех испытуемых субъектов. В этом случае обобщенный ложный допуск происходит, если испытуемый субъект, предоставляющий биометрическую пробу, и испытуемый субъект, предоставляющий биометрический контрольный шаблон, зарегистрированы, если произошел успешный сбор биометрической пробы и получено ложное совпадение. Обобщенный ложный недопуск происходит, если испытуемый субъект не зарегистрирован, или предложенный биометрический образец не может быть получен, или происходит ложное несовпадение. ОВЛД вычисляют по формуле

$$ОВЛД = ВЛС\ (1 - ВОСД) \cdot (1 - ВОР)^2. \quad (3)$$

ОВЛНД вычисляют по формуле

$$ОВЛНД = ВОР + (1 - ВОР) \cdot ВОСД + (1 - ВОР) \cdot (1 - ВОСД) \cdot ВЛНС. \quad (4)$$

2 При технологическом испытании биометрические контрольные шаблоны, полученные в результате биометрической регистрации, создают из всех образцов биометрических контрольных шаблонов, которые не вызывают отказа биометрической регистрации, и биометрические признаки создают из всех образцов биометрических проб, которые не вызывают отказа сбора данных. В этом случае ОВЛД вычисляют по формуле

$$ОВЛД = ВЛС\ (1 - ВОСД) \cdot (1 - ВОР). \quad (5)$$

ОВЛНД вычисляют по формуле

$$ОВЛНД = ВОР + (1 - ВОР) \cdot ВОСД + (1 - ВОР) \cdot (1 - ВОСД) \cdot ВЛНС. \quad (6)$$

9.6 Эксплуатационные характеристики биометрической системы идентификации

9.6.1 Общие положения

Определение вероятности ошибки биометрической идентификации зависит от рабочих характеристик и настроек используемых системы или алгоритма сравнения. Существует три основных параметра, определяющих эти характеристики:

- число биометрических контрольных шаблонов N, зарегистрированных в базе данных;
- индекс ранга R, где только кандидаты рангов от 1 до R рассматриваются в качестве потенциальных идентификаторов для испытуемого субъекта (R, как правило, ограничен длиной списка кандидатов L, возвращаемого испытуемой системой биометрической идентификации);
- порог принятия решения T, используемый для определения кандидатов, потенциально совпадающих с испытуемым субъектом.

Данные параметры должны быть определены для вычисления вероятности ошибок биометрической идентификации.

Примечание — Если R установлен равным N, то кандидаты возвращаются исключительно на основании превышения порога T. Аналогично если T установлен равным 0 (предполагается, что это минимально возможная степень схожести), то кандидаты возвращаются исключительно на основе значения ранга.

9.6.2 Вероятность ложноотрицательной биометрической идентификации

9.6.2.1 ВЛОИ — это доля транзакций биометрической идентификации испытуемых субъектов, зарегистрированных в биометрической системе (транзакции парной биометрической идентификации), для которых правильный идентификатор субъекта не включен в возвращенный список кандидатов, от

общего числа транзакций биометрической идентификации испытуемых субъектов, зарегистрированных в биометрической системе. ВЛОИ вычисляют по формуле

ВЛОИ = (число транзакций парной биометрической идентификации, при которых зарегистрированные пары не входят в список кандидатов)/ (число транзакций парной биометрической идентификации). (7)

Примечание — Биометрические системы идентификации могут быть сконфигурированы таким образом, чтобы возвращать кандидатов, удовлетворяющих некоторому критерию, например с результатом сравнения, превышающим порог принятия решения *T*, и/или возвращать до фиксированного числа ранга *R* наиболее совпадающих кандидатов. ВЛОИ можно определить как долю транзакций непарной биометрической идентификации, в которых либо пара имеет ранг выше *R*, либо значение результата сравнения для пары ниже порога принятия решения *T*.

В этом случае ВЛОИ (*N*, *R*, *T*) вычисляют по формуле

ВЛОИ (*N*, *R*, *T*) = (число транзакций парной биометрической идентификации, при которых зарегистрированные пары либо не входят в верхние ранги *R*, либо их результаты не выше порога принятия решения *T*)/(число транзакций парной биометрической идентификации). (8)

9.6.2.2 Экспериментатор может вычислить ВЛОИ для *N*, *R* и *T* в их соответствующих диапазонах.

9.6.3 Вероятность ложноположительной биометрической идентификации

9.6.3.1 ВЛПИ — это доля транзакций биометрической идентификации испытуемых субъектов, не зарегистрированных в биометрической системе (непарный поиск), для которых схожесть с высокоранговыми кандидатами, при наличии, превышает порог принятия решения, от общего числа транзакций биометрической идентификации испытуемых субъектов, не зарегистрированных в биометрической системе. ВЛПИ (*N*, *T*) вычисляют по формуле

ВЛПИ (*N*, *T*) = (число транзакций непарной биометрической идентификации, при которых результат высокоранговых кандидатов превышает порог принятия решения *T*)/ (число транзакций непарной биометрической идентификации). (9)

Взаимосвязь ВЛПИ (*N*, *T*) и ВЛОИ (*N*, 1, *T*) при различных порогах может быть построена в виде графика КОО.

9.6.3.2 Так как регистрационная база данных биометрической системы идентификации растет, изменения в суммарных эксплуатационных характеристиках для постоянной величины ВЛПИ (требующей изменения порога принятия решения) следует изображать в виде графика зависимости ВЛОИ (при ранге 1) от размера регистрационной базы данных. Для разных размеров базы данных может быть построено множество графиков КОО, отображающих зависимость ВЛПИ и ВЛОИ (см. рисунок Е.1).

9.6.4 Обобщенные вероятности ложноотрицательной и ложноположительной биометрической идентификации

Для сравнения биометрических систем, имеющих различные ВОР и ВОСД, следует использовать обобщенные ВЛОИ и ВЛПИ, которые включают в себя ошибки, возникающие при биометрической регистрации, сборе биометрических образцов и определении схожести. Метод обобщения должен соответствовать испытанию и должен быть указан в протоколе испытания.

Примечание — Как правило, обобщение должно включать в себя отказы биометрической регистрации как если бы регистрация завершилась, но соответствующий идентификатор не включен ни в один из списков кандидатов, а также отказы сбора данных, как если бы данные были получены, но был возвращен пустой список кандидатов.

9.6.5 Селективность

В системах биометрической идентификации, сконфигурированных для получения нескольких идентификаторов в списке кандидатов, количественная селективность представляет собой ожидаемое количество возвращаемых кандидатов, для которых сходство с биометрической пробой превышает порог *T* в транзакции непарной биометрической идентификации. СЕЛ (*N*, *R*, *T*) вычисляют по формуле

СЕЛ (*N*, *R*, *T*) = (число непарных кандидатов с показателем схожести, превышающим порог принятия решения *T*, удовлетворяющее рангу *R*)/ (число транзакций непарной биометрической идентификации). (10)

Примечание — Селективность и ВЛПИ будут отличаться при более низких порогах принятия решения, сходясь по мере уменьшения частоты ложноположительных результатов при более высоких порогах. Ложноположительные ошибки могут быть сосредоточены в определенных транзакциях.

9.6.6 Испытания эксплуатационных характеристик биометрической идентификации на замкнутом множестве

Эксплуатационные характеристики биометрической идентификации могут быть показаны в виде графика ХСС, полученного в результате испытания на замкнутом множестве. График ХСС отражает вероятность идентификации ранга *R* в зависимости от *R* (см. 10.4).

Вероятность идентификации ранга *R* — это вероятность того, что транзакция зарегистрированного в системе испытуемого субъекта включает в себя истинный пользовательский идентификатор в числе *R* первых возвращаемых кандидатов. При упоминании о единичном ранге идентификации следует ссылаться непосредственно на размер базы данных.

Пример — Вероятность идентификации ранга 1 на базе данных, состоящей из 250 записей, равна 95 %.

Вероятность идентификации ранга *R* вычисляют как 1 — ВЛОИ (*N*, *R*, 0).

При том, что использование графика ХСС достаточно распространено, такие графики не могут адекватно отображать диапазон вероятностей биометрической идентификации (например, в сравнительных испытаниях, где значения могут отличаться более чем на порядок). В таких случаях вместо графика ХСС следует построить график зависимости ВЛОИ (*N*, *R*, 0) от *R* на логарифмической шкале.

Примечание — Рекомендуемый алгоритм эффективного получения данных для графика ХСС приведен в приложении F.

9.6.7 Оценка вероятностей ошибок биометрической идентификации на основе результатов биометрической верификации

Оценка вероятностей ложноположительной и ложноотрицательной биометрической идентификации для биометрических систем идентификации может быть получена из КОО ВЛНС/ВЛС. Подобные оценки не учитывают корреляцию в сравнениях, касающихся одного и того же испытуемого субъекта, и, следовательно, являются неточными.

Пример — Эксплуатационные характеристики алгоритма биометрической идентификации, использующего единственный биометрический образец, в зависимости от размера базы данных N могут быть аппроксимированы с помощью следующих формул, которые подтверждены наблюдаемыми вероятностями ошибок биометрической идентификации на экспериментальных данных:

$$ВЛОИ = ВОСД + (1 – ВОСД) \cdot ВЛНС, \quad (11)$$

$$ВЛПИ = (1 – ВОСД) \cdot (1 – (1 – ВЛС)^N), \quad (12)$$

где N — число биометрических контрольных шаблонов в базе данных.

Примечания

1 При испытании биометрических систем идентификации, в которых проводят предварительный отбор образцов, вышеупомянутая модель эксплуатационной характеристики может быть расширена с помощью эксплуатационных характеристик для алгоритма предварительного отбора (см. приложение D).

2 В некоторых случаях ВЛПИ не масштабируется в соответствии с биномиальной формулой, так как поиск не реализуется как *N* независимых сравнений «один к одному». Это было бы так, если бы использовался быстрый древовидный поиск или если бы результаты вычислялись в зависимости от других биометрических контрольных шаблонов. В таких случаях при увеличении *N* ВЛПИ остается фиксированной, но ожидается, что ВЛОИ будет увеличиваться по мере вытеснения схожими непарными биометрическими контрольными шаблонами правильных пар.

9.6.8 Прогнозирование вероятностей ошибок биометрической идентификации на больших выборках

Определение эксплуатационных характеристик крупномасштабных биометрических систем идентификации (помимо объема испытаний) можно экстраполировать, используя оценки в первом приближении и эксплуатационные характеристики биометрической идентификации меньшей базы данных. В этом случае в протоколе испытаний указывают ту модель, которую следует использовать для экстраполяции эксплуатационных характеристик.

9.7 Анализ эксплуатационных характеристик в контролируемых экспериментальных условиях

9.7.1 Продольный анализ

9.7.1.1 Особое значение для долгосрочного использования биометрического контрольного шаблона имеет вопрос о том, необратимо ли изменяется соответствующий биометрический признак в результате старения субъекта. В определении термина «стабильность» (или «постоянство» по *[10]*) указано, что биометрический признак должен быть достаточно инвариантным во времени по отношению к данному алгоритму совпадения. Отсутствие стабильности — это признак старения биометрического контрольного шаблона, который свойственен биометрическому источнику и является по существу неизбежным и необратимым.

Пример — При биометрическом распознавании лица внешний вид изменяется по мере того, как мягкие ткани теряют свою эластичность, мышечный тонус и объем.

9.7.1.2 Старение субъекта проявляется в изменении результатов парного сравнения. Продольный анализ результатов, полученных путем сравнения биометрических образцов, собранных с течением времени, может стать подтверждением постоянства. Данные подтверждения могут быть представлены в виде трендов результатов сравнения и увеличения ВЛНС. Рекомендуется использовать регрессионные модели со смешанными эффектами, так как они способны регулировать дисбаланс между испытуемыми субъектами, нерегулярными биометрическими образцами, общими эффектами выборки и случайными индивидуальными эффектами. Продольный анализ приведен в *[11]*, а его применение в биометрии — в *[12]*.

9.7.1.3 В некоторых случаях в биометрии точность зависит от возраста субъекта даже при фиксированном промежутке времени между сбором биометрических образцов. Для таких случаев разработаны процедуры анализа возраста и старения субъекта (см. *[12]*).

9.7.2 Попарный анализ

В тех случаях, когда испытуемые субъекты используют два разных устройства или участвуют в двух разных экспериментальных условиях, полученные данные могут быть подвергнуты попарным испытаниям или построены в виде графика, отображающего разницу в результатах (например, показывают различия в распределении результатов или продолжительности транзакции).

9.8 Компромиссное определение ошибки

9.8.1 Измерения КОО должны быть проведены с использованием результатов сравнения при попытках парного и непарного сравнения. Результаты сравнения при попытках парного и непарного сравнения должны быть упорядочены. Любые выбросы должны быть изучены для определения ошибок, возникающих при маркировке. Изъятие любых результатов испытания должно быть задокументировано и должно обеспечивать проведение внешней оценки испытания.

9.8.2 Основой КОО является накопление упорядоченных результатов сравнения при попытках парного и непарного сравнения. Поскольку результаты сравнения могут иметь любые значения, каждая точка (x, y) графика КОО соответствует ВЛС и ВЛНС, использующим результат сравнения в качестве порога принятия решения. Если более высокие результаты сравнения соответствуют большему сходству между биометрической пробой и биометрическим контрольным шаблоном, ВЛС — это доля результатов непарного сравнения, больше (более схожи) или равных текущему значению параметра результата сравнения, от общего числа результатов непарного сравнения, а ВЛНС — это доля результатов непарного сравнения меньше (менее схожи) текущего значения параметра результата сравнения от общего числа результатов непарного сравнения. Данные могут быть сведены в таблицу в виде списка триплетов (ВЛС, ВЛНС, порог) или показаны в виде точечной диаграммы (см. 10.2).

Примечание — Рекомендуемый алгоритм получения данных для графика КОО приведен в приложении F.

9.8.3 КОО также допускается использовать для построения зависимости ВЛД от ВЛНД. ВЛД и ВЛНД зависят от ВЛС, ВЛНС, ВОСД и числа попыток, определенного политикой принятия решения. Транзакции нескольких попыток могут потребовать создания нового результата транзакции, основанного на степенях схожести части попыток (например, максимальное значение степени схожести для лучшей из трех попыток, определенных политикой принятия решения). Подобным образом графики КОО также могут быть использованы для отображения отношений между вероятностями ошибок биометрической идентификации.

9.9 Продолжительность транзакций

9.9.1 Показатели пропускной способности устанавливают число испытуемых субъектов, подвергаемых анализу в единицу времени, зависящее от скорости вычислений и взаимодействия пользователя с биометрической системой. Показатели пропускной способности для биометрической системы верификации, например для системы контроля и управления доступом, как правило, связаны со скоростью взаимодействия пользователя с биометрической системой в процессе сбора высококачественного биометрического образца. На показатели пропускной способности для биометрической системы идентификации, например для системы регистрации в программе социального обеспечения, может влиять время вычислительной обработки, необходимое для сравнения зарегистрированного биометрического образца с базой данных биометрических контрольных шаблонов. Поэтому в зависимости от приложения целесообразно определить время взаимодействия испытуемых субъектов с системой, а также время режима работы вычислительных аппаратных средств в зависимости от количества хранимых биометрических контрольных шаблонов.

9.9.2 Для определения скорости взаимодействия испытуемого субъекта с системой необходимо точно установить признаки начала и окончания транзакции. Эти признаки должны быть определены перед началом испытаний и указаны в протоколе испытаний. В протокол испытаний следует также включить краткий список действий, выполняемых испытуемыми субъектами, в рамках транзакции. Кроме того, при эксплуатации действия, необходимые после получения результата биометрической системы (например, прохождение через ворота, открытие двери, выход со станции), могут повлиять на способность следующего испытуемого субъекта взаимодействовать с системой. Измерение пропускной способности должно учитывать эти дополнительные действия, которые могут варьироваться в зависимости от результата биометрической системы.

9.9.3 С учетом того, что продолжительность транзакций может выходить далеко за пределы среднего значения, при включении в протокол испытания соответствующей информации следует использовать функцию распределения времени транзакций.

9.10 Вычислительная нагрузка

9.10.1 Некоторые биометрические приложения, такие как поиск идентификационных данных в больших регистрационных базах данных или сбор биометрических проб из видеоматериалов, могут быть вычислительно затратными, поэтому в таких случаях рекомендуется измерять вычислительную нагрузку. По мере масштабирования таких приложений доступные аппаратные ресурсы могут ограничивать пропускную способность или точность. Показатели вычислительной нагрузки включают в себя время транзакций и использование памяти, а также могут распространяться на рассмотрение таких аспектов, как использование центрального процессора, а также активность сети и диска.

Примечания

1 Вычислительная нагрузка биометрического поиска может зависеть от числа зарегистрированных биометрических контрольных шаблонов и их размера.

2 Вычислительную нагрузку можно измерять отдельно для различных элементов биометрической транзакции (например, для предварительного отбора).

9.10.2 Для указания в протоколе испытания общих вычислительных требований определенной транзакции (биометрической регистрации, биометрической верификации, биометрической идентификации) в биометрической системе необходимо измерить вычислительную нагрузку всех компонентов транзакции:

a) при биометрической регистрации:

- создание записи данных биометрической регистрации,
- создание биометрического индекса, при наличии,
- проверка дубликата биометрической регистрации (которая соответствует идентификационному поиску по уже существующим биометрическим контрольным шаблонам, полученным в процессе биометрической регистрации), если она реализована,
- сохранение биометрического контрольного шаблона в базе данных;

b) при биометрической верификации:

- получение набора биометрических признаков из собранного биометрического образца,
- извлечение биометрической регистрационной записи, соответствующей заявленной личности,

- попытка сравнения, включая дополнительные действия, например выравнивание (битовые сдвиги в кодах РОГ),

- решение о допуске/недопуске;

c) при биометрической идентификации:

- получение набора биометрических признаков из собранного биометрического образца,

- предварительный отбор для снижения нагрузки идентификационного поиска, если он реализован,

- идентификационный поиск по базе данных биометрических контрольных шаблонов,

- составление списка кандидатов и принятие решения о результатах биометрической идентификации.

Примечание — Вычислительная нагрузка биометрической идентификации, как правило, возрастает по мере увеличения числа зарегистрированных биометрических контрольных шаблонов. Вычислительная нагрузка для непарной биометрической пробы может быть выше, чем для парной биометрической пробы в том случае, когда парный биометрический контрольный шаблон найден до окончания просмотра всех биометрических контрольных шаблонов в базе данных.

9.10.3 Для сравнения эксплуатационных характеристик различных биометрических алгоритмов или систем необходимо учитывать различную вычислительную мощность аппаратного обеспечения, на котором работают эти системы, например: используя относительные эксплуатационные характеристики по сравнению с общим основным алгоритмом. Вычислительную нагрузку сравниваемых систем или алгоритмов рекомендуется измерять с использованием одного и того же аппаратного обеспечения и конфигурации.

9.10.4 Для сравнения биометрических систем идентификации, которые поддерживают повышение точности распознавания и снижение вычислительной нагрузки (например, за счет использования алгоритмов бинирования, предварительного отбора или индексации), в протоколе испытаний должны быть сведены в таблицу или нанесены на график результаты для каждой системы, показывающие:

- вычислительную нагрузку;

- точность биометрического распознавания (ВЛПИ, ВЛОИ) в пределах числа зарегистрированных биометрических контрольных шаблонов.

В протоколе испытания следует указывать показатели, относящиеся к методу сокращения нагрузки. Например, в случае предварительного отбора следует фиксировать вероятность ошибки предварительного отбора и степень проникновения. Любая модель, используемая для экстраполяции вычислительной нагрузки по мере увеличения числа зарегистрированных биометрических контрольных шаблонов, также должна быть представлена в протоколе испытания.

9.11 Неопределенность оценок

9.11.1 На оценку эксплуатационных характеристик влияют систематические и случайные ошибки. Случайные ошибки являются следствием естественных изменений испытуемых субъектов и предъявленных биометрических образцов. Систематические ошибки возникают из-за смещений в процедуре испытания, например когда определенные типы личностей недостаточно представлены в испытуемой группе. Систематические ошибки не являются полностью контролируемыми, поэтому в результатах оценки эксплуатационных характеристик будет присутствовать неопределенность. Несмотря на это неопределенность измеренных эксплуатационных характеристик должна быть оценена. Методы оценки неопределенности эксплуатационных характеристик приведены в приложении В.

9.11.2 Неопределенность, являющаяся следствием случайных факторов, уменьшается при увеличении объема испытания, и ее можно определить с помощью собранных данных. Систематическая неопределенность сохраняется независимо от объема испытания. Следует оценить неопределенность, возникающую из-за некоторых систематических ошибок. Например, проверка согласованности вероятностей ошибок для недостаточно представленной категории испытуемых субъектов с полными вероятностями ошибок может показать, изменятся ли вероятности ошибок при испытании должным образом сбалансированной группы. Часть эксплуатационных испытаний рекомендуется проводить повторно в других условиях окружающей среды для проверки чувствительности измеренных вероятностей ошибок к изменениям условий окружающей среды.

10 Графическое представление результатов

10.1 Распределения результатов

10.1.1 Общие положения

Гистограммы результатов парного и непарного сравнения могут быть показательны, особенно при отражении вариаций результатов сравнения в транзакциях, совершенных в различных условиях. Из-за диапазона и разброса собственных распределений результатов сравнения до построения гистограммы результатов следует рассмотреть возможность масштабирования результатов для облегчения сравнения результатов внутри систем и между ними.

10.1.2 «Диаграммы размаха»

Другой метод визуального суммирования распределений результатов определен как «диаграмма размаха» или «ящик с усами». Этот метод позволяет одновременно отображать распределения измерений для нескольких экспериментальных условий или устройств или сравнивать измерения между устройствами.

На рисунке 3 показан пример диаграммы «размаха», представленной в [*13*], в котором сравнивается распределение парных результатов сравнения для различных бесконтактно-контактных и контактно-контактных систем распознавания отпечатка пальца. На рисунке использованы «диаграммы размаха с вырезами». Медианные значения окружены выемкой соответствующего размера таким образом, что перекрывающиеся выемки подразумевают, что различия в медиане не являются статистически значимыми. Коробки представляют межквартильный диапазон каждого набора данных результатов. Точки данных, которые более чем в 1,5 раза превышают межквартильный диапазон выше верхнего квартиля или ниже нижнего квартиля, классифицируются как выбросы и отображаются красным крестом (+). «Усы» простираются от коробки до самых высоких и самых низких результатов, которые не классифицируются как выбросы.

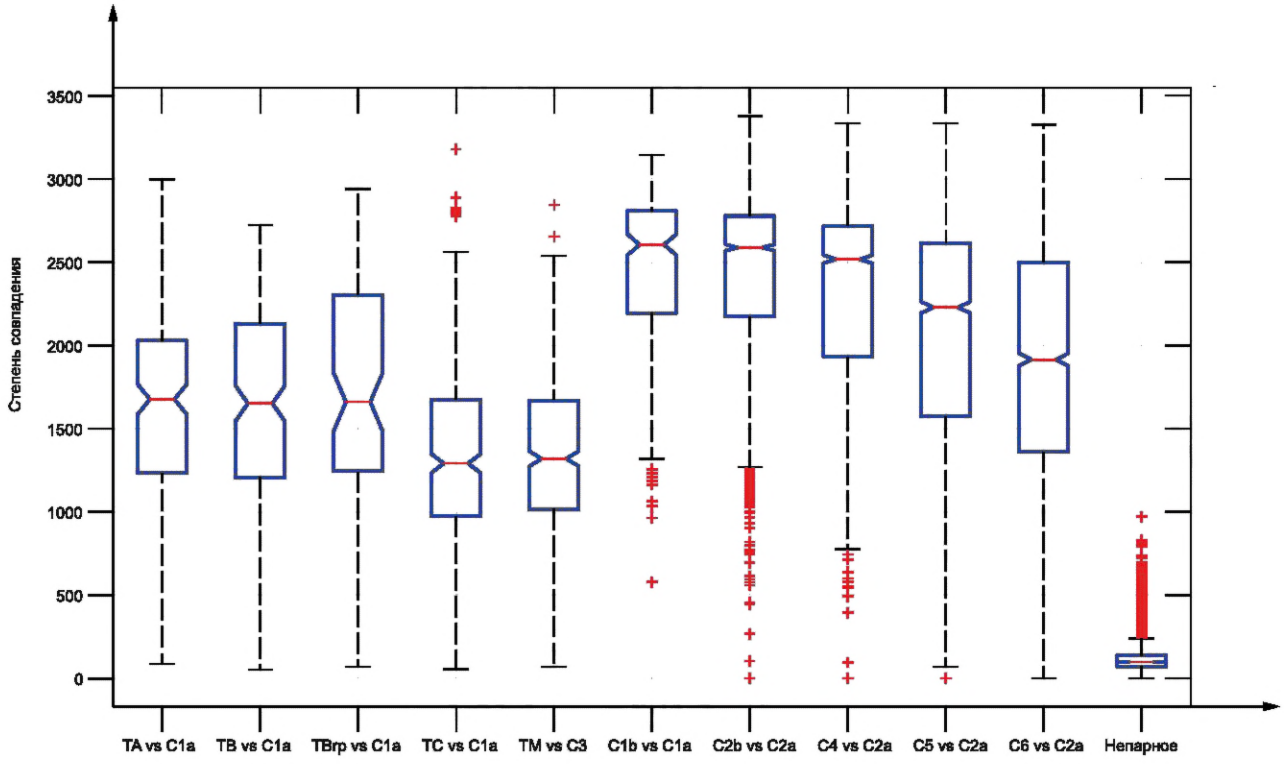

Рисунок 3 — Пример «диаграммы размаха»

10.2 График рабочей характеристики

Вероятность ошибки можно представить на графике в виде функции от порога принятия решения, например так, как на рисунке 4.

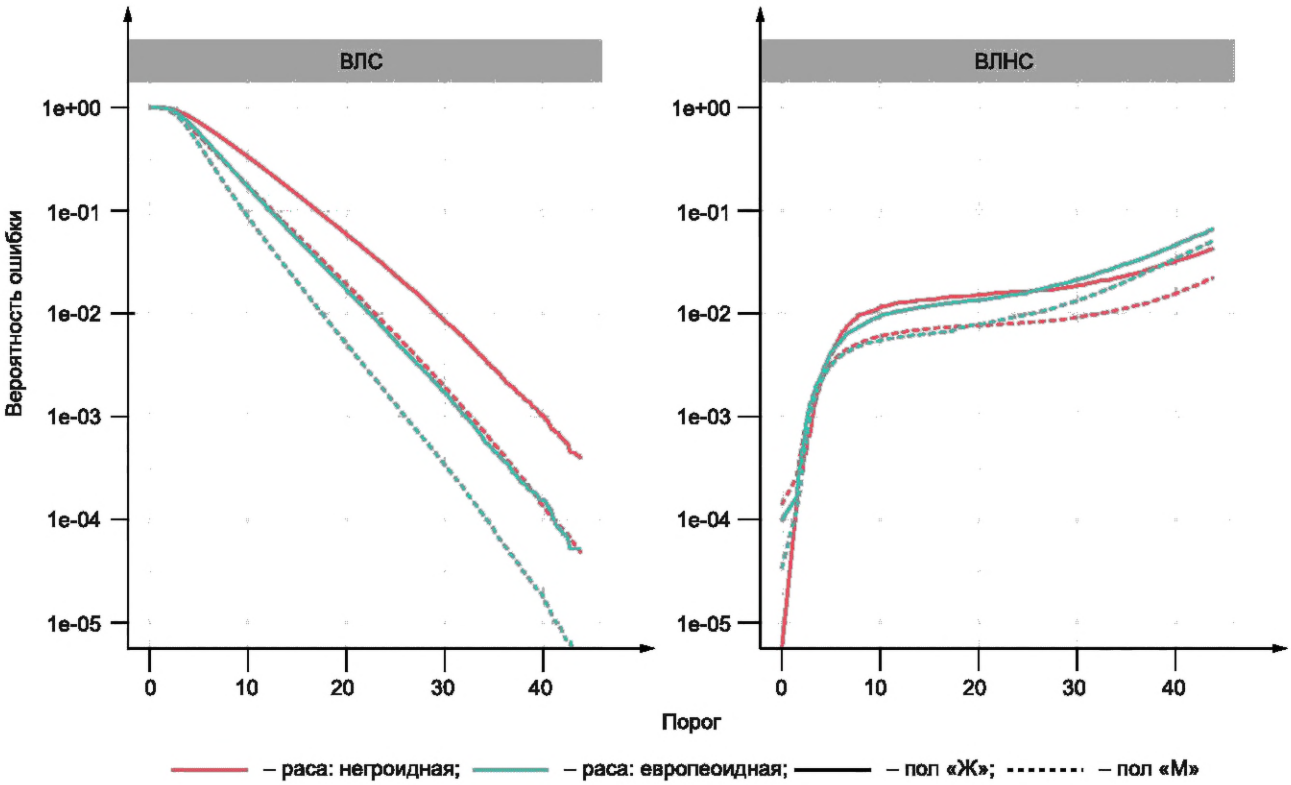

Рисунок 4 — Пример графиков РХ: изменения в распределении парных и непарных результатов в зависимости от расы и пола субъектов

10.3 График КОО

10.3.1 Эксплуатационные характеристики сравнения и (или) принятия решения биометрической системы могут быть изображены в виде графика КОО по всему диапазону порогов принятия решения. Графики КОО являются независимыми от порога принятия решения, что позволяет сравнивать эксплуатационные характеристики различных систем при одинаковых условиях или одной системы при различных условиях.

10.3.2 Графики КОО рекомендуется использовать для построения вероятностей ошибок совпадения (ВЛНС в зависимости от ВЛС) или вероятностей ошибок биометрической идентификации (ВЛОИ в зависимости от ВЛПИ). При сравнении эксплуатационных характеристик различных биометрических систем более информативным, чем графики, демонстрирующие вероятности ошибок, является график КОО ошибок принятия решения, который показывает общее влияние ошибок совпадения, получения изображений, сегментирования и биометрической регистрации.

10.3.3 На графике КОО по оси абсцисс (ось *x*) откладывают ложноположительную вероятность, а по оси ординат (ось *y*) — ложноотрицательную вероятность.

10.3.4 Шкалы осей, показывающие граничные значения, должны обеспечивать наглядное представление результатов. Для надлежащего определения вероятностей ошибок в интересующем диапазоне графики КОО, как правило, строят с использованием шкалы с нормальным отклонением или логарифмической шкалы:

a) линейная шкала: построение графика КОО с линейной шкалой по осям не рекомендуется для вероятностей ошибок, которые охватывают несколько порядков величины. Системы с низкими вероятностями ошибок группируются близко к началу отсчета координат, и тогда сложно определить различия в эксплуатационных характеристиках;

b) логарифмическая шкала: построение графика КОО с логарифмической шкалой по осям обеспечивает большую детализацию при низких вероятностях ошибок и помогает различать системы, работающие похожим образом;

c) шкала с нормальным отклонением: построение графика КОО со шкалой с нормальным отклонением по осям также обеспечивает большую детализацию при низких вероятностях ошибок. Как

правило, распределения парных и непарных результатов являются приблизительно Гауссовыми, и если это так, то при использовании оси с нормальным отклонением получается приблизительно линейный график КОО.

Примечание — График КОО, как первоначально предложено А. Мартином и др. (см. [*14*]), должен был быть построен со шкалой с нормальным отклонением по осям. Настоящим стандартом допускается использование других шкал.

На рисунке 5 показаны варианты использования различных шкал по осям при построении одних и тех же графиков КОО, а также неуместность применения линейной шкалы в данном случае.

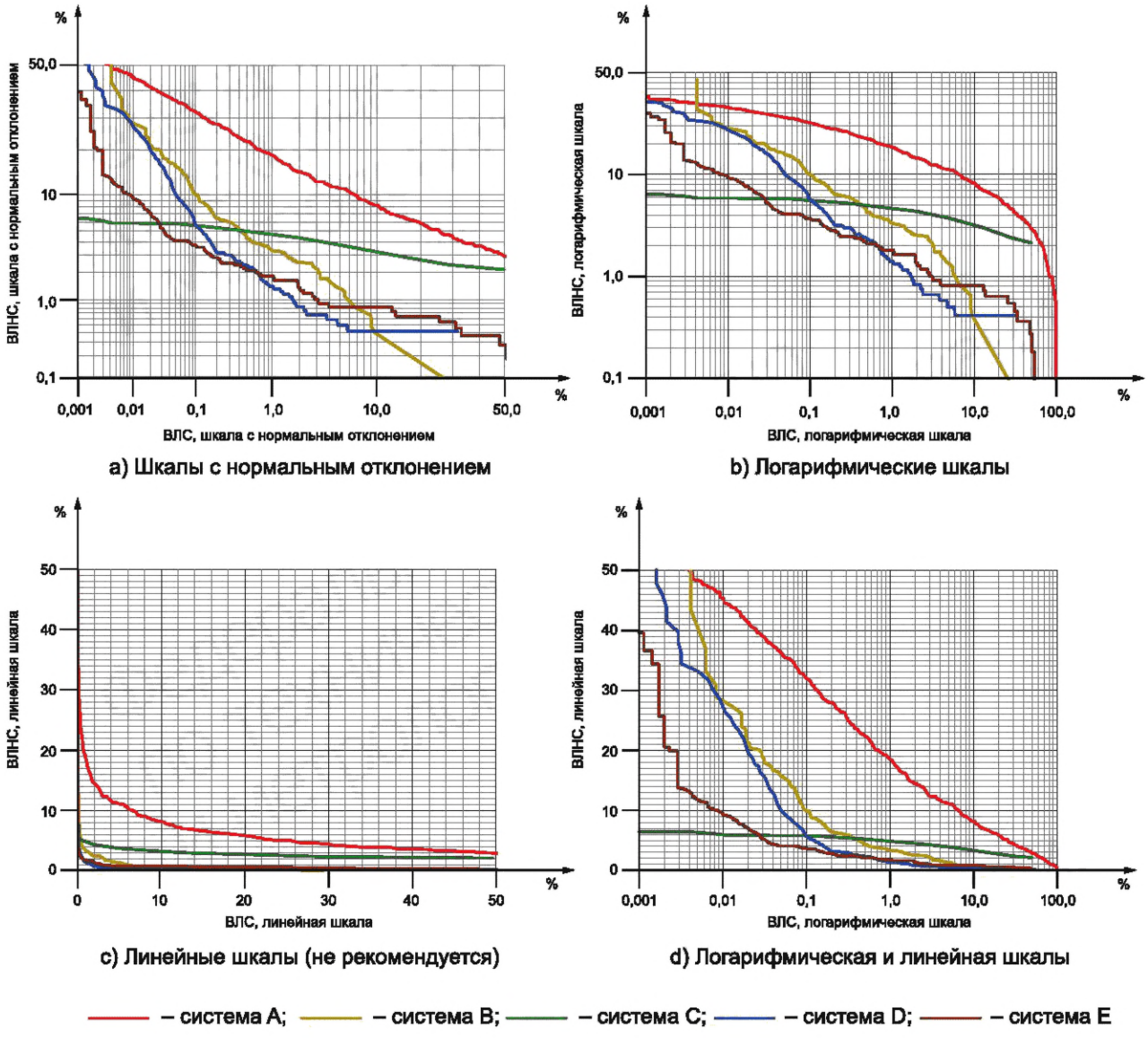

Рисунок 5 — Примеры графиков КОО с использованием различных шкал по осям

10.3.5 Используемая шкала должна быть определена в протоколе испытания таким образом, чтобы из представления графика КОО можно было вывести табличное представление данных. Шкалы осей должны быть согласованы между различными графиками в одном протоколе испытания. Если необходимо изменить шкалу, чтобы сохранить ясность, на рисунке с графиком следует приводить примечание, отмечающее изменение шкалы.

10.3.6 Рисунки G.1—G.4 содержат дополнительную информацию относительно интерпретации графика КОО.

10.4 График ХСС и график «ВЛОИ по рангу»

Для тех приложений, в которых система возвращает списки кандидатов операторам, результаты эксплуатационных характеристик часто отображают с помощью графика ХСС. Кривая отображает в зависимости от *R* долю транзакций, в которых идентификатор испытуемого субъекта включен в число *R* возвращаемых идентификаторов, от общего числа транзакций. Пример графика ХСС приведен на рисунке 6.

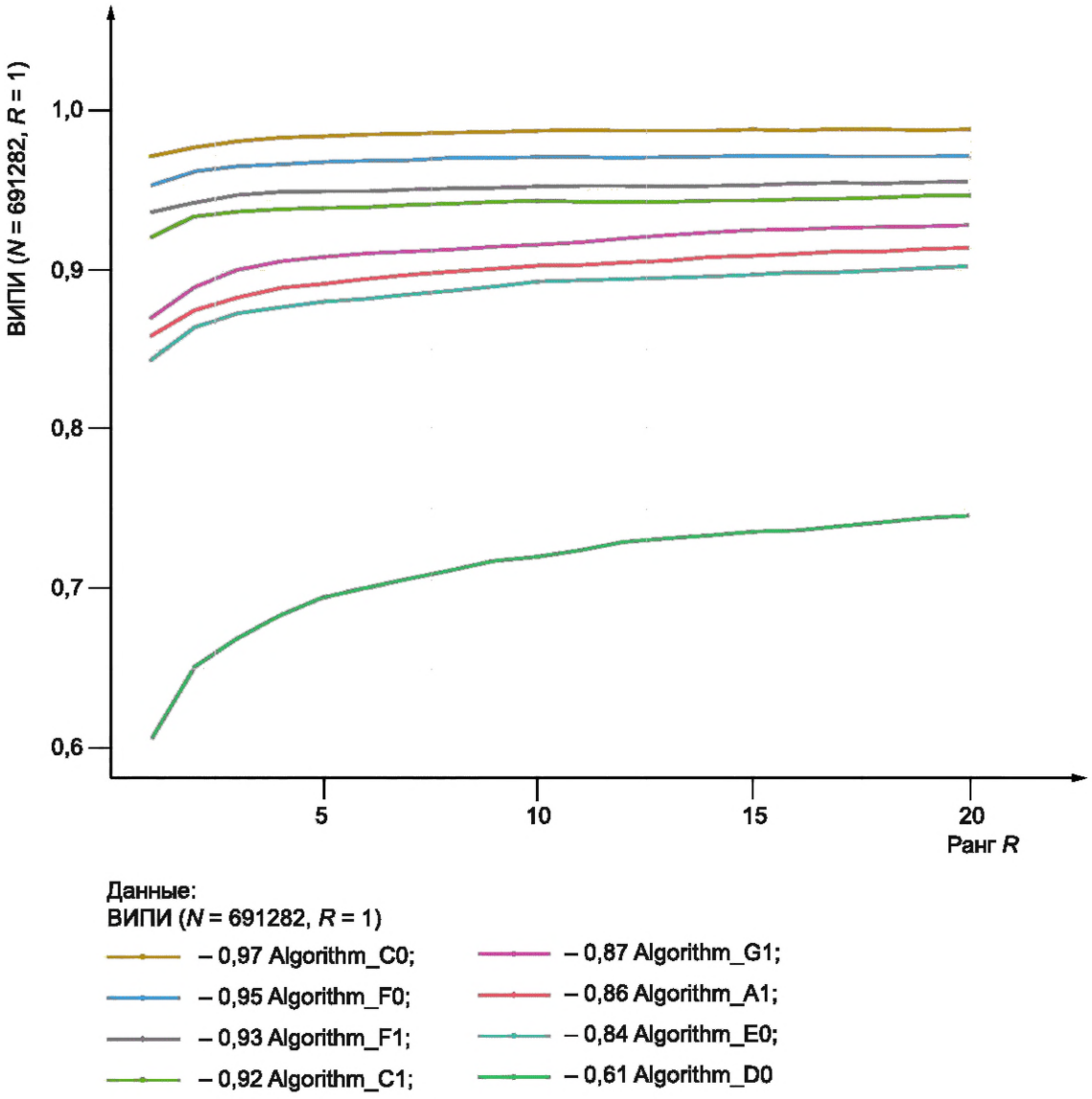

Рисунок 6 — Пример графика ХСС

Когда значения ВЛОИ охватывают более одного порядка величины, предпочтительным является график «ВЛОИ по рангу», показывающий зависимость ВЛОИ (*N*, *R*, 0) от ранга *R* на логарифмической шкале (см. рисунок 7).

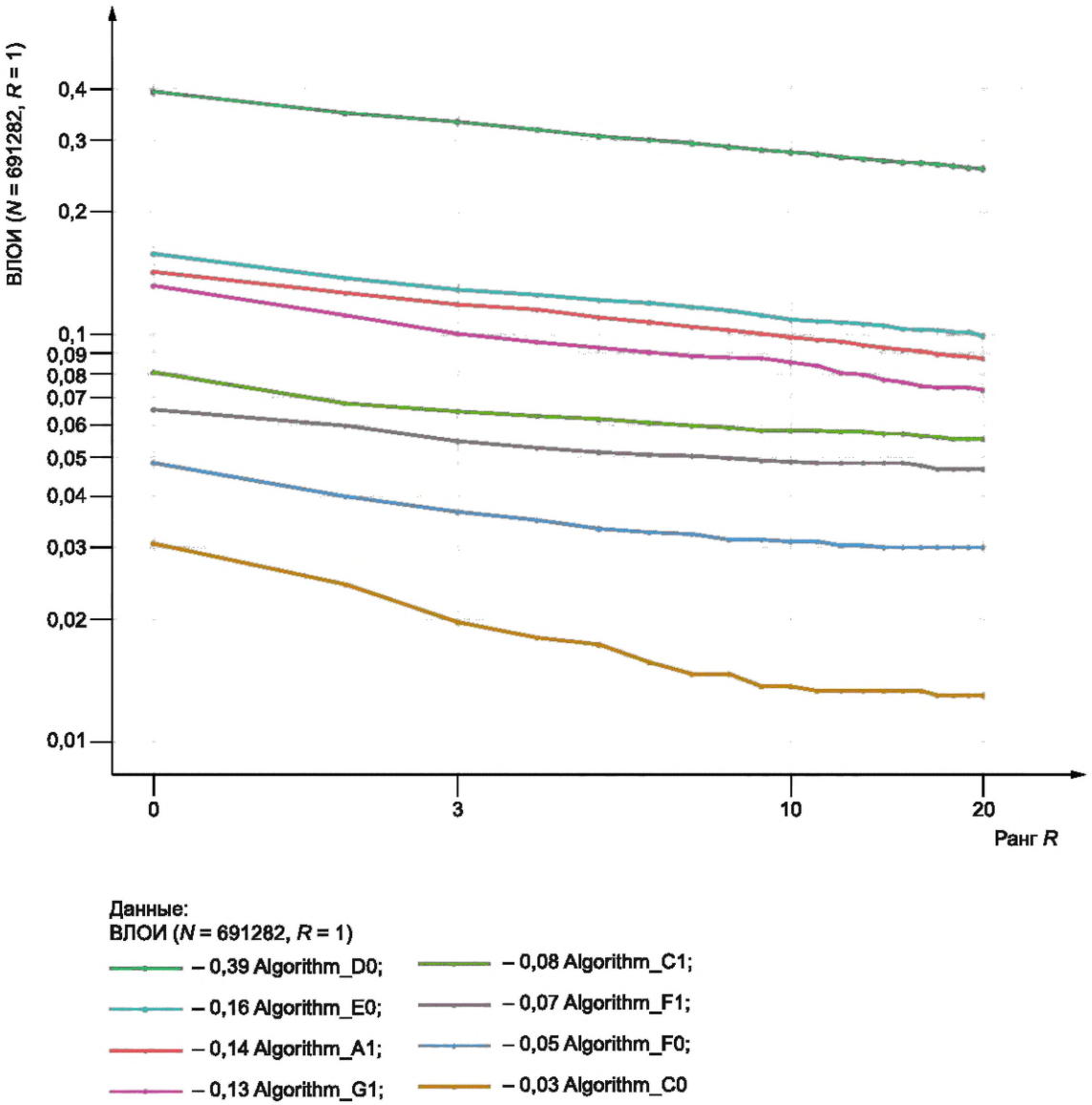

Рисунок 7 — Пример графика «ВЛОИ по рангу»

10.5 График «ВЛОИ по числу зарегистрированных испытуемых субъектов»

Если поиск выполняется в базах данных биометрических регистраций различных размеров, то результаты эксплуатационных характеристик должны быть показаны с помощью графика зависимости ВЛОИ (N, 1, 0) от числа зарегистрированных испытуемых субъектов N (см. рисунок 8).

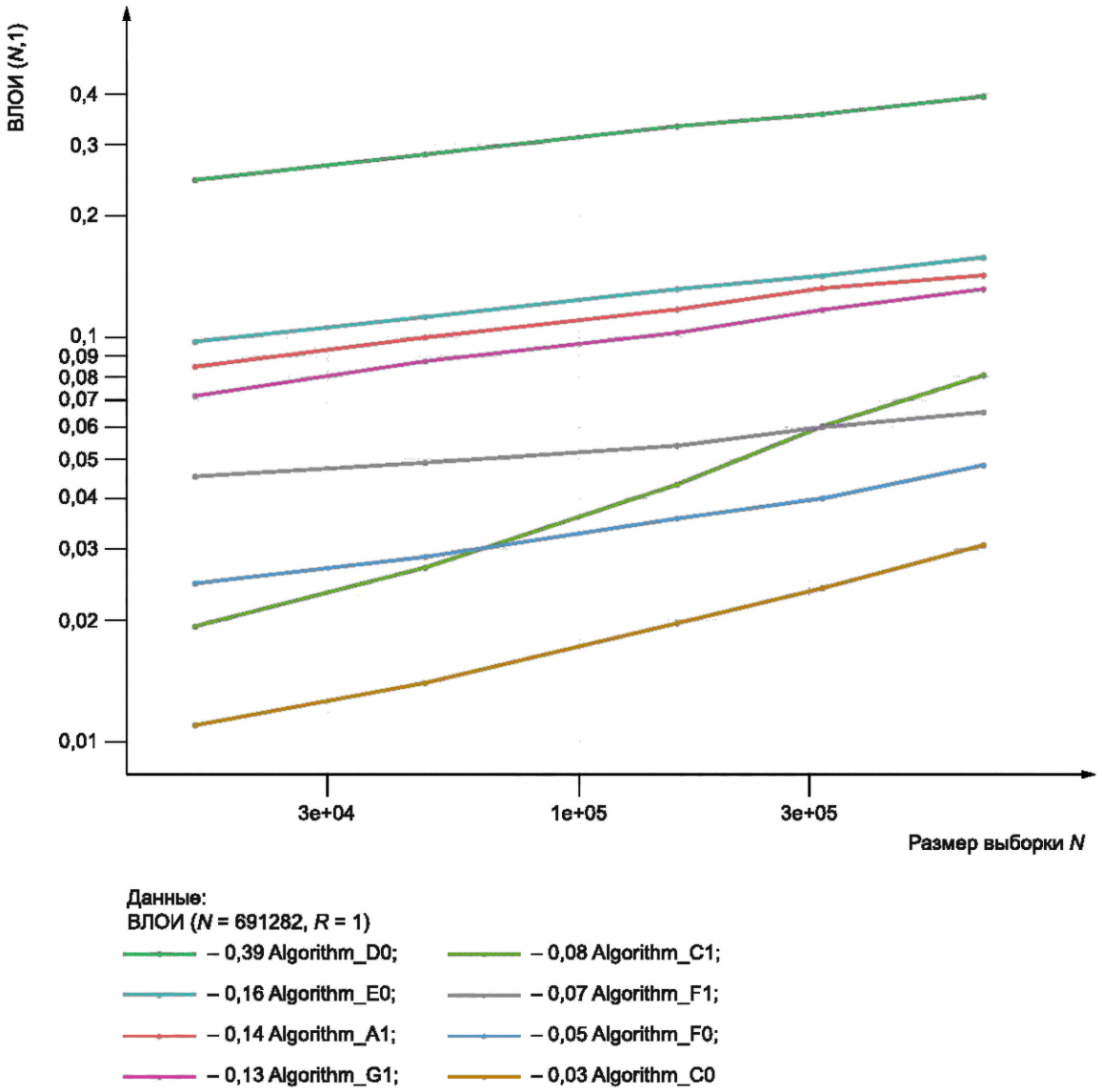

Рисунок 8 — Пример графика «ВЛОИ по числу зарегистрированных испытуемых субъектов»

10.6 Тепловые карты

Тепловые карты демонстрируют, как эксплуатационные характеристики изменяются в диапазоне ковариат при разработке эксперимента. На рисунке 9 приведен пример тепловой карты, показывающей изменение ВЛС в зависимости от возраста «самозванцев» и зарегистрированных пользователей, когда порог принятия решения установлен для достижения ВЛС, равной 1/10 000 для всего набора пар зарегистрированный пользователь — «самозванец». В цветовой гамме тепловой карты нейтральный серый соответствует целевому значению ВЛС, оттенки красного используют, если ВЛС повышается относительно этого значения, а оттенки синего — если ВЛС снижается относительно этого значения. Диагональное доминирование показывает, что ложные совпадения более вероятны, когда два сравниваемых образца принадлежат испытуемым субъектам, близким друг к другу по возрасту.

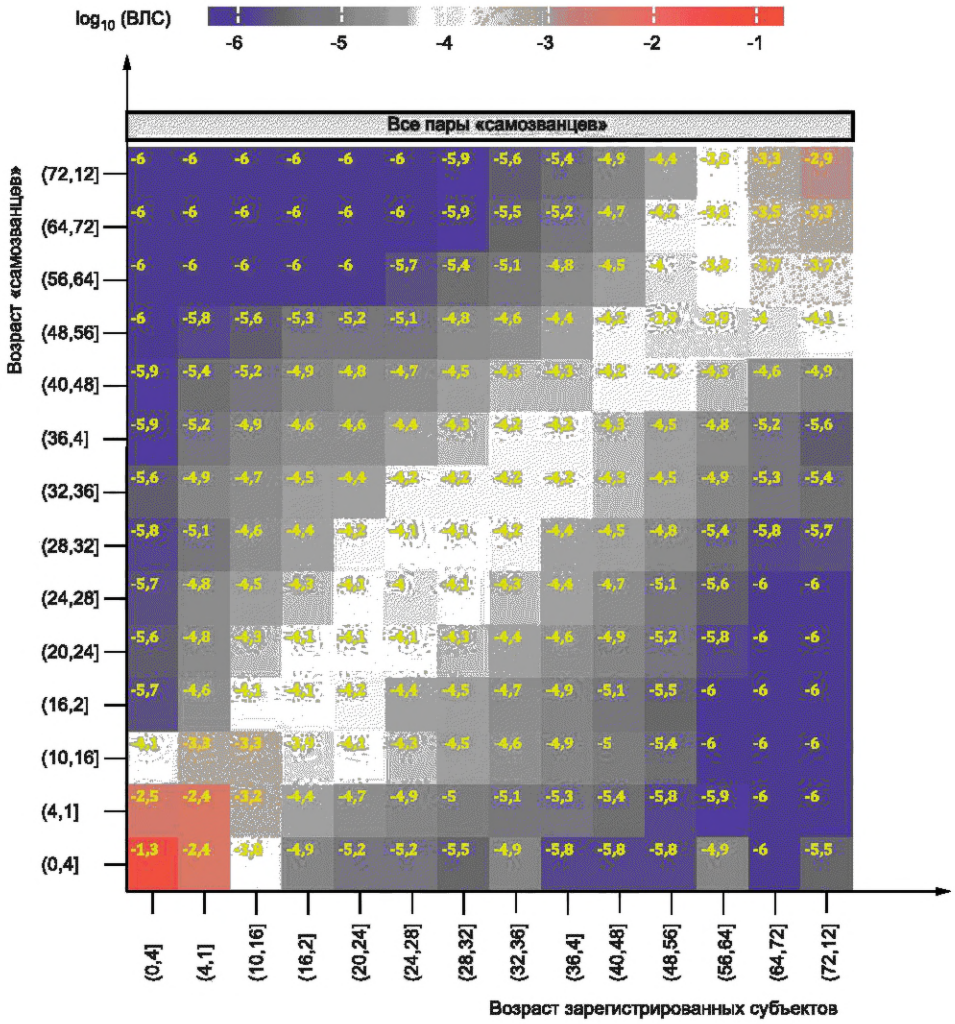

Рисунок 9 — Пример тепловой карты: изменение ВЛС из-за разницы в возрасте «самозванцев» и зарегистрированных пользователей

11 Хранение записей

11.1 Хранение записей должно соответствовать правилам учета и хранения персональной идентификационной информации:

a) исходные биометрические образцы, биометрические контрольные шаблоны и биометрические признаки (если они собраны) должны храниться с соблюдением требований нормативных документов в области защиты персональных данных, действующих на территории Российской Федерации;

b) результаты сравнения и решения, принимаемые системой, при наличии, должны быть сохранены.

Примечание — Результаты сравнения и решения не являются персональной идентификационной информацией без привязки к личности или биометрическим персональным данным.

11.2 Следует хранить записи, касающиеся методов, используемых для измерения эксплуатационных характеристик, а также личности сотрудников, ответственных за проведение биометрической регистрации и контролирующих сбор данных о транзакциях.

11.3 Необходимая информация должна обеспечивать:

a) возможность повторного проведения испытаний в условиях, максимально приближенных к первоначальным;

b) поддержку при выяснении факторов, влияющих на неопределенность результатов;

c) создание контрольного журнала;

d) поддержку сравнения результатов с результатами других испытаний, например для межлабораторного сравнения.

11.4 Для предотвращения потерь или изменений первоначальных данных испытания записи (рукописные или электронные) должны быть защищены. При необходимости внесения изменений следует сохранять копию оригинала с указанием всех изменений, внесенных в оригинал. Может потребоваться механизм, позволяющий удалить личную информацию испытуемого субъекта по его запросу.

11.5 При наличии ошибок (в процедурах сбора данных и т. д.) в записях должны быть указаны как ошибочные данные, так и правильные значения.

11.6 Удаление записей осуществляется в соответствии с требованиями национального законодательства и политикой организации, в которой хранят записи.

12 Протоколы эксплуатационных испытаний

12.1 Особенности протоколов испытаний

Эксплуатационные характеристики, такие как вероятности ошибок, время транзакций, вычислительная нагрузка и т. д., зависят от типа испытания, приложения и выборки. Для правильной интерпретации эксплуатационных характеристик необходимо представить информацию, приведенную в таблице 1, вместе с оценочными эксплуатационными характеристиками, перечисленными в 12.3—12.8.

Таблица 1 — Информация, приводимая в протоколах испытаний

Информация об испытании	Наличие в протоколе испытания	Информация для протокола испытания
Испытуемая(ые) система(ы)	Обязательно	Включение подробной информации об алгоритмах, биометрических датчиках, пользовательском интерфейсе, вспомогательном оборудовании и т. д.
Организация испытания	Обязательно	Испытательная лаборатория, место проведения испытания, дата проведения испытания
Вид испытания	Обязательно	При технологическом испытании: особенности используемой базы данных. При сценарном испытании: особенности тестируемого сценария. При оперативном испытании: подробная информация о приложении
Объем испытания	Обязательно	Число испытуемых субъектов; число образцов (пальцев, рук, глаз и т. д., зарегистрированных каждым испытуемым субъектом); число посещений каждого испытуемого субъекта; число транзакций каждого испытуемого субъекта (или образца испытуемого субъекта и т. д.) при каждом посещении
Испытуемая группа	Обязательно	Демографические данные испытуемой группы (возраст, пол и т. д.); способ, которым была собрана испытательная группа, а также степень, в которой испытательная группа отражает целевую выборку; уровень подготовки, инструктажа, ознакомления и навыков испытательной группы в вопросах использования биометрической системы
Условия проведения испытания	Обязательно	См. 8.3.2.1, 8.4.2 и С.2.6
Интервал времени между транзакциями биометрической регистрации и биометрического распознавания	Обязательно	См. 7.3.7
Пороги качества и принятия решения во время сбора данных	Обязательно	Используемые и рекомендуемые для целевого применения (если они отличаются) пороги

Окончание таблицы 1

Информация об испытании	Наличие в протоколе испытания	Информация для протокола испытания
Контроль факторов, воздействующих на эксплуатационные характеристики	Обязательно	См. 7.3 и приложение С
Процедуры испытания	Обязательно	Например, политика определения отказов биометрической регистрации; подробная информация о любых внештатных ситуациях, возникающих во время испытания, которые исключаются из анализа эксплуатационных характеристик
Оценка неопределенностей	Необязательно	Оценочная неопределенность в результатах эксплуатационных характеристик и метод оценки (см. 9.11 и приложение В)
Отклонение от требований	Необязательно	Любые отклонения от требования настоящего стандарта должны быть обоснованы. Допускается пренебречь одним показателем в пользу другого, например: установка случайного характера последовательности получения отпечатков пальцев на биометрической системе может запутать пользователя и привести к возникновению большого числа ошибок в маркировке

12.2 Сводные статистики

Не рекомендуется использовать сводные метрики, представленные одним числом, таким как РВО, ПОВО, площадь под кривой РХ. Если необходимо представить один количественный показатель, характеризующий биометрическую систему, то метод получения данного показателя должен учитывать такие факторы, как стоимость ошибки, целевой уровень безопасности биометрической системы и т. д., а информацию о нем приводят в протоколе испытания.

12.3 Информация об эксплуатационных характеристиках биометрической регистрации в протоколе испытания

В таблице 2 приведены эксплуатационные характеристики биометрической регистрации.

Таблица 2 — Эксплуатационные характеристики биометрической регистрации

Эксплуатационная характеристика	Наличие в протоколе испытания	Информация для протокола испытания
ВОР	Обязательно	См. 9.2.1
Продолжительность транзакции биометрической регистрации	Необязательно	См. 9.2.2. В дополнение к усредненной (средней или медианной) продолжительности транзакции должна быть представлена функция распределения времени биометрической регистрации, показывающая успешные и неуспешные биометрические регистрации
Вычислительная нагрузка транзакции биометрической регистрации	Необязательно	См. 9.10.2, перечисление а)

12.4 Информация об эксплуатационных характеристиках сбора данных в протоколе испытания

В таблице 3 приведены эксплуатационные характеристики сбора данных.

Таблица 3 — Эксплуатационные характеристики сбора данных

Эксплуатационная характеристика	Наличие в протоколе испытания	Информация для протокола испытания
ВОСД	Обязательно	См. 9.3.1
Продолжительность сбора данных	Необязательно	См. 9.3.2. В дополнение к усредненной (средней или медианной) продолжительности транзакции должна быть представлена функция распределения времени сбора данных, показывающая успешные и неуспешные попытки сбора данных

12.5 Информация об эксплуатационных характеристиках сравнения «один к одному» в протоколе испытания

В таблице 4 приведены эксплуатационные характеристики сравнения «один к одному».

Таблица 4 — Эксплуатационные характеристики сравнения «один к одному»

Эксплуатационная характеристика	Наличие в протоколе испытания	Информация для протокола испытания
ВЛС/ВЛНС	Обязательно	См. 9.4.1 и 9.4.2. ВЛС и соответствующая ВЛНС должны быть представлены по всему диапазону испытуемых порогов принятия решения. В случае нескольких рабочих точек рекомендуется использовать график КОО
ВОР	Обязательно	См. 12.3. В противном случае необходимо указать, что ВОР неизвестна
ВОСД	Обязательно	См. 12.4. В противном случае необходимо указать, что ВОСД неизвестна
Вычислительная нагрузка биометрического сравнения	Необязательно	—

12.6 Информация об эксплуатационных характеристиках биометрической системы верификации в протоколе испытания

В таблице 5 приведены эксплуатационные характеристики биометрической системы верификации.

Таблица 5 — Эксплуатационные характеристики биометрической системы верификации

Эксплуатационная характеристика	Наличие в протоколе испытания	Информация для протокола испытания
ВЛД/ВЛНД	Обязательно	См. 9.5.1 и 9.5.3. ВЛД и соответствующая ВЛНД должны быть представлены по всему диапазону испытуемых порогов принятия решения. В случае нескольких рабочих точек рекомендуется использовать график КОО
ВОР	Обязательно	См. 12.3. В противном случае необходимо указать, что ВОР неизвестна
ВОСД	Обязательно	См. 12.4. В противном случае необходимо указать, что ВОСД неизвестна
Продолжительность транзакции биометрической верификации	Необязательно	См. 9.5.4. В дополнение к усредненной (средней или медианной) продолжительности транзакции должна быть представлена функция распределения времени сбора данных, показывающая продолжительность принятых и отклоненных биометрических верификаций

Окончание таблицы 5

Эксплуатационная характеристика	Наличие в протоколе испытания	Информация для протокола испытания
ОВЛД/ОВЛНД	Необязательно	См. 9.5.5. Рекомендуется при сравнении биометрических систем, имеющих различные ВОР/ВОСД. Метод обобщения должен быть указан в протоколе испытания
Вычислительная нагрузка транзакции биометрической верификации	Необязательно	См. 9.10.2, перечисление b)

12.7 Информация об эксплуатационных характеристиках биометрической системы идентификации в протоколе испытания

В таблице 6 приведены эксплуатационные характеристики биометрической системы идентификации.

Таблица 6 — Эксплуатационные характеристики биометрической системы идентификации

Эксплуатационная характеристика	Наличие в протоколе испытания	Информация для протокола испытания
ВЛПИ/ВЛОИ	Обязательно	См. 9.6.2 и 9.6.3. ВЛПИ и соответствующая ВЛОИ должны быть представлены по всему диапазону испытуемых порогов принятия решения и рангов идентификации. В случае нескольких рабочих точек рекомендуется использовать график КОО. Допускается приводить несколько графиков КОО, соответствующих различному числу возвращаемых идентификаторов и различному числу биометрических контрольных шаблонов в регистрационной базе данных
Число зарегистрированных биометрических контрольных шаблонов	Обязательно	—
ВОР	Обязательно	См. 12.3. В противном случае необходимо указать, что ВОР неизвестна
ВОСД	Обязательно	См. 12.4. В противном случае необходимо указать, что ВОСД неизвестна
Селективность	Необязательно	См. 9.6.5
Результаты на замкнутом множестве	Необязательно	См. 9.6.6. Если проведено испытание на замкнутом множестве, то результаты должны быть представлены либо в виде графика ХСС, либо в виде графика «ВЛОИ по рангу» с информацией о числе зарегистрированных испытуемых субъектов
Продолжительность транзакции биометрической идентификации	Необязательно	См. 9.9. В дополнение к усредненной (средней или медианной) продолжительности транзакции должна быть представлена функция распределения времени сбора данных
Вычислительная нагрузка транзакции биометрической идентификации	Необязательно	См. 9.10.2, перечисление c) и 9.10.4. Вычислительная нагрузка может быть измерена для различного числа биометрических контрольных шаблонов, чтобы показать, как изменяется нагрузка с увеличением размера базы данных

12.8 Информация об эксплуатационных характеристиках в зависимости от различных факторов в протоколе испытания

12.8.1 Рекомендуется продемонстрировать различия в эксплуатационных характеристиках между отдельными лицами/классами лиц, например, указывая информацию о вероятностях ошибок/результатах сравнения/времени для различных классов лиц (например, мужчины/женщины). При испытаниях, где испытуемые субъекты совершают несколько парных транзакций, также рекомендуется предоставить гистограммы, показывающие, как индивидуальные вероятности ошибок изменяются в зависимости от испытуемого субъекта.

12.8.2 При испытаниях, учитывающих влияние контролируемого управляемого фактора на эксплуатационные характеристики [см. 7.3.2, перечисление а)], могут наблюдаться изменения как в ВЛНС, так и в ВЛС (или во ВЛОИ и ВЛПИ для биометрической системы идентификации). Экспериментатор должен построить два графика — зависимость ВЛНС от порога и зависимость ВЛС от порога, которые включают трассировки для каждого уровня контролируемого фактора (см. примеры на рисунке 4). Такие графики, как правило, показывают изменения в парных и непарных распределениях соответственно.

Нормальное КОО подходит для тех приложений, в которых пороги устанавливают отдельно для каждого уровня фактора. В тех случаях, когда общий порог используется на всех уровнях фактора, экспериментатор может построить график КОО так, как показано на рисунке 10, с линиями, соединяющими точки зафиксированного порога (показаны черным цветом на рисунке 10).

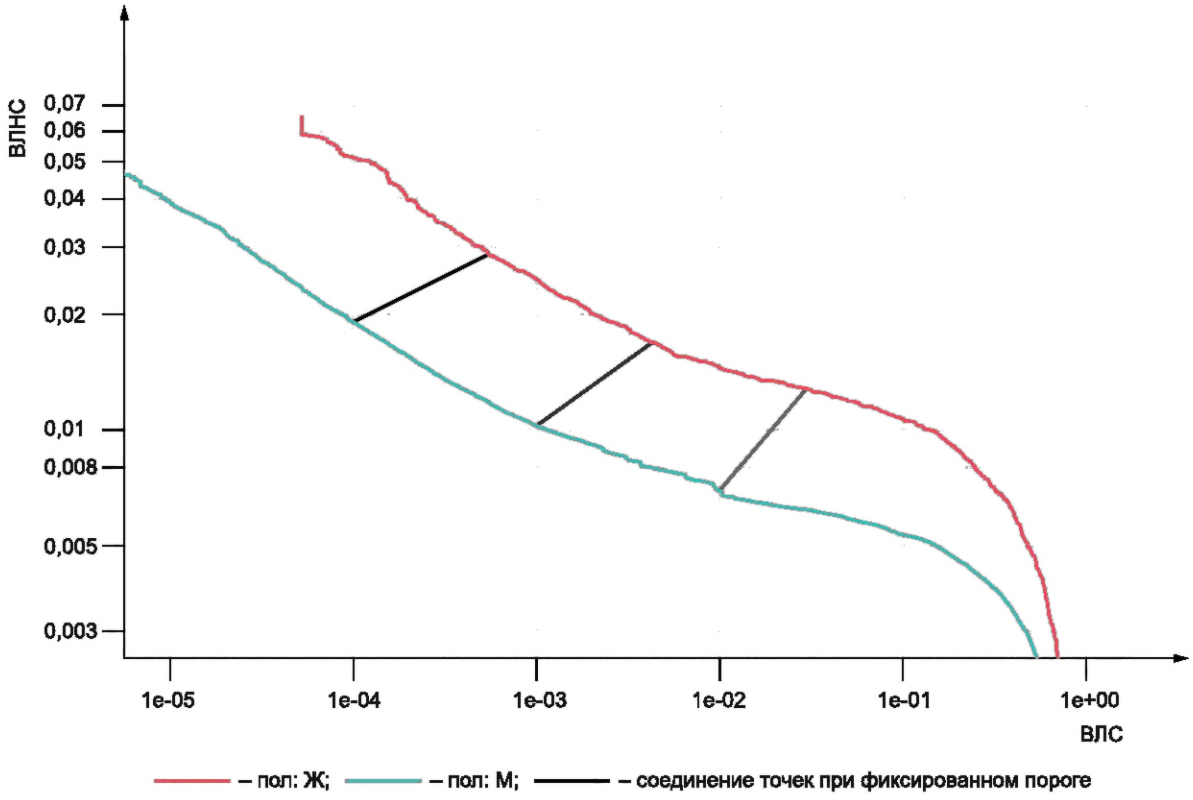

Рисунок 10 — Пример относительных эксплуатационных характеристик испытуемых субъектов мужского и женского пола для системы контроля доступа на основе биометрического распознавания лица

Приложение А
(справочное)

Различия между видами испытаний

Различия между видами испытаний приведены в таблице А.1.

Таблица А.1

Наименование показателя	Технологическое испытание	Сценарное испытание	Оперативное испытание
Объект испытания	Биометрический компонент (алгоритм сравнения или извлечения)	Биометрическая система	Биометрическая система
Истинная информация	Известна при условии, что установлены ошибки сбора данных и области пересечения объединенных данных	Известна при условии, что ошибки сбора данных и отказа учитывают нежелательное поведение испытуемого субъекта	Зависит от доступных контрольных и инструментальных средств, устанавливающих истинную информацию
Поведение испытуемого субъекта, контролируемое администратором испытания	Не контролируется в процессе испытания; может контролироваться во время записи данных, в противном случае считают неконтролируемым	Контролируется (до тех пор, пока поведение испытуемого субъекта не станет независимой величиной)	Не контролируется
Испытуемый субъект, имеющий сведения о результатах попытки в реальном времени	Нет	Да	Да
Воспроизводимость результатов	Воспроизводимые (фиксированная база данных)	Квазивоспроизводимые (если контролируется сценарий испытания и выборка)	Невоспроизводимые
Контроль параметров окружающей среды	Может выполняться во время записи данных, в противном случае данные считают неконтролируемыми	Контролируемые и (или) записаны	Неконтролируемые, идеально записаны
Запись взаимодействия с испытуемым субъектом	В процессе испытания не записывается; может записываться во время записи данных	Записывается	Записывается во время биометрической регистрации; может записываться во время биометрической верификации или биометрической идентификации
Протокол типичных результатов	Сравнение биометрических компонентов или модификаций компонентов (т. е. алгоритмов сравнения или извлечения или датчиков), определение критических эксплуатационных факторов	Сравнение биометрических систем; определение критических эксплуатационных факторов; измерение моделируемых эксплуатационных характеристик	Измерение эксплуатационных характеристик в условиях эксплуатации

Окончание таблицы А.1

Наименование показателя	Технологическое испытание	Сценарное испытание	Оперативное испытание
Эксплуатационные характеристики	Большая часть эксплуатационных характеристик (кроме сквозной пропускной способности); большая часть вероятностей ошибок; эксплуатационные характеристики, подходящие для широкомасштабной биометрической системы идентификации, когда сложно собрать большую испытуемую группу	Прогнозируемая сквозная пропускная способность, ВЛС, ВЛНС, ВОСД, ВОР, ВЛД, ВЛНД	Сквозная пропускная способность. Для испытания и определения ВЛД и ВЛНД необходимы знания об истинной информации
Ограничения	База данных, полученная с помощью одного или более датчиков, идентичность которых известна или неизвестна	Эксплуатационные, инструментальные системы	Эксплуатационные, инструментальные системы; как правило, доступны только вероятности принятия решения
Целевая выборка	Записанная	Реальная	Реальная
Примечание — В настоящей таблице приведены основные характеристики и отличительные особенности испытаний биометрических систем, но в некоторых случаях допускаются исключения.			

Приложение В
(справочное)

Объем испытаний и случайная неопределенность

В.1 Доверительные интервалы и объем испытаний для независимых одинаково распределенных результатов сравнений

В.1.1 Правило трех

Правило трех (см. [*4*], *[15]—[17]*) используют для определения наименьшей вероятности ошибки, которая может быть статистически значимо установлена для n независимых одинаково распределенных сравнений. Если значение вероятности ошибки p, для которого вероятность нулевой погрешности при n испытаниях является случайной и равна, например, 5 %, то

$$p \approx 3/n$$

с доверительной вероятностью 95 %*.

Пример — Если испытание 300 независимых биометрических образцов прошло без ошибок, то считают, что с доверительной вероятностью 95 % вероятность ошибки равна 1 % или менее.

Примечания

1 $p \approx 2/n$ с доверительной вероятностью 90 %.

2 Допущение о независимых одинаково распределенных результатах попыток может быть принято при испытании биометрических эксплуатационных характеристик, если каждая попытка парного сравнения осуществлялась разными испытуемыми субъектами и если каждая попытка непарного сравнения включала разные пары испытуемых субъектов. При n испытуемых субъектах могут быть выполнены только n статистически независимых попыток парного сравнения и только $n/2$ статистически независимых попыток непарного сравнения. При полном перекрестном сравнении всех представленных биометрических признаков биометрического образца с зарегистрированными биометрическими контрольными шаблонами получают намного больше попыток непарного сравнения и согласно *[6]* достигается меньшая неопределенность при взаимной зависимости попыток. Таким образом, кроме оперативного испытания следует ограничить данные единственной попыткой испытуемого субъекта, чтобы выполнить допущение о независимых одинаково распределенных результатах попыток.

В.1.2 Правило тридцати

В правиле тридцати утверждается, что для того, чтобы с доверительной вероятностью 90 % истинная вероятность ошибки находилась в диапазоне ±30 % от установленной вероятности ошибки, должно быть зарегистрировано не менее 30 ошибок (см. *[15]*). Например, если получены 30 ошибок ложного несовпадения при 3000 независимых попытках парного сравнения, можно с доверительной вероятностью 90 % утверждать, что истинная вероятность ошибки находится в диапазоне от 0,7 % до 1,3 %. Правило следует непосредственно из биномиального распределения при независимых попытках, и его можно применять с учетом ожидаемых эксплуатационных характеристик для выполнения оценки.

Пример — Требуемые эксплуатационные характеристики: ВЛНС — 1 % и ВЛС — 0,1 %. В соответствии с правилом тридцати необходимо, чтобы были выполнены 3000 попыток парного сравнения и 30 000 попыток непарного сравнения. Следует учитывать, что при удовлетворении требованию о независимости попыток сравнения необходимо, чтобы в испытаниях приняли участие 60 000 испытуемых субъектов. Альтернатива — найти компромисс путем повторного использования меньшего числа испытуемых субъектов, но это приведет к потере статистической значимости.

Примечание — Правило является общим для разных доверительных интервалов. Например, чтобы быть на 90 % уверенным в том, что истинная вероятность ошибки находится в диапазоне ±10 % установленного значения, необходимо, чтобы было выявлено не менее 260 ошибок. Чтобы быть на 90 % уверенным в том, что истинная вероятность ошибки находится в диапазоне ±50 % наблюдаемого значения, необходимо, чтобы было выявлено не менее 11 ошибок.

В.1.3 Число сравнений для обеспечения требуемой вероятности ошибки

В.1.3.1 Число статистически независимых сравнений, необходимых для обеспечения требуемой вероятности ошибки, показано на рисунке В.1. Например, никакое число ложных совпадений при n независимых непарных сравнениях не может обеспечить требуемую вероятность ошибки ложного совпадения $3/n$ с доверительной вероятностью 95 %**, в то время как 30 ошибок обеспечивают требуемую вероятность $41/n$.

---

* *Здесь и далее доверительная вероятность определена как 100 %-ный уровень значимости, т. е. доверительная вероятность 95 % соответствует уровню значимости 5 %.*

** *Исправлена ошибка оригинала. В соответствии с правилом трех требуемая вероятность ошибки ложного соответствия 3/n с доверительной вероятностью 95 % может быть обеспечена при нулевой наблюдаемой ошибке ложного совпадения.*

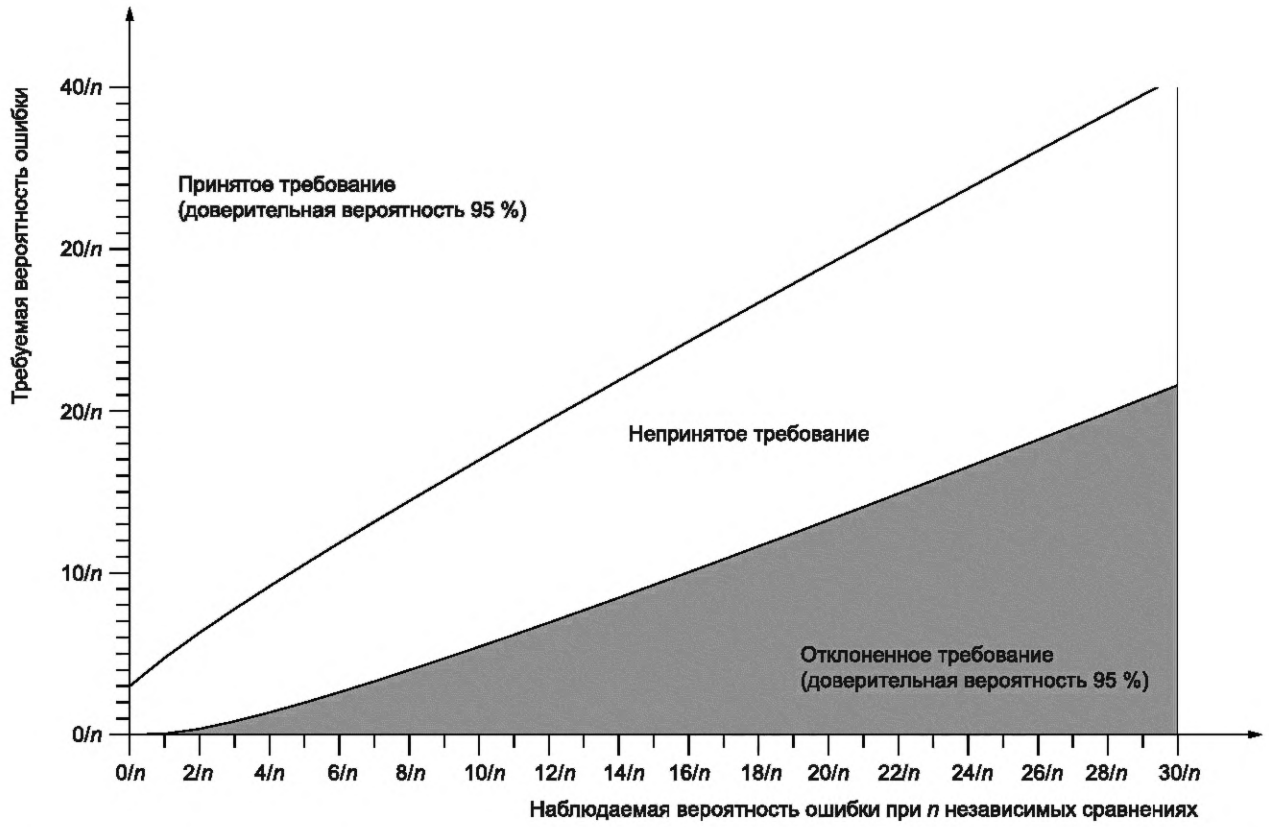

Рисунок В.1 — Области, определяемые с доверительной вероятностью 95 %, для принятия (или отклонения) требуемой вероятности ошибки при n независимых сравнениях

Примечание — Диаграмма, приведенная на рисунке В.1, обеспечивает корректное приближение, если требуемая вероятность ошибки не более 1 %.

В.1.3.2 Чтобы гарантировать статистическую независимость, испытуемые субъекты, предоставляющие биометрические пробы и биометрические контрольные шаблоны при каждой попытке непарного сравнения, должны быть различными и случайно извлеченными из целевой выборки. Данный подход неэффективен из-за низких ВЛС, так как для n независимых сравнений требуется $2n$ добровольцев.

В.1.3.3 Допускается использовать альтернативный метод перекрестного сравнения, но данный метод не гарантирует статистическую независимость. С n субъектами перекрестное сравнение попыток или биометрических контрольных шаблонов для каждой (неупорядоченной) пары может иметь низкую степень корреляции. Корреляции в пределах $n(n-1)/2$ попыток ложных совпадений уменьшают доверительную вероятность для обеспечения требуемого уровня ВЛС по сравнению с тем же числом независимых сравнений.

В.2 Дисперсия эксплуатационных характеристик как функция объема испытаний

По мере увеличения объема испытаний дисперсия оценок уменьшается, но масштабный коэффициент зависит от источника вариации.

Если все испытуемые субъекты совершают несколько попыток парного сравнения, то дисперсия наблюдаемой ВЛНС содержит компоненты, обусловленные:

- вариацией испытуемых субъектов, отнесенной к их числу;
- остаточной вариацией попыток парного сравнения, отнесенной к их числу.

Если испытуемые субъекты совершают несколько попыток и попытки непарного сравнения выполнены в режиме отложенного задания путем перекрестного сравнения данных попыток с биометрическими контрольными шаблонами от различного набора испытуемых субъектов, то дисперсия наблюдаемой ВЛС содержит компоненты, обусловленные:

- вариацией испытуемых субъектов, отнесенной к их числу;
- вариацией имитируемых биометрических контрольных шаблонов, отнесенной к их числу;
- вариацией попыток (отличается от рассчитанной вариации испытуемых субъектов), отнесенной к их числу;
- остаточной вариацией произведенных попыток непарного сравнения, отнесенной к их числу.

Примечание — Доддингтон и др. (см. [2]) показали существование «козлов», «ягнят» и «волков» в биометрических системах. «Козлы» — испытуемые субъекты, имеющие персональную ВЛНС значительно выше, чем

другие представители выборки; «ягнята» — испытуемые субъекты, чьи биометрические контрольные шаблоны имеют непропорциональную долю ложных совпадений, а «волки» — испытуемые субъекты, чьи биометрические образцы чаще показывают ложные совпадения. Это подразумевает, что для ВЛНС компонент дисперсии для испытуемых субъектов отличается от нуля; для ложного совпадения компоненты для испытуемых субъектов и для биометрических контрольных шаблонов отличаются от нуля.

В.3 Оценка дисперсии эксплуатационных характеристик

В.3.1 Общие положения

В данном подразделе приведены формулы и методы оценки дисперсии эксплуатационных характеристик. Дисперсия — статистическая мера погрешности, которую допускается использовать при оценке доверительных интервалов и др. Применение данных формул зависит от следующих предположений относительно распределения ошибок сравнения:

a) испытуемая группа является репрезентативной по отношению к целевой выборке. Это справедливо в том случае, если, например, испытуемые субъекты выбраны случайно из целевой выборки;

b) попытки различных испытуемых субъектов являются независимыми. Это не всегда выполнимо. Поведение испытуемых субъектов зависит от того, что они видят, что делают другие. Корреляции между испытуемыми субъектами будут незначительными по сравнению с корреляциями в пределах ряда попыток одним испытуемым субъектом;

c) попытки не зависят от порогов. В ином случае оценки вероятностей ошибок могут быть смещены, исключение составляет порог, используемый для сбора биометрических данных;

d) вероятности ошибок варьируются внутри выборки. Различные испытуемые субъекты могут иметь различные индивидуальные ВЛНС, и различные пары испытуемых субъектов могут иметь различные индивидуальные ВЛНС;

e) число наблюдаемых ошибок является достаточно большим. При отсутствии наблюдаемых ошибок при вычислении по формулам получают нулевую дисперсию, и в этом случае применяют правило трех. М. Шокерс и др. (см. *[16]*) исследуют условия, при которых применяемые методы, подобные представленным в настоящем приложении, будут обеспечивать соответствующие интервалы покрытия.

В.3.2 Дисперсия наблюдаемой ВЛНС

В.3.2.1 ВЛНС — единственная попытка испытуемых субъектов

Если каждый испытуемый субъект совершает единственную попытку, то наблюдаемую ВЛНС $\hat{p}$ вычисляют по формуле

$$\hat{p} = \frac{1}{n}\sum_{i=1}^{n} a_i, \tag{В.1}$$

а оценку дисперсии наблюдаемой ВЛНС $\hat{V}(\hat{p})$ вычисляют по формуле

$$\hat{V}(\hat{p}) = \frac{\hat{p}\cdot(1-\hat{p})}{n-1}, \tag{В.2}$$

где n — число зарегистрированных испытуемых субъектов;

a_i — число ложных несовпадений для i-го испытуемого субъекта.

Примечания

1 Вывод формулы (В.2) описан в научной литературе по статистике (например, см. *[17]*).

2 Данные формулы неправильно используют в тех случаях, когда испытуемые субъекты совершают несколько попыток. В общем случае не допускается заменять число испытуемых субъектов на n число попыток.

3 Данные формулы применяют для определения оценок дисперсий отказа сбора данных и отказа биометрической регистрации в случае одной попытки испытуемых субъектов.

В.3.2.2 ВЛНС — несколько попыток испытуемых субъектов

Если каждый испытуемый субъект совершает одинаковое число попыток, соответствующие оценки $\hat{p}$ и $\hat{V}(\hat{p})$ вычисляют по следующим формулам (см. *[17]*):

$$\hat{p} = \frac{1}{mn}\sum_{i=1}^{n} a_i, \tag{В.3}$$

$$\hat{V}\left(\hat{p}\right) = \frac{1}{(n-1)}\cdot\left(\frac{1}{m^2 n}\sum_{i=1}^{n} a_i^2 - \hat{p}^2\right), \tag{В.4}$$

где n — число зарегистрированных испытуемых субъектов;

m — число попыток, совершенных каждым испытуемым субъектом;

a_i — число ложных несовпадений для i-го испытуемого субъекта.

Примечания

1 Если $m = 1$, то для оценки применяют формулы (В.1) и (В.2).

2 Формулы (В.3) и (В.4) применяют для определения оценок дисперсий отказа сбора данных в случае нескольких попыток испытуемых субъектов.

В.3.2.3 ВЛНС — неравночисленные попытки испытуемых субъектов

Число попыток испытуемого субъекта может варьироваться. Некоторые субъекты могут не выполнить требуемое число попыток. Отказы сбора данных также могут стать причиной того, что попытки не будут учтены при вычислении ВЛНС. Если отсутствует корреляция между числом сделанных попыток и числом удачных попыток, то соответствующие оценки $\hat{p}$ и $\hat{V}(\hat{p})$ вычисляют по следующим формулам:

$$\hat{p} = \frac{\sum_{i=1}^{n} a_i}{\sum_{i=1}^{n} m_i}, \tag{В.5}$$

$$\hat{V}(\hat{p}) = \frac{\sum_{i=1}^{n} a_i^2 - 2\hat{p}\sum_{i=1}^{n} a_i m_i + \hat{p}^2 \sum_{i=1}^{n} m_i^2}{\frac{n-1}{n}\left(\sum_{i=1}^{n} m_i\right)^2}, \tag{В.6}$$

где n — число зарегистрированных испытуемых субъектов;

m — число попыток, совершенных i-м испытуемым субъектом;

a_i — число ложных несовпадений для i-го испытуемого субъекта.

Примечания

1 Данная оценка дисперсии по [*17*] — это приближение, представленное в удобной для применения форме.

2 При равном числе попыток m_i вычисление оценок проводят по формулам (В.3) и (В.4).

3 Если частота использования испытуемых субъектов коррелирует с числом удачных попыток (например, отсеянные испытуемые субъекты могут совершить дополнительные попытки для биометрического распознавания или, пользуясь системой более часто, могут привести к завышенным оценкам эксплуатационных характеристик в связи с эффектом привыкания), то формулы (В.5) и (В.6) не применяют, так как результат испытаний будет зависеть от малой группы часто встречающихся, но нетипичных испытуемых субъектов.

В.3.3 Дисперсия наблюдаемой ВЛС

Если проведен полный набор перекрестных сравнений, то наблюдаемую ВЛС $\hat{q}$ и оценку дисперсии наблюдаемой ВЛС $\hat{V}(\hat{q})$ вычисляют по следующим формулам соответственно:

$$\hat{q} = \frac{1}{mn \cdot (n-1)} \sum_{i=1}^{n} \sum_{j=1}^{n} b_{ij}, \tag{В.7}$$

$$\hat{V}(\hat{q}) \approx \frac{1}{m^2 \cdot n^2 \cdot (n-1)^2} \sum_{i=1}^{n} (c_i + d_i)^2 - \frac{4}{n} \cdot \hat{q}^2, \tag{В.8}$$

где n — число испытуемых субъектов (и зарегистрированных биометрических контрольных шаблонов);

m — число биометрических образцов каждого испытуемого субъекта;

b_{ij} — число биометрических образцов i-го испытуемого субъекта, ложно совпадающих с биометрическим контрольным шаблоном j-го испытуемого субъекта ($b_{ii} = 0$);

c_i — число ложных совпадений с биометрическим контрольным шаблоном i-го испытуемого субъекта, вычисляемое по формуле

$$c_i = \sum_{j=1}^{n} b_{ji}; \tag{В.9}$$

d_i — число ложных совпадений для i-го испытуемого субъекта, вычисляемое по формуле

$$d_i = \sum_{j=1}^{n} b_{ij}. \tag{В.10}$$

Формулы для более общего метода, не требующего точно m биометрических образцов для каждого испытуемого субъекта и допускающего неквадратичные матрицы числа биометрических контрольных шаблонов и биометрических проб, приведены в *[18]* [(4.1)—(4.12)].

В.4 Оценка доверительных интервалов

В.4.1 Общие положения

В.4.1.1 В соответствии с центральной предельной теоремой (см. *[17]*) при достаточно большом количестве попыток наблюдаемые вероятности ошибок должны подчиняться нормальному закону распределения. Если значения вероятностей ошибок близки к 0 %, а дисперсия не одинакова по выборке, то остается некоторая асимметрия до тех пор, пока число испытуемых субъектов не станет достаточно большим.

В.4.1.2 Согласно допущению о нормальном распределении границы $100(1 - \alpha)$ % доверительного интервала для наблюдаемых вероятностей ошибки вычисляют по формуле

$$\hat{p} \pm z \cdot (1-\alpha/2)\sqrt{\hat{V}(\hat{p})}, \qquad (B.11)$$

где $z(x)$ — квантили стандартного нормального распределения, т. е. площадь под кривой плотности вероятности стандартного нормального распределения с серединой в нуле и дисперсией, равной единице, в интервале от $-\infty$ до $z(x)$ равна x. Для 95 %-ного доверительного интервала значение $z(0{,}975) = 1{,}96$;

α — вероятность того, что доверительный интервал не содержит истинного значения вероятности ошибки;

$\hat{p}$ — наблюдаемая вероятность ошибки;

$\hat{V}(\hat{p})$ — оценка дисперсии вероятности ошибки.

В.4.1.3 Как правило, при применении формулы *(B.11)* доверительный интервал включает в себя отрицательные значения наблюдаемой вероятности ошибки, но отрицательных значений вероятностей ошибок быть не может. Это происходит вследствие отклонения от нормального распределения наблюдаемой вероятности ошибки. В таких случаях для определения доверительных интервалов следует использовать непараметрические методы, например самонастройку (см. *[19]—[21]*).

В.4.2 Самонастраивающиеся оценки дисперсии и доверительных интервалов

В.4.2.1 Если биометрическая система обеспечивает самонастраивающуюся оценку, то это устраняет необходимость делать предположения относительно распределения наблюдаемых вероятностей ошибок и зависимостей между попытками. Распределения и зависимости система определяет по имеющимся данным. При выполнении выборки с заменой первоначальных данных может быть создан самонастраивающийся биометрический образец, по которому проводят определение вероятности ошибки. При большом числе таких самонастраивающихся биометрических образцов может быть получено эмпирическое распределение, используемое для определения доверительных интервалов, оценки неопределенности и т. д.

В.4.2.2 Чтобы проиллюстрировать процесс, предположим, что необходимо оценить ВЛС, используя полный набор перекрестных сравнений с n испытуемыми субъектами, каждый из которых совершает по m попыток, которые будут сравниваться со всеми $(n - 1)$ несобственными биометрическими контрольными шаблонами. Значение x (a, v, t) обозначает результат сопоставления попытки a испытуемого субъекта v с биометрическим контрольным шаблоном t. Набор данных X для оценки ВЛС включает в себя результаты всех mn $(n - 1)$ перекрестных сравнений $X = \{ x(a, v, t) \mid i \in \{1,\ldots, n\}, j \in \{1,\ldots, n - 1\}\ a \in \{1,\ldots, m\}\}$. Каждый самонастраивающийся биометрический образец должен быть построен с помощью набора данных X методом, который повторяет структуру и зависимость первоначальных данных. Этот метод заключается в следующем:

a) выборка n испытуемых субъектов с заменой: $v(1)$, ..., $v(n)$ (выборка с заменой означает, что список будет содержать более чем одно появление одного и того же элемента);

b) для каждого $v(i)$ биометрического образца с заменой $(n - 1)$ несобственных биометрических контрольных шаблонов: $t(i, 1)$, ..., $t(i, n - 1)$;

c) для каждого $v(i)$ биометрического образца с заменой m попыток, выполненных испытуемым субъектом: $a(i, 1)$, ..., $a(i, m)$;

d) самонастраивающийся биометрический образец:

$$Y = \{ v(i), t(i, j)\ a(i, k) \mid i \in \{1,\ldots, n\}, j \in \{1,\ldots, n - 1\}\ a \in \{1,\ldots, m\}\}.$$

Создается множество самонастраивающихся биометрических образцов, и для каждого из них определяют ВЛС. Распределение значений самонастройки для ВЛС используют для аппроксимации наблюдаемой ВЛС.

В.4.2.3 По самонастраивающимся значениям определяют границы $100(1 - \alpha)$ % доверительного интервала: выбирают такие значения L (нижний предел) и U (верхний предел), что $\alpha/2$ самонастраивающихся значений будет меньше L, а $\alpha/2$ самонастраивающихся значений — больше U. Для определения границ 95 %-ного доверительного интервала следует использовать не менее 1000 самонастраивающихся образцов, а для 99 %-ного доверительного интервала — не менее 5000 самонастраивающихся образцов.

В.4.3 Разбиение на подмножества

В.4.3.1 Данный метод для определения границ доверительного интервала ошибок по наблюдаемым вероятностям ошибок заключается в разбиении собранных данных испытаний на непересекающиеся подмножества испытуемых субъектов и в построении графика КОО для каждого подмножества. Например, в протоколе испытаний (см. *[10]*) данный метод применен для определения эллипсов ошибки.

В.4.3.2 Основной метод определения эллипсов ошибки заключается в следующем:

a) собрать результаты эксплуатационных испытаний, при которых испытаны n испытуемых субъектов;

b) разделить целевую выборку на m (например, $m = 10$) непересекающихся подмножеств размером n/m;

c) построить график КОО для каждого подмножества;

d) установить порог t:

1) вычислить $x_i = (\text{ВЛС}_i, \text{ВЛНС}_i)$ при данном пороге для всех множеств $i = 1, ..., m$,

2) вычислить выборочное среднее значение $\overline{x}$ и выборочную ковариацию S по следующим формулам:

$$\overline{x} = \frac{1}{m}\sum_{i=1}^{m} x_i, \qquad (B.12)$$

$$S = \frac{1}{m-1}\sum_{i=1}^{m}\left(\left(x_i - \overline{x}\right)\cdot\left(x_i - \overline{x}\right)^T\right), \qquad (B.13)$$

3) вычислить собственные векторы и собственные значения S,

4) центр эллипса в $\overline{x}$, ориентация осей задается собственными векторами S, а длины полуосей пропорциональны квадратному корню из соответствующих собственных векторов, константа пропорциональности равна квадратному корню из критерия хи-квадрат для целевого уровня безопасности (при двух степенях свободы), деленному на $\sqrt{m}$,

5) согласно допущению о нормальном распределении эллипс ошибок обеспечивает доверительную границу для ВЛС и ВЛНС (вычисленных для всей целевой выборки) при пороге t;

e) повторить операции, указанные в перечислениях a)—d), при других порогах t.

Примечание — Аналогичную процедуру допускается использовать для биометрических систем идентификации путем разбиения поискового множества. Для оценки неопределенности в ВЛПИ непарное поисковое множество разбивают на M непересекающихся множеств. Для оценки достоверности в ВЛПИ разбивают парное поисковое множество.

Приложение С
(справочное)

Факторы, влияющие на эксплуатационные характеристики биометрических систем

С.1 Общие положения

В настоящем приложении приведено описание особенностей пользователя и факторов окружающей среды, влияющих на эксплуатационные характеристики биометрических систем. Данные факторы следует контролировать и/или фиксировать в процессе сбора данных.

При составлении плана испытания для каждого фактора определяют:

a) настройки биометрической системы, необходимые для минимизации влияния (или выяснения влияния) какого-либо фактора на эксплуатационные характеристики биометрических систем. Настройки могут содержать требования, например требования к тому, чтобы погрешность была постоянной или случайной при всех попытках, а влияние данного фактора было распределено равномерно среди испытуемых субъектов и попыток;

b) факторы, которые необязательно контролировать. Например, при сценарном испытании какой-либо фактор может оказывать такое же воздействие на биометрическую систему, как и при ее целевом применении. В других случаях предварительные испытания могут показать, что воздействие конкретных факторов является минимальным для данной системы;

c) информацию, которую следует записывать при испытании для определения:
   1) значимости (или незначимости) любого воздействующего фактора;
   2) особых случаев, при которых воздействующие факторы могут вносить систематическую ошибку в результаты.

Если проблема связана с опознаванием подмножества испытуемых субъектов, то следует сравнить вероятности ошибок данных для этого подмножества по отношению к остальным испытуемым субъектам.

Такая контрольная таблица в соответствии с настоящим приложением, содержащая рассмотренные и проанализированные факторы, может быть включена в протокол испытания.

Воздействующие факторы влияют в основном только на подмножества биометрических модальностей. Например, изменение освещения влияет только на биометрические системы, работающие в оптическом диапазоне длин волн (например, такие, которые регистрируют изображения лица, отпечатка пальца, сетчатки, РОГ или сосудов), а акустические помехи влияют на системы, основанные на звуке (например, биометрическая верификация диктора). Некоторые биометрические системы обеспечивают контроль данных факторов. Также могут быть выявлены другие факторы окружающей среды и воздействия на биометрические системы.

Влияние данных факторов может снизить качество биометрического образца, при этом увеличивается ВОР, ВОСД или ВЛНС. Кроме того, в случае зашумленных и некачественных изображений и сигналов возрастает ВЛС.

С.2 Список факторов

С.2.1 Демографические факторы

Демографические факторы включают в себя:

a) возраст испытуемого субъекта. Дети (характеризующиеся быстрым ростом) и пожилые люди (у которых биометрические характеристики могут долго восстанавливаться после повреждения) имеют тенденцию к большему количеству ложных несовпадений и отказов сбора данных, чем в среднем по выборке;

b) этническое происхождение, пол и род занятий испытуемого субъекта. Качество биометрической характеристики (для конкретной биометрической системы) может зависеть от этнического происхождения, пола и рода занятий испытуемого субъекта. Биометрическая система, настроенная на определенную целевую выборку, может работать хуже, если будет использована с другим этническим или половым составом выборки субъектов.

С.2.2 Факторы применения

Факторы применения включают в себя:

a) время между биометрической регистрацией и биометрической верификацией. Старение биометрического шаблона, т. е. изменение в биометрической характеристике испытуемого субъекта и методе предъявления, будет происходить в период времени между созданием регистрируемого биометрического контрольного шаблона и попыткой биометрической верификации или биометрической идентификации. Для некоторых модальностей эксплуатационные характеристики, определяемые в течение короткого промежутка времени после биометрической регистрации, когда внешность испытуемого субъекта и его поведение изменились незначительно, будут лучше полученных через несколько недель или месяцев;

b) время суток. Поведение и физиологические особенности испытуемого субъекта могут изменяться в течение суток;

c) осведомленность испытуемого субъекта. Когда испытуемые субъекты начинают понимать работу биометрической системы, они становятся более подготовленными к тому, чтобы самостоятельно принимать правильное положение, а также могут самостоятельно решить многие из возможных проблем, возникающих при биометрической верификации;

d) мотивация испытуемого субъекта. Испытуемые субъекты будут действовать по-разному согласно значимости биометрической транзакции.

С.2.3 Анатомические и биологические факторы, связанные с испытуемым субъектом

Анатомические и биологические факторы, связанные с испытуемым субъектом, включают в себя:

a) бороду и усы (оказывают влияние на биометрические системы идентификации по изображению лица);

b) облысение;

c) инвалидность, заболевание или недомогание, например:

1) ампутация (невозможно использовать биометрические системы идентификации по изображению руки или пальца),

2) артрит (трудно использовать биометрические системы идентификации по изображению руки или пальца),

3) слепота (невозможно использовать биометрические системы идентификации по изображению РОГ или сетчатки, для других биометрических систем слепота влияет на расположение испытуемого субъекта),

4) подкожные кровоизлияния (временно влияют на изображения лица или руки),

5) простуда или ларингиты (временно влияют на голос),

6) костыли (могут вызвать затруднение с устойчивостью),

7) опухоль (временно влияет на изображения лица или руки),

8) инвалидные кресла (для людей в инвалидных креслах биометрическая система может быть расположена на неподходящей высоте),

9) изменение состояния здоровья (может происходить быстрее, чем нормальные эффекты старения);

d) ресницы (длинные ресницы могут уменьшить видимость РОГ);

e) длинные ногти (влияют на расположение руки и пальца);

f) состояние подушечки пальца, например:

1) интервалы между гребнями кожи и их глубина,

2) сухой, потрескавшийся или влажный палец;

g) рост (очень высокие или очень низкие люди или находящиеся в инвалидных креслах могут испытывать затруднения с правильным расположением);

h) интенсивность цвета РОГ;

i) цвет кожи (может влиять на возможность биометрической системы правильно определять местонахождение лица или РОГ).

С.2.4 Факторы, связанные с поведением испытуемого субъекта

Факторы, связанные с поведением испытуемого субъекта, включают в себя:

a) диалект, акцент и родной язык (могут влиять на биометрические системы идентификации по голосу);

b) выражение, интонация и громкость голоса (влияют на биометрические системы идентификации по голосу);

c) выражение лица;

d) алфавит языка (влияет на биометрические системы идентификации, основанные на характерных признаках почерка);

e) неправильная речь или неправильное чтение фраз (влияет на биометрические системы идентификации по голосу);

f) движение (для некоторых биометрических систем необходимо, чтобы испытуемый субъект сохранял неподвижность, в то время как другие системы более соответствуют для работы с движущимся субъектом);

g) поза и расположение, например:

1) расположение перед камерой, профиль, угол,

2) наклон головы (влияет на биометрические системы идентификации по лицу и РОГ),

3) смещения и повороты (влияют на биометрические системы идентификации по отпечатку пальца и руки),

4) расстояние до камеры,

5) чрезмерно высокое или чрезмерно низкое расположение, отклонение влево или вправо;

h) предшествующая деятельность, например:

1) одышка (влияет на биометрические системы идентификации по голосу),

2) потливость (влияет на биометрические системы идентификации по отпечатку пальца),

3) плавание (сморщивание пальцев влияет на биометрические системы идентификации по отпечатку пальца);

i) стресс, напряжение, настроение или отвлекаемость.

С.2.5 Факторы, связанные с внешностью испытуемого субъекта

Факторы, связанные с внешностью испытуемого субъекта, включают в себя:

a) бинты или пластыри (могут изменять или маскировать части руки, лица или подушечки пальцев);

b) одежда и обувь:

1) головные уборы, сережки и шарфы (влияют на биометрические системы идентификации по изображению лица),

2) рукава (влияют на биометрические системы идентификации по изображениям руки),

3) высота каблука (изменяет рост пользователя),

4) брюки, юбки и обувь (влияют на опознавание походки);

c) контактные линзы (влияют на распознавание РОГ);

d) косметика (временно изменяет лицо);

e) очки, солнечные очки (частично скрывают лицо или РОГ);

f) искусственные ногти (изменяют расположение рук для биометрических систем идентификации по изображениям руки и пальца);

g) прическа и окраска волос (временно изменяют лицо);

h) кольца;

i) татуировки.

С.2.6 Воздействующие факторы окружающей среды

Воздействующие факторы окружающей среды включают в себя:

a) задний план:

1) цвет, структура, лишние лица или тени (влияют на эксплуатационные характеристики биометрических систем нахождения лиц),

2) помехи и другие голоса (изменяют зарегистрированный сигнал в биометрических системах идентификации по голосу, влияют на способность пользователя слышать инструкции);

b) уровень, направление освещенности или отражений (влияют на биометрические системы, в состав которых входит камера);

c) погодные условия:

1) температура и влажность (влияют на влажность подушечки пальца, видимость сосудов на инфракрасных изображениях),

2) дождь и снег (влажные волосы изменяют лицо).

С.2.7 Факторы, связанные с датчиком и аппаратурой

Факторы, связанные с датчиком и аппаратурой, включают в себя:

a) оставшиеся отпечатки, загрязнение:

- на объективе камеры,
- печатающем валике;

b) фокусное расстояние;

c) качество датчика (качество микрофона в системах передачи речевых сигналов и качество камеры в системах формирования изображения);

d) изменения датчика: изменения положения датчиков (при различных положениях одни и те же датчики могут работать по-разному. Различий будет больше, если применяют датчики различных моделей или типов);

e) износ датчика;

f) замена датчика;

g) канал передачи (может добавлять помехи к сигналу. Характеристики канала передачи могут изменяться между испытаниями. Например, маршрут сигнала и сети, используемые для разговора по телефону, могут изменяться, и качество сигнала может зависеть от канала передачи).

С.2.8 Факторы, связанные с интерфейсом пользователя

Факторы, связанные с интерфейсом пользователя, включают в себя:

a) обратную связь (эксплуатационные характеристики могут зависеть от результатов, получаемых испытуемыми субъектами по обратной связи. Например, испытуемый субъект видит свой представленный отпечаток пальца, что дает ему возможность изменить положение пальца для сбора биометрического образца надлежащего качества);

b) инструкцию;

c) наблюдателя (различные способы биометрической регистрации, привыкание наблюдателя и индивидуальные особенности наблюдателя).

С.3 Примеры протоколов

С.3.1 Положение пальца

Наблюдение: ориентиры на сканере показывают положение пальцев в допустимых для алгоритма пределах.

Контроль: не проводят.

Запись: не применяют.

С.3.2 Освещенность

Наблюдение: изменения освещенности из-за колебаний дневного света являются причиной проблем, возникающих при биометрической регистрации и биометрической верификации.

Контроль: испытания следует проводить в комнате без дневного освещения с постоянным уровнем освещенности.

Запись: не применяют.

Наблюдение: случайное освещение отражается на РОГ.

Контроль: регулируют блок для предохранения датчика от посторонних источников света.

Запись: не применяют.

С.3.3 Наличие очков

Наблюдение: установлено, что биометрическая система идентификации по изображению лица *X* практически неспособна регистрировать людей в очках.

Контроль: для испытания биометрической системы испытуемые субъекты должны быть без очков.

Запись: число людей, носящих очки, может быть включено в ВОР.

С.3.4 Факторы, связанные с загрязнением валика

Наблюдение: накопление масел на валике снижает эксплуатационные характеристики биометрической системы отпечатка пальца.

Контроль: регулярная очистка системы (график очистки).

Запись: записывают время проведения очистки системы.

С.3.5 Климатические условия

Наблюдение: влажные пальцы вызывают трудности с биометрической регистрацией или биометрической верификацией.

Контроль: не проводят, так как погодные условия предполагаются нормальными.

Запись: записывают температуру окружающей среды и влажность воздуха во время проведения испытания.

Приложение D
(справочное)

Эксплуатационные характеристики алгоритма предварительного отбора

D.1 Перед испытанием биометрических систем идентификации необходимо определить алгоритмы, которые будут использованы для предварительного отбора. Цель данных алгоритмов заключается в том, чтобы разграничить (уменьшить) количество биометрических контрольных шаблонов кандидатов для биометрической идентификации. Чтобы предварительно отобрать подмножество из всей базы данных биометрических контрольных шаблонов, применяют методы предварительного отбора с использованием непрерывной или исключительной классификации, и затем входной биометрический образец сравнивают с каждым биометрическим контрольным шаблоном предварительно отобранного подмножества.

D.2 Предварительный отбор является возможной стратегией оптимизации вычислительной нагрузки. В зависимости от характеристик алгоритмов, степени проникновения, размера регистрационной базы данных и характеристик оборудования отказ от предварительного отбора может оказаться более эффективным для данной биометрической системы. Любая оценка должна быть проведена в соответствии с рекомендациями поставщика системы.

D.3 Метод исключения при классификации является одним из методов предварительного отбора, в котором база данных биометрических контрольных шаблонов заранее разделена на подмножества. После классификации входного биометрического образца и определения его принадлежности к одному из подмножеств данный образец сравнивают только с частью биометрических контрольных шаблонов, принадлежащих его подмножеству. Применяют другие методы, например метод предварительного отбора типа непрерывной классификации (см. *[22]—[26]*). Такие методы могут работать аналогично обычному биометрическому сравнению с использованием более быстрого, но менее избирательного алгоритма.

Пример — Для алгоритма предварительного отбора необходим предварительный набор биометрических контрольных шаблонов. При идентификации собирают предварительный биометрический образец и выполняют поиск по предварительному набору контрольных шаблонов для определения подмножества предварительного отбора.

D.4 Процесс предварительного отбора из всего множества данных биометрических контрольных шаблонов может привести к ошибкам предварительного отбора, которые происходят, если при предъявлении биометрического образца одной и той же биометрической характеристики одного и того же испытуемого субъекта парный биометрический контрольный шаблон не находится в предварительно отобранном подмножестве кандидатов (в методе исключения, например, это происходит тогда, когда зарегистрированный биометрический контрольный шаблон и последующий биометрический образец одной и той же биометрической характеристики одного и того же испытуемого субъекта помещены в разные, не связанные подмножества).

D.5 Эксплуатационные характеристики алгоритма предварительного отбора отражают в протоколе испытания в следующих терминах:

a) вероятность ошибки предварительного отбора — доля попыток биометрической идентификации, когда биометрический контрольный шаблон, соответствующий входному биометрическому образцу, не находится в предварительно отобранном подмножестве биометрических контрольных шаблонов, которые необходимо сравнить с входным биометрическим образцом, от общего количества попыток биометрической идентификации;

b) степень проникновения — доля базы данных, в которой следует проводить поиск (т. е. усредненный размер предварительно отобранных подмножеств, отнесенный к размеру всей базы данных), усредненная по всем попыткам;

c) вычислительная нагрузка биометрической идентификации с использованием предварительного отбора и то, как это масштабируется с числом зарегистрированных биометрических контрольных шаблонов.

D.6 Базу данных, собранную для испытания в режиме отложенного задания, используют при испытании для определения вероятности ошибок проникновения и предварительного отбора. Испытуемый биометрический образец проверяют в базе данных для каждой попытки: предварительный отбор проводят по всем зарегистрированным биометрическим контрольным шаблонам, использующим предлагаемый алгоритм; отмечают число предварительно отобранных кандидатов и вычисляют вероятность ошибки предварительного отбора (при которых множество предварительно отобранных кандидатов не содержит идентификатор испытуемого субъекта, делающего попытку). Вероятность ошибки предварительного отбора определяют как число ошибок предварительного отбора, разделенное на общее число испытуемых биометрических образцов. Степень проникновения определяют как среднеарифметическое предварительно отобранных кандидатов по всем испытуемым биометрическим образцам, отнесенным к числу зарегистрированных биометрических контрольных шаблонов.

D.7 Как правило, алгоритм предварительного отбора имеет настраиваемые параметры. В общем случае, чем меньше среднеарифметическое предварительно отобранного подмножества (или больше число частей базы данных, что происходит в случае исключительной классификации), тем меньше степень проникновения, но больше

вероятность ошибки предварительного отбора. Данные конкурирующие факторы могут быть изображены в виде графика вероятности ошибки предварительного отбора в зависимости от степени проникновения.

D.8 Масштабирование вычислительной нагрузки для биометрической идентификации по мере увеличения количества биометрических контрольных шаблонов может быть экстраполировано с помощью соответствующей масштабирующей модели. Используемая модель масштабирования должна быть представлена в протоколе испытания вместе с результатами.

Примеры

1 В случае исключительной классификации вычислительная нагрузка может быть рассчитана следующим образом:

$$\text{Вычислительная нагрузка} = N \cdot p \cdot C + c + l,$$

где N — число зарегистрированных биометрических контрольных шаблонов;

p — степень проникновения;

C — вычислительные затраты одного сравнения «один к одному»;

c — вычислительные затраты на предварительный отбор биометрической пробы;

l — вычислительные затраты на составление списка кандидатов.

2 В случае применения алгоритма предварительного отбора вычислительная нагрузка может быть рассчитана следующим образом:

$$\text{Вычислительная нагрузка} = N \cdot p \cdot C + N \cdot c + l,$$

где c — вычислительные затраты одного сравнения «один к одному» в алгоритме предварительного отбора ($c \ll C$).

Приложение Е
(справочное)

Идентификационные эксплуатационные характеристики как функция размера базы данных

Е.1 Кривые КОО для биометрической системы распознавания лица в случае биометрической идентификации изображены на рисунке Е.1. Каждая кривая соответствует определенному объему выборки *N*. Значение ВЛПИ в значительной степени возрастает как $1 – (1 – \text{ВЛС})^N$ (для малых значений ВЛС допустимо приближение: $N \cdot$ ВЛС, т. е. линейная зависимость от *N*). Данная модель предполагает независимость биометрических образцов. Приведенные кривые КОО получены эмпирически, поэтому модель является приблизительной. По форме представленных зависимостей можно сделать вывод о трудности проведения биометрической идентификации при приемлемом фиксированном значении ВЛС.

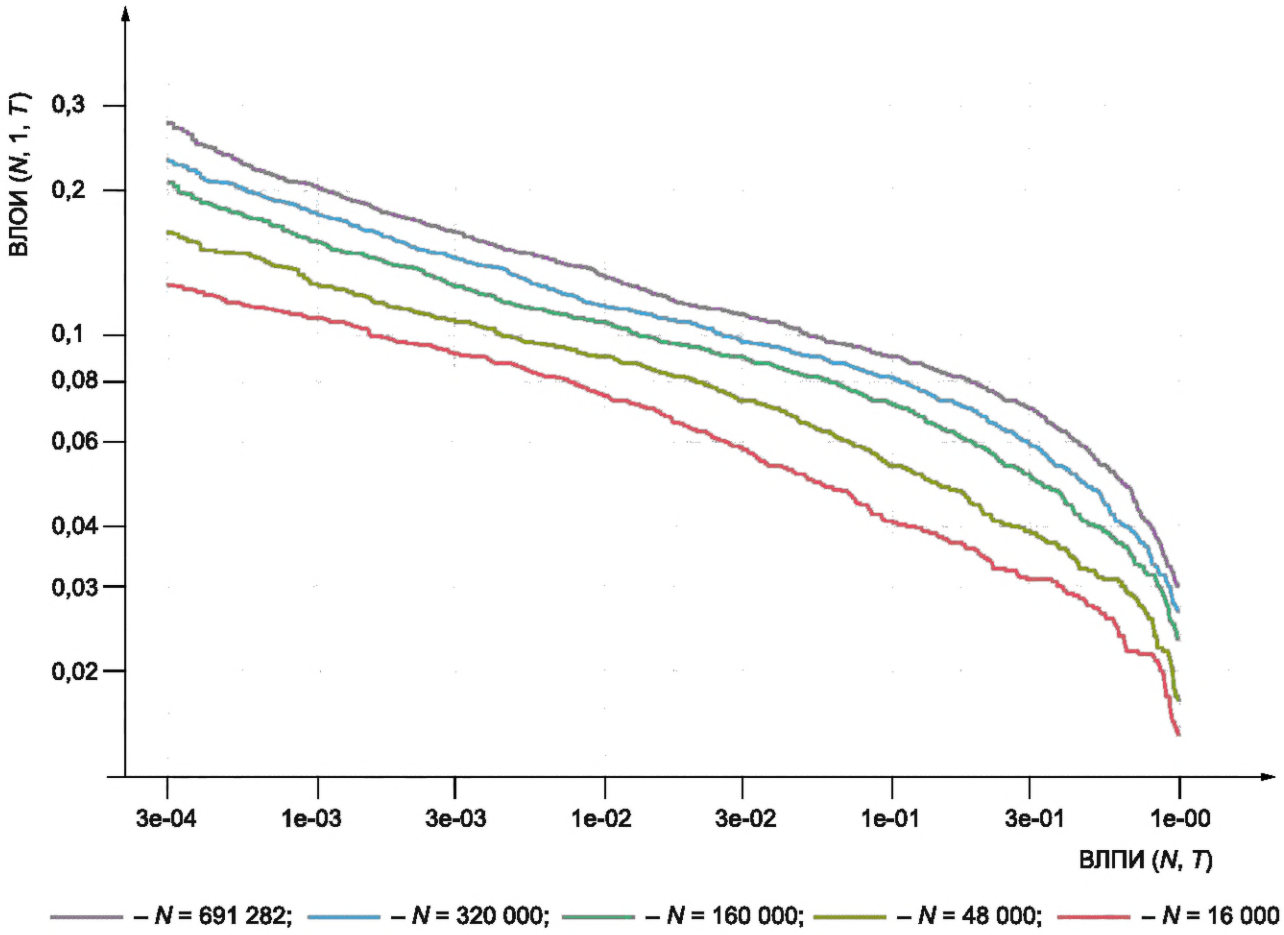

Рисунок Е.1 — Пример кривых КОО, показывающий ВЛОИ как функцию от ВЛПИ для зарегистрированных выборок размером 16 000, 48 000, 160 000, 320 000 и 691 282

Приложение F
(справочное)

Алгоритмы получения данных для графиков КОО и ХСС

F.1 Алгоритм получения данных для графика КОО

F.1.1 Код MATLAB для получения данных для графика КОО

Общедоступные программные пакеты для расчета и построения графиков КОО предоставлены NIST* (см. *[27]*). Приведенный ниже код Matlab основан на принятом ComputeDet.m от NIST_DETWare_V2.1.

```
function [FMR, FNMR, Threshold] = ComputeDet(mated_scores, nonmated_scores)
%
% Основано на ComputeDet.m от NIST_DETWare_V2.1
% ComputeDET рассчитывает (наблюдаемую) ВЛС и ВЛНС на основе показателей схожести
попыток парного и непарного сравнения.
%
% Для данного кода установлено, что совпадение происходит, когда % результат сравнения
выше порога, а несовпадение - когда результат % сравнения равен или ниже порога

num_mated = max(size(mated_scores));
num_nonmated = max(size(nonmated_scores));
total = num_mated+num_nonmated;

scores(1:num_mated,1) = mated_scores;
scores(1:num_mated,2) = 1;
scores(num_mated+1:total,1) = nonmated_scores;
scores(num_mated+1:total,2) = 0;

scores = sortrows(scores);

count_mated = cumsum(scores(:,2),1);
count_nonmated = num_nonmated - ([1:total]'- count_mated);

FNMR(1) = 0;
FMR(1) = 1.0;
FNMR(2:total+1) = count_mated ./ num_mated;
FMR(2:total+1) = count_nonmated ./ num_nonmated;
Threshold = scores(:,1)
return
```

F.1.2 Код Python для получения данных для графика КОО

```
import numpy as np    # install using pip install numpy or conda install numpy
def compute_det(true_scores, false_scores):
'''
Вычисляет кривую КОО по двум спискам/массивам результатов сравнений.
Входные данные:
true_scores (список или np.ndarray): Массив, содержащий результаты парных сравнений
(алгоритм, биометрическая верификация, биометрическая идентификация, результаты
сравнений для подлинного биометрического предъявления)
false_scores (список или np.ndarray): Массив, содержащий результаты непарных сравнений
(алгоритм, биометрическая верификация, биометрическая идентификация, результаты
сравнений при предъявлении атаки)
Выходные данные:
type1_errors (np.ndarray): Массив вероятностей ошибок 1-го рода – ВЛС (сравнение «один
к одному»), ВЛД (биометрическая верификация), ВЛПИ (биометрическая идентификация),
ВОКПА (обнаружение атаки на биометрическое предъявление)
type2_errors (np.ndarray): Массив вероятностей ошибок 2-го рода – ВЛНС (сравнение «один
к одному»), ВЛНД (биометрическая верификация), ВЛОИ (биометрическая идентификация),
ВОКПБП (обнаружение атаки на биометрическое предъявление)
thresholds (np.ndarray): Соответствующий массив порогов принятия решений
    '''
```

---

* *Национальный институт стандартов и технологий США (The National Institute of Standards and Technology).*

```
def __DETsort__(x):
    ndx = np.arange(x.shape[0])
    ind = np.argsort(x[:, 1], kind='mergesort')
    ndx = ndx[ind]
    ndx = ndx[::-1]
    ind = np.argsort(x[ndx, 0], kind='mergesort')
    ndx = ndx[ind]
    sorted_scores = x[ndx, :]
    return sorted_scores
true_scores = np.array(true_scores)
false_scores = np.array(false_scores)
num_true = true_scores.shape[0]
num_false = false_scores.shape[0]
total = num_true + num_false
type2_errors = np.zeros((total + 1))
type1_errors = np.zeros((total + 1))
scores = np.zeros((total, 2))
scores[:num_false, 0] = false_scores
scores[:num_false, 1] = 0
scores[num_false:, 0] = true_scores
scores[num_false:, 1] = 1
scores = __DETsort__(scores)
thresholds = scores[:, 0]
sum_true = np.cumsum(scores[:, 1], axis=0)
sum_false = num_false - (np.arange(1, total + 1) - sum_true)
type2_errors = sum_true / num_true
type1_errors = sum_false / num_false
return type1_errors, type2_errors, thresholds
```

F.1.3 Код *R* для получения данных для графика КОО

Приведенные выше коды Matlab и Python возвращают значения ВЛС и ВЛНС для стольких порогов значений, сколько существует результатов сравнения. В некоторых испытаниях, например при полном перекрестном сравнении в режиме отложенного задания, код может возвратить чрезмерное количество данных для построения графика. Приведенный ниже код *R* позволяет получать данные для заданного набора пороговых значений. В предлагаемом коде используется эмпирическая функция распределения *R* `ecdf ()`.

```
computeDETR <- function(mated_scores,nonmated_scores,thresholds_to_plot)
#
# Вычисляет наблюдаемые ВЛС и ВЛНС при заданном наборе порогов для построения графика
# Для данного кода установлено, что совпадение происходит, когда результат сравнения
выше порога, а несовпадение - когда результат сравнения равен или ниже порога
{
        # при необходимости отсортируйте thresholds_to_plot так, чтобы
        # данные для КОО были приведены в порядке возрастания порога
        thresholds <- sort(thresholds_to_plot)

        cdf_nonmated <- ecdf(nonmated_scores)
        cdf_mated <- ecdf(mated_scores)

        data.frame(Threshold = thresholds,
                   FMR = 1.0 - cdf_nonmated(thresholds),
                   FNMR = cdf_mated(thresholds))
```

F.2 Алгоритм получения данных для графика ХСС

Алгоритм эффективного получения данных для графика ХСС [ранг *R*, ВИПИ (*N*, *R*, 0)] имеет следующий вид (при предположении, что каждому испытуемому субъекту соответствует один биометрический контрольный шаблон и возможен случай, когда результат парного сравнения равен результату непарного сравнения).

Определение ранга биометрической идентификации для каждой попытки парного сравнения (*i*) проводят следующим образом:

1) поиск результата парного сравнения для данной попытки s_i;
2) подсчет количества результатов непарного сравнения для данной попытки x_i, которые больше, чем s_i;
3) подсчет количества результатов непарного сравнения для данной попытки y_i, которые равны s_i;
4) если при $y_i = 0$, попытка имеет ранг биометрической идентификации $x_i + 1$;

5) если $y_i > 0$, ранг определяется диапазоном значений $(x_i + 1),\ldots, (x_i + y_i + 1)$.

Для каждого ранга R вычисляют вероятность биометрической идентификации ранга R следующим образом:

1) вычисляют число попыток с рангом R и менее. Попытки, которые имеют диапазон рангов, считаются как сумма рангов из диапазона, не превышающих R;

2) деление на общее число попыток позволяет получить вероятность биометрической идентификации ранга R, которую строят в зависимости от R на графике ХСС.

То есть для испытания на замкнутом множестве с n попытками парной биометрической идентификации:

$$\text{ВИПИ}(N,R,0) = \frac{1}{n}\sum_{i=0}^{n}\begin{cases} 1 & \text{, если } x_i + y_i < R \\ (R - x_i)/(1 + y_i), & \text{если } x_i < R \le x_i + y_i, \\ 0 & \text{, если } R \le x_i \end{cases} \quad \text{(F.1)}$$

где x_i — число результатов непарных сравнений, значения которых больше результата парного сравнения;

y_i — число результатов непарных сравнений, значения которых равны результату парного сравнения;

n — число транзакций парных сравнений при биометрической идентификации на замкнутом множестве;

R — значение ранга, откладываемое по оси абсцисс на графике ХСС;

N — число зарегистрированных биометрических контрольных шаблонов.

Приложение G
(справочное)

Интерпретация графика КОО

На рисунках G.1—G.4 приведены интерпретации графика КОО.

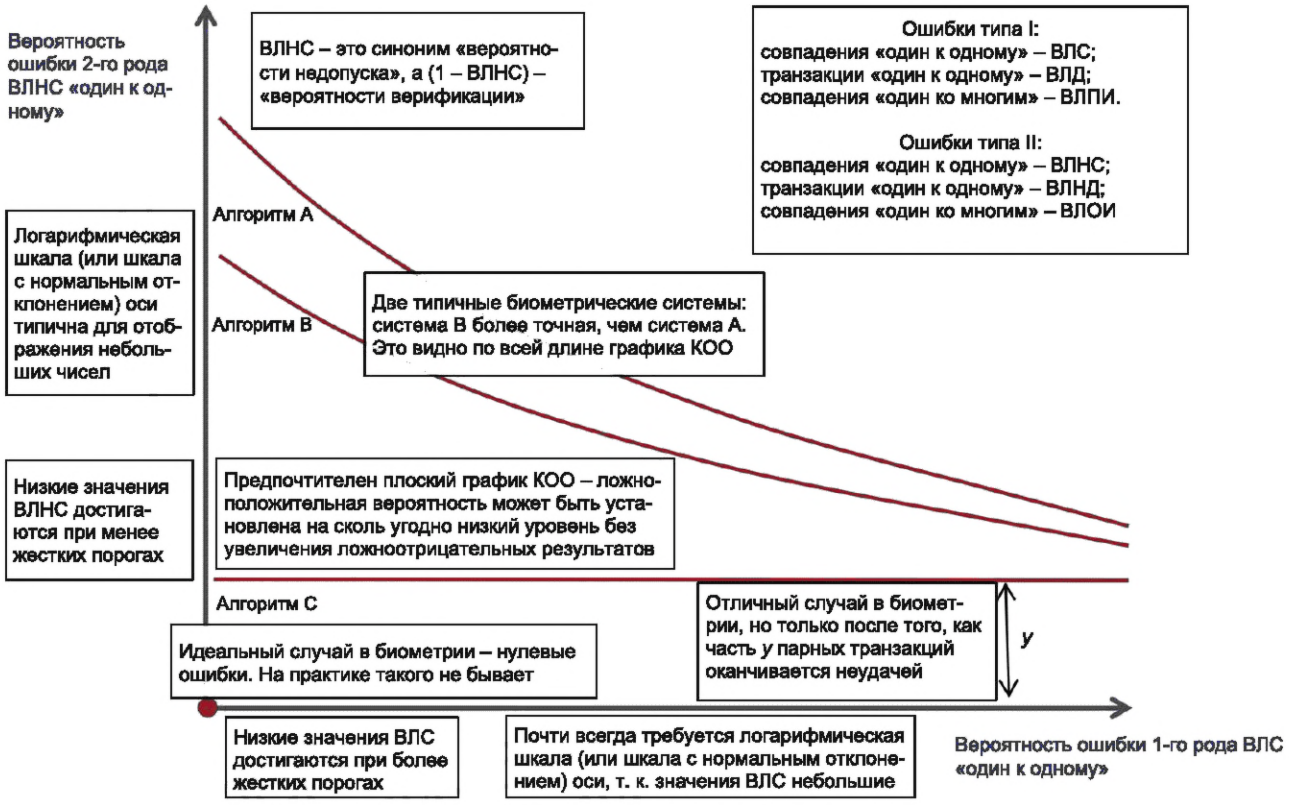

Рисунок G.1 — Интерпретация № 1 графика КОО: вероятности ошибок, характеристики и сравнения алгоритмов

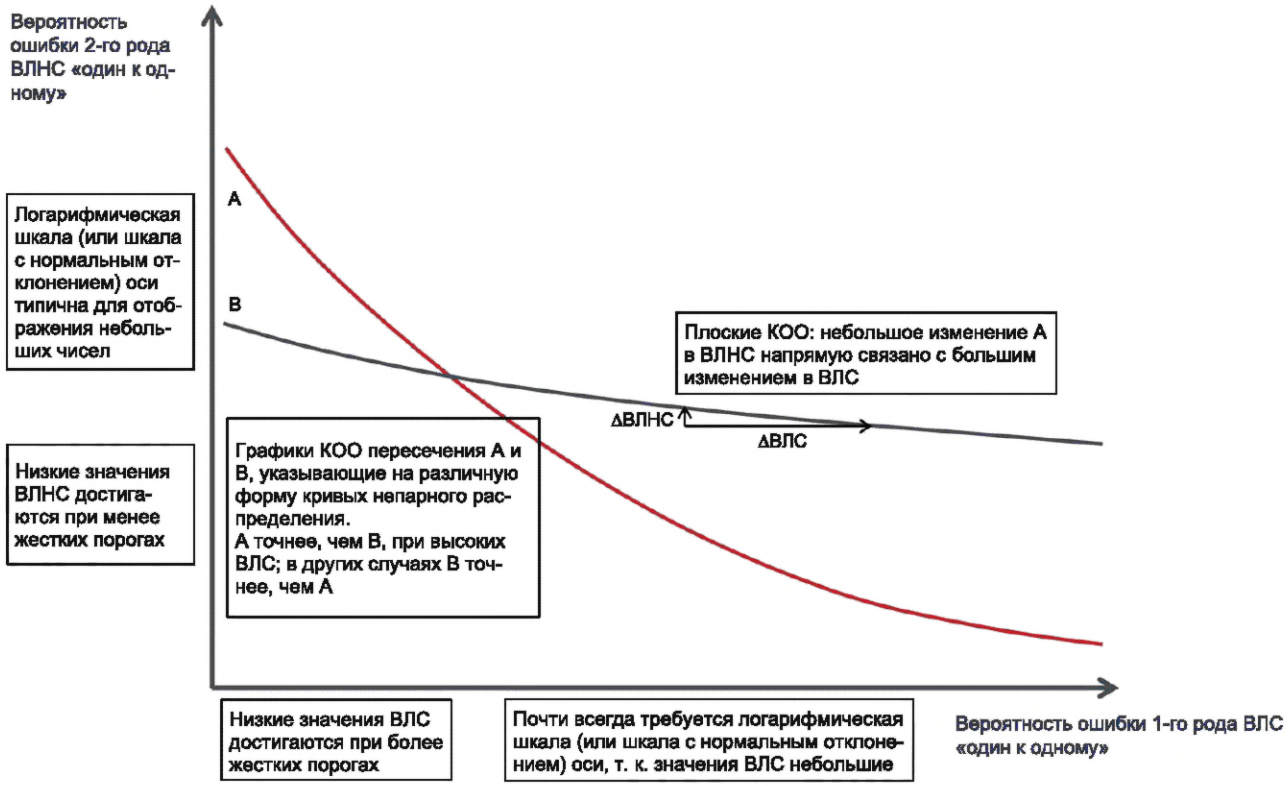

Рисунок G.2 — Интерпретация № 2 графика КОО

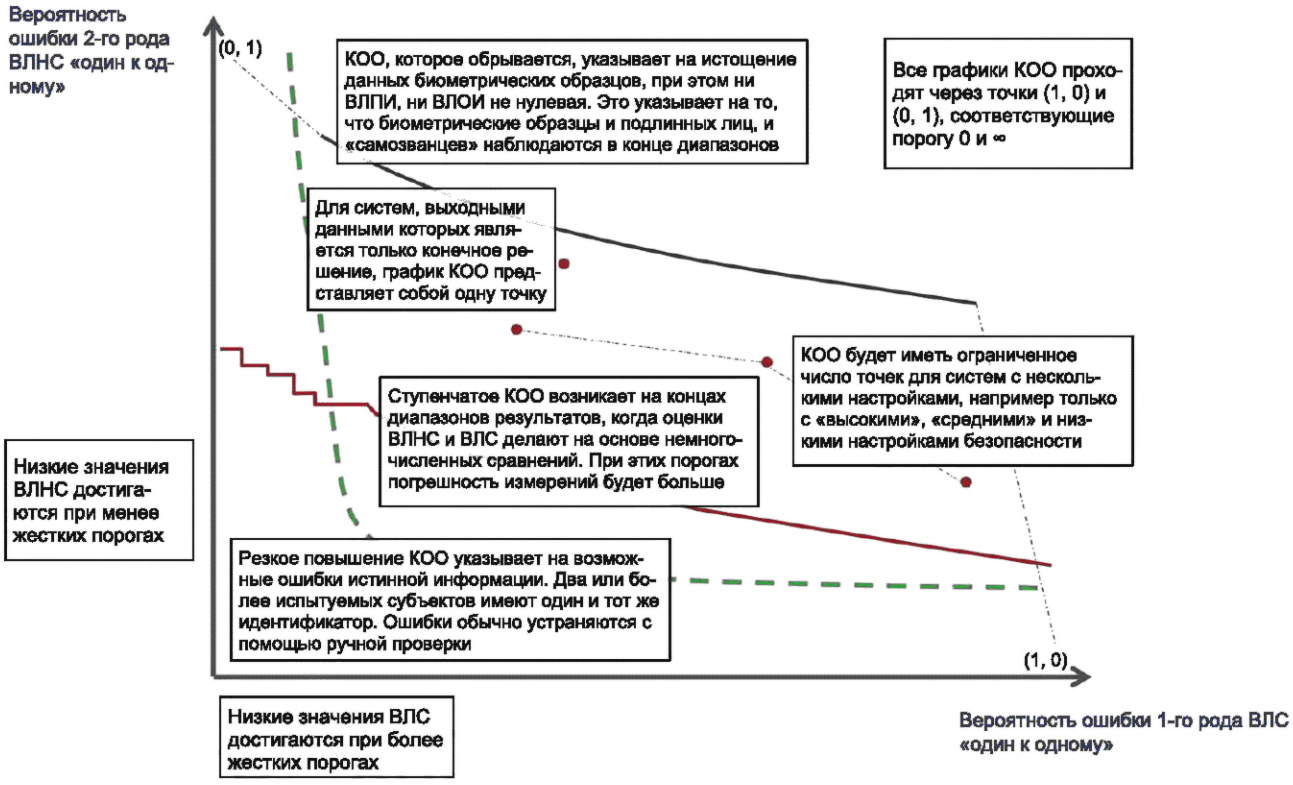

Рисунок G.3 — Интерпретация № 3 графика КОО: неидеальные испытания, наборы данных или системы

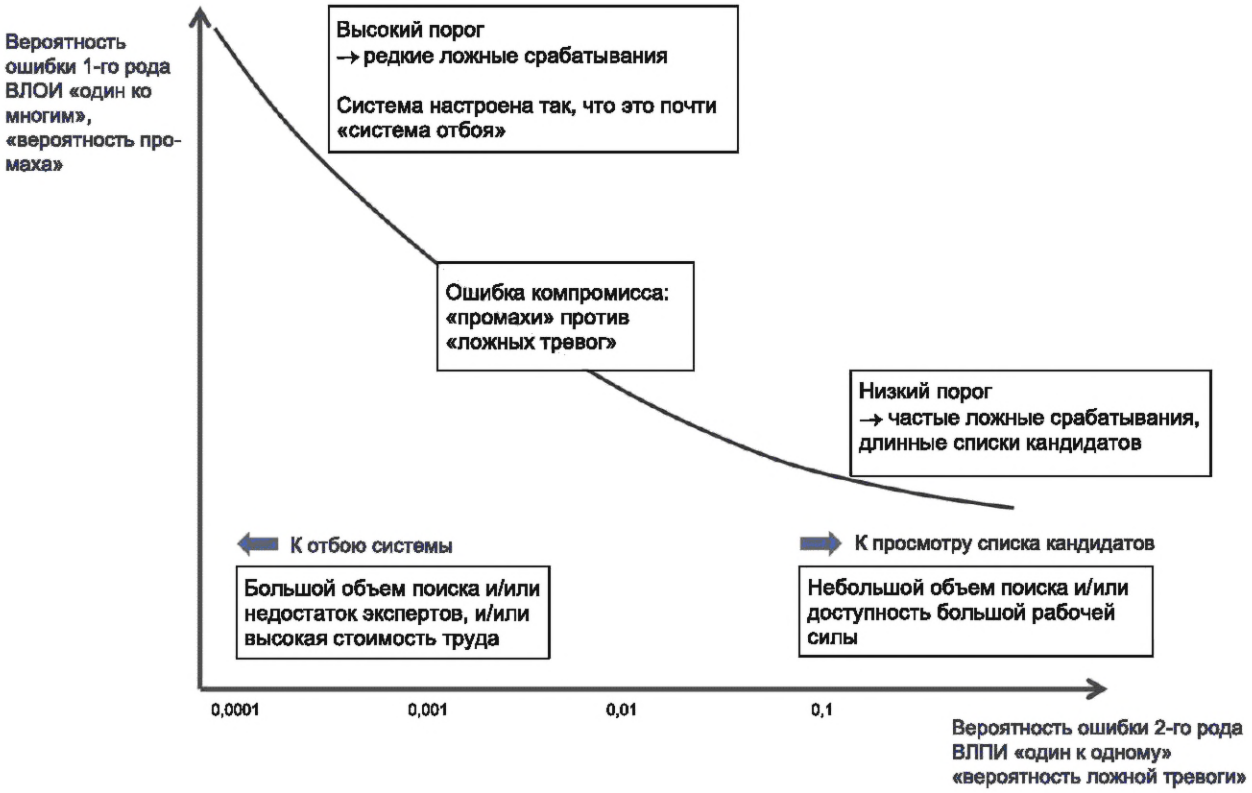

Рисунок G.4 — Интерпретация № 4 графика КОО: биометрическая идентификация ложноотрицательная (промахи) против ложноположительной (тревоги)

Приложение ДА
(справочное)

Сведения о соответствии ссылочного межгосударственного стандарта международному стандарту, использованному в качестве ссылочного в примененном международном стандарте

Таблица ДА.1

Обозначение ссылочного межгосударственного стандарта	Степень соответствия	Обозначение и наименование ссылочного международного стандарта
ГОСТ ISO/IEC 2382-37—2016	IDT	ISO/IEC 2382-37:2012* «Информационные технологии. Словарь. Часть 37. Биометрия»
Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандарта: - IDT — идентичный стандарт.		

* Заменен. Действует ИСО/МЭК 2382-37:2022.

Библиография

[1] HENNESSY, J.L. and PATTERSON, D.A. Computer Architecture: A Quantitative Approach, 2nd ed., Morgan Kaufman, San Francisco, 1996

[2] DODDINGTON, G., LIGGETT, W., MARTIN, A., PRZYBOCKI, M., REYNOLDS, D. Sheep, goats, lambs and wolves: A statistical analysis of speaker performance in the NIST 1998 speaker recognition evaluation. ICSLP, November 1998

[3] WAYMAN, J.L. Multi-finger penetration rate and ROC variability for automatic fingerprint identification systems. National Biometric Test Center, May 1999

[4] WAYMAN, J.L. Technical testing and evaluation of biometric identification devices. Biometrics: Personal identification in networked society, edited by A.K. Jain, et al., Kluwer, 2000, 345—368

[5] GODFREY, J., GRAFF, D., MARTIN, A. Public databases for speaker recognition and verification. ESCA Workshop on Automatic Speaker Recognition, Identification and Verification, 1994

[6] WAYMAN, J.L. Confidence interval and test size estimation for biometric data. Proceedings of the IEEE AutoID Conference, 1999

[7] NEWMAN, H.H., FREEMAN, F.N., HOLZINGER, J.K. Twins, Chicago University Press, 1937. Results on fingerprint similarity between identical twins cited in [31, table 10.20.1]

[8] DAUGMAN, J. and DOWNING, C. Epigenetic randomness, complexity, and singularity of human iris patterns. Proceeding of the Royal Society Biological Sciences, 2001, 268, 1737—1740

[9] JAIN, A.K., PRABHAKAR, S., PANKANTI, S. On the similarity of identical twin fingerprints. Pattern Recognition, 2002, 35(11), 2653—2663

[10] JAIN, A., BOLLE, R., PANKANTI, S. Introduction to biometrics, in: Jain, A., Bolle, R., Pankanti, S. Biometrics: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999, pp. 1—42

[11] FITZMAURICE, G.M., LAIRD, N.M., WARE, J.H. Applied Longitudinal Analysis, 2nd Edition, August 2011

[12] BEST-ROWDEN L. and JAIN, A.K. Longitudinal Study of Automatic Face Recognition, IEEE Trans Pattern Analysis Machine Intelligence, January 2017 gost.e-ecolog.ru

[13] LIBERT, J.,GRANTHAM, J., BANDINI, B., WOOD, S., GARRIS, M., KO, K., BYERS, F., WATSON, C. Guidance for Evaluating Contactless Fingerprint Acquisition Devices, NIST SP 500—305

[14] MARTIN, A., DODDINGTON, G., KAMM T., ORDOWSKI, M., PRZYBOCKI, M. The DET curve in assessment of detection task performance. Proc. Eurospeech '97, Rhodes, Greece, September 1997, Vol. 4, pp. 1895—1898

[15] DODDINGTON, G.R., PRZYBOCKI, M.A., MARTIN, A.F., REYNOLDS, D.A. The NIST speaker recognition evaluation: Overview methodology, systems, results, perspective. Speech Communication, 2000, 31(2—3), 225—254

[16] SCHUCKERS, M., HAWLEY, A., LIVINGSTONE, K., MRAMBA, N. A comparison of statistical methods for evaluating matching performance of a biometric identification device: a preliminary report, Biometric Technology for Human Identification 5404, 144—156, 2004

[17] SNEDECOR, G.W. and COCHRAN, W.G. Statistical methods, Iowa State University Press, 1967 (Sixth edition)

[18] SCHUCKERS, M. Computational Methods in Biometric Authentication, Springer London, 2010

[19] EFRON, B. and TIBSHIRANI, R.J. An introduction to the bootstrap, Chapman and Hall, 1997

[20] DIEGERT, K.V. Estimating performance characteristics of biometric identifiers. Proceedings of Biometrics Consortium Conference, San Jose, CA, June 1996

[21] BOLLE, R.M., RATHA, N., K., PANKANTI, S. Confidence interval measurement in performance analysis of biometric systems using the bootstrap. Proceedings of Workshop on Empirical Evaluation Methods in Computer Vision, Hawaii, December 2001

[22] MALTONI, D. et al. Handbook of Fingerprint Recognition, Springer, 2003

[23] LUMINI, A, MAIO, D., MALTONI, D. Continuous versus exclusive classification for fingerprint retrieval, Pattern Recognition Letters, Vol.18, No.10, pp.1027—1034, 1997

[24] UCHIDA, K., KAMEI, T., MIZOGUCHI, M., TEMMA, T. Fingerprint Card Classification with Statistical Feature Integration, Proceedings of the 14th International Conference on Pattern Recognition, Brisbane, Australia, pp.1833—1839, August 1998

[25] CAPPELLI, R., and MAIO, D. The State of the Art in Fingerprint Classification, in RATHA, N., and BOLLE, R. (Eds.) Automatic Fingerprint Recognition, Chapter 9, pp. 183—205

[26] KAMEI, T. Fingerprint Pre-selection Using Eigenfeatures for a Large-Size Database, in RATHA, N. and BOLLE, R. (Eds.), Automatic Fingerprint Recognition, Chapter 13, pp. 263—282

[27] NIST. Multimodal Information Group Tools. gost.e-ecolog.ru

УДК 004.93’1:006.89:006.354 ОКС 35.240.15

Ключевые слова: информационные технологии, биометрия, биометрическая идентификация, биометрическая верификация эксплуатационные испытания, эксплуатационные характеристики, протокол испытаний, принципы, структура

Редактор *Л.С. Зимилова*
Технический редактор *И.Е. Черепкова*
Корректор *М.И. Першина*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 02.10.2024. Подписано в печать 11.10.2024. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 8,84. Уч.-изд. л. 7,51.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «Институт стандартизации»
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