ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 72510— 2026

Информационные технологии

БИОМЕТРИЯ

Применение биометрии в мобильных устройствах

Издание официальное

Москва
Российский институт стандартизации
2026

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Федеральным государственным бюджетным учреждением «Российский институт стандартизации» (ФГБУ «Институт стандартизации») и Некоммерческим партнерством «Русское общество содействия развитию биометрических технологий, систем и коммуникаций» (Некоммерческое партнерство «Русское биометрическое общество»)

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 27 января 2026 г. № 43-ст

4 ВВЕДЕН ВПЕРВЫЕ

*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

© Оформление. ФГБУ «Институт стандартизации», 2026

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 2
5 Использование биометрии в мобильных устройствах 2
6 Биометрические службы внутри операционной системы мобильного устройства 8
7 Биометрические службы на уровне приложений в мобильных устройствах 10
8 Разработка биометрических приложений (с использованием биометрической библиотеки функций) 11
9 Руководство по функциональности и оперативной работе 14
10 Использование мультифакторной аутентификации 15
11 Руководство по биометрическим модальностям 16
Библиография 18

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

БИОМЕТРИЯ

Применение биометрии в мобильных устройствах

Information technology. Biometrics. Biometrics used with mobile devices

Дата введения — 2026—06—01

1 Область применения

Настоящий стандарт содержит руководство по разработке последовательного и безопасного метода биометрической (отдельной или с наличием небиометрического компонента) персонализации и аутентификации в мобильных устройствах, представленных на открытом рынке и предназначенных для личного пользования.

Руководство предназначено:

- для биометрической верификации («один к одному») или положительной биометрической идентификации («один ко многим»);
- сбора биометрических образцов в той мобильной среде, в которой условия являются неконтролируемыми и не удовлетворяют требованиям нормативно-правовых документов и нормативно-технической документации, устанавливающих требования к качеству биометрических образцов;
- оптимального использования мультифакторных методов биометрической и небиометрической персонализации и аутентификации (ПИН-коды, пароли, персональные данные).

Настоящий стандарт определяет функциональные элементы и компоненты мобильной биометрической системы в целом и характеристики компонентов. Настоящий стандарт содержит руководство по общей мобильной архитектуре со ссылкой на соответствующие стандарты.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

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

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

ГОСТ Р 58624.1 (ИСО/МЭК 30107-1:2016) Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 1. Структура

ГОСТ Р 58624.2 Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 2. Форматы данных

ГОСТ Р 58624.3 (ИСО/МЭК 30107-3:2017) Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 3. Испытания и протоколы испытаний

ГОСТ Р 71414.1 (ИСО/МЭК 19795-1:2021) Информационные технологии. Биометрия. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура

ГОСТ Р ИСО/МЭК ТО 19795-3 Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 3. Особенности проведения испытаний при различных биометрических модальностях

Издание официальное

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 изменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

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

3.1 **мобильное устройство** (mobile device): Портативное вычислительное устройство, как правило, имеющее экран дисплея с входом для устройства ввода аналоговой (графической или речевой) информации и/или миниатюрной клавиатурой.

Примечание — Примерами мобильных устройств являются ноутбуки, планшетные персональные компьютеры, портативные средства информационно-коммуникационных технологий, смартфоны, USB-устройства.

3.2 **персонализация (биометрия)** (personalization): Настройка изделия (устройства) под требования или права доступа конкретного индивида.

4 Сокращения

В настоящем стандарте применены следующие сокращения:

БИ — биометрический интерфейс (Biometric interface, BI);
ВМ — виртуальная машина;
ГИП — графический интерфейс пользователя (Graphical user interface, GUI);
ДСИ — доверенная среда исполнения (Trusted execution environment, TEE);
КБП — коммуникация ближнего поля (Near field communication, NFC);
САА — слой аппаратных абстракций (Hardware Abstraction Layer, HAL);
СГП — система глобального позиционирования (Global positioning system, GPS);
ОС — операционная система (Operating system, OS);
ПБФ — поставщик биометрической функции;
ПИН — персональный идентификационный номер (Personal Identification Number, PIN);
ПИП — прикладной интерфейс приложений;
ЭБ — элемент безопасности (Secure element, SE);
OTG — спецификация USB OTG[1)] (On-the-go — the USB connector of a smartphone);
USB — универсальная последовательная шина (Universal serial bus).

5 Использование биометрии в мобильных устройствах

5.1 Классификация использования биометрии в мобильных устройствах

5.1.1 Общие положения

Контекст использования мобильных устройств на высоком уровне может быть классифицирован по четырем вариантам. Во всех вариантах удобство использования и человеческий фактор должны быть учтены и интегрированы в процесс разработки приложения с применением возможностей биометрии.

[1)] Спецификация USB OTG — расширение спецификации USB 2.0 для соединения периферийных USB-устройств друг с другом без необходимости подключения к персональному компьютеру.

5.1.2 Общие положения для всех случаев использования

5.1.2.1 При внедрении биометрических служб в мобильные устройства независимо от используемой биометрии или приложения должны быть рассмотрены следующие функции:

а) сбор биометрического образца;

б) хранение биометрического контрольного шаблона;

в) обработка биометрического образца;

г) сравнение биометрического образца с биометрическим контрольным шаблоном.

5.1.2.2 Перечисленная в 5.1.2.1 базовая функциональность требует наличия определенных основных функций, включая:

а) сбор одного биометрического образца или более из последовательности образцов (т. е. изображение лица в режиме реального времени);

б) определение наилучшего(их) биометрического(их) образца(ов) на основе показателя качества;

в) обеспечение обратной связи передающему субъекту для предъявления биометрических характеристик (например, демонстрация овальной формы для позиционирования лица);

г) предоставление показателя качества для сбора биометрического образца;

д) предоставление обратной связи при отказе сбора биометрических данных/отказе биометрической регистрации;

е) предоставление информации о доступности датчиков на устройстве (например, камера, мультисенсорный экран, сканер отпечатков пальцев, СГП, акселерометр и т. д.) с соответствующими техническими деталями (например, разрешение сенсорного экрана, число одновременных касаний, разрешение камеры и т. д.);

ж) предоставление информации о том, какие биометрические модальности собраны в качестве биометрических образцов;

и) алгоритмы сравнения для каждой модальности «один к одному» и/или «один ко многим»;

к) получение результата сравнения или ошибки.

5.1.2.3 Приложение может выполнять дополнительные биометрические функции и основные функции управления идентификацией, такие как:

а) возможность сбора данных новой личности, удаления или изменения данных личности;

б) возможность обработки исключений;

в) обработка биометрических образцов.

Указанные функции могут быть частью структуры ОС.

Ключевым аспектом мобильных приложений являются неконтролируемые условия окружающей среды. Окружающая среда не контролируется службой, к которой человек пытается получить доступ, поэтому уровень доверия является важным фактором. Кроме того, окружающая среда может быть разной для каждого случая доступа и меняться со временем.

5.1.2.4 Для всех случаев необходимо учитывать следующие факторы:

а) должно быть принято решение о том, как именно будет выполнена биометрическая регистрация: контролируемым образом [внешняя проверка биометрического(их) образца(ов) с использованием некоторых средств] или неконтролируемым образом (пользователь самостоятельно оценивает результат биометрической регистрации, применяя или не применяя функции проверки качества в соответствии со стандартами). В случае неконтролируемой регистрации рекомендуется, чтобы в системе биометрической регистрации проводилась автоматическая проверка качества биометрических образцов, а также в случае сбора нескольких биометрических образцов — полноты набора биометрических образцов;

б) для защиты персональных данных пользователя устройства рекомендуется, чтобы при создании и хранении биометрические пробы и биометрические образцы были защищены за счет отсутствия внешнего доступа к ним (например, из стороннего приложения);

в) должна быть проанализирована возможность использования устройства более чем одним пользователем в отношении влияния на устройство и уровни доверия;

г) предполагается, что вычислительная мощность мобильного устройства менее вычислительной мощности персонального компьютера, в связи с чем рекомендуется анализировать производительность биометрической обработки мобильного устройства с учетом ресурсов устройства. Также следует проводить анализ эксплуатационных характеристик любого датчика или компонента сбора биометрических данных, встроенных в мобильное устройство, так как характеристики встроенного компонента сбора биометрических данных слабее характеристик эквивалентного специализированного автономного устройства сбора биометрических данных;

д) биометрические службы могут быть предоставлены ОС или сторонними приложениями. В любом случае биометрические службы должны работать в изолированной программной среде, для того чтобы ограничить возможность доступа биометрических служб к запуску вредоносного кода или к данным конфигурации, которые влияют на режим работы службы (например, к порогу принятия решения).

5.1.3 Доступ к устройству

Доступ к устройству является локальной службой устройства без необходимости использования онлайн-служб. Решение принимается на самом устройстве. Положительный результат приводит к разблокировке устройства, позволяет пользователю получить доступ к остальным сервисам и приложениям, установленным на устройстве или доступным удаленно.

Пример — Использование биометрических данных пользователя вместо пароля, ПИН-кода или графического шаблона для разблокировки устройства при его включении или после периода отсутствия активности.

Эта служба обеспечивает минимальный уровень доверия к устройству и содержащимся данным и приложениям. Приложения и доступ к отдельным данным могут потребовать дополнительную аутентификацию, которая повысит уровень доверия. Так как пользователю устройства может понадобиться доступ к службам с низким уровнем доверия (например, новостная лента), механизм разблокировки устройства должен способствовать в большей степени удобству, чем безопасности, и, следовательно, уровень доверия для данного вида использования следует считать низким.

Для удобства пользователей в сценариях с низким уровнем доверия после фиксированного количества неудачных попыток устройство может предложить альтернативную модальность или метод (например, пароль, ПИН-код или графический шаблон могут быть предложены в качестве альтернативного средства разблокировки).

5.1.4 Доступ к локальным приложениям, службам и/или данным

Доступ к локальным приложениям, службам и/или данным является локальной службой устройства без необходимости применения онлайн-служб. Решение принимается на самом устройстве и запрашивается приложением, для того чтобы разрешить продолжительное использование приложения, получить доступ к определенным службам или контролировать доступ к определенным защищенным данным. Эта служба должна выполняться исключительно на разблокированном устройстве и только приложением, доступным на главном экране во избежание несанкционированного доступа сторонними приложениями или службами.

Пример — Доступ к защищенной папке во внутренней памяти устройства через определенное приложение проводника файлов.

Требуемый уровень доверия зависит от приложения, пытающегося аутентифицировать пользователя, и степени доступа, поэтому может меняться. Это означает, что пороги (например, пороги качества или сравнения) могут иметь разные значения в зависимости от требуемого уровня доверия. Во избежание неправильного использования сторонними приложениями следует рассмотреть возможность ограничения значений порогов, для того чтобы они не блокировали систему и не пропускали всех зарегистрированных пользователей. Порог абсолютного промаха не должен перекрывать порог абсолютного попадания.

Примечание — Возможна ситуация, когда изготовитель биометрических служб не предоставляет разные уровни доверия и имеет фиксированные пороги.

5.2 Общие задачи интеграции биометрии в мобильные устройства

5.2.1 Сбор биометрических образцов

Получение биометрических данных, т. е. интеграция устройства сбора биометрических данных в мобильное устройство, зависит от биометрической модальности. Использование сенсорных экранов позволяет мгновенно интегрировать такие модальности, как рукописная подпись или динамика нажатия клавиш. Встроенная камера в большинстве мобильных устройств позволяет без затрат интегрировать функцию распознавания лиц или геометрии руки. Другими датчиками, которые интегрированы в современные мобильные устройства, являются акселерометры и гироскопы. С такими датчиками в качестве биометрических данных может быть использована походка пользователя (см. [1]). С помощью микрофона устройство может распознавать говорящего субъекта.

Размер экрана, а также место, где пользователь должен поставить подпись, могут повлиять на предоставляемую информацию или даже остановить сбор данных в связи с тем, что пользователь прикасается к экрану запястьем при подписании. Условия освещения во время получения фотографии лица (например, сильный задний свет) могут создавать недействительные образцы изображения лица. Кроме того, отсутствие стабилизатора изображения также может приводить к размытию образцов, серьезно влияющему на производительность. В случае применения походки расположение мобильных устройств является одним из параметров, в большой степени влияющих на собираемую информацию, так же как способ удержания смартфона влияет на изменения информации о жесте для подписи в воздухе. Таким образом, в данной области необходимы дальнейшие исследования.

Существуют другие биометрические модальности, для которых отсутствует датчик, встроенный в устройство. Для некоторых модальностей, таких как отпечатки пальцев или радужная оболочка глаза, изготовители устройств интегрируют устройства сбора биометрических данных. В некоторых случаях эти устройства сбора могут быть использованы исключительно собственными приложениями.

В случае применения сосудистого русла некоторые ноутбуки и планшеты оснащаются встроенным датчиком сосудистого русла. Другие модальности находятся на стадии исследования и прототипа или требуют внешних устройств сбора биометрических данных, подключаемых через OTG или Bluetooth.

5.2.2 Процесс аутентификации образца

В настоящем стандарте приведены требования к получению биометрических данных, в связи с чем разработчик должен предоставить средства для аутентификации пользователя, которые с точки зрения потребностей последнего обеспечат минимальное взаимодействие и наиболее быстрый и надежный процесс. Использование внешних устройств сбора биометрических данных не рекомендуется, но при необходимости следует применять, по крайней мере, беспроводной интерфейс. В этом случае шифрование обмениваемой информации является основным критерием для предотвращения атак «человек посередине»[1)].

Должны быть проанализированы условия эксплуатации для установки требований к устройству сбора биометрических данных, а также подробно изучены такие параметры, как температура, влажность, условия освещения (включая эффект прямого солнечного освещения), вибрации (например, во время ходьбы, при нахождении в поезде и т. д.) или шум.

Процесс аутентификации, в том числе его сложность, должны быть разработаны в соответствии с запросами приложения. Различные запросы могут потребовать разную аутентификацию, включая рекомендацию увеличить взаимодействие с пользователем при запросе доступа к чувствительной информации. Поэтому возможно применение такой стратегии, при внедрении которой для разблокировки устройства используется удобная для пользователя биометрия: для доступа к банковским реквизитам — беспроводная токен-аутентификация, для разрешения и подписания денежных переводов — биометрическое сравнение на идентификационной карте.

Большее значение имеет разработка решений с точки зрения пользовательского дизайна. Все процессы аутентификации следует разрабатывать доступными в использовании — их применение должно обеспечивать четкое взаимодействие, быть легко запоминаемым и быстро выполнимым. Требования безопасности могут повлиять на тот уровень, который может быть достигнут при реализации данной цели, поэтому разработчик должен находить баланс между безопасностью и удобством использования. Также важным фактором является вариативность способностей пользователей, в том числе лиц с ограниченными возможностями или инвалидностью. Приложения в целом и процесс аутентификации в частности должны быть сконструированы таким образом, чтобы пользовательский интерфейс мог быть адаптирован к потребностям пользователя (например, визуальная и аудиальная обратная связь, разные шрифты и размеры, различный контраст и т. д.). Для лиц, имеющих инвалидность, может быть рекомендовано использование внешних устройств для распознавания тех пользователей, у которых отсутствует мобильность или возможность слышать или видеть.

Для повышения удобства использования рекомендован общий интерфейс для всех приложений. Дополнительным преимуществом аутентификации является предоставление ОС напрямую. Это поможет не только обеспечить безопасность процесса, но и создать общий способ взаимодействия между пользователем и всеми приложениями, что упростит процесс, а также создаст надежное соединение во время аутентификации.

[1)] Атака «человек посередине» (Man-in-the-middle) — это тип интернет-атак, в процессе которых злоумышленник перехватывает канал связи, получая полный доступ к передаваемой информации.

5.2.3 Удобство пользования

5.2.3.1 Общие положения

Существует целый ряд особенностей в мобильных компьютерных средах, которые делают их пользовательский интерфейс отличным от пользовательского интерфейса персональных компьютеров и которые следует учитывать разработчикам.

Первоначальное различие между удобством использования мобильного устройства и персонального компьютера связано с большим многообразием мобильных устройств. Если применение мобильного устройства не предполагает нахождение пользователя в определенном месте, то это обеспечивает применение широкого спектра устройств, которые могут включать в себя ноутбуки, планшеты, телефоны и портативные электронные устройства. Каждое из этих устройств имеет разные способы использования, однако настоящий стандарт рассматривает общие атрибуты, применимые к планшетам, смартфонам и портативным электронным устройствам.

5.2.3.2 Условия окружающей среды

Мобильные приложения используют в различных условиях, как правило, неконтролируемых. Следует учитывать влияние этих условий на работу устройства. Например, на сбор речи влияют посторонние шумы (такие, как ветер, речь стороннего человека, фоновые звуки), а на сбор визуальных данных влияет освещение, отражения, люди и элементы на заднем фоне и движение.

5.2.3.3 Уменьшенный размер экрана

Уменьшенный размер экрана мобильных устройств требует от разработчиков предоставления основной визуальной информации, необходимой в определенный момент времени, и уменьшения посторонней визуальной информации. Снижение количества визуальной информации на экране подразумевает, что разработчик разбирается как в рабочем процессе приложения, так и в том, какая информация должна быть предоставлена пользователю в каждый момент работы приложения.

5.2.3.4 Ограниченные входные данные

Ввиду малого форм-фактора в мобильном устройстве уменьшается диапазон входных данных, для того чтобы получить преимущество ограниченного общего размера устройства. Это предусматривает различные варианты требований к входным данным, в частности для планшетов и телефонов распространен механизм ввода текста как часть экрана. Такая стратегия уменьшает необходимость в дополнительной клавиатуре, но влияет на ограниченную рабочую область экрана. Необходимо понимание рабочего процесса приложения — для того, чтобы экранная клавиатура не оказывала негативного влияния на визуальную обратную связь, предоставляемую пользователю.

Другие входные данные, такие как микрофон, камера, акселерометр и датчик отпечатков пальцев, присутствуют в различных устройствах и, несмотря на то, что они, как правило, используются несколькими приложениями, должны быть рассмотрены следующие аспекты для ситуаций, требующих высокой точности воспроизведения (например, сбор биометрических данных, а именно: речь, лицо или палец):

а) способно ли технически устройство ввода собирать информацию с достаточной точностью и на каком расстоянии;

б) может ли быть предоставлена пользователю инструкция для обеспечения сбора биометрического образца удовлетворительного качества;

в) имеется ли у пользователя намерение или возможность сбора биометрического образца требуемого качества.

5.2.3.5 Ограничения мощности обработки

Мобильные устройства являются компонентами оборудования с высокой мощностью, если рассматривать только исходные характеристики, однако эта мощность быстро уменьшается при внедрении ОС с интерактивными пользовательскими интерфейсами. Мобильное приложение будет иметь значительно меньше ресурсов и меньшую скорость работы по сравнению с версией приложения для персонального компьютера.

Мобильные приложения, особенно те из них, которые переносятся из версии, используемой для персонального компьютера, должны быть адаптированы для работы с ограниченной вычислительной мощностью и памятью. Приложение, в котором будут иметь место ожидание пользователя и отсутствие ответа на запросы пользователя, будет считаться пользователем неисправным. В первом случае необходимо сделать приложение реагирующим более быстро с задействованием меньшего объема ресурсов, в другом — могут быть введены сигналы об активной обработке приложения с указанием, что приложение выполняет определенные действия.

5.2.3.6 Когнитивная нагрузка

Когнитивная нагрузка является предметом обсуждения относительно удобства использования мобильных устройств в отличие от традиционных персональных компьютеров.

Если во время работы с персональным компьютером для пользователя когнитивная нагрузка будет единственной задачей, то для мобильных устройств обычным является выполнение пользователями других действий (например, вождение автомобиля и использование навигационного приложения на мобильном телефоне, движение во время переписки). При разработке интерфейса приложений должны быть учтены те пользователи, которые выполняют параллельные действия во время вычислений. По мере ввода дополнительных одновременных задач общая когнитивная нагрузка пользователя будет разделена между возникающими задачами, в связи с чем необходимо, чтобы приложения отображали наиболее подходящий интерфейс в любой момент рабочего процесса приложения, для того чтобы свести посторонние действия к минимуму (такие, как нажатия кнопок, изменения экрана и другие визуальные шумы), и предоставляли наиболее содержательную информацию при минимизации несвоевременных отвлечений.

5.2.3.7 Привлекательность для пользователя

То, как пользователи характеризуют мобильные приложения и как их внимание распределено при тестировании новых приложений, является еще одним аспектом удобства использования мобильных приложений.

На всех основных платформах мобильных ОС введена концепция «магазины приложений», в которой представлены самые разнообразные приложения для решения ряда вычислительных задач. С учетом объема приложений, доступных в этих магазинах, ожидаемо, что пользователи рассматривают мобильные приложения как более одноразовые продукты по сравнению с версиями приложений, используемых для персонального компьютера. И если одно приложение не будет соответствовать ожиданиям, то существует множество других приложений. В силу предоставления многих приложений на безвозмездной основе они, как правило, низкого качества. Это заставляет пользователей думать, что мобильные приложения являются одноразовыми, низкокачественными продуктами, которые следует быстро просматривать при поиске работающего решения. Из-за коммодитизации приложений и большого выбора приложений пользователи мобильных приложений, как правило, имеют низкий порог терпимости к плохому дизайну или дизайну, который не привлекает их внимание. Если одно приложение не работает, типичной реакцией является удалить его и установить замену.

Для того чтобы сделать приложение более привлекательным для пользователя, разработчики должны учитывать особенности удобства использования мобильных компьютерных сред.

5.2.4 Испытания решений

Должен быть определен уровень точности интеграции биометрии. Это должно быть сделано не только путем оценки алгоритма с набором биометрических образцов из базы данных, но также с использованием устройства сбора биометрических данных и анализа взаимодействия реальных пользователей с мобильным устройством. Должны быть проведены не только технологические испытания, но и сценарные испытания, включая испытания на стойкость к атакам на биометрическое предъявление по ГОСТ Р 71414.1 и ГОСТ Р 58624.1 — ГОСТ Р 58624.3.

Технологические испытания должны включать оценку безопасности, обеспечиваемой решением, и поиск уязвимостей не только на уровне датчиков, но и ОС.

Главная задача связана с необходимостью выполнения алгоритма в мобильном устройстве, которое будет тратить большое количество времени при использовании основных баз данных. Не менее важная задача заключается в необходимости проведения оценки безопасности всей ОС с фокусированием на хранении информации, доступе к этой информации и на обмене информацией с внешним миром.

Во время проведения сценарных испытаний важно проанализировать удобство использования решения, что означает участие реальных субъектов в нескольких сеансах и нескольких сценариях и положениях. Таким образом, испытания будут длительными и дорогостоящими. Но это также вызывает другие сложности. Одним из важных факторов оценки удобства использования системы является анализ удобства применения для новых пользователей технологии, т. е. граждан, которые ранее не были знакомы с такими устройствами и с биометрической аутентификацией. Так как технология становится все более распространенной, это будет все менее возможно в силу того, что большинство пользователей будут иметь доступ к этой технологии.

Устройства меняются очень быстро в связи с тем, что модели развиваются ввиду влияния маркетинга. Новые модели подразумевают изменения в размере, в периферийных устройствах, вычис-

лительной мощности, пользовательском интерфейсе и ОС. Эти изменения могут повлиять на производительность системы в рабочих условиях. Очевидно, что невозможно испытать систему на всех устройствах, поэтому следует определить стратегию испытаний для минимизации усилий при максимизации извлекаемых выводов.

6 Биометрические службы внутри операционной системы мобильного устройства

В данном разделе представлено несколько вариантов реализации биометрических функций внутри ОС мобильного устройства на абстрактном уровне. Этот список не является исчерпывающим, и могут существовать другие реализации.

С учетом общей архитектуры ОС, показанной на рисунке 1, в настоящем разделе рассматривается, что БИ разработан на уровне низкоуровневых библиотек с прямым доступом к ядру ОС и, следовательно, перенаправлением первого уровня на аппаратное обеспечение через САА.

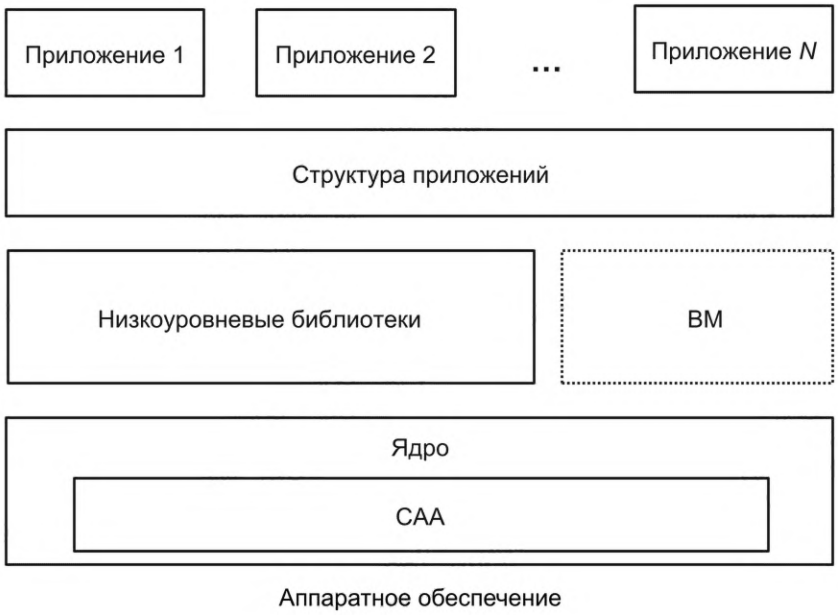


Рисунок 1 — Общая архитектура ОС мобильного устройства

Изготовитель ОС может предоставить БИ доступ ко всем ресурсам на оборудовании и предложить эти биометрические службы в структуре приложений, для того чтобы приложения могли использовать эти службы, вызывая соответствующий ПИП (см. рисунок 2).

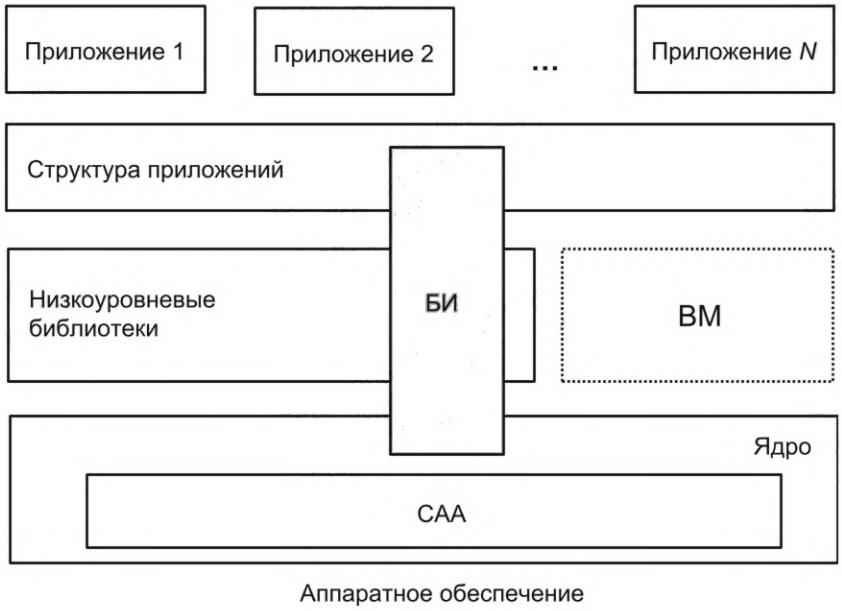


Рисунок 2 — Расположение БИ при разработке внутри ОС

В тех ОС, где имеется ВМ и изготовитель ОС готов предоставить службы БИ для приложений, выполняемых на ВМ, может быть установлена связь между ВМ и БИ.

Для обеспечения определенного уровня доверия БИ необходимо разрабатывать в изолированной программной среде («песочнице»), в которой другие службы не могут повлиять на реализацию БИ. Доступ к функциональности БИ должен быть обеспечен исключительно с помощью агрегированных функциональных методов, таких как:

- регистрация биометрического контрольного шаблона (т. е. биометрическая регистрация пользователя);
- верификация полученного биометрического образца с ранее сохраненным биометрическим контрольным шаблоном;
- идентификация полученного биометрического образца в наборе биометрических контрольных шаблонов, хранимых на устройстве;
- взаимодействие с пользователем через обратные вызовы (или аналогичные механизмы), которые предоставляют приложениям ГИП;
- обработка исключений как для системных ошибок, так и для пользовательских ошибок.

Изготовитель ОС может реализовать механизмы и политику обнаружения атак, и использование биометрической функциональности может быть заблокировано (временно или постоянно) при обнаружении атак.

Изготовитель ОС может предоставлять функциональность конфигурации, с помощью которой при использовании БИ выбирают различные параметры для определенных приложений и/или сценариев. Например, может быть обеспечено дискретное число уровней доверия с разными порогами (т. е. проверки качества, сравнения, обнаружения атаки на биометрическое предъявление и т. д.).

Изготовитель ОС для реализации БИ может создавать некоторые из следующих внутренних функций:

- сбор одного или нескольких биометрических образцов из последовательности образцов (т. е. изображение лица в реальном времени);
- создание наилучшего(их) биометрического(их) образца(ов) на основе некоторой метрики качества;
- предоставление показателя качества для сбора биометрического образца;
- предоставление информации о доступности датчиков на устройстве (например, камеры мультисенсорного экрана, сканера отпечатков пальцев, СГП, акселерометра и т. д.) с соответствующими техническими характеристиками (например, разрешение сенсорного экрана, количество мультисенсоров, разрешение камеры и т. д.);

- предоставление информации о том, какие биометрические модальности собраны в качестве контрольных шаблонов;
- алгоритмы сравнения для каждой модальности «один к одному» или «один ко многим».

Основными преимуществами данного подхода являются:

- использование машинного кода и отсутствие промежуточных уровней, которые могут приводить к потере производительности;
- прямой доступ ко всем доступным ЭБ устройства. Последнее преимущество особенно важно, так как создание ДСИ ОС может сделать двунаправленную выгоду между ДСИ и биометрическими службами.

С одной стороны, БИ может извлечь выгоду от выполнения в ДСИ и, следовательно, избежать многих потенциальных атак (в частности, атак «человек посередине»). БИ может извлечь выгоду из возможности использовать низкоуровневые ЭБ, которые могут надежно хранить биометрические контрольные шаблоны. С другой стороны, ДСИ может извлечь выгоду из того, что БИ имеет дополнительный механизм аутентификации пользователя, который больше опирается на данные пользователя, а не на то, что пользователь знает или что у пользователя есть.

7 Биометрические службы на уровне приложений в мобильных устройствах

В тех случаях, когда БИ не входит в ОС или существует потребность использования другого БИ в отличие от предоставляемого ОС (например, из-за использования другой модальности или большего доверия стороннему решению), БИ должен быть разработан на уровне приложения (см. рисунок 3). На рисунке 3 отражено, что БИ находится на одном уровне с остальными приложениями, но предоставляет общие службы, которые могут быть применены другими приложениями (например, от приложения *X* до приложения *Z*). Другие приложения на устройстве могут сосуществовать без использования БИ, такие как приложение 1 и приложение *N*, указанные на рисунке 3.

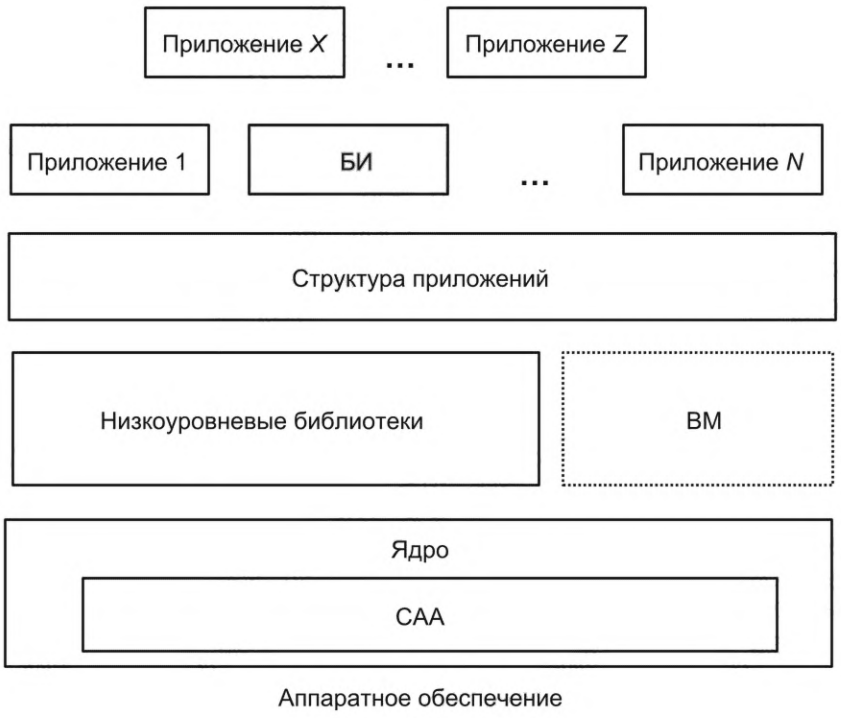


Рисунок 3 — Расположение БИ при разработке на уровне приложений

Рекомендации раздела 6 применимы для рассматриваемого варианта с изменением изготовителя ОС на изготовителя БИ в тех местах, где упомянут изготовитель ОС. В дополнение к этим рекомендациям применяют следующие:

а) ОС должна позволить структуре приложений создавать БИ в изолированной программной среде, которая запрещает доступ из других приложений к ее функциональности за пределами предоставленного общего интерфейса;

б) ОС должна допускать временный доступ к устройству сбора биометрических данных, относящемуся к аппаратному слою, поэтому в процессе сбора биометрических данных другое приложение или служба не может получить доступ ни к устройству, ни к памяти, зарезервированным для такого процесса.

Устройство сбора биометрических данных может быть внутренним или встроенным в устройство (например, сенсорный экран, микрофон и т. д.), или внешним через интерфейс связи (например, OTG, Bluetooth и т. д.);

в) как и в случае с устройством сбора биометрических данных, к модулю для хранения информации допустим только временный доступ при хранении или считывании биометрического контрольного шаблона. Рекомендуется, чтобы модуль для хранения позволял хранить информацию зашифрованным способом и с помощью внутренних механизмов аутентификации (например, включенных во многие смарт-карты).

При таком подходе сложнее создать ДСИ с использованием БИ, но если ОС предоставляет такие ДСИ, то рекомендуется, чтобы БИ был установлен внутри нее.

При разработке БИ в целом и для внедрения биометрических алгоритмов в частности рекомендуется использовать машинный код (по возможности), для того чтобы максимально сократить время выполнения биометрических операций.

8 Разработка биометрических приложений (с использованием биометрической библиотеки функций)

Несмотря на то, что изготовителем мобильных устройств или поставщиком ОС могут предлагаться коммерческие ПИП, рекомендуется использовать стандартизованные ПИП для обеспечения совместимости кодов и программ разработчиков и устранения необходимости адаптации биометрического решения к различным устройствам и приложениям.

Определение БИ представлено в разделах 6 и 7. Такой БИ должен быть связан со структурой приложений, которая может быть разработана в самой ОС или в стороннем приложении. В случае реализации структуры (см. [2]) в ОС структура должна обеспечить не только разработку БИ внутри ОС, но и службу на уровне приложений, предоставляемую третьей стороной, которая разделяет интерфейс исключительно со структурой, не открывая доступ к другим приложениям. Те приложения, которым необходимо использовать БИ, должны сделать запрос путем вызова структуры ПИП (см. [2]) (см. рисунок 4).

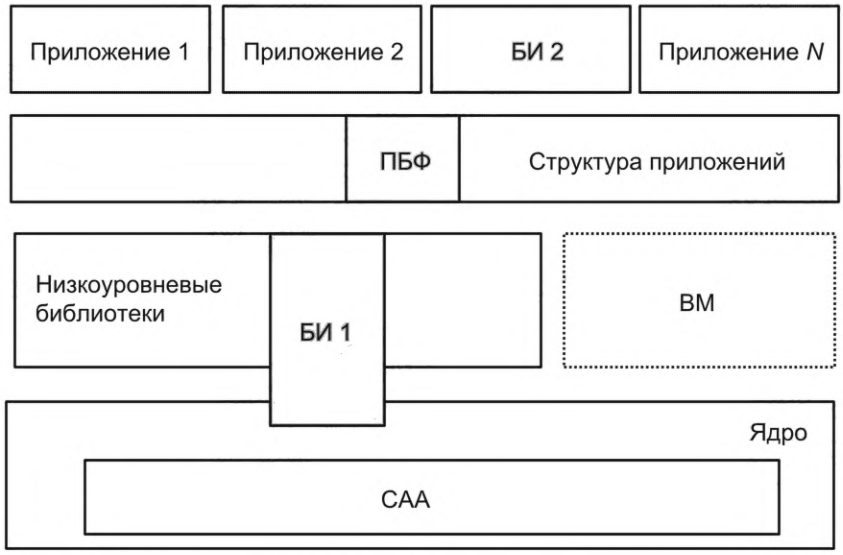


Рисунок 4 — Схема внедрения структуры (см. [2]) в ОС

В том случае, когда биометрическая структура не включена в ОС, один из способов реализации многоуровневой схемы представлен на рисунке 5.

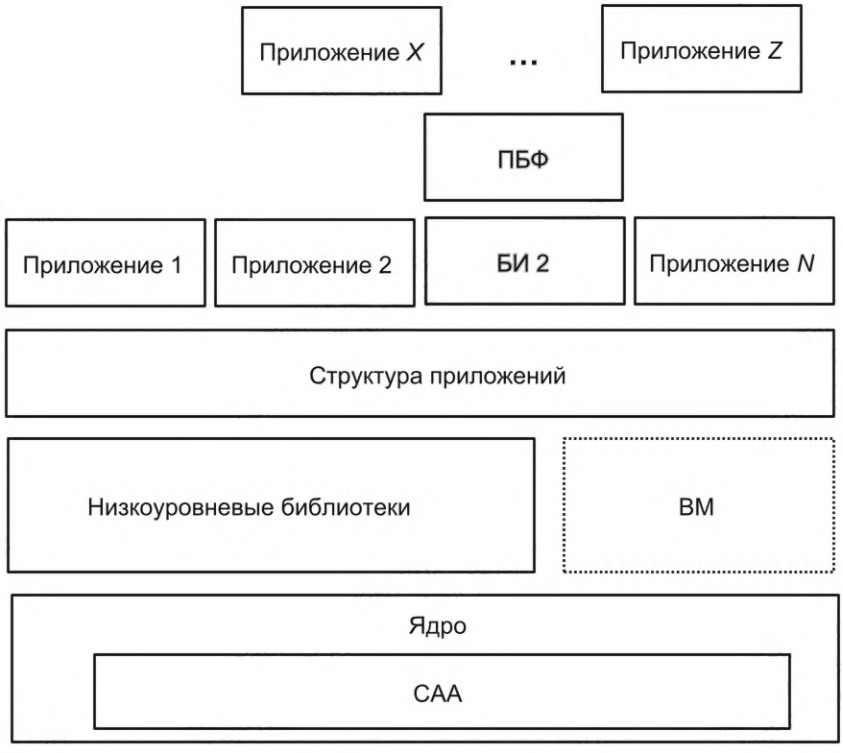


Рисунок 5 — Схема внедрения структуры (см. [2]) на уровне приложений

Важным вопросом является взаимодействие между БИ и приложением, в частности при взаимодействии с пользователем. Не рекомендуется, чтобы БИ самостоятельно обрабатывал процесс взаимодействия между пользователем и системой. Например, БИ с устройством сбора биометрических

данных может сопровождать все взаимодействия посредством отображения сообщений, освещения светодиодов и/или активации звуков на самом датчике. Такое взаимодействие может представлять обратную связь пользователю:

- о пальце, который необходимо поместить на датчик;
- о том, как именно улучшить положение образца в датчике (например, выравнивание биометрической характеристики по отношению к чувствительной области датчика);
- о том, было ли получение данных проведено корректно;
- о положительном или отрицательном результате биометрического сравнения.

В большинстве случаев может потребоваться, чтобы такое взаимодействие обрабатывалось приложением с использованием БИ и отображением всех сообщений и иллюстраций на экране устройства для того, чтобы избежать обращения с самим БИ и появления недостатков, таких как:

- ГИП БИ может быть не адаптирован к различным размерам и разрешениям, которые использует экран приложения;
- предоставленная обратная связь должна соответствовать виду и поведению основного приложения, включая использование логотипов поставщика службы;
- обратная связь должна быть адаптирована к языку идентифицируемого пользователя или к развертыванию системы.

Способом решения указанных проблем является использование функций обратного вызова. Функции обратного вызова должны быть разработаны для каждого этапа, на котором БИ требует взаимодействия с пользователем, и для каждого из вызываемых процессов. Приложение обеспечивает БИ выбранными функциями, так что БИ может вызывать их при обработке. Если БИ позволяет использовать функции обратного вызова для управления ГИП, необходимо предпринять определенные действия для проведения каждого процесса, требующего осуществления такого взаимодействия (например, сбора биометрических данных).

Приложение должно реализовать все связанные с ГИП функции соответствующего процесса. Эти функции включают:

- выбор функции для указания начала или конца процесса взаимодействия с пользователем. Поэтому должно быть определено, вызывается ли функция обратного вызова в начале или в конце процесса. Функция обратного вызова также может предоставить БИ информацию о действии пользователя, например отмену сбора данных. Информационный поток передается через параметры функции обратного вызова;
- функцию состояния. Иногда процесс БИ может включать несколько внутренних этапов, которые могут быть сконструированы как разные состояния. Функция состояния обеспечивает обратную связь относительно того, должен ли быть запущен или закончен определенный внутренний этап. Соответственно, должно быть определено, какой внутренний шаг обрабатывается, и эта информация будет предоставляться в качестве параметров функции обратного вызова. Через параметры также передается обратная связь от пользователя, такая как отмена всего процесса;
- функцию выполнения. В некоторых случаях может потребоваться предоставить пользователю обратную связь о ходе процесса в реальном времени. Например, система может отображать на экране изображение отпечатка или лица в реальном времени во время сбора. Для отображения потока данных может быть использована функция обратного вызова индикации прогресса.

После реализации функций обратного вызова для процесса приложение должно сообщить БИ перед вызовом процесса о функциях обратного вызова, которые будут использованы. Это осуществляется путем подписания БИ для выбранных событий ГИП и соответствующих функций обратного вызова. После подписания приложение может вызвать процесс (например, сбор биометрических данных). При завершении процесса приложение может отменить подписку на БИ из ранее подписанных событий.

Разработчик приложения должен знать об операциях и свойствах, которые БИ-компоненты включили в предложение приложения, для того чтобы знать, какой из методов следует вызывать. Разработчик приложения также должен проверить исключения, возникающие при любом вызове любого метода, и доступность вызываемой функциональности в этом БИ или наличие/отсутствие другой ошибки. Для упрощения кода приложения рекомендуется, чтобы разработчик приложения использовал методы высокого уровня, например методы, в которых все биометрические данные обрабатываются в БИ и не распространяются через приложение.

9 Руководство по функциональности и оперативной работе

9.1 Общее руководство

9.1.1 Руководство по функциональной архитектуре

При наличии большого числа функциональных архитектур настоящий стандарт ограничивается следующими ключевыми аспектами:

а) регистрация субъекта данных проводится только один раз приложением для каждого устройства (например, на ноутбуке, планшете и смартфоне);

б) биометрический контрольный шаблон хранится локально на устройстве;

в) аутентификация проводится локально на устройстве;

г) требования настоящего стандарта ограничены архитектурами, поддерживающими аутентификацию «один к одному» и распознавание «один ко многим»;

д) сбор может проводиться с помощью устройства, а также посредством физически или логически привязанного датчика.

9.1.2 Руководство по условиям и ограничениям окружающей среды

В подавляющем большинстве «фиксированных» биометрических приложений регистрация и верификация субъекта происходят в контролируемой среде, в которой освещение, температура, влажность, фоновый шум и т. д. могут быть оптимизированы для увеличения вероятности получения высококачественного биометрического образца.

Мобильные устройства, оборудованные биометрией, будут использованы в разных средах и условиях: в помещении и на улице, днем и ночью, при ярком солнечном освещении и в пасмурную погоду, под дождем, снегом и т. д., и пользователь (заплатив за такое устройство и зарегистрировав свои биометрические данные) во всех случаях будет ожидать корректной работы устройства.

Влияние факторов окружающей среды будет меняться в зависимости от модальности; яркий солнечный свет может неблагоприятно влиять на системы по изображению лица, радужной оболочке глаза и отпечаткам пальцев, в то время как высокий уровень фонового шума повлияет на устройства с распознаванием голоса.

Дополнительная информация приведена в разделе 11.

9.2 Руководство по регистрации

Несмотря на то что мобильные устройства все чаще включают такие биометрические возможности, как датчик отпечатков пальцев, камера для распознавания лица или распознавание радужной оболочки глаза, гарантии относительно того, что пользователи будут следовать инструкциям изготовителя о том, как они должны быть использованы, не существует.

Однако в случае использования биометрии на мобильных устройствах пользователи обязательно экспериментируют, для того чтобы понять, что будет принято. Например, они могут пробовать использовать различные выражения лица, ориентировать камеру на ухо или другие части тела, использовать сторону или кончик пальца, а не плоскую часть, и т. д. Пользователи могут воспользоваться искусственными биометрическими данными, пытаясь поместить неодушевленный предмет на датчик отпечатков пальцев или направить камеру на изображение лица. Такие попытки будут успешными или неуспешными в зависимости от того, как встроен датчик и какие пороги качества установлены.

Для приложений с низким уровнем безопасности, таких как разблокировка устройств, основной задачей будет являться не совместимость, а воспроизводимость. Независимо от того, следует ли пользователь указаниям изготовителя по регистрации выбранной биометрической модальности, более важным вопросом является, возможно ли надежно повторить процесс при последующей верификации/аутентификации (вероятно, на нескольких устройствах и в нескольких средах).

Распознавание подписи является хорошим примером регистрации, так как не требуется, чтобы человек использовал свою обычную подпись в биометрическом приложении. Имеет значение то, что при биометрической регистрации должна быть обеспечена достаточная детализация для индивидуализации шаблона, и образец должен быть воспроизведен при последующей верификации.

Тем не менее необходимость точно воспроизводить конкретный жест или выражение лица для их распознавания системой в последующем может быть не очевидна для пользователей, незнакомых с биометрическими технологиями.

Использование неконтролируемой биометрической регистрации на мобильных устройствах также влияет на существующие показатели качества биометрических данных, и, возможно, потребуются но-

вые алгоритмы проверки качества. Например, следует в большей степени учитывать сложность (и, следовательно, уникальность) представленного образца, а также степень, с которой пользователь сможет воспроизводить его в различных средах и на разных устройствах, в отличие от обычных проверок биометрического качества, разработанных для поддержки совместимости.

9.3 Руководство по аутентификации

В мобильном устройстве выполнена локальная неконтролируемая аутентификация. Особенности локальной неконтролируемой аутентификации совпадают с особенностями удаленной аутентификации, за исключением того, что биометрическая информация не передается на сервер. Это ослабляет требования безопасности с точки зрения передачи биометрической информации, но фокусирует внимание на том, как именно биометрическая информация хранится и используется в мобильном устройстве, а также на требованиях к приложениям, установленным на устройстве, для использования биометрических служб.

Не допускается доступ к биометрическим данным. Биометрические шаблоны должны храниться в ЭБ, а использование биометрических служб (например, регистрация, верификация и/или идентификация) должно проходить в ДСИ.

Биометрическая служба должна учитывать потенциальные атаки. По меньшей мере, должен быть использован механизм подсчета числа неудачных попыток верификации, при котором биометрическая служба блокируется, по крайней мере, для приложения, вызывающего эту службу.

Должны быть проведены оценка качества полученных образцов и отклонение образцов, если их качество не превышает определенный порог. При возможности следует добавить механизмы обнаружения атаки на биометрическое предъявление во избежание атак, таких как спуфинг.

10 Использование мультифакторной аутентификации

10.1 Объединение и результаты сравнения в мультибиометрии

Современное мобильное и непрофессиональное оборудование содержит ряд датчиков, которые могут поддерживать оценку нескольких биометрических модальностей. Датчики и алгоритмы, скорее всего, показывают более низкие уровни надежности результатов в индивидуальном режиме. В сложившихся обстоятельствах наиболее вероятным представляется вариант, при котором общий уровень надежности может быть повышен за счет определенного объединения модальностей. Важно, что простое объединение байесовских процедур «И» может оказаться неподходящим и что будет необходимо «ИЛИ». Такие сценарии требуют более глубокого понимания результатов сравнения и механизма их получения в каждом режиме датчика. Любые мероприятия по стандартизации должны касаться вопросов измерения и предоставления уровней надежности и результатов сравнения.

В биометрических алгоритмах традиционно использовалась одна модальность для верификации или идентификации человека (например, в алгоритмах распознавания речи используют запись голоса, в алгоритмах распознавания лица — изображение лица). В некоторых ситуациях, в частности в средах с высоким уровнем шумов, одна модальность может не обеспечить требуемый уровень надежности, и для его повышения предложены алгоритмы объединения.

В примере со слиянием распознавания голоса и лица в среде с высоким уровнем шумов объединение «ИЛИ» результативно отклоняет компонент распознавания голоса в шумной среде или компонент распознавания лиц в среде с плохими условиями освещения (например, слишком темными). Объединение «ИЛИ» уменьшает вероятность ложного недопуска, но увеличивает вероятность ложного допуска из-за увеличения вероятностей ложного недопуска обеих модальностей.

Объединение «И» увеличивает вероятность ложного недопуска. В примере с распознаванием голоса и лица шум или плохие условия освещения приведут к недопуску. Однако вероятность ложного допуска существенно сокращается, потому что злоумышленник должен быть верифицирован обеими модальностями.

Что касается атаки на биометрическое предъявление, то объединение «И» не повышает в значительной мере уровень безопасности, потому что обе модальности могут быть подделаны независимо друг от друга. Например, в примере с распознаванием голоса и лица злоумышленник может представить изображение или последовательность изображений для обмана модальности лица и запись голоса для обмана модальности голоса. Без сопоставления изображения (последовательности изображений) с записью голоса результат атаки является суммой результатов отдельных атак.

Противодействие атакам на биометрическое предъявление может быть повышено с помощью корреляции записи голоса и изображения лица (последовательности изображений). Корреляция может быть достигнута с помощью различных классов алгоритмов объединения, которые комбинированно работают с входным сигналом в отличие от итоговых результатов сравнения отдельных модальностей.

Дополнительная информация о мультимодальном и другом мультибиометрическом объединении представлена в ГОСТ Р 54411.

10.2 Объединение биометрического распознавания и небиометрических методов аутентификации для повышения уровня безопасности и/или удобства использования

Коммерческие мобильные устройства могут включать в себя датчики, такие как микрофоны, сенсорные экраны и камеры, или использовать периферийные биометрические датчики. С помощью таких датчиков можно проводить аутентификацию с использованием биометрических модальностей, включая голос, подпись, лицо, отпечаток пальца, радужную оболочку глаза и сосудистое русло. Требуются указания, позволяет ли применение нескольких биометрических модальностей повысить уровень безопасности или удобство использования.

Помимо мультибиометрических коммерческих мобильных устройств существуют другие датчики, которые могут быть использованы дополнительно к биометрическому распознаванию для обеспечения дополнительных уровней безопасности, например служба СГП или другие службы определения местоположения (в частности, местоположение ячейки телефонной сети или распознавание опознавательных объектов с помощью датчика камеры). Клавиатура также может быть использована для ввода дополнительных паролей, ПИН-кодов, других секретных или персональных данных для повышения уровня безопасности аутентификации.

Микрофон и распознавание голоса могут применяться для ввода дополнительных паролей, ПИН-кодов, других секретных или персональных данных.

При наличии акселерометров могут быть использованы движения жестикуляции в сравнении с ранее записанными движениями.

Необходимо определение того, как дополнительные датчики могут повысить уровень безопасности аутентификации или удобства использования.

11 Руководство по биометрическим модальностям

Удобство использования каждой биометрической модальности зависит от условий окружающей среды, например улицы, помещения, офиса, конференц-зала, вагона поезда или салона автомобиля.

Удобство использования зависит от цели и сценария, описанных в разделе 8, например блокировки, отображения почты, платежа, менеджера паролей, одного входа или разблокировки КБП.

Некоторые факторы окружающей среды могут ограничить сбор биометрических данных, так как освещение, шум, вибрация, температура, влажность влияют на удобство использования. Некоторые типы мобильных устройств, например телефоны и смартфоны, могут создавать дополнительные ограничения ввиду ожиданий операций, выполняемых одной рукой. Пользователи телефонов могут предоставлять свои отпечатки пальцев для разблокировки КБП в точке транзакции, не глядя на экран мобильного устройства, которое может находиться в кармане или сумке (см. 5.2.3).

В ГОСТ Р ИСО/МЭК ТО 19795-3 представлены примеры основных факторов влияния для каждой модальности, в том числе условий окружающей среды. В таблице 1 приведены примеры того, каким образом различные условия могут неблагоприятно влиять на различные модальности.

Таблица 1 — Примеры условий окружающей среды

Модальность	Фактор окружающей среды, влияющий на эксплуатационные характеристики
Лицо	Освещение: - основная освещенность (слишком светло/слишком темно); - направленное освещение (приводящее к теням на лице). Выражение лица субъекта.

Окончание таблицы 1

Модальность	Фактор окружающей среды, влияющий на эксплуатационные характеристики
Лицо	Положение головы субъекта. Использование макияжа и/или аксессуаров (шляпа, шарф, солнцезащитные очки и т. д.). Неконтролируемый и сложный фон. Быстрые изменения температуры и влажности, вызывающие конденсацию на объективе. Движение субъекта
Палец (оптические устройства)	Освещение: - прямое освещение, которое может влиять на производительность биометрического сканера. Температура и влажность могут приводить к чрезмерно сухой или чрезмерно влажной коже, усложняя сбор отпечатка пальца. Пыльная или загрязненная окружающая среда и субъекты, задействованные в ручной работе (например, строители), могут приводить: - к загрязнению рабочей поверхности биометрического сканера; - загрязнению пальцев и стиранию папиллярного узора. Быстрые изменения температуры и влажности, вызывающие конденсацию на объективе и/или рабочей поверхности биометрического сканера
Сосудистое русло	Положение. Поверхность руки: - загрязненная кожа; - перчатки или рукава
Голос	Основной уровень шума (очень тихо/очень шумно): - может влиять на то, как субъект разговаривает; - шумные условия среды делают трудным разделение голоса субъекта и фонового шума. Ветер может приводить к помехам у микрофона
Радужная оболочка глаза	Освещение: - основная освещенность (слишком светло/слишком темно); - расширение зрачка может отличаться в моменты регистрации и аутентификации, что приведет к низкой равномерности расширения. Аксессуары — очки/солнцезащитные очки/контактные линзы. Быстрые изменения температуры и влажности, вызывающие конденсацию на объективе. Движение субъекта или сенсорной платформы (например, движение поезда, судна или самолета)
Подпись	Температура: - очень низкая температура может осложнить воспроизведение подписи при регистрации; - субъект может быть в перчатках, создающих сложность при подписи. Движение субъекта или сенсорной платформы (например, движение поезда, судна или самолета)

Шумная и/или чрезмерно освещенная окружающая среда может помешать пользователю увидеть или услышать инструкции и обеспечить обратную связь (например, сильнее нажать на сканер отпечатков пальцев, отодвинуться назад от камеры и т. д.), что также оказывает влияние на удобство использования и эксплуатационные характеристики системы.

Библиография

[1] Derawi M.O., Gafurov D., Larsen R., Busch C., Bours P. Fusion of gait and fingerprint for user authentication on mobile devices, 2nd International Workshop on Security and Communication Networks (IWSCN), pp.1,6, 26—28 May 2010. doi: 10.1109/IWSCN.2010.5497989

[2] ИСО/МЭК 30106 (все части) Information technology — Object oriented BioAPI (Информационная технология. Объектно-ориентированный BioAPI)

УДК 004.931:006.89:006.354 ОКС 35.040

Ключевые слова: информационные технологии, мобильные устройства, биометрия в мобильных устройствах, устройства сбора биометрических данных, биометрический интерфейс

Редактор *Н.В. Таланова*
Технический редактор *И.Е. Черепкова*
Корректор *М.И. Першина*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 28.01.2026. Подписано в печать 20.02.2026. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 2,79. Уч.-изд. л. 2,37.

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