ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПНСТ 379— 2019 (ISO/IEC TR 30125:2016)

Информационные технологии

БИОМЕТРИЯ

Применение биометрии в мобильных устройствах

(ISO/IEC TR 30125:2016, Information technology — Biometrics used with mobile devices, MOD)

Издание официальное

Москва
Стандартинформ
2020

Предисловие

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

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 19 декабря 2019 г. № 56-пнст

4 Настоящий стандарт является модифицированным по отношению к международному документу ISO/IEC TR 30125:2016 «Информационные технологии. Применение биометрии в мобильных устройствах» (ISO/IEC TR 30125:2016 «Information technology — Biometrics used with mobile devices», MOD) путем изменения отдельных фраз (слов, значений показателей, ссылок), которые выделены в тексте курсивом. Внесение указанных технических отклонений направлено на учет потребностей национальной экономики Российской Федерации.

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

Сведения о соответствии ссылочного межгосударственного стандарта международному стандарту, использованному в качестве ссылочного в примененном международном документе, приведены в дополнительном приложении ДА.

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

5 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 и проведения его мониторинга установлены в ГОСТ Р 1.16—2011 (разделы 5 и 6).

Федеральное агентство по техническому регулированию и метрологии собирает сведения о практическом применении настоящего стандарта. Данные сведения, а также замечания и предложения по содержанию стандарта можно направить не позднее чем за 4 мес до истечения срока его действия разработчику настоящего стандарта по адресу: 107045, Москва, Сретенский тупик, д. 3, стр. 1, e-mail: standards@rusbiometrics.com и/или в Федеральное агентство по техническому регулированию и метрологии по адресу: 109074 Москва, Китайгородский проезд, д. 7, стр. 1.

В случае отмены настоящего стандарта соответствующая информация будет опубликована в ежемесячном информационном указателе «Национальные стандарты» и также будет размещена на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

Введение

Широкое использование и возможности мобильных технологий сформировали потребность людей вести свою личную и деловую жизнь в движении, хотя раньше она была ограничена домашней и офисной средой. Для удовлетворения данной потребности мобильная связь, приложения, установленные на мобильные устройства, и транзакции должны быть защищены для обеспечения конфиденциальности пользователя и целостности транзакций. Это необходимо для создания доверенной среды мобильных платформ, в которой могут участвовать как отдельные лица, так и предприятия, некоммерческие организации и правительства. Аутентификация пользователя, удостоверяющая его личность, является важной частью создания этой среды и создает определенные проблемы в том случае, когда пользователь осуществляет аутентификацию удаленно и его местоположение неизвестно, так как при этом высока вероятность имитации и мошенничества.

Аутентификацию пользователя часто проводят с использованием имени пользователя и пароля. При таком подходе применяют только одну категорию учетных данных — пароль и данную аутентификацию называют однофакторной аутентификацией (ОфА)*. Примером ОфА также является использование биометрии вместо пароля. В концепции мобильных приложений с высоким уровнем безопасности может потребоваться несколько категорий учетных данных. Применение более одной категории учетных данных называется многофакторной аутентификацией (МфА)**. МфА выполняют с использованием одного или нескольких факторов:

a) то, что знают (например, пароль);

b) то, чем владеют (например, удостоверение личности);

c) то, что является физиологической характеристикой (например, лицо, отпечатки пальцев, радужная оболочка глаза).

Аутентификация, удостоверяющая личность человека, может быть улучшена с помощью биометрического распознавания. Другие формы идентификации, такие как токены или пароли, не связаны с индивидом так же неотъемлемо, как биометрия, и имеют большую вероятность замещения или кражи. Аутентификация пароля и токена удостоверяет пароль или токен, а не владельца, и проверка подлинности ограничена уровнем доверия в отношении того, что пароль или токен предоставляется законным пользователем и не был получен злоумышленником.

Диапазон мобильных устройств и каналов связи, связанных с мобильными транзакциями, является большим и изменчивым. Широко распространенными мобильными устройствами являются смартфоны, планшеты, ноутбуки и другие интеллектуальные устройства на основе встроенных систем, а примерами каналов связи являются Интернет и глобальная система для мобильной связи (ГСМС)***. Владельцами мобильных устройств часто являются пользователи, но не во всех случаях; мобильные устройства могут принадлежать компании и предоставляться сотрудникам для использования.

Ряд производителей мобильных устройств производит устройства, содержащие устройства сбора различных данных. Теоретически такие устройства сбора могут быть использованы для сбора биометрических данных [например, камера для лица, сенсорный экран для пальца или ладони, микрофон для голоса, система глобального позиционирования (СГП) и акселерометры для походки]. Приложения, созданные для мобильных платформ, могут применять такие устройства для сбора биометрических данных в целях аутентификации.

Настоящий стандарт определяет использование биометрии в тех сценариях, в которых человек использует мобильное устройство для подключения к конкретной службе независимо от типа мобильного устройства и канала связи.

При использовании биометрии в указанных сценариях необходимо учитывать три ключевых фактора:

- условия окружающей среды сбора биометрических данных, при которых разработчикам приложений необходимы способы учета неконтролируемых условий окружающей среды сбора биометрических данных. Неконтролируемость условий окружающей среды сбора биометрических данных будет означать невозможность соответствия рекомендациям действующих биометрических стандартов для сбора биометрических данных (например, положение, фон и т. д.), а также повлечет за собой модифи-

---

* Single Factor Authentification (SFA).

** Multi Factor Authentification (MFA).

*** *Global System for Mobile Communications (GSM).*

кацию алгоритмов распознавания и/или порогов для учета снижения качества сбора биометрических данных, если приложение позволяет понизить уровень безопасности;

- конфиденциальность биометрических данных и последствия нарушения безопасности — размещение биометрических данных на коммерческих мобильных устройствах с уязвимостями безопасности и хранение биометрических данных в сторонних облачных реализациях. В настоящем стандарте указанные вопросы безопасности и конфиденциальности относятся к требованиям других стандартов, при их наличии, при этом продолжается работа в установлении критериев и рекомендаций для защиты информации, включая личную информацию. Определение требований безопасности для мобильных устройств не входит в область применения настоящего стандарта;

- биометрическое распознавание, что подразумевает относительную согласованность подхода к биометрическому распознаванию среди разработчиков приложений для соответствия рекомендациям и унифицированному интерфейсу для пользователей [*1*]. Существующие биометрические стандарты и соответствующие стандарты безопасности для биометрии недостаточно исчерпывающе решают вопросы сбора биометрических данных на коммерческих вычислительных мобильных устройствах с облачным распределением биометрических данных, поэтому необходима работа для установления критериев и рекомендаций.

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

БИОМЕТРИЯ

Применение биометрии в мобильных устройствах

Information technology. Biometrics. Biometrics used with mobile devices

Срок действия — с 2020—06—01
до 2023—06—01

1 Область применения

Настоящий стандарт определяет руководство по разработке последовательного и безопасного метода биометрической (отдельной или с наличием небиометрического компонента) персонализации и аутентификации в мобильной среде для систем, представленных на свободном рынке.

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 *международных и национальных стандартов* к форматам обмена биометрическими данными и качеству биометрических образцов;
- оптимального использования мультифакторных методов биометрической и небиометрической (ПИН-коды, пароли, персональные данные) персонализации и аутентификации.

Настоящий стандарт определяет структуру методов и подходов к удаленной и неконтролируемой биометрической регистрации, безопасному хранению и передаче биометрических и дополнительных персональных данных как в онлайн-режиме, так и в автономном режиме.

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.

В настоящем стандарте определены: a) пользователь мобильного устройства и b) работа на различных платформах, в частности мобильных устройствах, включая планшет, ноутбук и другие персональные вычислительные устройства. Контекст связан с тем, контролируется ли физически среда пользователя организацией, к которой пользователь запрашивает доступ.

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 Информационные технологии. Биометрия. Мультимодальные и другие мультибиометрические технологии

ГОСТ Р 58230 Информационные технологии. Идентификационные карты. Биометрическое сравнение на идентификационной карте

Издание официальное

ГОСТ Р 58292 (ИСО/МЭК 19795-2:2007) Информационные технологии. Биометрия. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 2. Методы проведения технологического и сценарного испытаний

ГОСТ Р 58295 (ИСО/МЭК 19794-6:2011) Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза

ГОСТ Р 58298 (ИСО/МЭК 19794-4:2011) Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальца

ГОСТ Р 58624 Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление

ГОСТ Р 58668.8 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 8. Данные изображения сосудистого русла

ГОСТ Р 58668.11 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 11. Данные голоса

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

ГОСТ Р ИСО/МЭК 19794-2 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца — контрольные точки

ГОСТ Р ИСО/МЭК 19794-5 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица

ГОСТ Р ИСО/МЭК 19794-7 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 7. Данные динамики подписи

ГОСТ Р ИСО/МЭК 19794-11 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 11. Обрабатываемые данные динамики подписи

ГОСТ Р ИСО/МЭК 29794-1 Информационные технологии. Биометрия. Качество биометрического образца. Часть 1. Структура

ГОСТ Р ИСО/МЭК 29794-6 Информационные технологии. Биометрия. Качество биометрического образца. Часть 6. Данные изображения радужной оболочки глаз

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

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): Небольшое, компактное, портативное, легкое 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** (personalization): Возможность настройки устройства реагировать определенным образом для 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);

САА — слой аппаратных абстракций;

СГП — система глобального позиционирования (Global positioning system, GPS);

ОИ — окупаемость инвестиций;

ОС — операционная система (Operating system, OS);

ПБФ — поставщик биометрической функции;

ПИП — прикладной интерфейс приложений;

ЭБ — элемент безопасности (Secure element, SE);

OTG — спецификация USB OTG* (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 на четыре варианта. Во всех вариантах удобство использования и человеческий фактор должны быть учтены и интегрированы в процесс разработки приложения с применением возможностей биометрии.

5.1.2 Общие положения для всех случаев использования

Необходимо учитывать уровень доверия, необходимый операторам и пользователям служб в мобильной среде. Он будет зависеть от характера служб и факторов окружающей среды, таких как местоположение, степень удаленного управления (при наличии), время, криптографические и другие процессы обеспечения безопасности. Анализ уровней безопасности и доверия выходит за рамки настоящего стандарта, поэтому в соответствующих разделах настоящего стандарта приведены высокий, средний и низкий уровни доверия со ссылкой на определяющие стандарты. Более подробная информация представлена в [2].

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

a) сбор биометрического образца;

b) хранение биометрического контрольного шаблона (в некоторых случаях удаленное от мобильного устройства);

c) обработка биометрических образцов;

d) сравнение биометрического образца с биометрическим контрольным шаблоном (который может быть удален от мобильного устройства).

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

a) сбор одного биометрического образца или более из последовательности образцов (т. е. изображение лица с изображения лица в реальном режиме);

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

c) обеспечение обратной связи передающей(ему) стороне/субъекту для предъявления биометрических характеристик (например, демонстрация овальной формы для позиционирования лица);

d) предоставление показателя качества для сбора биометрического образца;

---

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

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

f) предоставление информации о доступности устройств сбора на мобильном 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.);

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

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

i) получение результата сравнения или ошибки.

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

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

b) возможность обработки исключений;

c) обработка биометрических образцов.

Указанные функции могут быть частью структуры ОС. Необходимо учитывать, какие элементы могут находиться на мобильном устройстве и какие данные могут обрабатываться удаленно [например, через веб-службу Representable State Transfer, REST (передача репрезентативного состояния), Hypertext Transfer Protocol Group Encrypted Transfer, HTTP GET (протокол передачи гипертекста множественной зашифрованной передачи), Extensible Markup Language — Remote Procedure Call, XML-RPC (расширяемый язык разметки — вызов удаленных процедур и т. д.). В разных обстоятельствах могут быть использованы различные подходы даже для одного и того же приложения. Устройство может быть как подключено, так и не подключено. На уровне платформы пользователь должен видеть совместимость интерфейса.

Биометрическое сравнение может быть проведено в мобильном устройстве или передано на удаленный сервер в зависимости от варианта использования и требуемого уровня доверия.

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.

Также на различных интерфейсах системных компонентов может быть применена удаленная обработка. Это не только улучшит интероперабельность, но и позволит использовать биометрические возможности в тех системах, которые в противном случае были бы недоступны. Например, служба сбора данных, такая как WS-Biometric Devices (веб-сервисы — биометрические устройства), позволит мобильному устройству без встроенного сканера отпечатков пальцев получать отпечатки пальцев с использованием доступного сканера. Стандартный веб-сервис, такой как BIAS (услуги по подтверждению биометрической идентичности) может сделать то же самое для биометрической регистрации или биометрического распознавания, например в тех случаях, когда данные или возможности сравнения недоступны локально.

5.1.2.4 Для всех случаев необходимо учитывать следующие факторы:

a) 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 (например, согласно *серии стандартов ГОСТ Р ИСО/МЭК 29794*), и, при сборе нескольких биометрических образцов, полнота набора биометрических образцов;

b) для защиты персональных данных пользователя мобильного 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);

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

d) предполагается, что вычислительная мощность мобильного устройства менее вычислительной мощности настольного компьютера или сервера. В связи с чем рекомендуется анализировать произво-

дительность биометрической обработки мобильного устройства с учетом его ресурсов. Также следует проводить анализ эксплуатационных характеристик любого устройства сбора биометрических данных, встроенных в мобильное устройство, так как характеристики встроенного устройства сбора биометрических данных слабее характеристик эквивалентного специализированного автономного устройства сбора биометрических данных;

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

5.1.3 Доступ к мобильному устройству

Доступ к мобильному устройству является локальной службой мобильного устройства без необходимости использования онлайн-служб. Как правило, решение принимается на самом мобильном устройстве, и положительный результат приводит к разблокировке мобильного устройства и позволяет пользователю получить доступ к остальным сервисам и приложениям, установленным на мобильном устройстве или доступным удаленно.

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

Эта служба обеспечивает минимальный уровень доверия к мобильному устройству и содержащимся данным и приложениям. Приложения и доступ к отдельным данным могут потребовать дополнительную аутентификацию, которая повысит уровень доверия. Так как пользователю мобильного устройства может понадобиться доступ к службам с низким уровнем доверия (например, чтение новостей в общественной газете), механизм разблокировки мобильного устройств должен способствовать в большей степени удобству, чем безопасности, и, следовательно, уровень доверия для данного вида использования следует считать низким. Организация, предоставляющая мобильное устройство, может рассмотреть возможность повышения уровня доверия при необходимости обеспечения более строгого контроля использования мобильного устройства.

Для удобства пользователей в сценариях с низким уровнем доверия после фиксированного количества неудачных попыток мобильное 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 мобильного устройства без необходимости применения онлайн-служб. Как правило, решение принимается на самом мобильном 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 мобильном устройстве и только приложением, доступным на главном экране во избежание несанкционированного доступа сторонними приложениями или службами.

Пример — Доступ к защищенной папке во внутренней памяти мобильного 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 производитель биометрических служб не предоставляет разные уровни доверия и имеет фиксированные пороги.

5.1.5 Доступ к каналу связи

Доступ к каналу связи является онлайн-режимом функции, аналогичной 5.1.4, но где служба или данные, к которым запрашивается доступ, расположены в удаленной системе. Проводится попытка

мобильного устройства соединиться в онлайн-режиме и открыть канал связи для аутентификации в цифровом виде и регистрации на этом канале до получения доступа. Для аутентификации пользователя может быть использовано биометрическое распознавание.

Пример — Проверка оператором/владельцем канала того, что конкретный пользователь имеет право использовать конкретный канал связи для автоматической реализации порядка выставления счетов, кредитов и доступа.

Варианты доступа к каналу связи включают:

a) локальную биометрическую аутентификацию, реализованную через указанный механизм в виде токен-аутентификации, которой доверяет канал связи;

b) биометрический токен, который предъявляется локально и удаленно аутентифицируется системой контроля доступа к каналу связи;

c) биометрический образец, который отправляется в удаленную систему, контролирующую доступ к каналу связи, для обработки и аутентификации удаленно по зарегистрированной базе данных пользователей;

d) интегрированные системы, в которых объединены данные из более чем одного доверенного источника.

При разработке доступа к каналу связи следует учитывать такие же факторы, как и в 5.1.3, и, кроме того, следующие:

- режим идентификации или режим верификации — процессы, которые могут быть необходимы для идентификационной заявки, например идентификатора мобильного устройства, такого как International Mobile Station Equipment Identity, IMEI (международный идентификатор мобильного оборудования) или персональный идентификатор из данных, хранящихся на мобильном устройстве;
- время проверки аутентификации для канала связи.

5.1.6 Аутентификация удаленного ресурса или точки транзакции

Данная служба является онлайн-службой, которая может предоставлять функциональность процессов, описанных в 5.1.4, но при этом владелец/контролер удаленного объекта считает несущественным тот факт, что канал связи аутентифицирован.

Пример — Такие ситуации, при которых канал связи не был аутентифицирован с использованием биометрии и требования политики доступа и уровней доверия отличаются от требований поставщика канала связи. Как правило, подобная ситуация возникает тогда, когда канал связи обеспечивает передачу услуги Virtual Private Network, VPN (виртуальной частной сети).

Уровень безопасности канала связи может быть уменьшен с течением времени, поэтому обмениваемая биометрическая информация при ее наличии должна быть дополнительно защищена по протоколу связи.

5.2 Общие задачи интеграции биометрии в мобильные устройства

5.2.1 Вычислительная мощность

Недостаток вычислительной мощности мобильных устройств ранее был одной из причин нецелесообразности интеграции нескольких биометрических модальностей. В настоящее время после появления нового поколения 32-разрядных микропроцессоров с низким потреблением энергии задача изменилась. В частности, если при обработке биометрической информации внутри мобильного устройства потребуются вычисления, то это может произойти только в случае сравнения «один к одному» (например, биометрического образца с биометрическим контрольным шаблоном, хранимым на мобильном устройстве) или «один ко многим», если на мобильном устройстве хранятся несколько биометрических контрольных шаблонов, относящихся к разным пользователям. Сравнение «один ко многим» может быть выполнено непосредственно на мобильном устройстве, но с большей вероятностью будет выполнено на центральном сервере с использованием биометрического образца, полученного через мобильное устройство.

Получение биометрического образца и извлечение биометрических признаков могут занимать значительно более продолжительное время, чем биометрическое сравнение, особенно в варианте «один к одному». Кроме того, реализации для некоторых биометрических модальностей могут кодировать и сравнивать признаки из каждого доступного кадра, поэтому следует рассмотреть необходимость извлечения биометрических признаков и биометрического сравнения в режиме реального времени.

Примеры успешно реализованных биометрических модальностей в мобильных устройствах включают: отпечаток пальца [*3*], радужную оболочку глаза [*4*], лицо [*5*], ладонь [*6*], голос [*7*] и подпись [*8*]. Несмотря на то что обработка занимает больше времени ввиду ограниченной вычислительной мощности, во всех случаях не наблюдается увеличения вероятностей ошибок по сравнению с реализацией на настольных компьютерах. Разработчик должен подтвердить, что вероятность ошибок не изменилась.

5.2.2 Защита данных и конфиденциальность

В настоящее время мобильное устройство содержит большое количество персональных данных (т. е. данных пользователя, например фотографии, контакты, сообщения или финансовая информация) и/или конфиденциальной или служебной информации профессиональной жизни владельца мобильного устройства (т. е. профессиональных контактов, электронных писем, документов и т. д.). Защита подобной информации должна обеспечить доступ только уполномоченному лицу, поэтому должны быть использованы механизмы аутентификации. ПИН-код или образец жестикуляции могут быть увидены сторонними наблюдателями, так как мобильные устройства часто используют в общественных местах. Применение токенов незначительно распространено в мобильных устройствах, так как подключение токена будет сопровождаться ограничениями удобства пользования ввиду слота подключения токена (т. е. считывателя смарт-карт, подключенного по OTG или Bluetooth*). Кроме того, токен может быть потерян, украден или даже скопирован.

Для облегчения такого процесса могут быть использованы биометрические данные при условии, что мобильное устройство оборудовано устройством сбора биометрических данных, т. е. биометрическим сканером. Биометрический образец пользователя также является личными данными, которые должны быть защищены от несанкционированного доступа. Прямой доступ к биометрическому образцу позволит злоумышленнику выдавать себя за пользователя мобильного устройства либо на самом устройстве, либо в другом процессе аутентификации, использующем ту же самую биометрическую характеристику.

Чтение или копирование учетных данных должно быть запрещено. Кроме того, должна быть исключена возможность переопределения процесса аутентификации. По этой причине продемонстрированы традиционные уязвимости ИТ-решений. Так как большинство мобильных устройств являются платформами общего назначения с возможностью загрузки любого стороннего приложения, существует вероятность загрузки троянских программ, реализующих атаки «человек посередине» (man-in-the-middle)** для манипулирования данными или процессом аутентификации.

Подобно ПИН-коду или образцу жестикуляции пользователя биометрия может быть скопирована и повторно использована злоумышленником. Биометрические данные в большинстве случаев являются общедоступными (например, скрытые отпечатки пальцев, фотографии лица, фотография радужной оболочки глаза на расстоянии и т. д.). Таким образом, злоумышленник может получить необработанную информацию от пользователя и создать из нее искусственные биометрические образцы, пытаясь получить доступ к системе. Это называется атакой на биометрическое предъявление или спуфинг-атакой и требует включения механизмов обнаружения атак на биометрическое предъявление в процесс сбора биометрических данных. Подробная информация по обнаружению атак на биометрическое предъявление приведена в *серии стандартов ГОСТ Р 58624.* Целью указанных механизмов является обнаружение и, следовательно, отклонение предъявления биометрических образцов, которые могут считаться искусственными. В мобильных устройствах биометрия предназначена исключительно для аутентификации, а не идентификации. Поэтому такие атаки, как скрытие (т. е. избегание идентификации), выходят за рамки настоящего стандарта.

Несмотря на то что достижение 100 %-ной защиты данных практически невозможно, должно быть сделано много для повышения уровня конфиденциальности, достигаемого в современных мобильных устройствах.

Основной вопрос заключается в том, используется ли лучший метод аутентификации в соответствующее время для приложения. Аутентификация пользователя для разблокировки мобильного устройства или для банковского перевода представляет собой разные операции. Все зависит от того, какая информация хранится в мобильном устройстве, так что разблокировка мобильного устройства может быть более опасной, чем несанкционированный перевод.

---

* Производственная спецификация беспроводных персональных сетей.

** Man-in-the-middle — тип интернет-атак, в процессе которых злоумышленник перехватывает канал связи, получая полный доступ к передаваемой информации.

Важно отметить, что биометрия может быть использована наряду с токенами для повышения защиты. Все мобильные устройства GSM уже включают смарт-карту, т. е. модуль идентификации абонента (Subscriber Identity Module, SIM), которую можно применять для хранения идентификационных и персональных данных. Однако SIM-карта зависит от мобильного оператора, а также не извлекается из мобильного устройства, так что, если мобильное устройство украдено, токен также украден.

Новая перспективная возможность — применение других видов внешних персональных токенов, таких как бесконтактные смарт-карты, которые могут быть подключены к мобильному устройству с использованием таких интерфейсов, как NFC или Bluetooth Low Energy, BLE (Bluetooth с низким энергопотреблением). В этом случае пользователь может носить этот токен в своем кошельке, а устройство может подключаться к нему без необходимости применения дополнительных периферийных устройств, и тогда смарт-карта может быть снабжена криптографией с открытым ключом, для выполнения не только аутентификации, но и цифровой подписи. Для аутентификации с использованием токена могут быть применены ПИН-коды или биометрические данные при наличии у токена функций биометрического сравнения на карте (см. *ГОСТ Р 58230)*.

Независимо от использования или неиспользования внешних токенов следует учитывать дальнейшие действия по обеспечению более высокого уровня защиты данных. Доступны некоторые улучшения как со стороны пользователя (пользовательского интерфейса), так и непосредственно операционной системы. Основным фактором, который нужно учитывать, является способ блокировки мобильного устройства, в тот момент, когда его не используют. В настоящее время широко внедрены стратегии, касающиеся ПИН-кодов и образцов жестикуляции. Такие механизмы разблокировки могут быть скопированы путем наблюдения в процессе разблокировки. Некоторые пользователи пользуются этим механизмом, но не с целью безопасности, а во избежание нежелательных вызовов при переносе мобильного устройства в кармане или сумке. Большинство пользователей предпочитают образцы жестикуляции из-за легкости и скорости их ввода или распространенный ПИН-код, такой как 1212 (легко вводится, даже если не смотреть на экран). Эти факторы приводят к требованиям, которым должна соответствовать процедура разблокировки: удобная в использовании, легко запоминаемая, легкая для ввода и быстрая. Если какое-либо из этих требований не соблюдается, то высока вероятность того, что пользователь выберет более легкую версию или даже отменит весь процесс. Так как разблокировка мобильного устройства является первым шагом в обеспечении безопасности данных и процессов, хранимых на мобильном устройстве, должны быть рассмотрены новые решения, приведенные ниже.

С появлением коммерчески доступной технологии верификации сенсорных данных на смарт-устройствах была продемонстрирована новая альтернатива. Размещение пальца на устройстве сбора отпечатков пальцев является удобным процессом, легко запоминается, легко вводится, и если алгоритм достаточно быстрый, например менее 1 с, то и может быть очень удобным для пользователя. Так как несогласованное создание фальшивых образцов сложное и медленное, то этот метод атаки считается маловероятным для процесса разблокировки, что повышает уровень конфиденциальности.

Следует также учитывать защиту любых персональных данных. Если стороннее программное обеспечение может получить доступ к персональным данным пользователя, конфиденциальность пользователя будет нарушена. Эта защита может быть достигнута за счет использования ЭБ, например смарт-карт или отдельных частей микропроцессора, созданного для хранения секретной информации. ЭБ могут быть изготовлены таким образом, что секретную информацию невозможно считать, а только провести внутреннюю верификацию или обработку (например, схема цифровой подписи с ПИН-кодами или частными ключами). Такие ЭБ могут быть внутренними или внешними и содержать разное количество данных. Операционная система устройства может получить доступ к ЭБ в условиях безопасности, и это является наиболее эффективным способом для обеспечения безопасности во время работы с мобильным устройством. Включение ЭБ и упомянутых правил безопасности называется ДСИ.

Независимо от качества ДСИ на мобильном устройстве существуют дальнейшие риски для конфиденциальности и безопасности данных, связанные с передачей биометрической информации на центральный сервер. В этом случае необходимо правильно аутентифицировать центральный сервер и шифровать любые передаваемые биометрические данные. Также важно, чтобы центральный сервер и контролируемые им сущности обеспечивали наличие соответствующих протоколов безопасности. Как показывает опыт, большинство утечек данных происходит после того, как данные многих пользователей собраны в одном месте. Поэтому для любого приложения важно учитывать дополнительные риски, когда биометрические данные передаются на центральный сервер, а не остаются на мобильном устройстве.

Существует несколько стратегий для разработки ДСИ, но большинство из них противоречат удобству использования и потребностям или предпочтениям пользователей. Первая стратегия (самая радикальная) — это обеспечение мобильного устройства набором разрешенных приложений, разработанных и перепроверенных производителем мобильного устройства. В настоящее время данная стратегия не будет принята пользователями ввиду их желания устанавливать новые приложения, которые они считают интересными. Вторая стратегия заключается в том, что все устанавливаемые приложения должны поступать из авторизованного и проверенного источника. Это требует от разработчиков приложений следовать схемам сертификации для своих приложений, что в большинстве случаев повлечет за собой взимание платы с пользователей за использование приложений.

Эта стратегия приводит к следующим эффектам:

a) изготовитель мобильного устройства должен сертифицировать все разработанные приложения, что потребует увеличения объема ресурсов, которые могут быть обоснованы глубиной и сложностью многих приложений;

b) некоторые пользователи сочтут возможность использования несертифицированных приложений более важной, чем безопасность.

Пользователь должен быть осведомлен о последующих потерях в защите и конфиденциальности данных: необходима разъяснительная работа для пользователей мобильных устройств.

В третьей стратегии устройство разделено на две независимые среды:

a) безопасная среда с независимой памятью и сертифицированными приложениями, т. е. ДСИ;

b) незащищенная среда, в которой пользователь может устанавливать все необходимые, с его точки зрения, приложения, которые не имеют прямого доступа к данным, хранящимся в ДСИ.

Изменение окружения достигается простым нажатием кнопки, и каждая среда сопровождается своим набором цветов, так что пользователю легко управлять мобильным устройством при обеспечении разумного уровня защиты данных.

Защита изменения среды (в частности, активации ДСИ) может быть усовершенствована определенным типом аутентификации. Но в таком случае возникают описанные выше проблемы удобства использования, поэтому для данной задачи будет эффективным применение биометрической характеристики.

Альтернативой использованию ДСИ для защиты биометрических шаблонов, хранящихся на мобильных устройствах, является применение защищенных биометрических шаблонов [*9*]. Такие схемы хранят биометрические шаблоны в необратимой форме, и разделяются на биометрические криптосистемы и аннулируемую биометрию. Биометрические криптосистемы предоставляют механизмы для связывания или выпуска криптографических ключей. Данные схемы защищенных шаблонов помимо необратимости должны обладать также возобновляемостью и возможностью отзыва. Использование этих схем не является специфичным для ДСИ или ЭБ, таким образом, не требуется адаптация биометрической системы к различным средам, что облегчает интеграцию биометрической системы. Более подробная информация представлена в [*10*].

Если защита данных обеспечена с помощью биометрии, то следует рассмотреть обнаружение атаки на биометрическое предъявление. Должен быть проведен анализ уязвимости и оценен потенциал атаки для каждой идентифицированной уязвимости.

Для обнаружения атак на биометрическое предъявление либо в устройство сбора биометрических данных должны быть интегрированы дополнительные датчики, либо получение биометрических данных должно быть проведено в течение длительного времени для выявления как движений человека, которые отсутствуют в искусственных образцах, так и движений образца, созданных наличием искусственных слоев на реальных биометрических характеристиках злоумышленника.

Должны быть решены вопросы конфиденциальности и защиты персональных данных с использованием биометрии и других дополнительных данных. Эти вопросы выходят за рамки настоящего стандарта.

5.2.3 Сбор биометрических образцов

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 устройствами сбора данных, которые интегрированы в современных мобильных устройствах, являются акселерометры и гироскопы. С такими устройствами сбора данных может быть использована походка [*11*]. С помощью микрофона можно 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 походки расположение мобильных устройств является одним из параметров, в большой степени влияющих на собираемую информацию, также как способ удержания смартфона влияет на изменения в информации о жесте для подписи в воздухе. Таким образом, в данной области необходима дальнейшая работа.

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

В случае с сосудистым руслом некоторые мобильные устройства оснащаются встроенным устройствами сбора изображений сосудистого русла и являются коммерческими продуктами. Другие модальности находятся на стадии исследования и прототипа или требуют внешних устройств сбора биометрических данных, подключаемых через OTG или Bluetooth.

5.2.4 Процесс аутентификации образца

В настоящем стандарте обозначены 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 наиболее 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»*.

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, должен быть разработан в соответствии с запросами приложения. Разные 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 мобильного 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, применение которых должно обеспечивать четкое взаимодействие, легко запоминаться и которые должны быстро выполняться. 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 зависимых людей или людей с различными видами и степенями инвалидности. 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.). В случае инвалидности может быть рекомендовано использование внешних устройств сбора биометрических данных.

Для повышения удобства использования рекомендован общий интерфейс для всех приложений. Дополнительным преимуществом аутентификации является ее предоставление операционной системой 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.

---

* Man-in-the-middle — тип интернет-атак, в процессе которых злоумышленник перехватывает канал связи, получая полный доступ к передаваемой информации.

5.2.5 Удобство пользования

5.2.5.1 Общие положения

Существует целый ряд особенностей в мобильных компьютерных средах, которые делают их пользовательский интерфейс отличным от пользовательского интерфейса настольных 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 широкий спектр устройств, которые могут включать в себя ноутбуки, планшеты, телефоны и портативные электронные устройства. Каждое из этих мобильных устройств имеет разные способы использования, однако настоящий стандарт рассматривает общие атрибуты, применимые к планшетам, смартфонам и портативным электронным устройствам.

5.2.5.2 Условия окружающей среды

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

5.2.5.3 Ограниченные входные данные

Ввиду малого форм-фактора в мобильном устройстве уменьшается диапазон входных данных, для того чтобы получить преимущество ограниченного общего размера устройства. Это привело к различным вариантам 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 биометрический сканер отпечатков пальцев, присутствуют в различных мобильных устройствах и, несмотря на то что они, как правило, используются рядом приложений, должны быть рассмотрены следующие аспекты для ситуаций, требующих высокой точности воспроизведения (например, сбор биометрических данных, а именно — речь, изображение лица или отпечаток пальца):

a) способно ли технически устройство сбора данных собирать информацию с достаточной точностью и на каком расстоянии;

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

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

5.2.5.4 Ограничения мощности обработки

Мобильные устройства являются компонентами оборудования с высокой мощностью, если рассматривать только исходные характеристики, однако эта мощность быстро уменьшается при внедрении операционных систем с интерактивными пользовательскими интерфейсами. Мобильное приложение будет иметь значительно меньше ресурсов и меньшую скорость работы по сравнению с настольным приложением.

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 сломанным или неисправным. В одном 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.

5.2.5.5 Возможность подключения

Возможность подключения (к внешним ресурсам) должна рассматриваться как потенциальная проблема для использования мобильного приложения. Приложения, зависимые от внешних систем при выполнении обработки, должны иметь определенный метод работы в автономном режиме или сообщать пользователю, что внешний ресурс недоступен. Если приложение полностью зависит от внешнего ресурса, должны быть четкие и однозначные способы указания наличия соединения и проверки целостности соединения. Приложение должно также включать надежную обработку ошибок при потере

промежуточной транзакции соединения, при которой ни транзакция, ни приложение не должны приводить к сбою. Пользователи будут воспринимать приложения, которые приводят к сбою из-за проблем подключения или потери данных, как неисправные и не подходящие для использования.

5.2.5.6 Когнитивная нагрузка

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

Если во время работы с настольным компьютером для пользователя когнитивная нагрузка будет единственной задачей, то в случае мобильных устройств обычным является выполнение пользователями других действий (например, вождение автомобиля и использование навигационного приложения на мобильном телефоне, ходьба во время переписки). 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.

5.2.5.7 Привлекательность для пользователя

То, как пользователи думают о мобильных приложениях 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 настольными приложениями. И если одно приложение не будет соответствовать ожиданиям, то существует множество приложений для проб. Парадокс заключается в том, что 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.

Более подробная информация по взаимодействию с мобильной биометрией приведена в *[12]—[17]*.

5.2.6 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 (с использованием *серии стандартов ГОСТ Р 58292* и *серии стандартов ГОСТ Р 58624*).

Технологические испытания должны включать оценку безопасности, обеспечиваемой решением, и поиск уязвимостей не только на уровне устройств сбора биометрических данных, но и операционной системы.

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 операционной системы 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, то есть граждан, которые ранее не были знакомы с такими устройствами и с биометрическим распознаванием. Так как технология стано-

вится все более распространенной, это будет все менее возможно в силу того, большинство пользователей будут иметь доступ к этой технологии.

Мобильные устройства меняются очень быстро в связи с тем, что модели развиваются ввиду влияния маркетинга. Новые модели подразумевают изменения в размере, в периферийных устройствах, вычислительной мощности, пользовательском интерфейсе и операционной системе. 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.

5.2.7 Задачи, общие с другими сценариями и платформами

В дополнение ко всем предыдущим задачам применяют задачи, типичные для другого ИТ-приложения. В частности, важно, как именно должна быть выполнена интеграция биометрической аутентификации в каждом из приложений. Цель состоит в максимизации окупаемости инвестиций (ОИ) (*Return on Investment, ROI)*, для того чтобы такая рентабельность инвестиций повышала преимущества и сокращала время получения этих преимуществ.

Для снижения затрат на внедрение и, следовательно, повышение ОИ, необходим стандартизованный прикладной интерфейс приложений, ПИП *(Application Programming Interface, API).* В биометрии единственным стандартизованным ПИП для разработки приложения является BioAPI, определенный в *серии стандартов ГОСТ Р ИСО/МЭК 19784*. В настоящее время существуют работы по разработке объектно-ориентированной версии BioAPI, определенной на унифицированном языке моделирования UML (Unified Modeling Language, UML), а также Java и C #. Эти работы являются целевыми объектами в [*19*].

Другой задачей снижения стоимости внедрения является испытание решения. Благодаря применению общего процесса аутентификации для всех приложений могут быть сведены к минимуму соответствующие затраты. Новые достижения в создании методологии оценки биометрии в мобильных устройствах, в частности с учетом удобства использования, поможет снизить затраты на испытания, повышая в то же время достоверность и надежность результатов.

6 Биометрические службы внутри ОС 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 слой аппаратных абстракций (САА) *(Hardware Abstraction Layer, HAL).*

Рисунок 1 — Общая архитектура операционной системы мобильного устройства

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

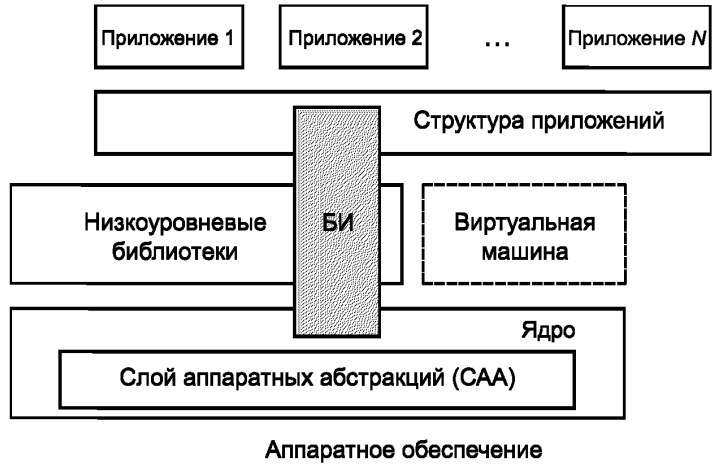

Рисунок 2 — Расположение биометрического интерфейса при разработке внутри операционной системы

В тех ОС, где имеется ВМ, и производитель 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 мобильном 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.

В том случае, если ОС поддерживает удаленные биометрические службы, необходимо учитывать следующие методы:

- предоставление метода хранения биометрического контрольного шаблона, обеспеченного удаленным сервером;
- предоставление функциональности по сбору биометрического образца:
  - в виде необработанной или обработанной записи данных,
  - с использованием шифрования по криптографическому протоколу, согласованному между мобильным устройством и удаленным сервером;
- включение, при возможности, механизмов взаимной аутентификации сервера и мобильного устройства для подтверждения достоверности и целостности обмениваемых биометрических данных.

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

Производитель ОС может предоставлять функциональность конфигурации, с помощью которой при использовании БИ выбирают различные параметры для определенных приложений и/или сцена-

риев. Например, может быть обеспечено дискретное число уровней доверия с разными порогами (т. е. проверки качества, сравнения, обнаружения атаки на биометрическое предъявление и т. д.).

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

- сбор одного или нескольких биометрических образцов из последовательности образцов (т. е. изображение лица из изображения лица в реальном времени);
- создание наилучшего биометрического(их) образца(ов) на основе некоторой метрики качества;
- предоставление показателя качества для сбора биометрического образца;
- предоставление информации о доступности устройств сбора данных на мобильном устройстве (например, камеры мультисенсорного экрана, сканера отпечатков пальцев, GPS, 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».

Необходимо учитывать, какие элементы могут находиться на мобильном устройстве и какая информация проходит через веб-службу. В разных обстоятельствах даже для одного и того же приложения могут быть приняты различные подходы. Устройство может быть подключено или не подключено, хотя при этом подходе, как правило, БИ реализуется с использованием устройств сбора данных, уже доступных на мобильном устройстве. На уровне платформы пользователь должен видеть согласованность интерфейса.

Основными преимуществами данного подхода являются:

a) использование машинного кода и отсутствие промежуточных уровней, которые могут приводить к потере производительности;

b) прямой доступ ко всем доступным элементам безопасности мобильного устройства. Последнее преимущество особенно важно, так как создание ДСИ ОС может сделать двунаправленную выгоду между ДСИ и биометрическими службами.

С одной стороны, БИ может выиграть от выполнения в ДСИ и, следовательно, избежать многих потенциальных атак (в частности, атаках «человек посередине»). БИ может извлечь выгоду из возможности использовать низкоуровневые элементы безопасности, 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 видно, что БИ находится на одном уровне с остальными приложениями, но предоставляет общие службы, которые могут быть применены другими приложениями (например, от приложения *H* до приложения *K*). Другие приложения на мобильном устройстве могут сосуществовать без использования БИ, такие как приложение 1 и приложение *N*, указанные на рисунке 3.

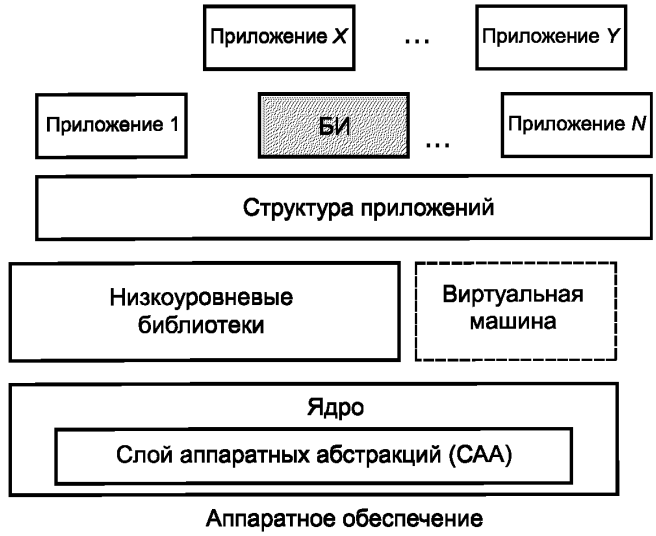

Рисунок 3 — Расположение биометрического интерфейса при разработке на уровне приложений

Рекомендации раздела 6 применимы для рассматриваемого варианта с изменением производителя ОС на производителя БИ в тех местах, где упомянут производитель ОС. В дополнение к этим рекомендациям применяются такие как:

a) 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;

b) 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 мобильному устройству, ни к памяти, зарезервированных для такого процесса.

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

c) 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), с учетом национальных требований в области криптографической защиты информации.

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 производителем 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 [*18*] 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. Тем приложениям, которым необходимо использовать БИ, должны сделать запрос путем вызова структуры ПИП, определенной в [*18*] (см. рисунок 4).

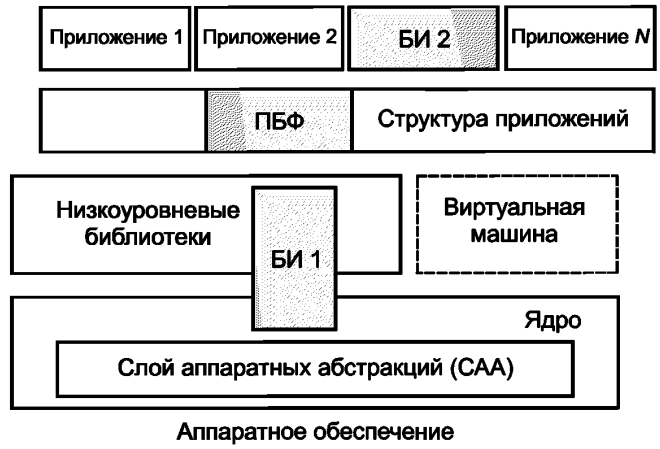

Рисунок 4 — Схема внедрения структуры [*18*] в операционную систему

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

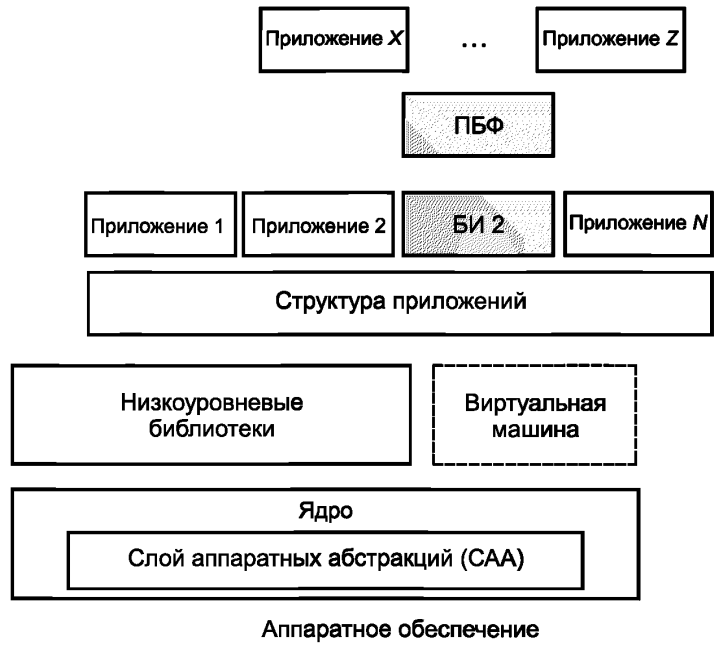

Рисунок 5 — Схема внедрения структуры [*18*] на уровне приложений

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 устройстве сбора данных. Такое взаимодействие может представлять обратную связь пользователю:

- о пальце, который необходимо поместить на рабочую поверхность биометрического сканера отпечатков пальцев;
- том, как именно улучшить положение образца (например, выравнивание биометрической характеристики по отношению к чувствительной области устройства сбора биометрических данных);
- том, было ли получение данных проведено корректно;
- 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 мобильного устройства, для того чтобы избежать обращения с самим БИ и появления недостатков, таких как:

- графический интерфейс пользователя 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. Поэтому, если БИ позволяет использовать функции обратного вызова для управления ГИП, необходимо предпринять определенные действия для проведения каждого процесса, требующего осуществление 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. Например, в начале процесса может быть представлено сообщение «Сбор данных указательного пальца правой руки», в конце процесса — «Сбор завершен. Спасибо!». Поэтому должно быть определено, вызывается 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 вы-

сокого уровня, например: методы, в которых все биометрические данные обрабатываются в БИ и не распространяются через приложение.

На различных интерфейсах системных компонентов могут эффективно использоваться веб-службы. Это не только улучшит совместимость, но и позволит внедрять биометрические возможности там, где они недоступны. Например, служба получения данных, такая как WS-Biometric Devices, позволит мобильному устройству без встроенного сканера отпечатка пальца получать отпечатки пальцев из доступного сканера. Стандартная веб-служба, такая как BIAS* [*19*], может аналогично проводить биометрическую регистрацию или биометрическое распознавание, например в тех случаях, когда локально недоступны данные или возможности сравнения.

9 Руководство функциональностью и оперативной работой

9.1 Общее руководство

9.1.1 Руководство по функциональной архитектуре

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

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

b) биометрический контрольный шаблон может храниться локально на мобильном устройстве или на центральных серверах (в облаке);

c) аутентификация может проводиться локально на мобильном устройстве или на центральных серверах (в облаке);

d) если приложение требует аутентификацию, даже если мобильное устройство находится в автономном режиме (т. е. без подключения), то регистрационные данные, включая биометрические контрольные шаблоны, будут распространены среди всех экземпляров приложения на мобильных устройствах через интерфейс управления облачными данными;

e) когда для инициирования процесса аутентификации использована коммуникация ближнего поля, то транзакция будет обмениваться данными, достаточными для обеспечения безопасного канала связи (например, Wi-Fi, GPS) для предоставления коммуникации по схеме «вопрос—ответ»;

f) настоящий стандарт ограничен архитектурами, поддерживающими биометрическую верификацию («один к одному») и биометрическую идентификацию («один ко многим»);

g) сбор может проводиться с помощью мобильного устройства, а также посредством физически или логически привязанного устройства сбора данных. В интернет-среде верификатор не может доверять результату «успешно»/«отказ» от клиента без определенных условий, потому что среды выполнения в большой степени зависят от пользователей, в том числе злоумышленников. Следовательно, верификатор должен проверить достоверность результата аутентификации.

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 мобильного 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 отпечатков пальцев, в то время как высокий уровень фонового шума повлияет на мобильное устройство с распознаванием голоса.

Дополнительная информация приведена в разделе 11.

---

* Услуги обеспечения биометрической идентификации (Biometric Identity Assurance Services).

9.2 Руководство по биометрической регистрации

9.2.1 Общее руководство по биометрической регистрации

Существующее руководство по наилучшей практике разработано для поддержки совместимости и поиска биометрических данных в разных приложениях и системах, соответствующие показатели качества биометрических образцов созданы для обеспечения соответствия.

9.2.2 Контролируемая биометрическая регистрация

В определенных сценариях является целесообразной контролируемая биометрическая регистрация пользователя на платформе, внешней по отношению к мобильному устройству. Одним из примеров является банковское приложение, когда биометрическая регистрация должна быть проведена в филиале банка, и далее биометрическая информация загружается в мобильное устройство пользователя. Такой сценарий позволит клиенту менять мобильное устройство без повторения процесса биометрической регистрации при условии, что загруженный биометрический шаблон имеет совместимость с предыдущим и новым мобильными устройствами.

Преимуществами такого подхода являются:

- отсутствие повторения процесса биометрической регистрации;
- наличие возможности у оператора при контролируемой биометрической регистрации предоставить клиенту всю необходимую информацию и провести обучение, что подразумевает:
  - устранение любых сомнений и вопросов клиента,
  - демонстрацию клиенту взаимодействия с устройством сбора данных и приложением;
- применение оператором доступных механизмов для проверки личности клиента и препятствование краже личности;
- оказание содействия пользователю в наилучшей биометрической регистрации с учетом различных ситуаций, с которыми ему придется столкнуться при последующем распознавании.

Необходимо учесть следующие аспекты:

- связь и сохранение биометрических данных в мобильном устройстве пользователя должны быть выполнены защищенным способом. Если установку проводят дистанционно, то информация должна быть зашифрована и выполнена взаимная аутентификация сервера и мобильного устройства;
- если биометрическую регистрацию и биометрическое распознавание проводят на разных платформах, алгоритмы обработки и/или сравнения будут обрабатывать любые различия в полученном биометрическом образце. Различные характеристики устройства сбора биометрических данных могут влиять на полученный биометрический образец и, следовательно, на эксплуатационные характеристики биометрического распознавания.

Различия во внешних условиях окружающей среды во время биометрической регистрации и использования мобильного устройства для распознавания могут оказывать значительное влияние на эксплуатационные характеристики. Этот аспект должен быть учтен при проектировании системы.

9.2.3 Неконтролируемая биометрическая регистрация

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

Однако в случае биометрии на мобильных устройствах пользователи обязательно экспериментируют, для того чтобы понять, что будет принято. Например, они могут пробовать делать 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 биометрический сканер отпечатков пальцев или направить камеру на изображение лица. Такие попытки будут успешными или неуспешными в зависимости от того, как встроен биометрический сканер и какие пороги качества установлены.

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

Распознавание подписи является хорошим примером, так как не требуется, чтобы человек использовал свою обычную подпись в биометрическом приложении. Имеет значение то, что при био-

метрической 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 новые 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 мобильных устройствах, в отличие от обычных проверок биометрического качества, разработанных для поддержки совместимости.

9.3 Руководство по аутентификации

9.3.1 Удаленная неконтролируемая аутентификация

После регистрации биометрические данные обеспечивают больший уровень доверия в неконтролируемой аутентификации зарегистрированной личности по сравнению с другими типами учетных данных, так как (см. введение) они связаны с человеком более тесно, чем такие учетные данные, как пароли или токены, которые могут быть украдены или потеряны.

9.3.1.1 Для обеспечения данного уровня доверия в мобильной среде должны быть реализованы надежные технические процедуры безопасности при разработке всех приложений и транзакций для гарантии того, что:

a) фактически проходит «живой» сбор соответствующих биометрических характеристик человека (например, отпечатков пальцев или радужной оболочки глаза) в момент запроса аутентификации, т. е. противодействие спуфингу, мошеннической подаче украденных изображений или других представлений биометрических характеристик зарегистрированного человека;

b) цифровые данные, получаемые мобильным приложением из собираемых биометрических данных, сертифицированы как надежно связанные с временным процессом сбора. Данный способ позволяет предотвратить способ мошенничества с использованием перехваченных и записанных данных от предыдущих регистраций зарегистрированного человека;

c) цифровое представление собранных биометрических данных проводят в одностороннем порядке, и это не позволяет использовать получаемые данные для создания синтетического изображения, которое может быть использовано для других мошеннических попыток аутентификации;

d) при возможности и целесообразности сбор и обработка биометрических данных индивида будут осуществлены на мобильном устройстве, которое авторизовано и зарегистрировано для использования.

9.3.1.2 Процедуры безопасности, обозначенные выше для процессов сбора и обработки биометрических данных на мобильных устройствах при удаленной и неконтролируемой аутентификации, должны сочетаться с соответствующими последующими процедурами для обеспечения того, что:

a) последующие транзакции в процессе аутентификации идентичности сохраняют целостность сертифицированных биометрических данных и других предоставленных учетных данных;

b) данные, необходимые для аутентификации, обрабатываются в последующих транзакциях только уполномоченными получателями, т. е. поставщиками служб (или их подлинными агентами), которые первоначально регистрировали соответствующих лиц.

9.3.2 Локальная неконтролируемая аутентификация

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 мобильном 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, так что биометрическая служба блокируется, по крайней мере, для приложения, вызывающего эту службу.

Должна быть проведена 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 устройств сбора биометрических данных, которые могут поддерживать оценку нескольких биометрических модальностей. Устройства сбора биометрических данных 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 работы устройства сбора биометрических данных. 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 самозванец 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.

ГОСТ Р 54411 содержит дополнительную информацию о мультимодальном и другом мультибиометрическом объединении.

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

Коммерческие мобильные устройства могут включать в себя устройства сбора данных, такие как микрофоны, сенсорные экраны и камеры, или использовать периферийные устройства сбора биометрических данных. С помощью таких устройств 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 устройств сбора данных, которые могут быть использованы дополнительно к биометрическому распознаванию для обеспечения дополнительных уровней безопасности, например: служба GPS или другие службы определения местоположения (в частности, местоположение ячейки телефонной сети или распознавание опознавательных объектов с помощью 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 устройства сбора данных могут повысить уровень безопасности аутентификации или удобства использования.

11 Руководство по выбору биометрических модальностей

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 NFC.

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 NFC 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 биометрические эксплуатационные характеристики
Лицо	Освещение: - основная освещенность (слишком светло/слишком темно); - направленное освещение (приводящее к теням на лице). Выражение лица субъекта. Положение головы субъекта. Использование макияжа и/или аксессуаров (шляпа, шарф, солнцезащитные очки и т. д.). Неконтролируемый и сложный фоны. Быстрые изменения температуры и влажности, вызывающие конденсацию на объективе. Движение субъекта или сенсорной платформы (например, движение поезда, судна или самолета)
Палец (оптические устройства)	Освещение: - прямое освещение 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; - пальцев и стиранию папиллярного узора. Быстрые изменения температуры и влажности, вызывающие конденсацию на объективе и/или рабочей поверхности биометрического сканера

Окончание таблицы 1

Модальность	Фактор окружающей среды, влияющий на биометрические эксплуатационные характеристики
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 отделение голоса субъекта от фона. 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 холодные условия среды могут 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.

Руководящие указания по качеству в *ГОСТ Р ИСО/МЭК 19794-2, ГОСТ Р ИСО/МЭК 19794-5, ГОСТ Р ИСО/МЭК 19794-7, ГОСТ Р ИСО/МЭК 19794-11* и в *ГОСТ Р ИСО/МЭК 29794-1, ГОСТ Р ИСО/МЭК 29794-6* не учитывают использование коммерческих мобильных устройств, таких как смартфоны и планшеты.

Приложение ДА
(справочное)

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

Таблица ДА.1

Обозначение ссылочного межгосударственного стандарта	Степень соответствия	Обозначение и наименование соответствующего международного стандарта
ГОСТ ISO/IEC 2382-37	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.		

Приложение ДБ
(справочное)

Сопоставление структуры настоящего стандарта со структурой примененного в нем международного документа

Таблица ДБ.1

Структура настоящего стандарта	Структура международного документа ISO/IEC TR 30125:2016
Приложение ДА Сведения о соответствии ссылочного межгосударственного стандарта международному стандарту, использованному в качестве ссылочного в примененном международном документе	
Приложение ДБ Сопоставление структуры настоящего стандарта со структурой примененного в нем международного документа	
Примечание — Сопоставление структуры стандартов приведено начиная с приложения ДА, так как предыдущие разделы стандартов идентичны.	

Библиография

[1] NISTIR 8003*, Design and Testing of a Mobile Touchscreen Interface for Multi-Modal Biometric Capture, May 2014

[2] ISO/IEC 29115, Information technology — Security techniques — Entity authentication assurance framework

[3] Khalil M.S., & Wan F.K. A review of fingerprint pre-processing using a mobile phone, International Conference on Wavelet Analysis and Pattern Recognition (ICWAPR), pp. 152, 157, 15—17 July 2012. doi:.10.1109/ICWAPR.2012.6294770

[4] Cho D., Park K.R., Rhee D.W. Real-time iris localization for iris recognition in cellular phone. In: SNPD. SAWN, 2005, pp. 254—9

[5] Vazquez-Fernandez, J., Garcia-Pardo, H., Gonzalez-Jimenez, D. and Perez-Freire, L.: Built-in face recognition for smart photo sharing in mobile devices. In IEEE International Conference on Multimedia and Expo (ICME), pp. 1—4 (2011)

[6] de Santos Sierra A., Guerra Casanova J., Avila C.S., Vera V.J. Silhouette-based hand recognition on mobile devices, 43rd Annual International Carnahan Conference on Security Technology, pp. 160, 166, 5—8 Oct. 2009. doi: 10.1109/CCST.2009.5335548

[7] http://www.mobioproject.org/ [Apr. 30.2013]

[8] Blanco-Gonzalo R., Sanchez-Reillo R., Miguel-Hurtado O., Liu-Jimenez J. Performance evaluation of handwritten signature recognition in mobile environments. IET Biometrics, 2013., 10.1049/iet-bmt.2013.0044

[9] Protection Biometric Template, Breebaart Jeroen, Yang Bian, Buhan-Dulman Ileana, Busch Christoph Datenschutz und Datensicherheit — DuD, 2009, 33(5), p. 299

[10] ISO/IEC/TR 24714-1, Information technology — Biometrics — Jurisdictional and societal considerations for commercial applications — Part 1: General guidance

[11] 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

[12] Lee H.C., Park K.R., Kang B.J., Park S.-J. A New Mobile Multimodal Biometric Device Integrating Finger Vein and Fingerprint Recognition, Proceedings of the 4th International Conference on Ubiquitous Information Technologies & Applications, pp.1, 4, 20—22 Dec. 2009. doi: 10.1109/ICUT.2009.5405686

[13] Sanchez-Reillo R., Lopez-Garcia M., Blanco-Gonzalo R., Liu-Jimenez J., Canto E. Universal Access through Biometrics in Mobile Scenarios, 47th IEEE International Carnahan Conference on Security Technology, Medellin (Colombia), Oct. 2013, pp. 59—64

[14] Blanco-Gonzalo R., Sanchez-Reillo R., Martinez-Normand L., Fernandez-Saavedra B., Liu-Jimenez J. Accessible Mobile Biometrics for Elderly. In ASSETS '15 Proceedings of the 17th International ACM SIGACCESS Conference on Computers & Accessibility, pp. 419—420

[15] Blanco-Gonzalo R., Sanchez-Reillo R., Miguel-Hurtado O., Bella-Pulgarin E. Automatic usability and stress analysis in mobile biometrics. Image Vis. Comput. 2014, 32 (12), pp. 1173—1180

[16] CEN, CENELEC, ETSI. EN 301 549. v1.1.1. accessibility requirements suitable for public procurement of ICT products and services in Europe, Feb. 2014.

[17] Theofanos M., Stanton B., Wolfson C. A. Usability and Biometrics-Ensuring Successful Biometric Systems. 2008

[18] ISO/IEC 30106 Information technology — Object oriented BioAPI

[19] ISO/IEC 30108 Information technology — Biometric Identity Assurance Services

* http://www.nist.gov/itl/iad/ig/upload/Design-and-Testing-of-a-Touchscreen-Interface-for-Multi-Modal-Biometric-Capture_NISTIR-8003-3.pdf

УДК 004.93'1:006.89:006.354 ОКС 35.040

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

БЗ 12—2019/115

Редактор *Л.С. Зимилова*
Технический редактор *И.Е. Черепкова*
Корректор *М.В. Бучная*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 20.12.2019. Подписано в печать 21.01.2020. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 4,18. Уч.-изд. л. 3,76.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,

117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru