ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 19794-11— 2015

Информационные технологии

БИОМЕТРИЯ

Форматы обмена биометрическими данными

Часть 11

Обрабатываемые данные динамики подписи

(ISO/IEC 19794-11:2013, IDT)

Издание официальное

Москва
Стандартинформ
2016

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Научно-исследовательским и испытательным центром биометрической техники Московского государственного технического университета имени Н.Э. Баумана (НИИЦ БТ МГТУ им. Н.Э. Баумана) на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 20 ноября 2015 г. № 1923-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 19794-11:2013 «Информационные технологии. Форматы обмена биометрическими данными. Часть 11. Обрабатываемые данные динамики подписи» (ISO/IEC 19794-11:2013 «Information technology — Biometric data interchange Formats — Part 11: Signature/sign processed dynamic data», IDT).

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

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты, сведения о которых приведены в дополнительном приложении ДА

5 ВВЕДЕН ВПЕРВЫЕ

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

*Правила применения настоящего стандарта установлены в ГОСТ Р 1.0—2012 (раздел 8). Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующие информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, 2016

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

Содержание

1 Область применения 1
2 Соответствие 1
3 Нормативные ссылки 2
4 Термины и определения 2
5 Соглашения в отношении данных 2
5.1 Система координат 2
5.2 Порядок следования байтов и битов 2
5.3 Зарегистрированный идентификатор типа формата 3
6 Отношения форматов данных 3
7 Записываемые данные подписи 3
7.1 Общие положения 3
7.2 Данные динамического события 4
7.3 Сводные данные признаков 5
8 Формат записи обрабатываемых данных динамики подписи 6
8.1 Общие положения 6
8.2 Блок «Общий заголовок» (General header) 6
8.3 Блок «Заголовок представления» (Representation header) 7
8.4 Блок «Данные динамического события» (Dynamic-event data) 12
8.5 Блок «Сводные данные признаков» (Overall feature data) 13
8.6 Блок «Дополнительные данные» (Extended data) 14
Приложение А (обязательное) Методология испытаний на соответствие 15
Приложение В (справочное) Спецификация ACH.1 для формата данных 16
Приложение С (справочное) Подписи, пригодные для аутентификации 18
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации 20
Библиография 21

Введение

Существует ряд коммерческих реализаций верификаций подписи, основанных на анализе динамических признаков подписи. Настоящий стандарт устанавливает формат обмена динамическими данными подписи, которые могут быть использованы для верификации подписи. Данный формат обеспечивает обмен данными без нарушения прав на интеллектуальную собственность разработчиков.

Для обеспечения совместимости набор признаков является обязательным для всех соответствующих стандарту реализаций, но формат записи также поддерживает собственные данные компании изготовителя. Использование собственных данных компании изготовителя регулируется аналогично использованию в ИСО/МЭК 19794-7, благодаря чему результаты производительности с использованием обязательных и собственных признаков являются сопоставимыми.

Признаки подписи, записываемые в формат, отражают значимые динамические события во время процесса получения подписи, и таким образом представляют собой «разумное» сжатие формата ИСО/МЭК 19794-7. С помощью данных признаков могут быть рассчитаны или оценены другие признаки подписи. Кроме того, с помощью значимых событий может быть экстраполирован формат 19794-7, и таким образом рассчитаны или оценены другие данные признаков подписи.

Запись состоит из последовательности представлений подписи и блока «Общий заголовок», относящегося ко всем представлениям. Каждое представление подписи записывается как блок «Заголовок представления» и последовательность блоков «Данные динамического события».

Дополнительно к блокам «Данные динамического события» записываются сводные данные признаков представления (блок «Сводные данные признаков»). Необходимо отметить, что все записываемые данные подписи должны быть записаны до любых преобразований (например, поворота или деформации шкалы времени). Записываемые данные — это либо исходные данные, либо данные, полученные из исходных данных.

Настоящий стандарт не определяет методы обработки, проводимые любыми алгоритмами сравнения. Признаки подписи, записанные в формате данных, могут быть использованы для анализа с помощью различных алгоритмов сравнения.

Формат, определенный в настоящем стандарте, основан на признаках (динамических событиях) в отличие от ИСО/МЭК 19794-7, в котором использованы точки отсчета.

Формат, определенный в настоящем стандарте, имеет номер версии 1.0.

Приложение А является обязательным и предназначено для определения элементов методологии испытаний на соответствие, тестовых утверждений и методик испытаний применительно к настоящему стандарту.

Приложение В является справочным и определяет формат записи с использованием АСН.1 (см. ИСО/МЭК 8824) и правил уплотненного кодирования АСН.1 (см. ИСО/МЭК 8825-2), что позволяет использовать инструменты АСН.1 для реализации.

Приложение С является справочным. В нем представлены рекомендации по определению пригодности подписи для целей безопасности с использованием признаков подписи, записанных в формате в соответствии с настоящим стандартом. В приложении С устанавливаются три показателя пригодности подписи: объем данных, сложность подписи и стабильность подписи. В приложении предложены измерения, которые могут быть проведены для оценки указанных показателей, однако измерения не представлены количественно, а также отсутствует структура для записи показателей.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

БИОМЕТРИЯ

Форматы обмена биометрическими данными

Часть 11

Обрабатываемые данные динамики подписи

Information technologies. Biometrics. Biometric data interchange formats.
Part 11. Signature/sign processed dynamic data

Дата введения — 2017—01—01

1 Область применения

Настоящий стандарт устанавливает формат обмена обрабатываемыми данными динамики подписи. Обрабатываемые данные динамики подписи рассчитываются по подписи в виде временной последовательности, регистрируемой биометрическими сканерами подписи (планшеты, вычислительные устройства с ручкой-пером или системы профессионального пера).

Формат обмена, описываемый в настоящем стандарте, является базовым, то есть может быть применен для целого ряда областей приложения, в которых используются рукописные подписи. В настоящем стандарте не рассматриваются требования или признаки, связанные с конкретными применениями.

Настоящий стандарт содержит определения используемых терминов, описание обрабатываемых данных динамики подписи, описание формата хранения данных, а также рекомендации по определению пригодности подписи для целей идентификации с использованием настоящего стандарта.

В соответствии с требованиями настоящего стандарта хранимые и передаваемые биометрические данные должны содержать сведения о времени регистрации, а также быть зашифрованными для обеспечения подлинности, целостности и конфиденциальности, однако данные вопросы не рассматриваются в настоящем стандарте.

2 Соответствие

Запись биометрических данных соответствует настоящему стандарту, если она удовлетворяет всем нормативным требованиям, имеющим отношение к:

a) структуре данных, значениям данных и отношениям между элементами данных, определенным в разделе 8 настоящего стандарта;

b) соотношению между значениями данных и входными биометрическими данными, из которых была произведена запись биометрических данных, как определено в разделе 8 настоящего стандарта.

Система, создающая записи биометрических данных, соответствует настоящему стандарту, если все производимые записи биометрических данных соответствуют настоящему стандарту (как определено ранее). В системе должны производиться записи биометрических данных, которые удовлетворяют не обязательно всем аспектам настоящего стандарта, а только тем, которые заявлены как поддерживаемые системой.

Издание официальное

Система, использующая записи биометрических данных, соответствует настоящему стандарту, если в ней могут быть считаны и использованы по назначению все записи биометрических данных, соответствующие настоящему стандарту (как определено ранее). В системе должны использоваться записи биометрических данных, которые удовлетворяют не обязательно всем аспектам настоящего стандарта, а только тем, которые заявлены как поддерживаемые системой.

3 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты, которые необходимо учитывать при его использовании. В случае датированных ссылок необходимо пользоваться только указанной редакцией. В случае недатированных ссылок следует пользоваться последней редакцией ссылочных документов, включая любые поправки и изменения к ним.

ISO/IEC 19785-2 Information technology — Common Biometric Exchange Formats Framework — Part 2: Procedures for the operation of the Biometric Registration Authority (Информационные технологии. Единая структура формата обмена биометрическими данными. Часть 2. Процедуры действий регистрационного органа в области биометрии)

ISO/IEC 19794-1 Information technology — Biometric data interchange formats — Part 1: Framework (Информационные технологии. Форматы обмена биометрическими данными. Часть 1. Структура)

4 Термины и определения

В настоящем стандарте применены термины и определения по ИСО/МЭК 19794-1, а также следующие термины с соответствующими определениями:

4.1 **динамическое событие** (dynamic event): Событие «отрыв пера», «касание пера» или «точка поворота».

4.2 **касание пера** (pen-down): Событие, начиная с которого перо касается рабочей поверхности биометрического сканера подписи.

4.3 **данные динамического события** (dynamic-event data): Данные, в которых записаны позиция пера, сила нажатия и время определенного динамического события.

4.4 **отрыв пера** (pen-up): Событие, начиная с которого перо не касается рабочей поверхности биометрического сканера подписи; следует после события «касание пера».

4.5 **представление подписи** (signature/sign representation): Данные, записанные для одной подписи.

Примечание — Представление подписи всегда начинается с события «касание пера» и заканчивается событием «отрыв пера», однако представление может включать в себя большее число событий «касание пера» и «отрыв пера».

4.6 **точка поворота** (turning point): Событие, при котором меняется знак направления, полученного из близлежащих отсчетов одного из каналов *X*, *Y* или *F*.

5 Соглашения в отношении данных

5.1 Система координат

Для описания положения пера используется двухмерная декартова система координат. Ось *X* должна соответствовать горизонтальной оси рабочей поверхности биометрического сканера подписи, при этом значение координаты *X* должно начинаться с нуля и увеличиваться при перемещении пера вправо. Ось *Y* должна соответствовать вертикальной оси рабочей поверхности биометрического сканера подписи, при этом значение координаты *Y* должно начинаться с нуля и увеличиваться при перемещении пера вверх.

5.2 Порядок следования байтов и битов

Старшие байты любых многобайтовых значений имеют более низкие адреса памяти и передаются раньше, чем младшие байты.

Внутри байта биты нумеруются от одного до восьми, где восьмой бит является старшим значащим битом (MSB), а первый бит — младшим значащим битом (LSB).

5.3 Зарегистрированный идентификатор типа формата

Записи данных, соответствующие настоящему стандарту, могут быть включены в записи биометрических данных (ЗБД), совместимые с ЕСФОБД* (ИСО/МЭК 19785-1). В данном подразделе приведены: идентификатор владельца формата блока биометрических данных (ББД) и идентификатор типа формата ББД, которые должны быть использованы при включении в ЗБД, совместимой с ЕСФОБД. Указанные идентификаторы регистрируются МАБП**, являющимся регистрационным органом ЕСФОБД (см. ИСО/МЭК 19785-2).

Владельцем форматов, определенных в комплексе стандартов ИСО/МЭК 19794 (ИСО/МЭК 19794), является ИСО/МЭК СТК 1/ПК 37, зарегистрированный идентификатор владельца формата 257 (0x0101). Идентификатор типа формата для формата, определенного в настоящем стандарте, приведен в таблице 1.

Таблица 1 — Идентификатор типа формата

Идентификатор типа формата ББД ЕСФОБД	Короткое имя	Полный идентификатор объекта
16 (0x0010)	signature-sign-processed-dynamic	{iso(1) registration-authority(1) CBEFF (19785) organization(0) jtc1-sc37(257) bdbs(0) signature-sign-processed-dynamic (16)}

6 Отношения форматов данных

Формат данных, определенный в настоящем стандарте, не обязательно используется в чистом виде в алгоритмах анализа динамики подписи при анализе признаков подписи. Информация, записываемая в формат данных в структурированном виде, является достаточной для определения различных признаков подписи для целого ряда алгоритмов. Блок-схема применения формата представлена на рисунке 1.

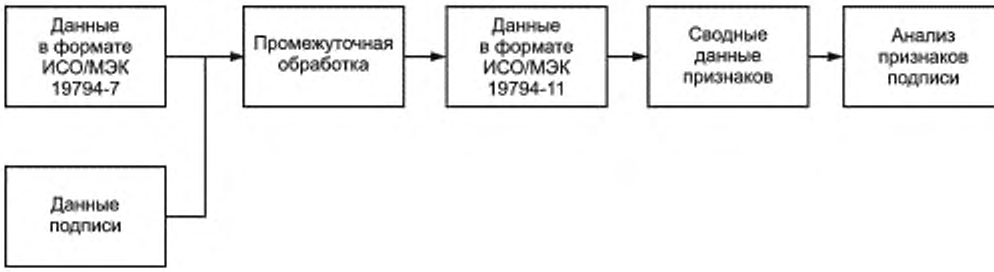

Рисунок 1 — Блок-схема применения формата

7 Записываемые данные подписи

7.1 Общие положения

Запись данных динамических событий в виде значимых динамических событий («касание пера», «отрыв пера» и «точка поворота») позволяет объединять события в сегменты и/или экстраполировать их на всю последовательность образцов подписи для последующего анализа признаков.

Данные динамики подписи должны быть записаны в виде последовательности блоков «Данные динамического события» для каждого значимого динамического события, за которым следует сводные данные признаков.

---

* ЕСФОБД — Единая структура форматов обмена биометрическими данными (Common biometric exchange formats framework (CBEFF)).

** МАБП — Международная ассоциация биометрической промышленности (International Biometric Industry Association (IBIA)).

7.2 Данные динамического события

Для любого динамического события, такого как:
a) касание пера,
b) отрыв пера,
c) точка поворота,
должны быть записаны координаты (*X* и *Y*), сила нажатия пера (*F*), время (*T*) и тип события.

7.2.1 Касание пера

Касание пера — событие, начиная с которого перо касается рабочей поверхности биометрического сканера подписи. Касание пера фиксируется при следующем условии для канала *F*:

$(F_{n-1} = 0)$ и $(F_n > 0)$

7.2.2 Отрыв пера

Отрыв пера — событие, начиная с которого перо отрывается от рабочей поверхности биометрического сканера подписи. Отрыв пера фиксируется при следующем условии для канала *F*:

$(F_{n-1} > 0)$ и $(F_n = 0)$

7.2.3 Точка поворота

Точка поворота — событие, когда меняется знак направления, полученного из близлежащих отсчетов одного из каналов *X*, *Y* или *F*; для обозначения отсчетов канала используется символ *Q*. Определяются два типа точек поворота:

Тип-1: изменение положительного направления на нуль (zero) или отрицательное (negative), в этом случае точка поворота канала *Q* фиксируется при следующих условиях:

$(\text{sign}^*(Q_{n-1} - Q_{n-2}) = \text{sign}(Q_n - Q_{n-1}) = \text{positive})$ и

$(\text{sign}\,(Q_{n+2} - Q_{n+1}) = \text{sign}(Q_{n+1} - Q_n) = \text{zero или negative})$,

или

$(\text{sign}\,(Q_{n-1} - Q_{n-2}) = \text{sign}(Q_n - Q_{n-1}) = \text{zero})$ и

$(\text{sign}\,(Q_{n+2} - Q_{n+1}) = \text{sign}(Q_{n+1} - Q_n) = \text{negative})$,

где Q_n — точка поворота канала *Q*.

Тип-2: изменение отрицательного направления на нуль (zero) или положительное (positive), в этом случае точка поворота канала *Q* фиксируется при следующих условиях:

$(\text{sign}\,(Q_{n-1} - Q_{n-2}) = \text{sign}(Q_n - Q_{n-1}) = \text{negative})$ и

$(\text{sign}\,(Q_{n+2} - Q_{n+1}) = \text{sign}(Q_{n+1} - Q_n) = \text{zero или positive})$,

или

$(\text{sign}\,(Q_{n-1} - Q_{n-2}) = \text{sign}(Q_n - Q_{n-1}) = \text{zero})$ и

$(\text{sign}\,(Q_{n+2} - Q_{n+1}) = \text{sign}(Q_{n+1} - Q_n) = \text{positive})$,

где Q_n — точка поворота канала *Q*.

До вычисления знака направления, полученного из близлежащих отсчетов, значения каналов *X*, *Y* и *F* должны быть сглажены с помощью фильтра скользящего среднего из *M* точек (*M* должно быть нечетным числом) согласно формуле

$$Q_i = \frac{1}{M} \sum_{m=-\frac{M-1}{2}}^{\frac{M-1}{2}} Q_i + m,$$

где Q_i — *i*-тый отсчет канала *Q*.

---

* Функция знака числа; возвращает значение плюс 1 для положительного числа, значение 0 для числа нуль, и значение минус 1 для отрицательного числа.

Единицей измерения *X* и *Y* является миллиметр (мм), *F* — Ньютон (Н), *T* — миллисекунда (мс). Для восстановления исходных значений целочисленные значения, указанные в записи, необходимо разделить на значения масштаба, указанные в блоке «Заголовок представления». Выбирая соответствующие значения масштаба, можно получить различные разрешения для разных приложений.

7.3 Сводные данные признаков

Дополнительными параметрами, которые должны быть записаны для полного анализа динамики подписи, являются:

a) Общее время

Общее время *T* определяется как разница во времени между первым и последним зафиксированными временными отсчетами подписи.

Единицей измерения является миллисекунда (мс).

Для восстановления исходного значения целочисленное значение, указанное в поле «Общее время» (Total time), необходимо разделить на значение масштаба *T*, указанное в блоке «Заголовок представления».

b) Расчетное общее число точек (ОЧТ) (является функцией времени и разрешения биометрического сканера подписи)

Измеренное общее число точек определяется как число координат подписи, записанных в виде целого числа.

c) Средние значения

$X_{ср}$ — среднее значение координаты *X*.

$Y_{ср}$ — среднее значение координаты *Y*.

$F_{ср}$ — среднее значение силы нажатия *F*.

$X_{ср}$, $Y_{ср}$, и $F_{ср}$ являются среднеарифметическими значениями координаты *X*, координаты *Y* и силы нажатия *F*, когда перо касается биометрического сканера подписи.

Единицей измерения $X_{ср}$ и $Y_{ср}$ является миллиметр (мм). Единицей измерения $F_{ср}$ является Ньютон (Н).

Для восстановления исходных значений целочисленные значения в полях «Среднее значение *X*» (*X* mean value) и «Среднее значение *Y*» (*Y* mean value) необходимо разделить соответственно на значения масштаба *X* и *Y*, указанные в блоке «Заголовок представления».

d) Стандартные отклонения

S_X — стандартное отклонение координаты *X*.

S_Y — стандартное отклонение координаты *Y*.

S_F — стандартное отклонение силы нажатия *F*.

Стандартное отклонение рассчитывается по формуле

$$S=\sqrt{\frac{\sum(v-m)^2}{n}}$$

где v — отсчеты координаты *X*, координаты *Y* и силы нажатия *F*,

m — среднеарифметические значения координаты *X*, координаты *Y* и силы нажатия *F*,

n — число отсчетов.

Единицей измерения S_X и S_Y является миллиметр (мм). Единицей измерения S_F является Ньютон (Н).

Для восстановления исходных значений целочисленные значения в полях «Стандартное отклонение *X*» (*X* standard deviation value) и «Стандартное отклонение *Y*» (*Y* standard deviation value) необходимо разделить соответственно на значения масштаба *X* и *Y*, указанные в блоке «Заголовок представления».

e) Коэффициент корреляции

R_{xy} — 1000 x (1 + коэффициент корреляции между *X* и *Y* с тремя значащими разрядами).

Коэффициент корреляции всегда положительный.

Коэффициент корреляции между X и Y рассчитывается по формуле

$$R = \frac{n \cdot \sum_i (x_i \cdot y_i) - \sum_i x_i \cdot \sum_i y_i}{\sqrt{(n \cdot \sum_i x_i^2 - (\sum_i x_i)^2) \cdot (n \cdot \sum_i y_i^2 - (\sum_i y_i)^2)}}$$

где n — число отсчетов.

8 Формат записи обрабатываемых данных динамики подписи

8.1 Общие положения

Настоящий стандарт определяет структуру записи обрабатываемых данных динамики подписи. Каждая запись должна относиться к одному субъекту и содержать не менее одного представления подписи. Структура записи организована следующим образом:

a) блок «Общий заголовок» фиксированной длины (15 байтов), содержащий информацию о записи;

b) тело* представления, содержащее отдельную запись обрабатываемых данных динамики подписи для каждого представления подписи и состоящее из:

i) блока «Заголовок представления» переменной длины, относящийся к отдельному представлению;

ii) последовательности блоков «Данные динамического события» и «Сводные данные признаков», относящихся к отдельному представлению;

iii) необязательного блока «Дополнительные данные» (см. 8.7).

8.2 Блок «Общий заголовок» (General header)

Структура блока «Общий заголовок» приведена в таблице 2.

Таблица 2 — Блок «Общий заголовок»

Поле	Длина, байт	Комментарий
Идентификатор формата (Format identifier)	4	Идентификатор формата должен быть записан тремя символами «SPD» в нуль-терминированной строке
Номер версии стандарта (Version number)	4	Номер версии стандарта должен быть записан в нуль-терминированной строке с тремя символами ASCII. Первый и второй символы обозначают номер версии стандарта, третий символ — номер поправки или изменения данной редакции. Настоящая версия стандарта имеет номер «010» — номер версии 1, номер редакции 0
Длина записи (Length of record)	4	Поле «Длина записи» должно содержать значение полной длины ЗОБД в байтах. Полную длину ЗОБД определяют как сумму длин блока «Общий заголовок» и всех записей представлений
Число представлений (Number of representations)	2	В поле «Число представлений» должно быть указано общее число представлений, включенных в ЗОБД. Обязательным является наличие минимум одного представления
Сертификационный флаг (Certification flag)	1	Поле «Сертификационный флаг» указывает на наличие блока «Сертификация» в каждом блоке «Заголовок представления». Значение 0x00 указывает на то, что ни одно из представлений не содержит блоков «Сертификация». Примечание — Поле «Сертификационный флаг» добавлено для обеспечения совместимости с будущими версиями форматов записи, в которых блоки «Заголовок представление» могут содержать блоки «Сертификация».

* В настоящем стандарте термин «тело» обозначает внутреннюю часть информационного объекта.

8.3 Блок «Заголовок представления» (Representation header)

8.3.1 Общие положения

Структура блока «Заголовок представления» приведена в таблицах 3 и 6.

Таблица 3 — Блок «Заголовок представления»

Поле	Длина, байт	Комментарий
Длина представления (Representation length)	4	Поле «Длина представления» должно содержать значение длины представления в байтах, включая длину полей блока «Заголовок представления»
Дата и время регистрации (Capture date and time)	9	Поле «Дата и время регистрации» должно содержать дату и время регистрации данного представления по Гринвичу (универсальное глобальное время). Значения данного поля должны быть закодированы в соответствии с требованиями ИСО/МЭК 19794-1
Идентификатор технологии биометрического сканера подписи (Capture device technology identifier)	1	Поле «Идентификатор технологии биометрического сканера» должно содержать класс технологии, используемой биометрическим сканером подписи для регистрации биометрического образца. Если технология неизвестна или не определена, то должно быть установлено значение 0x00. Допустимые значения приведены в таблице 4
Идентификатор изготовителя биометрического сканера подписи (Capture device vendor identifier)	2	Поле «Идентификатор изготовителя биометрического сканера подписи» должно содержать информацию о биометрической организации, являющейся владельцем продукта, производящего ЗОБД. Идентификатор изготовителя биометрического сканера подписи* должен быть закодирован в двух байтах и включать идентификатор организации-участника ЕСФОБД (зарегистрированный МАБП или другим разрешенным регистрационным органом). Если данное поле содержит нули, то изготовитель биометрического сканера подписи не определен
Идентификатор типа биометрического сканера подписи (Capture device type identifier)	2	Поле «Идентификатор типа биометрического сканера подписи» должно содержать информацию о типе продукта, создающего ЗОБД. Тип продукта определяется владельцем зарегистрированного продукта или другим разрешенным регистрационным органом. По возможности зарегистрированные типы продукта должны включать все допустимые комбинации планшета и пера как единого продукта. Если данное поле содержит нули, то тип биометрического сканера подписи не определен. Если идентификатор изготовителя биометрического сканера подписи равен 0x0000, то идентификатор типа биометрического сканера подписи также должен быть равен 0x0000
Запись данных о качестве (блоки «Качество») (Quality record)	От 1 до *n*	Запись данных о качестве должна состоять из поля «Число блоков «Качество» (1 байт), за которым следуют блоки «Качество» (если они имеются). В поле «Число блоков «Качество» должно быть указано число блоков «Качество» в виде целого числа без знака. Каждый блок «Качество» должен состоять из полей: - «Показатель качества», - «Идентификатор разработчика алгоритма оценки качества», - «Идентификатор алгоритма оценки качества». Поле «Показатель качества» (1 байт) должно определять количественное выражение расчетных эксплуатационных характеристик биометрического образца. Допустимыми значениями для показателя качества являются целые числа в диапазоне от 0 до 100, где бóльшие значения отражают более высокое качество. Значение 255 (0xFF) — неудачная попытка вычисления показателя качества.

* В оригинале стандарта ИСО/МЭК 19794-11:2013 допущена ошибка — вместо термина «Capture device vendor identifier» указан термин «Capture device algorithm vendor identifier».

Окончание таблицы 3

Поле	Длина, байт	Комментарий
		Поле «Идентификатор разработчика алгоритма оценки качества» должно содержать информацию об организации, предоставившей алгоритм оценки качества. Идентификатор разработчика алгоритма оценки качества должен быть закодирован в двух байтах и включать в себя идентификатор организации-участника ЕСФОБД (зарегистрированный МАБП или другим разрешенным регистрационным органом). Если данное поле содержит нули, то разработчик алгоритма оценки качества не определен. Поле «Идентификатор алгоритма оценки качества» (2 байта) определяет целочисленный код продукта, указанный разработчиком алгоритма оценки качества. Данное поле показывает, какой из алгоритмов (включая номер версии алгоритма) используется при вычислении показателя качества. Идентификатор алгоритма оценки качества должен быть зарегистрирован МАБП или другим разрешенным регистрационным органом. Если данное поле содержит нули, то алгоритм оценки качества не определен

8.3.2 Поле «Идентификатор технологии биометрического сканера подписи» (Capture device technology identifier)

Таблица 4 — Идентификатор технологии биометрического сканера подписи

Наименование	Длина, байт	Класс технологии
Идентификатор технологии биометрического сканера подписи	1	Значение поля «Идентификатор технологии биометрического сканера подписи» должно быть закодировано в 1 байте. Допустимыми значениями являются: - 0x00 — неизвестно или не определено, - 0x01 — электромагнитная технология, - 0x02 — полупроводниковая технология, - 0x04 — специальное перо с датчиками ускорения, - 0x08 — специальное перо с оптическими датчиками. Все остальные значения зарезервированы ПК37 для будущего использования

8.3.3 Запись данных о качестве (Quality record)

В соответствии с настоящим стандартом должно поддерживаться переменное число блоков «Качество» (Quality blocks) для каждого представления (рисунок 2). Каждый показатель качества должен быть закодирован в 5-байтовом блоке «Качество» (Quality block). Структура записи данных о качестве приведена в таблице 5.

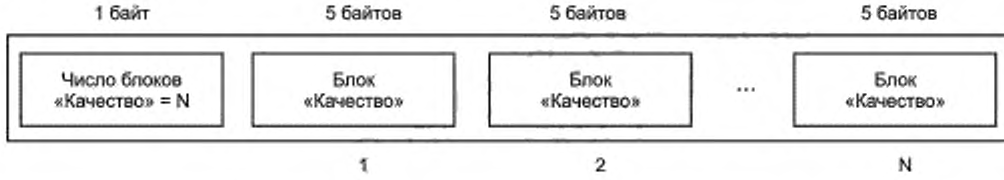

Рисунок 2 — Поддержка переменного числа блоков «Качество»

Таблица 5 — Структура записи данных о качестве

Наименование		Длина, байт	Допустимые значения	Примечание
Число блоков «Качество» (Number of quality blocks)		1	От 0 до 255	Поле «Число блоков «Качество» должно содержать число 5-байтовых блоков «Качество», следующих за данным полем. Значение 0 означает, что оценка качества не проводилась; соответственно, блоки «Качество» отсутствуют
Блок «Качество» (Quality Block)	Показатель качества (Quality score)	1	От 0 до 100, 255	0: минимальное значение показателя качества; 100: максимальное значение показателя качества; 255: неудачная попытка расчета показателя качества
	Идентификатор разработчика алгоритма оценки качества (Quality algorithm vendor ID)	2	От 0x0000 до 0xFFFF	Идентификатор разработчика алгоритма оценки качества должен быть зарегистрирован МАБП или другим разрешенным регистрационным органом как идентификатор организации-участника ЕСФОБД. Процедуры регистрации установлены в ИСО/МЭК 19785-2. Если данное поле содержит нули, то разработчик алгоритма оценки качества не определен
	Идентификатор алгоритма оценки качества (Quality algorithm ID)	2	От 0x0000 до 0xFFFF	Идентификатор алгоритма оценки качества должен быть зарегистрирован МАБП или другим разрешенным регистрационным органом как идентификатор организации-участника ЕСФОБД. Процедуры регистрации установлены в ИСО/МЭК 19785-2. Если данное поле содержит нули, то алгоритм оценки качества не определен

В соответствии с ИСО/МЭК 29794-1 поле «Показатель качества» определяет количественное выражение расчетных эксплуатационных характеристик биометрического образца. Допустимыми значениями для показателя качества являются целые числа в диапазоне от 0 (минимальное значение показателя качества) до 100 (максимальное значение показателя качества). Если при вычислении значения показателя качества произошла ошибка, то должно быть установлено значение 255. Данное значение показателя качества гармонизировано с ИСО/МЭК 19784-1, где значению 255 соответствует значение минус 1.

Примечание 1 — В стандартах БиоАПИ, в отличие от стандартов ИСО/МЭК 19794, используются целые числа со знаком.

Значение поля «Идентификатор разработчика алгоритма оценки качества» (2 байта) должно однозначно определять разработчика алгоритма оценки качества, чтобы обеспечить пользователю возможность различать оценки качества, сформированные различными алгоритмами. Идентификатор должен быть зарегистрирован МАБП или другим разрешенным регистрационным органом.

Поле «Идентификатор алгоритма оценки качества» (2 байта) определяет целочисленный код продукта, указанный разработчиком алгоритма оценки качества. Данное поле показывает, какой из алгоритмов разработчика (включая номер версии) был использован для вычисления показателя качества; значение поля должно быть в диапазоне от 1 до 65535.

Примечание 2 — Не допускается указывать в одном представлении несколько показателей качества, рассчитанных с использованием одного алгоритма (одинаковые идентификаторы разработчика и алгоритма).

8.3.4 Блок «Заголовок представления»

Таблица 6 — Блок «Заголовок представления»

Наименование	Длина, байт	Допустимые значения	Примечание
Значение масштаба *X* (*X* scaling value)	2	Экспонента: от 0x00 до 0x1F Дробь: от 0x00 до 0x7FF	Значение масштаба *X* должно быть записано в двух байтах. Пять старших битов первого байта должны определять экспоненту *E*, а оставшиеся 11 битов — дробь F_d*. Значение экспоненты *E* в виде целого числа без знака определяет степень по основанию 2 для значения масштаба, смещенную на 16. Допустимыми значениями являются целые числа от минус 16 до плюс 15. Для кодирования значения экспоненты к числу прибавляется 16, чтобы обеспечить представление в виде целого числа без знака. Для декодирования значения экспоненты из значения поля необходимо вычесть 16. Дробь F_d записывается в битовом поле, которое в двоичном представлении лежит с правой стороны от запятой мантиссы значения масштаба. Мантисса должно иметь значение в диапазоне 1 ≤ мантисса < 2. Значение масштаба рассчитывается по формуле $$s = \left(1 + \frac{F_d}{2^{11}}\right) \cdot 2^{E-16}.$$ Значение масштаба должно быть в диапазоне от 2^{-16} до $(1+2047/2048) \cdot 2^{15}$, то есть от 0,0000152587890625 до 65520. ***Пример: s = 1 при E = 16 и F_d = 0.*** Если значение масштаба неизвестно, значение поля должно содержать 0x00
Значение масштаба *Y* (*Y* scaling value)	2	Экспонента: от 0x00 до 0x1F Дробь: от 0x00 до 0x7FF	Значение масштаба *Y* должно быть записано в двух байтах. Пять старших битов первого байта должны определять экспоненту *E*, а оставшиеся 11 битов — дробь F_d. Значение экспоненты *E* в виде целого числа без знака определяет степень по основанию 2 для значения масштаба, смещенную на 16. Допустимыми значениями являются целые числа от минус 16 до плюс 15. Для кодирования значения экспоненты к числу прибавляется 16, чтобы обеспечить представление в виде целого числа без знака. Для декодирования значения экспоненты из значения поля необходимо вычесть 16. Дробь F_d записывается в битовом поле, которое в двоичном представлении лежит с правой стороны от запятой мантиссы значения масштаба. Мантисса должно иметь значение в диапазоне 1 ≤ мантисса < 2. Значение масштаба рассчитывается по формуле $$s = \left(1 + \frac{F_d}{2^{11}}\right) \cdot 2^{E-16}.$$

* Обозначение дроби F_d отличается от использованного обозначения в оригинале стандарта ИСО/МЭК 19794-11:2013 и введено для различия с обозначением силы нажатия *F*.

Продолжение таблицы 6

Наименование	Длина, байт	Допустимые значения	Примечание
			Значение масштаба должно быть в диапазоне от 2^{-16} до $(1+2047/2048) \cdot 2^{15}$, то есть от 0,0000152587890625 до 65520. ***Пример: s = 1 при E = 16 и F_d = 0.*** Если значение масштаба неизвестно, значение поля должно содержать 0x00
Значение масштаба *T* (*T* scaling value)	2	Экспонента: от 0x00 до 0x1F Дробь: от 0x00 до 0x7FF	Значение масштаба *T* должно быть записано в двух байтах. Пять старших битов первого байта должны определять экспоненту *E*, а оставшиеся 11 битов — дробь F_d. Значение экспоненты *E* в виде целого числа без знака определяет степень по основанию 2 для значения масштаба, смещенную на 16. Допустимыми значениями являются целые числа от минус 16 до плюс 15. Для кодирования значения экспоненты к числу прибавляется 16, чтобы обеспечить представление в виде целого числа без знака. Для декодирования значения экспоненты из значения поля необходимо вычесть 16. Дробь F_d записывается в битовом поле, которое в двоичном представлении лежит с правой стороны от запятой мантиссы значения масштаба. Мантисса должно иметь значение в диапазоне 1 ≤ мантисса < 2. Значение масштаба рассчитывается по формуле $$s = \left(1 + \frac{F_d}{2^{11}}\right) \cdot 2^{E-16}.$$ Значение масштаба должно быть в диапазоне от 2^{-16} до $(1+2047/2048) \cdot 2^{15}$, то есть от 0,0000152587890625 до 65520. ***Пример: s = 1 при E = 16 и F_d = 0.*** Если значение масштаба неизвестно, значение поля должно содержать 0x00
Значение масштаба *F* (*F* scaling value)	2	Экспонента: от 0x00 до 0x1F Дробь: от 0x00 до 0x7FF	Значение масштаба F_d должно быть записано в двух байтах. Пять старших битов первого байта должны определять экспоненту *E*, а оставшиеся 11 битов — дробь F_d. Значение экспоненты *E* в виде целого числа без знака определяет степень по основанию 2 для значения масштаба, смещенную на 16. Допустимыми значениями являются целые числа от минус 16 до плюс 15. Для кодирования значения экспоненты к числу прибавляется 16, чтобы обеспечить представление в виде целого числа без знака. Для декодирования значения экспоненты из значения поля необходимо вычесть 16.

Окончание таблицы 6

Наименование	Длина, байт	Допустимые значения	Примечание
			Дробь F_d записывается в битовом поле, которое в двоичном представлении лежит с правой стороны от запятой мантиссы значения масштаба. Мантисса должно иметь значение в диапазоне 1 ≤ мантисса < 2. Значение масштаба рассчитывается по формуле $$s = \left(1 + \frac{F_d}{2^{11}}\right) \cdot 2^{E-16}.$$ Значение масштаба должно быть в диапазоне от 2^{-16} до $(1+2047/2048) \cdot 2^{15}$, то есть от 0,0000152587890625 до 65520. ***Пример: s = 1 при E = 16 и F_d = 0.*** Если значение масштаба неизвестно, значение поля должно содержать 0x00
Число блоков «Данные динамического события» (Number of Dynamic-event data records)	4	От 0x01 до 0xFFFFFFFF	Значение поля должно определять общее число блоков «Данные динамического события» в представлении подписи
Число элементов фильтра скользящего среднего (Number of samples for moving average filter)	1	От 0x1 до 0xFF	Число элементов фильтра скользящего среднего. M должно быть нечетным числом. $$Q_i = \frac{1}{M} \sum_{m=-\frac{M-1}{2}}^{\frac{M-1}{2}} Q_{i+m}$$

8.4 Блок «Данные динамического события» (Dynamic-event data)

Каждое динамическое событие подписи должно быть внесено в блок «Данные динамического события». Структура блока «Данные динамического события» приведена в таблице 7. Записываются события точек поворота в плоскостях X и Y (при наличии данных, даже если перо не касается рабочей поверхности биометрического сканера подписи), касания пера и отрыва пера, а также при наличии данных о силе нажатия, дополнительно записываются точки поворота в канале F.

Таблица 7 — Блок «Данные динамического события»

Наименование	Длина, байт	Допустимые значения	Примечание
X	2	От 0x0 до 0xFFFF	Координаты X должны быть записаны в двух байтах. Допустимыми значениями являются целые числа от минус 32768 до плюс 32767, которые должны быть закодированы в виде целого числа без знака после добавления 32768 к каждому значению. Для положительных значений бит 8 старшего байта должен иметь значение 1, а для отрицательных значений — значение 0. Для декодирования нужно вычесть число 32768 из записанных значений

Окончание таблицы 7

Наименование	Длина, байт	Допустимые значения	Примечание
Y	2	От 0x0 до 0xFFFF	Координаты *Y* должны быть записаны в двух байтах. Допустимыми значениями являются целые числа от минус 32768 до плюс 32767, которые должны быть закодированы в виде целого числа без знака после добавления 32768 к каждому значению. Для положительных значений бит 8 старшего байта имеет значение 1, а для отрицательных значений — значение 0. Для декодирования нужно вычесть число 32768 из записанных значений
F	2	От 0x0 до 0xFFFF	Сила нажатия должна быть записана в двух байтах. Допустимыми значениями являются целые числа от 0 до 65535, которые должны быть закодированы в виде целого числа без знака. Если измерение силы нажатия не проводится, значение поля должно быть равно 0
T	2	От 0x0 до 0xFFFF	Время должно быть записано в двух байтах. Допустимыми значениями являются целые числа от 0 до 65535, которые должны быть закодированы в виде целого числа без знака
Тип события (Type of Event)	1	От 0x0 до 0x1F	Тип события должен быть записан в одном байте, где: Бит 1 — отрыв пера, Бит 2 — касание пера, Бит 3 — точка поворота в канале *X*, Бит 4 — точка поворота в канале *Y*, Бит 5 — точка поворота в канале *F*, Бит 6 — тип точки поворота в канале *X*, Бит 7 — тип точки поворота в канале *Y*, Бит 8 — тип точки поворота в канале *F*. В случае если все события произошли одновременно, значение данного поля должно быть равно 1. Типы точек поворота кодируются значением 0 для «Тип-1» и значением 1 для «Тип-2»

8.5 Блок «Сводные данные признаков» (Overall feature data)

Таблица 8 — Блок «Сводные данные признаков»

Наименование	Длина, байт	Допустимые значения	Примечание
Общее время (Total time)	2	От 0x0 до 0xFFFF	Общее время должно быть записано в двух байтах. Допустимыми значениями являются целые числа от 0 до 65535, которые должны быть закодированы в виде целого числа без знака
$X_{ср}$ (X_{mean})	2	От 0x0 до 0xFFFF	Среднее значение координаты *X* должно быть записано в двух байтах. Допустимыми значениями являются целые числа от минус 32768 до плюс 32767, которые должны быть закодированы в виде целого числа без знака после добавления 32768 к каждому значению. Для положительных значений бит 8 старшего байта должен иметь значение 1, а для отрицательных значений — значение 0. Для декодирования нужно вычесть число 32768 из записанных значений

Окончание таблицы 8

Наименование	Длина, байт	Допустимые значения	Примечание
$Y_{ср}$ (Y_{mean})	2	От 0x0 до 0xFFFF	Среднее значение координаты *Y* должно быть записано в двух байтах. Допустимыми значениями являются целые числа от минус 32768 до плюс 32767, которые должны быть закодированы в виде целого числа без знака после добавления 32768 к каждому значению. Для положительных значений бит 8 старшего байта должен иметь значение 1, а для отрицательных значений — значение 0. Для декодирования нужно вычесть число 32768 из записанных значений
$F_{ср}$ (F_{mean})	2	От 0x0 до 0xFFFF	Среднее значение силы нажатия *F* должно быть записано в двух байтах. Допустимыми значениями являются целые числа от 0 до 65535, которые должны быть закодированы в виде целого числа без знака
Стандартное отклонение *X* (Standard deviation *X*)	2	От 0x0 до 0xFFFF	Стандартное отклонение координаты *X* должно быть записано в двух байтах. Допустимыми значениями являются целые числа от 0 до 65535, которые должны быть закодированы в виде целого числа без знака
Стандартное отклонение *Y* (Standard deviation *Y*)	2	От 0x0 до 0xFFFF	Стандартное отклонение координаты *Y* должно быть записано в двух байтах. Допустимыми значениями являются целые числа от 0 до 65535, которые должны быть закодированы в виде целого числа без знака
Стандартное отклонение *F* (Standard deviation *F*)	2	От 0x0 до 0xFFFF	Стандартное отклонение силы нажатия *F* должно быть записано в двух байтах. Допустимыми значениями являются целые числа от 0 до 65535, которые должны быть закодированы в виде целого числа без знака
Коэффициент корреляции (Correlation coefficient)	2	От 0x1 до 0xFFFF	Коэффициент корреляции должен быть записан в двух байтах. Допустимыми значениями являются целые числа от 1 до 65535, которые должны быть закодированы в виде целого числа без знака

8.6 Блок «Дополнительные данные» (Extended data)

Поле «Длина блока «Дополнительные данные» (Extended data length) должно содержать число байтов информации, содержащейся в блоке «Дополнительные данные». Поле «Длина блока «Дополнительные данные» должно состоять из 2 байтов и представлять число байтов в виде целого числа без знака. Допустимыми значениями являются целые числа от 0 до 65535.

Необязательный блок «Дополнительные данные» позволяет включать данные, которые могут быть использованы алгоритмами сравнения. В настоящем стандарте требования к структуре блока «Дополнительные данные» не установлены. Если при наличии дополнительных данных они не распознаются алгоритмом сравнения, то они должны быть пропущены.

Примечание — Алгоритмы сравнения, обрабатывающие данные в формате настоящего стандарта, должны демонстрировать одинаковые показатели работы при обработке данных с наличием и отсутствием дополнительных данных. Если дополнительные данные присутствуют, а в алгоритме сравнения они не требуются, то они должны быть пропущены.

Приложение А
(обязательное)

Методология испытаний на соответствие

Настоящий стандарт определяет формат биометрических данных для хранения, записи и передачи одного или более представлений подписи. Каждое представление подписи сопровождается определенными метаданными, записанными в заголовке записи. Настоящее приложение определяет порядок проведения испытания для проверки корректности записи.

Цель настоящего стандарта не может быть в полной мере достигнута, пока биометрические продукты не пройдут испытания на соответствие требованиям настоящего стандарта. Соответствие реализаций требованиям является необходимым условием для обеспечения взаимодействия между реализациями, поэтому существует необходимость в стандартизированной методологии испытаний на соответствие, тестовых утверждениях и методиках испытаний применительно к конкретным биометрическим модальностям, которые рассмотрены в стандартах комплекса ИСО/МЭК 19794. Тестовыми утверждениями проверяется большинство требований настоящего стандарта, и соответствие результатов, полученных с помощью комплектов для проведения испытаний на соответствие, будет показывать степень соответствия реализаций настоящему стандарту. Все это является стимулирующим фактором для разработки данной методологии испытаний на соответствие.

Настоящее приложение предназначено для определения элементов методологии испытаний на соответствие, тестовых утверждений и методик испытаний применительно к настоящему стандарту.

Приложение В
(справочное)

Спецификация ACH.1 для формата данных

В.1 Абстрактный синтаксис кодирования данных динамики подписи

Настоящий стандарт определяет битовое представление формата записи обрабатываемых данных динамики подписи, что является удобным для передачи и/или хранения.

Целесообразно определить также информационное наполнение формата независимо от битового представления (абстрактный синтаксис), что позволит:

a) использовать различные виды кодирования информации (например, XML кодирование);

b) использовать различные представления в ядре операционной системы с применением структур, удобных для обработки на языках программирования C, C++ или Java;

c) использовать более широкий ряд инструментов в реализациях данных форматов;

d) упростить представления в ядре операционной системы биометрических сканеров подписи, которые не имеют архитектуры аппаратных средств с обратным порядком следования байтов;

e) более понятно описать значения в форматах.

В данном приложении абстрактный синтаксис определен с использованием ACH.1 (ИСО 8824-1 [1]). Стандартные виды кодирования обрабатываемых данных динамики подписи получаются путем применения к модулям ACH.1 (см. B.2*) правил основного уплотненного кодирования без выравнивания (BASIC-PER, см. ИСО 8825-2 [2]), включая дополнительные правила по уплотненному кодированию (PER).

При использовании абстрактного синтаксиса в качестве схемы, возможны преобразования между любыми закодированными значениями и представлениями в ядре операционной системы при любой архитектуре аппаратных средств и для любого языка программирования. Инструменты, которые преобразуют эти спецификации в структуры языка программирования, называются компиляторами ACH.1 и поддерживаются исполнительными программами, которые будут выполнять преобразования между представлениями в ядре операционной системы и любым кодированием, описанным в комплексе стандартов ИСО/МЭК 8825 (включая XML кодирование). Такие инструменты поддерживаются многими изготовителями и разработчиками. В частности, инструменты, которые выполняют преобразования между стандартными закодированными обрабатываемыми данными динамики подписи и представлениями в ядре операционной системы, являются доступными для большинства архитектур аппаратных средств и большинства языков программирования.

В.2 Формат обрабатываемых данных динамики подписи

```
Signature/signSignDynamicFormatModule
   {iso standard 19794 signature/sign-sign-processed-dynamic(11) modules(0) version(0)}
   DEFINITIONS
   PER INSTRUCTIONS
   -- Определение применяемых правил к уплотненному кодированию (PER)
   AUTOMATIC TAGS ::=
   BEGIN
Signature/signSignDynamicBlock ::= SEQUENCE {
   header GeneralHeader,
   body Body }
GeneralHeader ::= SEQUENCE {
   formatId [NULL] IA5String ("SPD"),
   standardVersion [NULL] IA5String (SIZE (3)),
   -- " 10" (space-one-zero) for this version
   lengthofRecord [SIZE 32]INTEGER,
   numberofRepresentations [SIZE 16]INTEGER,
   certificationFlag [SIZE 8]INTEGER}
Body ::= SEQUENCE {
   representation RepresentationHeaderValues,
   RepresentationBodyValues}
RepresentationHeaderValues ::= SEQUENCE {
   RepresentationLength* [SIZE 32] INTEGER (1..MAX)
   captureDateTime CaptureDateTimeValues,
```

---

* В оригинале стандарта ИСО/МЭК 19794-11:2013 допущена опечатка — вместо раздела B.2 указан раздел A.2.

```
    captureDeviceTechId INTEGER (0..255),
    captureDeviceVendId INTEGER (0..65535),
    captureDeviceTypeId INTEGER (0..65535),
    qualityRecord QualityBlockValues,
    certificationRecord INTEGER (0),
    xchannelScaling ScalingValue,
    ychannelScaling ScalingValue,
    tchannelScaling ScalingValue,
    fchannelScaling ScalingValue,
    numberofDynamicEvents [SIZE 32] INTEGER (1..MAX)
    numberofAveragingSamples INTEGER (1..255)}
CaptureDateTimeValues ::= OCTETSTRING (SIZE (9))
-- Строка октетов(Octet String) должна содержать 9 байтов, описанных в ИСО/МЭК 19794-1
QualityBlockValues ::= SEQUENCE {
    numberof Qualityblocks [SIZE 8] INTEGER (0..255),
    SEQUENCE OF {
    qualityScore [SIZE 8] INTEGER (0..100,255),
    qualityalgorithmVendId [SIZE 16] INTEGER (1..65535),
    qualityalgorithmId [SIZE 16] INTEGER (1..65535)} }
ScalingValue ::= SEQUENCE {
    exponent INTEGER (-16..15),
    fraction INTEGER (0..2047)}
    RepesentationBodyValues ::= SEQUENCE {
    DynamicEventData,
    FeatureData,
    extendedData [LENGTH 16] OCTET STRING OPTIONAL}
DynamicEventData ::= SEQUENCE {
    xCoordinate INTEGER (-32768..32767),
    yCoordinate INTEGER (-32768..32767),
    fValue INTEGER (0..65535),
    timeValue INTEGER (0..65535)
    typeofEvent [SIZE 8] INTEGER (0..255)}
FeatureData ::= SEQUENCE {
    totalTime INTEGER (0..65535),
    meanValues OverallMeanValues,
    sdValues StandardDeviation,
    cCoefficient INTEGER (1..65535) }
OverallMeanValues ::= SEQUENCE {
    meanX INTEGER (-32768..32767),
    meanY INTEGER (-32768..32767),
    meanF INTEGER (0..65535) }
StandardDeviation ::= SEQUENCE {
    sdX INTEGER (0..65535),
    sdY INTEGER (0..65535),
    sdF INTEGER (0..65535) }
END
```

Приложение С
(справочное)

Подписи, пригодные для аутентификации

В данном приложении рассмотрены показатели подписи, которые делают ее пригодной для аутентификации. Какие показатели подписи могут быть измерены для удовлетворения требований?

Известны три показателя для обеспечения эффективности:

- объем данных;
- сложность подписи;
- стабильность подписи.

С.1 Объем данных

Существует ли число оцифрованных координат, достаточное для анализа? Вопрос относительно объема данных можно было бы отнести к разрешению биометрического сканера подписи, но в данном случае более важно, как быстро человек ставит свою подпись. При слишком быстром вводе недостаточное число координат приведет к недостаточному объему данных для анализа. Обычно данная проблема возникает, когда кто-либо ставит свою подпись слишком быстро. Подпись может быть достаточно сложной и очень стабильной, но с недостаточным объемом числовых данных для работы алгоритмов анализа обрабатываемых данных динамики подписи. Такие подписи должны быть отклонены во время биометрической регистрации. Аналогичное ограничение используется в системах аутентификации по паролю, когда для обеспечения необходимого уровня безопасности устанавливается минимальное число цифр, например 7 или 8.

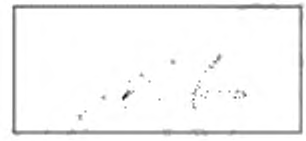

Рисунок С.1 — Пример подписи, которая является достаточно сложной, но с недостаточным объемом данных

Для анализа пригодности подписи объем данных оценивается числом записанных оцифрованных точек и проверкой соответствия его минимальному уровню.

С.2 Сложность подписи

Почему поднимается вопрос о сложности подписи? Хотя анализ динамики подписи и уменьшает вероятность подделки, необходимо иметь достаточно сложные данные. В качестве аналогии показателя сложности подписи можно рассматривать ситуацию, когда системы аутентификации отклоняют простые PIN-коды типа 1234 или 999, так как они могут быть легко подобраны, или когда пароли должны содержать буквы верхнего и нижнего регистров и/или наличие цифр или специальных символов.

Что такое сложная подпись? Легче объяснить, что такое слишком простая подпись. Очевидно, что «крестик» является слишком простой подписью. Даже с анализом динамики такая отметка-подпись является очень легко подделываемой и приводит к слишком низкому или нулевому уровню безопасности системы аутентификации.

Сложность подписи создают «петли». Именно петли обеспечивают вариабельность динамики подписи. Именно петли создают колебания скорости, ускорения, замедления, направления и т. п. Простой «крестик» не имеет петель или имеет очень малое число петлеобразных участков, что приводит к очень низкой вариабельности динамики подписи и тем самым к недостаточной сложности. Необходимо учитывать недостаточную сложность подписи. Такие подписи должны быть отклонены во время биометрической регистрации.

Для анализа пригодности подписи, объем данных оценивается числом записанных петлей и проверкой соответствия числа минимальному уровню.

С.3 Стабильность подписи

Почему необходимо проверять стабильность подписи человека? Разумеется, в основе биометрической системы с использованием подписи лежит обработка множества подписей человека. На самом деле любая биометрическая система должна обрабатывать естественные изменения, которые имеются в подписи у любого человека. Биометрическая система должна обеспечивать учет вариабельности подписи для предотвращения использования подписи мошенником. Другими словами, вариабельность снижает уровень безопасности, позволяя поддельной подписи быть ложно принятой.

Биометрическая система с использованием подписи должна обеспечивать взаимодействие с пользователем во время биометрической регистрации — или, точнее, отклонять пользователей, которые не взаимодействуют с системой во время биометрической регистрации. При биометрической регистрации должны быть отклонены предъявляемые образцы подписи в виде имен. Имена, превращенные в подписи, являются слишком изменчивыми — их вариабельность выходит за пределы нормального распределения.

Нормальное распределение лежит в основе определения стабильности подписи. Каждая характеристика динамики подписи является нормально распределенной. Любая подпись должна иметь достаточное число характеристик динамики, образующих кластеры, что обеспечивает ее уникальность и возможность верификации в системе аутентификации. Если значительная часть измеряемых и вычисляемых характеристик динамики имеют большую вариабельность или неудовлетворительную кластеризацию, то подпись должна быть признана нестабильной или слишком изменчивой во время биометрической регистрации. Если такую подпись принять во время биометрической регистрации, то это даст возможность мошенникам подделать подпись пользователя, хотя биометрическая система и сможет успешно обрабатывать очень вариабельные подлинные подписи.

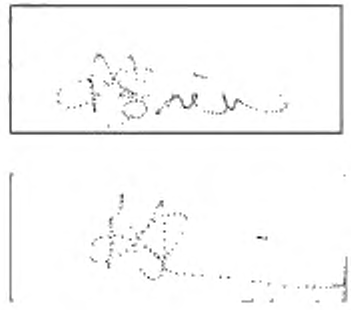

Рисунок С.2 — Пример подписи со значительной вариабельностью

Если во время биометрической регистрации среди всех зарегистрированных образцов подписи обнаружены один или два образца со значительной вариабельностью, то они могут быть отклонены как «выбросы» (резко выделяющиеся значения экспериментальных величин). Если большинство образцов или все образцы демонстрируют значительную вариабельность, то подпись должна быть отклонена как «слишком вариабельная».

Стабильность подписи является самым трудно оцениваемым показателем пригодности подписи, так как она является компромиссом между удобством использования и безопасностью. Например, компромиссом между числом регистрируемых образцов подписи и временем регистрации при продолжительном взаимодействии с пользователем. Хотя пользователь может иметь возможность во время биометрической регистрации отклонить некоторые образцы как нерепрезентативные, однако это происходит редко.

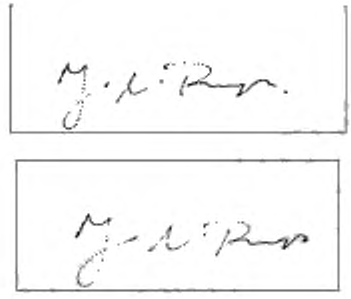

Рисунок С.3 — Пример двух пригодных образцов подписи

Непосредственное взаимодействие с пользователем очень важно для получения подписи хорошего качества. Важным элементом инструкции в биометрической системе с использованием подписи является разъяснение пользователям необходимости предоставления стабильной подписи с достаточным объемом данных и сложностью.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО/МЭК 19785-2	IDT	ГОСТ Р ИСО/МЭК 19785-2—2008 «Автоматическая идентификация. Идентификация биометрическая. Единая структура форматов обмена биометрическими данными. Часть 2. Процедуры действий регистрационного органа в области биометрии»
ИСО/МЭК 19794-1	IDT	ГОСТ ISO/IEC 19794-1—2015 «Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 1. Структура»
Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов: - IDT — идентичные стандарты.		

Библиография

[1] ISO/IEC 8824-1 Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation (Информационные технологии. Абстрактная синтаксическая нотация версии один (АСН.1). Часть 1. Спецификация основной нотации)

[2] ISO/IEC 8825-2 Information technology — ASN.1 encoding rules: Specification of Packed Encoding Rules (PER) (Информационные технологии. Правила кодирования АСН.1. Часть 2. Спецификация правил уплотненного кодирования (PER))

[3] ISO/IEC 8825-6 Information technology — ASN.1 encoding rules: Registration and application of PER encoding instructions (Информационные технологии. Правила кодирования АСН.1. Часть 6. Регистрация и применение команд кодирования PER)

[4] ISO/IEC 19794-7 Information technology — Biometric data interchange formats — Part 7: Signature/sign time series data (Информационные технологии. Форматы обмена биометрическими данными. Часть 7. Данные динамики подписи)

УДК 004.93'1:006.89:006.354 ОКС 35.040

Ключевые слова: информационные технологии, биометрия, форматы обмена биометрическими данными, обрабатываемые данные динамики подписи, динамика подписи, подпись

Редактор *Л.И. Потапова*
Технический редактор *В.Ю. Фотиева*
Корректор *И.А. Королева*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 27.01.2016. Подписано в печать 01.03.2016. Формат 60×84¼. Гарнитура Ариал.
Усл. печ. л. 3,26 Уч.-изд. л. 2,80. Тираж 33 экз. Зак. 683

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
www.gostinfo.ru gost.e-ecolog.ru

gost.e-ecolog.ru