ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 58624.2— 2019 (ИСО/МЭК 30107-2:2017)

Информационные технологии

БИОМЕТРИЯ

Обнаружение атаки на биометрическое предъявление

Часть 2

Форматы данных

(ISO/IEC 30107-2:2017, Information technology — Biometric presentation attack detection — Part 2: Data formats, MOD)

Издание официальное

Москва
Стандартинформ
2019

gost.e-ecolog.ru

Предисловие

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

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 31 октября 2019 г. № 851-ст

4 Настоящий стандарт является модифицированным по отношению к международному стандарту ИСО/МЭК 30107-2:2017 «Информационные технологии. Обнаружение атаки на биометрическое предъявление. Часть 2. Форматы данных» (ISO/IEC 30107-2:2017 «Information technology — Biometric presentation attack detection — Part 2: Data formats», 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 указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5—2012 (пункт 3.5).

Сведения о соответствии ссылочных национальных и межгосударственных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте, приведены в дополнительном приложении ДА.

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

5 ВВЕДЕН ВПЕРВЫЕ

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

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© ISO, 2017 — Все права сохраняются
© Стандартинформ, оформление, 2019

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

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Соответствие 2
5 Элементы данных 2
5.1 Общие положения 2
5.2 Входные данные ОАБП 3
5.3 Выходные данные ОАБП 5
Приложение А (справочное) Формальные спецификации 7
Приложение В (справочное) Примеры кодирования данных ОАБП 13
Приложение ДА (справочное) Сведения о соответствии ссылочных национальных и межгосударственных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте 14
Приложение ДБ (справочное) Сопоставление структуры настоящего стандарта со структурой примененного в нем международного стандарта 15

Введение

Предъявление артефакта или биометрической характеристики индивида подсистеме сбора биометрических данных с целью нарушения намеченной политики биометрической системы называется атакой на биометрическое предъявление. В серии стандартов «Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление» определены методы автоматического обнаружения атак на биометрическое предъявление (ОАБП).

Настоящий стандарт устанавливает требования к формату обмена данными результатов работы методов ОАБП. В настоящем стандарте определены значения элементов данных, используемых при создании форматов данных ОАБП (см. раздел 5), двоичного формата данных ОАБП на основе расширяемой спецификации ACH.1 (см. А.1) и текстового формата данных ОАБП с помощью описания XML-схемы (см. А.2). В приложении А определены формальные спецификации данных. В приложении В представлены примеры кодирования данных.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

БИОМЕТРИЯ

Обнаружение атаки на биометрическое предъявление

Часть 2

Форматы данных

Information technology. Biometrics. Biometric presentation attack detection. Part 2. Data formats

Дата введения — 2020—06—01

1 Область применения

Настоящий стандарт устанавливает требования к формату обмена данными результатов работы методов обнаружения атаки на биометрическое предъявление (ОАБП).

В настоящем стандарте определены двоичный формат данных и формат данных XML. Форматы обмена данными, определенные в настоящем стандарте, являются общими и могут использоваться в широком спектре областей применения. Настоящий стандарт не содержит требования, специфические для определенного приложения.

Атаки, рассмотренные в серии стандартов «Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление», направлены на биометрический сканер во время биометрического предъявления и сбора биометрических данных.

Настоящий стандарт не распространяется на другие типы атак.

Обеспечение криптографической защиты подлинности, целостности и конфиденциальности хранимых и передаваемых данных процесса ОАБП выходит за рамки области применения настоящего стандарта.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ ИСО 8601 Система стандартов по информации, библиотечному и издательскому делу. Представление дат и времени. Общие требования

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

ГОСТ ISO/IEC 19794-1 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 1. Структура

ГОСТ Р 58293 (ИСО/МЭК 19785-1:2015) Информационные технологии. Биометрия. Единая структура форматов обмена биометрическими данными. Часть 1. Спецификация элементов данных

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

ГОСТ Р ИСО/МЭК 8824-1 Информационная технология. Абстрактная синтаксическая нотация версии один (АСН.1). Часть 1. Спецификация основной нотации

ГОСТ Р ИСО/МЭК 8825-1 Информационная технология. Правила кодирования АСН.1. Часть 1. Спецификация базовых (BER), канонических (CER) и отличительных (DER) правил кодирования

ГОСТ Р ИСО/МЭК 8825-4 Информационная технология. Правила кодирования АСН.1. Часть 4. Правила XML кодирования (XER)

Издание официальное

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

3 Термины и определения

В настоящем стандарте применены термины по *ГОСТ ISO/IEC 2382-37, ГОСТ ISO/IEC 19794-1* и *ГОСТ Р 58624.1*.

4 Соответствие

Данные блока ОАБП соответствуют настоящему стандарту, если они отвечают обязательным требованиям, установленным в разделе 5 и А.1 или А.2 приложения А.

5 Элементы данных

5.1 Общие положения

Описание данных, получаемых в ходе работы подсистемы ОАБП и используемых проверяющей системой, представлено в разделе 5. Эти данные могут быть получены в любой точке системы. Следовательно, данные ОАБП, полученные для биометрического образца, могут изменяться на любом этапе сбора и последующей обработки биометрических образцов. Подсистема ОАБП использует входные данные (такие как пороги, биометрические образцы, дополнительные данные, например электрическая проводимость, коэффициент отражения света, индуктивность, ЭКГ и компоненты метода «запрос-ответ») и в результате работы получает выходные данные.

Процесс ОАБП включает в себя входные и выходные данные.

Входные данные включают в себя:

a) контекст сбора данных: биометрическая регистрация, биометрическая верификация или биометрическая идентификация;

b) уровень контроля со стороны оператора в процессе сбора;

c) текущий уровень риска, например недавняя попытка атаки;

d) категорию критериев ОАБП, то есть критерии являются общими для всех субъектов (глобальные критерии), индивидуальны для каждого субъекта или неизвестны;

e) дополнительные параметры, используемые в процессе ОАБП;

f) запросы, поставленные перед субъектом сбора данных;

g) дату и время сбора данных ОАБП;

h) идентификаторы биометрического сканера (идентификатор изготовителя биометрического сканера, идентификатор модели биометрического сканера и серийный номер биометрического сканера).

Выходные данные включают в себя:

a) элемент, указывающий на наличие данных ОАБП (помимо тех, что изначально связаны с биометрическими сигналами);

b) элемент, указывающий, было ли принято решение ОАБП, и, в случае принятого решения, абстрактное значение элемента;

c) результат ОАБП;

d) вектор результатов ОАБП;

e) расширенные данные ОАБП, связанные с биометрическим образцом;

f) идентификаторы методов ОАБП (идентификатор разработчика метода ОАБП, идентификатор метода ОАБП, идентификатор разработчика метода ОАБП с расширенными данными и идентификатор метода ОАБП с расширенными данными).

Примечание — Поскольку сбор данных биометрического образца и данных ОАБП может разделяться во времени и пространстве, выходные данные процесса ОАБП могут быть связаны не с одним полученным биометрическим образцом. Данные ОАБП могут относиться и к другим образцам, полученным в ходе текущей транзакции.

Если в записи данных содержатся физические и/или химические величины, то эти величины должны быть выражены в единицах, определенных в международной системе единиц (СИ).

5.2 Входные данные ОАБП

5.2.1 Цель сбора данных

Наличие: Необязательное

Абстрактные значения: ENROLMENT, VERIFICATION, IDENTIFICATION

Содержание: Данный элемент, при наличии, указывает цель процесса сбора данных. Абстрактное значение ENROLMENT указывает на то, что целью процесса сбора данных является биометрическая регистрация. Абстрактное значение VERIFICATION указывает на то, что целью процесса сбора данных является биометрическая верификация. Абстрактное значение IDENTIFICATION указывает на то, что целью процесса сбора данных является биометрическая идентификация.

5.2.2 Уровень контроля

Наличие: Необязательное

Абстрактные значения: UNKNOWN, CONTROLLED, ASSISTED, OBSERVED, UNATTENDED

Содержание: Данный элемент, при наличии, указывает уровень контроля процесса сбора биометрических данных со стороны лица, обслуживающего биометрическую систему. Биометрическое распознавание может выполняться в различных условиях (см. таблицу 1), начиная от контролируемых и заканчивая отсутствием лиц, обслуживающих биометрическую систему.

Таблица 1 — Режимы контроля

Абстрактное значение	Описание
UNKNOWN	Информация отсутствует
CONTROLLED	Оператор контролирует действия субъекта сбора биометрических данных с целью получения биометрических образцов
ASSISTED	Оператор может оказать помощь субъекту сбора биометрических данных, представляющему биометрические характеристики
OBSERVED	Оператор может наблюдать за работой биометрического сканера (включая дистанционное наблюдение, например видеонаблюдение), но не должен оказывать какую-либо помощь
UNATTENDED	Оператор (для наблюдения или оказания помощи) отсутствует

5.2.3 Уровень риска

Наличие: Необязательное

Абстрактные значения: Целые числа от 0 до 100

Содержание: Данный элемент, при наличии, указывает уровень риска в диапазоне значений между 0 и 100. Более низкое значение данного элемента указывает на более низкий риск, а более высокое значение — на более высокий риск. Данный элемент данных не следует включать в том случае, если уровень риска неизвестен.

Четкие требования к данному элементу данных отсутствуют, поэтому разработчики системы могут создать собственные качественные или количественные методики оценки рисков.

5.2.4 Категория критерия ОАБП

Наличие: Необязательное

Абстрактные значения: UNKNOWN, INDIVIDUAL, COMMON

Содержание: Данный элемент, при наличии, используется, чтобы различать критерии принятия решения ОАБП, характерные для отдельных субъектов сбора

биометрических данных, и критерии принятия решения ОАБП, общие для всех субъектов сбора биометрических данных. В таблице 2 представлены абстрактные значения данного элемента.

Таблица 2 — Абстрактные значения критериев ОАБП

Абстрактное значение	Описание
UNKNOWN	Критерии неизвестны
INDIVIDUAL	Критерии являются характерными для конкретного субъекта сбора биометрических данных
COMMON	Критерии являются общими для всех субъектов сбора биометрических данных

5.2.5 Параметры ОАБП

Наличие: Необязательное

Абстрактные значения: Любое печатное представление строки

Содержание: Данный элемент, при наличии, указывает любые дополнительные параметры, используемые для принятия решения ОАБП, например порог.

5.2.6 Запросы ОАБП

Наличие: Необязательное

Абстрактные значения: Одно или несколько печатных представлений строки

Содержание: Данный элемент, при наличии, указывает запросы, которые были поставлены перед субъектом сбора биометрических данных.

5.2.7 Время и дата сбора данных ОАБП

Наличие: Необязательное

Абстрактные значения: От 2000-01-01T00:00:00Z до 3000-12-31T23:59:59Z

Примечание — Для абстрактных значений даты и времени используют расширенный формат «дата — время» по *ГОСТ ИСО 8601*. Знак «*Z*» используют для указания применения UTC (Всемирное координированное время) при представлении даты и времени.

Содержание: Данный элемент, при наличии, определяет дату и время (UTC по *ГОСТ ИСО 8601*) начала сбора данных ОАБП с точностью до одной секунды.

5.2.8 Идентификатор изготовителя биометрического сканера

Наличие: Необязательное

Абстрактные значения: Целые числа от 1 до 65 535

Содержание: Данный элемент, при наличии, идентифицирует изготовителя биометрического сканера. Идентификатор изготовителя биометрического сканера, записываемый в данный элемент, должен быть присвоен регистрационным органом в области биометрии по *ГОСТ Р 58293*[*].

5.2.9 Идентификатор модели биометрического сканера

Наличие: Необязательное. Данный элемент следует включать только в том случае, если присутствует идентификатор изготовителя биометрического сканера.

Абстрактные значения: Целые числа от 1 до 65 535

Содержание: Данный элемент, при наличии, определяет модель биометрического сканера. Идентификатор модели биометрического сканера, записываемый в этот элемент данных, должен быть присвоен изготовителем биометрического сканера.

5.2.10 Серийный номер биометрического сканера

Наличие: Необязательное

Абстрактные значения: Любое печатное представление строки

Содержание: Данный элемент, при наличии, указывает конкретный биометрический сканер.

---

* Деятельность по присвоению уникальных идентификаторов биометрическим организациям, осуществляющим деятельность в Российской Федерации, и биометрическим продуктам, разрабатываемым и/или серийно выпускаемым, и/или реализуемым в Российской Федерации, а также ведение соответствующих реестров осуществляет Некоммерческое партнерство «Русское биометрическое общество», официально зарегистрированное Международной ассоциацией биометрии и идентификации (МАБИ) [The International Biometrics & Identification Association (IBIA)] в качестве ведущей организации ЕСФОБД (здесь и далее).

5.3 Выходные данные ОАБП

5.3.1 Решение ОАБП

Наличие: Необязательное

Абстрактные значения: ATTACK, NO_ATTACK, FAILURE_TO_COMPUTE

Примечание — В А.1 определены правила кодирования абстрактных значений в двоичном формате. Кодирование абстрактных значений в формате XML определено в А.2.

Содержание: Данный элемент, при наличии, указывает, была ли обнаружена подсистемой ОАБП попытка атаки на биометрическое предъявление. Абстрактное значение ATTACK указывает на то, что подсистема ОАБП обнаружила попытку атаки на биометрическое предъявление. Абстрактное значение NO_ATTACK указывает на то, что подсистема ОАБП не обнаружила попытку атаки на биометрическое предъявление. Абстрактное значение FAILURE_TO_COMPUTE указывает, что решение ОАБП не было принято.

5.3.2 Идентификатор разработчика метода ОАБП

Наличие: Необязательное

Абстрактные значения: Целые числа от 1 до 65 535

Содержание: Данный элемент, при наличии, идентифицирует разработчика метода ОАБП. Идентификатор разработчика, записываемый в данный элемент, должен быть присвоен регистрационным органом в области биометрии по *ГОСТ Р 58293*.

5.3.3 Идентификатор метода ОАБП

Наличие: Необязательное. Данный элемент данных следует включать в том случае, если присутствует идентификатор разработчика метода ОАБП.

Абстрактные значения: Целые числа от 1 до 65 535

Содержание: Данный элемент, при наличии, идентифицирует метод ОАБП. Идентификатор метода ОАБП, записываемый в этот элемент данных, должен быть присвоен разработчиком метода ОАБП.

В таблице 3 представлены идентификаторы метода ОАБП, не связанных с конкретным разработчиком. Для идентификаторов методов ОАБП, указанных в таблице 3, в качестве идентификатора разработчика метода ОАБП используется идентификатор 257 (0x0101).

Таблица 3 — Идентификаторы методов ОАБП, не связанных с конкретным разработчиком

Идентификатор разработчика метода ОАБП	Идентификатор метода ОАБП	Описание
257 (0x0101)	1 (0x0001)	Запрос/непроизвольный ответ
257 (0x0101)	2 (0x0002)	Запрос/произвольный ответ
257 (0x0101)	3 (0x0003)	Запрос/ответ, основанный на сочетании того, что знает субъект, и того, что является частью субъекта
257 (0x0101)	4 (0x0004)	Пассивное обнаружение витальности

5.3.4 Результат ОАБП

Наличие: Необязательное

Абстрактные значения: Целые числа от 0 до 100, FAILURE_TO_COMPUTE

Содержание: Данный элемент, при наличии, содержит результат ОАБП в диапазоне значений между 0 и 100. Подлинные биометрические предъявления, как правило, имеют низкое значение данного элемента. Атаки на биометрическое предъявление, как правило, имеют высокое значение данного элемента. Абстрактное значение FAILURE_TO_COMPUTE указывает на то, что вычисление результата ОАБП не удалось.

Абстрактное значение FAILURE_TO_COMPUTE результата ОАБП ведет к тому, что абстрактное значение решения ОАБП, при наличии, также должно быть FAILURE_TO_COMPUTE.

5.3.5 Идентификатор разработчика метода ОАБП с расширенными данными

Наличие: Необязательное. Данный элемент следует включать в том случае, если присутствуют расширенные данные ОАБП.

Абстрактные значения: Целые числа от 1 до 65 535

Содержание: Данный элемент, при наличии, идентифицирует разработчика метода ОАБП с расширенными данными. Идентификатор разработчика метода ОАБП с расширенными данными, записываемый в данный элемент данных, должен быть присвоен регистрационным органом в области биометрии по *ГОСТ Р 58293*.

5.3.6 Идентификатор метода ОАБП с расширенными данными

Наличие: Необязательное. Данный элемент следует включать в том случае, если присутствует идентификатор разработчика метода ОАБП с расширенными данными.

Абстрактные значения: Целые числа от 1 до 65 535

Содержание: Данный элемент, при наличии, идентифицирует метод ОАБП, используемый для расширенных данных. Идентификатор метода ОАБП с расширенными данными должен быть присвоен разработчиком метода ОАБП с расширенными данными. Идентификатор метода ОАБП, записываемый в данный элемент данных, должен быть присвоен регистрационным органом в области биометрии по *ГОСТ Р 58293*.

Примечание — В соответствии с *ГОСТ Р 58293* регистрация идентификаторов биометрических продуктов не является обязательной.

5.3.7 Расширенные данные ОАБП

Наличие: Необязательное

Абстрактные значения: Любая строка октетов

Содержание: Данный элемент, при наличии, включает дополнительную информацию, относящуюся к ОАБП, которая не может храниться в элементах данных, определенных выше. Структура этих данных определяется разработчиком указанного метода ОАБП.

Приложение А
(справочное)

Формальные спецификации

А.1 Двоичное кодирование

А.1.1 Общие положения

Необходимо определить формат данных независимо от битового представления (абстрактного синтаксиса). Это позволит:

a) использовать различные кодировки;

b) использовать различные встроенные представления с использованием структур, подходящих для простой обработки на языках программирования C, C++ или Java;

c) использовать больше программных средств при реализации данных форматов;

d) проще реализовать представление в оперативной памяти на аппаратной архитектуре без обратного порядка следования байтов;

e) реализовать более понятное описание значений в форматах.

Абстрактный синтаксис информации ОАБП определен в А.1.2 в модуле абстрактной синтаксической нотации версии 1 (АСН.1) в соответствии с *ГОСТ Р ИСО/МЭК 8824-1*. Данные ОАБП в двоичном формате должны получаться с применением отличительных правил кодирования (DER) АСН.1, установленных в *ГОСТ Р ИСО/МЭК 8825-1*, к значениям типов, определенных в модуле АСН.1 в А.1.2. Краткое описание DER приведено в А.1.3. Табличное представление кодировки данных представлено в А.1.4. В случае конфликтов модуль АСН.1, определенный в А.1.2, имеет преимущество. Модуль АСН.1, определенный в А.1.2, доступен по ссылке: gost.e-ecolog.ru
iso-iec/30107/-2/ed-1.

Использование абстрактного синтаксиса в качестве схемы позволит программным средствам проводить преобразование между кодировками значений и встроенными представлениями. Программные средства, преобразующие модули АСН.1 в структуры данных языка программирования, называются компиляторами АСН.1 и поддерживаются подпрограммами среды выполнения, которые позволяют проводить преобразование между встроенным значением и указанными кодировками. Данные программные средства доступны на нескольких аппаратных платформах и на нескольких языках программирования и поставляются несколькими разработчиками.

Для обеспечения обратной совместимости, то есть возможности чтения и понимания данных ОАБП на основе старой версии формата программными средствами на основе новой версии формата, ни один элемент АСН.1, указанный в А.1.2, не должен быть изменен. Если необходимо добавить новые элементы в SET, SEQUENCE или CHOICE в более поздней версии настоящего стандарта, они должны быть добавлены в конце после маркера расширения «...». Для обеспечения прямой совместимости, то есть возможности считывания данных ОАБП на основе новой версии формата программными средствами на основе старой версии формата, программные средства, считывающие данные ОАБП, должны игнорировать неизвестные элементы данных.

А.1.2 Абстрактный синтаксис информации ОАБП в АСН.1

Описанный модуль АСН.1 доступен по ссылке:

gost.e-ecolog.ru

- - Описанная спецификация АСН.1 была проверена на соответствие требованиям стандарта на АСН.1 с помощью системы поддержки операций АСН.1.

```
PADDataFormatModule
{ISO standard 30107 data-formats(2) modules(0) PAD-data(0) version(0)}
DEFINITIONS
IMPLICIT TAGS               ::=
BEGIN
      PADData               ::= [APPLICATION 98] SET {
            PADDecision               [0] PADDecision                    OPTIONAL,
            PADScoreBlockSequence     [1] PADScoreBlockSequence          OPTIONAL,
            PADExtendedDataSequence   [2] PADExtendedDataSequence        OPTIONAL,
            captureContext            [3] CaptureContext                 OPTIONAL,
            supervisionLevel          [4] SupervisionLevel               OPTIONAL,
            riskLevel                 [5] RiskLevel                      OPTIONAL,
            criteriaCategory          [6] CriteriaCategory               OPTIONAL,
            PADParameter              [7] PADParameter                   OPTIONAL,
            PADChallenge              [8] PADChallenge                   OPTIONAL,
            PADDataCaptureDateTime    [9] GeneralizedTime                OPTIONAL,
            captureDevice             [10] CaptureDevice                 OPTIONAL,
      ...
      }
```

```
      PADDecision                   ::= ENUMERATED {
            failure-to-compute(-1), - -  -1, encoded as FF (255)
            no-attack(0),
            attack(1),
            ...
      }
      PADScoreBlockSequence         ::= SEQUENCE OF PADScoreBlock
      PADScoreBlock                 ::= SET {
            vendorId                      [0] Id,
            mechanismId                   [1] Id,
            PADScore                      [2] PADScore,
            ...
      }
      Id                            ::= OCTET STRING (SIZE(2))
      PADScore                      ::= INTEGER {failure-to-compute(-1)} (-1..100, ...)
      PADExtendedDataSequence       ::= SEQUENCE OF PADExtendedDataBlock
      PADExtendedDataBlock          ::= SET {
            vendorId                      [0] Id,
            mechanismId                   [1] Id,
            data                          [2] OCTET STRING,
            ...
      }
      CaptureContext                ::= ENUMERATED {
            enrolment (0),
            verification (1),
            identification (2),
            ...
      }
      SupervisionLevel              ::= ENUMERATED {
            unknown (0),
            controlled (1),
            assisted (2),
            observed (3),
            unattended (4),
            ...
      }
      RiskLevel                     ::= INTEGER (0..100, ...)
      CriteriaCategory              ::= ENUMERATED {
            unknown (0),
            individual (1),
            common (2),
            ...
      }
      PADParameter                  ::= PrintableString
      PADChallenge                  ::= SEQUENCE OF PrintableString
      CaptureDevice                 ::= SET {
            vendorId                      [0] Id,
            modelId                       [1] Id,
            serialNumber                  [2] PrintableString                    OPTIONAL,
            ...
      }
END
```

А.1.3 Краткое описание отличительных правил кодирования

Кодирование информационного объекта по отличительным правилам кодирования состоит из трех компонентов (см. *ГОСТ Р ИСО/МЭК 8825-1*):

а) октеты тегов. Они определяют класс и номер тега информационного объекта и для каждого типа указывают, является его кодирование простым или составным. Возможны две формы:

1) для тегов с номером от 0 до 30 октеты тегов должны содержать единственный октет. Биты 8 и 7 представляют класс тега (см. таблицу А.1). Бит 6 указывает, является ли кодирование простым или составным (бит 6 должен быть равен нулю, если кодирование простое, и единице, если кодирование составное). Биты с 5 по 1 должны кодировать номер тега с битом 5 в качестве старшего значащего бита;

2) для тегов с номерами, большими или равными 31, октеты тегов должны содержать два или более октета. Первый октет должен быть закодирован таким же образом, как для тегов с номером от 0 до 30, за исключением того, что биты от 5 до 1 должны быть равны 1. Биты с 7 по 1 второго и последующих октетов должны быть равны номеру тега с битом 7 второго октета в качестве старшего значащего бита. Бит 8 каждого из последующих октетов, кроме последнего, должен иметь значение 1;

b) октеты длины. Они определяют количество октетов значений. Возможны две формы:

1) короткая форма может быть использована, если число октетов от 0 до 127: октеты длины должны состоять из одного октета. Бит 8 является нулевым, а биты с 7 по 1 кодируют число октетов;

2) короткая форма может быть использована, если число октетов от 128 до 2^{1008}-1: октеты длины должны содержать от 2 до 127 октетов. Бит 8 первого октета должен быть равен 1, биты с 7 по 1 первого октета должны кодировать число до 126 последующих октетов длины с битом 7 в качестве старшего значащего бита. Биты с 8 по 1 второго и последующих октетов должны быть равны числу октетов с битом 8 второго октета в качестве старшего значащего бита;

в) октеты значений. Для значений с простым кодированием октеты значений должны быть равны конкретному представлению значения. Для значений с составным кодированием октеты значений должны быть равны конкатенации компонентов значения, кодированных по отличительным правилам кодирования.

Таблица А.1 — Кодирование класса тега

Класс	Бит 8	Бит 7
Универсальный	0	0
Прикладной	0	1
Контекстно зависимый	1	0
Пользовательский	1	1

А.1.4 Табличное представление кодировки данных

В таблице А.2 представлены данные ОАБП в формате информационных объектов, закодированных в структуре тег, длина, значение (TLV). В таблице А.2 наличие каждого элемента данных указывается как «обязательное» или «необязательное». Обязательное наличие означает, что элемент данных должен присутствовать в структуре данных, содержащих его. Необязательное наличие означает, что элемент данных может быть пропущен. Могут применяться дополнительные условия.

Примечание — Все теги, кроме старшего, являются контекстно зависимыми, значения которых зависят от информационного объекта, содержащего тег.

Таблица А.2 — Структура записи данных ОАБП в двоичном формате

Тег	Длина	Значение							Наличие (обязательное или необязательное)
0x7F62	Переменная	Данные ОАБП							Необязательное
		Тег	Длина	Значение					
		0x80	0x01	Решение ОАБП (см. 5.3.1): кодирование см. в таблицах А.3 и А.4					Необязательное
		0xA1	Переменная	Последовательность блоков данных результатов ОАБП: может включать один и более блоков данных результатов ОАБП					Необязательное
				Тег	Длина	Значение			
				0x31	0x0B	Блок данных результатов ОАБП			Необязательное
						Тег	Длина	Значение	

Продолжение таблицы А.2

Тег	Длина	Значение							Наличие (обязательное или необязательное)
						0x80	0x02	Идентификатор разработчика метода ОАБП (см. 5.3.2): от 0x0001 до 0xFFFF	Обязательное (если присутствует блок данных результатов ОАБП)
						0x81	0x02	Идентификатор метода ОАБП (см. 5.3.3): от 0x0001 до 0xFFFF	Обязательное (если присутствует блок данных результатов ОАБП)
						0x82	0x01	Результат ОАБП (см. 5.3.4): от 0x01 до 0x64, кодирование абстрактного значения FAILURE_TO_COMPUTE см. в таблице А.4	Обязательное (если присутствует блок данных результатов ОАБП)
		0xA2	Переменная	Последовательность блоков расширенных данных ОАБП: может включать один и более блоков расширенных данных ОАБП, полученных с использованием различных методов ОАБП					Необязательное
				Тег	Длина	Значение			
				0x31	Переменная	Блок расширенных данных ОАБП			Необязательное
						Тег	Длина	Значение	
						0x80	0x02	Идентификатор разработчика метода ОАБП (см. 5.3.5): от 0x0001 до 0xFFFF	Обязательное (если присутствует блок расширенных данных ОАБП)
						0x81	0x02	Идентификатор метода ОАБП (см. 5.3.6): от 0x0001 до 0xFFFF	Обязательное (если присутствует блок расширенных данных ОАБП)
						0x82	Переменная	Расширенные данные ОАБП (см. 5.3.7)	Обязательное (если присутствует блок расширенных данных ОАБП)
		0x83	0x01	Цель сбора данных (см. 5.2.1): кодирование см. в таблице А.5					Необязательное
		0x84	0x01	Уровень контроля в процессе сбора данных (см. 5.2.2): кодирование см. в таблице А.6					Необязательное

Окончание таблицы А.2

Тег	Длина	Значение					Наличие (обязательное или необязательное)
		0x85	0x01	Уровень риска (см. 5.2.3): от 0x01 до 0x64			Необязательное
		0x86	0x01	Категория критерия ОАБП (см. 5.2.4): кодирование см. в таблице А.7			Необязательное
		0x87	Переменная	Параметры ОАБП (см. 5.2.5): печатное представление строки			Необязательное
		0xA8	Переменная	Последовательность запросов ОАБП: может включать один и более запросов ОАБП			Необязательное
				Тег	Длина	Значение	
				0x13	Переменная	Запросы ОАБП (см. 5.2.5): печатное представление строки	Необязательное
		0x89	0x0F	Дата и время начала сбора данных ОАБП (см. 5.2.7): значение должно состоять из следующего в данном порядке: - четыре байта, содержащие четырехзначное представление календарного года в кодировке UTF-8, - два байта, содержащие двузначное представление календарного месяца в кодировке UTF-8 (от 01 до 12), - два байта, содержащие двузначное представление календарного дня месяца в кодировке UTF-8 (с 01 по 31), - два байта, содержащие двузначное представление часа в течение дня в кодировке UTF-8 (от 00 до 23), - два байта, содержащие двузначное представление минуты в течение часа в кодировке UTF-8 (от 00 до 59), - два байта, содержащие двузначное представление секунды в течение минуты в кодировке UTF-8 (00-59), и - один байт, содержащий заглавную букву Z в кодировке UTF-8, обозначающую UTC (0x5A)			Необязательное
				Пример — 15 декабря 2005 г., 17:35:20 кодируется как 32303035 3132 3135 3137 3335 3230 0x5A			
		0xAA	Переменная	Данные о биометрическом сканере: только один биометрический сканер используется для каждого представления			Необязательное
				Тег	Длина	Значение	
				0x80	0x02	Идентификатор изготовителя биометрического сканера (см. 5.2.8): от 0x0001 до 0xFFFF	Обязательное (если присутствуют данные о биометрическом сканере)
				0x81	0x02	Идентификатор модели биометрического сканера (см. 5.2.9): от 0x0001 до 0xFFFF	Обязательное (если присутствуют данные о биометрическом сканере)
				0x82	Переменная	Серийный номер биометрического сканера (см. 5.2.10): печатное представление строки	Необязательное

Т а б л и ц а А.3 — Кодирование решения ОАБП

Абстрактное значение	Кодирование
NO_ATTACK	0x00
ATTACK	0x01

Т а б л и ц а А.4 — Кодирование абстрактного значения FAILURE_TO_COMPUTE

Абстрактное значение	Кодирование
FAILURE_TO_COMPUTE	0xFF

Т а б л и ц а А.5 — Кодирование цели сбора данных

Абстрактное значение	Кодирование
ENROLMENT	0x00
VERIFICATION	0x01
IDENTIFICATION	0x02

Т а б л и ц а А.6 — Кодирование уровня контроля

Абстрактное значение	Кодирование
UNKNOWN	0x00
CONTROLLED	0x01
ASSISTED	0x02
OBSERVED	0x03
UNATTENDED	0x04

Т а б л и ц а А.7 — Кодирование категории критерия ОАБП

Абстрактное значение	Кодирование
UNKNOWN	0x00
INDIVIDUAL	0x01
COMMON	0x02

А.2 XML-кодирование

А.2.1 Общие положения

Синтаксис элементов данных ОАБП в XML-документах, описанный в А.2.2, разработан на языке XML с использованием рекомендаций написания XML-схем.

Синтаксис элементов данных ОАБП в XML-документах должен основываться на XML-схеме, описанной в А.2.2, а не на модуле АСН.1, описанном в А.2.1 и правилах XML-кодирования (XER) для АСН.1, определенных в *ГОСТ Р ИСО/МЭК 8825-4*.

П р и м е ч а н и е — Стандарт, определяющий отображение модуля АСН.1 в XML-схеме, отсутствует. В результате применения XER, определенных в *ГОСТ Р ИСО/МЭК 8825-4*, для абстрактных значений АСН.1, напрямую получаются XML-документы, которые, однако, отличаются от XML-документов на основе XML-схемы, определенной в А.2.2.

А.2.2 Описание XML-схемы

Описание XML-схемы доступно по ссылке:

gost.e-ecolog.ru

Приложение В
(справочное)

Примеры кодирования данных ОАБП

В.1 Двоичный формат данных ОАБП

Значения данных ОАБП, используемые в примере кодирования, имеют тип PADData, который определен в модуле АСН.1 в А.1.2. Значение формально определено ниже с использованием нотации значений АСН.1:

```
value PADData ::= {
   PADDecision no-attack,
   PADScoreBlockSequence {
      {
         vendorId '0101'H,
         mechanismId '0004'H,
         PADScore 9
      }
   }
}
```

Описанное выше кодирование значений данных ОАБП с помощью отличительных правил кодирования АСН.1 дает строку октетов, показанную ниже (все числа в шестнадцатеричном представлении):

```
7F62                    - - Тег объекта данных ОАБП
   12                   - - Длина данных ОАБП: 18 октетов
      80                - - Тег решения ОАБП
         01             - - Длина решения ОАБП
            00          - - Значение решения ОАБП: NO_ATTACK
         A1             - - Тег последовательности блоков данных результатов ОАБП
            0D          - - Длина последовательности блоков данных результатов ОАБП: 13 октетов
               31       - - Тег блока данных результатов ОАБП
                  0B    - - Длина блока данных результатов ОАБП: 11 октетов
                     80 - - Тег идентификатора разработчика метода ОАБП
                        02 - - Длина идентификатора разработчика метода ОАБП: 2 октета
                           0101 - - Значение идентификатора разработчика метода ОАБП: 257
                        81 - - Тег идентификатора метода ОАБП
                           02 - - Длина идентификатора метода ОАБП: 2 октета
                              0004 - - Значение идентификатора метода ОАБП: 4
                                   - - (Пассивное обнаружение витальности)
                        82 - - Тег результата ОАБП
                           01 - - Длина результата ОАБП: 1 октет
                              09 - - Значение результата ОАБП: 9
```

В.2 XML-кодирование данных ОАБП

```
<?xml version="1.0" encoding="utf-8"?>
<PADData
   xmlns="gost.e-ecolog.ru                                    "
   xmlns:xsi="gost.e-ecolog.ru                                ">
   <PADDecision>NoAttack</PADDecision>
   <PADScoreBlockSequence>
      <PADScoreBlock>
         <VendorId>0101</VendorId>
         <MechanismId>0004</MechanismId>
         <PADScore>
            <Score>9</Score>
         </PADScore>
      </PADScoreBlock>
   </PADScoreBlockSequence>
</PADData>
```

Приложение ДА
(справочное)

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

Таблица ДА.1

Обозначение ссылочного национального, межгосударственного стандарта	Степень соответствия	Обозначение и наименование ссылочного международного стандарта
ГОСТ ИСО 8601—2001	IDT	ISO 8601:2000 «Элементы данных и форматы для обмена информацией. Обмен информацией. Представление дат и времени»
ГОСТ ISO/IEC 2382-37—2016	IDT	ISO/IEC 2382-37:2012 «Информационные технологии. Словарь. Часть 37. Биометрия»
ГОСТ ISO/IEC 19794-1—2015	IDT	ISO/IEC 19794-1:2011 «Информационные технологии. Форматы обмена биометрическими данными. Часть 1. Структура»
ГОСТ Р 58293—2018 (ИСО/МЭК 19785-1:2015)	MOD	ISO/IEC 19785-1:2015 «Информационные технологии. Единая структура форматов обмена биометрическими данными. Часть 1. Спецификация элементов данных»
ГОСТ Р 58624.1 (ИСО/МЭК 30107-1:2016)	MOD	ISO/IEC 30107-1:2016 «Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 1. Структура»
ГОСТ Р ИСО/МЭК 8824-1—2001	IDT	ISO/IEC 8824-1:1998 «Информационные технологии. Абстрактная синтаксическая нотация версии один (АСН.1). Часть 1. Спецификация основной нотации»
ГОСТ Р ИСО/МЭК 8825-1—2003	IDT	ISO/IEC 8825-1:1998 «Информационные технологии. Правила кодирования АСН.1. Часть 1. Спецификация базовых (BER), канонических (CER) и отличительных (DER) правил кодирования»
ГОСТ Р ИСО/МЭК 8825-4—2009	IDT	ISO/IEC 8825-4:2002 «Информационные технологии. Правила кодирования АСН.1. Часть 4. Правила XML кодирования (XER)»

Примечание — В настоящей таблице использованы следующие условные обозначения степени соответствия стандартов:

- IDT — идентичные стандарты;
- MOD — модифицированные стандарты.

Приложение ДБ
(справочное)

Сопоставление структуры настоящего стандарта со структурой примененного в нем международного стандарта

Таблица ДБ.1

Структура настоящего стандарта	Структура международного стандарта ИСО/МЭК 30107-2:2017
Приложение ДА Сведения о соответствии ссылочных национальных и межгосударственных стандартов международным стандартам, использованным в качестве ссылочных в применяемом международном стандарте	—
Приложение ДБ Сопоставление структуры настоящего стандарта со структурой примененного в нем международного стандарта	—
—	Библиография
Примечание — Сопоставление структуры стандартов приведено, начиная с приложения ДА, так как предыдущие разделы стандартов идентичны.	

УДК 004.93'1:006.89:006.354

ОКС 01.080.50
35.240.15

Ключевые слова: информационные технологии, биометрия, обнаружение атаки, биометрическое предъявление, формат данных

БЗ 11—2019/73

Редактор *Н.В. Таланова*
Технический редактор *И.Е. Черепкова*
Корректор *Е.Д. Дульнева*
Компьютерная верстка *Е.О. Асташина*

Сдано в набор 05.11.2019. Подписано в печать 27.11.2019. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 1,90.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ» для комплектования Федерального информационного фонда стандартов, 117418 Москва, Нахимовский пр-т, д. 31, к. 2.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru