ИКАО

Doc 9303

Машиносчитываемые проездные документы

Издание восьмое, 2021

Часть 1. Введение

Утверждено и опубликовано с санкции Генерального секретаря

Международная организация гражданской авиации

ИКАО

Doc 9303

Машиносчитываемые проездные документы

Издание восьмое, 2021

Часть 1. Введение

Утверждено и опубликовано с санкции Генерального секретаря

Международная организация гражданской авиации

Опубликовано отдельными изданиями на русском, английском,
арабском, испанском, китайском и французском языках
МЕЖДУНАРОДНОЙ ОРГАНИЗАЦИЕЙ ГРАЖДАНСКОЙ АВИАЦИИ.
999 Robert-Bourassa Boulevard, Montréal, Québec, Canada H3C 5H7

Загрузить и получить дополнительную информацию можно на сайте
www.icao.int/Security/mrtd.

Doc 9303. *Машиносчитываемые проездные документы*
Часть 1. *Введение*
ISBN 978-92-9265-336-1

ПОПРАВКИ

Об издании поправок сообщается в дополнениях к *Каталогу продукции и услуг ИКАО*; Каталог и дополнения к нему имеются на веб-сайте ИКАО www.icao.int. Ниже приводится форма для регистрации поправок.

РЕГИСТРАЦИЯ ПОПРАВОК И ИСПРАВЛЕНИЙ

ПОПРАВКИ		
№	Дата	Кем внесено

ИСПРАВЛЕНИЯ		
№	Дата	Кем внесено

ОГЛАВЛЕНИЕ

1. ВВЕДЕНИЕ

Работа ИКАО в области машиносчитываемых проездных документов началась в 1968 году с момента учреждения Авиатранспортным комитетом Совета Группы экспертов по паспортным карточкам. Эта Группа получила задание разработать рекомендации для стандартной паспортной книжки или карточки, которые можно подвергать машинному считыванию в интересах ускорения процесса проверки пассажиров сотрудниками службы паспортного контроля. Группа экспертов подготовила ряд рекомендаций, в том числе о принятии методики оптического распознавания знаков (OCR) в качестве предпочтительного варианта машиносчитываемой технологии, учитывая степень ее развития, рентабельность и надежность. В 1980 году разработанные Группой экспертов спецификации и инструктивный материал были опубликованы в качестве первого издания документа Doc 9303 под названием *"Паспорт с машиносчитываемыми характеристиками",* который в качестве основы использовали для выдачи первых машиносчитываемых паспортов в Австралии, Канаде и в Соединенных Штатах Америки.

В 1984 году ИКАО создала так называемую Техническую консультативную группу по машиносчитываемым проездным документам (TAG/MRTD), в состав которой вошли государственные должностные лица, специализирующиеся в области выдачи и пограничной проверки паспортов и прочих проездных документов. Она была создана для обновления и усовершенствования спецификаций, подготовленных Группой экспертов. Впоследствии круг полномочий Технической группы был расширен за счет включения сначала разработки спецификаций машиносчитываемых виз, а позднее – технических требований к машиносчитываемым карточкам, которые могут использоваться в качестве официальных проездных документов.

В 1998 году Рабочая группа по новым технологиям Группы TAG/MRTD приступила к работе над созданием наиболее эффективной системы биометрической идентификации и связанных с ней средств хранения данных для использования при применении МСПД, особенно в части, качающейся выдачи документов и решения иммиграционных вопросов. К тому времени, когда события 11 сентября 2001 года заставили государства уделять больше внимания вопросам обеспечения защиты проездных документов и идентификации их владельцев, основной объем этой работы был выполнен. Работа была быстро завершена и одобрена Группой TAG/MRTD и Авиатранспортным комитетом.

Подготовленные по итогам этой работы технические доклады об использовании биометрических решений и технологии бесконтактных интегральных схем, логической структуры данных (LDS) и инфраструктуры открытых ключей (PKI) были включены в том 2 части 1 (*Машиносчитываемые паспорта*) шестого издания документа Doc 9303 в 2006 году и в том 2 части 3 (*Машиносчитываемые официальные проездные документы*) третьего издания документа Doc 9303 в 2008 году.

2. СФЕРА ПРИМЕНЕНИЯ

Документ Doc 9303 состоит из различных самостоятельных документов, в которых сгруппированы общие, т. е. применимые ко всем МСПД спецификации, а также технические требования, относящиеся к конкретному формату МСПД. Обзор приводится в разделе 5.1 "Структура документа Doc 9303".

Эти спецификации не следует рассматривать как стандарт для национальных документов, удостоверяющих личность. Тем не менее государству, идентификационные документы которого признаются другими государствами в качестве действительных проездных документов, следует разрабатывать свои удостоверяющие личность документы таким образом, чтобы они соответствовали спецификациям в частях 3 и 4, 5 или 6 документа Doc 9303.

Хотя спецификации в части 4 документа Doc 9303 предназначены для конкретного применения в отношении паспортов, эти спецификации в равной мере применимы и к другим идентификационным документам размера ПД3, например пропуску ООН, удостоверению личности моряка и проездному документу беженца.

Настоящий материал представляет собой часть 1, в которой представлены технические требования документа Doc 9303. Здесь описывается структура тринадцати частей Doc 9303, содержится общая информация об ИКАО, а также приведены термины и сокращения, используемые в этих спецификациях.

3. ОБЩИЕ СООБРАЖЕНИЯ

3.1 Ведущая роль ИКАО

Инициатива ИКАО по разработке стандартных спецификаций паспортов и других проездных документов следовала традиции конференций по паспортным вопросам, проводимых Лигой Наций в 1920-х годах, и работе преемника Лиги Наций – Организации Объединенных Наций. Полномочия ИКАО по сохранению ведущей роли в этой области вытекают из Конвенции о международной гражданской авиации ("Чикагской конвенции"), которая охватывает обширный спектр требований, призванных обеспечить эффективную и упорядоченную деятельность гражданской авиации, включая положения о проверке пассажиров при прохождении пограничного контроля, а именно:

a) требование о том, чтобы авиапассажиры и экипажи воздушных судов соблюдали иммиграционные правила и правила паспортного контроля (статья 13);

b) требование о том, чтобы государства упрощали формальности пограничной проверки и предотвращали не вызванные необходимостью задержки (статья 22);

c) требование о том, чтобы государства сотрудничали в решении этих вопросов (статья 23);

d) требование о том, чтобы государства разрабатывали и принимали международные стандартные процедуры иммиграционной и таможенной проверки (статья 37 j)).

В соответствии с этим мандатом ИКАО разрабатывает и обновляет Международные стандарты Приложения 9 *"Упрощение формальностей)* к Чикагской конвенции для выполнения их государствами-членами. При разработке таких Стандартов основная исходная посылка заключается в том, что если полномочным государственным органам надлежит упрощать формальности проверки подавляющего большинства авиапассажиров, то эти полномочные органы должны быть в достаточной степени уверены в надежности проездных документов и в эффективности процедур проверки. Подготовка стандартных спецификаций проездных документов и содержащихся в них данных направлена на создание такой уверенности.

В 2004 году Ассамблея ИКАО подтвердила, что совместная разработка спецификаций в целях повышения защиты и целостности проездных документов должна осуществляться Организацией в первоочередном порядке. В качестве консультантов в состав Группы TAG/MRTD, помимо экспертов Международной организации по стандартизации (ИСО), входят специалисты Международной ассоциации воздушного транспорта (ИАТА), Международного совета аэропортов (МСА) и Международной организации уголовной полиции (ИНТЕРПОЛ).

В 2005 году входившие на тот момент в ИКАО 188 государств-членов утвердили новый Стандарт, согласно которому все государства должны начать выдавать машиносчитываемые паспорта в соответствии с документом Doc 9303 не позднее 2010 года. Срок действия всех проездных документов, не являющихся машиносчитываемыми, должен истекать не позднее 2015 года. Этот Стандарт вошел в 13-е издание (2011) Приложения 9 *"Упрощение формальностей".*

3.2 Относительные расходы и преимущества использования машиносчитываемых проездных документов

Опыт выдачи машиносчитываемых паспортов в соответствии со спецификациями Doc 9303 свидетельствует о том, что расходы на выпуск МСПД могут не превышать расходов на выпуск обычных документов, хотя затраты могут быть выше при внедрении средств биометрической идентификации и электронных проездных документов. По мере роста объема воздушных перевозок все большее число государств работают над упорядочением своих процедур проверки, используя для этого компьютерные базы данных и электронный обмен данными, и МСПД играют центральную роль в создании такой современной и отвечающей существующим потребностям системы. Разработка оборудования для считывания документов и получения доступа к базам данных может потребовать значительных инвестиций, хотя вполне можно ожидать, что такие расходы окупятся благодаря улучшению систем защиты, ускорению и повышению точности проверок с использованием таких систем. Использование МСПД в автоматизированных системах проверки также позволит государствам отказаться от таких бумажных документов, как пассажирские ведомости и регистрационные карточки при прилете и вылете, и сэкономить на административных расходах, связанных с выполнением соответствующих неавтоматизированных процедур.

3.3 Практическое использование

Базовый машиносчитываемый проездной документ, основанный на технологии считывания OCR, предназначен как для визуального, так и для машинного считывания.

Государства – члены ИКАО признали, что стандартизация является необходимостью и что выгоды принятия стандартных форматов паспортов и других проездных документов, указанных в документе Doc 9303, не ограничиваются очевидными преимуществами, которые получают государства в результате внедрения устройств машинного считывания и баз данных, используемых в автоматизированных системах проверки. На практике физические характеристики самих документов и элементы защиты содержащихся в них данных надежно предохраняют от возможности изменения, подлога или подделки документов. Кроме того, принятие стандартного формата зоны визуальной проверки МСПД упрощает проведение проверок сотрудниками авиакомпаний и государственных органов, в результате чего ускоряется процесс оформления пассажиров, не представляющих опасности, легче выявляются проблемные ситуации и улучшается положение дел с обеспечением правопорядка. Факультативное введение биометрической идентификации с помощью данных, хранящихся на бесконтактной интегральной схеме, позволит повысить безопасность и защищенность документа от мошенничества и тем самым облегчить законному владельцу документа получение виз для поездок и прохождение через системы пограничного контроля.

Примечание. Следует признать, что будут возникать ситуации, в которых невозможно обеспечить корректное сопряжение электронного МСПД со считывающим устройством на пограничном пункте. Это может произойти по ряду причин, и отказ электронного МСПД является лишь одной из таких причин. ИКАО подчеркивает, что электронный МСПД, который невозможно считать, тем не менее, остается действительным документом. Однако невозможность считывания может быть результатом мошенничества, и поэтому принимающему государству следует установить свои собственные процедуры на случай такой возможности, которые включали бы более внимательную проверку такого документа и его владельца, исходя при этом из того, что невозможность считывания не вызвана мошенничеством.

3.4 Подтверждение ИСО

Разделы технических требований документа Doc 9303 были подтверждены Международной организацией по стандартизации в качестве стандарта ИСО 7501. Такое подтверждение стало возможным благодаря использованию Группой TAG/TRIP в своей работе под эгидой ИСО механизма координации,

позволяющего получать от изготовителей проездных документов, считывающих устройств и других технических средств технические и конструктивные рекомендации. Благодаря такой организации работы спецификации ИКАО получили и, как ожидается, будут и впредь получать статус международных стандартов на основе упрощенной процедуры, установленной ИСО.

Механизм связи с ИСО успешно применяется не только для подтверждения новых спецификаций проездных документов в качестве стандартов ИСО, но и для принятия поправок к таким спецификациям. Поэтому последующие издания документа Doc 9303 будут представляться для подтверждения ИСО таким же образом, как и ранее.

4. ОПРЕДЕЛЕНИЯ И СПРАВОЧНЫЕ МАТЕРИАЛЫ

4.1 Сокращения

Сокращение	**Полная форма**
АСПК	Автоматизированная система пограничного контроля
ЗВП	Зона визуальной проверки
ЗЭС	Зона эффективного считывания
ИКАО	Международная организация гражданской авиации
ИС	Интегральная схема
МСВ-А	Машиносчитываемая виза полного размера (формат А)
МСВ-В	Машиносчитываемая виза малого размера (формат В)
МСЗ	Машиносчитываемая зона
МСОПД	Машиносчитываемый официальный проездной документ в форме карты
МСП	Машиносчитываемый паспорт
МСПД	Машиносчитываемый проездной документ
ПД1	Машиносчитываемый официальный проездной документ размера 1
ПД2	Машиносчитываемый официальный проездной документ размера 2
ПД3	Машиносчитываемый проездной документ размера 3
Электронный МСОПД	Электронный машиносчитываемый официальный проездной документ
Электронный МСП	Электронный машиносчитываемый паспорт
Электронный МСПД	Электронный машиносчитываемый проездной документ
3DES	Тройной DES
AA	Активная аутентификация
AFS	Специалист по борьбе с мошенничеством
AES	Усовершенствованный стандарт кодирования
AID	Идентификатор приложения
APDU	Блок данных протокола приложения
AO	Уполномоченный сотрудник
BAC	Базовый контроль доступа
BER	Базовые правила кодирования
BLOB	Большой двоичный объект
BSC	Сертификат подписи штрих-кода
CA	Сертифицирующий полномочный орган– также – Аутентификация чипа

Сокращение	Полная форма
CAM	Отображение для аутентификации чипа
CAN	Номер доступа к карточке
CAR	Идентификатор сертифицирующего полномочного органа
CBC	Связывание блоков шифра
CBEFF	Единая структура форматов обмена биометрическими данными
CCD	Прибор с зарядовой связью
CDS	Сертификат подписи документа
CIC	Бесконтактная интегральная схема
CID	Идентификатор карточки
CMAC	Код аутентификации сообщений на основе шифра
CMOS	Комплементарный металло-оксидный полупроводник
CRL	Список отзыва сертификатов
CSCA	Национальный сертифицирующий полномочный орган с правом подписи
CSD	Расстояние от камеры до предмета: расстояние между плоскостью глаз человека и оптическим центром линзы камеры
CVCA	Национальный сертифицирующий полномочный орган с правом верификации
DER	Особое правило кодирования
DES	Стандарт кодирования данных
DF	Выделенный файл
DG	Группа данных
DH	Диффи–Хеллман (алгоритм)
DN	Отличительное имя
DO	Объект данных
DOVID	Дифракционное оптически переменное устройство визуализации (дифракционный элемент с оптически изменяемыми свойствами, например, голографическим эффектом)
DS	Лицо, подписавшее документ
DSA	Алгоритм цифровой подписи
DTA	Цифровое разрешение на поездки
DTBS	Данные для подписания
DV	Верификатор документа
EAL	Уровень гарантии оценки
ECDH	Эллиптическая кривая Диффи–Хеллмана
ECDSA	Алгоритм цифровой подписи на основе эллиптических кривых

Сокращение	**Полная форма**
ECKA	Согласование ключа на основе эллиптической кривой
EEPROM	Электрически стираемая программируемая постоянная память
EF	Элементарный файл
EM	Расстояние от глаза до рта
eRP	Электронный вид на жительство
ETS	Электронная система оформления поездок
EVZ	Отображаемая зона глаз: зона в форме прямоугольника, где расстояние V до любой видимой части глазного яблока, равно, по меньшей мере, 5% длины IED
FAR	Коэффициент ложного допуска
FIPS	Федеральный стандарт обработки информации
FRR	Коэффициент ложного отказа
GM	Отображение общего типа
HD	Угол отклонения по горизонтали: максимально допустимое отклонение от горизонтальной воображаемой линии, проведенной от носа человека до линзы камеры
ICC	Карта на интегральной схеме
IED	Расстояние между центрами глаз
IFD	Устройство интерфейса
IM	Интегрированное отображение
IR	Инфракрасный свет
IS	Система проверки
IV	Начальный вектор
LDS	Логическая структура данных
MAC	Код аутентичности сообщения
MF	Мастер-файл
MTF	Функция передачи модуляции
MTF-20	Самая высокая пространственная частота, когда MTF составляет 20% или более
NAD	Адрес узла
NIST	Национальный институт стандартов и технологии
NTWG	Рабочая группа по новым технологиям
OCR	Оптическое распознавание знаков
OCR-B	Фонт оптического распознавания знаков, определенный в ИСО 1073-2
OID	Идентификатор объекта
OVD	Оптически переменное устройство
OVF	Оптически переменная характеристика

Сокращение	Полная форма
OVI	Оптически переменная краска
PACE	Установление соединения с аутентификацией паролем
PCD	Устройство соединения через малый зазор
PICC	Карта на интегральной схеме с индуктивной связью через малый зазор
PIX	Расширение имущественной принадлежности
PKI	Инфраструктура открытых ключей
RID	Зарегистрированный идентификатор
RFID	Радиочастотная идентификация
RGB	Красный-зелёный-синий
ROI	Область интереса
ROM	Постоянная память
RSA	Алгоритм Ривеста, Шамира и Адлемана
SFR	Пространственно-частотная характеристика
SHA	Алгоритм безопасного хэширования
SM	Безопасный обмен сообщениями
SNR	Отношение "сигнал-шум"
SO_D	Объект защиты документов
SPOC	Единое контактное лицо
sRGP	Стандартное цветовое пространство RGB, созданное для применения в мониторах, принтерах и в интернете с использованием основных цветов МСЭ-R BT.709
SSC	Счетчик порядковых номеров посылаемых сообщений
TA	Терминальная аутентификация
TAG/MRTD	Техническая консультативная группа ИКАО по машиносчитываемым проездным документам
TAG/TRIP	Техническая консультативная группа по программе идентификации пассажиров
TLV	Значение длины тега
TR	Технический доклад
UID	Уникальный идентификатор
UV	Ультрафиолетовый свет
VDS	Видимая цифровая подпись
VIS	Визовая информационная система Европейского Союза
VS	Лицо, подписавшее визу
VVA	Полномочный орган валидации визы
WSQ	Коротковолновое скалярное квантование

4.2 Термины и определения

Термин	Определение
Adobe RGB	Цветовое пространство RGB, предназначенное для охвата большей части цветов, получаемых на цветных принтерах CMYK, за счет использования основных цветов RGB на таких устройствах как экран компьютера
Алгоритм	Определенный математический процесс вычисления; набор правил, следуя которым будет получен заданный результат
Алгоритм безопасного хэширования (SHA)	Функция хэширования, установленная NIST и опубликованная в качестве федерального стандарта обработки информации FIPS-180
Алгоритм проверки	Компоненты программного обеспечения, позволяющие конкретное проведение программ проверки (например, поиск закономерностей)
Алгоритм Ривеста, Шамира и Адлемана (RSA)	Асимметричный алгоритм, изобретенный Роном Ривестом, Ади Шамиром и Леном Адлеманом. Он используется в криптографии открытых ключей и основан на том, что умножить два больших простых числа легко, но трудно факторизовать их из произведения
Алгоритм цифровой подписи (DSA)	Асимметричный алгоритм, опубликованный NIST в качестве FIPS 186. Этот алгоритм обеспечивает только функцию цифровой подписи
Асимметричность	Необходимость наличия разных ключей на каждом конце линии связи
Асимметричные ключи	Отдельная, но интегрированная пара ключей пользователя, состоящая из одного открытого ключа и одного закрытого ключа. Каждый ключ является односторонним, что означает, что ключ, используемый для шифрования информации, не может быть использован для дешифрования этой же информации
Асимметричный алгоритм	Тип криптографической операции с использованием одного ключа для шифрования открытого текста и второго ключа для дешифрования соответствующего шифрованного текста. Эти два ключа связаны друг с другом и называются парой ключей
Атака методом грубой силы	Испытание и перебор всех возможных ключей для проверки возможности получения открытого смыслового текста.
Аутентичность	Способность подтвердить, что логическая структура данных и ее компоненты созданы выдавшими документ государством или организацией
База данных аутентификации	В этой базе данных хранятся алгоритмы аутентификации для целей проведения программ проверок по каждой модели документа
Байт	Последовательность восьми битов, которые, как правило, обрабатываются как единое целое

Термин	Определение
Бесконтактная интегральная схема	Полупроводниковое устройство, которое хранит данные МСПД и осуществляет связь со считывающим устройством с использованием радиочастотной энергии в соответствии с ИСО/МЭК 14443
Биографические данные (биоданные)	Личные данные владельца документа, изображаемые в виде текста в зоне визуальной проверки, или машиносчитываемой зоне страницы биографических данных МСПД или на чипе, если имеется
Биометрическая верификация	Средство идентификации или подтверждения личности владельца МСПД путем измерения одной или нескольких индивидуальных личностных характеристик владельца
Биометрическая идентификация	Средство идентификации или подтверждения личности владельца МСПД путем оценки одной или нескольких личностных характеристик владельца
Биометрическая система	Автоматизированная система, способная: 1. брать биометрический образец у конечного пользователя для МСП; 2. извлекать биометрические данные из этого биометрического образца; 3. сравнивать значение(я) конкретных биометрических данных со значениями, содержащимися в одном или нескольких контрольных шаблонах; 4. определять, насколько точно совпадают данные, т. е. осуществлять предписанный процесс проверки на совпадение с учетом требований однозначной идентификации и аутентификации личности зарегистрированного пользователя применительно к конкретной транзакции; 5. указывать, была ли достигнута идентификация или верификация личности
Биометрическая характеристика, верифицируемая с помощью машины	Уникальная персональная идентификационная характеристика (например, изображение лица, отпечаток пальца или радужная оболочка), хранящаяся в электронном формате на чипе электронного МСПД
Биометрические данные	Информация, извлекаемая из биометрического образца и используемая либо для создания контрольного шаблона (данные шаблона), либо для сравнения с ранее созданным контрольным шаблоном (данные сравнения)
Биометрический образец	Исходные данные, захваченные в виде дискретного однозначного уникального и лингвистически нейтрального значения, представляющие собой биометрические характеристики зарегистрированного пользователя, захваченные биометрической системой (например, биометрический образец может включать изображение отпечатка пальца или его производное для целей аутентификации)
Биометрический параметр	Измеряемая индивидуальная физическая характеристика или личностная поведенческая черта, используемая для идентификации личности или для верификации предъявленной идентификационной информации зарегистрированного пользователя

Термин	**Определение**
Биометрический шаблон	Извлеченные и сжатые данные из взятого биометрического образца
Бит	Двоичная цифра. Минимально возможная единица исчисления информации в цифровом коде
Бланк документа	Бланком документа является проездной документ, не содержащий личных данных. Обычно бланки документов являются основным запасом, из которого изготавливаются персонализированные проездные документы
Блок	Строка или группа битов, которыми оперирует блочный алгоритм
Блок данных выдавшей организации	Ряд групп данных, записанных на факультативном устройстве увеличения емкости государством или организацией, выдавшими документ
Блок данных получателя	Ряд групп данных, записанных принимающим устройством или уполномоченной принимающей организацией на факультативном устройстве увеличения емкости
Блочный алгоритм	См. термин "блочный шифр"
Блочный шифр	Алгоритмы, которые преобразовывают открытый текст в блоки (строки или группы) битов
Бутстрэппинг	Метод проверки достоверности набора данных
Валидация/ валидировать	Процесс демонстрации того, что рассматриваемая система во всех отношениях соответствует техническим требованиям к этой системе
Верификация/ верифицировать	Биометрия: Процесс сравнения представленного биометрического образца с биометрическим контрольным шаблоном одного зарегистрированного пользователя, в отношении которого предъявляется идентификационная информация, с целью определить, совпадает ли он с шаблоном зарегистрированного пользователя. Ср. с термином "идентификация" Машинная аутентификация: верификация путем применения программы проверки к актуальным комплектам данных модели документа. Итогом верификации часто становится численное значение результата измерения
Видимая цифровая подпись (VDS)	Криптографически подписываемая структура данных, содержащая отличительные особенности документа, которая кодируется в виде штрих-кода в двух измерениях и печатается на документе
Владелец	Обладающее МСПД лицо, которое предоставляет биометрический образец для верификации или идентификации, предъявляя правильную или ложную идентификационную информацию. Лицо, взаимодействующее с биометрической системой для занесения в нее или проверки собственной идентификационной информации
Внеполосная	Относится к связи, которая осуществляется за пределами установленного ранее метода или канала связи
Водяной знак	Индивидуальный рисунок, обычно содержащий тональную градацию, который формируется в бумаге или другой основе в процессе изготовления, создается путем смещения содержащихся материалов и обычно видимый на свет

Термин	Определение
Вторичное изображение	См. термин "теневое изображение"
Выдача разрешения	Процедура в процессе проверки для определения возможности предоставления обслуживания
Галерея	База данных, содержащая биометрические шаблоны ранее зарегистрированных лиц, которая может просматриваться с целью обнаружения пробника
Гильошированный узор	Узор из непрерывных тонких линий, обычно создаваемый с помощью компьютера и образующий особое изображение, которое может быть в точности вновь воспроизведено с помощью оборудования, программного обеспечения и параметров, используемых при создании первоначального узора
Глобальная интероперабельность	Способность систем проверки (автоматизированных или неавтоматизированных) различных государств мира принимать данные и производить обмен ими, обрабатывать данные, полученные из систем других государств, и использовать эти данные при проведении проверок в соответствующих государствах. Достижение глобальной интероперабельности является одной из основных целей стандартизации спецификаций, предусматривающих помещение зрительно считываемых и машиносчитываемых данных во всех электронных МСПД
Глобально интероперабельная биометрика	Относится к изображению лица, как указано в части 9 документа Doc 9303
Глубокая печать "интаглио"	Процесс печати, используемый для изготовления защищенных документов, когда высокое давление печатания и специальные чернила используются для создания осязаемого рельефного изображения на поверхности документа
Государство выдачи	Страна, выдавшая МСПД
Группа данных	Серия взаимосвязанных элементов данных, сгруппированных в рамках логической структуры данных
Дальность считывания	Практически возможное максимальное расстояние между бесконтактной ИС с антенной и считывающим устройством
Данные для подписания (DTBS)	Сообщение, направляемое в качестве вводной информации к алгоритму генерирования подписи в схеме генерирования подписи
Двухслойный рисунок	Рисунок, составленный из переплетающегося муара небольших нерегулярных форм, напечатанный двумя или более цветами и требующий очень точной приводки в целях обеспечения целостности изображения
Дескриптор (отличительной черты)	Бит, являющийся уникальным идентификатором отличительной черты документа. Сопоставление дескрипторов отличительной черты и отличительных черт должно указываться в учетной записи
Директория открытых ключей (ДОК) ИКАО	Центральная база данных, выступающая в качестве хранилища сертификатов органов, подписывающих документы, мастер-списков CSCA, сертификатов подписывающих СА стран и списков отзыва сертификатов, выдаваемых участниками, вместе с системой их всемирного распространения; базу данных ведет ИКАО от имени участников в порядке содействия валидации данных в электронных МСПД

Термин	**Определение**
Дисторсия увеличения	Дефект изображения, при котором степень увеличения меняется в зависимости от расстояния от камеры и глубины резкости изображения лица
Дифракционное оптически переменное устройство	Защитный элемент, в структуре которого содержится голографическое или эквивалентное изображение, меняющееся в зависимости от угла зрения или освещения
Заблокированный (чип)	По завершении процесса персонализации чип ДОЛЖЕН быть заблокирован. Это означает, что команды персонализации не могут больше выполняться, а данные персонализации не могут более быть записанными на чип. Данные могут быть записаны на чип только после успешной реализации процедур механизма аутентификации (ТА). Заблокированный чип не может быть разблокирован.
Заголовок	Напечатанное слово или фраза для обозначения поля. В исключительных обстоятельствах, когда тексты на нескольких различных официальных языках не умещаются в поле данных, могут использоваться номера. Такие номера должны сопровождаться пояснительным текстом в другом месте МСП
Заделанное изображение	Изображение или информация, закодированные или включенные в основное визуальное изображение. См. также термин "стеганография"
Закрытый ключ	Закрытый компонент интегрированной асимметричной пары ключей (известный только пользователю), используемый в криптографии открытого ключа при дешифровании или подписании информации
Замена фотографии	Вид подлога, при котором фотография на документе заменяется другой фотографией после того, как указанный документ был выдан
Заполнение	Добавление дополнительных битов до требуемой длины с обеих сторон строки данных
Зарегистрированный пользователь	Человек, т. е. физическое лицо, которому выдан МСПД государством или организацией выдачи
Захват	Метод взятия биометрического образца у конечного пользователя
Защитная нитка	Тонкая полоска пластика или другого материала, вмонтированная или частично вмонтированная в основу в процессе изготовления бумаги. Такая полоска может быть металлизирована или частично деметаллизирована
Защищенное сообщение	Сообщение, которое защищено от незаконного изменения или подмены
Защищенность от подделки	Способность компонентов документа противостоять изменению
Значение экспозиции (EV)	Величина, которая представляет собой сочетание скорости срабатывания затвора и индекса диафрагмы фотоаппарата, в результате которого все комбинации, обеспечивающие одинаковую экспозицию, имеют одинаковое значение EV
Зона	Пространство, содержащее логически сгруппированные элементы данных в МСПД. Для МСПД определяются семь (7) зон

Термин	Определение
Зона визуальной проверки (ЗВП)	Те части МСПД (страницы данных при использовании МСП), которые предназначены для визуальной проверки, т. е. лицевые и оборотные (где применимо), которые не включены в МСЗ
Зона эффективного считывания (ЗЭС)	Общая для всех МСПД зона установленного размера, в которой машиносчитываемые данные, содержащиеся в МСЗ, могут быть считаны считывателем документа
Идентификатор	Уникальный ряд данных, используемый в биометрической системе в качестве ключа к идентификации лица и его соответствующих атрибутов. Примером идентификатора служит номер МСПД
Идентификатор приложения (AID)	Элемент данных, который определяет приложение. Приложения электронного МСПД используют стандартный AID, представляющий собой одну из четырех категорий AID. Он состоит из зарегистрированного идентификатора поставщика приложения (RID) и собственного добавления к идентификатору приложения (PIX)
Идентификация/ идентифицировать	Процесс "один ко многим", предусматривающий сравнение представленного биометрического образца со всеми биометрическими контрольными шаблонами в файле с целью определить, совпадает ли он с одним из шаблонов, и если совпадает, то установить личность владельца электронного МСПД. Биометрическая система, основанная на принципе "один ко многим", предназначена для идентификации на основе базы данных, а не для верификации заявленных идентификационных данных. Ср. с термином "верификация"
Идентификационная карта (ID-карта)	Карта, используемая в качестве документа для удостоверения личности
Извлечение	Процесс преобразования взятого биометрического образца в биометрические данные с тем, чтобы их можно было сравнить с контрольным шаблоном.
Изменяющееся лазерное изображение	Характеристика, создаваемая методом лазерной гравировки или лазерной перфорации, благодаря чему информация или изображение меняются в зависимости от угла зрения
Измерительный шаблон	Длина стороны измерительного шаблона: зоны измерения интенсивности имеют квадратную форму, размер которой составляет 30% расстояния между глазами; они используются для измерения интенсивности освещения щек, лба и подбородка
Изображение	Воспроизведение биометрического параметра, обычно фиксируемого при помощи видеоаппаратуры, фотокамеры или сканирующего устройства. Для целей биометрии хранится в цифровой форме
Инициализация (смарт-карты)	Процесс заполнения постоянной памяти (EEPROM и т. п.) данными, которые одинаковы для большинства карт, а также минимальным количеством индивидуальных для каждой конкретной карты элементов (например, серийный номер и ключи персонализации ICC)
Интегральная схема (ИС)	Электронный компонент, предназначенный для выполнения функций обработки данных и/или памяти
Интеграция систем	Процесс, с помощью которого лицевая, внутренняя и контактная системы карты владельца и приложения интегрируются друг с другом

Термин	**Определение**
Интероперабельность	Способность нескольких независимых систем или компонентов подсистем взаимодействовать
Интерфейс	Стандартное техническое определение связи между двумя компонентами
Информативный элемент	Включение кодированной информации в структуру данных документа или изображения, обычно в данные персонализации, особенно в фотографию
Инфракрасные пропадающие чернила	Чернила, образующие видимое изображение при освещении в визуальной части спектра, которые не могут быть обнаружены в инфракрасной зоне
Инфракрасные чернила	Чернила, видимые в инфракрасной части спектра
Инфраструктура открытых ключей (PKI)	Совокупность стратегий, процессов и технологий, используемых для верификации, регистрации и сертификации пользователей приложений защиты. В PKI для защиты связи используются криптография открытого ключа и практика сертификации ключа
Ирисовая печать	См. термин "радужная печать"
Исходный документ	Документ, используемый для удостоверения личности при обращении за проездным документом
Карта	Носитель, соответствующий требованиям ИСО/МЭК 7810, ИСО/МЭК 7811, ИСО 7812 и используемый для хранения информации
Карта на интегральных схемах (карта ИС, ICC)	Карта, в которую встроены одна или несколько ИС
Код аутентичности сообщения (MAC)	MAC представляет собой краткую форму сообщения, которая прилагается к самому сообщению. MAC не может быть вычислен или верифицирован, если неизвестен секретный ключ. Он прилагается отправителем и верифицируется получателем, который может обнаружить подделку сообщения
Код страны	Двух- или трехбуквенный код, определенный в ИСО 3166-1 и используемый для обозначения полномочного органа, выдавшего документ, или гражданства владельца документа
Комплект контрольных данных	Визуальные, инфракрасные и ультрафиолетовые изображения контрольного документа определяют программы проверки соответствующей модели документа
Комплект контрольных документов	Набор документов, комплект контрольных данных которых используется для определения программ проверки
Комплектование	Процесс сбора биометрических образцов у лица и последующей подготовки и хранения биометрических контрольных шаблонов, обеспечивающих идентификацию такого лица
Конечный пользователь	Лицо, взаимодействующее с биометрической системой для занесения в нее или проверки собственной идентификационной информации

Термин	Определение
Контрольные подборочные отметки	См. термин "указательные отметки"
Контрольный биометрический шаблон	Набор данных, которые определяют биометрические показатели лица, в дальнейшем используемый в качестве основы для сравнения с представляемым(ыми) биометрическим(ими) образцом(ами)
Контрольный номер	Номер, присваиваемый документу при его изготовлении для целей учета и безопасности
Конфиденциальные данные	Эти данные считаются более конфиденциальными, чем не конфиденциальные данные. Доступ к конфиденциальным данным СЛЕДУЕТ сделать более ограниченным. В документе Doc 9303-11 термин "терминальная аутентификация " означает интероперабельный механизм получения доступа к конфиденциальным данным. Если интероперабельность не требуется, могут использоваться другие механизмы
Коротковолновое скалярное квантование (WSQ)	Способ сжатия данных, применяемый, в частности, для хранения изображений отпечатков пальцев
Коэффициент ложного допуска (FAR)	Вероятность того, что биометрическая система ошибочно идентифицирует лицо или не сможет отказать самозванцу. Коэффициент ложного допуска определяется выражением FAR = NFA/NIIA или FAR = NFA/NIVA, где FAR – коэффициент ложного допуска, NFA – количество случаев ложного допуска, NIIA – количество попыток идентификации со стороны самозванцев и NIVA – количество попыток верификации со стороны самозванцев
Коэффициент ложного несовпадения	Альтернатива "коэффициенту ложного отказа"; используется во избежание путаницы в прикладных программах, отказывающих предъявителям при совпадении их биометрических данных с биометрическими данными зарегистрированного пользователя. В таких прикладных программах понятия допуска и отказа меняются местами, в связи с чем значения терминов "ложный допуск" и "ложный отказ" меняются на обратные
Коэффициент ложного отказа (FRR)	Вероятность того, что биометрическая система не сможет идентифицировать зарегистрированного пользователя или произвести верификацию правильности предъявленной идентификационной информации зарегистрированного пользователя. Коэффициент ложного отказа определяется выражением FRR = NFR/NEIA или FRR = NFR/NEVA, где FRR – коэффициент ложного отказа, NFR – количество случаев ложного отказа, NEIA – количество попыток идентификации со стороны зарегистрированных пользователей и NEVA – количество попыток верификации со стороны зарегистрированных пользователей. При этом предполагается, что попытки идентификации/верификации со стороны зарегистрированных пользователей являются репрезентативными для всей совокупности зарегистрированных пользователей. Коэффициент ложного отказа, как правило, не включает ошибки, связанные с "невозможностью получения информации"
Коэффициент ложного совпадения	Альтернатива "коэффициенту ложного допуска"; используется во избежание путаницы в прикладных программах, отказывающих предъявителям при совпадении их биометрических данных с биометрическими данными зарегистрированного пользователя. В таких прикладных программах понятия допуска и отказа меняются местами, в связи с чем значения терминов "ложный допуск" и "ложный отказ" меняются на обратные

Термин	**Определение**
Криптография	Наука о преобразовании информации в зашифрованную и неразборчивую с помощью алгоритма и ключа
Криптография открытого ключа	Вид асимметричного шифрования, когда все стороны владеют парами ключей, один из которых закрытый, а второй – открытый, для использования при шифровании и цифровой подписи данных
Кроп-фактор	Отношение диагонали полноформатного фотоаппарата (43,3 мм) к матрице отдельного фотоаппарата. Исходя из кроп-фактора, можно определить соответствующие объективы с фокусным расстоянием, обеспечивающие поле зрения, эквивалентное полноформатному фотоаппарату.
Лазерная перфорация	Процесс, при котором цифры, буквы или изображения создаются путем перфорирования основы с помощью лазера
Лазерное гравирование	Процесс, при котором личностные данные "выжигаются" с помощью лазера. Такие данные могут включать текст, фотографию и другие элементы защиты
Ламинат	Прозрачный материал, который может обладать элементами защиты и предназначенный для надежного прикрепления для защиты биографических данных или другой страницы документа
Ламинат или накладка с дифракционным устройством оптически изменяющегося изображения (DOVID)	Ламинат или накладка, содержащие DOVID, которые покрывают всю зону или расположены таким образом, чтобы защитить ключевые данные в документе
Линзовидный элемент	Элемент защиты, в котором линзовидная структура интегрирована в поверхность документа или используется в качестве средства верификации
Лист	Индивидуальная часть основы в паспорте, которая содержит более одной паспортной страницы
Лицо, подписывающее штрих-код	Подписывающее штрих-код лицо подписывает в цифровой форме данные (заголовок и сообщение), кодированные в штрих-коде. Подпись также хранится в штрих-коде.
Личность	Совокупность отличительных персональных и физических признаков, данных и качеств, позволяющих однозначно идентифицировать лицо среди других лиц. В биометрической системе личность обычно устанавливается при регистрации лица в системе с использованием так называемых исходных документов, таких как свидетельство о рождении и свидетельство о гражданстве
Логическая структура данных (LDS)	Логическая структура данных описывает, как должны храниться и форматироваться данные на бесконтактной ИС МСПД
Ложный допуск	Случай, когда биометрическая система ошибочно идентифицирует лицо или ошибочно верифицирует личность самозванца по предъявленной идентификационной информации

Термин	Определение
Ложный отказ	Случай, когда биометрическая система не может идентифицировать зарегистрированное лицо или не может верифицировать правильность предъявленной идентификационной информации зарегистрированного пользователя
Макушка головы	Верхняя часть головы без учета волос
Маркер	Вещество, не встречающееся в естественном виде, которое может быть добавлено к физическим компонентам МСПД и являющееся обычно элементом уровня 3, которое может быть обнаружено с помощью специального оборудования
Маркерное изображение	Фотография владельца МСПД, обычно представляющая собой изображение анфас, размеры которого скорректированы для выдерживания фиксированного расстояния между глазами. Оно может быть также слегка повернуто так, чтобы воображаемая горизонтальная линия между центрами глаз была параллельна верхней кромке прямоугольной фотографии, если этого не было достигнуто, когда делалась или вводилась оригинальная фотография
Маркированные чернила	Чернила, содержащие соединения, которые не являются естественно встречающимися веществами и которые могут быть обнаружены с применением специального оборудования
Мастер-ключ	Источник генерации цепи ключей
Мастер-список	Мастер-список представляет собой подписанный в цифровом формате список сертификатов CSCA, которым "доверяет" принимающее государство, выпускающее мастер-список (см. Doc 9303-12)
Материальная характеристика	Материальная характеристика предполагает включение в МСПД материала, который обычно не присутствует и не является очевидным при визуальной проверке. Присутствие такого материала можно обнаружить благодаря присутствию и объему соответствующей характеристики добавленного вещества
Машиносчитываемая виза (МСВ)	Виза, соответствующая спецификациям, содержащимся в части 7 документа Doc 9303. МСВ обычно размещается на визовой странице паспорта
Машиносчитываемая виза (МСВ-А) полного размера (формат А)	МСВ, соответствующая спецификациям размера, содержащимся в части 7 документа Doc 9303, полностью занимающая визовую страницу паспорта
Машиносчитываемая виза (МСВ-В) малого размера (формат В)	МСВ, соответствующая техническим требованиям части 7 документа Doc 9303, размер которой позволяет сохранять чистое место на паспортной визовой странице
Машиносчитываемая зона (МСЗ)	Зона установленного размера на МСПД, содержащая обязательные и факультативные данные, сформатированные для машинного считывания с применением методов OCR
Машиносчитываемый официальный проездной документ (МСОПД)	Документ, обычно в форме карты размера ПД1 или ПД2, который соответствует спецификациям частей 5 и 6 документа Doc 9303 и может использоваться для пересечения национальных границ по соглашению между соответствующими государствами

Термин	Определение
Машиносчитываемый официальный проездной документ размера 1 (ПД1)	Карта номинального размера, определенного для карты типа ID-1 (ИСО/МЭК 7810) (за исключением ее толщины)
Машиносчитываемый официальный проездной документ размера 2 (ПД2)	Карта или этикетка, соответствующая размерам, определенным для карты типа ID-2 (ИСО/МЭК 7810) (за исключением ее толщины)
Машиносчитываемый паспорт (МСП)	Паспорт, соответствующий спецификациям, содержащимся в части 4 документа Doc 9303. Обычно представляет собой книжку размера ПД3, содержащую страницы с информацией о владельце и государстве или организации выдачи и страницы для виз и прочих отметок. Машиносчитываемая информация содержится на двух строках текста OCR-B, каждая из которых включает 44 знака
Машиносчитываемый проездной документ (МСПД)	Выдаваемый государством или организацией официальный документ, соответствующий спецификациям документа Doc 9303, который используется его владельцем для международных поездок (например, МСП, МСВ, МСОПД) и содержит обязательные визуальные (визуально считываемые) данные и отдельные обязательные краткие данные в формате, пригодном для машинного считывания
Металлические чернила	Чернила, по внешнему виду напоминающие металл
Метамерные чернила	Соединение компонентов разных чернил, которые при определенных условиях (обычно при дневном свете) представляют один цвет, но эти компоненты не соответствуют друг другу по цвету при использовании световых волн другой длины
Микропечатный текст	Печатный текст или символы размером менее 0,25 мм/0,7 пункта кегля
Множественная биометрия	Использование более одного биометрического параметра
Модель документа	Модель документа охватывает серии национальных документов, имеющие одинаковый визуальный вид (например D, P, 1.2005), (D, P 2.2007) и (D,P, 3.2010). Одна страна в конкретный период времени может иметь в обращении несколько действительных моделей документов (например, GBR, P, 1, 2008) и (GBR, P, 2, 2010).
Морфинг	Технология манипулирования изображением, когда лица двух или более объектов трансформируются или сливаются в одно для получения одного лица на фотографии
Мошенническое изменение	Изменение подлинного документа для использования лицом, не имеющим на это права, для поездки в неразрешенный пункт назначения. Главным образом таким изменениям подвергаются биографические данные подлинного владельца, в частности, его фотография
Муар антисканирования	Изображение, обычно построенное из тонких линий при различном угловом размещении и заделанное в рисунок защитной основы. При обычном рассмотрении указанное изображение нельзя отличить от остальной защитной печати основы, но при сканировании или фотокопировании оригинала заделанное изображение становится видимым

Термин	Определение
Муаровый узор	Дефект изображения, напоминающий волнистые разводы, создаваемый в процессе фотографирования пейзажа или объекта, содержащий повторяющиеся детали (например, линии, точки и пр.), которые превышают разрешающую способность фотоаппарата
Набор данных аутентификации	Конкретный набор программ проверок модели документа в структуре базы данных аутентификации.
Накладка	Ультратонкая пленка или покрытие, которые могут наноситься на поверхность документа вместо ламината
Невозможность занесения в систему	Неспособность биометрической системы зарегистрировать лицо
Невозможность получения информации	Неспособность биометрической системы получить необходимый биометрический параметр для регистрации лица
Негласный съем информации	Несанкционированный перехват передаваемых данных
Нити	Небольшие нитеобразные частицы, заделанные в основу в процессе изготовления
Номер документа	Номер, уникальным образом идентифицирующий документ. Рекомендуется, чтобы номер документа и контрольный номер были идентичными
Обмен ключами	Процесс передачи сеансовых ключей в руки компетентных лиц
Обнаружение презентационного воздействия	Автоматическое обнаружение презентационного воздействия
Обычная отметка	Символ, который заменяет рукописную подпись владельца в случае, если владелец неспособен поставить подпись
Объект	Лицо, изображаемое на фотографии; данное лицо предназначено быть держателем МСПД
"Один к нескольким"	Сочетание идентификации "один ко многим" и верификации "один к одному". Как правило, процесс "один к нескольким" предполагает сравнение представленного биометрического образца с небольшим количеством биометрических контрольных шаблонов в файле. На него обычно делается ссылка при сопоставлении со списком "особого внимания", где указываются лица, требующие тщательной проверки идентификационной информации, или известные преступники, террористы и т. д.
"Один к одному"	Синоним термина "верификация"
"Один ко многим"	Синоним термина "идентификация"
Оконный или транспарентный элемент	Элемент защиты, создаваемый конструкцией основы, в котором часть основы изымается или заменяется транспарентным материалом, который может содержать дополнительные элементы защиты, такие как линзовидные структуры или осязаемые элементы

Термин	**Определение**
Оперативная память (RAM)	Энергозависимая память с произвольным доступом, используемая в интегральных схемах, которым необходимо энергопитание для сохранения данных
Операционная система	Программа управления различными прикладными программами, используемыми компьютером
Оптически изменяющийся элемент (OVF)	Изображение или элемент, цвет и/или рисунок которых меняется в зависимости от угла зрения или освещения. Примерами являются: элементы, включающие дифракционные структуры с высокой разрешающей способностью (устройства дифракционного оптически изменяющегося изображения (DOVID)), голограммы, меняющие цвет чернила (например, чернила с оптически изменяющимися свойствами) и другие дифракционные или отражающие материалы
Орган выдачи	Организация, выдающая МСПД
Орган, подписывающий визу (VS)	Полномочный орган, который получает данные из системы персонализации визы и который использует сертификат VS и соответствующий закрытый ключ для кодирования и проставления визуальной цифровой подписи
Орган, подписывающий список отклонений	Орган, который подписывает в цифровой форме список отклонений. Орган, подписывающий список отклонений, уполномочен своим национальным CSCA на выполнение этой функции путем выдачи сертификата на подписание списка отклонений
Орган, подписавший мастер-список	Орган, который подписывает в цифровом формате мастер-список сертификатов CSCA. Орган, подписывающий мастер-список, уполномочен его национальным CSCA на выполнение этой функции путем выдачи сертификата органа, подписывающего мастер-список
Ответ	Сообщение, возвращенное подчиненным компонентом главному после обработки команды, полученной подчиненным компонентом
Открытый ключ	Открытый компонент интегрированной асимметричной пары ключей, используемый для шифрования или верификации информации
Отличительная черта	Элемент документа, пригодный для доказательства его аутентичности (например, фотография, поглощающая инфракрасное излучение)
Отличительная черта (цифрового) документа	Особенность документа, которая может быть использована для верификации содержания документа. Примерами служат текстовая информация, такая как фамилия владельца или дата выдачи или печатное изображение владельца документа. Отличительная черта цифрового документа – это цифровая версия отличительной черты документа.
Отображенная подпись	Оригинальная подпись в письменной форме или цифровая репродукция оригинала
Отпечаток пальца (отпечатки пальцев)	Одно или несколько видимых воспроизведений поверхности отпечатка пальца(ев) владельца документа

Термин	Определение
Оценка	Число по шкале оценки от низкой до высокой, определяющее степень совпадения данных биометрического пробника (отыскиваемого лица) с конкретными данными из галереи (ранее зарегистрированным лицом)
Пара ключей	Пара цифровых ключей, а именно один открытый и один закрытый, которые используются для шифрования и подписи цифровой информации
Параллакс	Смещение или различие в видимом положении объекта, рассматриваемого вдоль двух различных линий зрения, измеряемое в виде угла или половины угла наклона между этими двумя линиями
Персонализация	Процесс, с помощью которого фотография, подпись и биографические данные вносятся в документ
Персональный идентификационный номер (PIN)	Цифровой код защиты, используемый как механизм местной верификации "один к одному" с целью убедиться, что владелец карты действительно является физическим лицом, которому разрешены доступ или получение определенного обслуживания, например право открытия определенной информации на карте
Повторное изображение	Повторяющееся изображение фотографии владельца, воспроизводимое в документе любым способом
Подбородок	Центральная, выдвинутая вперед часть нижней челюсти
Подделка	Несанкционированное копирование или воспроизводство подлинного защищенного документа, осуществляемое с помощью любых средств
Подлог	Мошенническое изменение любой части подлинного документа
Подписывающий документы орган	Орган, который выдает биометрический документ и удостоверяет, что внесенные в этот документ данные являются подлинными, и делает это таким образом, чтобы можно было обнаружить мошеннические изменения
Поле	Часть зоны, предназначенная для размещения индивидуального элемента данных
Политика обеспечения безопасности системы	Совокупность законов, правил и практики, регулирующих управление конфиденциальной информацией и другими ресурсами, а также их защиту и распространение в рамках конкретной системы
Полное изображение (лица) анфас	Фотография владельца МСПД, изготовленная в соответствии с техническими требованиями документа Doc 9303
Полномочный орган валидации виз (VVA)	Полномочный орган, который осуществляет валидацию видимой цифровой подписи на визе на основании политики в области валидации
Полномочный орган регистрации (RA)	Лицо или организация, несущие ответственность за идентификацию и аутентификацию заявителя на получение цифрового сертификата. RA не выдает и не подписывает сертификаты
Полномочный орган, выдавший документ	Орган, уполномоченный на выдачу МСПД законному владельцу

Термин	Определение
Порог	Контрольная оценка. Сравнение итогового значения программы проверки с соответствующим пороговым значением приводит к принятию решения "соответствует-не соответствует"
Постоянная память только для чтения (ROM)	Энергонезависимая память, которая заполняется один раз, как правило в ходе изготовления ИС. Она применяется для хранения операционных систем и алгоритмов, используемых полупроводником карты на интегральной схеме во время транзакций
Презентационное воздействие	Презентация предмета или особенности человека подсистеме сбора биометрических данных таким образом, что это может противоречить предусмотренным принципам биометрической системы
Приводка "с лицевой до оборотной стороны" (сквозная приводка)	Рисунок, напечатанный на обеих сторонах документа или на внутренней странице МСП, который при просмотре страницы на свет образует взаимопереплетенное изображение
Принимающее государство	Страна, проверяющая МСПД владельца
Пробник	Биометрический шаблон зарегистрированного пользователя, личность которого требуется установить
Проверка	Действия государства или организации, связанные с проверкой МСПД, предъявленного лицом (владельцем МСПД), совершающим поездку, и верификацией его аутентичности
Проверка уровня 1	Поверхностное изучение для быстрой проверки в пункте использования (легко идентифицируемые визуальные или тактильные характеристики)
Проверка уровня 2	Осмотр подготовленными инспекторами с использованием простого оборудования
Проверка уровня 3	Проверка экспертами-криминалистами
Проверять на совпадение/ проверка на совпадение	Процесс сравнения биометрического образца с ранее записанным шаблоном и оценки уровня сходства. Решение о допуске или отказе базируется на том, превышает ли оценка установленный порог
Программа проверки	Процедура проверки конкретных особенностей элемента (например, проверка наличия фотографии в инфракрасном свете).
Произвольный доступ	Способ хранения данных, при котором конкретные элементы данных можно извлекать без необходимости последовательного просмотра всех хранящихся данных
Проникающие номерные чернила	Чернила, содержащие цветовой компонент, которые проникают глубоко в основу
Пропуск ООН	Документ, в общем аналогичный паспорту, выдаваемый под эгидой наднационального органа (например, Организации Объединенных Наций)
Прямой захват	Процесс взятия биометрического образца путем взаимодействия между владельцем МСПД и биометрической системой

Термин	Определение
Радиальная дисторсия	Несовершенство изображения, при котором уровень увеличения меняется в зависимости от расстояния от оптической оси
Радужная (ирисовая) печать	Метод, при котором два или более цветов красок печатаются одновременно на одном прессе в целях создания контролируемого слияния цветов, аналогичного эффекту радуги. Также называется призматической, или ирисовой печатью
Размер шаблона	Объем памяти компьютера, занимаемый биометрическими данными
Разрешение на поездку	Разрешение в электронной и/или бумажной форме, выданное принимающим государством и разрешающее пассажиру совершить путешествие
Расстояние между глазами	Длина линии, соединяющей центры левого и правого глаз
Расстояние от глаза до рта	Расстояние между центром лица (M) и серединой рта (характерная точка 2.3 согласно ИСО/МЭК 14496-2).
Реактивные чернила	Чернила, которые содержат защитные реагенты в целях предотвращения попыток удаления с помощью химического стирания (изъятия), благодаря чему происходит видимая реакция при контакте документа с отбеливателем или растворителем
Регистрация	Процесс внесения идентификационной информации лица в биометрическую систему, увязки уникального идентификатора с данной личностью, а также сбора и записи соответствующих атрибутов лица в системе
Рельефный (трехмерный) рисунок (медальон)	Защитный фоновый рисунок, включающий изображение, созданное таким образом, чтобы создавалось впечатление, что данное изображение выдавлено или вдавлено на поверхности основы
Рисунок из черных и белых линий	Рисунок, составленный из тонких линий, часто в форме гильошированного узора, и иногда используемый в качестве границы защищаемого документа. Указанный рисунок видоизменяется от позитивного до негативного изображения по мере его рассмотрения вдоль страницы
Самозванец	Лицо, которое обращается за получением документа и получает его, выдавая себя за другое лицо, или лицо, которое изменяет собственные физические характеристики, чтобы представить себя другим лицом с целью использования документа такого лица
Сертификат	Электронный файл, удостоверяющий, что пара криптографических ключей принадлежит лицу или оборудованию или компоненту программного обеспечения, указанных в сертификате. Сертификат выпускается сертифицирующим полномочным органом. Подписывая сертификат, сертифицирующий полномочный орган утверждает связь между личностью лица или компонента и парой криптографических ключей. Сертификат может быть отозван, если он больше не удостоверяет действительность такой связи. Сертификат отличается ограниченным периодом действия
Сертификат X.509 v3	Международно признанный электронный документ, используемый для подтверждения идентификации и владения открытым ключом в сети связи. Он содержит наименование выдавшего органа, идентификационную информацию пользователя и цифровую подпись выдавшего органа

Термин	Определение
Сертификат органа, подписывающего визу	Сертификат, содержащий информацию, идентифицирующую орган, который ставит видимую цифровую подпись на визу, и содержащий открытый ключ, соответствующий закрытому ключу, с помощью которого была создана подпись
Сертификат открытого ключа	Информация об открытом ключе юридического лица, подписанная сертифицирующим полномочным органом и поэтому постоянно упоминаемая
Сертифицирующий полномочный орган (CA)	Надежный орган, выдающий цифровые сертификаты для PKI
Симметричный алгоритм	Тип криптографической операции с использованием одного и того же ключа или набора ключей как для шифрования открытого текста, так и для расшифровки соответствующего зашифрованного текста
Синтетический материал	Не имеющий бумажной основы материал, используемый для страниц биографических данных или карт. Термин "синтетический" используется как синоним термина "пластиковый", который охватывает такие материалы, как поликарбонат, полиэтилен и аналогичные материалы и их сочетания
Система	Специальная установка ИТ с определенными целями и операционной средой
Система обозначений штрих-кода	Сопоставление сообщений и штрих-кодов называется системой обозначений. Такое сопоставление определяется в спецификациях штрих-кода и включает в себя кодирование единичных цифр или знаков, размер так называемой "тихой" зоны вокруг штрих-кода, а также расчет контрольных сумм для целей коррекции ошибок г
Система открытого ключа	Криптографический метод с использованием пары ключей, один из которых закрытый, а второй – открытый. Если шифрование произведено с использованием открытого ключа, то для дешифрования необходимо применять соответствующий закрытый ключ, и наоборот
Система проверки	Система, используемая для проверки МСПД любым государственным или частным органом, которому необходимо установить достоверность МСПД и использовать данный документ для верификации личности, например пограничными властями, авиакомпаниями и другими перевозчиками, финансовыми учреждениями
Сквозная приводка (приводка "с лицевой до оборотной стороны")	См. термин "приводка "с лицевой до оборотной стороны""
Скимминг	Электронное считывание данных, хранящихся на бесконтактной ИС, без получения разрешения на такое считывание документа
Скрытое изображение	Спрятанное изображение, образуемое с помощью рельефного изображения, состоящего из линейных структур, которые варьируются по направлению и профилю, в результате чего создается спрятанное изображение, появляющееся под определенными углами зрения, которое создается методом глубокой печати "интаглио"

Термин	Определение
Сообщение	Минимальный набор информации, имеющей смысл, которая передается от отправителя к получателю. Эта информация может состоять из одной или нескольких транзакций карты или информации, связанной с транзакцией карты
Сопоставление 1:1	Биометрический процесс (алгоритм), сравнивающий образец фотографии с зарегистрированным образцом в заявленных идентификационных данных, также называемый "верификация"
Сопоставление 1:N	Биометрический процесс (алгоритм), направленный на поиск ранее неизвестного образца фотографии среди энного числа зарегистрированных образцов в базе данных, также называемый "идентификация".
Сопоставление биометрических данных	Процесс с использованием алгоритма, в ходе которого сравниваются шаблоны, полученные на основе биометрических контрольных данных, с непосредственно снимаемыми биометрическими данными, в результате чего определяется их соответствие или несоответствие
Список отзыва сертификатов (CRL)	Список отозванных сертификатов. Таким образом документы, связанные с (подписанные) сертификатом, включенным в CRL, утрачивают доверие
Сертификат подписи штрих-кода (BSC)	BSC представляет собой сертификат, который содержит открытый ключ лица, подписывающего штрих-код. Сертификаты лица, подписывающего штрих-код, используются для подтверждения действительности данных, которые были подписаны открытым ключом лица, подписывающего штрих-код.
Список отклонений	Подписанный список, выпущенный государством выдачи и перечисляющий несоответствия в проездных документах и/или ключах и сертификатах
Спуфинг	Фальсификация адреса отправителя сообщения для получения незаконного входа в защищенную систему. *Примечание. Разновидностями спуфинга являются выдача себя за другое лицо, имитация пользователем другого лица, несанкционированное проникновение вслед за зарегистрированным пользователем и подделка*
Сравнение	Процесс сопоставления биометрического образца с ранее введенным в память контрольным шаблоном или шаблонами. См. также термины "один ко многим" и "один к одному"
Стандарт кодирования данных (DES)	Метод кодирования данных, оговоренный в FIPS 46-3
Стандартный источник света D65 МКО	Широко используемый стандартный источник света, определенный Международной комиссией по освещению (МКО) и являющийся частью источников света серии D, старающихся представить стандартные условия освещения на открытом воздухе в различных частях мира
Стеганография	Изображение или информация, закодированные или скрытые в первичном визуальном изображении
Стойка АСПК	Стойка автоматизированной системы пограничного контроля для проверки электронных машиносчитываемых проездных документов.

Термин	Определение
Страница данных	Страница паспортной книжки, предпочтительно вторая или предпоследняя страница, которая содержит биографические данные владельца документа. См. термин "биографические данные"
Страница данных МСП	Страница МСП фиксированного размера, содержащая стандартные визуальные и машиносчитываемые данные
Структура форматов обмена общей биометрической информацией (CBEFF)	Общий формат файлов, способствующий обмену и интероперабельности биометрических данных
Структурная характеристика	Структурная характеристика предполагает включение измеримой структуры в МСПД. Присутствие такой структуры может быть ограничено и измерено с помощью индикаторного устройства
Схема цифровой (криптографической) подписи	Кортеж трех алгоритмов. Алгоритм генерирования ключей принимает параметр безопасности в качестве вводной информации, а в качестве выходной информации - пару ключей, включающую в себя закрытый и открытый ключи. Алгоритм подписи принимает закрытый ключ и сообщение в качестве вводной информации, а на выходе дает криптографическую подпись. Алгоритм верификации принимает открытый ключ в качестве вводной информации, сообщение и подпись, а на выходе указывает "действительная", если подпись была генерирована с использованием алгоритма генерирования подписи с закрытым ключом из пары ключей и сообщением в качестве вводной информации, в противном случае указывает и "недействительная"
Тактильный элемент	Элемент поверхности, дающий отчетливое "осязание" документа
Теневое изображение	Синоним термина "вторичное изображение". Повторное изображение фотографии владельца документа, меньшее по контрастности, и/или насыщению, и/или размеру
Термоусаживаемый ламинат	Ламинат, предназначенный для наложения на страницу биографических данных паспортной книжки путем применения температуры и давления
Термохромные чернила	Чернила, которые изменяют цвет, когда напечатанное изображение подвергается воздействию тепла (например, тепла тела)
Удостоверяющий документ	Документ, используемый для удостоверения личности владельца и органа, выдавшего документ, в который могут вноситься данные, необходимые в целях предполагаемого использования этого документа
Указательные отметки	Эти отметки печатаются на наружной кромке каждой страницы в последовательном порядке, начиная с верхней кромки первой страницы со снижением на следующей странице и т. д. Регистрационная отметка на последней странице находится в нижней части. Такой метод печати позволяет получить непрерывную полосу на кромке паспорта. Изъятие любой страницы будет выглядеть как разрыв. При печати в ультрафиолетовом свете эта полоса будет видна только при ультрафиолетовом освещении. Также называются "контрольными подборочными отметками"
Уполномоченная принимающая организация	Организация, которая уполномочена обрабатывать официальные проездные документы (например, эксплуатант воздушного судна), и в этом качестве в будущем может получить разрешение на регистрацию данных с использованием факультативной технологии увеличения емкости

Термин	Определение
Управление ключами	Процесс, с помощью которого криптографические ключи предоставляются для использования взаимодействующими уполномоченными сторонами
Устройство интерфейса	Любой терминал, устройство связи или установка, с которыми карта ICC связана во время операции
Устройство оптически изменяющегося изображения (OVD)	Элемент защиты, изменяющий различные цвета или изображения в зависимости от угла зрения или условий верификации
УФ-матовая основа	Основа, не дающая различимого флуоресцентного эффекта при освещении ультрафиолетовым светом
Участник ДОК	Государство – член ИКАО или другой орган, выдающие или намеревающиеся выдавать электронные МСПД, которые отвечают условиям участия в ДОК ИКАО
Физическая виза	Проездной документ из полиграфической фольги, вкладываемый в паспорт пассажира
Физическая охрана	Диапазон мер безопасности, применяемых в процессе производства в целях предотвращения кражи и несанкционированного доступа к данному процессу
Флуоресцентные чернила	Чернила, содержащие вещество, которое светится при воздействии света определенной длины волны, обычно УФ
Фосфоресцентные чернила	Чернила, содержащие пигмент, SHAкоторый светится при воздействии света определенной длины волны; реактивное свечение остается видимым, но затем постепенно угасает после удаления источника света
Фотография	Визуальное представление изображения лица владельца МСПД в печатной и хранимой в электронном виде форме
Фотокабина	Автоматизированная система цифровой съемки идентификационных фотографий в общественных местах или в офисах; в кабине созданы тщательно контролируемые условия освещенности, предусмотрены фотоаппарат, устройства освещения и периферийные устройства, такие как принтеры; кабина имеет входы с одной или двух сторон, закрываемые светоотражающими занавесями, обеспечивающими защиту от внешнего света
Фото киоск	Полуавтоматизированная система для цифровой съемки идентификационных фотографий на стойке; она предусматривает наличие фотоаппарата и устройства освещения и, как правило, имеет отдельную панель, установленную позади объекта для создания требуемого фона; во всех остальных случаях она открыта
Фотохромные чернила	Чернила, которые подвергаются обратимому изменению цвета под воздействием света определенной длины волны
Химические сенсибилизаторы	Защитные реагенты, предназначенные для защиты от попыток удаления с помощью химического стирания, при применении которых после вступления отбеливателей и растворителей в контакт с документом проявляются необратимые цвета

Термин	**Определение**
Хэш	Математическая формула, с помощью которой сообщение произвольной длины переводится в уникальную строку чисел фиксированной длины, известную под названием "краткая форма сообщения", которая в этом виде представляет первоначальное сообщение. Хэш является односторонней функцией, а это означает, что невозможно произвести обратный процесс и вернуть первоначальное сообщение. Кроме того, хэш-функция не обеспечивает получения одинаковой сжатой формы сообщения из двух различных источников
Целостность	Возможность подтвердить, что логическая структура данных и ее компоненты, созданные государством или организацией выдачи, не изменены
Центр глаза	Середина линии, соединяющей внутренний и внешний углы глаза. *Примечание 1. Центры глаз представляют собой характерные точки 12.1 и 12.2, как определено в ИСО/МЭК 14496-2.* *Примечание 2. Внутренний и внешний углы глаза определены в ИСО/МЭК 14496-2. Они представляют собой характерные точки 3.12 и 3.8 для правого глаза и 3.11 и 3.7 для левого глаза*
Центр лица	Середина линии, соединяющей центры двух глаз
Цифровая (криптографическая) подпись	Результат криптографической операции, обеспечивающей валидацию информации электронными средствами. Это НЕ подпись владельца МСПД, отображаемая в цифровой форме
Цифровая подпись	Сокращенное название видимой цифровой подписи.
Цифровое разрешение на поездку	Электронная виза, выдаваемая и соблюдаемая на территории выдающего ее государства.
Цифровой водяной знак	См. термин "стеганография"
Чернила, изменяющие цвет	Чернила, изменяющие свои визуальные характеристики в зависимости от угла зрения и/или качества стимулирующего источника (света)
Шаблон/контрольный шаблон	Данные, представляющие собой биометрические показатели зарегистрированного пользователя, используемые биометрической системой для сравнения с представляемыми впоследствии биометрическими образцами
Шифр	Тайнопись на основе использования ключа или набора заранее определенных правил или символов
Шифрование	Сокрытие информации на основе использования ключа таким образом, чтобы она не была понятна несанкционированному лицу
Штрих-код	Оптическое, машиносчитываемое, одномерное или двумерное изображение данных, касающихся объекта, к которому оно прилагается

Термин	Определение
Электрически стираемая программируемая постоянная память (EEPROM)	Технология энергонезависимой памяти, когда данные могут быть электрически стерты и перезаписаны
Электронный машиносчитываемый паспорт (электронный МСП)	МСПД размера ПД3, соответствующий спецификациям части 4 документа Doc 9303, который дополнительно содержит бесконтактную интегральную схему, обеспечивающую способность биометрической идентификации владельца. Обычно называется "электронным паспортом"
Электронный машиносчитываемый проездной документ (электронный МСПД)	МСПД (паспорт, виза или карта), содержащий встроенный чип бесконтактной интегральной схемы, который обеспечивает возможность использования его для биометрической идентификации владельца МСПД в соответствии со стандартами, установленными в соответствующей части документа Doc 9303 *"Машиносчитываемые проездные документы"*
Электронный машиносчитываемый официальный проездной документ (электронный МСОПД)	МСОПД размера ПД1 или ПД2, соответствующий спецификациям части 5 или части 6 документа Doc 9303, дополнительно содержащий чип бесконтактной интегральной схемы и обеспечивающий возможность биометрической идентификации владельца
Электронный паспорт	Общепринятое название электронного МСП. См. термин "электронный машиносчитываемый паспорт (электронный МСП)"
Энергонезависимая память	Полупроводниковая память, которая сохраняет содержащуюся информацию при отключении питания (т. е. ROM, EEPROM)
Этикетка	Самоклеющаяся бирка, используемая в качестве страницы данных паспорта. Такой метод не рекомендуется для широкого применения, особенно для удостоверяющих личность документов длительного пользования
"Якорь доверия"	В криптографических системах с иерархической структурой уполномоченный орган, доверие к которому принимается как должное, а не выводится теоретическим путем

4.3 Ключевые слова

Приводимые ниже ключевые слова используются для обозначения требований.

Слова "ДОЛЖЕН", "НЕ ДОЛЖЕН", "ТРЕБУЕТСЯ", "SHALL" (в русском языке передается глаголом в настоящем времени), "SHALL NOT" (в русском языке передается отрицательной формой глагола в настоящем времени), "СЛЕДУЕТ", "НЕ СЛЕДУЕТ", "РЕКОМЕНДУЕТСЯ", "МОЖЕТ" и "ФАКУЛЬТАТИВНО" пишутся в документе Doc 9303 заглавными буквами, и их следует понимать так, как указано в документе RFC 2119:

ДОЛЖЕН	Это слово или слова "ТРЕБУЕТСЯ" или "SHALL" означают, что данное определение в спецификации является абсолютным требованием спецификации

НЕ ДОЛЖЕН	Эти слова или слова "SHALL NOT" означают, что данное определение в спецификации является абсолютным запрещением
СЛЕДУЕТ	Это слово или прилагательное "РЕКОМЕНДУЕМЫЙ" означает, что могут существовать обоснованные причины в особых обстоятельствах игнорировать отдельный пункт, однако при этом полностью должны осознаваться и тщательно взвешиваться все последствия, прежде чем будет выбран другой курс действий
НЕ СЛЕДУЕТ	Эти слова или слова "НЕ РЕКОМЕНДУЕМЫЙ" означают, что могут существовать обоснованные причины в особых обстоятельствах для особого поведения, допустимого или даже полезного, однако при этом полностью должны осознаваться и тщательно взвешиваться все последствия этого, прежде чем предпринимать какие-либо особые действия, упомянутые в этом объяснении
МОЖЕТ	Это слово или причастие "ФАКУЛЬТАТИВНО" означает, что данный пункт действительно факультативный. Какой-то пользователь может выбрать вариант включения этого пункта потому, что этого требует особое применение или он считает, что это расширит применение, а другой пользователь может отказаться от этого. Один вид применения, который не включает какого-либо конкретного варианта, ДОЛЖЕН быть готовым взаимодействовать с другим применением, которое включает такой вариант, хотя, возможно, с пониженной функциональностью. Аналогичным образом применение, которое не включает какой-либо особый вариант, ДОЛЖНО быть готово взаимодействовать с другим видом применения, которое не включает этот вариант (конечно, за исключением характеристик, обеспечиваемых этим вариантом)
УСЛОВНО	Использование какого-либо пункта зависит от использования других пунктов. Поэтому дополнительно оговаривается, при каких условиях данный пункт ТРЕБУЕТСЯ или РЕКОМЕНДУЕТСЯ. Это дополнительное ключевое слово используется в документе Doc 9303 (не входит в документ RFC 2119)

Рекомендации по использованию. Определенные здесь модальные выражения следует использовать осторожно и умеренно. В частности, они ДОЛЖНЫ использоваться только тогда, когда это действительно необходимо для обеспечения взаимодействия или ограничения действий, которые потенциально могут привести к нанесению ущерба (например, ограничение повторных передач). Например, их не следует использовать в попытке навязать конкретную форму осуществления в случае, если такой метод не требуется для обеспечения интероперабельности.

Соображения, касающиеся безопасности. Эти термины часто используются для определения поведения, имеющего последствия с точки зрения безопасности. Последствия невыполнения того, что ДОЛЖНО делаться или что СЛЕДУЕТ делать, либо действий, которые согласно спецификации производиться НЕ ДОЛЖНЫ или производить НЕ СЛЕДУЕТ, с точки зрения безопасности могут быть весьма незначительными. Авторам документа следует не спеша и внимательно изучить последствия невыполнения рекомендаций или требований с точки зрения безопасности, так как в большинстве случаев специалисты по внедрению не будут располагать тем опытом и результатами обсуждений, которые были положены в основу конкретной спецификации.

В тех случаях, когда элементы внедряются ФАКУЛЬТАТИВНО, они ДОЛЖНЫ внедряться, как это указано в документе Doc 9303.

В документе Doc 9303 добавления носят информативный характер. Если делается заявление о соблюдении положений (информативного) добавления, то ключевые слова, используемые в таком добавлении, ДОЛЖНЫ употребляться, как указано.

4.4 Идентификаторы объектов

В частях 10, 11 и 12 документа Doc 9303 указаны идентификаторы объектов ИКАО. В настоящем разделе перечислены эти фактические идентификаторы объектов ИКАО:

```
-- Механизм защиты ИКАО
id-icao OBJECT IDENTIFIER::={joint-iso-itu-t(2) international(23) icao(136)}

id-icao-mrtd OBJECT IDENTIFIER ::= {id-icao 1}

id-icao-mrtd-security OBJECT IDENTIFIER ::= {id-icao-mrtd 1}

-- Объект защиты LDS
id-icao-mrtd-security-ldsSecurityObject OBJECT IDENTIFIER ::= {id-icao-
mrtdsecurity 1}

-- Мастер-список CSCA
id-icao-mrtd-security-cscaMasterList OBJECT IDENTIFIER ::= {id-icao-mrtdsecurity
2}

id-icao-mrtd-security-cscaMasterListSigningKey OBJECT IDENTIFIER ::= {id-
icaomrtd-security 3}

-- Протокол активной аутентификации
id-icao-aaProtocolObject OBJECT IDENTIFIER ::= {id-icao-mrtd-security 5}

-- Изменение названия CSCA
id-icao-mrtd-security-extensions OBJECT IDENTIFIER ::= {id-icao-mrtd-security
6}

id-icao-mrtd-security-extensions-nameChange OBJECT IDENTIFIER ::= {id-icaomrtd-
security-extensions 1}

-- Список типов документа, см. TR "Ведение LDS и PKI"
id-icao-mrtd-security-extensions-documentTypeList OBJECT IDENTIFIER ::= {idicao-
mrtd-security-extensions 2}

-- Идентификаторы базовых объектов списка отклонений
id-icao-mrtd-security-DeviationList OBJECT IDENTIFIER ::= {id-icao-mrtdsecurity
7}

id-icao-mrtd-security-DeviationListSigningKey OBJECT IDENTIFIER ::= {id-
icaomrtd-security 8}

id-Deviation-CertOrKey OBJECT IDENTIFIER ::= {id-icao-DeviationList 1}

id-Deviation-CertOrKey-DSSignature OBJECT IDENTIFIER ::= {id-DeviationCertOrKey
1}

id-Deviation-CertOrKey-DSEncoding OBJECT IDENTIFIER ::= {id-DeviationCertOrKey 2}

id-Deviation-CertOrKey-CSCAEncoding OBJECT IDENTIFIER ::= {id-DeviationCertOrKey
3}

id-Deviation-CertOrKey-AAKeyCompromised OBJECT IDENTIFIER ::= {idDeviation-
CertOrKey 4}
```

```
id-Deviation-LDS OBJECT IDENTIFIER ::= {id-icao-DeviationList 2}

id-Deviation-LDS-DGMalformed OBJECT IDENTIFIER ::= {id-Deviation-LDS 1}

id-Deviation-LDS-SODSignatureWrong OBJECT IDENTIFIER ::= {id-Deviation-LDS 3}

id-Deviation-LDS-COMInconsistent OBJECT IDENTIFIER ::= {id-Deviation-LDS 4}

id-Deviation-MRZ OBJECT IDENTIFIER ::= {id-icao-DeviationList 3}

id-Deviation-MRZ-WrongData OBJECT IDENTIFIER ::= {id-Deviation-MRZ 1}

id-Deviation-MRZ-WrongCheckDigit OBJECT IDENTIFIER ::= {id-Deviation-MRZ 2}

id-Deviation-Chip OBJECT IDENTIFIER ::= {id-icao-DeviationList 4}

id-Deviation-NationalUse OBJECT IDENTIFIER ::= {id-icao-DeviationList 5}

-- Идентификаторы объектов LDS2
id-icao-mrtd-security-lds2 OBJECT IDENTIFIER ::= {id-icao-mrtd-security 9}

id-icao-lds2Signer OBJECT IDENTIFIER ::= {id-icao-mrtd-security-lds2 8}

id-icao-tsSigner OBJECT IDENTIFIER ::= {id-icao-lds2Signer 1}

id-icao-vSigner OBJECT IDENTIFIER ::= {id-icao-lds2Signer 2}

id-icao-bSigner OBJECT IDENTIFIER ::= {id-icao-lds2Signer 3}

id-icao-lds2-travelRecords OBJECT IDENTIFIER ::= {id-icao-lds2 1}

id-icao-lds2-travelRecords-application OBJECT IDENTIFIER ::= { id-icao-lds2-
travelRecords 1}

id-icao-lds2-travelRecords-access OBJECT IDENTIFIER ::= { id-icao-lds2-
travelRecords 3}

id-icao-lds2-visaRecords OBJECT IDENTIFIER ::= {id-icao-lds2 2}

id-icao-lds2-visaRecords-application OBJECT IDENTIFIER ::= { id-icao-lds2-
visaRecords 1}

id-icao-lds2-visaRecords-access OBJECT IDENTIFIER ::= { id-icao-lds2-visaRecords
3}

id-icao-lds2-additionalBiometrics OBJECT IDENTIFIER ::= {id-icao-lds2 3}

id-icao-lds2- additionalBiometrics-application OBJECT IDENTIFIER ::= { id-
icaolds2- additionalBiometrics 1}

id-icao-lds2- additionalBiometrics-access OBJECT IDENTIFIER ::= { id-icao-lds2-
additionalBiometrics 3}

-- Идентификаторы объектов SPOC
id-icao-spoc OBJECT IDENTIFIER ::= {id-icao-mrtd-security 10}
```

```
id-icao-spocClient OBJECT IDENTIFIER ::= {id-icao-spoc 1}

id-icao-spocServer OBJECT IDENTIFIER ::= {id-icao-spoc 2}

-- Идентификаторы объектов VDS
id-icao-vds OBJECT IDENTIFIER ::= { id-icao-mrtd-security 11}

-- Идентификаторы объектов DTC

id-icao-dtc OBJECT IDENTIFIER ::= { id-icao-mrtd-security 12}

id-icao-dtcSigner OBJECT IDENTIFIER ::= {id-icao-dtc 1}

id-icao-dtcAttributes OBJECT IDENTIFIER ::= {id-icao-dtc 2}

id-icao-dtcCapabilitiesInfo OBJECT IDENTIFIER ::= {id-icao-dtcAttributes 1}

-- Идентификаторы объектов EF.DIR
id-EFDIR OBJECT IDENTIFIER ::= { id-icao-mrtd-security 13}
```

4.5 Использование примечаний

Примечания к стандартам ИСО/МЭК носят информативный характер, тогда как примечания в документе Doc 9303 являются частью нормообразующего текста и используются для того, чтобы выделить те или иные требования или предоставить дополнительную информацию.

5. УКАЗАНИЯ ПО ИСПОЛЬЗОВАНИЮ ДОКУМЕНТА DOC 9303

5.1 Структура документа Doc 9303

Документ Doc 9303 состоит из тринадцати частей. Каждая часть посвящена конкретному компоненту МСПД. Части документа Doc 9303 составлены таким образом, чтобы орган, выдающий МСПД, мог скомпоновать полную подборку соответствующих спецификаций, относящихся к конкретному типу МСПД (форм-фактор). Взаимосвязь между этими форм-факторами и частями документа Doc 9303 описана в разделе 5.2 данной части 1.

В перечисленных ниже частях содержится полный набор спецификаций документа Doc 9303, относящихся к машиносчитываемым проездным документам.

Часть 1. Введение

Настоящий документ представляет собой часть 1.

Часть 2. Спецификации, касающиеся безопасности разработки, изготовления и выдачи МСПД

В части 2 содержатся обязательные и факультативные спецификации в отношении мер предосторожности, которые должны принимать полномочные органы, выдающие проездные документы, в целях обеспечения защиты своих МСПД, средств их персонализации и выдачи законным владельцам от актов мошенничества. Также приводятся обязательные и факультативные спецификации для средств физической защиты помещений, где изготовляются, персонализируются и выдаются МСПД, и для проверки персонала, занятого в этих операциях.

Часть 3. Спецификации, общие для всех МСПД

В части 3 определены спецификации, общие для машиносчитываемых проездных документов (МСПД) размеров ПД1, ПД2 и ПД3, в том числе необходимые для обеспечения глобальной интероперабельности с использованием визуальной проверки и средств машинного считывания (оптического распознавания знаков). Подробные технические требования, применимые к каждому типу документов, содержатся в частях 4–7 документа Doc 9303.

Часть 4. Спецификации машиносчитываемых паспортов (МСП) и других МСПД размера ПД3

В части 4 определены конкретные технические требования для машиносчитываемых паспортов (МСП) размера ПД3 и других машиносчитываемых проездных документов (МСПД) размера ПД3. Для краткости во всем тексте части 4 используется термин МСП; за исключением особо оговоренных случаев, все содержащиеся в этой части спецификации в равной мере относятся ко всем другим МСПД размера ПД3.

Часть 5. Спецификации машиносчитываемых официальных проездных документов (МСОПД) размера ПД1

В части 5 определены технические требования, конкретно относящиеся к машиносчитываемым официальным проездным документам (МСОПД) размера ПД1.

Часть 6. Спецификации машиносчитываемых официальных проездных документов (МСОПД) размера ПД2

В части 6 определены технические требования, конкретно относящиеся к машиносчитываемым официальным проездным документам (МСОПД) размера ПД2.

Часть 7. Машиносчитываемые визы

Часть 7 определяет спецификации для машиносчитываемых виз (МСВ), которые обеспечивают совместимость и глобальный обмен с использованием как визуальных средств (визуальное считывание), так и средств машинного считывания. Спецификации для виз, если они выдаются государством и приемлемы для принимающего государства, могут использоваться для целей поездок. МСВ как минимум содержат оговоренные данные в форме, доступной для визуального считывания и считывания методами оптического распознавания знаков, представленными в части 7.

Часть 7 содержит технические требования к визам формата A и формата B и основана на материале части 2 *"Машиносчитываемые визы"* третьего издания документа Doc 9303 (2005).

Часть 8. Проездные документы для использования в чрезвычайных ситуациях

В части 8 содержится инструктивный материал и спецификации по экстренно выдаваемым проездным документам (ETD). Цель этого инструктивного материала заключается в стимулировании применения единого подхода к выдаче ETD в целях повышения степени защищенности документа, защиты физических лиц, обеспечения большей уверенности сотрудников пограничного контроля при обработке ETD в портах и рассмотрения уязвимых мест, создаваемых непоследовательностью практики и особенностями системы безопасности. В части 8 также рассматриваются вопросы использования видимых цифровых подписей в ETD.

Часть 9. Применение средств биометрической идентификации и электронного хранения данных в МСПД

В части 9 определяются технические требования, дополняющие спецификации на базовые МСПД, которые изложены в частях 3, 4, 5, 6 и 7 документа Doc 9303, для использования государствами, решившими выдавать электронные машиносчитываемые проездные документы (электронные МСПД), которые могут использоваться любым принимающим государством, имеющим соответствующее оборудование для считывания с документа гораздо большего объема данных, касающихся самого электронного МСПД и его владельца. Они включают обязательные глобально интероперабельные биометрические данные, которые могут вводиться в системы распознавания черт лица и, факультативно, в системы распознавания отпечатков пальцев или радужной оболочки глаза. Этими спецификациями предусматривается хранение глобально интероперабельных биометрических данных в форме изображений высокой разрешающей способности.

Часть 10. Логическая структура данных (LDS) для хранения биометрических и других данных на бесконтактной интегральной схеме (ИС)

В части 10 определена логическая структура данных (LDS) электронных МСПД, необходимая для обеспечения глобальной интероперабельности. Технология расширения емкости бесконтактной интегральной схемы, содержащейся в МСПД, в случае ее выбора государством или организацией выдачи ПОЗВОЛЯЕТ получить доступ к этим данным принимающему государству. В части 10 определены спецификации в отношении стандартной организации таких данных. Они требуют идентификации всех обязательных и факультативных элементов данных и нормативного упорядочения и/или группирования элементов данных, чтобы ОБЕСПЕЧИТЬ глобальную интероперабельность при считывании деталей (элементов данных), записанных на факультативном устройстве увеличения емкости в МСПД (электронном МСПД).

Часть 11. Механизмы защиты МСПД

Часть 11 содержит спецификации, позволяющие государствам и поставщикам реализовать элементы криптографической защиты машиносчитываемых проездных документов (электронных МСПД) для обеспечения доступа к ICC в режиме "только для чтения".

Часть 11 содержит криптографические протоколы для:

- предотвращения скимминга данных с бесконтактной ИС;
- предотвращения перехвата обмена информацией между ИС и считывающим устройством;
- обеспечения аутентификации данных, хранящихся на ИС, на основе PKI, описанной в части 12, и обеспечения аутентификации самой ИС.

Часть 12. Инфраструктура открытых ключей для МСПД

В части 12 содержится определение инфраструктуры открытых ключей (PKI) для внедрения и использования электронных МСПД. Определяются требования для государств или организаций выдачи, в том числе относительно функционирования сертифицирующего полномочного органа (CA), который выдает сертификаты и списки CRL. Также определены требования в отношении принимающих государств и используемых ими систем проверки для валидации таких сертификатов и CRL.

Часть 13. Видимые цифровые подписи для неэлектронных документов

В части 13 описываются цифровые подписи, обеспечивающие аутентичность и целостность неэлектронных документов относительно недорогим, но очень надежным образом с использованием асимметрической криптографии. Информация на неэлектронных документах криптографически подписана, подпись закодирована в виде двухмерного штрих-кода и напечатана на самом документе.

5.2 Взаимосвязь между форм-факторами МСПД и соответствующими частями документа Doc 9303

Из таблицы 1-1 видно, какие части документа Doc 9303 имеют отношение к конкретным типам МСПД (форм-факторам).

Таблица 1-1. Таблица перекрестных ссылок на форм-факторы

	Часть документа Doc 9303												
	1	2	3	4	5	6	7	8	9	10	11	12	13
МСПД размера ПД3 (МСП)	√	√	√	√									
Электронный МСПД размера ПД3 (электронный МСП)	√	√	√	√					√	√	√	√	
МСОПД размера ПД1	√	√	√		√								
Электронный МСОПД размера ПД1	√	√	√		√				√	√	√	√	
МСОПД размера ПД2	√	√	√			√							
Электронный МСОПД размера ПД2	√	√	√			√			√	√	√	√	
МСВ	√	√	√				√						√
ETD	√	√	√					√					√

6. СПРАВОЧНЫЕ МАТЕРИАЛЫ (НОРМАТИВНЫЕ)

Некоторые положения международных стандартов, упоминаемых в настоящем тексте, входят в материал документа Doc 9303. При наличии расхождений между спецификациями документа Doc 9303 и упоминаемыми стандартами, содержащими конкретные требования к машиносчитываемым проездным документам, включая машиносчитываемые визы, преобладающую силу имеют спецификации, содержащиеся в данном документе.

Приложение 9 Конвенция о международной гражданской авиации (Чикагская конвенция). Приложение 9 *"Упрощение формальностей".*

RFC 2119 С. Бреднер. Ключевые слова для обозначения уровня требований в RFC. BCP 14, RFC 2119. Март 1997 г.

— КОНЕЦ —

ISBN 978-92-9265-336-1