ИКАО

Doc 9303

Машиносчитываемые проездные документы

Издание восьмое, 2021

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

Утверждено и опубликовано с санкции Генерального секретаря

Международная организация гражданской авиации

ИКАО

Doc 9303

Машиносчитываемые проездные документы

Издание восьмое, 2021

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

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, Quebec, Canada H3C 5H7

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

Doc 9303. ***Машиносчитываемые проездные документы***
Часть 2. ***Спецификации, касающиеся безопасности разработки, изготовления и выдачи МСПД***
Заказ № 9303P2
ISBN 978-92-9265-462-7 (бумажная копия)

ПОПРАВКИ

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

РЕГИСТРАЦИЯ ПОПРАВОК И ИСПРАВЛЕНИЙ

ПОПРАВКИ		
№	Дата	Кем внесено

ИСПРАВЛЕНИЯ		
№	Дата	Кем внесено

ОГЛАВЛЕНИЕ

Страница

1. СФЕРА ПРИМЕНЕНИЯ 1

2. ЗАЩИТА МСПД И СРЕДСТВ ЕГО ВЫДАЧИ 1

3. АВТОМАТИЗИРОВАННАЯ ВЕРИФИКАЦИЯ ДОКУМЕНТОВ 2

3.1 Типы элементов 3
3.2 Базовые принципы 5
3.3 Автоматизированная аутентификация и электронные МСПД 5

4. ОХРАНА МЕСТ ИЗГОТОВЛЕНИЯ (РАЗРАБОТКА И ПРОИЗВОДСТВО) И ВЫДАЧИ МСПД ... 6

4.1 Способность к восстановлению 7
4.2 Физическая защита и контроль доступа 7
4.3 Учет производственных материалов 8
4.4 Транспортировка 8
4.5 Персонал 8
4.6 Кибербезопасность 8

5. ПРЕДОСТАВЛЕНИЕ ИНФОРМАЦИИ О НОВЫХ МСПД 9

6. ПРЕДОСТАВЛЕНИЕ ИНФОРМАЦИИ ОБ УТЕРЯННЫХ И ПОХИЩЕННЫХ МСПД 9

6.1 Инициативные каналы связи с владельцами документов 9
6.2 Организация национальных баз данных об утерянных, похищенных и аннулированных проездных документах 10
6.3 Обмен информацией об утерянных, похищенных и аннулированных проездных документах с ИНТЕРПОЛом и систематическая выверка документов по базам данных ИНТЕРПОЛа в рамках первичного контроля 10
6.4 Введение мер контроля для выявления случаев представления утерянного, похищенного или аннулированного документа при пересечении границы 11

7. СПРАВОЧНЫЕ МАТЕРИАЛЫ (НОРМАТИВНЫЕ) 13

ДОБАВЛЕНИЕ А К ЧАСТИ 2. СТАНДАРТЫ ЗАЩИТЫ МСПД (ИНФОРМАЦИОННОЕ) ..... Доб А-1

A.1 Сфера применения ..... Доб А-1
A.2 Введение ..... Доб А-1
A.3 Основные принципы ..... Доб А-2
A.4 Основные угрозы целостности проездных документов ..... Доб А-3
A.5 Элементы и методы защиты ..... Доб А-4

Страница

ДОБАВЛЕНИЕ B К ЧАСТИ 2. АВТОМАТИЗИРОВАННАЯ ВЕРИФИКАЦИЯ ЭЛЕМЕНТОВ ЗАЩИТЫ ДОКУМЕНТОВ (ИНФОРМАЦИОННОЕ) ..... Доб B-1

B.1 Сфера применения ..... Доб B-1
B.2 Считывающие устройства для документов и системы автоматизированной аутентификации ..... Доб B-1
B.3 Элементы защиты и их применение для автоматизированной аутентификации ..... Доб B-3
B.4 Критерии выбора элементов защиты, пригодных для автоматизированной верификации Доб B-14

ДОБАВЛЕНИЕ C К ЧАСТИ 2. ОПТИЧЕСКАЯ АВТОМАТИЗИРОВАННАЯ АУТЕНТИФИКАЦИЯ (ИНФОРМАЦИОННОЕ) ..... Доб C-1

C.1 Введение ..... Доб C-1
C.2 Определения ..... Доб C-3
C.3 Каталог общих процедур проверки ..... Доб C-9
C.4 Рекомендации относительно автоматизированной аутентификации МСПД ..... Доб C-16
C.5 Контроль за соблюдением процедур защиты данных ..... Доб C-54
C.6 Библиография ..... Доб C-56

ДОБАВЛЕНИЕ D К ЧАСТИ 2. ПРЕДОТВРАЩЕНИЕ МОШЕННИЧЕСТВА, СВЯЗАННОГО С ПРОЦЕССОМ ВЫДАЧИ (ИНФОРМАЦИОННОЕ) ..... Доб D-1

D.1 Сфера применения ..... Доб D-1
D.2 Мошенничество и его предупреждение ..... Доб D-1
D.3 Рекомендуемые меры борьбы с мошенничеством ..... Доб D-2
D.4 Процедуры предотвращения мошенничества при обращении за документом ..... Доб D-2
D.5 Контроль за центрами выдачи ..... Доб D-4

ДОБАВЛЕНИЕ E К ЧАСТИ 2. ОСНОВНЫЕ СООБРАЖЕНИЯ, КАСАЮЩИЕСЯ БАЗЫ ДАННЫХ ASF/SLTD (ИНФОРМАЦИОННОЕ) ..... Доб E-1

1. СФЕРА ПРИМЕНЕНИЯ

Настоящая часть содержит обязательные и факультативные спецификации в отношении мер предосторожности, которые надлежит принимать полномочным органам, выдающим проездные документы, для обеспечения защиты своих МСПД и средств их персонализации и выдачи законным владельцам от актов мошенничества. Приводятся также обязательные и факультативные технические требования, касающиеся физической защиты помещений, в которых проводится изготовление, персонализация и выдача МСПД, а также проверки персонала, участвующего в этой работе.

Увеличение числа путешественников во всем мире и ожидаемое сохранение этой тенденции наряду с ростом международной преступности, терроризма и незаконной иммиграции вызывают все бóльшую обеспокоенность относительно защиты проездных документов, в связи с чем возникла необходимость в выработке рекомендаций, касающихся возможных действий по повышению устойчивости этих документов к попыткам нарушения их защиты или ненадлежащего использования. По сложившейся практике документ Doc 9303 не содержит рекомендаций о конкретных элементах защиты проездных документов. Каждое государство выдачи таких документов может предусматривать такие меры предосторожности, которые оно считает целесообразными для защиты выдаваемых национальных проездных документов от актов подделки, подлога и других видов нарушения целостности, избегая при этом действий, которые могли бы негативно отразиться на способности машинного считывания с использованием технологии OCR.

Учитывая необходимость повышения уровня защиты документов, технические консультанты ИКАО считают целесообразным опубликовать свод "рекомендуемых минимальных стандартов защиты", которым все государства могли бы руководствоваться при выдаче машиносчитываемых проездных документов. С учетом этого:

- в добавлении A приводятся рекомендации относительно усиления мер защиты машиносчитываемых проездных документов;
- в добавлении B содержатся рекомендации, касающиеся автоматизированной аутентификации элементов обеспечения безопасности, предусмотренных для этих документов;
- в добавлении C описываются меры защиты, которые следует принимать для обеспечения безопасности в ходе операций по персонализации и перевозке документов;
- в добавлении D приводится описание рисков мошенничества, связанных с процессом применения и выдачи МСПД.

2. ЗАЩИТА МСПД И СРЕДСТВ ЕГО ВЫДАЧИ

До выдачи проездного документа проводится установление личности владельца и его права на получение проездного документа в соответствии с Программой идентификации пассажиров (TRIP) ИКАО, рекомендациями которой предусматривается установление подлинности личности [ICAO EOI]; соответствующая информация размещена на веб-сайте по адресу: https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx.

При разработке МСПД и средств его выдачи предусматриваются меры защиты документа от мошеннических актов в течение срока его действия. Методы мошеннических актов можно классифицировать следующим образом:

- *Подделкой* является создание, полностью или частично, документа, который напоминает подлинный МСПД, с намерением использования его как если бы он был подлинным. Подделки могут выпускаться путем дублирования или имитации оригинальных методов изготовления и используемых при этом материалов или применения методов копирования.

- *Мошенническое изменение, также именуемое подлогом,* предполагает изменение подлинного документа в попытке использования его для поездки лицом, не имеющим на это права, в неразрешенный пункт назначения. Чаще всего таким изменениям подвергаются биографические данные подлинного владельца, в частности его фотография.

- *Самозванцы.* "Самозванец" определяется как лицо, выдающее себя за другое лицо. Необходимо предусматривать элементы защиты, способствующие визуальному и/или автоматизированному обнаружению случаев мошеннического использования МСПД самозванцем.

- *Спуфинг* (злонамеренное искажение информации). Фальсификация адреса источника передаваемой информации с целью получения незаконного входа в систему безопасности.

  Примечание. К видам спуфинга относятся: имитация личности (Impersonating), маскировка под законного пользователя (masquerading), проникновение в систему под прикрытием законного пользователя (piggybacking) и подделка (mimicking).

- *Морфинг (morphing).* Морфинг представляет собой технологию преобразования изображения, позволяющую трансформировать и объединить изображения двух или более конкретных лиц в целях создания одного фотографического изображения лица.

Существуют признанные методы обеспечения защиты от перечисленных выше типов мошеннических актов. К ним относятся использование материалов, не имеющихся в широком доступе, узкоспециализированных систем проектирования и производственных процессов, требующих специального оборудования и опыта. В добавлении А к настоящей главе перечислены некоторые известные методы обеспечения защиты МСПД, позволяющие сотруднику, проводящему проверку, обнаружить подделку или мошенническое изменение документа визуально или с помощью простейшего оборудования, например увеличительного стекла или ультрафиолетовой лампы.

Все МСПД, соответствующие требованиям документа Doc 9303, должны использовать конкретные базовые элементы защиты, указанные в таблице А-1 добавления А.

3. АВТОМАТИЗИРОВАННАЯ ВЕРИФИКАЦИЯ ДОКУМЕНТОВ

За последнее десятилетие достигнут значительный прогресс в области автоматизированной аутентификации машиносчитываемых проездных документов (МСПД). Новые технологии, используемые при проектировании элементов обеспечения безопасности МСПД и разработке систем аутентификации (считывающие устройства, программные средства и т. д.), обеспечили возможность введения автоматизированной системы аутентификации документации в состав ряда контрольных инфраструктур и процессов (например, пограничный контроль).

Однако несмотря на то, что технические достижения обеспечивают более высокий уровень безопасности и эффективности эксплуатационных процессов, эксперты, изготовители и полномочные органы, работающие в этой области, сталкиваются с новыми проблемами. Некоторые из основных проблем заключаются в следующем: недостаточный уровень согласования и стандартизации используемых процессов и

недостаточный уровень координации между основными сторонами – участниками этих процессов, в результате чего элементы и компоненты систем разрабатываются независимо и без учета основных последствий, обусловленных их взаимодействием. Более того, сложность и разнообразие имеющихся в настоящее время на рынке систем значительно затрудняет проведение их оценки и/или сравнения.

В настоящем разделе содержатся рекомендации относительно автоматизированной аутентификации элементов защиты, включенных в МСПД в соответствии со спецификациями документа Doc 9303. Основой настоящего раздела являются положения добавления A к настоящей части и рекомендуемые в нем стандарты защиты. В добавлении B содержатся рекомендации, касающиеся автоматизированной верификации элементов защиты (основанных на материалах, использовании защищенной печати и методах защиты от копирования) на основе использования возможностей устройств для считывания документов, обеспечивающих захват изображений с высокой разрешающей способностью в визуальном, инфракрасном и ультрафиолетовом спектральном диапазонах. Наконец, в добавлении C приводится перечень рекомендаций, отражающих передовую практику, которые предназначены для основных сторон, участвующих в разработке, внедрении и использовании автоматизированных систем аутентификации и их основных компонентов.

Цель рекомендаций, содержащихся в настоящем разделе, заключается в улучшении защиты машиносчитываемых проездных документов во всем мире путем использования процедур автоматизированной верификации документов, учитывающих:

- структуру машиносчитываемых проездных документов, определенную в документе Doc 9303, с обеспечением обратной совместимости;

- элементы защиты, рекомендуемые в добавлении A к настоящей части;

- использование технических возможностей усовершенствованных считывающих устройств, установленных во всем мире для обработки электронных МСПД в соответствии с рекомендациями, содержащимися в добавлениях B и C настоящей части

Вместе с тем каждое государство должно провести оценку рисков, связанных с автоматизированной аутентификацией документов на своей национальной границе, в целях выявления наиболее значимых преимуществ и минимизации рисков. Документ Doc 9303 не определяет какой-либо элемент в качестве средства обеспечения глобальной интероперабельности при автоматизированной верификации документов, поскольку использование какого-либо одного элемента во всем мире сделает его весьма уязвимым к мошенническим актам. Поэтому в целях сведения рисков к минимуму государствам следует применять разнообразные элементы защиты.

3.1 Типы элементов

Существуют три основные категории машинноверифицируемых элементов защиты. Ниже приводится их описание и примеры элементов защиты, поддающиеся автоматизированной верификации.

3.1.1 Структурные элементы

Структурный элемент предполагает включение поддающейся измерению структуры в или на страницу данных МСПД. Речь идет об элементе защиты, содержащем какую-либо форму верифицируемой информации, основанной на физической структуре элемента. В качестве примеров можно привести следующее:

- интерференционные характеристики голограммы или другого устройства с оптически изменяющимися свойствами, которые можно быть однозначно идентифицировать при помощи соответствующего считывающего устройства;

- светоотражающее изображение, встроенное в защитный ламинат;
- контролируемое пропускание света через определенные зоны подложки.

3.1.2 Вещественные элементы

Вещественный элемент предполагает включение в МСПД материала, который обычно не присутствует в нем и наличие которого не является очевидным при визуальной проверке. Наличие такого материала может быть обнаружено за счет присутствия и параметров соответствующего свойства добавленного материала. При этом идентифицируется определенная характеристика материала, используемого при построении данного элемента. В частности, в качестве примеров можно привести следующее:

- использование пигментов, обычно в чернилах, которые реагируют особым и необычным способом на свет определенной длины волны (который может быть инфракрасным или ультрафиолетовым) или обладают магнитными или электромагнитными свойствами;
- включение в компонент страницы данных материалов, например волокон, индивидуальные размеры или распределение по размерам которых соответствует предопределенному техническому условию.

3.1.3 Информационные элементы

Видимое изображение на странице данных МСПД может содержать скрытую информацию, обнаружить которую можно с помощью соответствующего приспособления, встроенного в считыватель. Такая скрытая информация может находиться в защищенной странице данных, но чаще ее включают в раздел личных данных, особенно в напечатанную фотографию.

Включение скрытой информации в страницу данных МСПД может потребовать применения вещественных или структурных элементов для обеспечения нескольких уровней защиты. В этом контексте термин "стеганография" означает особый класс информационных элементов, имеющих, как правило, форму цифровой информации, которая скрыта внутри изображения, обычно либо на фотографии владельца, либо на защищенном напечатанном фоне. Такую информацию можно декодировать с помощью приспособления, встроенного в полностраничное считывающее устройство, которое рассчитано на обнаружение этого элемента в конкретном месте. Такой информацией может быть, например, номер проездного документа. В этом случае считывающее устройство можно запрограммировать на сравнение обнаруженного таким образом номера проездного документа с номером проездного документа, указанным в МСЗ. Для такого сравнения не требуется допуск к каким-либо данным, хранящимся на бесконтактной ИС электронного МСПД. Примерами элементов такого типа являются:

- закодированные данные, хранящиеся в документе на магнитных носителях, таких как специальные защитные нити;
- рисунки, включающие скрытые данные, которые можно обнаружить только при просмотре с использованием определенной длины волны света, оптических фильтров или специальных программных средств обработки изображения.

В более сложных формах объем хранящейся информации может быть значительным, и она может верифицироваться с помощью электронного сравнения с данными, хранящимися на бесконтактной ИС электронного МСПД.

3.2 Базовые принципы

Все три типа элементов, а именно структурные, вещественные и информационные, могут включаться в проездные документы для верификации с помощью предназначенных для этого считывающих устройств. В настоящее время имеются считывающие устройства, которые могут обнаружить такие элементы и использовать реакцию для подтверждения аутентичности документа. Основное внимание в добавлении B уделяется элементам, которые можно верифицировать с помощью детекторного оборудования, встроенного в считывающее устройство МСПД и используемое в ходе нормального процесса считывания.

Автоматизированная верификация элементов защиты документа предусматривает использование специальной технологии проверки, позволяющей проверить подлинность проездного документа. Для подтверждения аутентичности ее следует применять не изолированно, а в сочетании с методами визуальной проверки элементов защиты документа, что становится для проверяющего сотрудника эффективным новым средством верификации проездных документов.

Элементы защиты документа, предназначенные для автоматизированной верификации, являются факультативными элементами защиты, которые могут включаться в МСПД по усмотрению полномочного органа выдачи.

Размер элементов защиты, предназначенных для автоматизированной верификации, может варьироваться от менее 1 мм^2 (0,04 дюйма^2) до всей площади страницы документа. На рис. 1 показаны рекомендуемые места расположения этих элементов на странице данных МСПД в целях обеспечения интероперабельности. В интересах обратной совместимости рекомендуется вводить элементы, предназначенные для автоматизированной аутентификации, на указанных местах и зонах.

3.3 Автоматизированная аутентификация и электронные МСПД

Использование в электронном МСПД полностью отвечающей требованиям бесконтактной ИС открывает прекрасные возможности для автоматизированной аутентификации. Тем не менее, автоматизированная аутентификация с использованием бесконтактной ИС не срабатывает, если:

- бесконтактная ИС имеет дефект и не может установить связь или
- отсутствуют сертификаты для проверки подлинности и целостности данных на бесконтактной ИС.

Поэтому требуется альтернатива автоматизированной аутентификации. Это особенно важно для сценария автоматизированного пограничного контроля (АВС), когда для считывания и валидации электронного МСПД используется считывающее устройство, а не сотрудник службы пограничного контроля. В качестве надежного альтернативного средства повышения доверия к данным, используемым при принятии решений на границе, применяются системы оптической автоматизированной аутентификации.

Функционирующая бесконтактная ИС в электронном МСПД может также оказать содействие проведению оптической автоматизированной аутентификации посредством хранения информации об элементах, определяемых методом оптической автоматизированной аутентификации, и их координат в соответствующих группах данных (ГД).

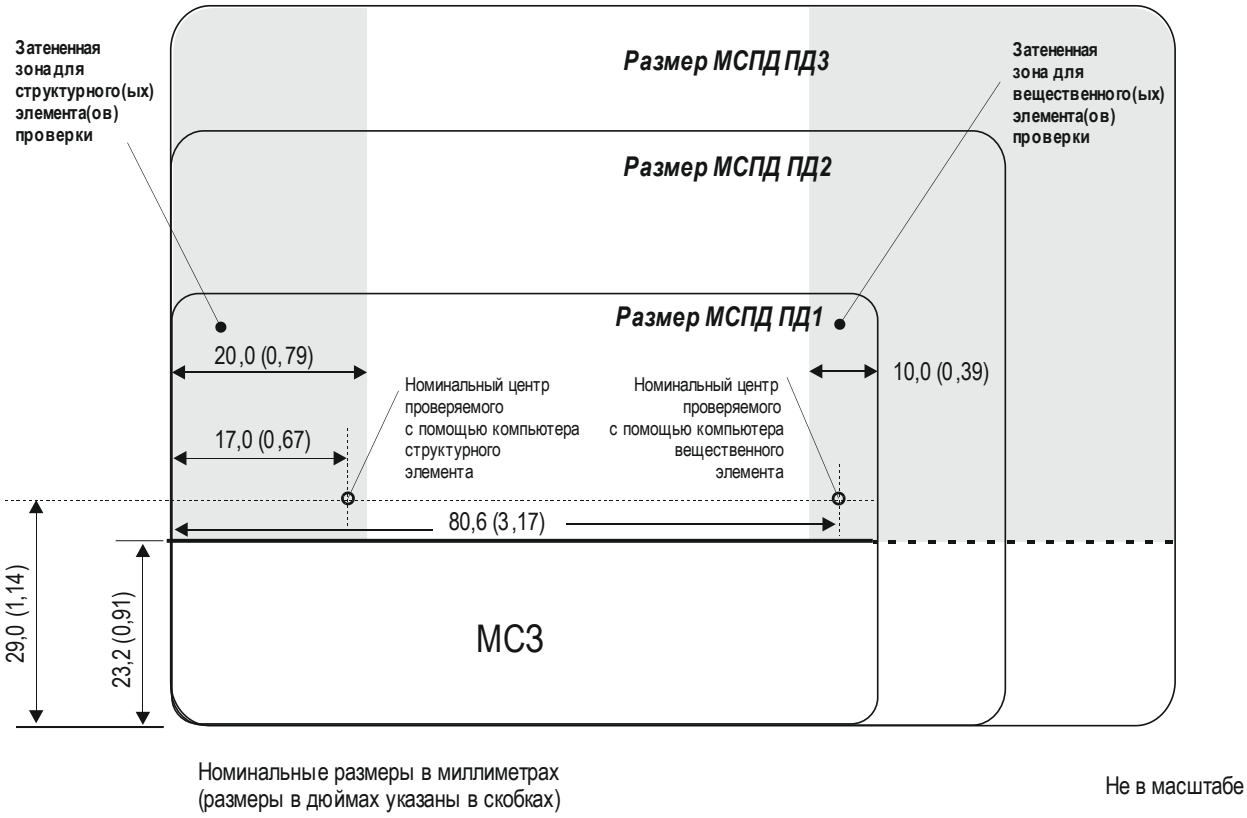

Рис. 1. Три размера МСПД, включая МСП (размер ПД3), с рекомендуемым расположением элементов проверки документа с помощью компьютера. Затененный участок слева рекомендуется для включения структурного элемента, а затененный участок справа – для включения вещественного элемента

4. ОХРАНА МЕСТ ИЗГОТОВЛЕНИЯ (РАЗРАБОТКА И ПРОИЗВОДСТВО) И ВЫДАЧИ МСПД

Государство, выдающее МСПД, обеспечивает соответствующую охрану помещений, в которых печатаются, переплетаются, персонализируются и выдаются МСПД, а также надлежащую проверку благонадежности персонала, занимающегося этой работой. Соответствующая охрана также обеспечивается при перевозке МСПД из одного объекта на другой и при доставке МСПД их владельцам. Рекомендации относительно способов выполнения этих требований содержатся в добавлении С.

При планировании объектов, предназначенных для производства и выдачи документов, необходимо учитывать следующие факторы:

1) способность к восстановлению;

2) физическую защиту и контроль доступа;

3) учет производственных материалов и МСПД;

4) транспортировку;

5) персонал;

6) кибербезопасность.

4.1 Способность к восстановлению

Государствам следует принимать надлежащие меры для обеспечения того, чтобы производство МСПД продолжалось в таких чрезвычайных ситуациях, как наводнение, пожар и отказ оборудования. Рекомендуются, в частности, следующие меры:

- рассредоточение средств производства и выдачи;
- дополнительные производственные объекты, если производство централизовано;
- объекты для выдачи в чрезвычайных ситуациях;
- оперативный доступ к запасным частям и средствам поддержки;
- наличие нескольких поставщиков всех компонентов МСПД.

Рекомендуется, чтобы государства учитывали возможные режимы отказа при проектировании объектов изготовления и выдачи, с тем чтобы исключить наиболее распространенные отказы и очевидные причины отказов.

4.2 Физическая защита и контроль доступа

Государствам следует контролировать доступ на объекты изготовления и выдачи документов. Контроль следует осуществлять по зонам, и требования к доступу в каждую зону должны быть соизмеримыми с ценностью охраняемого имущества.

В качестве примеров передовой практики на производственных объектах можно привести следующие:

- проволочное ограждение или сплошные стены вокруг производственных объектов;
- помещения сейфового типа для хранения изготовленных неперсонализированных МСПД и ключевых компонентов защиты для изготовления МСПД;
- пропускная система контр доступа между зонами;
- системы видеонаблюдения внутри объекта и за его пределами;
- охрана периметра;
- круглосуточное присутствие персонала служб безопасности.

Государствам следует также учитывать действующие меры защиты в организациях, поставляющих компоненты МСПД на объекты по их изготовлению, так как кража или продажа таких компонентов может упростить подделку МСПД.

В центрах по выдаче документов необходимо предусмотреть подсобные помещения, отделенные от помещений, открытых для публики, доступ в которые должен контролироваться. Сотрудникам необходимо предоставлять адекватные меры защиты с учетом местных обстоятельств.

4.3 Учет производственных материалов

Государствам следует обеспечивать учет всех материалов, используемых при изготовлении МСПД, и согласовывать данные о производстве и заказах МСПД, с тем чтобы можно было убедиться в отсутствии недостающих МСПД или их компонентов.

Бракованные материалы, МСПД и компоненты МСПД следует надежным образом уничтожать с надлежащим учетом.

Как правило, уменьшение числа объектов по выдаче и изготовлению документов облегчает учет материалов. Однако при этом следует учитывать необходимость обеспечения устойчивости системы и приемлемого уровня обслуживания клиентов.

4.4 Транспортировка

Государствам рекомендуется использовать защищенные средства транспортировки МСПД и компонентов МСПД; обычно адекватным является метод, применяемый для перевозки денежных средств, кроме случаев транспортировки особо ценного имущества (например, голографических матриц).

Государствам следует сводить к минимуму объем материалов, перевозимых в любой партии, с тем чтобы уменьшить последствия кражи. В частности, не следует перевозить полные наборы печатных форм одной партией.

4.5 Персонал

Государствам следует обеспечивать, чтобы весь персонал проходил проверку на благонадежность с подтверждением личных данных и получением допуска к работе с ценным имуществом. Сотрудникам следует выдавать документы, удостоверяющие их личность и дающие право доступа в охраняемые зоны, допуск в которые им требуется по служебной необходимости.

4.6 Кибербезопасность

Объекты, занимающиеся изготовлением и выдачей документов, уязвимы к разнообразным кибератакам, а именно:

1) вирусы и другие вредоносные программы – как на обычных вычислительных средствах, так и на производственном оборудовании;

2) сетевые атаки типа "отказ в обслуживании" через каналы запросов МСПД и сетевые службы, связанные с системами изготовления и выдачи документов;

3) несанкционированный доступ в системы, позволяющий злоумышленникам выпускать паспорта или получать личные данные или криптографическую информацию (например, закрытые ключи для изготовления электронных МСПД).

Вопрос о мерах противодействия выходит за рамки настоящего документа. Государствам следует консультироваться на эту тему с национальными техническими ведомствами.

5. ПРЕДОСТАВЛЕНИЕ ИНФОРМАЦИИ О НОВЫХ МСПД

Государству, приступающему к выпуску МСПД нового вида, рекомендуется информировать все другие государства об особенностях нового МСПД, в том числе об очевидных элементах защиты, желательно с предоставлением ведомству принимающего государства, отвечающему за проверку подлинности паспортов, персонализированных образцов для использования в качестве справочного материала. Такие образцы следует направлять в установленные контактные пункты, согласованные с принимающими государствами.

6. ПРЕДОСТАВЛЕНИЕ ИНФОРМАЦИИ ОБ УТЕРЯННЫХ И ПОХИЩЕННЫХ МСПД

Обмен информацией об утерянных, похищенных или аннулированных проездных документах является одним из элементов ключевой стратегии усиления пограничного контроля и смягчения последствий хищения персональных данных и мошеннических действий в иммиграционной сфере. Поэтому государствам следует рассматривать возможность реализации перечисленных ниже оперативных процедур по нейтрализации угроз в области организации пограничного контроля и обеспечения национальной безопасности:

1. инициативные каналы связи с владельцами документов;

2. организация национальных баз данных об утерянных, похищенных и аннулированных проездных документах;

3. обмен информацией об утерянных, похищенных и аннулированных проездных документах с ИНТЕРПОЛом и систематическая выверка документов с использованием баз данных ИНТЕРПОЛа в рамках первичного контроля;

4. введение мер контроля для выявления возможности представления потерянного, похищенного или аннулированного документа при пересечении границы.

6.1 Инициативные каналы связи с владельцами документов

Государствам следует обеспечивать, чтобы владельцы проездных документов были в полной мере информированы о своей ответственности в связи с использованием и хранением проездных документов, а также о процедурах информирования в случае их утери или хищения. Рекомендации по безопасному хранению проездных документах в домашних условиях и во время поездки могут способствовать предотвращению утери или хищения проездных документов. При выдаче документов их владельцев следует информировать о надлежащих действиях (включая своевременное уведомление) и каналах уведомления об утерянных или похищенных документах. Для оказания содействия в этом процессе государства могут информировать владельцев проездных документов о различных каналах конфиденциального уведомления об утерянных и похищенных документах, в том числе лично, по телефону, обычной почтой и различными средствами электронной связи, включая Интернет.

Государства также должны принимать надлежащие меры для обеспечения информирования владельцев проездных документов о возможных сбоях, неудобствах и дополнительных расходах в случае предъявления в ходе поездки на пунктах пограничного контроля утерянных, похищенных или аннулированных

документов. При этом необходимо подчеркивать, что в случае уведомления об утере/хищении проездного документа он аннулируется и не может более использоваться, но может быть конфискован властями при попытке его использования.

Необходимо иметь национальное законодательство или любой подходящий механизм, которые обязывали бы владельцев проездных документов незамедлительно уведомлять об утере или хищении проездного документа. До представления такого уведомления новые проездные документы выдавать не следует.

6.2 Организация национальных баз данных об утерянных, похищенных и аннулированных проездных документах

Государствам, использующим национальные базы данных о проездных документах для оказания помощи при верификации статуса выданных на национальном уровне проездных документов, следует принимать меры для обеспечения актуальности такой информации. Уведомления об утерянных и похищенных документах, полученные от их владельцев, необходимо своевременно регистрировать в таких системах для обеспечения точности оценки рисков с использованием этих систем. Государствам следует также рассмотреть возможность регистрации в этих базах данных информации о выявлении утерянных, похищенных или аннулированных проездных документов. Помимо обновления таких баз данных государствам следует обеспечивать беспрепятственный доступ к ним пограничных и полицейских ведомств.

6.3 Обмен информацией об утерянных, похищенных и аннулированных проездных документах с ИНТЕРПОЛом и систематическая выверка документов по базам данных ИНТЕРПОЛа в рамках первичного контроля

Государствам следует участвовать в глобальном обмене актуальной и точной информацией о статусе проездных документов в порядке поддержки действий национальных полицейских и пограничных органов, а также в усилиях по смягчению последствий хищения персональных данных. Обмен информацией об утерянных, похищенных и аннулированных проездных документах позволяет:

a) повысить действенность работы пограничной службы;

b) помочь в выявлении случаев хищения персональных данных или мошеннических действий в иммиграционной сфере при пограничном контроле или в других ситуациях, когда такой документ представляют для удостоверения личности;

c) повысить вероятность выявления террористов, путешествующих по фальшивым документам;

d) повысить вероятность выявления преступной деятельности, включая контрабанду людей;

e) помочь в возврате национальных документов;

f) уменьшить затраты, связанные с использованием утерянных, похищенных или аннулированных документов в противозаконных целях.

Автоматизированный поисковый центр (ASF)/база данных об утерянных и похищенных проездных документах (SLTD) ИНТЕРПОЛа дает государствам возможность эффективного, действенного и своевременного обмена информацией об утерянных, похищенных и аннулированных проездных документах. Государствам следует обмениваться информацией об утерянных и похищенных документах, которые выданы, а также о бланках документов, похищенных в центрах изготовления или выдачи или при перевозке. В добавлении D перечислены факторы, которые необходимо учитывать при принятии решения об участии в ASF/SLTD.

Государствам следует систематически проводить выверку документов по базам данных ИНТЕРПОЛа в качестве первичной меры контроля для обеспечения того, чтобы границы пересекали только владельцы действительных проездных документов. Проверка статуса проездных документов с использованием этих баз данных позволяет получить те же выгоды, которые дает обмен информацией об утерянных, похищенных и аннулированных документах.

6.4 Введение методов выявления случаев представления утерянного, похищенного или аннулированного документа при пересечении границы

Государствам необходимо соблюдать действующие национальные законы и международные соглашения об использовании проездных документов и пограничном контроле при проверке путешественников на своих пограничных пунктах. Все путешественники с заявленными проездными документами (утерянными, похищенными, аннулированными) рассматриваются как не имеющие преступных намерений, пока не будет доказано обратное.

6.4.1 В случае, когда проездной документ "засветился" в базе данных об утерянных, похищенных или аннулированных документах ИНТЕРПОЛа

Не следует запрещать въезд или препятствовать выезду путешественника только на том основании, что его документ указан в базе данных об утерянных, похищенных или аннулированных проездных документах. Прежде чем пойти на такие действия, государству необходимо предпринять множество шагов. Если путешественник имеет проездной документ, внесенный в базу данных ASF/SLTD в качестве утерянного, похищенного или аннулированного, государству следует, при наличии возможности, связаться со страной выдачи и уведомления, чтобы убедиться в том, что данный документ действительно зарегистрирован в качестве утерянного, похищенного или аннулированного проездного документа. Государствам следует также проводить собеседование с путешественниками, чтобы проверить их личность или гражданство и определить, являются ли они законными владельцами данных проездных документов.

Если документ содержит микросхему, государству следует провести биометрическую верификацию в рамках усилий по определению действительной личности путешественника. Государству следует также выяснить, вносились ли изменения в данные и является ли документ подлинным.

6.4.2 Оформление законного владельца проездного документа в пункте пограничного контроля

При работе с законными владельцами проездных документов государствам следует исходить из того, что лица, которые идентифицированы как законные обладатели проездного документа, заявленного в качестве утерянного, похищенного или аннулированного, не обязательно пытаются совершить уголовное преступление. Вместо того чтобы стремиться наказать таких лиц, государствам следует изыскать возможность изъятия этих документов из обращения, сведя при этом к минимуму возможные нарушения в поездке. В тех случаях, когда это допускается национальным законодательством, государства могут рассмотреть альтернативные методы оформления таких путешественников, отличные от тех, которые применяются в отношении лиц, намеренно пытающихся незаконно въехать в страну с помощью мошенничества с личными данными.

Путешественники, въезжающие в иностранное государство по документу, заявленному в качестве утерянного, похищенного или аннулированного в результате ошибки в данных	Органу пограничного контроля в принимающем государстве следует связаться с полномочным органом выдачи для подтверждения ошибки в данных. Получив такое подтверждение, государства могут рассматривать такой документ как действительный проездной документ, однако при этом следует рекомендовать путешественнику по возвращении в свою страну связаться с полномочным органом выдачи. Полномочным органам, выдающим проездные документы в государстве выдачи, следует принять все необходимые меры для изъятия такого документа из базы данных об утерянных, похищенных и аннулированных документах. Государствам следует также рассмотреть возможность замены такого документа без дополнительных расходов для владельца
Граждане, пытающиеся выехать из своей страны по документу, который заявлен в качестве утерянного или похищенного	В тех случаях, когда существует контроль выезда, пограничная служба должна сообщить таким путешественникам, что их документы не действительны для поездки и что они должны получить действительный проездной документ, прежде чем начинать путешествие, так как утерянные, похищенные и аннулированные проездные документы считаются недействительными
Граждане, пытающиеся выехать из своей страны по аннулированному документу	В тех случаях, когда существует контроль выезда, пограничная служба должна проконсультироваться с национальными правоохранительными органами для определения мер и законодательных положений, которые можно использовать для предотвращения выезда таких путешественников из страны. Если это допускается, пограничным/полицейским органам следует воспрепятствовать выезду путешественников из государства
Граждане, пытающиеся покинуть страну и вернуться в свою страну по документу, заявленному в качестве утерянного, похищенного или аннулированного	В тех случаях, когда существует контроль выезда и подтверждены личность и гражданство владельца, сотрудники пограничного контроля могут пропустить таких путешественников, но должны проинформировать их о том, что представленный документ является недействительным и что им может быть отказано перевозчиком в посадке на борт. В том случае, если путешественники возвращаются в свою страну по документу, заявленному в качестве утерянного, похищенного или аннулированного, сотрудники пограничной службы могут, если это разрешено национальным законодательством и/или международной договоренностью, изъять или конфисковать такой документ для возвращения его органу выдачи. Путешественникам, документы которых были изъяты или конфискованы, следует рекомендовать получить новые действительные проездные документы
Граждане, пытающиеся покинуть иностранное государство и проследовать в третью страну по документу, заявленному в качестве утерянного, похищенного или аннулированного	В тех случаях, когда существует контроль выезда, пограничная служба должна информировать путешественников о том, что их проездные документы недействительны, что им может быть отказано в посадке на борт перевозчиком и что у них могут возникнуть трудности по прибытии в следующий пункт назначения

Путешественники, въезжающие в иностранное государство по документу, заявленному в качестве утерянного, похищенного или аннулированного	Принимающее государство должно рекомендовать путешественникам, которым было разрешено подняться на борт, обратиться в свое консульство или посольство для получения действительного проездного документа, прежде чем они продолжат свое путешествие. Оформление путешественников, которым было отказано в разрешении на въезд, может производиться в соответствии с национальным законодательством

6.4.3 Оформление путешественников после определения того, что они не являются законными владельцами документа, заявленного в качестве утерянного, похищенного или аннулированного

Определив, что путешественник не является законным владельцем документа, пограничный/полицейский орган направляющего или принимающего государства должен попытаться выяснить, каким образом путешественник получил такой документ, включая возможный сговор с законным владельцем, а также, если это допускается национальным законодательством, действуя в сотрудничестве с государством выдачи, выяснить, были ли выданы дополнительные фиктивные документы на это имя. Если установлено, что путешественник представил утерянный, похищенный или аннулированный проездной документ, государству необходимо провести расследование в отношении такого путешественника и, если применимо, предъявить обвинение в совершении уголовного преступления и/или депортировать из страны.

Государству следует конфисковать документ для целей судебного разбирательства, в том числе по вопросам иммиграции и беженцев, но по завершении этих разбирательств возвратить документ в государство выдачи. Следует также, если это допускается национальным законодательством, предоставить выдавшему документ органу как можно больше информации об обстоятельствах изъятия документа.

Государствам также следует обеспечивать, чтобы лица без права на въезд оформлялись в соответствии с положениями Приложения 9 ИКАО *"Упрощение формальностей"* к Конвенции о международной гражданской авиации.

7. СПРАВОЧНЫЕ МАТЕРИАЛЫ (НОРМАТИВНЫЕ)

Некоторые положения международных стандартов, упоминаемые в настоящем тексте, представляют собой положения документа Doc 9303. Если между спецификациями, содержащимися в документе Doc 9303, и стандартами, на которые делаются ссылки, имеются различия, то для выполнения конкретных требований к изготовлению машиносчитываемых проездных документов, включая машиносчитываемые визы, приоритетную силу имеют спецификации, приводимые в этом документе.

Приложение 9 *"Упрощение формальностей"* к Конвенции о международной гражданской авиации (Чикагской конвенции).

Программа TRIP ИКАО, содержащая рекомендации относительно подтверждения подлинности личности [ICAO EOI]; соответствующая информация размещена на веб-сайте по адресу: https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx.

— — — — — — — —

ДОБАВЛЕНИЕ А К ЧАСТИ 2. СТАНДАРТЫ ЗАЩИТЫ МСПД (ИНФОРМАЦИОННОЕ)

А.1 СФЕРА ПРИМЕНЕНИЯ

В настоящем добавлении содержатся рекомендации об усилении защиты машиносчитываемых проездных документов, изготовленных в соответствии со спецификациями Doc 9303. Данные рекомендации охватывают вопросы защиты материалов, используемых при изготовлении документов, применяемые методы печатания с защитой от подделок и копирования и процессы, используемые при производстве бланков документов. Также рассматриваются аспекты безопасности, относящиеся к персонализации и защите биографических данных в документе. Настоящее добавление предназначено для всех полномочных органов, выдающих проездные документы.

А.2 ВВЕДЕНИЕ

В настоящем добавлении перечислены угрозы целостности проездных документов, которым часто подвергаются эти документы, и ответные меры, которые могут приниматься для защиты этих документов и связанных с ними систем персонализации. Перечисляемые элементы и/или методы защиты от этих угроз подразделяются на: 1) базовые элементы и/или методы защиты, считающиеся необходимыми, и 2) дополнительные элементы и/или методы, из которых государствам предлагается выбирать те, которые рекомендованы для обеспечения повышенного уровня защиты.

При таком подходе признается, что элемент или метод, который может быть необходимым для защиты документов одного государства, может оказаться излишним или маловажным для другого государства, использующего иные системы изготовления. Поэтому намеченный подход, позволяющий государствам делать выбор из разных систем документов (печатные документы, пластиковые карты и т. д.) и определять сочетание элементов и/или методов защиты, наиболее отвечающих их конкретным потребностям, является более предпочтительным, чем "универсальные" методы. Однако чтобы обеспечить выбор сбалансированного ряда элементов и/или методов защиты, каждое государство должно провести оценку своих национальных проездных документов с точки зрения риска для определения наиболее уязвимых аспектов и выбрать дополнительные элементы и/или методы, оптимально решающие эти конкретные проблемы.

Цель рекомендаций в настоящем добавлении заключается в улучшении защиты машиносчитываемых проездных документов во всем мире путем определения базового уровня для государств выдачи. Ничто в этих рекомендациях не препятствует и не мешает государствам внедрять другие, более совершенные элементы защиты по своему усмотрению в целях достижения более высокого стандарта защиты по сравнению с минимальными рекомендуемыми элементами и методами, изложенными в настоящем добавлении.

В материал добавления включена сводная таблица с перечнем типичных угроз, связанных с нарушением целостности проездных документов, а также некоторых элементов и методов защиты, которые могут способствовать обеспечению защиты от этих угроз.

A.3 ОСНОВНЫЕ ПРИНЦИПЫ

Производство и хранение паспортных книжек и проездных документов, включая процессы персонализации, должны осуществляться в безопасных и контролируемых условиях с принимаемыми на местах соответствующими мерами безопасности в целях защиты помещений от несанкционированного доступа. Если процесс персонализации является децентрализованным или персонализация осуществляется в месте, географически отделенном от места, где изготавливаются бланки проездных документов, следует принимать надлежащие меры предосторожности при перевозке бланков документов и любых связанных с защитой материалов в целях обеспечения их безопасности в процессе транспортировки и охраны по прибытии. При перевозке бланки паспортных книжек или других проездных документов должны содержать уникальный номер документа. У паспортов номер паспорта должен проставляться на всех страницах, помимо страницы биографических данных, на которой он может впечатываться в процессе персонализации.

Должна обеспечиваться полная отчетность по всем материалам защиты, использованным при изготовлении как качественных, так и бракованных проездных документов, а также полная выверка на каждом этапе процесса производства с ведением регистрации в целях учета всех использованных защищенных материалов. Необходимо вести контрольный журнал на достаточном уровне детализации для учета каждой единицы защищенного материала, используемого при производстве, который должен подвергаться независимой проверке лицами, непосредственно не участвующими в изготовлении документов. Следует сохранять записи учета всех уничтожаемых отходов материалов защиты и бракованных документов, заверенные руководителем в целях обеспечения подотчетности.

Используемые в производстве проездных документов материалы должны быть контролируемых видов, где это применимо, и приобретаться только у добросовестных поставщиков материалов, используемых для защиты. Следует использовать материалы с ограниченной сферой применения, обеспечивающие высокую степень защиты, и избегать материалов, общедоступных на открытом рынке.

Для создания защитного фона следует избегать исключительной зависимости от использования общедоступных пакетов программного обеспечения, предназначенных для графического дизайна. Однако такие пакеты программного обеспечения могут использоваться совместно со специальной программой защиты дизайна.

В проездные документы должны включаться элементы и/или методы защиты в целях предохранения от незаконного изготовления, несанкционированного изменения и других форм подделок, включая изъятие и замену страниц в паспортной книжке, особенно страницы, содержащей биографические данные. В дополнение к элементам, включаемым для защиты чистых бланков документа от подлогов и подделок, особое внимание следует уделять защите биографических данных от изъятия или изменения. Проездной документ должен содержать достаточное количество элементов и/или методов защиты, позволяющих обнаружить любую попытку фальсификации.

Требуется обоснованный подбор элементов, материалов и методов защиты в целях обеспечения полной совместимости и защиты документов в течение срока их действия.

Настоящее добавление в основном касается элементов, которые помогают обеспечить защиту проездных документов от подлога и мошеннической замены, однако имеется другая категория элементов защиты (элементы уровня 3), которые охватывают скрытые (секретные) элементы, предназначенные для аутентификации путем проведения судебной экспертизы, или с помощью специального оборудования для верификации. Очевидно, что располагать информацией о конкретных материалах и структуре таких элементов должно весьма ограниченное число людей, которым это положено по служебной необходимости. Цель таких элементов, в частности, заключается в подтверждении аутентичности документов, когда требуются неоспоримые доказательства аутентичности (например, в суде). Каждый проездной документ должен содержать по крайней мере один скрытый элемент защиты в качестве основного.

Важные общие стандарты и рекомендуемая практика в отношении периода действительности паспортного документа, принципа "один паспорт на одно лицо", конечных сроков выдачи машиносчитываемых паспортов и изъятия из обращения паспортов, не являющихся машиносчитываемыми, и другие инструктивные материалы содержатся в Приложении 9 ИКАО *"Упрощение формальностей".*

Отсутствуют какие-либо другие приемлемые средства хранения данных в целях глобальной интероперабельности, кроме бесконтактной ИС, которая определена ИКАО в качестве технологии, обеспечивающей расширение возможностей использования в МСПД.

A.4 ОСНОВНЫЕ УГРОЗЫ ЦЕЛОСТНОСТИ ПРОЕЗДНЫХ ДОКУМЕНТОВ

Нижеуказанные угрозы целостности документов, перечисленные не в порядке их значимости, представляют собой способы мошенничества в отношении документа, его выдачи и применения:

- подделка всего проездного документа;
- замена фотографии;
- изъятие/изменение данных в зоне визуальной проверки или машиносчитываемой зоне на странице данных МСП;
- создание фальсифицированного документа или его частей с использованием материалов, взятых из законных документов;
- изъятие и замена целой страницы (страниц) или виз;
- изъятие записей на страницах для виз и странице для заметок;
- кража подлинных бланков документов;
- выдача себя за другое лицо (вымышленная личность, измененный внешний вид);
- манипулирование бесконтактной ИС (если имеется) физическим или электронным способом.

Обнаружить элементы защиты можно с помощью проверки на любом из следующих трех уровней:

- Уровень 1. Поверхностное изучение для быстрой проверки в пункте использования (легко идентифицируемые визуальные или тактильные характеристики).
- Уровень 2. Осмотр подготовленными инспекторами с использованием простого оборудования.
- Уровень 3. Проверка экспертами-криминалистами.

Для поддержания защиты и целостности документа следует на периодической основе проводить его рассмотрение, включая любые результирующие изменения его структуры. Это позволит использовать новые элементы защиты документа и подтверждать способность противостоять попыткам нарушения его целостности и совершения мошеннических действий, включая:

- замену фотографии;
- отслаивание ламината или другие виды нарушения структуры;

- создание аналогов бесконтактной ИС и других компонентов;
- модификацию любого элемента данных;
- стирание или изменение другой информации;
- копирование, воспроизведение или создание факсимильной копии;
- эффективность элементов защиты на всех трех уровнях: поверхностное изучение, осмотр подготовленными инспекторами с использованием простого оборудования и проверка экспертами-криминалистами;
- доверие и простоту аутентификации на втором уровне.

В целях обеспечения защиты от этих и других угроз проездной документ должен содержать ряд элементов и методов защиты, интегрированных оптимальным образом внутри документа. Хотя некоторые элементы могут обеспечивать защиту от нескольких видов угроз, ни один из элементов не может обеспечить защиту от всех этих видов. Точно так же, ни один элемент защиты не обладает 100-процентной эффективностью в устранении какой-либо одной категории угрозы. Наилучшая защита обеспечивается на основе сбалансированного набора элементов и методов, которые сочетают различные комплексные формы защиты документа, объединенные в целях сдерживания или выявления актов мошенничества.

A.5 ЭЛЕМЕНТЫ И МЕТОДЫ ЗАЩИТЫ

В нижеследующих разделах элементы и методы защиты и другие меры защиты описываются в соответствии с этапами, реализуемыми в ходе изготовления и процесса персонализации и создания компонентов проездного документа в отношении:

1) материалов основы;
2) защиты структуры и печатания;
3) защиты от копирования, подделки или мошеннического изменения;
4) методов персонализации.

Государствам выдачи рекомендуется включать все основные элементы/меры и выбирать ряд дополнительных элементов/мер из приведенного перечня, предварительно проведя полную оценку риска, связанного с их проездными документами. Если не указано иное, то можно считать, что элементы защиты применяются ко всем частям проездного документа, включая обложку и переплет книжки, и ко всем внутренним страницам паспорта, состоящим из страницы биографических данных, форзацев и визовых страниц. Необходимо следить за тем, чтобы элементы защиты не препятствовали машинному считыванию проездного документа.

A.5.1 Материалы основы

A.5.1.1 Бумага, используемая для страниц проездного документа

Основные элементы:

- ультрафиолетовая матовая бумага или основа с контролируемой реакцией на ультрафиолетовое излучение таким образом, что при облучении ультрафиолетовым светом испускает флуоресценцию, отличную по цвету от бело-голубого света, используемого в широкодоступных материалах, содержащих оптические отбеливатели;
- водяной знак, включающий два или более оттенков серого цвета на странице биографических данных и на страницах визы;
- соответствующие химические сенсибилизаторы в бумаге, по крайней мере на странице биографических данных (если это совместимо с методом персонализации);
- легкоразрываемая бумага с надлежащей поглощающей способность и шероховатостью.

Дополнительные элементы:

- регистрационный водяной знак с напечатанным рисунком;
- водяной знак на странице данных, отличающийся от водяного знака на визовых страницах, для предотвращения замены страниц;
- водяной знак, изготавливаемый в цилиндрической форме;
- невидимые флуоресцентные волокна;
- видимые (флуоресцентные) волокна;
- защитные нити (скрытые или открытые), содержащие дополнительные элементы защиты, такие как микроизображения и флуоресценция;
- маркер, предназначенный для обнаружения с помощью специального оборудования;
- элемент защиты, изготовленный методом лазерной перфорации.

A.5.1.2 Бумага или другая основа в виде наклейки, используемой в качестве страницы проездного документа, содержащей биографические данные

Основные элементы:

- ультрафиолетовая матовая бумага или основа с контролируемой реакцией на ультрафиолетовое излучение, в результате которой при облучении ультрафиолетовыми лучами бумага испускает флуоресценцию, отличную по цвету от бело-голубого света, используемого в широкодоступных материалах, содержащих оптические отбеливатели;
- соответствующие химические сенсибилизаторы в бумаге (как правило, не могут применяться в пластиковой подложке наклейки);

- невидимые флуоресцентные волокна;
- видимые (флуоресцентные) волокна;
- система связывающих и/или других характеристик, препятствующих снятию наклейки без четко видимых ее повреждений и любых ламинатов или накладок, используемых вместе с этой наклейкой.

Дополнительные элементы:

- защитные нити (скрытые или открытые), содержащие дополнительные элементы защиты, такие как микроизображения и флуоресценция;
- можно использовать водяной знак в бумаге страницы данных в виде бумажной наклейки;
- элемент защиты, изготовленный методом лазерной перфорации;
- штампованный рисунок на наклейке, позволяющий обнаружить попытки фальсификации.

A.5.1.3 Аспекты защиты бумаги, используемой для внутренней стороны обложки паспортной книжки

Нет необходимости использовать водяной знак на бумаге, применяемой для внутренней стороны обложки паспортной книжки. Хотя это определенно не рекомендуется, если внутренняя сторона обложки используется как страница биографических данных (см. A.5.5.1), то могут применяться альтернативные меры для обеспечения эквивалентного уровня защиты от всех попыток, связанных с помещением страницы данных на внутренней обложке.

Бумага, из которой изготавливается внутренняя сторона обложки, должна содержать соответствующие химические сенсибилизаторы, если внутренняя сторона обложки используется в качестве страницы биографических данных. Бумага с химическими сенсибилизаторами должна быть совместимой с методом персонализации и связывающим веществом, используемым для наклеивания форзаца на обложку паспорта.

A.5.1.4 Синтетические основы

Если основа, используемая для страницы биографических данных (или наносимой наклейки) паспортной книжки или карты МСПД, полностью состоит из пластика или его разновидности, то многие элементы защиты, описанные в пп. A. 5.1.1–A.5.1.3, включать обычно невозможно. В таких случаях должны предусматриваться дополнительные элементы защиты, включая дополнительные впечатываемые элементы защиты, улучшенные методы персонализации и использование элементов с оптически изменяющимися свойствами в дополнение к рекомендациям, изложенным в пп. A. 5.2–A.5.5.2. Государствам следует обеспечивать, чтобы пластиковые основы изготавливались в контролируемых условиях и содержали такие характеристики, как регулируемый уровень флуоресценции, позволяющие отличить их от основы стандартных финансовых карточек.

Основные элементы:

- структура страницы данных должна обеспечивать сопротивляемость физическому расслоению;
- ультрафиолетовая матовая основа с контролируемой реакцией на ультрафиолетовое излучение, в результате которого при облучении ультрафиолетовыми лучами бумага испускает

флуоресценцию, отличную по цвету от бело-голубого света, используемого в широкодоступных материалах, содержащих оптические отбеливатели;

- необходимо принимать надлежащие меры для надежного и долговременного помещения страницы данных в машиносчитываемый проездной документ;
- оптически изменяющийся элемент.

Дополнительные элементы:

- скрытый или открытый элемент;
- осязаемый элемент;
- элемент защиты, изготовленный методом лазерной перфорации.

A.5.2 Защитная печать

A.5.2.1 Фон и печатание текста

Основные элементы (см. раздел 4.2 "Термины и определения" *в части 1 документа Doc 9303):*

- двухцветный гильошированный узор защитного фона[1];
- радужная печать;
- микропечатный текст;
- защитный фон страницы биографических данных, напечатанный рисунком, который отличается от рисунка страниц визы или других страниц документа.

Дополнительные элементы:

- одноцветная или многоцветная глубокая печать, состоящая из рисунка "черная линия – белая линия" на одной или нескольких последних листах или визовых страницах;
- скрытое (глубокое) изображение;
- несканируемый узор;
- двухслойный защитный узор;
- элемент рельефного (трехмерного) рисунка;

1. Если гильошированный узор создан на компьютере, то воспроизводимое на документе изображение должно быть таковым, чтобы нельзя было обнаружить наличие структуры элементов изображения. Узоры могут изображаться в качестве позитивных изображений, когда линии изображения выступают с белыми пробелами между ними, либо в качестве негативных изображений, когда линии изображений выступают белым цветом с напечатанными между ними пробелами. Двухцветное гильоширование является рисунком, включающим гильошированные узоры, которые создаются путем наложения двух элементов гильоширования, воспроизводимых контрастными цветами.

- приводка "с лицевой до оборотной стороны" (сквозная приводка);
- намеренная ошибка (например, орфографическая);
- каждая страница для виз напечатана с различным рисунком защитного фона;
- осязаемый элемент защиты;
- уникальный(ые) шрифт(ы).

A.5.2.2 Чернила

Основные элементы:

- ультрафиолетовые флуоресцентные чернила (видимые или невидимые) на странице биографических данных и на всех визовых страницах;
- реактивные чернила, когда основой страниц документа или наклейки является бумага, по крайней мере для страницы биографических данных (если это совместимо с методом персонализации).

Дополнительные элементы:

- чернила с оптически изменяющимися свойствами;
- металлические чернила;
- проникающие номерные чернила;
- метамерные чернила;
- инфракрасные пропадающие чернила;
- инфракрасные абсорбирующие чернила;
- фосфоресцирующие чернила;
- маркированные чернила;
- невидимые чернила, которые испускают флуоресценцию различных цветов под воздействием волн разной длины.

A.5.2.3 Нумерация

Настоятельно рекомендуется присваивать уникальный номер в качестве номера паспорта.

Основные элементы:

- номер паспорта должен иметься на всех страницах документа и на странице биографических данных документа;
- номер документа печатается и/или перфорируется;

- номер документа на наклейке наносится специальными цифрами или шрифтом и печатается чернилами, которые флуоресцируют в ультрафиолетовых лучах в дополнение к изображению видимым цветом;

- номер на странице данных паспорта, изготовленной на синтетической основе, или на карте МСПД можно наносить с использованием такого же метода, что и при нанесении биографических данных в процессе персонализации;

- на картах МСПД номер должен иметься на обеих сторонах карты.

Дополнительные элементы:

- если номер перфорируется, предпочтительным является метод лазерной перфорации. Перфорация номера на странице данных является не обязательной, однако, если она используется, необходимо следить за тем, чтобы она не нарушала четкости изображения или визуальной зоны и никоим образом не препятствовала машинному считыванию. Желательно перфорировать обложку паспорта;

- если номер печатается, то в идеальном варианте следует использовать специальные цифры или шрифт и чернила, которые флуоресцируют в ультрафиолетовых лучах в дополнение к изображению видимом цветом.

A.5.2.4 Специальные меры защиты при использовании неламинированных страниц биографических данных

Поверхность страницы данных должна быть защищена от загрязнения при нормальном использовании, включая регулярное считывание МСЗ, и от попыток фальсификации.

Если страница документа используется для биографических данных, которые не защищены ламинатом или накладкой в качестве защитного покрытия (см. пп. A.5.3.2, A.5.4.3 и A.5.4.4), предусматривается дополнительная защита путем использования глубокой печати, включающей скрытое изображение и микропечатание, предпочтительно с использованием меняющих цвет чернил (например, чернил с оптически изменяющимися свойствами).

A.5.2.5 Специальные меры защиты при использовании пластиковых карт и страниц биографических данных из пластика

Если проездной документ полностью изготовлен из пластика, то используются элементы защиты с оптически изменяющимися свойствами, которые при изменении угла зрения дают другое изображение. Такие элементы могут иметь форму скрытого изображения, двояковыпуклого изображения, изменяющих цвет чернил или дифракционных элементов изображения с оптически изменяющимися свойствами.

A.5.3 Защита от копирования

A.5.3.1 Необходимость защиты от копирования

Современный уровень разработок общедоступных методов цифрового воспроизведения и вытекающие из этого возможности подделки означают, что необходимы высококачественные элементы защиты

в виде элементов с оптически изменяющимися свойствами или другие эквивалентные методы для противодействия копированию и сканированию. Необходимо сделать упор на защиту страницы биографических данных паспортной книжки, проездной карты или визы, основываясь на независимой сложной технологии, использующей оптически изменяющиеся свойства, или на других эквивалентных средствах, дополняющих иные методы защиты. Особое внимание следует уделять легко идентифицируемым визуальным или тактильным элементам, которые выявляются в ходе проверки уровня 1.

Надлежащее включение элементов с изменяющимися характеристиками или других эквивалентных устройств в структуру страницы биографических данных должно также обеспечивать защиту данных от мошеннического изменения. Компоненты с оптически изменяющимися свойствами и все соответствующие материалы защиты, используемые для создания многослойной структуры, также должны быть защищены от подлога.

A.5.3.2 Методы защиты от копирования

С учетом минимальных рекомендаций, изложенных в пп. A.5.4.3 и A.5.4.4 в отношении необходимости ламинирования, элементы защиты с оптически изменяющимися свойствами следует использовать на странице биографических данных паспортной книжки, проездной карты или визы в качестве *основного элемента*.

Если страница биографических данных паспортной книжки, проездной карты или визы защищена ламинатом или накладкой, в такую страницу следует вносить элементы с оптически изменяющимися свойствами (предпочтительно на основе дифракционной структуры и с характеристиками предотвращения фальсификации). Такие элементы не должны влиять на разборчивость внесенных данных.

Если страницей биографических данных является заключенная в оболочку бумажная наклейка или страница в паспорте, то биографические данные должны быть надлежащим образом защищены с помощью ламината или других мер, обеспечивающих эквивалентную защиту от изменения и/или удаления данных.

Если машиносчитываемая страница биографических данных паспортной книжки сделана полностью из синтетической основы, то следует вносить элемент с оптически изменяющимися свойствами. Рекомендуется включать дифракционный элемент с оптически изменяющимися свойствами для достижения повышенного уровня защиты от копирования.

Вместо элементов с оптически изменяющимися свойствами могут использоваться другие средства, предоставляющие эквивалентный уровень защиты, например открытые или закрытые элементы, лазерная перфорация и т. д.

Если проездной документ не защищен накладкой или ламинатом, то используются элементы с оптически изменяющимися свойствами (предпочтительно на основе дифракционной структуры) с применением надпечатки глубокой печатью или других типографских методов.

A.5.4 Методы персонализации

A.5.4.1 Персонализация документа

Речь идет о процессе, с помощью которого фотография, подпись или другие биографические данные, относящиеся к владельцу документа, заносятся в проездной документ. Эти данные содержат подробную информацию о личности владельца и представляют исключительно высокий риск с точки зрения

возможности подделки или мошеннического изменения. Одним из наиболее распространенных видов подделки документов является изъятие фотографии из украденного или незаконно приобретенного проездного документа и ее замена фотографией другого лица. Документы с вклеенной фотографией личности владельца особенно подвержены замене фотографии. Поэтому в МСПД вклеенные фотографии использовать НЕ разрешается.

A.5.4.2 Защита от изменения

В целях обеспечения надлежащей защиты данных от попыток подделки или мошеннического изменения настоятельно рекомендуется вносить биографические данные, включая фотографию, подпись (если она предусмотрена на странице биографических данных) и основную информацию о выдаче, в базовый материал документа. Для персонализации документа таким образом существует целый ряд технических приемов, включая следующие (приводятся не в порядке их значения, при этом не исключается возможность появления новых технологий):

- лазерная порошковая печать;
- термическая декалькомания;
- струйная печать;
- фотографические процессы;
- лазерная гравировка.

Те же методы персонализации документа могут также использоваться для внесения данных на страницу для отметок. Метод лазерной порошковой печати не следует использовать для персонализации виз или других документов, не защищенных ламинатным покрытием.

Полномочным органам следует проводить испытания процессов и методов персонализации с целью воспрепятствовать возможным злоупотреблениям.

A.5.4.3 Выбор системы документа

Выбор конкретного метода относится к компетенции отдельных государств выдачи и будет зависеть от ряда факторов, а именно: количества изготавливаемых проездных документов, структуры документа, будет ли документ заполняться личными данными в процессе изготовления документа или паспорта или после того, как подготовлен чистый бланк этого документа или паспорта, а также принята ли в стране централизованная или децентрализованная система выдачи паспортов.

Независимо от того, какой метод выбран, следует принимать меры предосторожности в целях защиты личной информации от попыток фальсификации данных. Это важно, поскольку, хотя отказ от практики вклеивания фотографии уменьшает риск ее замены, незащищенные биографические данные по-прежнему могут быть подделаны и требуют защиты либо путем наложения термоусаживаемого (или эквивалентного) ламината, обладающего характеристиками ломкости, либо с использованием эквивалентной технологии, позволяющей обнаружить попытки нарушения целостности.

A.5.4.4 Защита от замены фотографии и изменения данных на странице биографических данных паспортной книжки, проездной карты или визы

Основные элементы:

- персонализация фотографии и всех биографических данных путем включения их в основной материал;
- наложение фонового элемента (например, гильошировки) на зону фотографии;
- использование реактивных чернил и химических сенсибилизаторов в бумаге;
- видимый защитный элемент должен накладываться на фотографию, не ухудшая ее видимости; рекомендуется использование элемента с оптически изменяющимися свойствами;
- термоусаживаемый (или эквивалентный) ламинат или сочетание технологии персонализации и материала основы, обеспечивающие эквивалентную защиту от замены и/или подделки фотографии и других биографических данных.

Дополнительные элементы:

- изображение подписи владельца может сканироваться и налагаться на печатный текст;
- включение в документ стенографического изображения;
- вторичное изображение фотографии владельца;
- элементы информации в машиносчитываемой форме, описываемые в частях 9–12 документа Doc 9303.

A.5.5 Дополнительные меры защиты паспортных книжек

A.5.5.1 Местоположение страницы биографических данных

Государствам рекомендуется помещать страницу данных на одну из внутренних страниц (вторая или предпоследняя страница). Если страница данных располагается на внутренней стороне обложке МСП, следует иметь в виду, что обычный метод конструирования, используемый при изготовлении паспортных обложек, облегчает совершение мошенничества с использованием страницы данных (обычно замена фотографии или всей страницы). Однако государство выдачи может помещать страницу данных паспорта на обложку при условии, что метод изготовления обложки, используемой в его паспорте, обеспечивает уровень защиты от всех видов мошенничества, аналогичный тому, который достигается при помещении страницы данных на внутреннюю страницу. Тем не менее, помещать страницу биографических данных на обложку категорически НЕ рекомендуется.

A.5.5.2 Замена всей страницы

Внимание государств выдачи обращается на тот факт, что после того, как наклеиваемые фотографии в паспортах были заменены страницами с интегрированными биографическими данными, имели место случаи подмены всей страницы, при этом вся страница паспорта, содержащая биографические данные, изымалась и заменялась поддельной страницей. Хотя совершить подмену всей страницы в целом сложнее,

чем подмену наклеенной фотографии, тем не менее, для противодействия этой категории риска важно принять нижеуказанные рекомендации. Как и в отношении всех других видов мошенничества с документами, для предотвращения замены всей страницы лучше применять определенные сочетания элементов защиты, чем полагаться на какой-то один элемент, который в случае его раскрытия может подорвать целостность всего проездного документа.

Основные элементы:

- применяемые методы переплета страниц книжки должны препятствовать попыткам изъятия страниц без видимых следов распаривания;
- защитный фон страницы биографических данных, рисунок которого отличается от рисунка страниц для виз;
- нумерация страниц интегрирована в защитный узор на визовых страницах;
- серийный номер на каждом листе, желательно перфорированный.

Дополнительные элементы:

- многоцветная и/или флуоресцентная, например ультрафиолетовая швейная нить;
- программируемое изображение, прошитое нитью;
- переплет с использованием УФ-клея;
- подборочные или указательные отметки, напечатанные на кромке каждой визовой страницы;
- перфорированные лазером защитные элементы на странице биографических данных;
- биографические данные печатаются на внутренней странице в дополнение к странице данных.

Если используются самоклеющиеся этикетки, то рекомендуется учитывать дополнительные требования к защите, описанные в пп. A.5.1.2 и A.5.2.4, включая интеграцию такой этикетки с машиносчитываемым проездным документом через номер паспорта.

A.5.6 Контроль качества

Проверки и контроль качества на всех этапах производственного процесса и от одной партии продукции к другой необходимы для поддержания единообразия выпускаемых проездных документов. Сюда следует включать проверки обеспечения качества (ОК) всех материалов, используемых при изготовлении документов, и четкости машиносчитываемых строк. Единообразие выпускаемых проездных документов имеет огромное значение, поскольку инспекторы иммиграционных служб и сотрудники органов пограничного контроля рассчитывают на возможность распознавания фальшивых документов по изменениям внешнего вида или характеристик документа. Изменения качества, внешнего вида или характеристик подлинного проездного документа государства усложняют обнаружение поддельных или подложных документов.

A.5.7 Контроль безопасности производства и продукции

Серьезную угрозу целостности МСП государства выдачи представляет несанкционированный вынос из производственных помещений подлинных готовых, но не персонализированных МСП или компонентов, из которых могут быть изготовлены МСП.

A.5.7.1 Защита от кражи и злоумышленного использования бланков подлинных документов или компонентов документов

Бланки документов должны храниться в запертых и надлежащим образом контролируемых помещениях. Необходимо принимать следующие меры безопасности:

Основные меры:

- адекватная физическая охрана помещений с контролем доступа к зонам доставки, отправления и производства и средствам хранения документов;
- ведение подробного журнала регистрации учета и выверки всех материалов (использованных, неиспользованных, бракованных или испорченных) с заверенными соответствующими записями;
- серийная нумерация всех бланков документов и других компонентов, требующих особых мер защиты, с подробной регистрацией данных о каждом документе с момента изготовления до момента отправления, если применимо;
- по мере необходимости, регистрация номеров отслеживания и контрольных номеров других основных компонентов документов (например, рулонов или листов ламината, средств с оптически изменяющимися характеристиками);
- защищенные средства для перевозки бланков документов и других основных компонентов документов (если применимо);
- оперативный обмен данными между правительствами и пограничными органами о всех случаях утери и хищения бланков проездных документов и направление такой информации в базу данных ИНТЕРПОЛа об утерянных и похищенных документах;
- введение надлежащих мер контроля в целях защиты производственных процессов от внутренних мошеннических актов;
- проверка благонадежности персонала.

Дополнительные меры:

- установка замкнутых систем видеонаблюдения/видеозаписи (CCTV) во всех производственных помещениях, если это разрешено;
- централизованная система хранения и персонализации бланков документов с минимальным количеством центров.

Таблица А-1. Краткое изложение рекомендаций по обеспечению защиты

Компоненты	*Базовые элементы*	*Дополнительные элементы*
Материалы основы (А.5.1)		
Бумажные основы (А.5.1.1)	– контролируемая УФ-реакция; – двухтоновый водяной знак; – химические сенсибилизаторы; – надлежащие характеристики абсорбции и поверхности	– зарегистрированный водяной знак; – разные водяные знаки на странице данных и визовых страницах; – цилиндрические формы для водяных знаков; – невидимые флуоресцентные волокна; – видимые (флуоресцентные) волокна; – защитная нить; – маркеры; – элементы защиты, выполненные с помощью лазерной перфорации
Бумажные или другие основы в форме этикетки (А.5.1.2)	– контролируемая УФ-реакция; – химические сенсибилизаторы; – невидимые флуоресцентные волокна; – видимые (флуоресцентные) волокна; – система клеящих материалов	– защитная нить; – водяной знак; – элементы защиты методом лазерной перфорации; – защитный рисунок методом штамповки
Синтетические основы (А.5.1.4)	– сопротивляемость расслоению структуры; – оптически матовый материал; – средства защиты страницы данных; – элементы с оптически изменяющимися характеристиками; – см. пп. А5.2–А5.5, по мере необходимости	– оконные или транспарентные элементы; – тактильные элементы; – элементы лазерной перфорации
Печатание с обеспечением защиты (А.5.2)		
Фон и печатание текста (А.5.2.1)	– двухцветная гильошированная основа; – радужная печать; – микропечатание; – уникальный рисунок страницы данных	– глубокая печать; – скрытое изображение; – элементы противодействия сканированию; – двухслойный защитный рисунок; – рельефный рисунок; – приводка "с лицевой до оборотной стороны"; – преднамеренная ошибка; – индивидуальный рисунок на каждой странице; – тактильный элемент; – уникальные шрифты

Компоненты	*Базовые элементы*	*Дополнительные элементы*
Чернила (A.5.2.2)	– ультрафиолетовые флуоресцентные чернила; – реактивные чернила	– чернила с оптически изменяющимися свойствами; – металлические чернила; – проникающие чернила для нумерации; – метамерические чернила; – инфракрасные пропадающие чернила; – инфракрасные абсорбируемые чернила; – фосфоресцирующие чернила; – маркированные чернила; – невидимые чернила
Нумерация (A.5.2.3)	– нумерация на всех листах; – напечатанный и/или перфорированный номер; – нумерация специальным шрифтом для этикеток; – идентичные методы нумерации и внесения биографических данных на синтетических основах и картах	– нумерация документа методом лазерной перфорации; – специальные гарнитуры
Методы персонализации (A.5.4)		
Защита от замены и изменения фотографии (A.5.4.4)	– интеграция биографических данных; – защитный фон, перекрывающий зону фотографии; – реактивные чернила и химические сенсибилизаторы в бумаге; – видимые средства защиты, перекрывающие зону фотографии; – термоусаживаемый защитный ламинат или эквивалентный элемент	– отображение подписи; – стеганографическое изображение; – дополнительное(ые) изображение(я) фотографии; – биометрические элементы согласно части 9
Дополнительные элементы защиты для паспортных книжек (A.5.5)		
Замена страницы (A.5.5.2)	– технология защищенного прошивания; – ультрафиолетовая флуоресцентная нить для прошивания; – уникальный рисунок страницы данных; – интеграция номеров страниц в защитный рисунок; – серийный номер на каждом листе	– многоцветная нить для прошивания; – запрограммированный швейный муар; – использование ультрафиолетового клея для переплета; – индексные отметки на каждой странице; – элементы защиты, выполненные методом лазерной перфорации; – биографические данные на внутренней странице

Компоненты	*Базовые элементы*	*Дополнительные элементы*
Контроль и защита средств производства и продукции (A.5.7)		
Защита от кражи и ненадлежащего использования (A.5.7.1)	– адекватные меры физической защиты; – детальная регистрация; – серийные номера на бланках документов, если необходимо; – номера отслеживания и контрольные номера компонентов, если необходимо; – защита при перевозке бланков документов; – международный обмен информацией об утерянных и похищенных документах; – процедуры защиты от внутренних мошеннических действий; – проверки благонадежности персонала	– системы CCTV в производственных помещениях; – централизованная система хранения и персонализации

Примечание 1. Перечень дополнительных элементов не является исчерпывающим, и государствам и организациям выдачи рекомендуется вводить другие элементы защиты, конкретно не упомянутые в настоящем добавлении.

Примечание 2. Описания в таблице в силу необходимости являются сокращенной формой основного текста. Для упрощения поиска в колонке "Компоненты" вышеприведенной таблице указаны номера соответствующих разделов настоящего добавления.

Примечание 3. Некоторые элементы повторяются в таблице по нескольку раз. Это означает, что данный конкретный элемент обеспечивает защиту от нескольких видов угроз. Включать такой элемент в какой-либо конкретный документ необходимо лишь один раз.

Примечание 4. Существует множество других факторов, связанных с защитой паспортов, помимо упомянутых здесь. Дополнительные рекомендации содержатся в добавлениях B и C. Поэтому добавления A, B и C следует рассматривать в совокупности в интересах целостности процесса выдачи документов.

Примечание 5. Любые прямые или косвенные ссылки на конкретные термины и/или технологии предназначены исключительно для описания таких терминов и технологий в их оригинальной форме и не имеют какой-либо связи с конкретными распространителями или поставщиками таких технологий.

— — — — — — — —

ДОБАВЛЕНИЕ В К ЧАСТИ 2. АВТОМАТИЗИРОВАННАЯ ВЕРИФИКАЦИЯ ЭЛЕМЕНТОВ ЗАЩИТЫ ДОКУМЕНТА (ИНФОРМАЦИОННОЕ)

B.1 СФЕРА ПРИМЕНЕНИЯ

В настоящем добавлении содержатся рекомендации в отношении автоматизированной аутентификации элементов защиты в самом документе (материалов, защитной печати и методов защиты от копирования), а также рекомендации о технологиях считывания, обеспечивающие возможности автоматизированной аутентификации документов.

B.2 СЧИТЫВАЮЩИЕ УСТРОЙСТВА ДЛЯ ДОКУМЕНТОВ И СИСТЕМЫ АВТОМАТИЗИРОВАННОЙ АУТЕНТИФИКАЦИИ

Для проверки традиционных и новых элементов защиты МСПД важно располагать техническими средствами считывания, ориентированными на многообразие существующих видов проездных документов. Такие считывающие устройства должны быть оснащены соответствующими сенсорными элементами, предназначенными для наиболее распространенных и современных элементов автоматизированной аутентификации. Этот вопрос, естественно, связан с общемировой проблемой затрат и инфраструктуры.

B.2.1 Стандартные считывающие устройства

Стандартные считывающие устройства, используемые на пограничных пунктах, обычно оснащены следующим сенсорным оборудованием:

- средствами ввода изображения в видимом, ультрафиолетовом и инфракрасном диапазоне с высоким разрешением (как минимум 300 точек на дюйм (dpi)), позволяющими считывать МСЗ (предпочтительно в инфракрасной полосе спектра) и обрабатывать изображение других элементов (в видимом диапазоне спектра);

- считывающими устройствами бесконтактных ИС, соответствующими требованиям ИСО 14443 (на частоте 13,56 МГц).

Как правило, стандартные считывающие устройства позволяют обнаружить и верифицировать следующие элементы защиты:

- считывание и верификацию цифр в МСЗ;

- считывание и пассивную аутентификацию бесконтактной ИС (и в качестве факультативной функции активную аутентификацию);

- проверку общих элементов безопасности (матовая УФ-бумага, ИК-считывание МСЗ,…).

Дополнительные возможности этих считывающих устройств зависят исключительно от программного обеспечения, а не от оборудования, и поэтому вполне могут быть введены по усмотрению принимающего государства без дополнительных затрат, связанных со специальным оборудованием. Программное обеспечение считывающих устройств может предусматривать:

- распознавание рисунка с использованием баз данных (на основе изображений в видимом, УФ- и ИК-диапазоне);
- считывание и аутентификацию цифровых водяных знаков (стеганографические элементы) для проверки подлинности;
- обнаружение и считывание (алфавитно-цифровой) информации и будущих элементов защиты;
- обнаружение и считывание элементов защиты в виде вделанных в пластик светоизлучающих диодов.

B.2.2 Усовершенствованные считывающие устройства

Кроме того, усовершенствованные считывающие устройства могут использовать следующие сенсорные средства, предназначенные для аутентификации особых элементов защиты:

- коаксиальное освещение для верификации рефлекторных защитных накладок;
- освещение с помощью лазерных диодов или LED для верификации специальных защитных элементов, например дифракционных оптически изменяющихся средств (DOVID);
- магнитные сенсоры для специальных элементов основы, например, для верификации магнитных нитей;
- специальные устройства для анализа или обнаружения поляризации;
- устройства передачи и освещения информации на странице данных для верификации зарегистрированных водяных знаков, лазерной перфорации, оконных элементов и сквозных считывателей; требуется специальная геометрия считывающего устройства, позволяющая помещать только страницу данных (без обложки) в считывающее устройство.

Обычно установка усовершенствованных считывающих устройств, требующих специального оборудования, регулируется национальными/двусторонними/многосторонними/патентными соглашениями.

B.2.3 Базовые системы, инфраструктура открытых ключей (PKI)

Для аутентификации некоторых типов машиносчитываемых элементов может потребоваться базовая система или PKI. Такой системой может быть существующая PKI МСПД (наиболее значительной частью которой является ДОК ИКАО), в рамках которой государства могут обмениваться информацией об используемых элементах защиты логической структуры данных, защищенных с помощью сертификатов.

B.3 ЭЛЕМЕНТЫ ЗАЩИТЫ И ИХ ПРИМЕНЕНИЕ ДЛЯ АВТОМАТИЗИРОВАННОЙ АУТЕНТИФИКАЦИИ

В нижеследующих разделах описываются основные элементы и методы защиты, которые указаны в положениях о стандартных средствах защиты в добавлении A, и приводятся разъяснения относительно возможностей автоматизированной аутентификации таких механизмов защиты. Для выбора элементов защиты из добавления A полномочные органы выдачи могут использовать приведенные ниже таблицы, чтобы выяснить, какие возможности автоматизированной аутентификации существуют для таких элементов.

B.3.1 Материалы основы

B.3.1.1 Бумажные страницы проездного документа

Элементы защиты	*Сенсорные устройства, необходимые для автоматизированной аутентификации*					*Рисунок фиксированный/ меняющийся*	*Метод автоматизированной аутентификации*
	Стандартное считывающее устройство				*Усовершенствованное считывающее устройство*		
	Видимый	*УФ*	*ИК*	*ВЧ*	*Специальный сенсор*		
Базовые элементы							
Контролируемая УФ-реакция		X					Интенсивность УФ-излучения
Двухтоновый водяной знак					Передача	Фиксированный	Сравнение рисунков
Химические сенсибилизаторы							N/A
Надлежащие характеристики поглощения и поверхности							N/A
Дополнительные элементы							
Зарегистрированный водяной знак					Передача	Фиксированный	Сравнение рисунков
Различные водяные знаки на странице данных и визовых страницах					Передача	Фиксированный	Сравнение рисунков*
Водяной знак в цилиндрической форме					Передача	Фиксированный	Сравнение рисунков
Невидимые флуоресцентные волокна		X	X			Фиксированный/меняющийся	Сравнение рисунков

Элементы защиты	*Сенсорные устройства, необходимые для автоматизированной аутентификации*					*Рисунок фиксированный/ меняющийся*	*Метод автоматизированной аутентификации*
	Стандартное считывающее устройство				*Усовершенствованное считывающее устройство*		
	Видимый	*УФ*	*ИК*	*ВЧ*	*Специальный сенсор*		
Видимые (флуоресцентные) волокна	X	X				Фиксированный/меняющийся	Сравнение рисунков
Защитная нить	X	X			Передача, магнитная	Фиксированный	Сравнение рисунков
Маркер					Особый	Фиксированный/меняющийся	Зависит от маркера
Элемент защиты методом лазерной перфорации					Передача	Фиксированный/меняющийся	Сравнение рисунков

* Требуется взаимодействие пользователей; неприемлемо для автоматизированных систем пограничного контроля.

B.3.1.2 Бумажная или другая основа в форме этикетки

Элементы защиты	*Сенсорные устройства, необходимые для автоматизированной аутентификации*					*Рисунок фиксированный/ меняющийся*	*Метод автоматизированной аутентификации*
	Стандартное считывающее устройство				*Усовершенствованное считывающее устройство*		
	Видимый	*УФ*	*ИК*	*ВЧ*	*Специальный сенсор*		
Базовые элементы							
Контролируемая УФ-реакция		X					Интенсивность УФ-излучения
Химические сенсибилизаторы							N/A
Невидимые флуоресцентные волокна		X	X			Фиксированный/меняющийся	Сравнение рисунков
Видимые (флуоресцентные) волокна	X	X				Фиксированный/меняющийся	Сравнение рисунков

Элементы защиты	*Сенсорные устройства, необходимые для автоматизированной аутентификации*					*Рисунок фиксированный/ меняющийся*	*Метод автоматизированной аутентификации*
	Стандартное считывающее устройство				*Усовершенствованное считывающее устройство*		
	Видимый	*УФ*	*ИК*	*ВЧ*	*Специальный сенсор*		
Клеящиеся материалы							N/A
Дополнительные элементы							
Защитная нить	X				Передача, магнитная	Фиксированный	Сравнение рисунков
Водяной знак					Передача	Фиксированный	N/A
Защитный элемент, создаваемый методом лазерной перфорации					Передача	Фиксированный/меняющийся	Сравнение рисунков
Защитный рисунок, наносимый методом штамповки					Передача	Фиксированный	Сравнение рисунков

B.3.1.3 Синтетические основы

Элементы защиты	*Сенсорные устройства, необходимые для автоматизированной аутентификации*					*Рисунок фиксированный/ меняющийся*	*Метод автоматизированной аутентификации*
	Стандартное считывающее устройство				*Усовершенствованное считывающее устройство*		
	Видимый	*УФ*	*ИК*	*ВЧ*	*Специальный сенсор*		
Базовые элементы							
Структура, устойчивая к расслаиванию							N/A
Оптически матовый материал		X					Интенсивность УФ-излучения
Защита страницы данных							N/A
Оптически изменяющиеся характеристики							См. п. A5.3
См. пп.A.5.2–A.5.5, при необходимости							

Элементы защиты	*Сенсорные устройства, необходимые для автоматизированной аутентификации*					*Рисунок фиксированный/ меняющийся*	*Метод автоматизированной аутентификации*
	Стандартное считывающее устройство				*Усовершенствованное считывающее устройство*		
	Видимый	*УФ*	*ИК*	*ВЧ*	*Специальный сенсор*		
Дополнительные элементы							
Оконный или транспарентный элемент					Передача	Фиксированный	Сравнение рисунков
Осязаемый элемент					Светоотражающий	Фиксированный/меняющийся	Сравнение рисунков
Элемент с лазерной перфорацией					Передача	Фиксированный/меняющийся	Сравнение рисунков
Характеристики поверхности	X		X		Светоотражающий	Фиксированный	Сравнение рисунков

B.3.2 Защитная печать

B.3.2.1 Фон и печатание текста

Элементы защиты	*Сенсорные устройства, необходимые для автоматизированной аутентификации*					*Рисунок фиксированный/ меняющийся*	*Метод автоматизированной аутентификации*
	Стандартное считывающее устройство				*Усовершенствованное считывающее устройство*		
	Видимый	*УФ*	*ИК*	*ВЧ*	*Специальный сенсор*		
Базовые элементы							
Двухцветный гильошированный фон	X	X	X			Фиксированный	Сравнение рисунков
Радужная печать	X	X			Камера с высоким разрешением	Фиксированный	Сравнение рисунков

Элементы защиты	*Сенсорные устройства, необходимые для автоматизированной аутентификации*					*Рисунок фиксированный/ меняющийся*	*Метод автоматизированной аутентификации*
	Стандартное считывающее устройство				*Усовершенствованное считывающее устройство*		
	Видимый	*УФ*	*ИК*	*ВЧ*	*Специальный сенсор*		
Микропечатный текст	X	X	X		Камера с высоким разрешением	Фиксированный	Сравнение рисунков
Уникальный рисунок страницы данных	X					Фиксированный	Сравнение рисунков
Дополнительные элементы							
Глубокая печать	X	X	X			Фиксированный	Сравнение рисунков*
Скрытое изображение							N/A
Схема антисканирования	X				Камера с высоким разрешением	Фиксированный	Сравнение рисунков
Двухтоновый защитный рисунок					Передача	Фиксированный	Сравнение рисунков*
Рельефный элемент					Светоотражающий	Фиксированный	Сравнение рисунков
Сквозная приводка					Передача	Фиксированный	Сравнение рисунков
Преднамеренная ошибка	X	X	X			Фиксированный	OCR, сравнение рисунков
Уникальный рисунок на каждой странице	X	X				Фиксированный	Сравнение рисунков**
Осязаемый элемент					Светоотражающий	Фиксированный	Сравнение рисунков
Уникальный(ые) шрифт(ы)	X	X	X				Сравнение рисунков

* Нецелесообразно для считывания паспортов.

** Требует взаимодействия с пользователем; неприемлемо для автоматизированных систем пограничного контроля.

B.3.2.2 Чернила

Элементы защиты	*Сенсорные устройства, необходимые для автоматизированной аутентификации*					*Рисунок фиксированный/ меняющийся*	*Метод автоматизированной аутентификации*
	Стандартное считывающее устройство				*Усовершенствованное считывающее устройство*		
	Видимый	*УФ*	*ИК*	*ВЧ*	*Специальный сенсор*		
Базовые элементы							
УФ-флуоресцентные чернила		X				Фиксированный/меняющийся	Сравнение рисунков
Реактивные чернила					Специальный		Зависит от чернил
Дополнительные элементы							
Чернила с оптически меняющимися свойствами	X				Переменное освещение	Фиксированный/меняющийся	Сравнение рисунков
Металлические чернила			X			Фиксированный/меняющийся	Сравнение рисунков
Проникающие номерные чернила					Специальный	Меняющийся	Сравнение рисунков на обеих сторонах
Метамерические чернила	X	X	X			Фиксированный	Оптические фильтры и сравнение рисунков
Инфракрасные пропадающие чернила	X		X			Фиксированный/меняющийся	Сравнение рисунков
Инфракрасные абсорбирующие чернила			X			Фиксированный/меняющийся	Сравнение рисунков
Фосфоресцентные чернила		X	X			Фиксированный/меняющийся	Сравнение рисунков
Маркированные чернила					Специальный	Фиксированный	Сравнение рисунков

Элементы защиты	*Сенсорные устройства, необходимые для автоматизированной аутентификации*					*Рисунок фиксированный/ меняющийся*	*Метод автоматизированной аутентификации*
	Стандартное считывающее устройство				*Усовершенствованное считывающее устройство*		
	Видимый	*УФ*	*ИК*	*ВЧ*	*Специальный сенсор*		
Невидимые чернила		X	X			Фиксированный	Сравнение рисунков
Магнитные чернила					Магнитный	Фиксированный/меняющийся	Сравнение рисунков
Антистоксовые чернила			X			Фиксированный/меняющийся	Оптические фильтры и сравнение рисунков

B.3.2.3 Нумерация

Элементы защиты	*Сенсорные устройства, необходимые для автоматизированной аутентификации*					*Рисунок фиксированный/ меняющийся*	*Метод автоматизированной аутентификации*
	Стандартное считывающее устройство				*Усовершенствованное считывающее устройство*		
	Видимый	*УФ*	*ИК*	*ВЧ*	*Специальный сенсор*		
Базовые элементы							
Нумерация на всех листах. Напечатанный и/или перфорированный номер	X		X			Фиксированный/меняющийся	OCR, сравнение рисунков
Специальный шрифт для нумерации	X		X			Фиксированный/меняющийся	OCR, сравнение рисунков
Идентичная методика нанесения номеров и биографических данных на синтетическую основу и карты							N/A

Элементы защиты	*Сенсорные устройства, необходимые для автоматизированной аутентификации*					*Рисунок фиксированный/меняющийся*	*Метод автоматизированной аутентификации*
	Стандартное считывающее устройство				*Усовершенствованное считывающее устройство*		
	Видимый	*УФ*	*ИК*	*ВЧ*	*Специальный сенсор*		
Дополнительные элементы							
Нумерация документа методом лазерной перфорации					Передача	Фиксированный/меняющийся	Сравнение рисунков
Специальные гарнитуры	X					Фиксированный/меняющийся	OCR, сравнение рисунков

B.3.3 Защита от копирования

Элементы защиты	*Сенсорные устройства, необходимые для автоматизированной аутентификации*					*Рисунок фиксированный/меняющийся*	*Метод автоматизированной аутентификации*
	Стандартное считывающее устройство				*Усовершенствованное считывающее устройство*		
	Видимый	*УФ*	*ИК*	*ВЧ*	*Специальный сенсор*		
Базовые элементы							
Оптически изменяющиеся элементы на странице биографических данных	X				Меняющееся освещение	Фиксированный/меняющийся	Сравнение рисунков
OVD с наложенной глубокой печатью при отсутствии ламината							N/A
Дополнительные элементы							
Машиносчитываемый элемент с дифракционными оптически изменяющимися свойствами					Лазер	Фиксированный/меняющийся	Декодирование

Элементы защиты	*Сенсорные устройства, необходимые для автоматизированной аутентификации*					*Рисунок фиксированный/ меняющийся*	*Метод автоматизированной аутентификации*
	Стандартное считывающее устройство				*Усовершенствованное считывающее устройство*		
	Видимый	*УФ*	*ИК*	*ВЧ*	*Специальный сенсор*		
Защитный элемент создаваемый методом, лазерной перфорации					Передача	Фиксированный/меняющийся	Сравнение рисунков
Антисканирующий рисунок	X				Камера с высоким разрешением	Фиксированный	Сравнение рисунков

B.3.4 Методы персонализации

B 3.4.1 Защита от замены и изменения фотографий

Элементы защиты	*Сенсорные устройства, необходимые для автоматизированной аутентификации*					*Рисунок фиксированный/ меняющийся*	*Метод автоматизированной аутентификации*
	Стандартное считывающее устройство				*Усовершенствованное считывающее устройство*		
	Видимый	*УФ*	*ИК*	*ВЧ*	*Специальный сенсор*		
Базовые элементы							
Интеграция биографических данных							N/A
Слияние защитного фона с зоной фотографии							N/A
Реактивные чернила и химические сенсибилизаторы в бумаге							N/A
Наложение видимых защитных средств на зону фотографии	X				Меняющееся освещение	Фиксированный/меняющийся	Сравнение рисунков
Термоусаживаемый защитный ламинат или эквивалентный элемент	X					Фиксированный/меняющийся	Сравнение рисунков

Элементы защиты	*Сенсорные устройства, необходимые для автоматизированной аутентификации*					*Рисунок фиксированный/ меняющийся*	*Метод автоматизированной аутентификации*
	Стандартное считывающее устройство				*Усовершенствованное считывающее устройство*		
	Видимый	*УФ*	*ИК*	*ВЧ*	*Специальный сенсор*		
Дополнительные элементы							
Отображение подписи							N/A
Стеганографический элемент	X	X	X			Фиксированный/меняющийся	Декодирование
Дополнительные изображения фотографии	X	X	X	X		Меняющийся	Сравнение рисунков
Биометрический элемент согласно части 9				X		Меняющийся	РЧ-считыватель

B 3.5 Дополнительные меры защиты для паспортных книжек

Элементы защиты	*Сенсорные устройства, необходимые для автоматизированной аутентификации*					*Рисунок фиксированный/ меняющийся*	*Метод автоматизированной аутентификации*
	Стандартное считывающее устройство				*Усовершенствованное считывающее устройство*		
	Видимый	*УФ*	*ИК*	*ВЧ*	*Специальный сенсор*		
Базовые элементы							
Технология защищенного прошивания							N/A
Сшивание УФ-флуоресцентными нитями		X				Фиксированный	Сравнение рисунков
Уникальный рисунок страницы данных	X					Фиксированный	Сравнение рисунков
Интеграция номеров страниц в защитный рисунок	X	X			Камера с высоким разрешением		Сравнение рисунков
Серийный номер на каждом листе							N/A

Элементы защиты	*Сенсорные устройства, необходимые для автоматизированной аутентификации*					*Рисунок фиксированный/ меняющийся*	*Метод автоматизированной аутентификации*
	Стандартное считывающее устройство				*Усовершенствованное считывающее устройство*		
	Видимый	*УФ*	*ИК*	*ВЧ*	*Специальный сенсор*		
Дополнительные элементы							
Сшивание многоцветной нитью	X	X				Фиксированный	Сравнение рисунков
Программируемое сшивание	X	X				Фиксированный	Сравнение рисунков
Сшивание с использованием УФ-клея							N/A
Указательные отметки на каждой странице							N/A
Защитный элемент, создаваемый методом лазерной перфорации					Передача	Фиксированный/меняющийся	Сравнение рисунков
Биографические данные на внутренней странице							N/A

B 3.6 Дополнительные меры защиты, пригодные для автоматизированной аутентификации

Перечисленные ниже защитные элементы пригодны для автоматизированной аутентификации, но не указаны в добавлении A.

Элементы защиты	*Сенсорные устройства, необходимые для автоматизированной аутентификации*					*Рисунок фиксированный/ меняющийся*	*Метод автоматизированной аутентификации*
	Стандартное считывающее устройство				*Усовершенствованное считывающее устройство*		
	Видимый	*УФ*	*ИК*	*ВЧ*	*Специальный сенсор*		
Базовые элементы							
Считывание МСЗ и верификация цифровых данных	X		X			Фиксированный/меняющийся	Вычисление контрольной суммы

Элементы защиты	*Сенсорные устройства, необходимые для автоматизированной аутентификации*					*Рисунок фиксированный/ меняющийся*	*Метод автоматизированной аутентификации*
	Стандартное считывающее устройство				*Усовершенствованное считывающее устройство*		
	Видимый	*УФ*	*ИК*	*ВЧ*	*Специальный сенсор*		
Считывание и пассивная аутентификация (+AA) бесконтактной ИС				X			РЧ-считыватель
Обнаружение и считывание защитных элементов на основе LED в пластике	X	X	X	X		Фиксированный/меняющийся	Использование РЧ для приведения в действие LED в пластике
Обнаружение и считывание отображаемой (буквенно-цифровой) информации будущих защитных элементов	X	X	X	X		Фиксированный/меняющийся	Использование РЧ для запитывания индикаторов в пластике
Обнаружение и верификация материалов на основе светоотражающей фольги	X				Коаксиальное освещение	Фиксированный/меняющийся	Сравнение рисунков
Штрих-коды	X	X	X			Меняющийся	Декодирование

B.4 КРИТЕРИИ ВЫБОРА ЭЛЕМЕНТОВ ЗАЩИТЫ, ПРИГОДНЫХ ДЛЯ АВТОМАТИЗИРОВАННОЙ ВЕРИФИКАЦИИ

Если государство выдачи рассматривает возможность внесения в свои МСПД элементов защиты, пригодных для автоматизированной аутентификации, или принимающее государство планирует установить считывающие системы, обеспечивающие автоматизированную аутентификацию МСПД, необходимо учитывать различные критерии для выбора таких элементов.

Как и в процессе выбора глобально интероперабельных биометрических технологий или методов хранения данных, эти критерии включают следующие элементы:

- безопасность: наиболее важный критерий;
- доступность, но на исключительной основе для защищенных документов (желательно наличие нескольких поставщиков);
- двойное применение, т. е. дополнительная реализация конкретного элемента, помимо автоматизированной аутентификации, например общие характеристики предотвращения копирования или визуальная проверка;

- возможность персонализации (т. е. придание индивидуального характера) элемента, пригодного для автоматизированной аутентификации, путем введения информации из паспорта для защиты личных данных (например, номера паспорта, фамилии) для того, чтобы избежать повторного использования частей подлинного паспорта;

- совместимость с процессами выдачи МСПД;

- совместимость (с существующими и стандартизированными свойствами МСПД);

- совместимость с процессами контроля на границе и в других местах (например, беспрепятственный доступ к основным элементам защиты, не требующий дополнительного времени);

- интероперабельность;

- наличие сенсорных устройств;

- затраты (связанные с элементами и сенсорами);

- аспекты интеллектуальной собственности (ИС), например патенты;

- первичная или вторичная проверка;

- время, требуемое для фактического использования данного элемента;

- возможные трудности, связанные с процессами изготовления и/или персонализации книжек;

- срок службы, т. е. с учетом соответствующих спецификаций ИСО и ИКАО в отношении МСПД.

— — — — — — — —

ДОБАВЛЕНИЕ С К ЧАСТИ 2. ОПТИЧЕСКАЯ АВТОМАТИЗИРОВАННАЯ АУТЕНТИФИКАЦИЯ (ИНФОРМАЦИОННОЕ)

С.1 ВВЕДЕНИЕ

Для аутентификации машиносчитываемых проездных документов (МСПД), являющейся составной частью отлаженной системы пограничного контроля, включая контрольно-пропускные пункты автоматизированной системы пограничного контроля (АВС), масштабы использования информационных технологий (IT), возможности которых выходят за пределы простого извлечения и проверки МСЗ документов и автоматической проверки оптических элементов, постоянно расширяются. Существенное повышение эффективности технических средств, используемых для автоматизированной аутентификации документов, внесло существенный вклад в увеличение количества и разнообразия систем аутентификации. Однако значительно возросший поток пассажиров по-прежнему является серьезной проблемой для лиц, занимающихся разработкой, изготовлением и развертыванием систем аутентификации и МСПД
.

В состав систем аутентификации, используемых для автоматизированной проверки подлинности МСПД, входит ряд компонентов, которые должны надлежащим образом взаимодействовать между собой. Более того, элементы обеспечения защиты машиносчитываемых документов должны проектироваться и внедряться с учетом возможностей систем аутентификации и результатов аналитической оценки, выполненной опытными специалистами-практиками.

В настоящем добавлении содержится ряд рекомендаций для основных сторон, участвующих в проектировании, внедрении и эксплуатации соответствующих систем и их основных компонентов; в этой связи основные задачи заключаются в следующем:

- повысить степень осведомленности основных заинтересованных сторон, например, поставщиков защищенных документов, изготовителей считывающего оборудования и государственных органов, относительно соответствующих вопросов автоматизированной аутентификации, связанных с обеспечением защиты;
- предложить каталог общих процедур проверок и соответствующую терминологию;
- подготовить рекомендации для разработчиков защищенных документов, изготовителей систем аутентификации и операторов.

Цель настоящего добавления заключается в оказании поддержки специалистам-практикам в проектировании и разработке систем аутентификации. Однако при этом важно иметь в виду, что система аутентификации должна использоваться для оказания содействия оператору [1] в подготовке экспертного заключения и не рассматриваться в качестве единственного средства принятия решений, особенно в отношении элементов защиты, которые нельзя проверить с помощь аппаратуры и верифицировать которые может только человек-оператор.

1. Оператор. Лицо, которое в процессе проверки документов непосредственно взаимодействует с системой аутентификации (например, взаимодействие со считывающим устройством в ручном режиме).

В настоящем добавлении рассматривается только оптический элемент аутентификации МСПД, а масштабы рекомендаций ограничиваются данными, получаемыми с помощью полностраничных считывающих устройств, т. е. полномасштабными изображениями документа, о чем говорится в добавлении В настоящей части. Более того, в рекомендациях не проводится различие между первым, вторым и третьим уровнями инспекции, поскольку полностраничные считывающие устройства могут использоваться в каждом из этих сценариев. В целом портативные устройства (пока) не рассматриваются, что обусловлено их ограниченными оптическими возможностями в части, касающейся использования различных источников света (ультрафиолетовый (UV) и инфракрасный свет (IR) не используются), поэтому предлагаемым требованиям они не отвечают.

В разделе С.2 приводятся основные положения и терминология, необходимые для более полного осознания процесса оптической автоматизированной аутентификации. Вопрос о согласовании и стандартизации процедур проверки рассматривается в разделе С.3, где приводится каталог общих процедур проверки. В разделе С.4 основное внимание уделяется выработке рекомендаций для изготовителей систем аутентификации, а в разделе С.5 приводится краткое описание ряда подходов и методик, связанных с обработкой данных в соответствии с политикой обеспечения защиты данных.

С.1.1 Терминология

Несмотря на то, что для непосредственно затрагиваемых сторон рекомендации и инструктивные указания не носят обязательного характера, в части 1 документа Doc 9303 содержится принятая терминология, обеспечивающая возможность однозначного описания того, что должно соблюдаться для достижения целей, определенных в настоящем документе.

Эта терминология рассматривается в качестве практического средства систематизации рекомендаций и инструктивных указаний в порядке их значимости и ее не следует путать с совокупностью рестриктивных требований, аналогичных используемым в классических стандартах (например, ИСО). Настоящая терминология используется в целях предоставления целевой группе четких, точных и недвусмысленных указаний относительно того, что соответствует и что не соответствует передовой практике.

С.1.2 Влияние электронных проверок на процесс аутентификации

Несмотря на то, что основное внимание уделяется оптическому элементу аутентификации МСПД, необходимо учитывать и ее электронный элемент. Основываясь на современном уровне развития технологий, с большой степенью вероятности можно ожидать того, что в процессе аутентификации будет иметь место взаимодействие между чипом (электронного МСПД) и радиочастотным (РЧ) модулем (полностраничного считывающего устройства). Для наилучшего осознания некоторых рекомендаций, приводимых в настоящем документе, важно иметь в виду, что оптические и электронные проверки (в случае их применения) являются взаимодополняющими процессами, способствующими достижению результата в целом.

Особый интерес представляют два аспекта взаимодействия между электронными и оптическими проверками: сравнение оптических и электронных данных и последствия, обусловленные проведением проверки на предмет наличия чипа, если присутствие такового предполагается. С точки зрения этих двух аспектов нельзя пренебрегать влиянием электронной проверки, на что обращается внимание в соответствующих рекомендациях.

С.2 ОПРЕДЕЛЕНИЯ

В приводимом ниже разделе изложена соответствующая терминология, предназначенная для использования в дальнейшем. Описание процесса проверки МСПД в целом приводится в разделе С.2.1, а его детальное рассмотрение – в разделе С.2.2. Вопрос о влиянии электронного элемента процесса аутентификации рассматривается в разделе С.1.2.

С.2.1 Процесс идентификации и верификации МСПД

Верификация аутентичности проездного документа предусматривает проведение проверки оптических элементов защиты документа. Она выполняется с помощью системы аутентификации[2], в состав которой входят следующие компоненты: полностраничное считывающее устройство (считыватель), программные средства аутентификации[3], база данных аутентификации и (факультативно) справочная база данных.

Полностраничный считыватель формирует полномасштабные изображения проездного документа для их проверки с использованием различных источников света. Этот так называемый *набор оперативных данных* (полномасштабные изображения документа)[4] передаются полностраничным считывателем для их обработки с использованием программных средств аутентификации.

Обычно программные средства аутентификации определяют так называемую *модель документа,* т. е. документа, в котором в качестве входных данных используется информация машиносчитываемой зоны (МСЗ) и/или дополнительная информация (например, информация о конкретной структуре документа, дата выдачи, информация о конкретных оптических элементах и т. д.). Модель документа охватывает те серии документа территории/государства, которые имеют одинаковые оптические характеристики.

В соответствии с техническими рекомендациями, изложенными в документе [BSI-TR-03135], модель документа определяется посредством кода страны (C), типа документа (T), индивидуального идентификационного номера (N) и года первой выдачи (Y):

Модель документа: = (C, T, N, Y)[5]

Код страны (C) должен соответствовать трехбуквенному коду, указанному в документе Doc 9303 ИКАО.

Тип документа (T) также конкретно определяется документом Doc 9303 ИКАО.

Идентификационный номер (N) должен представлять собой индивидуальное целое число, возрастающее в хронологическом порядке, начиная с 1, которое характеризует модель или поколение документа.

---

2. В рамках системы аутентификации приводится описание комбинаций полностраничного считывателя, программных средств аутентификации, включая базу данных аутентификации, и (факультативно) экспертную справочную базу данных.
3. Программные средства аутентификации обеспечивают получение набора оперативных данных с полностраничного считывателя. Они предоставляют ряд алгоритмов аутентификации, обеспечивающих возможность применения обычных процедур проверки с учетом набора оперативных данных.
4. Набор оперативных данных. Видимое, IR и UV изображение проверяемого документа, подлежащего верификации с использованием считывающей системы. Эти изображения используются для проведения инспекции документа.
5. В настоящем добавлении особое внимание уделяется только оптическому элементу автоматической аутентификации документов. Это означает, что документы, оптические элементы которых идентичны, а электронные элементы - отличаются, рассматриваются в качестве относящихся к одной и той же модели документа.

Год (Y) представляет собой четырехзначное целое число, обозначающее год, в котором впервые был выдан документ конкретной модели. Если год не известен, то это значение не указывается.

Например, две модели находящегося в обращении британского паспорта, выданные в 2008 и 2010 гг., имеют следующие идентификаторы: (GBR, P, 1, 2008) и (GBR, P, 2, 2010).

Для идентификации модели документа применяются различные подходы технического характера. Одним из них является получение информации, содержащейся в МСЗ (см. раздел С.4.3.2). Если используется МСЗ, но ее недостаточно для однозначного определения модели документа, необходимо использовать дополнительные параметры документа (например, рисунки), позволяющие конкретизировать результаты идентификации, особенно при рассмотрении ряда действующих моделей документа одной и той же страны (например, британский паспорт)[6].

Программные средства аутентификации направляют идентификатор модели документа в базу данных аутентификации, где хранится информация о так называемых *процедурах проверки*. Эти процедуры проверки определяют процедуры испытаний, подлежащие применению в отношении набора оперативных данных этой конкретной модели проездного документа. Конкретный набор процедур проверки, так называемый *набор данных аутентификации*, определяется для каждой модели документа. После получения идентификатора модели документа из базы данных аутентификации в программные средства аутентификации направляется соответствующий набор данных. Более подробная информация, касающаяся формирования базы данных аутентификации, приводится в разделе С.2.2. (см. рис. С-1.)

6. В некоторых странах, таких как Австралия, для разграничения различных моделей или серий документов, используется буква, обозначающая серию (например, серия N). Несмотря на то, что на национальном уровне этот метод может оказаться достаточным, он не очень эффективен для проведения международной классификации, что обусловлено недостаточной степенью стандартизации. В этой связи, настоящий документ основан на рекомендациях [BSI-TR-03135], которые для целей международной классификации, считаются более приемлемыми.

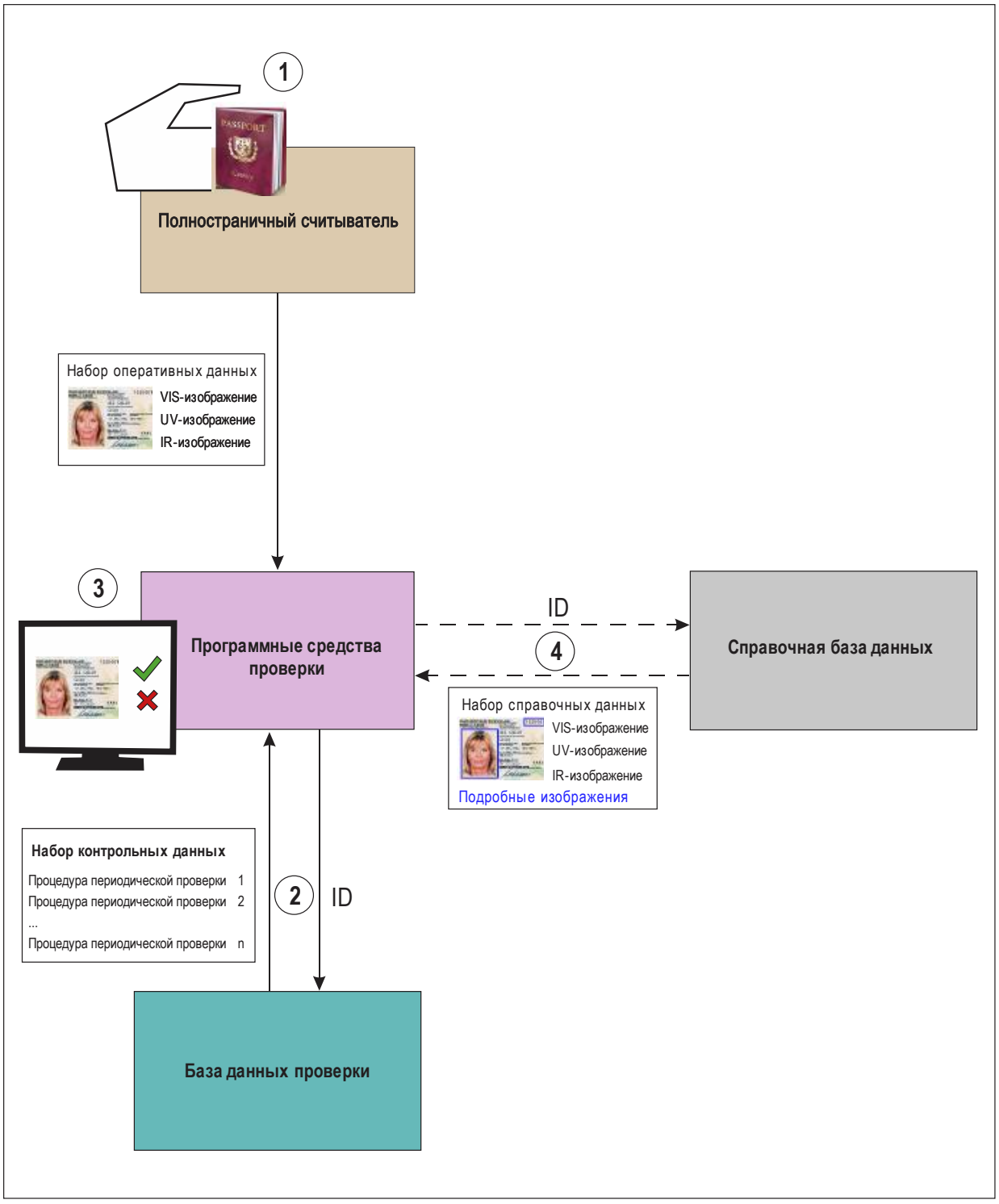

Рис. С-1. Процесс идентификации и верификации документов; цифрами обозначена очередность реализации соответствующего этапа процесса

Затем с помощью программных средств аутентификации проводится верификация. В отношении набора оперативных данных документа применяются обычные процедуры проверки. Как правило, результатом такого контроля являются "проверка пройдена или проверка не пройдена". Результат "проверка пройдена" означает, что проверенный документ не имеет каких-либо отклонений от нормы, а результат "проверка не пройдена" означает обратное. В зависимости от применяемого сценария ответственность за интерпретацию результатов (проверка пройдена или не пройдена) несет человек-оператор.

Если набор оперативных данных нельзя однозначно применить в отношении конкретной модели документа, то (на факультативной основе) можно использовать поднабор обычных процедур проверки. Такие процедуры проверки определяются независимо от модели документа.

Для оказания поддержки человеку-оператору в проведении ручной верификации программные средства аутентификации, основываясь на идентифицированной модели документа, могут запросить в справочной базе данных так называемый *набор справочных данных.* В наборе справочных данных содержатся изображения модели документа, видимые в белом, IR и UV свете; в него могут быть также включены более подробные изображения частей документа, а также дополнительные текстуальные описания. Однако для фактической системы аутентификации наличие так называемой справочной базы данных, которая на практике называется *экспертной базой данных*, не является обязательным. На рис. С-1 приводится описание процесса идентификации и верификации документов.

С.2.2 Подробная организационная структура базы данных аутентификации

В базе данных аутентификации хранится индивидуальный набор обычных процедур проверки для каждой модели документа. Например, обычные процедуры проверки для модели немецкого документа 2007 года отличаются от обычных процедур, которые должны применяться к модели британского документа 2008 года.

Набор обычных процедур проверки основан на спецификации проведения испытаний на предмет определения свойств оптических элементов защиты. Например, обычная процедура проверки 1 на рис. С-2 предусматривает проверку того, является фотография поглощающей при видимом свете. В этом случае фотография представляет собой оптический элемент, который проверяется на наличие свойств поглощения при видимом свете (см. источник света 1 n, используемый в рамках обычной процедуры проверки 1). Реализация этой процедуры проверки осуществляется посредством использования алгоритма, обеспечиваемого программными средствами аутентификации (см. алгоритм аутентификации 1, используемый в рамках обычной процедуры проверки 1). В этом случае алгоритм 1 является алгоритмом аутентификации, осуществляющим проверку яркости элемента. Для сравнения в рамках процедуры проверки x на рис. С-2 показана проверка того, являются ли чернила люминесцентными в UV свете в пределах зоны фотографии посредством использования алгоритмов "проверки рисунка" (алгоритм n программных средств аутентификации на рис. С-2). Этот пример четко свидетельствует о том, что при воздействии различных источников света оптический элемент защиты может продемонстрировать наличие различных свойств (см. рис. С-3).

С точки зрения правил ЕС, касающихся минимальных стандартов на элементы защиты и биометрические параметры в паспортах и проездных документах[7], эти процедуры проверки можно обоснованно разделить на три категории: материал, способ печатания и персонализация.

7. Резолюция Совета (ЕС) No 2252/2004 от 13 декабря 2004 года.

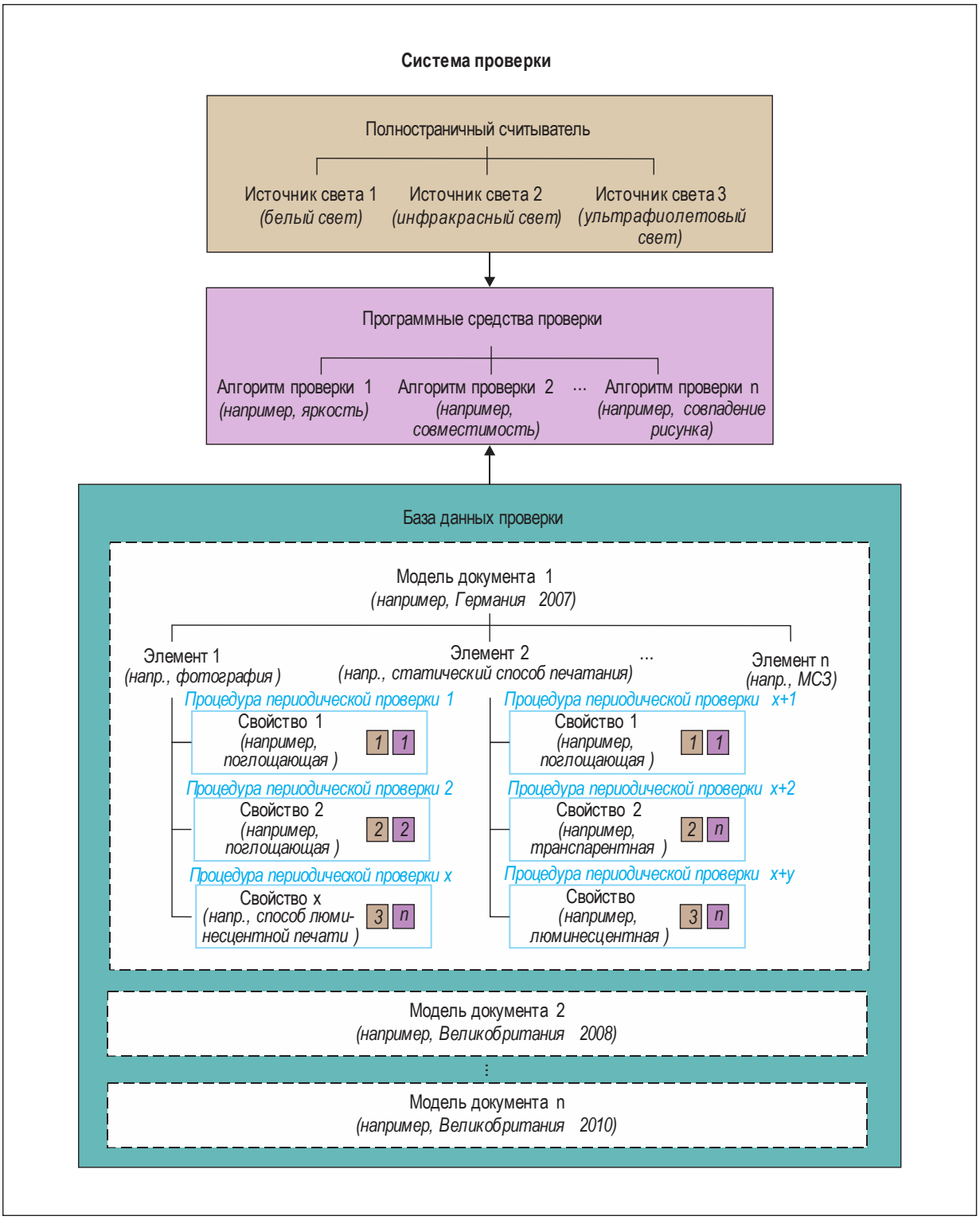

Рис. С-2. Схематическая диаграмма структуры системы аутентификации

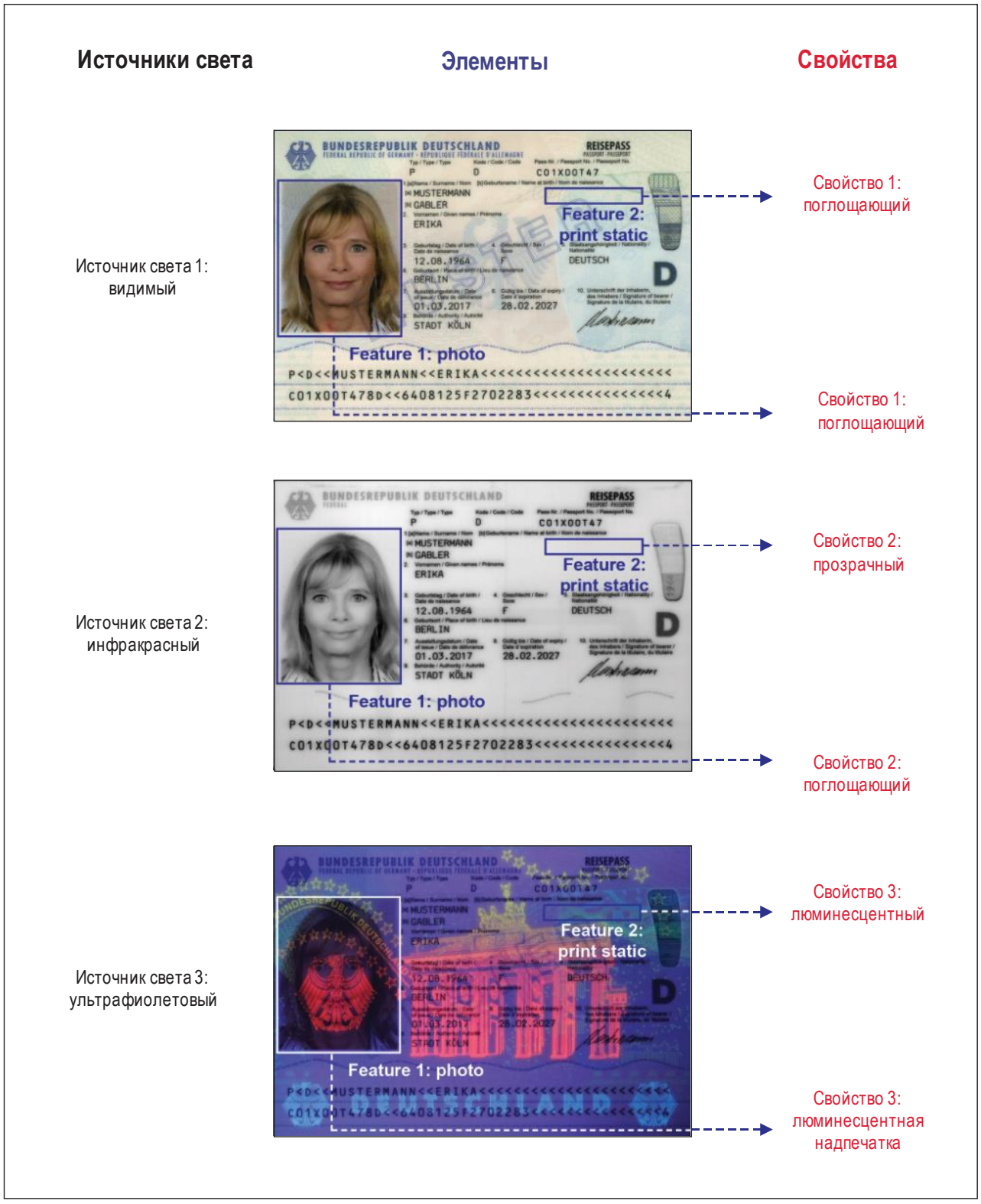

Рис. С-3. Элементы и свойства, демонстрируемые немецким паспортом под воздействием различных источников света

С.3 КАТАЛОГ ОБЩИХ ПРОЦЕДУР ПРОВЕРКИ

Для реализации процедур проверки все разработчики систем аутентификации определяют свои собственные идентификаторы. Для каждой модели документа эти процедуры проверки отличаются; однако зачастую идентификаторы упомянутых процедур проверки не являются самоочевидными. В этой связи, как правило, совместимость процедур проверки, реализуемых в отношении одной и той же модели документа, в рамках различных систем аутентификации не обеспечиваются.

Для решения этой проблемы можно составить каталог практичных процедур проверки проездных документов, основанных на спектрально-селективных элементах защиты. Содержание этого каталога можно будет распространить на будущие версии настоящих инструктивных указаний, сохранив при этом предлагаемую систему условных обозначений. В рамках реализации соответствующих, так называемых, спектрально-селективных процедур проверки регистрируются различные реакции проверяемого документа при воздействии на него видимого (VI – видимого света) или невидимого (UV – ультрафиолетового и IR – инфракрасного света). На основе результатов проведения этих трех видов проверок (VI, UV, IR) можно установить поглощающую, рефлективную и люминесцентную реакции этих элементов. В определенной последовательности о отношении этих спектрально-селективных процедур проверки используются обозначения общих процедур проверки, определенные в документе [BSI-TR-03135].

Применение этого каталога общих процедур проверки позволит в значительной степени улучшить вышеупомянутую ситуацию и обеспечить возможность более полного осознания механизмов автоматизированной аутентификации.

С.3.1 Описание общих процедур проверки

Однозначные (определенные ниже) идентификаторы процедур проверки, определенные для оптической автоматизированной аутентификации, основаны на спектральной реакции элементов защиты проездных документов. Объективно их можно подразделить на перечисленные ниже четыре категории, информация о которых приводится в добавлении А:

- проверка свойств материала (подложки). Проводится проверка реакции печатной подложки; например, яркость при воздействии UV света;
- проверка свойств, обеспечиваемых способами печати. Проверке подвергаются элементы, которые наносятся на документ/впечатываются в него независимо от персонализации, например, оттиск формуляра;
- проверка элементов защиты от копирования; обычно дифракционных или голографических элементов или ламинированных материалов;
- проверка свойств, предусмотренных технологией изготовления документов (персонализация). Проверке подвергаются элементы персонализации, например, фамилия владельца документа.

Зрительное восприятие элементов, относящихся к категории "защита от копирования", в значительной степени зависит от геометрии освещения. Поэтому в целом элементы этой категории, которые хорошо подходят для проверки человеком, могут быть очень проблематичными для автоматизированной аутентификации. По этой причине в рамках предлагаемых процедур проверки элементы данной категории не рассматриваются.

В состав определенных ниже 48 общих процедур проверки входят, так называемые, *базовые процедуры проверки (BR)* и *комбинированные процедуры проверки (CR)*. Базовые процедуры проверки

являются индивидуальными процедурами, в рамках которых рассматривается одно свойство (например, IR-поглощение) одного элемента. Комбинированные процедуры проверки представляют собой логические комбинации базовых процедур проверки. В этой связи имеется возможность проверить несколько свойств одного элемента, таких как IR – поглощение и прозрачность в видимом свете.

Согласно документу [BSI-TR-03135] в отношении базовых процедур проверки используются приводимые ниже сокращенные определения:

Базовая процедура проверки:= (XX, YY, ZZ)

XX – определяет источник света, используемый в ходе реализации базовых процедур проверки изображения:

- **IR** – инфракрасный свет
- **UV** – ультрафиолетовый свет
- **VI** – видимый (белый) свет

YY – является идентификатором, характеризующим оптические свойства конкретного элемента:

- **AB** – поглощающие (свойство чернил)
- **BR** – яркость (свойство подложки, например, яркая при воздействии UV-света)
- **FR** – характеристики пространственной частоты рисунков (узоров) (например, характеристики рисунков, полученные после преобразования пространственной частоты, например, после выполнения пространственного преобразования Фурье)
- **LU** – люминесцентный (свойство рисунков, например, они становятся видимыми при воздействии UV-света)
- **TL** – просвечивающиеся (свойство чернил просвечиваться сквозь подложку)
- **TR** – прозрачные (свойство чернил, например, чернила становятся прозрачными при воздействии IR-света)

ZZ – является идентификатором[8] самого элемента или его местоположения в документе:

- **FI** – волокна
- **FU** – полная (детальная) страница данных
- **IS** – напечатанный элемент, который уже имеется на подложке (чернила для статической печати)

8. В рамках настоящей системы условных обозначений характерные для модели документа свойства обозначаются как "статичные" (такие, как UV-надпечатка государственного герба), а свойства, характерные для документа (индивидуальные/персонализированные) обозначаются как "динамичные" (такие, как UV-надпечатка, повторяющая номер документа).

- **MR** – машиносчитываемая зона (МСЗ)
- **OM** –надпечатанная МСЗ
- **CA** – номер доступа к карточке (сокращенно: CAN)
- **BC** – элемент "штрих-код"
- **PD** – персонализированное "динамичное" перфорирование
- **PS** – перфорирование, показывающее "фиксированный" контент
- **PH** – зона фотографии
- **SP** – зона размещения дополнительной фотографии
- **OP** – надпечатанная фотография
- **TH** – защитная нить
- **VZ** – зона визуальной проверки (ЗВП)
- **WM** – водяной знак
- **ID** – любой другой персонализированный "динамичный" элемент (чернила для динамичной печати), например, дополнительная фотография
- **AF** – любой дополнительный элемент, который нельзя отнести к элементам, указанным выше

Если общая процедура проверки состоит из нескольких процедур, то каждой отдельной процедуре проверки необходимо присваивать порядковый номер.

Ниже представлена информация о выполнении общих процедур проверок, результаты которых представлены в виде приводимых ниже сокращенных терминов [9]:

Проверка свойств материала: (12 BR + 1 CR)

- **(IR, AB, PS)** → (IR, поглощающий статическая перфорация). Проверить, является ли статическая перфорация видимой в IR-свете.
- **(IR, AB, TH)** → (IR, поглощающий, наличие защитной нити). Проверить, является ли защитная нить видимой в IR-свете.
- **(IR, AB, WM)** → (IR, поглощающий, наличие водяного знака). Проверить, является ли водяной знак видимым в IR-свете.
- **(UV, BR, FU)** → (UV, яркость, полномасштабная страница). Проверить на предмет яркости полномасштабной страницы данных в UV-свете.

9. Процедуры проверок, основанные на AF, подробно не рассматриваются, поскольку их можно совместить с каждым из упомянутых источников света и оптическими свойствами.

- **(UV, BR, MR)** → (UV, яркость, МСЗ). Проверить на предмет яркости в МСЗ в UV-свете.
- **(UV, BR, PH)** → (UV, яркость, фотография). Проверить на предмет яркости в зоне фотографии в UV-свете.
- **(UV, BR, VZ)** → (UV, яркость, ЗВП). Проверить на предмет яркости в зоне визуальной проверки (ЗВП) в UV-свете.
- **(UV, LU, FI)** → (UV, люминесцентный, наличие волокон). Проверить на наличие волокон, люминесцирующих в UV-свете.
- **(UV, LU, PS)** → (UV, люминесцирующий, фиксированная перфорация). Проверить на наличие фиксированной перфорации, люминесцирующей в UV-свете.
- **(UV, LU, TH)** → (UV, люминесцентный, наличие защитной нити). Проверить на наличие защитной нити, люминесцирующей в UV-свете.
- **(VI, TR, TH)** → (VI, прозрачный, наличие защитной нити). Проверить, является ли защитная нить прозрачной при видимом свете.
- **(VI, AB, PS)** → (VI, поглощающий, статистическая перфорация). Проверить, является ли статическая перфорация видимой в видимом свете.
- **(IR, AB, TH)** ° (**VI, TR, TH)** → (IR, поглощающий, наличие защитной нити) в сочетании с (VI, прозрачный, наличие защитной нити). Проверить, является ли защитная нить видимой в IR-свете, прозрачной в видимом свете.

Проверка свойств, обеспечиваемых способами печати:(8 BR + 2 CR)

- **(IR, AB, IS)** → (IR, поглощающий, чернила для статической печати). Проверить, являются ли чернила, используемые для статической печати, поглощающими в IR-свете.
- **(IR, TL, IS)** → (IR, прозрачный, чернила для статической печати). Проверить, являются ли чернила на оборотной странице данных (обычно название страницы) прозрачными в IR-свете и поддаются обнаружению на IR-изображении страницы данных.
- **(IR, TR, IS)** → (IR, прозрачная, чернила, используемые для статической печати). Проверить, являются ли чернила, используемые для статической печати, прозрачными в IR-свете.
- **(UV, LU, IS)** → (UV, люминесцентный, чернила для статической печати). Проверить, являются ли чернила, используемые для статической печати, люминесцентными в UV-свете.
- **(UV, LU, OM)** → (UV, люминесцентный, надпечатанная МСЗ). Проверить, являются чернила, используемые для статической печати, люминесцентными в зоне МСЗ в UV-свете.
- **(UV, LU, OP)** → (UV, люминесцентный, надпечатанная фотография). Проверить, являются ли чернила, используемые для статической печати, люминесцентными в UV-свете.
- **(VI, AB, IS)** → (VI, поглощающий, чернила, используемые для статической печати). Проверить, являются ли чернила, используемые для статической печати, поглощающими в видимом свете.

- **(VI, TR, IS)** → (VI, прозрачный, чернила, используемые для статической печати). Проверить, являются ли чернила, используемые для статической печати, прозрачными в видимом свете.

- **(IR, TR, IS)** ° **(IR, AB, IS)** → (IR, прозрачный, чернила, используемые для статической печати) в сочетании с (IR, поглощающая, чернила, используемые для статической печати). Проверить, являются ли части статической печати поглощающими в IR-свете, а другие части того же элемента – прозрачными в IR-свете.

- **(IR, TR, IS)** ° **(VI, AB, IS)** → (IR, прозрачная, чернила, используемые для статической печати) в сочетании с (VI, поглощающий, чернила, используемые для статической печати). Проверить, являются ли чернила, используемые для статической печати, прозрачными в IR-свете и поглощающими в видимом свете.

Проверка свойств персонализации: (28 BR + 3 CR)

- **(IR, AB, ID)** → (IR, поглощающий, чернила, используемые для динамической печати). Проверить, являются ли чернила, используемые для динамической печати, поглощающими в IR-свете.

- **(IR, AB, MR)** → (IR, поглощающий, МСЗ B900 проверка). Проверить, является ли МСЗ видимой в IR-свете.

- **(IR, AB, CA)** → (IR, поглощающий, CAN). Проверить, является ли CAN видимым в IR-свете.

- **(IR, AB, BC)** → (IR, поглощающий, наличие штрих-кода). Проверить, является ли штрих-код видимым в IR-свете.

- **(IR, AB, PD)** → (IR, поглощающий, динамическая перфорация). Проверить, является ли динамическая перфорация видимой в IR-свете.

- **(IR, AB, PH)** → (IR, поглощающий, фотография). Проверить, является ли фотография видимой в IR-свете.

- **(IR, FR, PH)** → (IR, частота, фотография), Проверить, обладает ли рисунок ожидаемыми характеристиками после преобразования пространственной частоты.

- **(IR, AB, SP)** → (IR, поглощающий, наличие дополнительной фотографии). Проверить, является ли дополнительная фотография видимой в IR-свете.

- **(IR, TR, SP)** → (IR, прозрачный, наличие дополнительной фотографии). Проверить, является ли дополнительная фотография прозрачной в IR-свете.

- **(IR, TR, ID)** → (IR, прозрачный, чернила для динамической печати). Проверить, являются ли чернила, используемые для динамической печати прозрачными в IR-свете.

- **(IR, TR, PH)** → (IR, прозрачный, фотография). Проверить прозрачность фотографии в IR-свете.

- **(UV, FR, PH)** → (UV, частота, фотография). Проверить, обладает ли рисунок ожидаемыми характеристиками после преобразования пространственной частоты.

- **(UV, LU, SP)** → (UV, люминесцентная, наличие дополнительной фотографии). Проверить, является ли дополнительная фотография люминесцентной в UV-свете.

- **(UV, LU, BC)** → (UV, люминесцентный, наличие штрих-кода). Проверить, является штрих-код люминесцентным в UV-свете.

- **(UV, LU, ID)** → (UV, люминесцентный, чернила для динамической печати). Проверить, являются ли чернила, используемые для динамической печати, люминесцентными в UV-свете.

- **(UV, LU, PD)** → (UV, люминесцентный, динамическая перфорация). Проверить, являются ли знаки динамической перфорации люминесцентными в UV-свете.

- **(VI, AB, ID)** → (VI, поглощающий, чернила для динамической печати). Проверить, являются ли чернила, используемые для динамической печати, видимыми при видимом свете.

- **(VI, AB, MR)** → (VI, поглощающий, МСЗ). Проверить, является ли МСЗ видимой в видимом свете.

- **(VI, AB, CA)** → (VI, поглощающий, CAN). Проверить, является ли CAN видимым при видимом свете.

- **(VI, AB, BC)** → (VI, поглощающий, наличие штрих-кода). Проверить, является ли штрих-код видимым в видимом свете.

- **(VI, TR, BC)** → (VI, прозрачный, наличие штрих-кода). Проверить, является ли штрих-код прозрачным в видимом свете.

- **(VI, AB, PD)** → (VI, поглощающий, динамическая перфорация). Проверить, является ли динамическая перфорация видимой в видимом свете.

- **(VI, AB, PH)** → (VI, поглощающий, фотография). Проверить, является ли фотография видимой в видимом свете.

- **(VI, AB, SP)** → (VI, поглощающий, наличие дополнительной фотографии). Проверить, является ли дополнительная фотография видимой в видимом свете.

- **(VI, TR, SP)** → (VI, прозрачный, наличие дополнительной фотографии). Проверить, является ли дополнительная фотография прозрачной в видимом свете.

- **(VI, FR, PH)** → (VI, частота, фотография). Проверить, обладает ли рисунок ожидаемыми характеристиками после преобразования пространственной частоты.

- **(VI, AB, SP)** → (VI, поглощающий, наличие дополнительной фотографии). Проверить, является ли дополнительная фотография видимой при видимом свете.

- **(VI, TR, ID)** → (VI, прозрачный, чернила для динамической печати). Проверить, являются ли чернила, используемые для динамической печати, прозрачными в видимом свете.

- **(IR, TR, ID) (VI, AB, ID)** → (IR, прозрачный, чернила для динамической печати) в сочетании с (VI, поглощающий, чернила для динамической печати). Проверить, являются ли чернила, используемые для динамической печати, прозрачными в IR-свете, а также поглощающими в видимом свете.

- **(IR, TR, SP)** ° **(VI, AB, SP)** → (IR, прозрачный, наличие дополнительной фотографии) в сочетании с (VI, поглощающий, наличие дополнительной фотографии). Проверить, является ли дополнительная фотография прозрачной в IR-свете, а также поглощающей в видимом свете.

- **(VI, TR, BC)** ° **(IR, AB, BC)** → (VI, прозрачный, наличие штрих-кода) в сочетании с (IR, поглощающий, наличие штрих-кода). Проверить, является ли штрих-код прозрачным в видимом свете, а также поглощающим в IR-свете.

Приводимый ниже порядок комбинированной проверки определяется совместно для двух классов проверок: печатание и персонализация:

- **(IR, TR, IS)** ° **(VI, AB, IS)** ° **(IR, AB, ID)** → (IR, прозрачный, чернила для статической печати) в сочетании с (VI, поглощающий, чернила для статической печати) в сочетании с (IR, поглощающий, чернила для динамической печати). Проверить, являются ли чернила, используемые для статической печати, поглощающими в видимом свете и прозрачными в IR-свете. Кроме того, является ли элемент, созданный с помощью динамической печати, видимым в IR-свете в том же положении.

С точки зрения значимости для процесса проверки процедуры, указанные выше, неравнозначны. Например, как таковой результат реализации процедуры проверки (VI, AB, ID) особого значения не имеет. Хотя для обнаружения подделки в сочетании с другой процедурой проверки (IR, TR, ID) он приобретает особую значимость.

Свойства и элементы, имеющие непосредственное отношение к выявлению подделок, следует инкорпорировать путем инвертирования логики процедур проверки. Например, конкретную конфигурацию имитируемых защитных волокон следует проверять на предмет отсутствия этого рисунка (те.VI, TR, IS).

Таблица С-1 дает общее представление о классификации системы общих процедур проверки. В матрице сгруппированы три компонента идентификаторов проверки: элемент, источник света и свойство. Содержание строк, колонок и клеток поясняет общие базовые процедуры проверки. Предусмотренные классы проверок помечены цветами: зеленый (материал), голубой (способ печати) желтый (персонализация).

Таблица С-1. Матричное представление общих базовых процедур проверки. Сокращенно оптические свойства обозначаются следующим образом: AB – поглощающие (свойства чернил); BR – яркость (свойство подложки); FR – пространственная частота (свойство рисунков); LU – люминесцентность (свойство рисунков); TL – просвечивающиеся (свойства чернил просвечиваться через подложку); TR – прозрачные (свойства чернил); классы проверок помечены цветами: зеленый (материал), голубой (способ печати) и желтый (персонализация).

Элемент		*Источник света*		
		VI	*UV*	*IR*
Волокна	FI		LU	
Полная страница данных	FU		BR	
Элемент статической печати	IS	{AB. TR}	LU	{AB, TR, TL}
МСЗ	MR	AB	BR	AB
Надпечатанная МСЗ	OM		LU	
CAN	CA	AB		AB
Штрих-код	BC	{AB, TR}	LU	AB
Персонализованная перфорация (динамичная)	PD	AB	LU	AB

Элемент		*Источник света*		
		VI	*UV*	*IR*
Перфорация на подложке (статическая)	PS	AB	LU	AB
Фотография	PH	{AB, FR}	{BR, FR}	{AB, FR, TR}
Дополнительная фотография	SP	{AB, TR}	LU	{AB, TR}
Фотография с надпечаткой	OP		LU	
Защитная нить	TH	TR	LU	AB
Зона визуальной проверки (ЗВП)	VZ		BR	
Водяной знак	WM			AB
Персонализованный динамичный элемент	ID	{AB, TR}	LU	{AB, TR}
Дополнительный элемент	AF	{AB,BR,LU, TL,TR}	{AB,BR,LU, TL,TR}	{AB,BR,LU, TL,TR}

C.4 РЕКОМЕНДАЦИИ ОТНОСИТЕЛЬНО АВТОМАТИЗИРОВАННОЙ АУТЕНТИФИКАЦИИ МСПД

В процессе основанной на использовании автоматизированных устройств аутентификации задействованы следующие основные компоненты: документ, полностраничный считыватель и программные средства аутентификации (включая базу данных аутентификации, см. раздел C.2.2). Однако зачастую эти компоненты проектируются/изготавливаются без учета их взаимозависимости, особенно в части, касающейся формата защищенного документа. Для того чтобы автоматизированную аутентификацию можно было проводить оптимальным образом исключительно важно обеспечить взаимное бесперебойное взаимодействие этих компонентов.

В следующих разделах приводятся рекомендации относительно эффективной и действенной разработки документа (см. раздел C.4.1), полностраничного считывателя (см. раздел C.4.2), программных средств аутентификации (см. раздел C.4.3), базы данных аутентификации (см. раздел C.4.4) и справочной базы данных (см. раздел C.4.5). В разделе C.4.6 в качестве примера в рамках сценариев использования показана реализация рекомендаций, сделанных в предыдущих разделах, в целях оказать администратору текущих операций[10] помощь в планировании эксплуатации систем оптической аутентификации.

Как правило, при обсуждении рекомендаций, касающихся различных компонентов, следует учитывать разницу во времени, необходимом для внесения изменений:

- программные средства системы контроля: 1–12 мес.;

10. Администратор текущих операций представляет собой организацию, ответственную за административное обеспечение всех процессов, связанных с эксплуатацией инфраструктуры аутентификации, и управление ими. Администратор текущих операций создает каналы связи с поставщиками/изготовителями изделий, используемых в готовой системе аутентификации, и обеспечивают их функционирование.

- аппаратные средства системы контроля: 3– 5 лет;

- защищенный документ: 10–20 лет (включая, как правило, период эмитирования, составляющий 5–10 лет, и срок действия, составляющий 5–10 лет).

С.4.1 Разработчики документов

При разработке документа с оптическими элементами, обеспечивающими максимально возможную защиту, осуществление контроля оператором не должно быть единственной целью разработчика документа. Используемые в документе элементы защиты должны также обеспечивать возможность автоматизированной аутентификации. В дополнение к базовому формату МСПД, отвечающему требованиям документа Doc 9303 ИКАО, в последующих разделах приводится краткая информация об элементах, приемлемых для автоматизированной аутентификации. Кроме того, в последующих разделах будут также кратко рассмотрены элементы, которые, даже несмотря на их значение для проведения контроля оператором, могут воспрепятствовать автоматизированной аутентификации (см. раздел С.4.1.2). В контексте автоматизированной аутентификации эти элементы определяются как "потенциально нежелательные". Разработчиков документов не следует удерживать от включения этих элементов в документ, однако при рассмотрении вопроса о включении им следует учитывать возможное (негативное) влияние на процесс автоматизированной аутентификации.

С.4.1.1 Элементы, подходящие для автоматизированной аутентификации

Рекомендации, касающиеся элементов, подходящих для автоматизированной аутентификации, приводятся ниже. Эти элементы выбраны в силу того, что их несложно обнаружить на VI, IR и UV-изображениях, однако в то же время они значительно затрудняют деятельность лиц, занимающихся подделкой документов.

A.1 **Определить однозначные элементы идентификации.** Характерной практикой некоторых государств является выпуск последующих моделей документов в течение относительно короткого периода времени в целях улучшения защитных свойств своих МСПД. Наглядными примерами преемственных моделей документов являются модели британского паспорта (GBR, P, 1, 2008) и (GBR, P, 2, 2010). В этой связи в процессе разработки документа необходимо определить элементы, обеспечивающие возможность однозначной идентификации модели документа (например, штрих-код[11], содержащий информацию о модели документа).

A.2 **Определить элементы, изучаемые под воздействием всех трех источников света.** Несмотря на то, что стандартной характеристикой полностраничных считывателей является захват изображений под воздействием этих источников света, практический опыт свидетельствует о том, что лицам, занимающимся подделкой документов, довольно трудно надлежащим образом воспроизвести элементы, подлинность которых можно определить с использованием более чем одного из этих источников света. Поэтому определение наличия оптических элементов защиты под воздействием всех трех источников света (VI, IR и UV) существенно усложняет производство поддельных документов.

A.3 **Определить элементы в трех категориях.** Обеспечение сбалансированного использования элементов защиты в таких категориях, как "материал", "способ печати" и "персонализация" также усложняет подделку документов. В этой связи в каждой категории элементы должны определяться в соответствии с положениями документа Doc 9303 ИКАО.

11. Этот пример использования штрих-кода не противоречит рекомендациям частей 9 и 10 документа Doc 9303, касающимся электронного хранения биометрических данных.

A.4 **Определить элементы для обеих сторон идентификационных (ID) карт.** ID-карты размера ID-1 можно размещать в полностраничном считывателе любой стороной. Поэтому разработчики документов проектируют ID-карты размера ID-1 с элементами идентификации и верификации, имеющимися на обеих сторонах, что позволяет производить идентификацию и верификацию независимо от стороны карты.

A.5 **Определить элементы, неодинаково реагирующие на различные источники света.** Элементы документа, неодинаково реагирующие на различные источники света (см. рис. С-4), оказывают существенную помощь в уменьшении вероятности успешного изготовления мошенниками соответствующих фальшивых документов. Поэтому для автоматизированной аутентификации необходимо использовать элементы, наличие и/или отсутствие которых можно проверить посредством соответствующего источника света (например, это обеспечивается посредством использования метамерных чернил; этот процесс, показанный на рис. С-4, также называется разбивкой элемента защиты в IR-свете и проверяется посредством обычных (IR, TR, IS) (VI, AB, IS)).

A.6 **Определить элементы, приобретающие различные цвета в UV-свете.** Элементы, светящиеся различными цветами под воздействием UV-света (см. рис. С-5) могут значительно усложнить процессы их воспроизведения, поэтому использовать эти элементы рекомендуется. В то же время в дополнение к простой проверке на наличие этого элемента в процессе автоматизированной аутентификации можно проверить колористическую гамму этого элемента. Более того, рекомендуется использовать цвета, существенно отличающиеся с точки зрения их координат хроматичности, что упростит их распознавание оборудованием. Люминесцентные свойства соответствующих чернил имеют тенденцию к ухудшению, что дополнительно усложняет процесс надежного автоматизированного обнаружения.

Рис. С-4. Паспорт (CZE, P, 1, 2011). Разбивка заголовка текста в IR-свете

Рис. C-5. Паспорт (GBR, P, 2, 2010). Двухцветный рисунок в UV-свете[12]

A.7 **Определить рисунки с индивидуальным контентом, например с вторичным изображением лица.** Рекомендуется определить индивидуальные рисунки, которые можно проверить на предмет их свойств и сравнить с контентом, уже имеющимся на странице данных. Например, вторичное изображение лица можно сравнить с первичным изображением лица, причем эти два изображения могут иметь аналогичные или различные спектральные свойства. Приводимый ниже перечень рисунков, на которых имеются вторичные изображения лица, призван проиллюстрировать эту рекомендацию, однако он не является исчерпывающим и его не следует рассматривать в качестве четко сформулированной рекомендации в отношении этих конкретных элементов:

a) Вторичное изображение лица представляет собой уменьшенное повторное изображение лица, видимое при видимом свете и прозрачное в IR-свете (поддается проверке посредством (VI, AB, ID) ° (IR, TR, ID)).

b) Оптически изменяемые чернила (OVI) и дифракционные оптически изменчивые устройства визуализации (DOVID), являющиеся средством персонализации, например посредством лазерной гравировки или лазерной абляции (см. рис. C-6). На приводимом рис. C-6 в качестве примера элемента показаны различные цвета, видимые под различными углами зрения в видимом свете (первое и второе изображение) и слабовидимое в пропущенном свете вторичное изображение лица (третье изображение). В IR-свете можно получить четкое вторичное изображение лица и сравнить его с первичным изображением лица. Этот элемент можно проверить посредством выполнения следующей комбинированной проверки: (IR, AB, ID) ° (VI, AB, IS) ° (IR, TR, IS), что представляет собой троекратную комбинацию.

12. Источник: http://edisontd.net/.

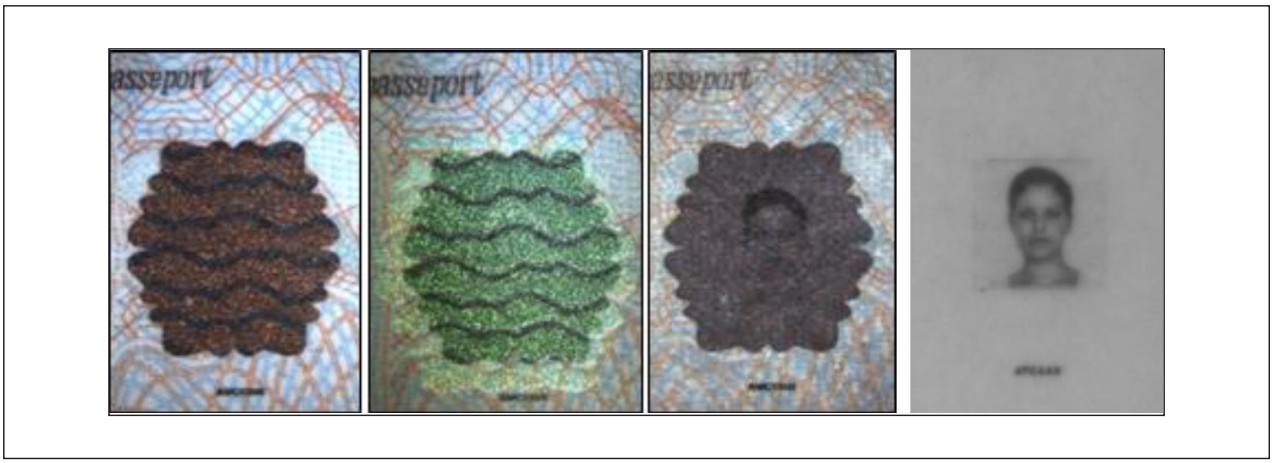

Рис. С-6. Паспорт (HUN, P, 1, 2006). Выполненное с использованием OVI персонализированное изображение, рассматриваемое под различными углами в пропущенном свете и IR-свете

c) Лазерная гравировка персональных данных, реагирующая противоположным ("в виде негатива") образом (см. рис. С-7). На рис. С-7 представлен наглядный пример элемента, изображение которого можно получить при видимом свете, и который представляет собой негативное вторичное изображение лица при его рассмотрении под двумя различными углами.

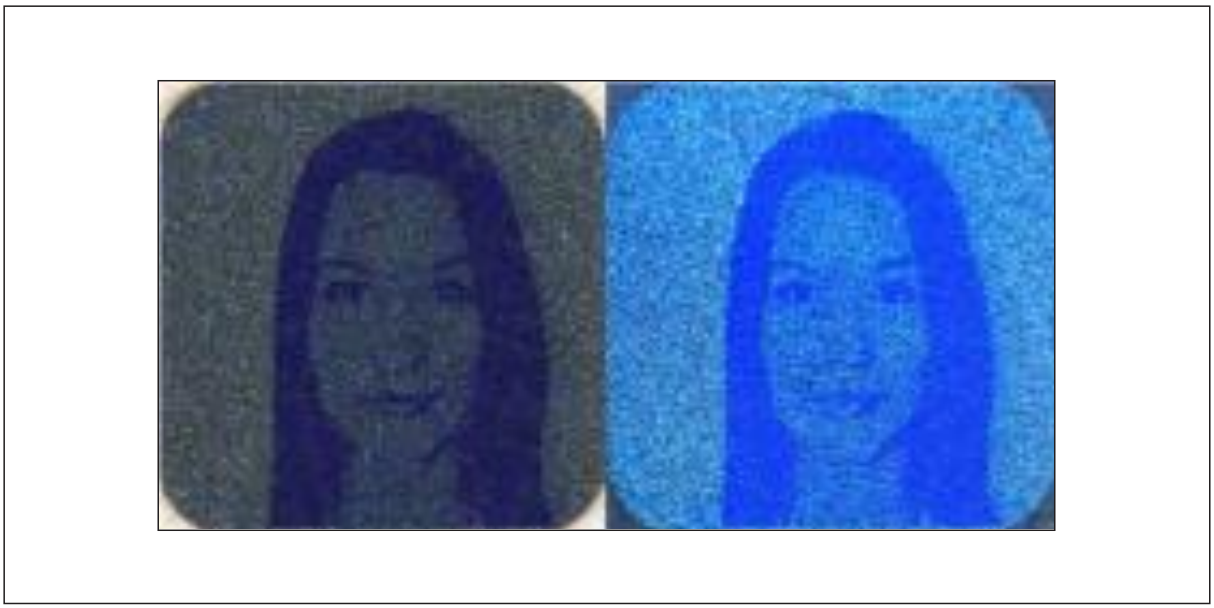

Рис. С-7. Паспорт (LVA, P, 1, 2015). Выполненная методом лазерного гравирования персонализация "негативного изображения", рассматриваемого под различными углами зрения в видимом свете

A.8 **Определить элементы, сохраняющие свою стабильность в течение срока действия МСПД.** Со временем качество некоторых элементов может ухудшаться. Например, в течение периода действия МСПД цвета рисунков в UV-свете могут потускнеть. С течением времени клеи накладки могут привезти к значительной потере четкости рисунков, рассматриваемых в UV-свете,

в результате чего может иметь место значительная потеря четкости рисунков, рассматриваемых в UV-свете, и, как следствие этого, возможное получение неточных результатов проверки данного элемента. В этой связи рекомендуется определить элементы, которые в течение срока действия МСПД в максимально возможной степени сохраняют свою стабильность.

A.9 **Определить нереального владельца документа для использования его личности в образцах документов.** Для выработки стандартизированного подхода к идентификации образцов документов гражданство владельца в образцах рекомендуется указывать как "UTO".

C.4.1.2 Элементы, потенциально препятствующие автоматизированной аутентификации

В настоящем разделе рассматриваются элементы, которые могут потенциально препятствовать автоматизированной аутентификации (в контексте, упоминавшемся в начале раздела C.4.1):

- **Элементы, частично налагаемые друг на друга.** Элементы, частично налагаемые друг на друга и определяемые без учета их взаимозависимости, при воздействии источника света могут взаимодействовать негативно. Дифракционные эффекты DOVID могут помешать считыванию страницы данных (см. рис. C-8).

Рис. C-8. Паспорт (AUT, P, 1, 2006).
Голографический защитный ламинат со следами оптической дисторсии

- **Элементы, расположенные вблизи верхней кромки документа.** Практический опыт свидетельствует о том, что оптические свойства элементов, расположенных вблизи верхней кромки (например, как показано на приводимом примере), могут мешать автоматизированной аутентификации и приводить к уменьшению зоны получения изображения. Частичное изображение этого элемента может привести к ошибкам.

- **Элементы, видимые только при высоком разрешении.** Основываясь на современном уровне развития технологии, следует отметить, что большинство полностраничных считывателей, используемых в настоящее время в системах аутентификации, обеспечивают максимальную номинальную разрешающую способность 400 ppi, а реальная оптическая разрешающая способность находится на уровне, который меньше даже этого значения. Элементы, видимые только при высоком разрешении, превышающем 400 ppi (например, микротексты, гильошированные изображения), обнаружению имеющимися на современном рынке полностраничными считывателями не поддаются (см. рис. С-9). Однако в ближайшем будущем эти элементы можно будет верифицировать с помощью полностраничных считывателей, разрешающая способность которых составляет 600 ppi или более.

Рис. С-9. Паспорт (D, P, 1, 2017). Сравнение изображения микротекста в высоком разрешении (1000 ppi) с изображением того же текста, полученного с помощью полностраничного считывателя (400 ppi)

- **Элементы, внешний вид которых зависит от индивидуальной обработки.** Некоторые элементы потенциально не подходят для автоматизированной аутентификации, поскольку они могут существенно изменить внешний вид документа, т. е. в зависимости от расположения страницы считывателя документа содержание фактического изображения может в определенной степени отличаться. В качестве примера ниже приводятся два таких элемента:

  а) *Оконный элемент. В зависимости от расположения страницы данных и обложки в считывателе документа* через окно можно увидеть контент обложки, корпус считывателя, кончик пальца или отсутствие контента в окне (см. рис. С-10), что приводит к появлению отраженного света.

  Одностороннее окно на ID-карточках размера ID-1, т. е. оконный элемент, который можно увидеть только с лицевой стороны, более подходит для автоматизированной аутентификации, поскольку на рисунке С-10 контент окна не изменяется и не препятствует процессу проверки на оборотной стороне каточки.

b) *Прозрачный лист, накладываемый на всю страницу.* В процессе захвата изображения наличие (или отсутствие) таких листов, может привести к получению различных результатов (см. рис. C-11).

Трудности, связанные с использованием этих элементов, можно преодолеть посредством надлежащей подготовки операторов (в случае проверки документов человеком) или подготовки руководств для пользователей (в случае использования автоматизированных систем пограничного контроля).

- **Дополнительные страницы для вклейки виз.** Паспорта, формат которых изменяется посредством внесения в них дополнительных страниц для вклейки виз, могут стать слишком объемными для геометрии, предусмотренной обычными полностраничными считывателями.

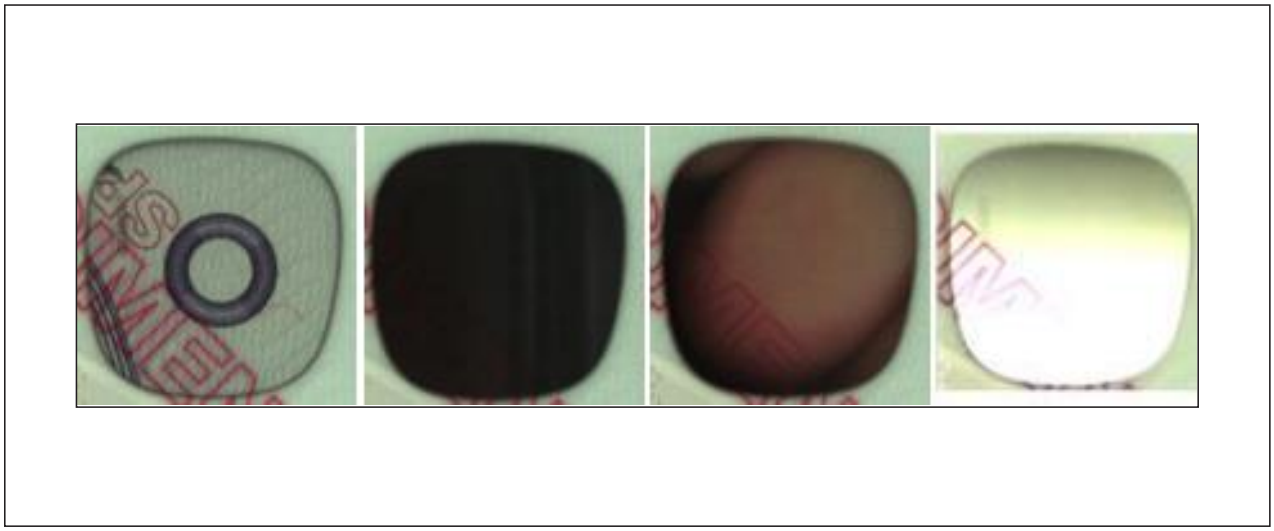

Рис. C-10. Паспорт (SWE, P, 1, 2012). Оконный элемент с изменяющимся контентом; слева направо: внутренняя часть лицевой стороны обложки, корпус считывателя, кончик пальца, блик, возникающий в результате отражения света

Рис. C-11. Паспорт (BEL, P, 1, 2008). Слева: страница данных обычного исполнения; справа: страница данных с наложением прозрачного листа для проведения визуальной проверки

С.4.2 Изготовитель полностраничных считывающих устройств

Надежность процесса аутентификации зависит не только от функциональных возможностей полностраничного считывателя, используемого в этом процессе. Непосредственное влияние на качество изображений, обрабатываемых с помощью программных средств аутентификации, также оказывают практичность и простота использования применяемых полностраничных считывателей (см. раздел С.4.3) что, в свою очередь, автоматически сказывается на общем результате реализации процесса аутентификации. В процессе проектирования полностраничных считывателей следует учитывать общие рекомендации, приводимые в настоящем разделе:

B.1 **Гарантировать использование надлежащих длин волн светового спектра.** Регистрация изображений с использованием надлежащих длин волн является необходимым условием для проведения соответствующего анализа оптических элементов/свойств. Например, элемент, который, как предполагается, должен быть прозрачным в IR-свете, может стать видимым на IR-изображении, если захват произведен с использованием надлежащей длины волны соответствующего светового спектра. Это может привести к получению недостоверных наборов оперативных данных и, как следствие этого, к неправильной интерпретации результатов проверок оптических элементов. При регистрации изображений наборов оперативных данных необходимо использовать следующие длины волн соответствующих световых спектров:

- VI: спектральный диапазон 400–700 нм
- IR: длина волны в диапазоне 850–950 нм[13]
- UV: 365 нм

Несмотря на то, что некоторые считыватели паспортов обеспечивают возможность использования более коротких длин волн (например, 254 и 313 нм), эта технология широкого распространения пока не получила и в дальнейшем в рамках настоящего документа она не рассматривается.

B.2 **Гарантировать минимальное разрешение.** Качество набора оперативных данных, подлежащих обработке с помощью программных средств аутентификации, определяемое количеством пикселей на дюйм (сокращенно: ppi), оказывает непосредственное влияние на точность процесса аутентификации. Практический опыт свидетельствует о том, что минимальная разрешающая способность для наборов оперативных данных составляет 385 ppi [BSI-TR-03135], хотя для многих свойств защищенной печати предпочтительной является разрешающая способность при захвате изображения, составляющая 600 ppi и выше.

B.3 **Обеспечивать представление изображений в стандартных форматах.** Наборы оперативных данных предоставляются в наиболее широко используемых/обеспечиваемых форматах. В качестве примера можно использовать следующие форматы: BMP, JPG (включая JPG2000) и PNG.

B.4 **Обеспечивать захват изображения вплоть до размера ID-3.** Полностраничный считыватель должен обеспечивать возможность верификации МСПД всех размеров, предусмотренных документом Doc 9303. Поэтому зона захвата изображения должна быть приемлемой для документов вплоть до размера ID-3. Несмотря на то, что этот документ ориентирован на использование полностраничных считывателей, следует иметь в виду наличие сценариев применения, не требующих проведения верификации МСПД всех размеров, и полностраничный считыватель необходим лишь для сканирования документов конкретного размера (например, портативные устройства).

13. Это значение определено на основе рекомендаций, содержащихся в части 3 документа Doc 9303.

B.5 **Гарантировать захват всех областей с одинаковым качеством.** Полностраничный считыватель обеспечивает возможность захвата всей станицы данных с одинаковым качеством. Например, этого можно достичь посредством однородного освещения поверхности захвата.

B.6 **Гарантировать минимальное время реагирования и постоянную интенсивность.** Источник света, используемый для захвата изображения, должен обеспечивать минимальное время реагирования и постоянную интенсивность света, поскольку любое ухудшение параметров света в процессе аутентификации может привести к формированию наборов оперативных данных, не отвечающих установленным требованиям.

B.7 **Гарантировать постоянное качество изображения.** Источники света однотипных полностраничных считывателей, могут излучать свет, характеристики которого отличаются, что обусловлено отклонениями в процессе производства. Кроме того, с течением времени интенсивность источников света полностраничных считывателей может измениться. В этой связи функциональные возможности полностраничных считывателей должны обеспечивать компенсацию отклонений и, таким образом, поддерживать постоянное качество в течение всего периода эксплуатации независимо от конкретно используемого устройства. Ниже приводятся два примера, наглядно иллюстрирующие возможность реализации этой рекомендации:

a) Изготовитель предусматривает наличие функциональных возможностей для управления цветом и выполнения дополнительной калибровки (например, посредством таблицы поправок) и выполняет настройку полностраничного считывателя с учетом требований заказчика (например, яркость, время экспонирования).

b) Изготовитель оснащает считыватели встроенными датчиками, обеспечивающими возможность компенсации отклонений в автоматическом режиме.

B.8 **Обеспечивать возможность настройки времени экспонирования в UV-свете посредством программных средств аутентификации.** Зачастую для обеспечения оптимального освещения документов различных моделей требуется различное время экспонирования в UV-свете. В этом случае информация о времени облучения в UV-свете хранится в базе данных аутентификации. Поэтому полностраничный считыватель позволяет настраивать время экспонирования в UV-свете на основе информации о UV-настройках, хранящейся в базе данных аутентификации (см. п. D.8 раздела C.4.4.2).

B.9 **Обеспечивать возможность захвата нескольких UV-изображений.** Полностраничный считыватель должен обеспечивать возможность захвата нескольких изображений с различными настройками времени экспозиции, например, для комбинации UV-элементов, обеспечивающей высокую контрастность при люминесценции (например, высокодинамичный диапазон).

B.10 **Обеспечивать возможность получения безбликовых изображений.** На полученном изображении могут появляться блики, которые, зачастую, охватывают биографические данные или элементы защиты страницы данных. Поэтому на изображениях, получаемых с помощью полностраничных считывателей, должно быть как можно меньше бликов. Этого можно достичь за счет захвата нескольких изображений, видимых в белом свете под различными углами, или посредством использования рассеянного освещения.

B.11 **Предусматривать наличие прижимного механизма для плоского размещения документа в зоне захвата.** Как отмечалось ранее, удобство использования полностраничных считывателей оказывает непосредственное влияние на эффективность и скорость процесса аутентификации. Поэтому в полностраничном считывателе должны быть предусмотрены механические устройства для плоского прижимание документа к окну, что обеспечивает возможность надлежащего считывания информации, содержащейся на страницах документа.

B.12 **Обеспечить возможность выполнения операций одной рукой.** Кроме того, следует обеспечить возможность использование считывателя одной рукой, причем процесс считывания должен быть симметричным, позволяющим эксплуатировать считыватель праворукими и леворукими пользователями.

B.13 **Обеспечивать предоставление интерактивного руководства пользователя.** Наличие интерактивного руководства пользователя не только повышает степень удобства использования операторами считывателей документов, но также помогает существенно сократить продолжительность процесса аутентификации в целом. Особую роль наличие руководства пользователя играет на автоматизированных контрольно-пропускных пунктах пограничного контроля, где, как правило, используется принцип самообслуживания. В противоположность стационарным пунктам проверки документов владельцы документов самостоятельно используют аппаратные средства аутентификации. В этой связи считыватель документов должен располагать возможностью предоставить интерактивное руководство пользователя. Это требование может быть реализовано посредством, например, прямого предоставления информации о ходе захвата изображения документа, размещенного на поверхности захвата (например, использование метафор при работе со сканнером). В этом случае у пользователя имеется прямая обратная связь, и он может более оперативно получать информацию о том, правильно ли он разместил документ в считывателе документов.

B.14 **Обеспечивать наличие аппаратных средств с высокой степенью отказоустойчивости.** В зависимости от сценария развертывания оборудования полностраничные считыватели подвергаются воздействию ряда внешних условий (неправильное обслуживание, влажность и т. д.). С течением времени наличие этих внешних условий может в той или иной степени привести к повреждению основных компонентов (например, появление царапин на поверхности захвата) полностраничного считывателя, что ускоряет процесс износа или даже приводит к поломке устройства. В этой связи в полностраничных считывателях рекомендуется использовать отказоустойчивые компоненты аппаратных средств.

C.4.3 Изготовитель программных средств аутентификации

Приводимые ниже предложения основаны на технических рекомендациях [BSI-TR-03135] Федерального управления информационной безопасности (BSI), поскольку в настоящее время только оно обеспечивает выработку решений для государственного сектора в этой области. В соответствии с этими рекомендациями настоятельно рекомендуется внедрять программные средства аутентификации. Последующие рекомендации следует рассматривать в качестве положений, дополняющих документ [BSI-TR-03135].

Просьба рассмотреть приводимые ниже технические рекомендации, касающиеся программных средств аутентификации:

C.1 **Обеспечивать возможность обработки предварительно записанных изображений.** Программные средства аутентификации также работают без аппаратных средств и должны обеспечивать возможность обработки предварительно записанных изображений (минимальные требования к изображениям приводятся в пп. B.1, B.2 и B.3 раздела C.4.2). Особое значение эта функциональная возможность имеет для процессов автоматизированной оценки. Однако необходимо исключить применение программных средств аутентификации для обработки заранее записанных изображений в процессе выполнения основных производственных операций, поскольку такой подход может быть использован в качестве вектора атаки. В этой связи реализация интерфейса, применяемого для обработки заранее записанных изображений, должна ограничиваться конкретными конфигурациями (например, подготовка к проведению оценки).

C.2 **Обеспечивать возможность обработки изображений из различных аппаратных источников.** Программные средства обеспечивают возможность обработки изображений, полученных, как минимум, от двух полностраничных считывателей без ухудшения результатов верификации. Поэтому изготовитель программных средств аутентификации предоставляет спецификацию с описанием свойств изображений, направляемых для обработки с помощью программных средств (цветовое пространство, контраст и т. д).

C.3 **Абстрагировать GUI (графический интерфейс пользователя) от программных и аппаратных средств аутентификации.** В большинстве случаев процесс оптической аутентификации МСПД сопровождается электронной проверкой МСПД и биометрической верификацией изображения лица владельца документа и, возможно, отпечатка пальца. Кроме того, должны выполняться проверки анкетных данных, например с использованием Шенгенской информационной системы (SIS). В этой связи между GUI и конкретными компонентами программных и аппаратных средств, необходимых для проведения проверок документов, биометрической информации и анкетных данных, рекомендуется использовать уровень абстракции. В этом случае обеспечивается независимость GUI о этих компонентов. Более того, упомянутые компоненты можно легко переключить без изменения GUI.

В последующих разделах рекомендации, сделанные для изготовителей программной продукции, структурированы в соответствии с операциями, выполняемыми в процессе аутентификации. Документ необходимо опознать (см. раздел C.4.3.1), идентифицировать (см. раздел C.4.3.2) и, впоследствии, верифицировать (см. раздел C.4.3.3). Более того, процесс в целом должен быть визуализирован (см. раздел C.4.3.4) и задокументирован с использованием соответствующих механизмов регистрации (см. раздел C.4.3.5).

C.4.3.1 Опознавание документа

В отношении распознавания документов, размещаемых на поверхности считывателя, даются следующие рекомендации:

C.4 **Обеспечивать возможность распознавания документа в автоматическом или ручном режиме.** Программные средства аутентификации обеспечивают механизмы инициирования распознавания документа в автоматическом или ручном режиме. Возможность ручного инициирования особенно важна в тех случаях, когда система распознавания документов в автоматическом режиме работает не надлежащим образом.

C.5 **Обеспечивать возможность компенсации углового смещения и, соответственно, кадрирования считанной страницы данных.** Процесс захвата изображения начинается автоматически после размещения полной страницы личных данных на поверхности захвата. Программные средства аутентификации позволяют компенсировать возможное угловое смещение и автоматически выровнять изображение. Кроме того, в процессе аутентификации выполняется кадрирование считанной страницы данных для последующей обработки.

C.6 **Обеспечивать распознавание документов на основе имеющихся оптических элементов.** Присутствие документа распознается лишь на основе использования их оптических свойств. Процесс распознавания реализуется оптическим способом даже в том случае, когда предполагаемый чип отсутствует или функционирует ненадлежащим образом (см. раздел C.1.3).

С.4.3.2 Идентификация

Необходимым предварительным условием для верификации документа является правильная идентификация его модели. В отношении идентификации набора оперативных данных сделаны следующие рекомендации:

С.7 **Идентифицировать модель документа.** Необходимо идентифицировать модель документа независимо от применяемого метода, при том условии, что применяемый метод гарантирует правильную идентификацию модели документа. Наиболее распространенными методами, используемыми для идентификации модели документа, являются МСЗ (включая анализ рисунка) или только анализ рисунка.

С.8 **Обеспечивать возможность оперативной идентификации посредством МСЗ.** Если для идентификации модели МСЗ используется в качестве основного источника исходных данных, то программные средства аутентификации должны использовать методы и маршруты, обеспечивающие возможность оперативной реализации процесса идентификации. Ниже приводятся два примера, иллюстрирующие порядок возможного выполнения этих рекомендаций:

a) для считывания информации МСЗ и определения модели документа следует начинать с захвата IR-изображения;

b) поскольку формирование изображения с полным разрешением может потребовать много времени, оперативный захват IR-изображения для проведения своевременного анализа МСЗ можно выполнить с разрешением меньшим минимально рекомендуемого для IR-изображения, используемого в целях идентификации.

С.9 **Обеспечивать наличие резервного средства, если в IR-свете МСЗ считыванию не поддается.** Должна обеспечиваться однозначная идентификация модели документа с использованием всех средств, если сам документ позволяет сделать это. Даже в том случае, когда в IR-свете МСЗ считыванию не поддается (требованиям ИКАО не соответствует), документ должен идентифицироваться правильно. Поэтому изготовитель программных средств должен обеспечивать возможность реализации резервных решений, таких как оптическое распознавание знаков (OCR) в VI-изображении для проведения анализа МСЗ, если печать МСЗ производилась без использования чернил, поглощающих IR.

С.10 **Предоставлять однозначную информацию о модели документа.** Изготовитель программных средств должен представлять однозначную ссылку на модель документа, обеспечивающую доступ к набору аутентификационных данных этой модели документа, содержащихся в базе данных аутентификации.

С.11 **Обеспечивать возможность частичной идентификации.** Программные средства аутентификации должны обеспечивать возможность управления конфигурацией процесса частичной аутентификации в целях существенного уменьшения количества случаев ложной неудавшейся идентификации. Тем не менее, оценка результатов частичной идентификации требует взаимодействия с оператором и наличия специальных знаний в области МСПД с целью ручного выбора правильной модели документа, поэтому для каждого сценария такой вид идентификации не подходит, например для контрольно-пропускных пунктов автоматических систем пограничного контроля (АВС).

С.12 **Обеспечивать возможность ручной идентификации.** Система должна обеспечивать возможность полностью ручного выбора модели документа вместо автоматизированного процесса и/или аннулирования выбора, сделанного компьютером, в том случае, когда реализуемый системой автоматизированный процесс дает сбой. Более того, система должна обеспечивать возможность

ручной идентификации, если частичную идентификацию выполнить нельзя. Ручная идентификация требует взаимодействия с оператором и наличия специальных знаний в области МСПД, поэтому для каждого сценария она не подходит (например, в рамках АВС ее использовать нецелесообразно).

С.13 **Обеспечивать двустороннюю идентификацию ID- карточек.** Документы размера ID-1 являются особенными в том плане, что МСЗ расположена не на странице личных данных (где размещено изображение лица). Однако ID-карточки размера ID-1 можно помещать в полностраничный считыватель любой стороной. В этой связи документы размера ID-1 должны поддаваться идентификации с любой стороны (см. рекомендацию А.4 в разделе С.4.1.1).

С.14 **Обеспечивать возможность идентификации образцов документов.** Программные средства аутентификации должны также обеспечивать возможность идентификации образцов или опытных экземпляров документов и соответствующим образом информировать оператора без нарушения процесса аутентификации (см. рекомендацию А.9 в разделе С.4.1.1).

Рекомендации, касающиеся визуализации процедуры идентификации в графическом интерфейсе пользователя, приводится в разделе С.4.3.4.

С.4.3.3 Верификация

Рекомендации в отношении верификации документов приводятся ниже:

С.15 **Выполнять минимальное количество спектрально-селективных проверок.** Спектрально-селективные проверки должны выполняться для проверки поглощающих, отражающих или люминесцентных реакций набора оперативных данных. Даже при отсутствии возможности идентификации документа необходимо выполнить следующие проверки:

a) (IR, AB, MR): эта процедура проверки, известная как B900-тест, может быть выполнена без выбора модели документа;

b) (UV, BR, FU): с некоторыми ограничениями в отношении точности эту проверку можно также выполнить на предмет контроля неидентифицированных комплектов оперативных данных.

В случае идентификации модели документа в дополнение к вышеупомянутым выполняются следующие проверки (т. е. проверка оптически противоположного свойства):

c) (IR, TR, *ZZ*): по крайней мере выполняется одна проверка на предмет изучения дополнительного свойства "прозрачный в IR-свете" по сравнению с (IR, AB, MR);

d) (UV, LU, *ZZ*): по крайней мере выполняется одна проверка на предмет изучения дополнительного свойства "люминесцентный в IR-свете" по сравнению с (UV, BR, FU).

С.16 **Выполнять проверку соответствия МСЗ.** Помимо минимального количества спектрально-селективных проверок необходимо проводить проверки достоверности (например, на предмет выявления ошибок в МСЗ, трехбуквенном коде ИКАО) с использованием всех документов для получения гарантий обеспечения минимального уровня защиты, включая случай неидентификации.

С.17 **Выполнять проверки во всех категориях.** Программные средства аутентификации выполняют регулярные проверки во всех трех категориях (материал, способ печати и метод эмиссии) и охватывает изображения, получаемые с помощью всех трех источников света (см. рекомендацию А.3 в разделе С.4.1.1, предназначенную для разработчиков документов).

С.18 **Выполнять проверку на наличие чипа.** Если в конкретной модели документа предполагается наличие RF-чипа, но он не работает или, как представляется, отсутствует, то это, в дополнение к результатам проверки оптических элементов, однозначно должно привести к выдаче предупреждения (см. раздел С.1.3).

С.19 **Выполнять проверку динамических рисунков.** Рекомендуется обеспечить наличие алгоритмов для сравнения динамических рисунков (например, фотография, подпись). Например, изображение лица можно сравнить с дополнительным изображением лица, размещенным на странице данных (см. рис. С-12 и рекомендацию А.7 в разделе С.4.1.1, предназначенную для разработчиков документов).

Рис. С-12. Паспорт (EST, P, 1, 2013). Верификация изображения лица в видимом свете и его сравнение с изображением лица, напечатанном чернилами, люминесцирующими в UV-свете

С.20 **При необходимости объединять процедуры проверок.** Некоторые элементы можно проверить посредством использования различных процедур. Например, элементы, которые по-разному реагируют на воздействие различных источников света, выполняют функцию источника исходных данных для проведения отдельных проверок (см. рекомендацию А.5 в разделе С.4.1.1, предназначенную для разработчиков документов). В этой связи рекомендуется логически объединять результаты таких проверок или оценочные результаты посредством функции принятия решений. Например, результатом комбинированной проверки может стать принятие положительного решения даже в том случае, когда количественный показатель результатов будет несколько ниже своего порогового значения.

С.21 **Выполнять контроль избыточным кодом в нескольких позициях.** В отношении элементов, неоднократно используемых в документе, необходимо также выполнять соответствующую процедуру проверки в нескольких позициях с использованием наборов оперативных данных. Например, для модели документа (D, P, 1, 2007), представленного на рис. С-13, символическое изображение орла в UV-свете можно проверить в нескольких позициях. Процедура проверок, выполняемая в нескольких позициях, называется процедурой контроля избыточным кодом.

Помимо неоднократного использования одного элемента статистические данные свидетельствуют о том, что одни элементы в большей степени подвергаются подделке, чем другие. Например, во многих случаях лица, занимающиеся фальсификацией, изменяют дату окончания срока действия или заменяют изображение лица. Поэтому рекомендуется выполнять проверки, обеспечивающие возможность с резервированием обнаруживать атаки на эти "конфиденциальные" элементы.

С.22 **Выполнять контроль избыточным кодом элементов, приобретающих в UV-свете различные цвета.** Проверку избыточным кодом рекомендуется также выполнять в отношении элементов, которые в UV-свете приобретают на документе различные цвета (см. рекомендацию А.6 и рис. С-5 в разделе С.4.1.1, предназначенные для разработчиков документов).

С.23 **Сопоставлять и проверять информацию обеих страниц ID-карточки.** Результаты сканирования второй страницы автоматически увязывается с результатами предыдущего сканированием, если эти страницы являются страницами одного и того же ID-документа. Кроме того, рекомендуется проверять обе стороны документов размера ID-1, что позволит получить общий результат верификации для обеих сторон и в максимальной степени увеличить количество оптических элементов, используемых для аутентификации документов (см. рекомендацию А.4 в разделе С.4.1.1, предназначенную для разработчиков документов).

С.24 **Обеспечивать возможность проведения перекрестной проверки личных данных, содержащихся на нескольких страницах.** Личные данные владельца документа должны быть идентичными, независимо от того, на какой странице они находятся. Например, предполагается, что личные данные на странице данных паспорта должны быть идентичны личным данным на потенциально существующей визе. В этой связи рекомендуется выполнять перекрестные проверки нескольких страниц, если, например, при этом ожидается, что персонализированный контент должен быть идентичным/дублированным.

Рис. С-13. Дублирующая верификация рисунка

C.25 **Выполнять процедуры проверки с учетом их значимости.** Не всегда необходимо или целесообразно выполнять полный набор проверок лишь потому, что это технически возможно сделать с использованием оперативного набора данных. Более эффективный подход будет заключаться в проведении оценки уместности этих проверок в увязке с процессом верификации. По сравнению с другими процедурами проверок некоторые методика позволяют получить более полезные результаты и информацию, обеспечивающие возможность проведения более точного анализа результатов верификации. В этой связи:

a) проверки следует проводить с учетом их уместности/значимости, а результаты должны немедленно отображаться в графическом интерфейсе пользователя (см. раздел C.4.3.4 "Визуализация");

b) результаты проверок должны комбинироваться посредством функции принятия решений, что отличается от выполнения простой логической схемы И-комбинации (т. е. использование взвешенных результатов проверок). Функции принятия решений должны вноситься в каталог XML (см. рекомендацию C.46 в разделе C.4.3.5 "Регистрация").

C.26 **Рассматривать вопрос об отклонении параметров элементов.** С течением времени элементы защиты могут изменяться, что обусловлено износом МСПД в процессе использования. Например, в UV-свете некоторые цвета могут ухудшиться, поэтому в течение срока действия МСПД эти элементы должны постоянно и надежно проверяться. В этой связи следует рассматривать вопрос о допусках для их использования в ходе проверок.

C.27 **Выявлять характерные признаки злонамеренного вмешательства.** Помимо проведения верификации программные средства аутентификации должны обеспечивать возможность выявления признаков злонамеренного вмешательства, таких как "повреждение бумаги", "следы порезов", "замена фотографии" или "складки на ламинатном покрытии", если условия освещения позволяют сделать это. Методику реализации процедуры проверок можно также применять при проведении проверок на предмет обнаружения подделок.

Рекомендации относительно визуализации процедур верификации на графическом интерфейсе пользователя приводятся в следующем разделе.

C.4.3.4 Визуализация

Визуализация результатов аутентификации представляет собой процесс, посредством которого пользователю системы аутентификации предоставляется визуальная обратная связь и информация о результатах процесса аутентификации. Визуализация должна посредством графического интерфейса пользователя (GUI).

GUI, используемый для визуализации результатов оптических проверок, должен обеспечивать предоставление пользователю только наиболее актуальной информации, позволяющей с первого взгляда выявить несоответствие. Ниже эта информация подразделяется на так называемые "область представления сводной информации о реализации процесса" (см. C.29), "область просмотра результатов оптического исследования" (см. C.30) и "область представления результатов углубленного оптического исследования", содержащую более подробную информацию (см. C.35).

Рекомендации, касающиеся выбора необходимой информации и ее представления в компактном виде, приводятся ниже.

C.28 **Отображать информацию обо всех проверках документов посредством одного GUI.** GUI может входить в состав поставляемых программных средств аутентификации или предоставляться и использоваться в рамках отдельного уровня абстракции. Независимо от этого рекомендуется, чтобы один GUI обеспечивал отображение результатов всех типов выполненных проверок (электронных, биометрических, оптических и проверок анкетных данных). Это значительно снижает нагрузку на оператора системы и облегчает проведение оценки результатов, что обусловлено более совершенным представлением общих сведений о процессе. Более того, особое внимание следует уделять отклонениям от нормы и несоответствиям (см. рекомендации C.41–C.45).

C.29 **Всегда показывать область представления *сводной информации о реализации процесса.*** В этой области следует отображать информацию об общих результатах оптической аутентификации, которая должна представляться пользователям на входной странице (наглядный пример информации GUI, предоставляемой на стационарном контрольно-пропускном пункте пограничного контроля, приводится на рис. C-14). Эта область должна всегда находиться в поле зрения пользователя независимо от выбора дополнительных элементов, обусловленных конкретными результатами верификации. В области представления сводной информации о процессе должен показываться один общий результат оптической аутентификации, сопровождаемой символом светофора. Более того, в этой области должно отображаться обрезанное изображение лица на странице данных рядом с изображением лица, хранимым в памяти чипа, если он имеется.

C.30 **Обеспечивать отображение области просмотра результатов оптического исследования на начальной странице.** В этой области показываются общие результаты оптических проверок, которые следует выводить на начальную страницу оператора.

a) В этой области должна содержаться следующая информация (см. рис. C-14):

- По умолчанию VI-изображение документа (в видимом свете). Оператор должен иметь возможность изменять изображения, принятые по умолчанию, на изображения в IR или UV-свете, в зависимости от конкретных требований.

- личные данные владельца документа, содержащиеся в MC3: фамилия, имя, дата рождения, пол, гражданство и факультативные данные.

- данные документа: тип документа, номер документа, государство или организация выдачи, дата истечения срока действия и факультативные данные.

Рис. С-14. Пример начальной страницы GUI на стационарном контрольно-пропускном пункте пограничного контроля

- Извлеченные данные MCЗ, позволяющие сравнить их с данными MCЗ, напечатанными в документе.

- Кнопку, обеспечивающую возможность ручного инициирования процесса считывания документа.

- Обрезанное изображение лица на странице данных рядом с изображением лица, хранимым на чипе, если он имеется (см. раздел С.1.3) для оперативного обнаружения замены фотографии.

b) Кроме того, в области просмотра результатов оптического исследования рекомендуется отображать следующую информацию:

- возраст владельца, а также остающийся срок действия документа. Эту информацию оператор моет оценить без особых усилий и более оперативно, чем данные, содержащиеся в MCЗ.

C.31 **Выбирать более подробную информацию одним нажатием кнопки мыши.** В области просмотра результатов оптического исследования оператор лишь одним нажатием кнопки мыши должен получать доступ к дополнительной странице, содержащей более подробную информацию относительно оптической верификации: *область представления результатов углубленного оптического исследования* (см. C.35). Например, на образце GUI, представленном на рис. C-14, более подробную информацию можно извлечь, выбрав область "Данные документа".

C.32 **Представлять результаты с использованием сигналов светофора.** Согласно документу [BSI-TR-03135] результаты реализации процессов оптической проверки должны отображаться с использованием сигналов светофора (например, красный/зеленый/желтый/серый). В дополнение к цвету в рамках системы светофора должны использоваться однозначные символы, отражающие результаты проверки (например, галочка или перекрестие). Это особенно важно для пользователей, страдающих красно-зеленой цветовой слепотой. Более того, структура представления должна быть одинаковой для всех областей GUI (например, отрицательные результаты всегда показываются одним и тем же символом и цветом).

C.33 **Представлять результаты в соответствии с требованиями документов [BSI-TR-03135].** Система светофора должна обеспечивать согласованное представление информации, отражающей следующие результаты верификации: **положительный**, **отрицательный**, **неопределенный** или верификация **не обеспечивается/не выполняется,** как определено в документе [BSI-TR-03135]. Таблица C-2 иллюстрирует используемый в настоящем документе общий порядок отображения информации о результатах проверки. Методика ее представления основана на положениях документа [BSI-TR-03135] и ее следует использовать в ходе практического применения GUI.

Таблица C-2. Представление информации посредством системы светофора

Результат верификации	*Цвет сигнала светофора*
Положительный	Зеленый
Отрицательный	Красный
Неопределенный	Желтый
Не обеспечивается / не выполняется	Серый
Прекращена	Черный

C.34 **Отображать результаты в упрощенном виде.** В качестве альтернативы в рамках системы светофора можно использовать упрощенное представление, предусматривающее применение только зеленого и красного цветов. Как показано в таблице C-3, зеленый цвет может использоваться для отображения положительного результата верификации, а красный цвет для отображения любого другого результата.

Таблица С-3. Представление информации в упрощенном виде с использованием системы светофора

Результат верификации	*Цвет светофора*
Положительный	Зеленый
Отрицательный	Красный
Неопределенный	
Не обеспечена / не выполнена	Серый
Прекращена	

Дополнительное представление информации в упрощенном виде будет заключаться в отнесении представленных в таблице С-3 последних четырех результатов верификации к категории "красный".

С.35 **Отображать более подробную информацию в специально предназначенной для этой цели *области представления результатов углубленного оптического исследования.*** Просмотр более подробных дополнительных данных возможен лишь при расширении области, содержащей дополнительную информацию относительно различных процессов и результатов оптической аутентификации. Цель заключается в предоставлении пользователю информации, необходимой для выполнения дополнительного анализа, если в этом имеется необходимость.

а) В области представления результатов углубленного оптического исследования должна содержаться следующая информация (см. пример на рис. С-15):

- изображение документа в VI, IR и UV-свете. Эти три изображения должны находиться рядом друг с другом.

- Специальный идентификатор модели документа, присваиваемый изготовителем программных средств аутентификации, если в общей форме отобразить идентификатор модели документа, предложенный в разделе С.2.1, не представляется возможным.

- Перечень выбранных процедур проверок с указанием их результатов посредством сигналов светофора. В контексте пограничного контроля сотрудник пограничного контроля должен рассматривать лишь наиболее важную верификационную информацию в форме, удобной для восприятия человеком. В этой связи результаты реализации общих процедур проверок объединяется в приводимые ниже три категории, описываемые простыми и понятными терминами:

  — Читаемость MCЗ в IR-свете: соответствующий сигнал светофора показывает результат реализации процедуры общей проверки (IR, AB, MR).

  — Яркость в UV-свете: соответствующий сигнал светофора показывает сводный результат реализации общей процедуры проверки (UV, BR, FU), (UV, BR, VZ), (UV, BR, PH) и (UV, BR, MR).

  — Проверка рисунка: соответствующий сигнал светофора показывает сводный результат реализации оставшихся общих процедур проверок, выполненных в отношении этого документа (см. раздел С.3).

- Кроме того, согласно документу [BSI-TR-03135] следует визуализировать результаты перечисленных ниже проверок с использованием сигналов светофора:

  — Соответствие MC3

  — Дата истечения срока действия

Рис. C-15. Наглядный пример области представления результатов углубленного оптического исследования

- Извлеченная MC3.

- В процессе аутентификации элементы, извлеченные из оптически считываемой MC3, сравниваются с элементами MC3, хранимыми в памяти чипа (если имеется). Элементы данных оптической MC3 должны отображаться совместно с результатом(ами) такого сравнения. Результат(ы) должен(ы) отображаться с использованием сигналов светофора, применявшихся в рамках GUI.

b) Кроме того, в области представления результатов углубленного оптического исследования рекомендуется отображать следующую информацию:

- Модель идентифицированного документа в форме, удобной для восприятия человеком, например, D 2007. В среде пользователей GUI применение предусмотренного документом [BSI-TR-03135] стандартного идентификатора модели документа может, по всей вероятности, вместо ясности внести больше неопределенности. Поэтому представление в GUI идентификатора модели должно основываться на наличии общей договоренности с оператором системы аутентификации.

- Элементы данных, извлеченные из оптически считываемой МСЗ, и элементы данных, извлеченные из чипа, должны отображаться рядом (см. раздел C.1.3).

C.36 **Обеспечивать предоставление рекомендаций пользователям в процессе считывания документов.** В процессе считывания документов пользователю следует рекомендовать не извлекать документ до окончания процесса считывания (см. рекомендацию B.13 в разделе C.4.2). Например, эту рекомендацию можно реализовать посредством вывода на дисплей в процессе считывания индикатора процесса. Эту рекомендацию можно поместить в области представления сводной информации о процессе.

C.37 **Обеспечивать отображение информации, содержащейся в центральных базах данных.** Если в процессе аутентификации требуется запросить систему ведения баз анкетных данных, то на странице отображения результатов оптической проверки можно представить информацию, извлеченную из этой системы, если она коррелируется с результатами оптической аутентификации, например, изображение лица, извлеченное из централизованной системы визовой информации (C-VIS).

C.38 **Обеспечивать однотипность структуры МСПД.** Для всех типов машиносчитываемых документов (например, паспорта, национальные идентификационные карточки, карточки, удостоверяющие вид на жительство и т. д.) структура GUI должна быть одинаковой. Например, информацию, полученную в процессе оптической аутентификации обеих сторон карточки размера ID-1, следует отображать аналогично информации, визуализирующей результаты верификации паспортов (одна область представления сводной информации о процессе, одна область просмотра результатов оптического исследования и одна область представления результатов углубленного оптического исследования).

C.39 **Оказывать содействие операторам в проведении многостраничной верификации.** Верификация обеих сторон документа размера ID-1 требует оказания содействия пользователю в интерактивном режиме. В отношении карточки, размещаемой на поверхности захвата, пользователь должен получить указание о том, что следующим этапом может стать представление второй страницы.

C.40 **Обеспечивать возможность сравнения контента паспорта и визы/электронного вида на жительство (eRP):**

a) *Оказывать содействие операторам в проведении многостраничной верификации.* При проведении верификации паспорта пользователя следует предупредить о том, что для пересечения границы владельцу паспорта необходимо иметь визу/eRP. Например, это предупреждение можно разместить в виде подсказки на странице обзора. Для пользователя такая подсказка должна означать, что возможно следующим этапом станет проверка визы/eRP в полностраничном считывателе.

b) *Обеспечивать наличие паспортной информации.* В процессе оптической аутентификации виз/eRP области обзора и результатов углубленного исследования, содержащие результаты аутентификации паспорта, должны находиться в состоянии готовности, что, при необходимости, обеспечивает возможность переключения на них.

c) *Обеспечивать возможность проведения сравнения в области сводной информации о процессе.* Помимо оптически захватываемого со страницы данных изображения лица на визе/eRP должно присутствовать изображение лица (см. пример на рис. С-16). Кроме того, должны быть показаны изображение лица владельца паспорта, хранимое на чипе (если имеется, см. раздел С.1.3), и изображение, полученное из системы запроса визовой информации (например, европейская VIS) или с чипа eRP (см. С.37).

d) *Обеспечивать возможность проведения сравнения в области представления результатов углубленного оптического исследования визы.* В процессе аутентификации такие элементы данных, как: фамилия, имя, дата рождения, пол, гражданство, извлеченные из оптической МСЗ визы, сравниваются с аналогичными элементами МСЗ страницы данных паспорта и/или чипа (см. раздел С.1.3). Элементы данных МСЗ визы должны отображаться совместно с результатом(ами) этого сравнения. Результат(ы) должен(ы) показываться с использованием системы светофора, к применявшейся в отношении остальных элементов GUI. В этой области должны также указываться возраст владельца документа и оставшийся срок действия визы, поскольку по сравнению с данными, содержащимися в МСЗ, это позволит оператору легко и более оперативно оценить эту информацию.

Рис. С-16. Наглядный пример сравнения паспорта и визы

Рекомендации, касающиеся отображения ошибок, приводятся ниже:

С.41 **Выделять только несоответствия.** В процессе аутентификации цветовое выделение необходимо использовать только для того, чтобы обратить внимание на наличие несоответствий (например, в случае проверки с отрицательным результатом, как показано на рис. С-14). Такой подход оказывает значительную помощь пользователю в оценке с первого взгляда наиболее актуальной информации, отображаемой с помощью GUI.

С.42 **Отображать ошибки в области сводной информации о процессе.** Если документ не является подлинным, то сигнал светофора, предназначенного для оптической аутентификации, должен показывать общий отрицательный результат. Если модель документа идентификации не поддается, то светофор, оценивающий общий результат оптической аутентификации, должен выдать предупреждение.

С.43 **Отображать ошибки в области просмотра результатов оптического исследования.** Если ошибки обусловлены оптическими отклонениями, их необходимо показывать следующим образом:

a) *Несоответствие спектрально-селективного свойства.* Если ошибка возникает в результате реализации процедуры спектрально-селективной проверки, то изображение в соответствующем спектре света должно отображаться в области оптических данных документа, а не представляться в виде стандартного VI-изображения (например, если (UV, BR, FU) не срабатывает, то должно показываться UV-изображение). Кроме того, область просмотра результатов оптического исследования должна ограничиваться рамкой красного цвета.

b) *МСЗ не соответствует.* Если ошибка обусловлена проверкой МСЗ на соответствие, то соответствующую часть извлеченной МСЗ, включая контрольную сумму, следует выделять красным цветом. Кроме того, соответствующие несовпадающие личные данные и область, содержащую личные данные, должны выделяться красным цветом (см. рис.С-17). Оператор должен иметь возможность вручную скорректировать МСЗ и посредством кнопки инициировать проведение повторной процедуры считывания.

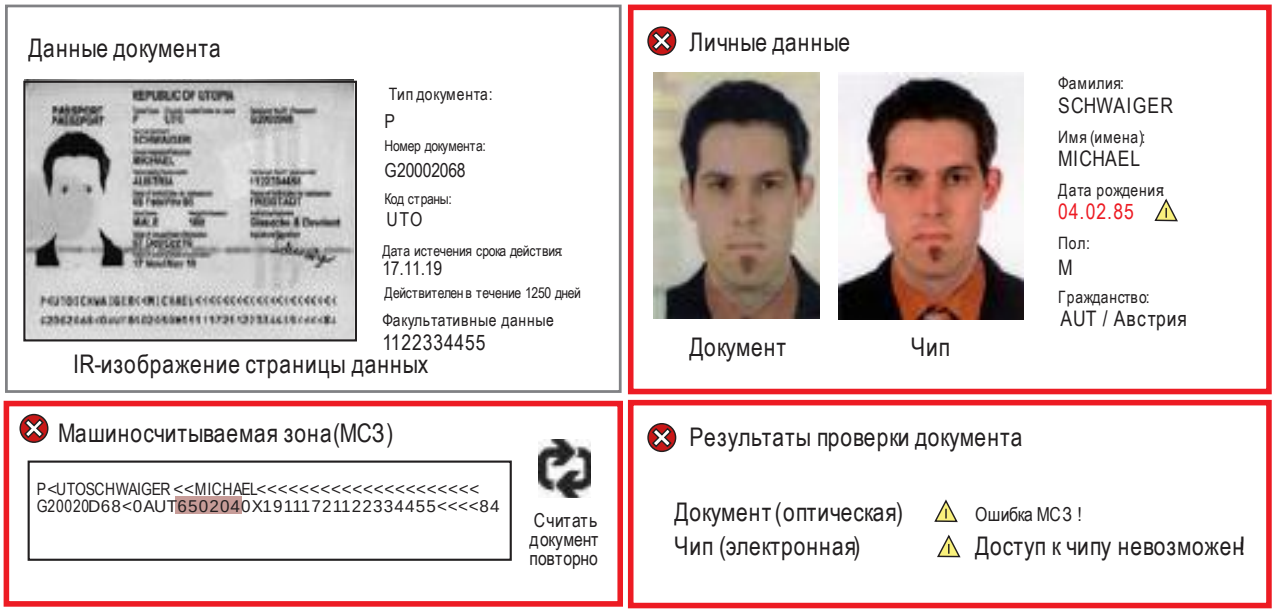

Рис. С-17. Наглядное представление визуализации ошибок. Несоответствие МСЗ

c) *Срок действия документа истек.* Если срок действия документа истек, то дату истечения срока действия следует выделить красным цветом.

d) *Чип не обнаружен.* Если в идентифицированном документе предполагается наличие электронного чипа, но обнаружить его нельзя (см. раздел С.1.3), то должно выдаваться предупреждение. Предупреждающий знак должен четко отличаться от символов светофора, используемых для отображения результатов проверки (например, предупреждающий знак в виде треугольника желтого цвета).

С.44 **Отображать ошибки в области представления результатов углубленного оптического исследования.** Если ошибки возникают в результате оптических несоответствий, то информацию о них следует отображать следующим образом:

a) *Документ не идентифицирован.* Если модель документа идентифицировать нельзя, то результатом реализации процесса идентификации модели документа должен стать предупреждающий знак. Предупреждающий знак должен четко отличаться от знаков светофора, используемых для отображения результатов проверки (например, предупреждающий знак в виде треугольника желтого цвета, см. рис. С-18). Предупреждающий текст должен размещаться рядом с предупреждающим знаком, например " Модель документа идентифицировать нельзя".

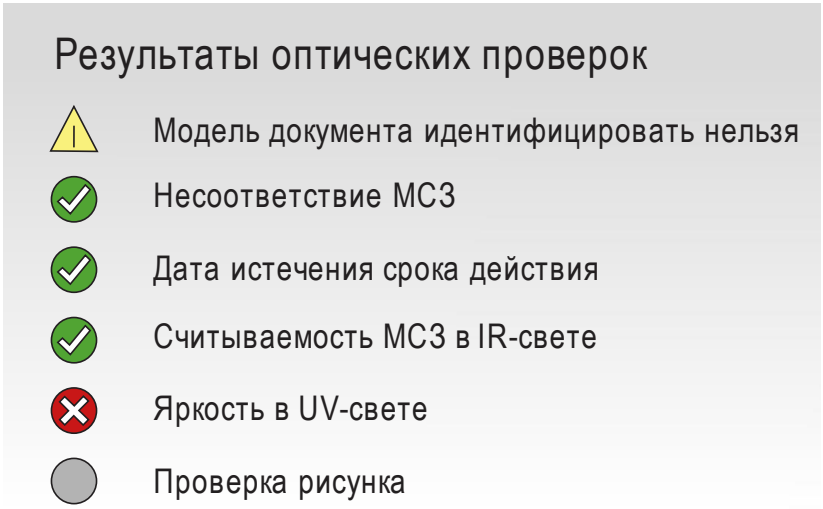

Рис. С-18. Наглядный пример визуализации ошибки. Модель документа и отрицательный результат верификационной проверки

b) *Отрицательный результат верификационной проверки.* В ходе каждой верификационной проверки, информация о которой выводится на страницу результатов углубленного исследования (см. рис. С-18), отрицательный результат проверки должен приводить к срабатыванию красного сигнала светофора. Соответствующие элементы неудовлетворительной проверки должны выделяться на соответствующем изображении, например, посредством красного прямоугольника, ограничивающего исследуемую зоны элементов (например, IR-изображение MC3 в связи с отрицательным индексом считываемости MC3 в IR-свете).

c) *Противоречивая информация чипа.* В отношении данных каждой МСЗ, которые не соответствуют данным оптической страницы и чипа (см. раздел С.1.3), несоответствующая пара данных должна выделяться красным цветом (и сопровождаться предупреждающим знаком, см. рис. С-19).

d) *Несоответствующая общая контрольная цифра.* Ошибки, касающиеся контрольной цифры (см. главу 4 "МСЗ" в части 3 документа Doc 9303), могут свидетельствовать о манипулировании контрольными цифрами, например внесение в МСЗ неправильной контрольной цифры с целью не допустить использования механизмов контроля доступа (например, базового контроля доступа (BAC)). В отношении каждой неудавшейся проверки оптической МСЗ полученная контрольная цифра соответствующего элемента МСЗ должна отображаться рядом с требуемой контрольной цифрой.

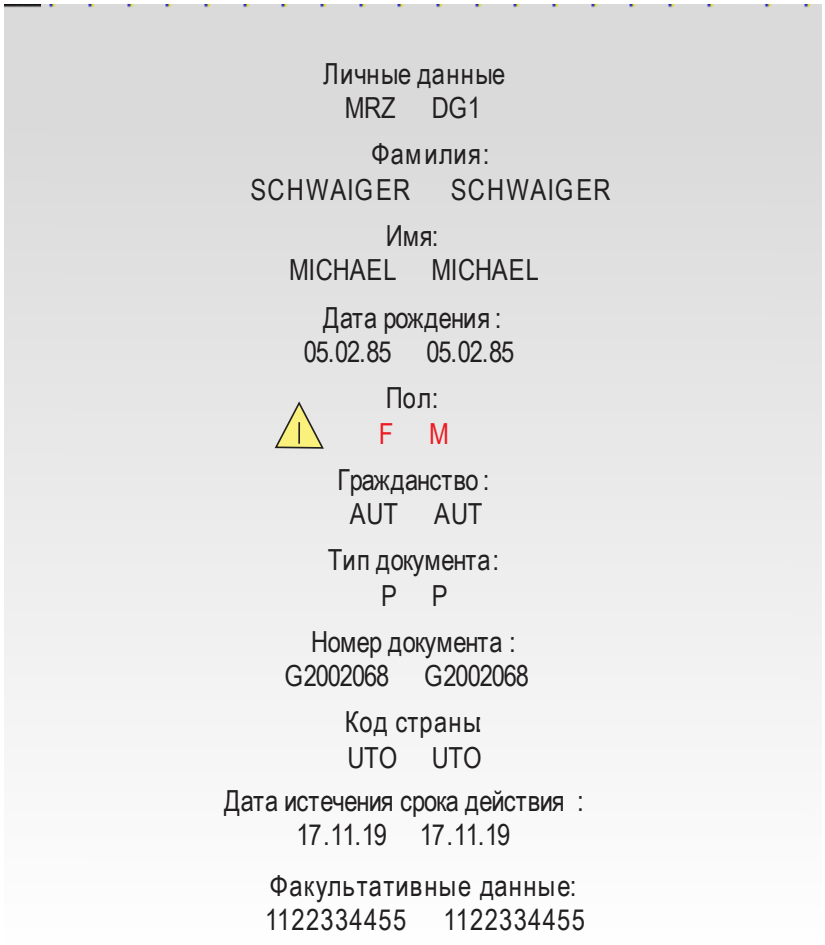

Рис. С-19. Наглядный пример визуализации ошибки. Данные МСЗ

С.45 **Отображать ошибки, возникающие при сравнении данных паспорта и визы/eRP.** Если хотя бы один из сопоставляемых показателей МСЗ паспорта и визы/eRP отличается, то информация об этом несоответствии должна отображаться следующим образом:

a) *Область обзора визы/eRP.* Сопоставляемые данные МСЗ (фамилия, имя, дата рождения, пол и гражданство) паспорта должны отображаться на странице обзора визы/eRP рядом с данными МСЗ визы/eRP. Каждая несоответствующая пара данных должна выделяться красным цветом и сопровождаться предупреждающим знаком (см. пример на рис. С-20).

Рис. С-20. Наглядный пример сравнения данных визы и паспорта

b) *Область просмотра результатов углубленной проверки данных визы/eRP.* Сопоставляемые элементы данных МСЗ, которые в визе/eRP и паспорте отличаются, следует отражать парами, выделять красным цветом и сопровождать предупреждающим знаком.

С.4.3.5 Регистрация

В отношении регистрации процесса автоматизированной оптической аутентификации применяются следующие рекомендации:

С.46 **Регистрацию XML файлов выполнять в соответствии с требованиями документа [BSI-TR-03135].** Регистрация должна выполняться в соответствии со схемами XML, определенными в документе [BSI-TR-03135], в котором также, помимо подробных оптических результатов, содержатся результаты электронной и комбинированной (оптической и электронной) верификации документа. Например, это обеспечивает возможность:

a) регистрации идентификатора общих процедур проверок, являющихся составным элементом специализированных процедур проверок (см. раздел С.3);

b) ввода процедур проверок в режиме молчания, т. е. проверка выполняется и ее результаты регистрируются, однако эти результаты проверки в общем результате процесса аутентификации не учитываются. Особое значение это имеет в случае проведения оценки новых процедур проверки, алгоритмов или пороговых значений.

Оператору может потребоваться дополнительная информация относительно спектрально-селективных проверок для ее использования при оценке и обновлении основной базы данных, что гарантирует последовательность и высокое качество данных в долгосрочной перспективе. Эта информация аналогична для всех документов конкретной модели документа; например для функции принятия решения, текстуальных пояснений относительно процедур проверок и секции переноса изображений из справочной базы данных. В этой связи изготовитель должен предоставить каталог XML в машиносчитываемой форме в соответствии со схемой XML, определенной в документе [BSI-TR-03135], в котором обобщается вся информация относительно спектрально-селективных проверок. Учитывая формат, каталог можно интегрировать в результаты оценки.

C.47 **Обеспечивать возможность регистрации факультативных данных изображений.** Схемы XML, определенные в документе [BSI-TR-03135], обеспечивают возможность, но не непосредственное регулирование, хранение обработанных комплектов операциыных данных и обрезанных изображений и отображение зоны поиска выполненных проверок. Программные средства аутентификации должны располагать возможностью хранения упомянутых данных изображений в структуре данных XML. Рекомендации для администратора текущих операций, касающиеся хранения данных изображений в соответствии с действующими правилами защиты данных, содержатся в разделе C.5.

C.48 **Предусматривать возможность обезличивания личных данных.** Программные средства должны предусматривать возможность обезличивания набора оперативных данных непосредственно после аутентификации с целью обеспечить их постоянное хранение для проведения дополнительного исследования. Рекомендации, касающиеся обезличивания, см. в разделе C.5.1.

C.4.4 Изготовитель базы данных аутентификации

Как отмечалось в разделах C.2.1 и C.2.2, в базе данных аутентификации содержится определенный набор процедур проверки для различных моделей документов. Она непосредственно взаимодействует с программными средствами аутентификации, которым эта база данных передает набор процедур проверки, соответствующих идентифицируемой модели документа. Учитывая создание новых моделей документов и постоянно возрастающее количество подделок, исключительно важно иметь в наличии содержащуюся в хорошем состоянии и гибкую базу данных аутентификации. В последующих разделах приводится сводная информация о рекомендациях в отношении баз данных, касающихся процесса обновления (см. раздел C.4.4.1), и способности к изменению конфигурации баз данных (см. раздел C.4.4.2).

C.4.4.1 Обновление баз данных

Приводимые ниже рекомендации, касающиеся процесса обновления, предназначены для изготовителей баз данных аутентификации:

D.1 **Обмениваться информацией относительно новых моделей документов или подделок.** Изготовитель баз данных аутентификации создает специализированный канал связи с администратором текущих операций в целях защищенной передачи пакетов информации о новых моделях документов, подлежащих внесению в базу данных. Изготовитель обменивается с администратором текущих операций информацией относительно новых моделей документов, используя один из перечисленных ниже методов:

a) *Обмен посредством передачи исходного образца.* В этом случае исходный образец новой модели документа или подделки должен предоставляться для определения и загрузки в базу данных соответствующего набора процедур проверки. Созданный канал связи и соответствующие процедуры должны учитывать национальное законодательство в области защиты данных (см. раздел С.5).

b) *Обмен посредством программных средств ввода данных.* В этом случае администратору текущих операций должны быть предоставлены программные средства ввода данных для формирования соответствующего комплекта оперативных данных о новых моделях документов и подделок. В этом наборе данных как минимум должно содержаться одно VI, UV и IR-изображение. В идеальном случае такие программные средства ввода данных должны обеспечивать возможность формирования нескольких изображений одного цветового спектра (аналогично фотографии с расширенным динамическим диапазоном). Набор данных передается изготовителю для определения соответствующего набора процедур проверки, подлежащего включению в следующую версию базы данных. Для этой цели изготовитель должен рекомендовать перечень приемлемых устройств ввода данных.

D.2 **Регулярно обновлять базу данных.** База данных аутентификации обеспечивает возможность регулярного запланированного обновления информации (минимум раз в три месяца). База данных аутентификации также позволяет вносить целевые изменения по специальному (срочному) запросу:

a) если изготовитель получил новую информацию относительно подлинных документов или подделок и в сотрудничестве с администратором текущих операций обновил документальную базу данных на основе этой информации (см. D.1 a), или

b) если оператор сформировал набор оперативных данных с использованием программных средств ввода данных (подлинный документ или подделки) и направил его изготовителю (см. D.1 b).

D.3 **Предоставлять скорректированные версии.** По умолчанию изготовитель базы данных аутентификации должен предоставлять оператору полные обновленные версии. Скорректированные версии должны также рассылаться в целях экономии времени и пропускной способности.

D.4 **Предоставлять достаточный объем документации, касающейся изменений.** При обновлении базы данных изготовитель баз данных аутентификации должен предоставлять достаточный объем документации, касающейся изменений, внесенных в базу данных.

С.4.4.2 Содержание и способность к изменению конфигурации базы данных

В настоящем разделе приводится предназначенный для изготовителей баз данных аутентификации перечень рекомендаций, касающихся содержания и способности к изменению конфигурации баз данных:

D.5 **Предоставлять сокращенный контент.** Базы данных аутентификации должны выпускаться с различным объемом данных и поддаваться настройке с учетом различных сценариев. Например, масштаб коммерческих сценариев носит ограниченный характер, а тип проверяемых документов, как правило, является очень специфичным (например, аутентификация документов в компаниях по сдаче автомобилей в аренду). В этой связи рекомендуется предоставлять базы данных аутентификации, отвечающие конкретным потребностям коммерческих сценариев, посредством понижения степени их сложности. Предоставляя базы данных с сокращенным контентом, изготовитель обеспечивает гарантии сохранения их экономической эффективности и простоты интеграции в различные установки.

D.6 **Распределять проверки с учетом уровня их значимости.** Проверки должны распределяться с учетом уровня значимости, что позволяет программным средствам аутентификации выполнять проверки в порядке их значимости (см. рекомендацию С.25 a), предназначенную для изготовителей программных средств аутентификации, о которой говорится в разделе С.4.3).

D.7 **Предусматривать возможность использования различных эксплуатационных режимов.** Различные сценарии использования требуют обеспечения различных уровней защиты в части, касающейся признания или отклонения документов. Например, на стационарных контрольно-пропускных пунктах пограничного контроля особое внимание уделяется обеспечению высокого уровня безопасности, а в рамках коммерческих сценариев акцент, как правило, делается на создание бóльших удобств для владельца документа. Поэтому база данных аутентификации должна, как минимум, обеспечивать два различных эксплуатационных режима: режим обеспечения высокого уровня безопасности и режим обеспечения максимального уровня удобств.

D.8 **Предусматривать предоставление информации о длительности экспонирования конкретной модели документа в UV-свете.** Как отмечалось в разделе С.4.2, зачастую различные модели документов требуют различной длительности экспонирования в UV-свете. Например, для надлежащей проверки конкретных элементов в UV-свете некоторые модели документов требуют более длительного UV-облучения. Поэтому в базе данных аутентификации должна содержаться информация относительно настроек времени экспонирования, необходимого для соответствующих моделей документов, с тем чтобы программные средства аутентификации могли автоматически выбирать соответствующую конфигурацию полностраничного считывателя (см. п. В.8 раздела С.4.2).

D.9 **Оказывать поддержку использованию программ серверной установки.** Рекомендуется поставлять базу данных аутентификации, способную также функционировать в рамках программы серверной установки. В этом случае различные программные средства аутентификации смогут получать доступ к единой базе данных аутентификации. Кроме того, две или несколько баз данных аутентификации смогут работать в качестве кластера, доступного для нескольких программных продуктов аутентификации.

С.4.5 Изготовитель справочной базы данных

Несмотря на то, что справочная база данных не является непосредственной частью системы аутентификации (см. раздел С.2.1), ее можно использовать в качестве дополнительного источника информации, если на основе автоматизированной аутентификации четко определить подлинность документа не представляется возможным. В этом случае справочная база данных способна оказать поддержку оператору посредством предоставления подробной информации относительно соответствующей модели документа, например, высококачественное изображение элементов, текстуальные пояснения и информацию о характерных признаках подделки (цель которой заключается в проведении контроля второй линии/исследования с привлечением вспомогательного подразделения). Примером справочной базы данных, предоставляемой Европейским союзом, является система FADO (интерактивная информационная система, содержащая данные о фальшивых и подлинных документах). Общеизвестным аналогом FADO является система PRADO [14] (интерактивный государственный реестр подлинных документов).

В случае использования изготовителем справочной базы данных необходимо рассмотреть ряд практических соображений. В настоящем разделе эти соображения рассматриваются в виде рекомендаций:

E.1 **Предусматривать возможность автоматизированного получения выходных данных.** Справочная база данных получает и обрабатывает однозначную ссылку на модель документа

14. http://prado.consilium.europa.eu/en/homeindex.html.

в качестве входной информации процесса идентификации. В качестве выходных данных она должна также предоставлять набор справочных данных, соответствующих этой ссылке.

E.2 **Обеспечивать возможность ручного выбора набора данных.** В дополнение к автоматизированному выбору набора справочных данных оператор также имеет возможность ручного поиска и выбора конкретного набора данных, используя для этого GUI.

E.3 **Предусматривать возможность предоставления подробной информации относительно подлинных документов.** В справочной базе данных содержится информация о подлинных документах, и она может сопровождаться соответствующими описаниями характерных подделок. Обеспечивается предоставление подробного описания специфических свойств моделей справочных документов, а каждый контент сопровождается текстовым описанием.

В этом контексте следует отметить наличие дополнительной возможности рассмотрения такой базы данных, как EDISON-TD. Для расширения использования коммерческих баз данных можно применять механизмы, описание которых приводится в рекомендации D.1.

С.4.6 Администратор текущих операций

Так называемый *администратор текущих операций* представляет собой организацию, ответственную за административное обеспечение всех процессов, связанных с эксплуатацией инфраструктуры аутентификации, и управление ими. Операторы являются сотрудниками администратора управления текущими операциями, которые непосредственно взаимодействуют с системой аутентификации.

Конкретная реализация запланированных операций зависит от сценария проверки. Ниже приводится описание примерных сценариев:

- **Стационарный пограничный контроль** (SBC). В этом случае функцию администратора текущих операций выполняют государственные полномочные органы, ответственные за осуществление стационарного пограничного контроля (например, пограничная полиция). Обычно в такой ситуации операторы очень хорошо знакомы с процессом оптической верификации документов. Масштабы проверок являются внушительными, что обусловлено очень большим количеством и разнообразием проверяемых документов. Более того, система требует активного взаимодействия и оценки операторов, непосредственно работающих как с системой, так и с владельцами документов.

- **Автоматизированный пограничный контроль на контрольно-пропускных пунктах ABC.** В рамках этого сценария использования контрольно-пропускных пунктов ABC функции администратора текущих операций также выполняют государственные полномочные органы; часто при осуществлении такого контроля больше внимания уделяется оперативной, а не доскональной аутентификации документов. В этом случае операторами являются хорошо подготовленные сотрудники пограничной службы, которые обычно осуществляют контроль за тем, чтобы на контрольно-пропускных пунктах ABC соблюдались требования в отношении минимального объема визуализации. В отличие от стационарного пограничного контроля эта система используется пассажирами, что обуславливает необходимость наличия подробного руководства для пользователей, вопрос о котором в настоящем руководстве не рассматривается.

- **Аутентификация документов в коммерческих целях** (CP). В этом случае функции администратора текущих операций выполняют коммерческие структуры (например, в банках). В отличие от ранее упомянутых сценариев операторы, как правило, не знакомы с процессом оптической верификации, а по сравнению с пограничным контролем масштабы проверки, как правило, являются меньшими.

Возможности приобретаемых компонентов должны соответствовать потребностям администратора текущих операций и требованиям сценария развертывания оборудования. В настоящем разделе рекомендации, предназначенные для изготовителей полностраничных считывателей (см. раздел С.4.2), разработчиков программных средств аутентификации (см. раздел С.4.3), изготовителей баз данных аутентификации (см. раздел С.4.4) и справочных баз данных (см. раздел С.4.5), увязываются со сценариями использования. Рекомендации, касающиеся осуществления мониторинга за соблюдением правил защиты данных, приводятся в разделе С.5.

В таблице С-4 ниже содержится сводная информация о целесообразном использовании в рамках каждого сценария рекомендаций, предназначенных для изготовителей полностраничных считывателей.

Таблица С-4. Рекомендации в отношении полностраничных считывателей, сгруппированные по сценариям проверок

Изготовитель полностраничных считывателей				
№	*Краткое описание*	*Сценарий использования*		
		SBC	ABC	CP
B.1	Гарантировать использование надлежащих длин волн светового спектра	X	X	X
B.2	Гарантировать минимальное разрешение	X	X	X
B.3	Обеспечивать представление изображений в стандартных форматах	X	X	X
B.4	Обеспечивать захват изображения вплоть до размера ID-3	X	X	X
B.5	Гарантировать захват всех областей с одинаковым качеством	X	X	X
B.6	Гарантировать минимальное время реагирования и постоянную интенсивность	X	X	X
B.7	Гарантировать постоянное качество изображения	X	X	
B.8	Обеспечивать возможность настройки времени экспонирования в UV-свете посредством программных средств аутентификации	X	X	
B.9	Обеспечивать возможность захвата нескольких UV-изображений	X		
B.10	Обеспечивать возможность получения безбликовых изображений	X	X	
B.11	Предусматривать наличие прижимного механизма для плоского размещения документа в зоне захвата	X	X	X
B.12	Обеспечить возможность выполнения операций одной рукой	X	X	X

Изготовитель полностраничных считывателей				
№	*Краткое описание*	*Сценарий использования*		
		SBC	ABC	CP
B.13	Обеспечивать предоставление интерактивного руководства пользователя		X	X[15]
B.14	Обеспечивать наличие аппаратных средств с высокой степенью отказоустойчивости	X	X	X

В таблице C-5 приводится сводная информация о целесообразном использовании в рамках каждого сценария рекомендаций, предназначенных для разработчиков программных продуктов аутентификации.

Таблица C-5. Рекомендации в отношении программных средств аутентификации, сгруппированные по сценариям проверок

Изготовитель программных средств аутентификации				
№.	*Краткое описание*	*Сценарий использования*		
		SBC	ABC	CP
C.1	Обеспечивать возможность обработки предварительно записанных изображений [16]	X		
C.2	Обеспечивать возможность обработки изображений из различных аппаратных источников	X	X	X
C.3	Абстрагировать GUI (графический интерфейс пользователя) от программных и аппаратных средств аутентификации	X	X	X
Распознавание документов				
C.4	Обеспечивать возможность распознавания документа в автоматическом или ручном режиме	X	X[17]	
C.5	Обеспечивать возможность компенсации углового смещения и,	X	X	X

15. Как представляется, порядок использования руководства для пользователей в значительной степени зависит от сценария коммерческого использования.
16. Эта рекомендация важна для оценки программных продуктов аутентификации.
17. К сценарию автоматизированного пограничного контроля ручное распознавание документов неприменимо.

Изготовитель программных средств аутентификации				
№.	*Краткое описание*	*Сценарий использования*		
		SBC	ABC	CP
	соответственно, кадрирования считанной страницы данных			
C.6	Обеспечивать распознавание документов на основе имеющихся оптических элементов	X	X	X
Идентификация				
C.7	Идентифицировать модель документа	X	X	X
C.8	Обеспечивать возможность оперативной идентификации посредством МСЗ	X	X	X
C.9	Обеспечивать наличие резервного средства, если в IR-свете МСЗ считыванию не поддается	X	X	X
C.10	Предоставлять однозначную информацию о модели документа	X		
C.11	Обеспечивать возможность частичной идентификации	X		
C.12	Обеспечивать возможность ручной идентификации	X		
C.13	Обеспечивать двустороннюю идентификацию ID- карточек	X	X	X
C.14	Обеспечивать возможность идентификации образцов документов	X	X	X
Верификация				
C.15	Выполнять минимальное количество спектрально-селективных проверок	X	X	X
C.16	Выполнять проверку соответствия МСЗ	X	X	X
C.17	Выполнять проверки во всех категориях	X	X	X
C.18	Выполнять проверку на наличие чипа	X	X	X
C.19	Выполнять проверку динамических рисунков	X	X	X
C.20	При необходимости объединять процедуры проверок	X	X	X
C.21	Выполнять контроль избыточным кодом в нескольких позициях	X		X
C.22	Выполнять контроль избыточным кодом элементов, приобретающих в UV-свете различные цвета	X		

Изготовитель программных средств аутентификации				
№.	*Краткое описание*	*Сценарий использования*		
		SBC	ABC	CP
C.23	Сопоставлять и проверять информацию обеих страниц ID-карточки	X	X	X
C.24	Обеспечивать возможность проведения перекрестной проверки личных данных, содержащихся на нескольких страницах	X	X	X
C.25	Выполнять процедуры проверки с учетом их значимости	X	X	X
C.26	Рассматривать вопрос об отклонении параметров элементов	X	X	X
C.27	Выявлять характерные признаки злонамеренного вмешательства	X	X	X
Визуализация				
C.28	Отображать информацию обо всех проверках документов посредством одного GUI	X	X	X
C.29	Всегда показывать область представления *сводной информации о реализации процесса*	X	X	X
C.30	Обеспечивать *отображение области просмотра результатов оптического исследования* на начальной странице	X		
C.31	Выбирать более подробную информацию одним нажатием кнопки мыши	X	X	
C.32	Представлять результаты с использованием сигналов светофора	X	X	X
C.33	Представлять результаты в соответствии с требованиями документов [BSI-TR-03135]	X	X	X
C.34	Отображать результаты в упрощенном виде	X	X	X
C.35	Отображать более подробную информацию в специально предназначенной для этой цели *области представления результатов углубленного оптического исследования*	X		
C.36	Обеспечивать предоставление рекомендаций пользователям в процессе считывания документов	X	X	X
C.37	Обеспечивать отображение информации, содержащейся в центральных базах данных	X		
C.38	Обеспечивать однотипность структуры МСПД	X		X

Изготовитель программных средств аутентификации				
№.	*Краткое описание*	*Сценарий использования*		
		SBC	ABC	CP
C.39	Оказывать содействие операторам в проведении многостраничной верификации	X		
C.40	Обеспечивать возможность сравнения контента паспорта и визы/электронного вида на жительство (eRP)	X		
C.41	Выделять только несоответствия	X	X	X
C.42	Отображать ошибки в области сводной информации о процессе	X	X	X
C.43	Отображать ошибки в области просмотра результатов оптического исследования	X		
C.44	Отображать ошибки в области представления результатов углубленного оптического исследования	X		
C.45	Отображать ошибки, возникающие при сравнении данных паспорта и визы/eRP	X		
Регистрация				
C.46	Регистрацию XML файлов выполнять в соответствии с требованиями документа [BSI-TR-03135]	X	X	X
C.47	Обеспечивать возможность регистрации факультативных данных изображений	X	X	X
C.48	Предусматривать возможность обезличивания личных данных	X	X	X

Ниже в таблице С-6 приводится сводная информация о целесообразном использовании в рамках каждого сценария рекомендаций, предназначенных для изготовителей баз данных аутентификации.

Таблица С-6. Рекомендации в отношении баз данных аутентификации, сгруппированные по сценариям проверок

Изготовитель баз данных аутентификации				
№	*Краткое описание*	*Сценарий использования*		
		SBC	ABC	CP
D.1	Обмениваться информацией относительно новых моделей документов или подделок	X	X	
D.2	Регулярно обновлять базу данных	X	X	X
D.3	Предоставлять скорректированные версии	X	X	X
D.4	Предоставлять достаточный объем документации, касающейся изменений	X	X	X
D.5	Предоставлять сокращенный контент			X
D.6	Распределять проверки с учетом уровня их значимости	X	X	X
D.7	Предусматривать возможность использования различных эксплуатационных режимов	X	X	X
D.8	Предусматривать предоставление информации о длительности экспонирования конкретной модели документа в UV-свете	X	X	X
D.9	Оказывать поддержку использованию программ серверной установки	X	X	X

Ниже в таблице С-7 приводится сводная информация о целесообразном использовании в рамках каждого сценария рекомендаций, предназначенных для изготовителей справочных баз данных.

Таблица С-7. Рекомендации в отношении справочных баз данных, сгруппированные по сценариям проверок

Изготовитель справочных баз данных				
№	*Краткое описание*	*Сценарий использования*		
		SBC	ABC	CP
E.1	Предусматривать возможность автоматизированного получения выходных данных	X		
E.2	Обеспечивать возможность ручного выбора набора данных	X		X[18]
E.3	Предусматривать возможность предоставления подробной информации относительно подлинных документов	X		X[18]

С.5 КОНТРОЛЬ ЗА СОБЛЮДЕНИЕМ ПРОЦЕДУР ЗАЩИТЫ ДАННЫХ

Процесс оптической аутентификации может дать неожиданный результат, обусловленный одной из перечисленных ниже причин:

- Обнаружен поддельный документ.
- Поддельный документ классифицирован в качестве подлинного.
- Подлинный документ классифицирован в качестве поддельного.
- При обработке документа с помощью полностраничного считывателя произошла ошибка, например, в процессе аутентификации имело место извлечение документа из считывателя.
- Модель документа идентификации не поддается.

В этих случаях исключительно важно, чтобы администратор текущих операций имел возможность проанализировать причину принятия неправильного решения. Поэтому информацию, полученную в процессе аутентификации, которая может содержать личные данные, необходимо зарегистрировать проанализировать. В этой связи возникает вопрос об обеспечении защиты данных, поскольку без согласия владельца документа или наличия обоснованной причины хранить личные данные даже в зашифрованном виде не разрешается. Для администратора текущих операций могут быть сделаны следующие рекомендации:

18. В зависимости от случая коммерческого применения (CP) важно учитывать объем имеющейся информации.

F.1 **Регистрировать информацию о результатах аутентификации.** Информация о результатах реализации процедуры аутентификации, которая не содержит личных данных (например, идентифицированная модель документа, результаты аутентификации, результаты реализации процедур проверок и т. д.) должна регистрироваться в соответствии с требованиями документа [BSI-TR-03135]. Поэтому набор оперативных данных, МСЗ и ЗВП из процесса регистрации исключены. С точки зрения времени такая отчетная информация не является критической, и ее можно использовать для проведения статистического анализа.

F.2 **Устанавливать обратную связь с изготовителем.** Для оптимизации программных средств аутентификации можно использовать регулярную обратную связь с эксплуатационными подразделениями. В этой связи отчетную информацию, о которой говорится в рекомендации F.1, следует регулярно направлять изготовителю программных средств аутентификации.

F.3 **При наличии соответствующих оснований обеспечивать хранение неизмененного набора оперативных данных.** Наилучшим образом анализ ошибок можно выполнить на основе того же набора оперативных данных, который представлялся для проведения аутентификации. В этой связи неизмененный набор оперативных данных рекомендуется хранить в схеме XML, определенной в документе [BSI-TR-03135], если это может быть сделано с учетом обеспечения конфиденциальности данных. Для регистрации имеются следующие возможности:

a) *Хранение набора оперативных данных с согласия владельца документа.* Если это допускается сценарием, то набор оперативных данных можно хранить, вначале получив на это согласие владельца документа. Такой подход можно использовать только в рамках сценариев, обеспечивающих возможность связи с владельцами документов, такими, как пилоты, но не на постоянной основе. Более того, по истечении определенного в контракте периода времени этот набор оперативных данных должен быть удален безвозвратно.

b) *Хранение набора оперативных данных в случае ошибки.* Личные данные разрешается хранить в течение определенного в контракте периода времени при наличии достаточных оснований для хранения, например в случае возникновения ошибки в процессе аутентификации. Если такая возможность предусматривается сценарием, то этот период времени можно использовать для анализа ошибки на основе неизмененного набора оперативных данных, который впоследствии должен быть удален безвозвратно.

c) *Регистрация областей, рассчитанных на обеспечение конфиденциальности.* Во избежание проблем с обеспечением конфиденциальности данных при одновременном сохранении возможности проведения ориентировочного анализа можно регистрировать только "рассчитанные на обеспечение конфиденциальности" обрезанные изображения, визуализирующие область поиска, охватываемую проверкой. В этих рассматриваемых областях не должны размещаться полные изображения лица, МСЗ или ЗВП; что касается всех процессов аутентификации, то информацию, содержащуюся в этих областях, без ограничения по времени можно хранить в схемах XML, определенных в документе [BSI-TR-03135].

F.4 **При наличии соответствующих оснований обеспечивать обезличивание изображений.** Еще одно предложение относительно избежания проблем, обусловленных обеспечением конфиденциальности при одновременном хранении полного комплекта оперативных данных без ограничений по времени, заключается в обезличивании содержащихся в этом комплекте личных данных. При использовании этого метода анализ областей, содержащих личные данные, провести сложно, в то время как части документа, не связанные с личными данными, могут анализироваться в полном объеме.

Примечание. Пояснения, касающиеся использования термина "проблемы, обусловленные обеспечением конфиденциальности данных". Администратор текущих операций должен пояснить значение используемого в рекомендациях F.1–F.4 термина "проблемы, обусловленные обеспечением конфиденциальности данных", например, посредством разработки концепции обеспечения конфиденциальности данных. Рекомендации, касающиеся хранения комплектов оперативных данных, сделанные в пунктах F.3 и F.4, можно объединить, например в рекомендацию о хранении информации, содержащейся в областях, рассчитанных на обеспечение конфиденциальности.

С.6 БИБЛИОГРАФИЯ

[BSI-TR-03135] BSI, Machine Authentication for Public Sector Applications, TR-03135, 2017. url: https://www.bsi.bund.de/tr03135/

[FRONTEX-ABC] FRONTEX: Best Practice Technical Guidelines for Automated Border Control (ABC) Systems, 2012

— — — — — — — —

ДОБАВЛЕНИЕ D К ЧАСТИ 2. ПРЕДОТВРАЩЕНИЕ МОШЕННИЧЕСТВА, СВЯЗАННОГО С ПРОЦЕССОМ ВЫДАЧИ (ИНФОРМАЦИОННОЕ)

D.1 СФЕРА ПРИМЕНЕНИЯ

В настоящем добавлении описываются риски мошенничества, связанного с процессом обращения за получением и выдачей МСПД. Эти риски объясняются растущими выгодами обладания МСПД, который может быть использован для подтверждения личности и гражданства его владельца. В добавлении рекомендуются меры предосторожности, которые могут быть приняты государством выдачи для предотвращения такого мошенничества.

D.2 МОШЕННИЧЕСТВО И ЕГО ПРЕДУПРЕЖДЕНИЕ

Возможные основные виды мошенничества, которые могут иметь место в процессе выдачи:

- кража подлинных бланков МСПД и заполнение их с целью сделать похожими на действительные;

- обращение за получением МСПД под вымышленным именем с использованием подлинного доказательства гражданства и/или идентификационной информации, украденных у другого лица или приобретенных каким-либо иным неправомерным способом;

- обращение за получением МСПД под вымышленным именем с использованием фальшивого доказательства гражданства и/или средства идентификации личности;

- использование МСПД, которые ложно объявлены или не объявлены украденными и/или похищенными и могут предоставляться людям, которые могут использовать их в мошеннических целях на основе сходства внешности или в мошеннических целях с неоднократной заменой фотографии;

- расчет на то, что сотрудники службы МСПД смогут выдать МСПД в нарушение правил, манипулируя системой оформления МСПД.

Существует еще две категории, в рамках которых заявители обращаются за получением паспорта под собственными именами, но с целью соучастия в последующем мошенническом использовании МСПД путем:

- изменения выданного подлинного документа, чтобы сделать его пригодным для предъявителя, не являющегося лицом, которому МСПД выдан;

- обращения с просьбой о выдаче МСПД с намерением передать или продать его кому-либо, кто внешне похож на подлинного владельца.

D.3 РЕКОМЕНДУЕМЫЕ МЕРЫ БОРЬБЫ С МОШЕННИЧЕСТВОМ

В целях противодействия вышеупомянутым угрозам полномочному органу государства по выдаче МСПД рекомендуется принимать перечисленные ниже меры в рамках наличия адекватных ресурсов для их реализации.

На должность руководителя службы безопасности, непосредственно подотчетного руководителю полномочного органа по выдаче, следует назначить лицо, обладающее соответствующей квалификацией. Руководитель службы безопасности должен отвечать за установление, соблюдение и, по мере необходимости, обновление процедур безопасности.

На каждом объекте, где производится выдача МСПД, следует назначить сотрудника по вопросам безопасности. Сотрудник по вопросам безопасности должен отвечать за осуществление и обновление процедур обеспечения безопасности и подчиняться непосредственно руководителю службы безопасности.

Необходимо ввести процедуры проверки, обеспечивающие набор персонала только после подтверждения личности и при условии отсутствия судимости в прошлом и финансовой состоятельности. Кроме того, следует регулярно проводить контрольные проверки для выявления сотрудников, которые в силу изменившихся обстоятельств могут поддаться искушению заняться мошеннической деятельностью.

Следует мотивировать весь персонал полномочного органа по выдаче МСПД на позитивное отношение к вопросам безопасности. Необходимо ввести систему поощрения любого сотрудника, который сообщит об инцидентах и предложит меры по предотвращению мошенничества.

Необходимо вести контроль за учетом таких основных компонентов, как бланки книжек и защитное ламинатное покрытие. Каждое такое изделие должно иметь индивидуальный порядковый мер и храниться в запертом охраняемом складском помещении. В начале каждого рабочего дня или каждой рабочей смены следует выдавать только требуемое количество изделий. Лицо, которому выдаются изделия, в конце смены должно отчитаться за каждое из них, заполнив либо форму персонального учета, либо форму учета бракованной продукции. В конце рабочего периода все изделия следует возвращать на охраняемый склад после еще одного подсчета двумя сотрудниками с регистрацией индивидуальных номеров. Такие записи должны храниться по крайней мере до истечения срока действия выданных МСПД.

Бракованные изделия или материалы подлежат уничтожению в контролируемых условиях с регистрацией индивидуальных номеров.

Процесс выдачи следует подразделить на отдельные операции, осуществляемые в разных помещениях внутри объекта. Цель такого разделения – обеспечить, чтобы ни один сотрудник не мог осуществить весь процесс выдачи без проникновения в одну или несколько производственных зон, на доступ в которые у него нет разрешения.

D.4 ПРОЦЕДУРЫ ПРЕДОТВРАЩЕНИЯ МОШЕННИЧЕСТВА ПРИ ОБРАЩЕНИИ ЗА ДОКУМЕНТОМ

Нижеуказанные процедуры рекомендуются для предотвращения выдачи подлинного МСПД в результате получения мошеннического заявления.

Орган по выдаче МСПД должен назначить соответствующее число специалистов по борьбе с мошенничеством (СБМ), прошедших подготовку высокого уровня по выявлению всех видов мошенничества при обращении за получением МСПД. На каждом объекте, в котором рассматриваются заявления о выдаче МСПД и ведется прием заявителей, должен присутствовать по крайней мере один СБМ. Такой специалист

должен быть постоянно готов оказать помощь тем сотрудникам, которые занимаются обработкой заявлений (уполномоченные сотрудники (УС)), при рассмотрении подозрительных заявлений. СБМ должны проводить регулярное обучение УС для повышения их осведомленности о потенциальных рисках, связанных с мошенничеством.

Полномочный орган по выдаче МСПД должен установить тесные связи с организациями, выдающими исходные документы, такие как свидетельства о рождении и браке и водительские удостоверения. Возможность доступа к базе данных свидетельств о смерти помогает в предотвращении случаев мошенничества, связанных с обращением за выдачей МСПД от имени умершего человека. Государство должно следить за тем, чтобы учреждения, хранящие записи о рождении, браке и смерти, согласовывали свои действия и хранили информацию в базе данных, защищенный доступ к которой следует предоставлять полномочному органу, выдающему МСПД. Это необходимо для того, чтобы обеспечить оперативную верификацию подлинности представленных исходных документов и убедиться в том, что заявление не подано, например, от имени умершего лица. Заявителям, обратившимся за получением МСПД, которые ранее такого документа не имели, следует предложить лично явиться в центр по выдаче МСПД с необходимыми исходными документами для беседы с УС и, при необходимости, с СБМ.

Такая процедура может также использоваться при обработке заявлений о выдаче МСПД взамен документа, срок действия которого истекает. В качестве альтернативы и при условии, что центр по выдаче МСПД располагает адекватной базой данных, содержащей персональную информацию, включая фотографии, заявления о замене могут обрабатываться на основе представления документов, включая новую фотографию, по почте. В таких случаях желательно, чтобы подлинное заявление и новые фотографии заверялись ответственным лицом. При подаче заявления о выдаче нового МСПД следует требовать возвращения документа, срок действия которого истекает.

Центр по выдаче МСПД должен ввести процедуры, препятствующие мошеннической выдаче более одного МСПД человеку, пытающемуся выдать себя за нескольких лиц. При этом полезно провести проверку хранящихся в компьютерных базах данных фотографий с использованием средств распознавания черт лица и, по возможности, отпечатков пальцев.

Применяемые в центре по выдаче МСПД процедуры должны не допускать возможности выбора подателем заявления уполномоченного сотрудника, который будет его обслуживать. И наоборот, организация работы не должна разрешать самостоятельный выбор сотрудником заявлений для обработки.

При выдаче МСПД ребенку младшего возраста следует требовать присутствия в центре по выдаче, желательно, обоих родителей и ребенка. Это снижает риск незаконного вывоза или похищения ребенка одним из родителей.

Замену МСПД, объявленного утерянным или похищенным, следует проводить только после исчерпывающих проверок, включая личную беседу с заявителем.

Такую информацию, как номера утерянных или похищенных МСПД, следует направлять в базу данных ИНТЕРПОЛа. Доступ в такую базу данных предоставляется всем участвующим странам и может использоваться для составления списков особого внимания.

D.5 КОНТРОЛЬ ЗА ЦЕНТРАМИ ВЫДАЧИ

Государству следует рассмотреть возможность выдачи всех МСПД в одном или максимум в двух центрах. Это позволит сократить количество объектов, где хранятся бланки документов и другие защитные компоненты. Контроль в таком центре может быть гораздо строже, чем в каждом из нескольких пунктов выдачи. Введение принципа централизованной выдачи потребует создания центров, где можно проводить беседу с заявителями. Кроме того, поскольку стандартные МСПД не могут выдаваться немедленно, необходимо предусмотреть порядок выдачи МСПД в экстренных случаях.

— — — — — — — —

ДОБАВЛЕНИЕ E К ЧАСТИ 2. ОСНОВНЫЕ СООБРАЖЕНИЯ, КАСАЮЩИЕСЯ БАЗЫ ДАННЫХ ASF/SLTD (ИНФОРМАЦИОННОЕ)

Законодательные требования	Прежде чем вводить практику представления информации в базу данных ИНТЕРПОЛа ASF/SLTD, государствам следует выяснить, допускает ли существующая законодательная база возможность предоставления на международной основе доступа к элементам информации, содержащейся в проездных документах граждан. Если потребуются поправки к законодательству, государствам необходимо обеспечить надлежащее освещение следующих моментов: 1. сбор и хранение данных; 2. положения о конфиденциальности личной информации (включая ее защиту); 3. разрешение на предоставление данных международному сообществу; 4. жизненный цикл и неопровержимый характер данных
Элементы данных	Для обмена информацией о потерянных, украденных и аннулированных проездных документах разработан стандартный набор данных, относящихся в большей степени к информации о документе, чем о владельце документа. При представлении информации в эту базу данных государствам необходимо заполнить следующие требуемые поля данных: 1. идентификационный номер проездного документа*; 2. тип документа (паспорт или иной); 3. государство выдачи – кодовое наименование ИКАО; 4. статус документа (например, похищенный бланк); 5. страна, где произошло хищение (обязательно только для похищенных бланков проездных документов). *Если проездной документ персонализирован, необходимо указать номер документа, содержащийся в МСЗ; если речь идет о бланке книжки, указать серийный номер, если эти номера не совпадают
Сбор информации	Государствам следует обеспечивать, чтобы методы сбора информации об утерянных и похищенных проездных документах (т. е. разговоры по телефону, онлайн-формы) были исчерпывающими и способствовали безопасному сбору всех данных, требуемых для представления в ASF/SLTD

Своевременное и точное представление данных	Эффективность базы данных ASF/SLTD ИНТЕРПОЛа зависит от оперативного и точного представления информации. Поэтому государствам следует обеспечивать наличие систем и процессов, гарантирующих наиболее оперативный обмен информацией, чтобы воспрепятствовать попыткам использования утерянных, похищенных или аннулированных проездных документов в пунктах пограничного контроля. Государствам следует стремиться обмениваться такой информацией на ежедневной основе. Как правило, после получения информации о том, что проездной документ более не находится во владении лица, которому он принадлежит на законном основании, или аннулирован, полномочный орган выдачи должен официально зафиксировать эту информацию в национальной базе данных (если он ее ведет и обновляет) и в базе данных ASF/SLTD. Государствам следует также постоянно следить за тем, чтобы такие данные были точными и достоверными. Необходимо избегать ошибок при вводе данных и следить за тем, чтобы представлялась вся требуемая информация о документе, поскольку за точность представляемой информации отвечает полномочный орган выдачи. Ошибки при представлении данных могут привести к нарушениям в поездках и затратам как для путешественника, так и для государства выдачи. Поэтому государствам следует принимать необходимые меры для обеспечения точности регистрации и представления информации об утерянных, похищенных и аннулированных проездных документах. Государствам следует организовать круглосуточную службу для оперативного запроса дополнительной информации в ИНТЕРПОЛ от имени государства
Оптимизация национальных баз данных об утерянных, похищенных и аннулированных проездных документах	Государствам, которые ведут национальные базы данных об утерянных, похищенных и аннулированных проездных документах, следует рассмотреть возможность использования автоматизированных методов передачи такой информации в ИНТЕРПОЛ для оптимизации этой работы

— КОНЕЦ —

ISBN 978-92-9265-462-7