



ИКАО

Doc 9303

Машиносчитываемые проездные документы Издание седьмое, 2015

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



Утверждено Генеральным секретарем и опубликовано с его санкции

Международная организация гражданской авиации



ИКАО

Doc 9303

Машиносчитываемые проездные документы
Издание седьмое, 2015

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

Утверждено Генеральным секретарем и опубликовано с его санкции

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
ISBN 978-92-9249-937-2

© ИКАО, 2016

Все права защищены. Никакая часть данного издания не может воспроизводиться, храниться в системе поиска или передаваться ни в какой форме и никакими средствами без предварительного письменного разрешения Международной организации гражданской авиации.

ОГЛАВЛЕНИЕ

	<i>Страница</i>
1. СФЕРА ПРИМЕНЕНИЯ	1
2. ЗАЩИТА МСПД И СРЕДСТВ ЕГО ВЫДАЧИ	2
3. КОМПЬЮТЕРНАЯ ВЕРИФИКАЦИЯ ДОКУМЕНТОВ	2
3.1 Типы элементов	3
3.2 Базовые принципы	4
3.3 Компьютерная аутентификация и электронные МСПД	6
4. ОХРАНА МЕСТ ИЗГОТОВЛЕНИЯ И ВЫДАЧИ МСПД	6
4.1 Способность к восстановлению	6
4.2 Физическая защита и контроль доступа	7
4.3 Учет производственных материалов	7
4.4 Транспортировка	8
4.5 Персонал	8
4.6 Кибербезопасность	8
5. ПРЕДОСТАВЛЕНИЕ ИНФОРМАЦИИ О НОВЫХ МСПД	8
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	9
6.3 Обмен информацией об утерянных, похищенных и аннулированных проездных документах с ИНТЕРПОЛ и систематическая выверка документов по базам данных ИНТЕРПОЛ в рамках первичного контроля	10
6.4 Введение мер контроля для выявления случаев представления утерянного, похищенного или аннулированного документа при пересечении границы	10
ДОБАВЛЕНИЕ А К ЧАСТИ 2. СТАНДАРТЫ ЗАЩИТЫ МСПД (ИНФОРМАЦИОННОЕ)	Доб А-1
А.1 Сфера применения	Доб А-1
А.2 Введение	Доб А-1
А.3 Основные принципы	Доб А-2
А.4 Основные угрозы целостности проездных документов	Доб А-3
А.5 Элементы и методы защиты	Доб А-4

ДОБАВЛЕНИЕ В К ЧАСТИ 2. КОМПЬЮТЕРНАЯ ВЕРИФИКАЦИЯ ЭЛЕМЕНТОВ ЗАЩИТЫ ДОКУМЕНТА (ИНФОРМАЦИОННОЕ).....		Доб В-1
V.1	Сфера применения.....	Доб В-1
V.2	Считывающие устройства для документов и системы компьютерной аутентификации.....	Доб В-1
V.3	Элементы защиты и их применение для компьютерной аутентификации.....	Доб В-2
V.4	Критерии выбора элементов защиты, пригодных для компьютерной верификации.....	Доб В-14
ДОБАВЛЕНИЕ С К ЧАСТИ 2. ПРЕДОТВРАЩЕНИЕ МОШЕННИЧЕСТВА, СВЯЗАННОГО С ПРОЦЕССОМ ВЫДАЧИ (ИНФОРМАЦИОННОЕ).....		Доб С-1
C.1	Сфера применения.....	Доб С-1
C.2	Мошенничество и его предупреждение.....	Доб С-1
C.3	Рекомендуемые меры борьбы с мошенничеством.....	Доб С-2
C.4	Процедуры предотвращения мошенничества при обращении за документом.....	Доб С-2
C.5	Контроль за центрами выдачи.....	Доб С-4
ДОБАВЛЕНИЕ D К ЧАСТИ 2. ОСНОВНЫЕ МОМЕНТЫ, СВЯЗАННЫЕ С БАЗОЙ ДАННЫХ ASF/SLTD (ИНФОРМАЦИОННОЕ).....		Доб D-1

1. СФЕРА ПРИМЕНЕНИЯ

В седьмом издании документа Дос 9303 изменена структура спецификаций ИКАО для машиночитываемых проездных документов. Без внесения принципиальных изменений в конкретные технические требования данное новое издание Дос 9303 скомпоновано в виде свода спецификаций машиночитываемых официальных проездных документов размера 1 (ПД1), машиночитываемых официальных проездных документов размера 2 (ПД2) и машиночитываемых проездных документов размера 3 (ПД3), а также виз. Такой комплект спецификаций состоит из различных самостоятельных документов, в которых сгруппированы общие, т. е. применимые ко всем МСПД, спецификации, а также технические требования, относящиеся к конкретному формату МСПД.

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 большую обеспокоенность вопросами защиты проездных документов, в связи с чем возникла необходимость в выработке рекомендаций относительно возможных действий по повышению их устойчивости к попыткам нарушения их защиты или ненадлежащего использования. По сложившейся практике документ Дос 9303 не содержит рекомендаций о конкретных элементах защиты проездных документов. Каждое выдающее такие документы государство может предусматривать такие меры предосторожности, которые оно считает целесообразным 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 желательным опубликовать свод "рекомендуемых минимальных стандартов защиты", которыми все государства могли бы руководствоваться при выдаче машиночитываемых проездных документов. С учетом этого:

- в добавлении А к настоящей части описываются меры защиты, которые следует принимать в рамках структуры МСПД и в помещениях, в которых они изготавливаются;
- в добавлении В описываются факультативные средства обеспечения компьютерной верификации документов;
- в добавлении С описываются меры защиты, которые следует принимать для обеспечения безопасности в ходе операций по персонализации и перевозке документов.

2. ЗАЩИТА МСПД И СРЕДСТВ ЕГО ВЫДАЧИ

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 себя¹ за другое лицо. Необходимо предусматривать элементы защиты, способствующие визуальному и/или автоматизированному обнаружению случаев мошеннического использования МСПД самозванцем.

Существуют признанные методы обеспечения защиты от перечисленных выше типов мошеннических актов. К ним относятся использование материалов, не имеющих 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 проводящему проверку сотруднику 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. КОМПЬЮТЕРНАЯ ВЕРИФИКАЦИЯ ДОКУМЕНТОВ

Полномочный орган, выдающий проездной документ, может включить в свой МСПД один или несколько элементов защиты, требующих использования детекторного оборудования для обнаружения и верификации их присутствия в пределах нормативного времени прохождения иммиграционного контроля. В настоящем разделе содержатся рекомендации относительно аутентификации с помощью компьютеров элементов защиты, включенных в МСПД в соответствии со спецификациями документа Doc 9303. Элементы защиты, подлежащие верификации с помощью машины, помогают подтвердить аутентичность подлинного документа, изготовленного из оригинальных материалов. В добавлении В содержатся рекомендации относительно компьютерной аутентификации элементов защиты в самом документе (включая материалы, защитную печать и методы защиты от копирования), а также рекомендации по технологиям считывания, применимым к компьютерной аутентификации документов. В основу настоящего раздела положены материал добавления А к настоящей части и рекомендуемые в нем стандарты защиты с использованием мер защиты, рекомендуемых в добавлении, и с учетом расширения функциональных возможностей современных считывающих устройств, уже установленных на пограничных пунктах, в целях обеспечения обработки и верификации электронных машиносчитываемых проездных документов (электронных МСПД).

¹ Во всех случаях, когда в настоящем документе употребляются грамматические формы мужского рода, их следует рассматривать как относящиеся к лицам как мужского, так и женского пола.

Благодаря широкой реализации инициативы ИКАО по использованию электронных документов во всем мире выдаются миллионы электронных МСПД, соответствующих спецификациям документа Doc 9303. Эти передовые концепции документов требуют применения считывающих устройств для проездных документов, позволяющих считывать бесконтактные ИС в пунктах аутентификации документов, обычно в пунктах въезда на границе государства. Такие усовершенствованные считывающие устройства позволяют не только считывать бесконтактные ИС, но и получать изображение высокой четкости в видимом, инфракрасном и ультрафиолетовом спектре.

Цель рекомендаций в настоящей главе заключается в улучшении защиты машиносчитываемых проездных документов во всем мире путем использования процедур компьютерной аутентификации документов в полном соответствии со:

- структурой машиносчитываемых проездных документов, определенной в документе Doc 9303, с обеспечением обратной совместимости;
- элементами защиты, рекомендуемыми в добавлении А к настоящей части;
- использованием технических возможностей усовершенствованных считывающих устройств, установленных во всем мире для обработки электронных МСПД.

Вместе с тем каждое государство должно провести оценку рисков, связанных с аутентификацией документов с помощью компьютеров на своей национальной границе, в целях выявления наиболее значимых преимуществ и минимизации рисков. Документ Doc 9303 не определяет какой-либо элемент как средство глобальной интероперабельности при верификации документов с помощью машин, поскольку использование какого-либо одного элемента во всем мире сделает этот элемент 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 элементов защиты, верифицируемых с помощью компьютеров. Ниже приводятся их описания наряду с примерами элементов защиты, которые можно верифицировать с помощью машины.

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. Приводятся, в частности, следующие примеры:

- интерференционная характеристика голограммы или другого устройства с оптически изменяющимися свойствами, которое может быть однозначно идентифицировано при помощи соответствующего считывающего устройства;
- изображение с обратным отражением, 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. Примеры включают, в частности:

- 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, которую можно обнаружить с помощью соответствующего приспособления, встроенного в устройство для считывания. Такая скрытая информация может находиться в защищенной странице данных, но чаще ее включают в персональные данные, 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 персональной фотографии, либо на защищенном напечатанном фоне. Такую информацию можно декодировать с помощью приспособления, встроенного в полноразмерное 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 любым данным, хранящимся на бесконтактной ИС электронного МСПД. Примеры элементов такого типа включают, в частности:

- 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. В добавлении В рассказывается главным образом об элементах, которые можно верифицировать с помощью детекторного оборудования, встроенного в считывающее устройство МСПД и используемое в ходе нормального процесса считывания.

При верификации элементов защиты документа с помощью компьютера используется технология автоматизированной проверки для оказания помощи при верификации подлинности проездного документа. Ее следует использовать не изолированно для подтверждения аутентичности, а в сочетании с методами визуальной проверки элементов защиты документа, предоставляющих проверяющему сотруднику эффективное новое средство верификации проездных документов.

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

Размер элементов защиты, предназначенных для компьютерной верификации, может варьироваться от менее 1 мм² (0,04 дюйма²) 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 компьютерной аутентификации, на указанных местах и зонах.

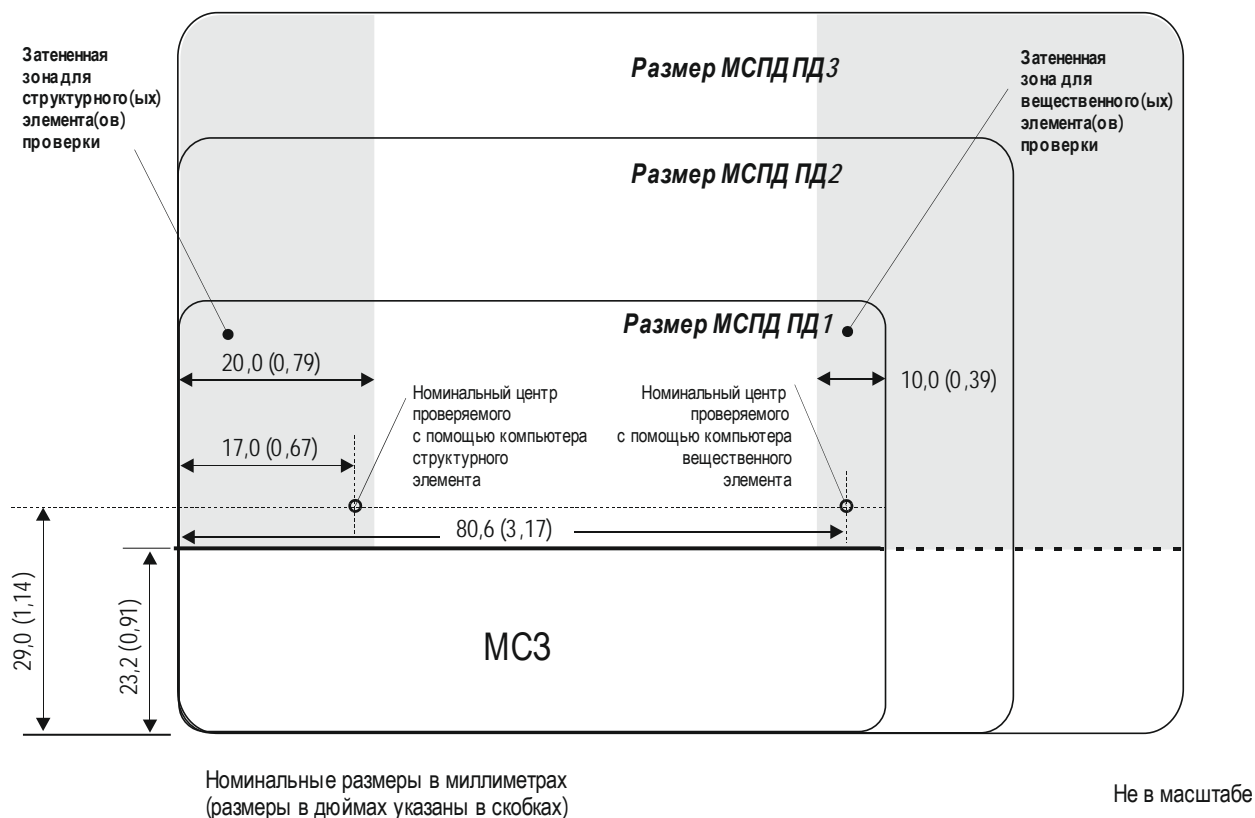


Рис. 1. Три размера МСПД, включая МСП (размер ПД3), с рекомендуемым расположением элементов проверки документа с помощью компьютера. Затененный участок слева рекомендуется для включения структурного элемента, а затененный участок справа – для включения вещественного элемента

3.3 Компьютерная аутентификация и электронные МСПД

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

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

Поэтому требуется альтернатива компьютерной аутентификации. Это особенно важно для сценария автоматизированного пограничного контроля (АВК), когда для считывания и валидации электронного МСПД используется компьютерное считывающее устройство, а не сотрудник службы пограничного контроля. Такие альтернативные средства компьютерной аутентификации повышают доверие к данным, используемым при принятии решений на границе.

Функционирующая бесконтактная ИС в электронном МСПД также может помочь при компьютерной аутентификации путем хранения элементов компьютерной аутентификации и их координат в соответствующих группах данных (ГД).

4. ОХРАНА МЕСТ ИЗГОТОВЛЕНИЯ 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 контролирования 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, доступ 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 компьютерных 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 персональные 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 ИНТЕРПОЛ и систематическая выверка документов с использованием баз данных ИНТЕРПОЛ 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 документов 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 прини-

мать 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 ИНТЕРПОЛ и систематическая выверка документов по базам данных ИНТЕРПОЛ 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) ИНТЕРПОЛ 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 ИНТЕРПОЛ 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 Если проездной документ "засветился" в базе данных об утерянных, похищенных или аннулированных документах ИНТЕРПОЛ

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. Государству следует также провести собеседование с путешественником, чтобы проверить его личность или гражданство и определить, является ли он законным владельцем данного проездного документа.

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 персональными данными.

<p><i>Путешественники, въезжающие в иностранное государство по документу, заявленному в качестве утерянного, похищенного или аннулированного в результате ошибки в данных</i></p>	<p>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 страну связаться с полномочным органом выдачи.</p> <p>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</p>
<p><i>Граждане, пытающиеся выехать из своей страны по документу, который заявлен в качестве утерянного или похищенного</i></p>	<p>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</p>

<p><i>Граждане, пытающиеся выехать из своей страны по аннулированному документу</i></p>	<p>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 такого путешественника из страны. Если это допускается, пограничным/полицейским органам следует воспрепятствовать выезду путешественников из государства</p>
<p><i>Граждане, пытающиеся покинуть страну и вернуться в свою страну по документу, заявленному в качестве утерянного, похищенного или аннулированного</i></p>	<p>В тех случаях, когда существует контроль выезда и подтверждены личность и гражданство владельца, сотрудники пограничного контроля могут пропустить такое лицо, но должны информировать его о том, что представленный документ является недействительным и что ему может быть отказано перевозчиком в посадке на борт.</p> <p>В том случае, если путешественник возвращается в свою страну по документу, заявленному в качестве утерянного, похищенного или аннулированного, сотрудники пограничной службы могут, если это разрешено национальным законом 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</p>
<p><i>Граждане, пытающиеся покинуть иностранное государство и проследовать в третью страну по документу, заявленному в качестве утерянного, похищенного или аннулированного</i></p>	<p>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</p>
<p><i>Путешественники, въезжающие в иностранное государство по документу, заявленному в качестве утерянного, похищенного или аннулированного</i></p>	<p>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</p>

6.4.3 Оформление путешественника после того, как было установлено, что он не является законным владельцем документа, заявленного в качестве утерянного, похищенного или аннулированного

Установив, что путешественник не является законным обладателем 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 вернуть 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.

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 помочь предохраниться от этих угроз.

А.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 если 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 пути 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 осуществляться 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. Должен вестись 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 предотвращения 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 либо путем проведения судебной экспертизы, либо с помощью специального оборудования для верификации. Очевидно, что иметь информацию 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".

Не имеется других приемлемых средств хранения данных в целях глобальной интероперабельности, кроме бесконтактной ИС, которая определена ИКАО в качестве технологии расширения емкости для 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 включать новые элементы защиты документа и подтверждать способность противостоять попыткам нарушения его целостности и мошеннических действий, включающих:

- 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 простота 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.

А.5 ЭЛЕМЕНТЫ И МЕТОДЫ ЗАЩИТЫ

В нижеследующих разделах элементы и методы защиты и другие меры защиты описываются в соответствии с этапами, которые осуществляются 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 сенсibilизаторы в бумаге, по крайней мере на странице биографических данных (если это совместимо с методом персонализации);
- бумага с надлежащей поглощающей способностью, шероховатостью и легкоразрываемая.

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 нити;
- видимые (флуоресцентные) нити;
- 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 таким образом, что при облучении ультрафиолетовыми лучами испускает флуоресценцию, отличную по цвету от бело-голубого света, используемого в широкодоступных материалах, содержащих оптические отбеливатели;
- соответствующие химические сенсibilизаторы в бумаге (как правило, не могут применяться в пластиковой подложке наклейки);

- невидимые флуоресцентные нити;
- видимые (флуоресцентные) нити;
- система связывающих и/или других характеристик, препятствующих снятию наклейки без четко видимых повреждений наклейки 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 обложки паспортной книжки

Нет необходимости использовать водяной знак на бумаге, применяемой для внутренней обложки паспортной книжки. Хотя это определено не рекомендуется, если внутренняя обложка 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 страница обложки, должна содержать соответствующие химические сенсibilизаторы, если внутренняя обложка используется в качестве страницы биографических данных. Бумага с химическими сенсibilизаторами 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. 5.1.1–5.1.3, 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. 5.2–5.5.2. 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 таким образом, что при облучении ультрафиолетовыми лучами 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.

А.5.2 Защитная печать

А.5.2.1 Фон и печатание текста

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

- двухцветный гильошированный узор защитного фона¹;
- 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.

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

А.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.

А.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 перфорруется;

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

**А.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. 5.3.2, 5.4.3 и 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).

**А.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.

А.5.3 Защита от копирования

А.5.3.1 Необходимость защиты от копирования

Современный уровень разработок общедоступных методов цифрового воспроизведения и вытекающие отсюда возможности подделки означают, что необходимы высококачественные элементы защиты в форме характеристик 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 компонентов 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.

А.5.3.2 Методы защиты от копирования

С учетом минимальных рекомендаций, изложенных в пп. 5.4.3 и 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.

А.5.4 Методы персонализации

А.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 вклеенные фотографии не разрешается использовать на МСПД.

А.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.

А.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 клеивания 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.

А.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 сенсбилизаторов 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;
- дополнительное изображение фотографии владельца;
- элементы информации в машиносчитываемой форме, описываемые в частях 9–12 документа Дос 9303.

А.5.5 Дополнительные меры защиты паспортных книжек

А.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 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.

А.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 распарывания;

- 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, желателен 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 наклейки, то рекомендуется учитывать дополнительные требования к защите, описанные в пп. А.5.1.2 и А.5.2.4, включая интеграцию такой наклейки с машиносчитываемым проездным документом через номер паспорта.

А.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.

А.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.

А.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 ИНТЕРПОЛ 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 защите

<i>Компоненты</i>	<i>Базовые элементы</i>	<i>Дополнительные элементы</i>
Материалы основы (А.5.1)		
Бумажные основы (А.5.1.1)	<ul style="list-style-type: none"> – контролируемая УФ-реакция; – двухтоновый водяной знак; – химические сенсibilизаторы; – надлежащие характеристики абсорбции и поверхности 	<ul style="list-style-type: none"> – зарегистрированный водяной знак; – разные водяные знаки на странице данных и визовых страницах; – цилиндрические формы для водяных знаков; – невидимые флуоресцентные нити; – видимые (флуоресцентные) нити; – заделанные нити; – маркеры; – элементы защиты, выполненные с помощью лазерной перфорации

Компоненты	Базовые элементы	Дополнительные элементы
Бумажные или другие основы в форме наклейки (А.5.1.2)	<ul style="list-style-type: none"> – контролируемая УФ-реакция; – химические сенсibilизаторы; – невидимые флуоресцентные нити; – видимые (флуоресцентные) нити; – система клеящих материалов 	<ul style="list-style-type: none"> – защитная нить; – водяной знак; – элементы защиты методом лазерной перфорации; – защитный рисунок методом штамповки
Синтетические основы (А.5.1.4)	<ul style="list-style-type: none"> – сопротивляемость расслоению структуры; – оптически матовый материал; – средства защиты страницы данных; – элементы с оптически изменяющимися характеристиками; – см. пп. 5.2–5.5, по мере необходимости 	<ul style="list-style-type: none"> – оконные или прозрачные элементы; – тактильные элементы; – элементы лазерной перфорации
Печатание с обеспечением защиты (А.5.2)		
Фон и печатание текста (А.5.2.1)	<ul style="list-style-type: none"> – двухцветная гильошированная основа; – радужная печать; – микропечатание; – уникальный рисунок страницы данных 	<ul style="list-style-type: none"> – 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
Чернила (А.5.2.2)	<ul style="list-style-type: none"> – ультрафиолетовые флуоресцентные чернила; – реактивные чернила 	<ul style="list-style-type: none"> – чернила с оптически изменяющимися свойствами; – металлические чернила; – проникающие чернила для нумерации; – метамерические чернила; – инфракрасные исчезающие чернила; – инфракрасные абсорбируемые чернила; – фосфоресцирующие чернила; – маркированные чернила; – невидимые чернила

Компоненты	Базовые элементы	Дополнительные элементы
Нумерация (А.5.2.3)	<ul style="list-style-type: none"> – нумерация на всех листах; – напечатанный и/или перфорированный номер; – нумерация специальным шрифтом для наклеек; – идентичные методы нумерации и внесения биографических данных на синтетических основах и картах 	<ul style="list-style-type: none"> – нумерация документа методом лазерной перфорации; – специальные гарнитур
Методы персонализации (А.5.4)		
Защита от замены и изменения фотографии (А.5.4.4)	<ul style="list-style-type: none"> – интеграция биографических данных; – защитный фон, перекрывающий зону фотографии; – реактивные чернила и химические сенсоризаторы в бумаге; – видимые средства защиты, перекрывающие зону фотографии; – термоусаживаемый защитный ламинат или эквивалентный элемент 	<ul style="list-style-type: none"> – отображение подписи; – стеганографическое изображение; – дополнительное(ые) изображение(я) фотографии; – биометрические элементы согласно части 9
Дополнительные элементы защиты для паспортных книжек (А.5.5)		
Замена страницы (А.5.5.2)	<ul style="list-style-type: none"> – технология защищенного прошивания; – ультрафиолетовая флуоресцентная нить для прошивания; – уникальный рисунок страницы данных; – интеграция номеров страниц в защитный рисунок; – серийный номер на каждом листе 	<ul style="list-style-type: none"> – 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 (А.5.7)		
Защита от кражи и ненадлежащего использования (А.5.7.1)	<ul style="list-style-type: none">– 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	<ul style="list-style-type: none">– 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 несколько 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 В и С. Поэтому добавления А, В и С 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 II. КОМПЬЮТЕРНАЯ ВЕРИФИКАЦИЯ ЭЛЕМЕНТОВ ЗАЩИТЫ ДОКУМЕНТА (ИНФОРМАЦИОННОЕ)

В.1 СФЕРА ПРИМЕНЕНИЯ

Настоящее добавление содержит рекомендации в отношении компьютерной аутентификации элементов защиты в самом документе (материалов, защитной печати и методов защиты от копирования), а также рекомендации о технологиях считывания для компьютерной аутентификации документов.

В.2 СЧИТЫВАЮЩИЕ УСТРОЙСТВА ДЛЯ ДОКУМЕНТОВ И СИСТЕМЫ КОМПЬЮТЕРНОЙ 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 компьютерной аутентификации. Этот вопрос, естественно, связан с общемировой проблемой затрат и инфраструктуры.

В.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), 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.

В.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.

В.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.

В.3 ЭЛЕМЕНТЫ ЗАЩИТЫ И ИХ ПРИМЕНЕНИЕ ДЛЯ КОМПЬЮТЕРНОЙ АУТЕНТИФИКАЦИИ

В нижеследующих разделах описываются основные элементы и методы защиты, которые указаны в положениях о стандартных средствах защиты в добавлении А, и приводятся разъяснения относительно

возможностей компьютерной аутентификации таких механизмов защиты. Для выбора элементов защиты из добавления А полномочные органы выдачи могут использовать приведенные ниже таблицы, чтобы выяснить, какие возможности компьютерной аутентификации существуют для таких элементов.

В.3.1 Материалы основы

В.3.1.1 Бумажные страницы проездного документа

Элементы защиты	Сенсорные устройства, необходимые для компьютерной аутентификации				Специальный сенсор	Рисунок фиксированный/меняющийся	Метод компьютерной аутентификации	
	Стандартное считывающее устройство							Усовершенствованное считывающее устройство
	Видимый	УФ	ИК	ВЧ				
Базовые элементы								
Контролируемая УФ-реакция		Х					Интенсивность УФ-излучения	
Двухтоновый водяной знак					Передача	Фиксированный	Сравнение рисунков	
Химические сенсibilизаторы							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 нити		Х	Х			Фиксированный/меняющийся	Сравнение рисунков	
Видимые (флуоресцентные) нити	Х	Х				Фиксированный/меняющийся	Сравнение рисунков	

Элементы защиты	Сенсорные устройства, необходимые для компьютерной аутентификации				Специальный сенсор	Рисунок фиксированный/меняющийся	Метод компьютерной аутентификации	
	Стандартное считывающее устройство							Усовершенствованное считывающее устройство
	Видимый	УФ	ИК	ВЧ				
Защитная нить	Х	Х			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.

В.3.1.2 Бумажная или другая основа в форме наклейки

Элементы защиты	Сенсорные устройства, необходимые для компьютерной аутентификации				Специальный сенсор	Рисунок фиксированный/меняющийся	Метод компьютерной аутентификации	
	Стандартное считывающее устройство							Усовершенствованное считывающее устройство
	Видимый	УФ	ИК	ВЧ				
Базовые элементы								
Контролируемая УФ-реакция		Х					Интенсивность УФ-излучения	
Химические сенсibilизаторы							N/A	
Невидимые флуоресцентные нити		Х	Х			Фиксированный/меняющийся	Сравнение рисунков	
Видимые (флуоресцентные) нити	Х	Х				Фиксированный/меняющийся	Сравнение рисунков	
Клеящиеся материалы							N/A	

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

В.3.1.3 Синтетические основы

Элементы защиты	Сенсорные устройства, необходимые для компьютерной аутентификации					Рисунок фиксированный/меняющийся	Метод компьютерной 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. 5.3
См. пп. 5.2–5.5, при необходимости							

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

В.3.2 Защитная печать

В.3.2.1 Фон и печатание текста

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

Элементы защиты	Сенсорные устройства, необходимые для компьютерной аутентификации				Специальный сенсор	Рисунок фиксированный/меняющийся	Метод компьютерной аутентификации	
	Стандартное считывающее устройство							Усовершенствованное считывающее устройство
	Видимый	УФ	ИК	ВЧ				
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 привodka					Передача	Фиксированный	Сравнение рисунков	
Преднамеренная ошибка	X	X	X			Фиксированный	OCR, сравнение рисунков	
Уникальный рисунок на каждой странице	X	X				Фиксированный	Сравнение рисунков [#]	
Тактильный элемент					Светоотражающий	Фиксированный	Сравнение рисунков	
Уникальный(ые) шрифт(ы)	X	X	X				Сравнение рисунков	

* Нецелесообразно для считывания паспортов.

[#] Требуется взаимодействие с пользователем; неприемлемо для автоматизированных систем пограничного контроля.

В.3.2.2 Чернила

Элементы защиты	Сенсорные устройства, необходимые для компьютерной аутентификации				Специальный сенсор	Рисунок фиксированный/меняющийся	Метод компьютерной аутентификации	
	Стандартное считывающее устройство							Усовершенствованное считывающее устройство
	Видимый	УФ	ИК	ВЧ				
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 компьютерной аутентификации					Рисунок фиксированный/меняющийся	Метод компьютерной 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

В.3.2.3 Нумерация

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

В.3.3 Защита от копирования

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

В.3.4 Методы персонализации

В.3.4.1 Защита от замены и изменения фотографий

Элементы защиты	Сенсорные устройства, необходимые для компьютерной аутентификации					Рисунок фиксированный/меняющийся	Метод компьютерной 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 сенсibilизаторы 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 компьютерной аутентификации				Специальный сенсор	Рисунок фиксированный/меняющийся	Метод компьютерной аутентификации	
	Стандартное считывающее устройство							Усовершенствованное считывающее устройство
	Видимый	УФ	ИК	ВЧ				
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	ВЧ-считыватель	

В 3.5 Дополнительные меры защиты для паспортных книжек

Элементы защиты	Сенсорные устройства, необходимые для компьютерной аутентификации				Специальный сенсор	Рисунок фиксированный/меняющийся	Метод компьютерной аутентификации	
	Стандартное считывающее устройство							Усовершенствованное считывающее устройство
	Видимый	УФ	ИК	ВЧ				
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 компьютерной аутентификации					Рисунок фиксированный/меняющийся	Метод компьютерной 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, лазерная перфорация					Передача	Фиксированный/меняющийся	Сравнение рисунков
Биографические данные на внутренней странице							N/A

В 3.6 Дополнительные меры защиты, пригодные для компьютерной аутентификации

Перечисленные ниже защитные элементы пригодны для компьютерной аутентификации, но не указаны в добавлении А.

Элементы защиты	Сенсорные устройства, необходимые для компьютерной аутентификации					Рисунок фиксированный/меняющийся	Метод компьютерной 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 компьютерной аутентификации				Специальный сенсор	Рисунок фиксированный/меняющийся	Метод компьютерной аутентификации	
	Стандартное считывающее устройство							Усовершенствованное считывающее устройство
	Видимый	УФ	ИК	ВЧ				
Считывание и пассивная аутентификация (+AA) бесконтактной ИС				X			ВЧ-считыватель	
Обнаружение и считывание защитных элементов на основе LED в пластике	X	X	X	X		Фиксированный/меняющийся	Использование ВЧ для приведения в действие LED в пластике	
Обнаружение и считывание отображаемой (буквенно-цифровой) информации будущих защитных элементов	X	X	X	X		Фиксированный/меняющийся	Использование ВЧ 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	

В.4 КРИТЕРИИ ВЫБОРА ЭЛЕМЕНТОВ ЗАЩИТЫ, ПРИГОДНЫХ ДЛЯ КОМПЬЮТЕРНОЙ ВЕРИФИКАЦИИ

Если государство выдачи рассматривает возможность внесения в свои МСПД элементов защиты, пригодных для компьютерной аутентификации, или принимающее государство планирует установить считывающие системы, обеспечивающие компьютерную 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 компьютерной аутентификации, например общие характеристики предотвращения копирования или визуальная проверка;

- возможность персонализации (т. е. придание индивидуального характера) элемента, пригодного для компьютерной 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. ПРЕДОТВРАЩЕНИЕ МОШЕННИЧЕСТВА, СВЯЗАННОГО С ПРОЦЕССОМ ВЫДАЧИ (ИНФОРМАЦИОННОЕ)

С.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.

С.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 заявитель обращается за получением паспорта под собственным именем, 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.

С.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 поддаваться 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 номер и храниться в запечатом 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.

С.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 (сотрудники, выдающие разрешения [СВР]), при рассмотрении подозрительных заявлений. СБМ должны проводить регулярное обучение СВР 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.

Заявителю, обратившемуся за МСПД, который ранее такого документа не имел, следует предложить лично явиться в центр по выдаче МСПД с необходимыми исходными документами для беседы с СВР 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 с персональной информацией, 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 сотрудника СВР, 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 ИНТЕРПОЛ. Доступ в такую базу данных предоставляется всем участвующим странам и может использоваться для составления списков особого внимания.

С.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 D К ЧАСТИ 2. ОСНОВНЫЕ МОМЕНТЫ, СВЯЗАННЫЕ С БАЗОЙ ДАННЫХ ASF/SLTD (ИНФОРМАЦИОННОЕ)

<p>Законодательные требования</p>	<p>Прежде чем вводить практику представления информации в базу данных ИНТЕРПОЛ 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:</p> <ol style="list-style-type: none"> 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
<p>Элементы данных</p>	<p>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:</p> <ol style="list-style-type: none"> 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). <p>*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</p>
<p>Сбор информации</p>	<p>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</p>

<p>Своевременное и точное представление данных</p>	<p>Эффективность базы данных ASF/SLTD ИНТЕРПОЛ 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.</p> <p>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.</p> <p>Государствам следует организовать круглосуточную службу для оперативного запроса дополнительной информации в ИНТЕРПОЛ от имени государства</p>
<p>Оптимизация национальных баз данных об утерянных, похищенных и аннулированных проездных документах</p>	<p>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</p>

ISBN 978-92-9249-937-2



9

789292

499372