Doc 9855
AN/459

Рекомендации по использованию публичного Интернета в авиационных целях

Утверждено Генеральным секретарем
и опубликовано с его санкции

Издание первое — 2005

Международная организация гражданской авиации

Опубликовано Международной организацией гражданской авиации отдельными изданиями на русском, английском, арабском, испанском, китайском и французском языках. Всю корреспонденцию, за исключением заказов и подписки, следует направлять в адрес Генерального секретаря ИКАО.

Заказы на данное издание направлять по одному из следующих нижеприведенных адресов, вместе с соответствующим денежным переводом (тратта, чек или банковское поручение) в долл. США или в валюте страны, в которой размещается заказ. Заказы с оплатой кредитными карточками ("Виза", "Мастеркард" или "Американ экспресс") направлять в адрес Штаб-квартиры ИКАО.

International Civil Aviation Organization. Attention: Document Sales Unit, 999 University Street, Montreal, Quebec, Canada H3C 5H7
Telephone: +1 (514) 954-8022; Facsimile: + 1 (514) 954-6769; Sitatex: YULCAYA; E-mail: sales@icao.int; World Wide Web: http://www.icao.int

China. Glory Master International Limited, Room 434B, Hongshen Trade Centre, 428 Dong Fang Road, Pudong, Shanghai 200120
Telephone: +86 137 0177 4638, Facsimile: +86 21 5888 1629; E-mail glorymaster@online.sh.cn

Egypt. ICAO Regional Director, Middle East Office, Egyptian Civil Aviation Complex, Cairo Airport Road, Heliopolis, Cairo 11776
Telephone: +20 (2) 267 4840; Facsimile: +20 (2) 267 4843; Sitatex: CAICAYA; E-mail: icao@idsc.net.eg

France. Directeur régional de l'OACI, Bureau Europe et Atlantique Nord, 3 *bis*, villa Émile-Bergerat, 92522 Neuilly-sur-Seine (Cedex)
Téléphone: +33 (1) 46 41 85 85; Fax: +33 (1) 46 41 85 00; Sitatex: PAREUYA; Courriel: icaoeurnat@paris.icao.int

Germany. UNO-Verlag CmbH, Am Hofgarten 10, D-53113 Boon
Telephone: +49 (0) 2 28-9 49 0 20; Facsimile: + 49 (0) 2 28-9 49 02 22; E-mail: info@uno-verlag.de; World Wide Web: http://www.uno-verlag.de

India. Oxford Book and Stationery Co., Scindia House, New Delhi 110001 *or* 17 Park Street, Calcutta 700016
Telephone: +91 (11) 331-5896; Facsimile: +91 (11) 51514284

India. Sterling Book House — SBH, 181, Dr. D. N. Road, Fort, Bombay 400001
Telephone: +91 (22) 2261 2521, 2265 9599; Facsimile: +91 (22) 2262 3551; E-mail: sbh@vsnl.com

Japan. Japan Civil Aviation Promotion Foundation, 15-12, 1-chome, Toranomon, Minato-Ku, Tokyo
Telephone: +81 (3) 3503-2686; Facsimile: +81 (3) 3503-2689

Kenya. ICAO Regional Director, Eastern and Southern African Office, United Nations Accommodation, P.O.Box 46294, Nairobi
Telephone: +254 (20) 622 395; Facsimile: +254 (20) 623 028; Sitatex: NBOCAYA; E-mail: icao@ icao.unon.org

Mexico. Director Regional de la OACI, Oficina Norteamérica, Centroamérica y Caribe, Av. Presidente Masaryk No. 29, 3er. piso,
Col. Chapultepec Morales, C.P. 11570, México, D.F.
Teléfono: +52 (55) 52 50 32 11; Facsímile: +52 (55) 52 03 27 57; Correo-e: icao _nacc@mexico.icao.int

Nigeria. Landover Company, P.O. Box 3165, Ikeja, Lagos
Telephone: +234 (1) 4979780; Facsimile: +234 (1) 4979788; Sitatex: LOSLORK; E-mail: aviation@landovercompany.com

Peru. Director Regional de la OACI, Oficina Sudamérica, Apartado 4127, Lima 100
Teléfono: +51 (1) 575 1646; Facsímile: +51 (1) 575 0974; Sitatex: LIMCAYA; Correo-e: mail@lima.icao.int

Russian Federation. Aviaizdat, 48, Ivan Franco Street, Moscow 121351, Telephone: +7 (095) 417-0405; Facsímile: +7 (095) 417-0254

Senegal. Directeur régional de l'OACI, Bureau Afrique occidentale et centrale, Boîte postale 2356, Dakar
Téléphone: +221 839 9393; Fax: +221 823 6926; Sitatex: DKRCAYA; Courriel: icaodkr@ icao.sn

Slovakia. Air Traffic Services of the Slovak Republic, Levoté prevádzkové sluzby Slovenskej Republiky, State Interprise, Letisco M.R. Stefánika,
823 07 Bratislava 21, Telephone: +421 (7) 4857 1111; Facsimile: +421 (7) 4857 2105

South Africa. Avex Air Training (Pty) Ltd., Private Bag X102, Halfway House, 1685, Johannesburg
Telephone: +27 (11) 315-0003/4; Facsimile: +27 (11) 805-3649; E-mail: avex@iafrica.com

Spain. A.E.N.A. - Aeropuertos Españoles y Navegación Aérea, Calle Juan Ignacio Luca de Tena, 14, Planta Tercera, Despacho 3.11,
28027 Madrid; Teléfono: +34 (91) 321-3148; Facsímile: +34 (91) 321-3157; Correo e: sscc.ventasoaci@aena.es

Switzerland. Adeco-Editions van Diermen, Attn: Mr. Martin Richard Van Diermen, Chemin du Lacuez 41, CH-1807 Blonay
Telephone: +41 021 943 2673; Facsimile: +41 021 943 3605; E-mail: mvandiermen@adeco.org

Thailand. ICAO Regional Director, Asia and Pacific Office, P.O. Box 11, Samyaek Ladprao, Bangkok 10901
Telephone: +66 (2) 537 8189; Facsimile: +66 (2) 537 8199; Sitatex: BKKCAYA; E-mail: icao_apac@bangkok.icao.int

United Kingdom. Airplan Flight Equipment Ltd. (AFE), 1a Ringway Trading Estate, Shadowmoss Road, Manchester M22 5LH
Telephone: +44 161 499 0023; Facsimile: +44 161 499 0298; E-mail: enquiries@afeonline.com;
World Wide Web: http://www.afeonline.com

2/05

Каталог изданий и аудиовизуальных учебных средств ИКАО

Ежегодное издание с перечнем всех имеющихся в настоящее время публикаций и аудиовизуальных учебных средств. В ежемесячных дополнениях сообщается о новых публикациях, аудиовизуальных учебных средствах, поправках, дополнениях, повторных изданиях и т. п.

Рассылаются бесплатно по запросу, который следует направлять в Сектор продажи документов ИКАО.

Doc 9855
AN/459

Рекомендации по использованию публичного Интернета в авиационных целях

Утверждено Генеральным секретарем и опубликовано с его санкции

Издание первое — 2005

Международная организация гражданской авиации

ПОПРАВКИ

Об издании поправок регулярно сообщается в *"Журнале ИКАО"* и в ежемесячном *дополнении к Каталогу изданий и аудиовизуальных учебных средств ИКАО*, которыми рекомендуется пользоваться для справок. Ниже приводится форма для регистрации поправок.

РЕГИСТРАЦИЯ ПОПРАВОК И ИСПРАВЛЕНИЙ

ПОПРАВКИ			
№	Дата выпуска	Дата внесения	Кем внесено

ИСПРАВЛЕНИЯ			
№	Дата выпуска	Дата внесения	Кем внесено

ПРЕДИСЛОВИЕ

Настоящий документ подготовлен при содействии Исследовательской группы по использованию публичного Интернета в авиационных целях (AUPISG) для оказания помощи государствам в условиях расширения использования публичного Интернета (далее "Интернет") для некоторых авиационных видов применения.

В настоящем документе содержатся рекомендации по использованию Интернета в качестве средства связи для некритичных по времени авиационных видов применения "земля – земля". Термин "некритичный по времени" означает, что информация, передаваемая по Интернету, не оказывает непосредственного влияния на активный полет. Определенное внимание также уделено материалу, который может оказать помощь государствам при аккредитации поставщиков авиационной информации по Интернету.

Как представляется, выполнение рекомендаций, изложенных в настоящем документе, позволит исключить или свести до минимума возможность принятия государствами и международными организациями, принимающими решение об использовании Интернета для некоторых эксплуатационных видов применения, несовместимых/отличающихся процедур.

В этих рекомендациях содержится информация о наилучшей практике высокого уровня, а не подробные технические требования; они основаны на использовании проверенных эксплуатационных процедур и серийных продуктов (COTS). Следует отметить, что приведенные примеры могут быстро устареть, поскольку технология Интернета развивается быстрыми темпами. На момент реализации рекомендуется использовать наиболее подходящее решение. Кроме того, рекомендации не охватывают те услуги, которые обычно предоставляются по специализированным инфраструктурам связи, например по выделенным линиям связи или интрасетям, где может использоваться технология, основанная на Интернете.

В документе содержится краткая историческая справка, изложены общие соображения, касающиеся всех основанных на Интернете аэронавигационных служб, и соображения в отношении особых видов обслуживания.

Наконец, следует иметь в виду, что положения настоящего документа не отражает позицию ИКАО о том, где и когда следует или не следует использовать Интернет в авиационных целях. На более позднем этапе ИКАО может выработать такую позицию, если в этом возникнет необходимость.

ОГЛАВЛЕНИЕ

ПОЯСНЕНИЕ ТЕРМИНОВ

Примечание. Приводимые ниже пояснения призваны способствовать пониманию терминов в контексте их использования в настоящем документе.

Браузер. Программные средства, обеспечивающие загрузку и визуализацию web-страницы. Браузер интерпретирует код HTML или XML (см. ниже) из файлов web-страниц, выполняет встроенные сценарии и программы, обеспечивая там, где это необходимо, кодирование/декодирование с целью защиты информации, отображает графики (за исключением только текстовых браузеров), проигрывает музыку и видеозаписи и обеспечивает установление связи с соответствующими страницами.

Брандмауэр. Устройство, обеспечивающее защиту ресурсов частной сети от пользователей из других сетей. В принципе, брандмауэр, работая в тесном взаимодействии с маршрутизатором, фильтрует все сетевые пакеты для определения того, следует ли их направлять к месту их назначения. Брандмауэр часто устанавливается отдельно от остальной сети, с тем чтобы ни один входящий запрос не мог быть неопределенно направлен к ресурсам частной сети.

Виртуальная частная сеть (VPN). Сеть, которая в публичной сети (например, Интернет) использует защищенный, аутентифицированный "туннель". Конечные точки туннеля VPN аутентифицируются, как правило, с использованием однозначной аутентификации. Содержание отделяется от публичной сети посредством кодирования.

Всемирная паутина (WWW). Протокол Интернета, использующий язык HTML, гипертекст и гиперсреду для создания страниц, связанных с другими страницами. Страницы WWW могут включать в себя графики, аудио- и видеозаписи, и также текстовую информацию.

Вторжения, вызывающие отказ в обслуживании законных пользователей (DoS). Попытки подавить сайт Интернета или сервер. Результат вторжения заключается в том, что законные пользователи конкурируют с нападающей стороной за получение доступа к тем же ресурсам. Это будет приводить к блокировке законных пользователей или разрушению инфраструктуры в целом и остановке ее функционирования. Распределенные DoS (DDoS) вторжения координируются из различных мест и бороться с ними может быть намного труднее. Часто DoS используется нападающей стороной в качестве отвлекающего маневра, с тем чтобы скрыть попытки входа в систему.

Гиперсреда. Аналогична гипертексту, однако включает другие взаимосвязанные мультимедийные средства, такие как графики, звуко- и видеозаписи.

Гипертекст. Разновидность текста, включающего в себя визуальные ссылки на другие страницы текста или среду, доступ к которым обеспечивается посредством нажатия на ссылки или выбора их.

Демилитаризованная зона (DMZ). Сеть, расположенная между двумя сетями. Она не является ни частью внутренней сети, ни непосредственной частью Интернета. Инфраструктура, размещенная в пределах DMZ, в определенной степени защищена от внешней атаки, однако она по-прежнему считается уязвимой.

Интегрированная операционная система (OS). Элемент или функция, встроенная в операционную систему компьютера (например, путеводитель по сети Интернет (Internet Explorer) в Windows.

Интернет. Система взаимосвязанных в глобальном масштабе компьютерных сетей, использующая протокол управления передачей/протокол Интернет (TCP/IP) для передачи и восстановления информации.

Интрасеть. Частная сеть в рамках одной организации, которая использует TCP/IP для передачи и восстановления информации. Как правило, сайты в рамках Интрасети для Интернета закрыты и доступ к ним обеспечивается только членам Организации.

Инфраструктура открытых ключей (PKI). Система цифровых сертификатов, сертифицирующих полномочных органов и других регистрационных полномочных органов, которая проверяет и аутентифицирует истинность каждой стороны, участвующей в транзакции Интернет. В настоящее время PKI разрабатываются и какой-либо единой PKI или даже единого согласованного стандарта для определения PKI не существует.

Маршрутизатор. Устройство, определяющее следующую точку сети, в которую должен быть направлен пакет данных на пути к месту его назначения. Маршрутизатор подключается как минимум к двум сетям и определяет, по какому пути отправлять дальше пакет данных, основываясь на своей текущей оценке состояния сетей, к которым он подключен. Маршрутизаторы создают или ведут таблицу располагаемых маршрутов и используют эту информацию для определения наилучшего маршрута для взятого пакета данных.

Матрица независимых дисковых накопителей с избыточностью (матрица изначально независимых дисковых накопителей с избыточностью) (RAID). Метод хранения аналогичных данных в различных местах (поэтому с избыточностью), обеспечивающий возможность сбалансированного перекрытия операций ввода/вывода, в результате чего улучшаются характеристики. Избыточность увеличивает среднюю наработку на отказ (MTBF), повышая тем самым отказоустойчивость. Для операционной системы RAID является единственным логическим жестким диском.

Однозначная аутентификация. Двухэлементный метод аутентификации, основанный на какой-то информации, известной пользователю (например, пароль/PIN) и на чем-то, чем располагает пользователь (например, аутентификатор). Двухуровневые мандаты обеспечивают в значительной степени более надежную аутентификацию пользователей (см. RSA SecurID).

Оценка риска. Оценка угроз системе, вероятности того, что эти угрозы будут реализованы, и оценка последствий такой реализации.

Порт. Предопределенный внутренний адрес, выполняющий функцию магистрали от конкретного приложения к транспортному уровню (TCP) или наоборот.

Поставщик авиационных услуг Интернет (IASP). Аккредитованная компания, предоставляющая аэронавигационную информацию с использованием Интернет в качестве средства связи.

Поставщик услуг Интернет (ISP). Компания, предоставляющая доступ к Интернету и инфраструктуре связи.

Протокол (защищенный) передачи гипертекстов (https). Стандартный механизм обмена закодированной информацией в Web. HTTP функционирует на основе SSL.

Протокол защищенных сокетов (SSL). Метод кодированной связи по Интернету. SSL обеспечивает передачу неизмененной информации лишь предполагаемому получателю. Часто

технология SSL используется при оплате покупок в режиме "онлайн" или на банковских сайтах в целях защиты кредитных карточек или другой конфиденциальной информации.

Протокол Интернет (IP). Протокол, используемый для маршрутизации пакетов данных от источника до места назначения в условиях Интернет (взаимосвязанных сетей).

Протокол управления передачей (TCP). Протокол связи (используемый в Интернете), обеспечивающий надежную связь между главными ЭВМ в сети с пакетной коммутацией данных или соединение таких сетей.

Расширяемая спецификация языка (язык XML). Один из этапов эволюции web-форматов данных (помимо языка HTML).

Сервер. Компьютер или устройство в сети, обеспечивающее доставку сетевых ресурсов или управление ими. Например, файловый сервер представляет собой компьютер и запоминающее устройство, призванное хранить файлы. Любой пользователь сети может хранить файлы в сервере. Сервер печати представляет собой компьютер, управляющий одним или несколькими печатающими устройствами, а сетевой сервер представляет собой компьютер, управляющий сетевым трафиком. Сервер базы данных представляет собой компьютерную систему, которая обрабатывает запросы к базе данных. Часто серверы являются выделенными; это означает, что они не выполняют каких-либо других задач, помимо своих серверных задач. Однако в мультипроцессорных операционных системах один компьютер может одновременно выполнять несколько программ. В этом случае под сервером может пониматься программа, управляющая ресурсами, а не компьютером в целом.

Унифицированный указатель информационного ресурса (URL). Указатель местоположения ресурса в Интернете. Он может быть введен в окно местоположения браузера для подключения к желаемой ячейке (например, web-сайт).

Цифровой сертификат. Электронные средства проверки мандата пользователя при выполнении деловых или других операций на Web. Сертификат выдается сертифицирующим полномочным органом (CA). В нем содержится имя пользователя, серийный номер, дата истечения срока действия, копия открытого ключа держателя сертификата (используется для шифровки и дешифровки сообщений и цифровых подписей) и цифровая подпись полномочного органа, выдающего сертификат, с тем чтобы получатель мог проверить подлинность сертификата. Некоторые цифровые сертификаты отвечают требованиям рекомендации X.509 секции стандартизации электросвязи Международного союза электросвязи. Цифровые сертификаты могут храниться в системных реестрах, с тем чтобы аутентифицированные пользователи могли просматривать открытые ключи других пользователей.

Экстрасеть. Сеть, дополняющая закрытую интрасеть посредством предоставления доступа клиентам, поставщикам, субподрядчикам и другим пользователям за пределами Организации, которым необходимо получить от Организации выборочную информацию. Она недоступна для всех пользователей Интернета.

Электронная почта (email). Один из стандартных протоколов Интернета, позволяющий пользователям, имеющим различные компьютеры и операционные системы, обмениваться информацией друг с другом. Email позволяет пользователю вести переписку с одним или несколькими адресатами. Почта принимается и хранится почтовым сервером в пределах Организации или поставщиком Интернет-сервиса до тех пор, пока получатель не войдет в систему и не заберет почту.

Язык разметки гипертекста (язык HTML). Система кодирования, используемая для создания web-страницы (WWW). Страница, записанная с помощью языка HTML, представляет собой текстовой файл, включающий в себя дескрипторы в угловых скобках, которые управляют видами

и размерами шрифтов, вставкой графиков, форматом таблиц и фреймов, введением абзацев, вызовами коротких работоспособных программ и гипертекстовыми ссылками на другие страницы.

RSA. Система кодирования и аутентификации Интернета, использующая алгоритм, разработанный Роном Ривестом, Ади Шамиром и Леонардом Адлеманом в 1977 году. Этой системой владеет компания RSA Security, которая лицензирует технологии описания алгоритмов.

SecurID. Разработанный RSA метод SecurID® является механизмом "однозначной идентификации", обуславливающей необходимость использования маркера и личного идентификационного номера (PIN).

Web-сайт. Одна или несколько соединенных web-страниц, имеющих общую принадлежность, управление или тему.

_____

Глава 1

ИСХОДНАЯ ИНФОРМАЦИЯ

1.1 Слово "Интернет" ("Internet") является сокращенным вариантом фразы "взаимосвязанная сеть" ("interconnected network"). Однако то, что под этим обычно понимается, и то, что является предметом настоящего документа, т. е. "публичный Интернет" (или просто "Интернет"), представляет собой слабо организованное международное сотрудничество автономных взаимосвязанных сетей, которые для межсетевого обмена используют протокол управления передачей/протокол Интернет (TCP/IP). Тесно связанный с ним термин "Всемирная паутина (WWW)" относится к глобальной сети серверов (программные средства, установленные в компьютерах, которые подключены к Интернету), которые обеспечивают возможность смешения и совместной обработки текстовых, графических, аудио- и видеофайлов и ссылок (активные соединения с другими web-ячейками или ресурсами).

1.2 Начало Интернету положили проводившиеся в середине 1960-х гг. в Соединенных Штатах Америки научные исследования, направленные на создание защищенной сети вычислительных машин. В результате этой деятельности была создана сеть Управления перспективных исследовательских программ (подразделение министерства обороны) (ARPANET), функционирование которой началось с соединения компьютеров нескольких университетов в Соединенных Штатах Америки в 1969 г. Несмотря на то, что первый обмен электронной почтой по сети ARPANET был осуществлен в 1972 г., многие считают 1 января 1983 г. "официальным" началом функционирования Интернета, поскольку в этот день сеть перешла на использование стека протоколов TCP/IP, разработанных в середине 1970-х гг. и принятых правительством Соединенных Штатов Америки в 1978 г. Постепенно к сети ARPANET подключились другие сети, и Интернет начал расширяться. Сама ARPANET прекратила свое существование в 1989 г., однако Интернет продолжил свое бурное развитие в связи с повышением к нему интереса и появлением мощных персональных компьютеров, линий передачи данных, таких, как оптико-волоконные, и локальные/широкомасштабные сети. В 1995 г. управление трафиком Интернет было передано коммерческому сектору.

1.3 Как правило, пользователи арендуют обслуживание в Интернете у коммерческих поставщиков услуг Интернет (ISP). Постоянно возрастающий спрос на Интернет, свидетельством которого является небывалый рост количества пользователей (с 200 млн. в 1998 г. до почти 500 млн. в начале 2002 г.), служит наилучшим стимулом для поставщиков услуг к постоянному повышению производительности/улучшению характеристик своих систем и предоставлению более качественного конкурентоспособного обслуживания. В этой связи можно сделать вывод о том, что в целом в тех случаях, когда обслуживание Интернет предоставляется на коммерческой основе (и разрешена конкуренция), вероятность получения приемлемого уровня обслуживания со временем увеличивается.

1.4 Традиционно сообщество гражданской авиации предпочитает иметь свои собственные специализированные системы, что обусловлено соображениями надежности, целостности, безопасности и их влиянием на безопасность полетов. Это обуславливает нежелание многих авиационных специалистов официально закреплять использование Интернета, который не находится под контролем какой-либо авиационной организации. Тем не менее учитывая широкие возможности его применения, доступность (особенно для широкой публики), обоснованную стоимость, скорость и простоту использования, некоторые государства приступили к использованию Интернета в определенных областях (например, метеорология и службы аэронавигационной

информации). Кроме того, в некоторых регионах мира, в которых отсутствуют адекватные специализированные системы авиационной связи или их создание экономически необоснованно в связи с очень низким объемом трафика, Интернет используется в качестве средства связи "земля – земля".

1.5 ИКАО активно использует предоставляемое Интернетом обслуживание (главным образом, электронную почту и доступ к web) для рассылки информации, документации и административной связи. Простота доступа/использования и высокий уровень целостности этих видов обслуживания в значительной степени расширили общие возможности процесса связи Организации. Однако Организация осторожно подходит к идее использования Интернета для видов применения, связанных с безопасностью полетов. В основном это обусловлено тем, что Организация прилагает значительные усилия по стандартизации систем связи, которые обеспечивают строгое выполнение эксплуатационных требований, касающихся безопасности полетов и авиационной безопасности, предполагая, что государства будут выполнять их в соответствии с региональными аэронавигационными планами.

1.6 В области связи "земля – земля" для замены устаревающей сети авиационной фиксированной электросвязи (AFTN) ИКАО разработала современную систему обработки сообщений ОВД (AMHS), являющуюся компонентом связи "земля – земля" сети авиационной электросвязи (ATN). Аналогично AFTN (и общей сети обмена данными ИКАО (CIDIN)) AMHS является специализированной системой, обеспечивающей виды применения, связанные с безопасностью аэронавигации. Однако на данный момент масштабы внедрения этой системы носят лишь очень ограниченный характер, поэтому на создание истинно глобальной авиационной системы обмена сообщениями уйдут многие годы. Между тем возникла Интернет, ставшая популярной средой, позволяющей обеспечивать удовлетворение потребностей авиационного сообщества в обмене сообщениями. Кроме того, в отличие от AFTN, CIDIN и AMHS, которые являются закрытыми сетями, т. е. доступными только для санкционированных авиационных пользователей, Интернет открыта для широкой публики, поэтому пилоты или другие текущие и потенциальные пользователи аэронавигационной информации могут иметь доступ к банкам данных и, при необходимости, взаимодействовать с соответствующими авиационными полномочными органами из дома или из любого другого места, где имеется соответствующее соединение. Поэтому Интернет выгодно дополняет используемый в настоящее время официальный порядок ведения авиационной связи.

1.7 Учитывая вышеизложенное и выполняя рекомендации региональных групп планирования и осуществления проекта, а также недавно проходившего Специализированного совещания по метеорологии (MET) (2002), ИКАО инициировала проведение исследований, касающихся использования публичного Интернета, для всех категорий авиационных видов применения (пока лишь в контексте связи "земля – земля"), надлежащим образом учитывая при этом соображения надежности, целостности, доступности и безопасности. Рекомендации, содержащиеся в настоящем документе, являются первыми результатами этих исследований.

1.8 В настоящем документе содержатся рекомендации относительно использования Интернета для некритичных по времени авиационных видов применения "земля – земля". Как правило, эти виды применения охватывают рассылку/обмен информацией между:

a) полномочным органом государства и пользователями (в пределах государства);

b) двумя или несколькими государственными полномочными органами;

c) третьей стороной (обычно коммерческой организацией) и пользователем (в том же или другом государстве(ах)).

1.9 Пользователи аэронавигационной информации должны иметь гарантии в том, что используемое ими обслуживание предоставляется источником, утвержденным государством, и что оно надлежащим образом организовано и обеспечивает целостную связь. Данная проблема приобретает еще более сложный характер, когда информация передается по Интернету. Это обуславливает необходимость задействования двух процессов аккредитации, один из которых связан с источниками аэронавигационной информации, а второй – с передачей этой аэронавигационной информации по Интернету. Рекомендации, изложенные в настоящем документе, в основном касаются предоставления аэронавигационной информации по Интернету.

_____

Глава 2

ОТВЕТСТВЕННОСТЬ ГОСУДАРСТВ

2.1 ОБЩИЕ ПОЛОЖЕНИЯ

2.1.1 В целом использование Интернета в качестве средства предоставления или обмена оперативной информацией не освобождает государства от их обязательств и ответственности за внедрение авиационной фиксированной службы (AFS) и других средств и служб, определенных региональным соглашением и документально закрепленных в региональных аэронавигационных планах ИКАО.

2.1.2 Кроме того, аналогично любому другому средству или службе использование Интернета для передачи данных и обмена сообщениями между государствами должно осуществляться на основе двусторонних, многосторонних или региональных соглашений и надлежащим образом отражаться в региональных аэронавигационных планах.

2.1.3 Государствам, которые допускают использование Интернета, следует:

a) аккредитовать организации (далее именуемые поставщиками авиационных услуг Интернет (IASP)), которые будут обеспечивать предоставление/обмен информацией, основанные на Интернете;

b) обеспечивать наличие соответствующих информационных технологий и опыта в области информационной безопасности в целях осуществления контроля за процессом аккредитации, описание которого приводится ниже.

2.1.4 Для целей аккредитации/осуществления контроля за IASP государствам следует:

a) публиковать и постоянно обновлять перечень аккредитованных IASP с подробной информацией о предоставляемом обслуживании и датой истечения срока аккредитации;

b) требовать от IASP информировать пользователей о любых ограничениях, связанных с предоставлением обслуживания. Кроме того, IASP должен дать точное определение аварийного или резервного обслуживания. Например, в случае отказа системы Интернета в ходе представления плана полета пользователь должен оповестить службу воздушного движения или службу обеспечения полетов и представить информацию с использованием обычных средств;

c) требовать от IASP уменьшать вероятность случайного представления неправильной информации за счет использования хорошо спроектированных интерфейсов пользователей и обеспечивать соответствующую подготовку пользователей;

d) проводить повторную аккредитацию IASP не менее чем через три года или в тех случаях, когда IASP вносит крупные изменения в свою организационную структуру или инфраструктуру.

2.2 ПРИМЕНИМЫЕ ПОЛОЖЕНИЯ ИКАО

2.2.1 В главе 3 Приложения 15 *"Службы аэронавигационной информации"* конкретно определяется ответственность государств в отношении предоставления аэронавигационной информации и функций службы аэронавигационной информации. Содержащиеся в Приложении положения касаются создания системы качества обмена аэронавигационной информацией, авторских прав и т. д. В основе подхода, используемого в Приложении 15, лежит статья 28 Конвенции о международной гражданской авиации, согласно которой каждое государство обязуется предоставлять всю без исключения информацию, имеющую отношение и необходимую для производства полетов воздушных судов, занятых в международной гражданской авиации, в пределах его территории, а также в районах за пределами его территории, где данное государство несет ответственность за обслуживание воздушного движения.

2.2.2 Особо следует отметить раздел 3.1 главы 3 Приложения 15, в котором говорится о том, что соответствующее государство несет ответственность за публикуемую информацию в тех случаях, когда оно предоставляет обслуживание аэронавигационной информацией, предоставляет это обслуживание совместно с другим государством или передает полномочия на предоставление обслуживания неправительственному учреждению. Соответственно в случае использования Интернета государствами в качестве дополнительного средства распространения своей аэронавигационной информации государствам следует обеспечить наличие соответствующей системы качества и процедур в целях подкрепления информации, предоставляемой в рамках своих обязанностей, и аккредитацию Интернет-сайтов, на которых такая информация размещается.

2.2.3 В п. 2.2 главы 2 Приложения 3 *"Метеорологическое обеспечение международной аэронавигации"* конкретно определяются обязанности государств в отношении предоставления, гарантии качества и использования метеорологической информации.

2.2.4 В п. 1.3 главы 1 Приложения 4 *"Аэронавигационные карты"* конкретно определяются обязанности государств в отношении предоставления аэронавигационных карт, а в п. 2.17 главы 2 содержится требование относительно управления качеством аэронавигационных данных на картах.

2.3 АККРЕДИТАЦИЯ IASP

2.3.1 Аккредитация IASP отличается от аккредитации источников аэронавигационной информации. Аккредитация источников данных, включая сбор, форматирование и актуальность данных, является необходимым условием аккредитации IASP и в настоящем документе не рассматривается.

2.3.2 Для того чтобы информация, предоставляемая по Интернету, отвечала наилучшей используемой практике с точки зрения обеспечения ее конфиденциальности, целостности, аутентичности и готовности, необходимо разработать процедуру аккредитации IASP, предоставляющего информацию и услуги по сети Интернет. В последующих пунктах приводятся соответствующие рекомендации.

2.3.3 Желательно, чтобы государства требовали от IASP выполнения процедур, приводимых на рис. 2-1. Отдельно государства могут дополнить эти процедуры.

2.3.4 В приводимых ниже пунктах приводится описание основных элементов типового процесса аккредитации, описание которого иллюстрируется на рис. 2-1.

План обслуживания

2.3.5 IASP должен представить описание услуг, подлежащих предоставлению по Интернету. Описание услуг должно включать в себя следующую информацию:

a) тип услуги (услуг). Типовые услуги охватывают службу аэронавигационной информации (САИ), МЕТ, связь типа AFTN и представление планов полета, но не ограничиваются ими;

b) район применимости (например, локальная, региональная или глобальная);

c) целевой рынок (например, авиация общего назначения, деловая авиация, коммерческая авиация).

Наличие плана обслуживания является необходимым условием процесса управления риском.

Оценка риска

2.3.6 После разработки плана обслуживания IASP необходимо рассмотреть вопрос о рисках, связанных с предоставлением такого обслуживания в Интернете. Рекомендации по оценке риска содержатся в главе 3.

Техническое описание системы

2.3.7 Определив риски, связанные с предоставлением обслуживания, IASP должен спроектировать свою систему таким образом, чтобы уменьшить эти риски до приемлемого уровня с учетом обслуживания, которое он планирует предоставлять. Рекомендации по стратегии снижения риска приводятся в главе 3.

Планирование предоставления обслуживания

2.3.8 Завершив подготовку плана обслуживания, проведение оценки риска и проектирование системы, IASP необходимо рассмотреть вопрос о том, каким образом будет обеспечиваться требуемый уровень качества обслуживания.

Техническое обслуживание системы

2.3.9 IASP необходимо иметь план технического обслуживания, с тем чтобы обеспечить непрерывное функционирование системы, отвечающее типу обслуживания, предлагаемого авиационным пользователям. Этот план должен предусматривать проведение регулярного профилактического технического обслуживания аппаратных и программных средств. Особое значение имеет регулярное обновление программных средств, обеспечивающих безопасность. IASP также необходимо определить перечень подлежащих хранению запасных частей к оборудованию, с тем чтобы обеспечить соблюдение требований в отношении "времени ремонта".

Соглашение об обслуживании с поставщиком услуг Интернет (ISP)

2.3.10 IASP должен иметь соглашение об обслуживании со своим ISP, определяющее требования к готовности обслуживания, включая время ремонта, представление информации об отказах, увеличение количества контактных точек и подготовку ежемесячных отчетов о функционировании обслуживания.

Архивирование данных и транзакций

2.3.11 IASP необходимо обеспечивать соответствие изложенным в Приложениях ИКАО требованиям в отношении управления данными применительно к предоставляемым услугам. Это предусматривает регистрацию информации о предоставляемых данных в любой момент времени и регистрацию транзакций, подтверждающую предоставляющие данные конкретным пользователям.

Примечание. В случае ведения регистрационных журналов приложений, сети и/или доступа, период хранения информации будет определяться государствами. 30 календарных дней (согласно тому II "Правила связи, включая правила, имеющие статус PANS" *Приложения 10* "Авиационная электросвязь"*) для хранения сообщений AFTN в целом считается приемлемым сроком. Однако в случае получения уведомления об авиационном происшествии, инциденте или опаздывающем воздушном судне или по запросу государств IASP должен хранить данные, имеющие отношение к этому событию, в течение неограниченного периода времени или до тех пор, пока удаление этих данных не будет санкционировано законом. IASP должен предоставлять такие данные по запросу государства в виде удобочитаемой, поддающейся проверке и заверенной копии.*

Запланированное/незапланированное отключение системы

2.3.12 IASP должен иметь план на случай устранения перерывов в обслуживании.

Устранение аварий

2.3.13 IASP должен иметь план устранения аварий, масштабы которого будут зависеть от типа предоставляемых им услуг.

Мониторинг действующей системы

2.3.14 IASP следует разработать ряд критериев характеристик и целевых показателей, которые будут позволять государственному аккредитующему полномочному органу определять, соответствуют ли характеристики обслуживания целевым показателям.

Выдача лицензий на обслуживание

2.3.15 Аккредитующий полномочный орган государства должен провести оценку предусмотренных конструкцией системы IASP процессов и планирования в ходе обслуживания для определения возможности выполнения IASP своего плана обслуживания и убедиться в наличии стратегии смягчения последствий, обеспечивающей снижение до приемлемого уровня рисков, определенных в ходе оценки риска.

2.3.16 До первоначальной аккредитации государства могут потребовать продемонстрировать предлагаемое в Интернете обслуживание с целью удостовериться в том, что система отвечает критериям характеристик.

2.3.17 Кроме того, государства могут предложить IASP провести тщательную проверку системы с привлечением соответствующей компании, специализирующейся на оценке безопасности информационных технологий. Испытания должны предусматривать "проверку на проникновение", проверку портов и серверов и проведение необходимых проверок с целью убедиться в том, что в операционную систему и программы (включая антивирусные) внесены самые последние корректировки/ модификации, связанные с обеспечением безопасности.

2.3.18 Государствам следует аккредитовать IASP для реализации своего плана обслуживания на фиксированный период времени (например, один или два года). В тех случаях, когда IASP подает заявку на возобновление аккредитации, он должен представить подкрепляющие исторические данные о характеристиках.

2.3.19 Аккредитация не должна носить трансферабельный характер, о чем IASP следует уведомить других поставщиков web-сайтов, с которыми он взаимодействует. IASP следует четко указать государство, аккредитовавшее его предоставлять аэронавигационную информацию по Интернету, и сообщить о том, какую информацию он аккредитован представлять (с учетом плана обслуживания, который он представил аккредитующему полномочному органу государства).

2.3.20 Согласно действующим положениям ИКАО аккредитация распространяется лишь на предоставление обслуживания пользователям, осуществляющим перевозки в аккредитующее государство и из него. Государства могут согласовать вопрос об использовании договоренностей, заключенных на основе взаимности.

Предоставление/контроль обслуживания

2.3.21 IASP следует активно контролировать рабочие характеристики обслуживания, предоставляемого по Интернету. Критерии характеристик, определенные в плане обслуживания, должны контролироваться с такой периодичностью, которая позволяет оперативно корректировать не отвечающие стандартам характеристики. IASP следует вести полную регистрацию информации о контроле характеристик. Эти записи могут проверяться аккредитующим полномочным органом государства в течение периода аккредитации обслуживания и должны представляться в тех случаях, когда IASP обращается с просьбой о возобновлении аккредитации.

2.3.22 IASP следует указывать на своем web-сайте ссылки, обеспечивающие возможность обратной связи авиационных пользователей с IASP.

2.3.23 IASP следует обеспечивать согласованную линию связи с полномочным аккредитующим органом государства, позволяющую авиационным пользователям проверять статус его аккредитации и направлять отзывы или замечания непосредственно аккредитирующему полномочному органу государства.

2.4 ВЗИМАНИЕ СБОРОВ

2.4.1 Государства несут значительные расходы на предоставление аэронавигационной и/или метеорологической информации. В большинстве государств эти расходы возмещаются за счет взимания с пользователей сборов за аэронавигационное обслуживание. Однако в условиях развития современных информационных технологий и коммерциализации деятельности конечные пользователи могут принять решение о получении этих продуктов у соответствующего государства или коммерческого поставщика, являющегося третьей стороной.

2.4.2 Поэтому могут возникать обстоятельства, при которых коммерческие организации или государства стремятся получить аэронавигационную информацию и другие аэронавигационные документы у составляющего их государства. В этих случаях государство-составитель может заключить с заинтересованной стороной отдельное соглашение, касающееся условий и затрат, если таковые имеют место, которое будет распространяться на предоставление такой информации для ее последующей повторной публикации. Однако следует отметить, что Приложением 15 предусматривается безвозмездный обмен аэронавигационной информацией между Договаривающимися государствами ИКАО.

2.4.3 В целом системы взимания сборов с целью возмещения расходов должны соответствовать принципам, изложенным в документе *"Политика ИКАО в отношении аэропортовых сборов и сборов за аэронавигационное обслуживание"* (Doc 9082).

2.5 ПОКАЗАТЕЛИ ХАРАКТЕРИСТИК

2.5.1 Государству следует рассмотреть вопрос об определении обязательных показателей характеристик для каждого вида обслуживания. Эти показатели характеристик должны носить ориентированный на пользователя характер и могут определяться по согласованию с сообществом пользователей. В целом в перечень показателей характеристик целесообразно включить следующее:

a) ***Готовность.*** Доступ к обслуживанию может не обеспечиваться в течение периода, не превышающего установленный показатель в любом календарном месяце, а отказ любого индивидуального вида обслуживания не должен превышать другой установленный показатель. Это включает в себя плановое отключение в связи с техническим обслуживанием. Четко установленные периоды будут отличаться в зависимости от типа предоставляемого обслуживания.

b) ***Доступность.*** Обслуживание должно обеспечивать отображение страниц пользователем со скоростью не менее установленной. Можно ввести второй показатель, если пользователям необходимо загружать большое количество файлов данных.

Примечание. Показатели характеристик устанавливаются по усмотрению государства, однако они должны находиться в разумных пределах. Кроме того, государствам следует придерживаться принятой поставщиками политике, согласно которой предполагается, что аналогичные виды обслуживания отвечают примерно аналогичным критериям.

2.6 ИНТЕЛЛЕКТУАЛЬНАЯ СОБСТВЕННОСТЬ

2.6.1 В настоящее время в большинстве государств еще рассматривается вопрос об авторских правах при передаче информации в онлайновом режиме, однако можно предположить, что содержание, защищенное национальным законодательством, в равной степени защищено и в том случае, когда информация размещается в Интернете. Несмотря на то что материал, предоставляемый государствам по Интернету, должен, как правило, защищаться аналогично материалу печатных копий, его размещение в Интернете связано с более высокой степенью риска нарушения авторских прав. Наиболее вероятно, что нарушителем будет сторона, копирующая защищенный авторскими правами материал полностью или значительную часть его без согласия государства.

2.6.2 Некоторые государства могут принять решение об обеспечении своих авторских прав в отношении определенной информации (в письменной или электронной форме или в виде визуальной карты). В этой связи такие государства могут воспользоваться своим правом и отказать в выдаче разрешения какой-либо стороне на копирование и дальнейшую публикацию этого материала. Государства, заинтересованные в упрощении распространения своего материала, могут, в соответствии со своими обязательствами перед ИКАО и национальным законодательством, в качестве условия выдачи лицензии на копирование и дальнейшую публикацию аэронавигационной информации потребовать проведения соответствующего контроля качества и проверки какой-либо третьей стороной.

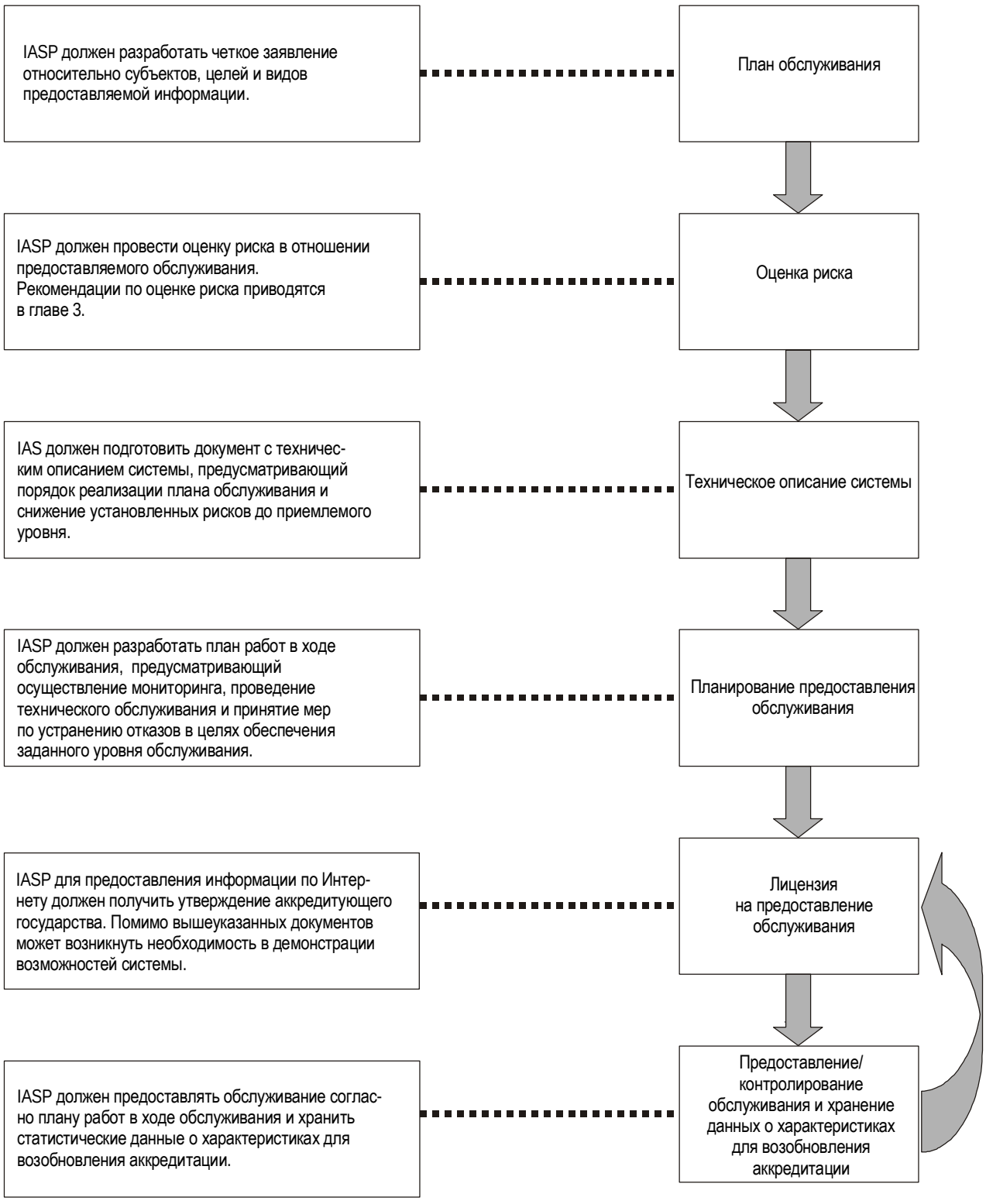

Рис. 2-1. Типовой процесс оценки IASP

2.6.3 Наиболее эффективным способом информирования пользователей о наличии авторских прав на публикацию информации в Интернете является оперативное размещение IASP на своем web-сайте уведомления об авторских правах ©, в котором четко говорится о том, что пользователь может и что не может делать с материалом, защищенным авторскими правами, и информации о юридических действиях в случае их нарушения. В добавлении к настоящей главе приводится образец используемого в одном государстве уведомления об авторских правах.

2.6.4 Еще одной возможностью снижения риска нарушения авторских прав является использование программ с защитой от копирования или программ управления цифровыми правами, таких как цифровые водяные знаки.

— — — — — — — —

Добавление к главе 2

ОБРАЗЕЦ УВЕДОМЛЕНИЯ ОБ АВТОРСКИХ ПРАВАХ

Примечание. Приводимое ниже уведомление об авторских правах используется в Австралии в отношении основанного на Интернете предоставления статической информации САИ. Оно воспроизводится с любезного разрешения Организации Airservices Australia.

Глава 3

ТЕХНИЧЕСКИЕ СООБРАЖЕНИЯ

3.1 КЛАССИФИКАЦИЯ СООБЩЕНИЙ

3.1.1 Стек протоколов Интернета гарантирует целостность сообщений, передаваемых в обычных условиях. Однако, являясь средой общественного пользования, Интернет подвержен некоторым видам вторжения, целью которых является взлом защиты (например, отказ в обслуживании или компьютерные вирусы), которые могут серьезно замедлить или даже временно прекратить его нормальное функционирование.

3.1.2 Для обеспечения аутентичности, целостности или конфиденциальности сообщений могут использоваться системы защиты информации. Однако эти меры не могут противодействовать перегрузке сети (в связи со случайным возобновлением большого объема трафика или преднамеренными помехами). Использование Интернета в авиационных целях должно ограничиваться обменом некритичными по времени сообщениями, информацией или данными. В контексте настоящего документа выражение "некритичный по времени" означает, что передаваемая информация не оказывает непосредственного влияния на активный полет.

3.1.3 В этой связи необходимо точно определить, какие аэронавигационные сообщения относятся к вышеупомянутой категории некритичных по времени. Согласно предусмотренным томом II Приложения 10 категориям сообщений и приоритетов (для передачи по сети AFTN) к некритичным по времени и, таким образом, приемлемым для передачи по сети Интернет относятся перечисленные ниже категории сообщений:

a) некоторые метеорологические (MET) сообщения (см. главу 4 настоящего руководства);

b) сообщения о регулярности полетов;

c) некоторые сообщения САИ (см. главу 5 настоящего руководства);

d) планы полетов и соответствующие сообщения (см. главу 5 настоящего руководства);

e) административные сообщения;

f) служебные сообщения (где применимо).

3.1.5 Несмотря на вышеизложенное, некоторые типы сообщений, которые считаются критичными по времени для воздушного судна в полете, могут рассматриваться в качестве некритичных по времени, когда они используются в предполетном контексте. Дополнительная информация о сообщениях MET и САИ, которые рассматриваются в качестве некритичных по времени, приводится соответственно в главах 4 и 5.

3.1.6 В тех случаях, когда критичные по времени данные предоставляются только для сведения, пользователей необходимо уведомлять о том, что если такие данные предполагается использовать в критичном по времени контексте (например, для передачи информации воздушному судну в полете), то их следует получать по соответствующим каналам.

3.2 СОДЕРЖАНИЕ

3.2.1 При разработке своего обслуживания IASP следует учитывать материал, приводимый в последующих пунктах.

3.2.2 Пользователи обслуживания должны иметь четкое представление о типах информации, предоставляемой в рамках обслуживания. Например, пользователям необходимо конкретно знать, какая информация предоставляется в рамках обслуживания, с тем чтобы обеспечить получение ими всего необходимого материала для своих операций.

3.2.3 Аккредитованные службы, предоставляющие метеорологическую информацию, должны, как минимум, обеспечивать полный набор продуктов, предусмотренных Приложением 3 (*Метеорологическое обеспечение международной аэронавигации*), и предоставляемых государством, и которые относятся к категории некритичных по времени для безопасности полетов или предполетной подготовки.

3.2.4 Пользователю должны быть четко известны источники информации, используемые аккредитуемой службой.

3.2.5 Пользователи обслуживания должны быть уверены в достоверности предоставляемой информации.

3.2.6 Историческая, неэксплуатационная или неаккредитированная информация должна быть четко помечена как таковая, если она предоставляется той же службой, которая предоставляет эксплуатационную информацию, например, информация, срок действия которой истек, архивная информация.

Примечание. Неаккредитованная информация может включать в себя дополнительную информацию или дополнительные услуги, находящиеся в стадии разработки, или их предварительные варианты.

3.2.7 Пользователь должен иметь доступ к процедурам, поясняющим порядок наилучшего использования аккредитованных услуг.

3.3 ОЦЕНКА И УПРАВЛЕНИЕ РИСКОМ

3.3.1 В рамках ранее определенного процесса аккредитации необходимо, чтобы IASP задействовал процесс постоянной оценки и управления риском в отношении обслуживания, которое он предлагает предоставлять.

3.3.2 Оценка и снижение степени риска требуют проведения анализа условий работы системы с учетом физических, логических, систематических и процедурных аспектов.

3.3.3 Для управления рисками, связанными с предоставлением основанных на Интернете авиационных услуг, необходимо иметь представление о характере этих рисков. Это обеспечивается за счет процесса оценки риска. После определения рисков могут быть предприняты соответствующие меры, обеспечивающие снижение степени риска до приемлемого уровня (т. е. уровня, приемлемого для IASP и аккредитующего государства).

3.3.4 Рекомендации настоящего раздела призваны дополнить стандартный процесс управления риском и рассмотреть вопросы, характерные для информационных технологий.

3.3.5 Дополнительная информация, имеющая отношение к настоящему разделу, содержится в документе ISO/IEC 17799:2000 *"Information Technology — Code of Practice for Information Security Management".*

3.3.6 В популярном изложении этот вопрос также рассматривается в книге Бруса Шнейера *"Secrets and Lies, Digital Security in a Networked World"* (John Wiley & Sons, Inc., 2004; ISBN: 0-471-45380-3).

3.4 ПРОЦЕСС ОЦЕНКИ РИСКА

3.4.1 Оценку риска рекомендуется проводить в следующем порядке:

a) определить ресурсы, подвергаемые угрозе, и их стоимость в рамках процесса, который иногда называют оценкой чувствительности;

b) определить чувствительность этих ресурсов;

c) определить угрозы этим ресурсам;

d) определить источники угрозы;

e) определить или оценить вероятность того, что эти угрозы будут реализованы на практике и окажут влияние на ресурсы;

f) определить последствия в случае воздействия на ресурсы;

g) на основе оценки последствий и вероятности определить риск для ресурса;

h) принять решение о необходимых корректирующих мерах, если уровень риска неприемлем (например, технические и процедурные меры безопасности);

i) провести повторную оценку риска с учетом корректирующих мер. Были ли корректирующие меры успешными/достаточными?

3.4.2 Оценку риска следует выполнять повторно с учетом любой используемой стратегии снижения риска до тех пор, пока риск не будет считаться приемлемым. Кроме того, оценку и управление риском следует осуществлять в течение всего срока предоставления обслуживания. Важно также иметь в виду, что необходимые действия по снижению риска должны соответствовать стоимости защищаемых ресурсов. В отношении каждого вида угрозы должна предоставляться следующая информация: "вид угрозы", "источник угрозы", "вероятность (реализации)", "последствия" и, наконец, "риск".

Определение ресурсов, подвергаемых угрозе

3.4.3 До рассмотрения вопроса о соответствующих мерах безопасности важно четко определить то, что подлежит защите. Во всех системах это будет охватывать:

a) саму систему, включая физическое оборудование и приложения;

b) данные в системе;

c) репутацию организации/торговой марки.

3.4.4 Важно рассмотреть вопрос о схеме сети и соответствующем потоке данных, поступающих в систему и выходящих из нее. Каждая система с внешним соединением также подвергается риску, поэтому в отношении таких систем следует проводить дополнительную оценку риска.

Определение чувствительности

3.4.5 Перечисленные ниже факторы характеризуют чувствительность типичной системы к различным вторжениям:

a) ***конфиденциальность –*** чувствительность информации или ресурсов к несанкционированному раскрытию содержания, характеризуемая соответствующим грифом или кодом, каждый из которых подразумевает степень возможного ущерба в результате несанкционированного раскрытия содержания информации;

b) ***целостность –*** чувствительность информации или ресурсов к возможному изменению или уничтожению;

c) ***готовность –*** чувствительность службы, предоставляющей информацию или обеспечивающей доступ к ресурсам, в части, касающейся ее неготовности обеспечивать эксплуатационные функции;

d) ***аутентичность –*** чувствительность службы к возможному получению доступа незарегистрированным пользователем к информации или ресурсам.

Определение угроз ресурсам

3.4.6 Для каждой категории чувствительности характерна угроза, описание которой приводится ниже:

a) ***Перехват, в результате которого возникает угроза "конфиденциальности".*** Эта угроза заключается в получении каким-либо лицом несанкционированного доступа к информации. Может ли это лицо получить доступ к конфиденциальной информации, которую этому лицу просматривать не разрешено (например, по коммерческим или юридическим соображениям)? Необходимо также рассмотреть вопрос об угрозе информации в процессе передачи.

b) ***Модификация, в результате которой возникает угроза "целостности".*** Эта угроза заключается в умышленном вмешательстве в систему или изменении данных. Например, имеет ли кто-либо возможность внесения ложных данных с целью искажения прогноза? Имеется ли возможность нарушения нормального функционирования самой системы таким образом, что она продолжает работать, однако ее выходные данные являются неправильными? Имеется ли возможность изменения данных, размещенных на платформе IASP? Имеется ли возможность нарушения целостности данных в процессе передачи от аккредитованного источника поставщику авиационных услуг Интернет (IASP); от IASP пользователю; от пользователя IASP (например, AFTN, представление планов полетов и входные данные метеорологических наблюдений)? Поддается ли обнаружению такое умышленное вмешательство?

c) ***Прерывание, в результате которого возникает угроза "готовности".*** Обладает ли обслуживание характеристиками, приемлемыми для эксплуатационного использования? Будет ли ухудшаться уровень обслуживания при пиковом спросе? Имеется ли возможность блокирования использования ресурсов? Можно ли помешать зарегистрированным пользователям представлять информацию за счет массированной загрузки службы ложными входными данными (например, атака с целью отказа в обслуживании (DoS))? Наиболее характерным примером является чрезмерное количество подключений к web-серверам, в результате которых зарегистрированные пользователи лишаются доступа к обслуживанию.

d) ***Имитация, в результате которой возникает угроза "аутентичности".*** Эта угроза заключается в том, что кто-то выдает себя за другого. Например, можно ли в Интернет-службе гарантировать, что "клиенты", входящие в систему, фактически являются теми, за кого они себя выдают, поскольку они могут быть лицами, пытающимися получить обслуживание бесплатно. Имеется ли возможность проверки того, что лицо, пытающееся получить доступ администратора, фактически является законным администратором? Могут ли пользователи проверить, что они взаимодействуют с реальной службой, а не с чем-то, за что выдает себя нападающая сторона? В частности, при пользовании Интернетом могут возникнуть трудности с подтверждением того, что на другом конце соединения действительно находится то лицо или устройство, которое там должно быть.

3.4.7 Перечисленные выше виды угроз, как правило, могут проявлять себя во многих областях, некоторые из которых приводятся ниже:

a) ***данные/информация:*** неготовность, прерывание (потеря), перехват, изменение, фальсификация или уничтожение;

b) ***служащие/персонал:*** упущения, ошибки, халатность, неосмотрительность, леность, вредительство или недостаток знаний;

c) ***сеть (Интранет, Интернет и т. д.):*** несанкционированный доступ, операции по техническому обслуживанию, отказ или попытки проникновения в защищенную систему (например, перехват, розыгрыши, поддельная идентификация, нарушение целостности или отказ в обслуживании);

d) ***аппаратные средства:*** операции по техническому обслуживанию, отказ (включая отказ питания) или кража;

e) ***программные средства и система:*** прерывание, модификации/изменения или отказ.

Определение источников угрозы

3.4.8 Вероятность вторжения и его последствия могут зависеть от источника вторжения. Целесообразно дополнительно классифицировать угрозы по их источникам. Ниже приводится наиболее простая классификация источников потенциальных угроз:

a) персонал (штатный);

b) персонал (администраторы);

c) консультанты/подрядчики;

d) конкуренты;

e) хакеры (неквалифицированные, но многочисленные);

f) хакеры (опытные, высококвалифицированные);

g) политически заинтересованные и организованные структуры;

h) природные события.

Определение вероятности реализации угрозы

3.4.9 Этот элемент оценки риска принимает объективный характер. Здесь необходимо рассмотреть два фактора:

a) ***Простота вторжения.*** Это зависит от задействованных мер безопасности, типа установленной системы и местоположения системы. Это также зависит от уровня навыков источника угрозы и имеющихся у этого источника возможностей, а также от располагаемых ресурсов. Со временем это может измениться. Некоторые виды вторжений могут рассматриваться в качестве чисто теоретических и очень сложных для реализации, однако в случае разработки средства их автоматизации они переходят в категорию вторжений, предпринять которые более легко.

b) ***Побудительные мотивы источника угрозы.*** Наличие возможности у какого-либо лица осуществить вторжение еще не означает, что это лицо сделает это. Поэтому важно понять побудительные мотивы источников угрозы.

3.4.10 Например, в типичной современной организации большинство штатного персонала не имеет прямого доступа к их web-серверу (т. е. доступ обеспечивается только через браузер). Поэтому даже при наличии побудительных мотивов большинству сотрудников будет относительно трудно инициировать вторжение (особенно при наличии мониторинга). Совершенно иное положение с "системным администратором". Даже непреднамеренно системный администратор может вызвать серьезное нарушение, и в этом случае практически отсутствует защита от таких потенциальных вторжений. Таким образом на системного администратора возлагается большая ответственность.

3.4.11 Аналогичным образом неквалифицированные хакеры всегда совершают попытки проникновения в web-серверы, а побудительным мотивом и предметом для гордости в основном является количество взломанных систем. Если обеспечивается сопровождение и обновление систем программного обеспечения, уровень риска может быть довольно низким. Однако высококвалифицированные хакеры могут совершить успешное вторжение практически в любой сервер. В этом случае возникает вопрос о причине вторжения в конкретную организацию.

3.4.12 Несмотря на то что естественные события (например, пожары, землетрясения, наводнения или торнадо) происходят редко, они будут оказывать влияние на предоставление обслуживания и в этой связи их также необходимо учитывать в процессе управления риском.

Определение последствий угрозы

3.4.13 Такой анализ по-прежнему является субъективным. Цель заключается в том, чтобы ответить (в максимально возможной степени) на такие вопросы, как:

a) Каковы расходы на восстановление поврежденных данных?

b) Какова стоимость этих данных?

c) Какова стоимость ущерба, нанесенного репутации Организации?

d) Каковы неустойки по договору?

e) Каковы эксплуатационные последствия для пользователя, обусловленные потерей или отсутствием информации?

3.4.14 Последствия или степень тяжести будут основываться на характерных для системы факторах, включая характер угрозы, функциональные возможности системы, ее интерфейсы с операционными системами, критичность предоставляемых данных, непрерывность бизнеса и пользователь информации, но не ограничиваясь ими.

Оценка риска

3.4.15 Если последствия и вероятность оцениваются с использованием стандартной формы управления риском (очень незначительные/незначительные/средние/высокие/исключительно высокие), то риск можно рассчитать абсолютно аналогичным образом (т. е. на основе последствий и вероятности, где последствия представляют собой влияние на систему/организацию, а вероятность – возможность реализации угрозы как таковой с учетом типа угрозы и источника угрозы, а также уровня навыков и заинтересованности).

Стратегии снижения риска

3.4.16 Важно использовать стратегии снижения риска, учитывая при этом стоимость или степень тяжести последствий отказа обслуживания. Например, небольшим IASP, предоставляющим предполетную информацию для авиации общего назначения, снижать уровень риска может потребоваться в значительно меньшей степени, чем IASP, обеспечивающим предоставление планов полета и услуги по предполетному инструктажу агентствам, эксплуатирующим коммерческие воздушные суда. Несмотря на то что масштабы стратегии снижения риска и стоимость обслуживания взаимоувязаны, следует всегда предпринимать обоснованные меры для сохранения целостности аэронавигационных данных.

3.4.17 Следует отметить, что наиболее важным фактором стратегии снижения риска является управление корректировкой прикладных программ. Независимо от того, насколько хорошо спроектирована и реализована система, при использовании устаревших программных средств (т. е. самые последние корректировки не внесены) обслуживание будет уязвимо к вторжению.

3.4.18 Стратегии снижения риска группируются по категории чувствительности, защиту которой они обеспечивают. Ниже приводится перечень основных категорий чувствительности и возможных соответствующих стратегий снижения риска:

a) конфиденциальность:

1) обеспечивается реализация процессов, гарантирующих конфиденциальность данных, хранимых поставщиком обслуживания;

2) гарантируется конструкцией системы, архитектурой сети и процедурами жизненного цикла снижение, до приемлемого уровня, вероятности нарушения доступа в систему;

3) снижается, до приемлемого уровня, вероятность "похищения" конфиденциальных данных в процессе обмена между поставщиком обслуживания и пользователем за счет использования, при необходимости, кодирования данных;

4) с учетом уровня тяжести последствий обеспечивается снижение, до приемлемого уровня, вероятности доступа к сайту неаутентифицированного или неправильно аутентифицированного пользователя;

5) с учетом уровня тяжести последствий в соответствующих случаях вводится имя пользователя или пароль и/или используются другие механизмы аутентификации пользователя;

6) вводится регистрация пользователя и процесс проверки, соответствующие уровню тяжести последствий;

7) реализуется политика ответственности пользователя, условия и режим которой соответствуют уровню тяжести последствий;

8) обеспечивается соответствующее управление паролями;

9) обеспечивается безопасная утилизация оборудования;

b) целостность:

Примечание. В п. 3.2.8 главы 3 Приложения 15 содержится требование об обеспечении в рамках системы качества целостности аэронавигационных данных;

1) обеспечивается получение исходных данных из гарантированного источника;

2) гарантируется, что изменение или переформатирование исходных данных не наносит ущерба их целостности;

3) обеспечивается снижение, до приемлемого уровня, вероятности изменения данных в процессе обмена между гарантированным источником и поставщиком обслуживания посредством того, что:

i) обеспечивается снижение, до приемлемого уровня, вероятности искажения данных, хранимых поставщиком обслуживания;

ii) обеспечивается снижение, до приемлемого уровня, вероятности изменения данных в процессе обмена между поставщиком обслуживания и пользователем;

iii) обеспечивается возможность восстановления "чистых" данных в случае разрушения данных, хранимых поставщиком обслуживания;

iv) обеспечивается снижение, до приемлемого уровня, вероятности вмешательства в хранимые данные через web-сайт;

v) обеспечивается ведение журналов регистрации транзакций с пользователем с отметкой даты и времени в целях защиты от непризнания участия (должна обеспечиваться возможность восстановления фактических данных, к которым был обеспечен доступ, в целях проверки получения пользователем сообщения, если данные не архивировались);

c) готовность:

1) заключаются соглашения об уровне обслуживания с ISP (включая любую соответствующую техническую поддержку), которые обеспечивают уровень готовности, соответствующий значимости сайта;

2) конструкция системы обеспечивает уровень дублирования, соответствующий значимости сайта;

3) конструкция системы, архитектура сети и процессы управления жизненным циклом обеспечивают снижение, до приемлемого уровня, вероятности предумышленного вывода платформы из строя (например, хакинг, вирусы, "черви", отказ в обслуживании, распределенный отказ в обслуживании или естественные события, такие как лавинная маршрутизация);

4) конструкция системы, архитектура сети, процессы управления жизненным циклом и обучение обеспечивают снижение, до приемлемого уровня, вероятности вывода платформы из строя в результате непреднамеренных действий;

5) внедряется процесс обратной связи с клиентами в целях обеспечения возможности идентификации проблем, касающихся характеристик, и передачи этой информации поставщику обслуживания;

d) аутентичность:

1) обеспечивается возможность оперативной проверки пользователем факта аккредитации поставщика (для государства, в которое пользователь желает начать выполнять полеты);

2) обеспечивается возможность проверки пользователем того, что поставщик обслуживания является тем, за кого он себя выдает;

3) обеспечивается возможность проверки поставщиком, при необходимости, того, кем является пользователь.

3.4.19 Кроме того, при необходимости, IASP должен иметь возможность убедиться в том, что соответствующая информация доставлена пользователю. Для этого существует служба защиты от нарушения участия.

3.4.20 Завершив проведение первоначальной оценки риска, следует перейти к интерактивному этапу процесса управления риском, в рамках которого рассматриваются меры по снижению риска и проводится новая оценка риска до тех пор, пока IASP (и аккредитующее государство) не убедятся в том, что оставшиеся риски являются приемлемыми. Кроме того, в ходе предоставления обслуживания будут определены новые виды риска. В рамках процесса управления риском следует рассмотреть эти факторы и провести повторную оценку существующих и новых рисков с учетом имеющейся информации и наилучшей практики.

3.4.21 В добавлении к настоящей главе приводится перечень отдельных видов угрозы и стратегий управления риском в увязке с рекомендуемой и используемой в настоящее время практикой реализации этих стратегий в условиях использования информационных технологий.

3.4.22 Кроме того, в подготовленном Организацией Open Web Application Security Project (OWASP) (http://www.owasp.org) документе *"The Ten Most Critical Web Application Security Vulnerabillities",* 2004 Update, определяется ряд стратегий снижения степени уязвимости в связи с использованием web-приложений.

— — — — — — — —

Добавление к главе 3

НАИЛУЧШАЯ СОВРЕМЕННАЯ ПРАКТИКА РЕАЛИЗАЦИИ СТРАТЕГИЙ СНИЖЕНИЯ РИСКА В УСЛОВИЯХ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Примечание. Поскольку технология Интернета развивается быстрыми темпами, конкретные технические решения, предлагаемые в колонке " Наилучшая современная практика"; являются примерами решений, используемых на момент публикации.

Стратегия снижения риска	Категория чувствительности	Наилучшая современная практика	Подлежит использованию, когда степень тяжести последствий является	
			низкой	высокой
Осуществлять аутентификацию пользователей, соответствующую уровню угрозы	Аутентичность	• Анонимный доступ пользователей.	T	
		• Обязательное использование имени пользователя и пароля при входе в систему.	T	
		• Использование имени пользователя, пароля при входе в систему с отдельным личным идентификационным номером (PIN) для конкретных функций.		T
		• Цифровой сертификат (например, SSL).		T
		• Протокол защищенной передачи (https).		T
		• RSA SecurID.		T
		• Виртуальная частная сеть (VPN), интегрированная операционная система (OS).		T
		• Резервные программные средства пользователей (аутентификация маркеров)		T
Осуществлять регистрацию пользователей и процесс проверки, соответствующие уровню угрозы	Аутентичность	• Онлайновая регистрация без проверки.	T	
		• Документально оформляемая регистрация с проверкой.	T	
		• Онлайновая регистрация с проверкой.		T
		• Документально оформляемая регистрация с проверкой.		T
		• Онлайновая регистрация с передачей подробной информации о доступе по альтернативному каналу (т. е. электронная и обычная почта, что обеспечивает возможность фактической идентификации зарегистрированного пользователя		T
Определять для пользователей сроки и условия соответствующие уровню угрозы	Аутентичность	• Сохранение конфиденциальности пароля; исключение совместного использования.	T	
		• Всегда полностью выходить из сайта.	T	
		• Информировать поставщика обслуживания об изменениях соответствующей информации	T	
Осуществлять кодирование данных, соответствующее уровню конфиденциальности	Целостность	• HTTPS, SSL.	T	
		• PKI (и другие)		T

Стратегия снижения риска	Категория чувствительности	Наилучшая современная практика	Подлежит использованию, когда степень тяжести последствий является	
			низкой	высокой
Снижать, до приемлемого уровня, вероятность изменения данных в процессе обмена между гарантированным источником и поставщиком обслуживания	Целостность	• Использование Интернета с соответствующим кодированием и аутентификацией (HTTPS, SSL).	T	
		• Использование схемы защищенной частной или виртуальной частной сети (VPN) для получения данных от гарантированного источника. Исключение использования публичного Интернета без соответствующим образом защищенной схемы VPN		T
Снижать, до приемлемого уровня, вероятность изменения данных, хранимых поставщиком обслуживания. Снижать, до приемлемого уровня, вероятность изменения данных в процессе обмена между поставщиком обслуживания и пользователем. Снижать, до приемлемого уровня, вероятность вмешательства в хранимые данные через web-сайт	Целостность	• Использование брандмауэров программных средств и защищенной инфраструктуры; исключение прямого доступа к хранимым данным.	T	
		• Использование физических брандмауэров, серверов-посредников, систем защиты от вмешательства в главные вычислительные машины (HIPS) и систем обнаружения вмешательства в сеть (NIDS), при необходимости.		T
		• Внедрение двухуровневых брандмауэров, каждый из которых поставляется различными изготовителями, для уменьшения вероятности повышения степени уязвимости поставщика обслуживания.		T
		• Проверка поставщика и использование цифровых сертификатов.		T
		• Исключение использования операторов в качестве промежуточного звена системы и обеспечение передачи данных непосредственно пользователям (достижение этой цели обеспечит SSL).		T
		• Установка инфраструктуры брандмауэров между web-сервером и прикладным сервером (если таковые имеются) и информационными складами в дополнение к внешним границам для создания DMZ (демилитаризованных зон).		T
		• Использование различных DMZ для разделения функциональных компонентов (т. е. web-сервер, прикладной сервер, сервер базы данных)		T
Обеспечивать возможность восстановления "чистых" данных в случае разрушения данных, хранимых поставщиком обслуживания. Обеспечивать ведение журналов регистрации транзакций с пользователем с отметкой даты и времени в целях защиты от непризнания участия (должна обеспечиваться возможность восстановления фактических данных, к которым был обеспечен доступ, в целях проверки получения пользователем сообщения, если данные не архивировались)	Целостность	• Хранение журналов регистрации в интероперабельных форматах, таких, как ASCII.	T	
		• Обеспечение цифровой подписи файлов журналов регистрации.		T
		• Обеспечение управления системой и резервирования данных из защищенного домена.		T
		• Обеспечение хранения резервных данных в защищенном домене.		T
		• Внедрение внесайтового хранения для целей восстановления разрушенных архивов		T

Стратегия снижения риска	Категория чувствительности	Наилучшая современная практика	Подлежит использованию, когда степень тяжести последствий является	
			низкой	высокой
Внедрять процесс обратной связи с клиентами в целях идентификации и устранения возникающих у них проблем	Все категории	• Создание службы поддержки клиентов с телефонной связью и системы отслеживания сообщений о возникающих проблемах. • Обеспечение обратной связи с клиентами по электронной почте и использовании системы отслеживания сообщений о возникающих проблемах	T	T
Обеспечивать возможность оперативной проверки аккредитации поставщика (для государства, в которое пользователь хочет начать перевозки). Обеспечивать возможность проверки пользователем того, является ли поставщик обслуживания тем, за кого он себя выдает. Обеспечивать, при необходимости, возможность проверки поставщиком того, кем является пользователь	Конфиден-циальность	• Проверка пользователя с использованием имени пользователя и пароля. • Проверка пользователя с использованием цифровых сертификатов клиента. • Проверка поставщика с использованием цифровых сертификатов. • Размещение на сайте официальной эмблемы, свидетельствующей об аккредитации (и в каком государстве). • Размещение гипертекстовой ссылки на аккредитационный сайт государства. На аккредитационном сайте государства должна размещаться подробная информация о характере обслуживания, на предоставление которого аккредитован поставщик, а также дата аккредитации и дата ее окончания	T T T T	T
Заключать с ISP соглашения об уровне обслуживания, обеспечивающие степень готовности, соответствующей значимости сайта	Готовность	• Определение соглашения об уровне обслуживания с ISP, включая положения о нарушении обслуживания, готовности и диапазоне частот. • Определение контракта на техническое обслуживание оборудования для физической инфраструктуры, который должен включать в себя положения об уровне обслуживания. • Обеспечение гарантий в том, что выбранный ISP может предоставить достаточную полосу частот, с учетом дополнительного объема для любого прогнозируемого расширения обслуживания	T T T	

Стратегия снижения риска	Категория чувствительности	Наилучшая современная практика	Подлежит использованию, когда степень тяжести последствий является	
			низкой	высокой
Гарантировать возможность обеспечения конструкцией системы пропускной способности и дублирования, соответствующих значимости сайта	Готовность	• Сведение до минимума количества единичных отказов или последствий любого отказа.	T	
		• Обеспечение горячего резерва/холодного резерва/ комплекта запасных частей (при необходимости) для основного оборудования (серверы, маршрутизаторы и т. д.) с целью оперативного устранения отказов.	T	
		• Оценка потребностей в пропускной способности системы (т. е. за счет применения конструкции, обеспечивающей реализацию наилучшей практики и/или проверки загрузки системы).	T	
		• Определение физической инфраструктуры с учетом предполагаемой пропускной способности.		T
		• Установка кластеров серверов/групп серверов и уравнителей нагрузки.	T	
		• Установка быстро заменяемых дисководов/матриц независимых дисковых накопителей с избыточностью (RAID) с целью сведения до минимума последствий отказа диска.		T
		• Установка сдвоенных (дублированных) информационных складов.		T
		• Использование сдвоенной сетевой инфраструктуры (включая подключение к Интернет через ISP); не обязательно привлекать отдельные компании, если одна компания может обеспечить надежную инфраструктуру.		T
		• Заключение контрактов на поставки оборудования и инфраструктуры сети с различными поставщиками (не обязательно с изготовителем) на случай финансового краха или промышленных конфликтов.	T	
		• Установка серверов с источниками бесперебойного питания (UPS) на случай кратковременных отказов электропитания.		T
		• Установка UPS с резервными дизель-генераторами на случай более длительных отказов электропитания.		T
		• Обеспечение совершенно независимой инфраструктуры для устранения аварийных ситуаций и поддержания непрерывности обслуживания	T	
Конструкция системы, архитектура сети и процессы управления жизненными циклами обеспечивают снижение, до приемлемого уровня, вероятности предумышленного вывода платформы из строя (например, хакинг, вирусы (черви), отказ в обслуживании, распределенный отказ в обслуживании, лавинная маршрутизация и т. д.).	Готовность	• Реализация стратегии повышения надежности системы, обеспечивающей соответствующий уровень надежности системы за счет удаления или отключения всех компонентов, которые не требуются для ее функционирования. Это может включать введение ограничений на доступ (порты и протоколы), ограничение количества пользователей, использование паролей, контроль доступа, определение прав индивидуальных пользователей и групп и обнаружение вмешательства.	T	
		• Реализация стратегии модификации программных средств, обеспечивающей обновление программных средств системы и поддержание их на надлежащем уровне.		T
		• Установка анти-DOS оборудования – пакетные фильтры/"защищенные" маршрутизаторы.	T	

Стратегия снижения риска	Категория чувствительности	Наилучшая современная практика	Подлежит использованию, когда степень тяжести последствий является	
			низкой	высокой
Конструкция системы, архитектура сети, процессы управления жизненными циклами и обучение должны обеспечивать снижение, до приемлемого уровня, вероятности непреднамеренного вывода платформы из строя		• Использование антивирусных программных средств и обновление программного обеспечения.		T
		• Установка антивирусных программных средств различных поставщиков для уменьшения вероятности повышения степени уязвимости поставщика обслуживания.	T	
		• Определение предполагаемых тенденций в области доступа пользователей/использование системы и объема трафика.	T	
		• Оценка достаточности диапазона частот для обеспечения характерных потребностей и объемов трафика.	T	
		• Определение соответствующих процедур проверки, обеспечивающих проведение модернизации обслуживания без нарушения функциональных возможностей и негативных последствий для представления обслуживания.	T	
		• Определение соответствующих процедур развертывания оборудования, обеспечивающих проведение модернизации обслуживания без нарушения функциональных возможностей и негативных последствий для предоставления обслуживания.		T
		• Исключение возможности использования бюджета каждого пользователя для ведения параллельных сеансов, инициируемых различными IP адресами.		T
		• Задействование (автоматизированное) отказо-безопасного приложения, готового к использованию в том случае, когда основной сайт находится в офлайновом режиме.		T
		• Проведение соответствующей подготовки персонала и использованию процедур для разработки, развертывания и технического обслуживания службы.		T
		• Осуществление круглосуточного контроля в течение всей недели инфраструктуры и применений при наличии документально оформленных процедур устранения и/или предотвращения дальнейшего распространения ожидаемых проблем		T

Глава 4

ВОПРОСЫ, КАСАЮЩИЕСЯ МЕТЕОРОЛОГИЧЕСКОЙ ИНФОРМАЦИИ

4.1 ВВЕДЕНИЕ

4.1.1 Согласно Приложению 3 *"Метеорологическое обеспечение международной аэронавигации"* Договаривающиеся государства соглашаются предоставлять ряд видов обслуживания, которые включают в себя, как минимум, наблюдения и прогнозы, необходимые для принятия оперативных решений районными диспетчерскими центрами, центрами полетной информации, летно-эксплуатационными агентствами, летными экипажами или командирами воздушных судов. Цель настоящей главы заключается в определении метеорологической информации, которую можно предоставлять по Интернету, и в каком контексте.

4.2 КРИТИЧНЫЕ ПО ВРЕМЕНИ МЕТЕОРОЛОГИЧЕСКИЕ СООБЩЕНИЯ

4.2.1 Метеорологическая информации, перечень которой приводится в п. 4.2.2, в случае ее предоставления по Интернету не должна использоваться для принятия критичных по времени оперативных решений в полете или непосредственно перед вылетом. В отношении такой информации будет использоваться термин "критичная по времени метеорологическая информация", и в случае ее использования в таком контексте ее следует рассылать по каналам авиационной фиксированной службы (AFS), поскольку ее характеристики обеспечивают своевременное получение таких сообщений.

4.2.2 Согласно тому II Приложения 10 *"Авиационная электросвязь"* сообщения, содержащие авиационную метеорологическую информацию, относятся к одной из двух категорий, а именно "сообщения, касающиеся безопасности полетов" или "метеорологические сообщения". К числу авиационных метеорологических сообщений, касающихся безопасности полетов, которые в вышеупомянутом контексте можно рассматривать в качестве критичных по времени, относятся:

a) информация SIGMET;

b) специальные донесения с борта (AIREP);

c) сообщения AIRMET;

d) консультативные сообщения о вулканическом пепле;

e) консультативные сообщения о тропических циклонах;

f) измененные прогнозы по аэродрому (TAF).

4.3 НЕКРИТИЧНЫЕ ПО ВРЕМЕНИ МЕТЕОРОЛОГИЧЕСКИЕ СООБЩЕНИЯ

4.3.1 Перечисленная ниже метеорологическая информация рассматривается в качестве некритичной по времени, и ее можно предоставлять по Интернету:

a) метеорологическая информация, касающаяся прогнозов, например, TAF, зональные и маршрутные прогнозы и результаты соответствующих наблюдений, таких как регулярные метеорологические сводки по аэродрому (METAR) и специальные метеорологические сводки по аэродрому (SPECI);

b) метеорологическая информация, предоставляемая всемирными центрами зональных прогнозов (ВЦЗП), например, карты особых явлений погоды и карты ветра, температуры и относительной влажности;

c) консультативные сообщения о вулканическом пепле в графическом формате (VAG), предоставляемые консультативными центрами по вулканическому пеплу;

d) зональные прогнозы GAMET;

e) прогнозы погоды по маршруту (ROFOR).

Примечание. В этот перечень могут также входить бинарная универсальная форма для предоставления метеорологических данных (BUFR) и обработанные закодированные метеорологические данные в виде значений в узлах регулярной сетки, выраженных в двоичной форме (GRIB).

4.3.2 Обслуживание, предоставляемое эксплуатантам и членам летных экипажей для целей предполетного планирования, оперативный контроль над которым осуществляется централизованно, рассматривается в качестве некритичного по времени. Метеорологическая информация, предназначенная для проведения эксплуатантами предполетного планирования, может включать в себя следующее:

a) информация о текущих и прогнозируемых параметрах ветра в верхних слоях атмосферы, температурах воздуха в верхних слоях атмосферы до высот тропопаузы и геопотенциальных высот, информация о максимальной скорости ветра и изменения к ней;

b) информация о текущих и ожидаемых особых явлениях погоды по маршруту и струйных течениях и изменения к ней;

c) прогнозы для взлета;

d) METAR и там, где имеется возможность, SPECI для аэродрома вылета, взлета и запасных аэродромов по маршруту, аэродрома предполагаемой посадки и запасных аэродромов пункта назначения в соответствии с региональным аэронавигационным соглашением;

e) TAF и изменения к ним для аэродрома вылета и предполагаемой посадки и для взлета, полета по маршруту и запасных аэродромов пункта назначения в соответствии с региональным аэронавигационным соглашением;

f) информация SIGMET и соответствующие специальные донесения с борта для соответствующих маршрутов в целом, как определено региональным аэронавигационным соглашением.

Глава 5

ВОПРОСЫ, КАСАЮЩИЕСЯ СЛУЖБ АЭРОНАВИГАЦИОННОЙ ИНФОРМАЦИИ (САИ)

5.1 ВВЕДЕНИЕ

5.1.1 Цель настоящей главы заключается в определении аэронавигационной информации и возможного контекста ее предоставления по Интернету.

5.1.2 Стандарты и Рекомендуемая практика (SARPS) Приложения 15 *"Службы аэронавигационной информации"*, Приложения 4 *"Аэронавигационные карты"* и инструктивный материал, содержащийся в *Руководстве по службам аэронавигационной информации"* (Doc 8126), разработаны в целях обеспечения единообразия и последовательности при предоставлении аэронавигационной информации.

5.1.3 Несмотря на то что услуги, предоставляемые по Интернету службами аэронавигационной информации, можно сориентировать на удовлетворение эксплуатационных потребностей пользователей (персонал, обеспечивающий производство полетов, включая летные экипажи, планирование полетов и летные тренажеры, а также подразделения служб воздушного движения, ответственные за службу полетной информации, и службы, ответственные за предполетную информацию), они должны отвечать требованиям вышеупомянутых стандартов.

5.1.4 Должна быть задействована система управления качеством, обеспечивающая предоставление пользователям необходимых гарантий и уверенности в том, что рассылаемая аэронавигационная информация отвечает установленным требованиям к качеству данных и прослеживаемости (см. п. 3.2.5 главы 3 Приложения 15).

5.2 КРИТИЧНАЯ ПО ВРЕМЕНИ АЭРОНАВИГАЦИОННАЯ ИНФОРМАЦИЯ

5.2.1 Перечисленная ниже аэронавигационная информация рассматривается в качестве критичной по времени, и в случае предоставления по Интернету она не должна использоваться для принятия критичных по времени оперативных решений в полете или непосредственно перед вылетом:

a) динамическая информация временного характера, такая как действующие, национальные и зарубежные NOTAM (включая SNOWTAM, ASHTAM и контрольные перечни);

b) другая информация срочного характера, предоставляемая летным экипажам открытым текстом в виде предполетных информационных бюллетеней (PIB).

5.2.2 В п. 5.3.2.1 главы 5 Приложения 15 говорится о том, что для рассылки NOTAM по возможности используется сеть AFS.

5.2.3 В соответствующих случаях при предоставлении расширенных бюллетеней предполетной информации или продуктов с использованием специального формата или графиков, необходимо обеспечивать предоставление по крайней мере таких услуг, которые бы предоставлялись в условиях использования печатных публикаций.

5.3 НЕКРИТИЧНАЯ ПО ВРЕМЕНИ АЭРОНАВИГАЦИОННАЯ ИНФОРМАЦИЯ

5.3.1 Перечисленные ниже виды статической и базовой информации САИ рассматриваются в качестве некритичных по времени, и их можно предоставлять по Интернету:

a) ***Статическая информация.*** Документально оформленная информация постоянного или долгосрочного характера, такая, как:

1) Сборники аэронавигационной информации (AIP) (в которых содержится информация об аэродромах, подробное описание районов полетной информации (РПИ), навигационных средств, карты, схемы, данные о препятствиях, информация о воздушных трассах и т. д.);

2) поправки к AIP, вносимые в ходе регламентации и контролирования аэронавигационной информации (AIRAC) и регулярные поправки;

3) дополнения к AIP, как AIRAC, так и регулярные дополнения;

4) циркуляры аэронавигационной информации (AIC);

5) ежемесячно публикуемый открытым текстом перечень действующих NOTAM, в котором также содержится информация о самых последних поправках к AIP, опубликованные AIC и контрольный перечень дополнений к AIP;

6) ежемесячно публикуемые NOTAM, содержащие контрольный перечень действующих NOTAM, в которых также содержится информация о самых последних поправках к AIP, дополнения к AIP и, по крайней мере, AIC, подлежащие международной рассылке.

b) ***Базовая информация.*** Данные, необходимые для обработки другой информации, которые могут включать в себя постоянные, не предоставляемые пользователям долгосрочные или статические данные (например, справочные перечни, специальные/регулярные маршруты, файлы рассылки, критерии отбора, соответствующие критерии).

5.4 ПРЕДОСТАВЛЕНИЕ СТАТИЧЕСКОЙ И БАЗОВОЙ ИНФОРМАЦИИ

5.4.1 Статическая и базовая информация может носить постоянный или долгосрочный характер. Необходимо указывать дату вступления в силу этой информации. Каждая публикация должна датироваться. Если страницы имеют различные даты вступления в силу, то каждая страница должна индивидуально датироваться. В тех случаях, когда элементы данных публикуются независимо, необходимо четко определять их дату вступления в силу.

5.4.2 В отношении информации, перечисленной в части 1 добавления 4 Приложения 15, в соответствии с системой регулирования (AIRAC) необходимо использовать единую дату вступления в силу с интервалами в 28 дней; кроме того, аналогичный подход рекомендуется использовать в

отношении информации, перечисленной в части 2 (подробная информация содержится в главе 6 Приложения 15). Для упрощения перехода от даты вступления в силу к следующей дате публикации (цикл дат AIRAC) аэронавигационная информация предыдущего, текущего и следующего цикла должна предоставляться на установленный период. При предоставлении такого обслуживания возрастает значимость четкого определения даты вступления в силу всех типов аэронавигационной информации.

5.4.3 Интернет может использоваться для предоставления информации в рамках системы AIRAC. Однако должна по-прежнему обеспечиваться соответствующая возможность предоставления информации в распечатанном виде (см. раздел 6.2 Приложения 15). Система AIRAC предназначена для предоставления конкретным получателям информации для предварительного планирования: поставщикам САИ, являющимся третьими сторонами, авиационным агентствам, изготовителям и составителям баз данных и т. д. Рекомендуется обеспечивать конфиденциальность (см. главу 3 настоящего Руководства). Необходимо, чтобы организации, рассматривающие вопрос о предоставлении такой информации, были уверены в том, что пользователи хорошо осведомлены о системе AIRAC и располагают полной информацией относительно дат вступления в силу, касающихся такой информации.

5.5 ПРЕДОСТАВЛЕНИЕ КАРТ

5.5.1 Положения Приложений 4 и 15 распространяются на содержание и визуальное представление типов карт, предусмотренных Приложением 4 ИКАО, и других карт AIP, включая карты, предоставляемые по Интернету службами аэронавигационной информации государств. Карты должны представляться в масштабах, сопоставимых с требованиями Приложения 4. Если разрешается изменение масштаба, для сведения пользователей должна быть доведена информация о диапазоне масштабов, который будет обеспечивать сохранение качества карт. Предполагается, что в ближайшем будущем большинство карт, предоставляемых по Интернету, будет идентично визуальному представлению используемых в настоящее время карт в распечатанном виде. Однако некоторые картографические и географические информационные системы (GIS) располагают возможностью предоставления карт в форматах с расширенными функциональными возможностями, включая обеспечение возможности контроля со стороны пользователей карт за отображаемой информацией. В тех случаях, когда электронные карты представляются в таких форматах, важно, чтобы вся соответствующая информация первоначально отображалась пользователю и исключалась возможность деселекции критичной для безопасности полетов информации.

5.5.2 Оптимальные графические форматы для представления схемы и карт по Интернету могут отличаться от тех, которые используются при подготовке документации, поэтому их необходимо выбирать с учетом перечисленных ниже общих соображений:

a) наличие возможностей вывода графических данных, обеспечиваемых программными средствами выпуска картографической продукции или сканерами;

b) доступность размещенных карт для клиентов (совместимость с операционными системами, web-браузерами, системами воспроизведения цветов и принтерами клиентов);

c) функциональные возможности карт и качество изображения;

d) размер данных карт (и в этой связи время передачи);

e) является ли формат открытым или коммерческим стандартом и каковы связанные с этим расходы.

Глава 6

ВОПРОСЫ, КАСАЮЩИЕСЯ ПЛАНОВ ПОЛЕТА

6.1 ВВЕДЕНИЕ

6.1.1 Цель настоящей главы заключается в предоставлении рекомендаций относительно представления и управления планами полетов (в рамках авиационной фиксированной службы (AFS)) с использованием Интернета.

6.1.2 Интернет может использоваться в качестве средства обеспечения приложений для представления и получения планов полета непосредственно от пользователей. Кроме того, Интернет обеспечивает возможность обратной связи в отношении принятия планов полета и позволяет проводить консультации и изменять/отменять представленные планы полетов. Обеспечиваемые Интернетом приложения, связанные с планами полетов, часто предлагаются совместно с приложениями в области САИ и МЕТ, что позволяет получить полный комплект требуемой аэронавигационной информации.

6.2 ПРЕДСТАВЛЕНИЕ ПЛАНОВ ПОЛЕТА

6.2.1 Следует придерживаться стандартного формата планов полета и критериев оценки, описание которых приводится в документе *"Правила аэронавигационного обслуживания. Организация воздушного движения"* (PANS-ATM, Doc 4444).

6.2.2 Использование Интернета для представления планов полета позволяет уменьшить объем работ, выполняемый вручную подразделениями служб воздушного движения, обеспечивающими предоставление донесений с использованием прикладных программ пользователей для сбора синтаксически правильных планов полета и их надежной передачи для дальнейшей обработки в эксплуатационных условиях использования планов полета.

6.2.3 Следует отметить, что при использовании такого интерфейса Интернета система может быть уязвима к вторжению, вызывающему отказ в обслуживании (DoS). При неограниченном и неконтролируемом представлении планов полета не исключена возможность отказа другим законным пользователям в доступе к обслуживанию. Кроме того, в полностью автоматизированной системе также не исключена возможность воздействия на существующие функционирующие системы. Для уменьшения риска DoS-атак необходимо внедрять процедуры автоматизированного или ручного контроля.

6.2.4 Представление планов полета по Интернету можно без особых трудностей распространить на полеты, в отношении которых план полета представлять не требуется. Например, это может упростить контроль за полетами, выполняемыми по правилам визуальных полетов, в целях поиска и спасания.

6.3 УПРАВЛЕНИЕ ПЛАНАМИ ПОЛЕТОВ

6.3.1 Интернет может обеспечить пользователям прямой доступ к такой информации, как подтверждение, изменение или отклонение представленных планов полета в автоматизированном

или контролируемом режиме в реальном масштабе времени при условии наличия средств связи и необходимых интерфейсов.

6.3.2 Пользователь должен иметь обратную связь в отношении принятия плана полета, что обеспечивает возможность проведения консультаций и изменения/отмены представленного плана полета. Основной риск для функционирующих систем заключается в несогласованности приложений Интернета с соответствующими интерфейсами к AFS.

_____

Глава 7

ДРУГИЕ ВИДЫ ПРИМЕНЕНИЯ

7.1 ПРИЛОЖЕНИЯ ДЛЯ ПЕРЕДАЧИ СООБЩЕНИЙ ТИПА AFTN

7.1.1 Известно, что в настоящее время в исключительных случаях Интернет используется в качестве альтернативного средства обмена сообщениями типа AFTN между государствами (например в тех случаях, когда специализированные каналы связи отсутствуют/ненадежны или их использование экономически невыгодно в связи с незначительным уровнем трафика).

7.1.2 В случае использования основанной на Интернете связи типа AFTN следует придерживаться процедур, касающихся формата, обработки и хранения сообщений, предусмотренных томом II Приложения 10.

7.1.3 Следует надлежащим образом учитывать изложенные в главе 3 настоящего Руководства положения в отношении оценки риска и процессов управления.

— КОНЕЦ —

ТЕХНИЧЕСКИЕ ИЗДАНИЯ ИКАО

Ниже приводится статус и общее описание различных серий технических изданий, выпускаемых Международной организацией гражданской авиации. В этот перечень не включены специальные издания, которые не входят ни в одну из указанных серий, например "Каталог аэронавигационных карт ИКАО" *или* "Метеорологические таблицы для международной аэронавигации".

Международные стандарты и Рекомендуемая практика принимаются Советом ИКАО в соответствии со статьями 54, 37 и 90 Конвенции о международной гражданской авиации и для удобства пользования называются Приложениями к Конвенции. Единообразное применение Договаривающимися государствами требований, включенных в Международные стандарты, признается необходимым для безопасности и регулярности международной аэронавигации, а единообразное применение требований, включенных в Рекомендуемую практику, считается желательным в интересах безопасности, регулярности и эффективности международной аэронавигации. Для обеспечения безопасности и регулярности международной аэронавигации весьма важно знать, какие имеются различия между национальными правилами и практикой того или иного государства и положениями Международного стандарта. В случае же несоблюдения какого-либо Международного стандарта Договаривающееся государство, согласно статье 38 Конвенции, обязано уведомить об этом Совет. Для обеспечения безопасности аэронавигации могут также иметь значение сведения о различиях с Рекомендуемой практикой, и, хотя Конвенция не предусматривает каких-либо обязательств в этом отношении, Совет просил Договаривающиеся государства уведомлять не только о различиях с Международными стандартами, но и с Рекомендуемой практикой.

Правила аэронавигационного обслуживания (PANS) утверждаются Советом и предназначены для применения во всем мире. Они содержат в основном эксплуатационные правила, которые не получили еще статуса Международных стандартов и Рекомендуемой практики, а также материалы более постоянного характера, которые считаются слишком подробными, чтобы их можно было включить в Приложение, или подвергаются частым изменениям и дополнениям и для которых процесс, предусмотренный Конвенцией, был бы слишком затруднителен.

Дополнительные региональные правила (SUPPS) имеют такой же статус, как и PANS, но применяются только в соответствующих регионах. Они разрабатываются в сводном виде, поскольку некоторые из них распространяются на сопредельные регионы или являются одинаковыми в двух или нескольких регионах.

В соответствии с принципами и политикой Совета подготовка нижеперечисленных изданий производится с санкции Генерального секретаря.

Технические руководства содержат инструктивный и информационный материал, развивающий и дополняющий Международные стандарты, Рекомендуемую практику и PANS, и служат для оказания помощи в их применении.

Аэронавигационные планы конкретизируют требования к средствам и обслуживанию международной аэронавигации в соответствующих аэронавигационных регионах ИКАО. Они готовятся с санкции Генерального секретаря на основе рекомендаций региональных аэронавигационных совещаний и принятых по ним решений Совета. В планы периодически вносятся поправки с учетом изменений требований и положения с внедрением рекомендованных средств и служб.

Циркуляры ИКАО содержат специальную информацию, представляющую интерес для Договаривающихся государств, включая исследования по техническим вопросам.

ISBN 92-9194-590-0

9/05, R/P1/70

Заказ № 9855
Отпечатано в ИКАО