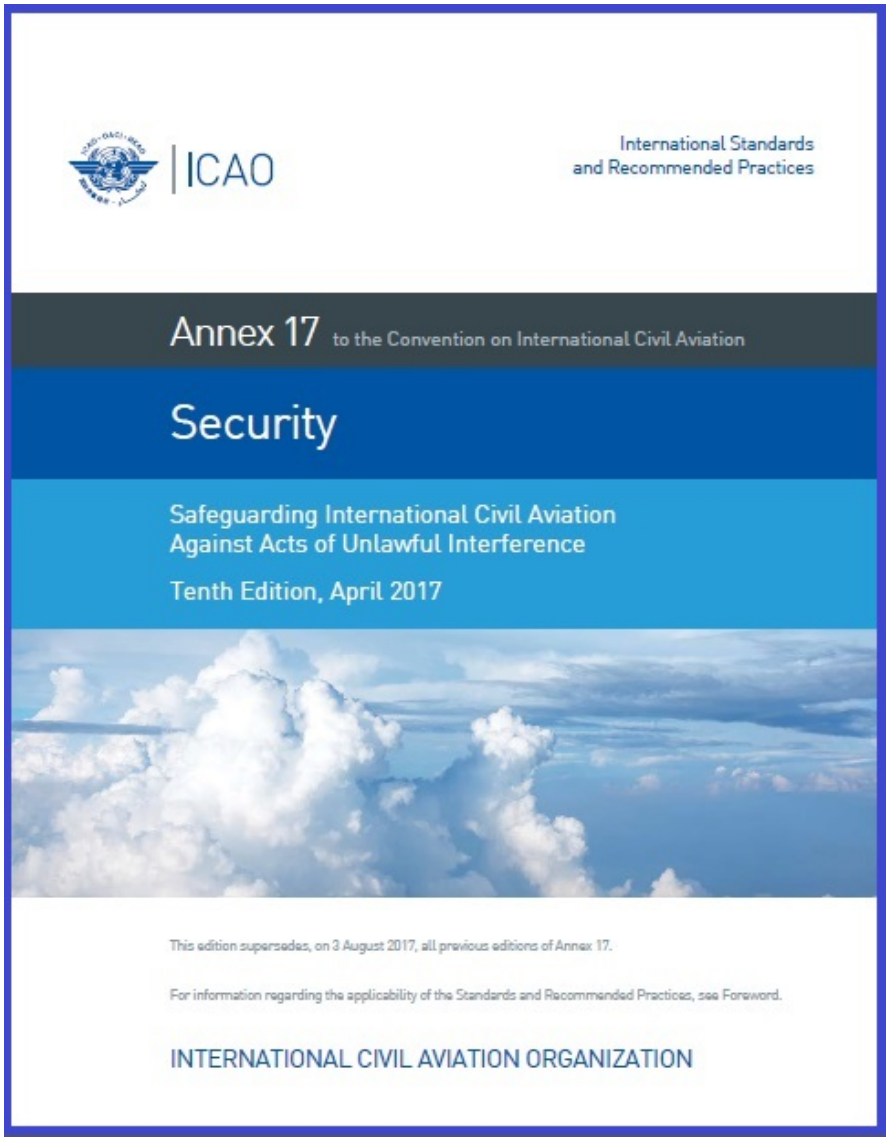
МИНИСТЕРСТВО ТРАНСПОРТА РОССИИ
ФГУП ГосНИИ ГА

Московский региональный учебный центр ИКАО по АБ

Кибербезопасность в гражданской авиации

Докладчик:

Лаврентьев Олег Юрьевич, директор Московского регионального учебного центра ИКАО по АБ – НЦ-24 ФГУП ГосНИИ ГА



Приложение 17 «Безопасность»:

- **Поправка 12 (9-е издание)** от 01.07.2011 – введено понятие «киберугроза»;

- **Поправка 15 (10-е издание)** от 03.08.2017 – изменена редакция существующих положений, касающихся проведения оценок риска и мер защиты от «киберугроз»;

- **Поправка 16 (10 издание)** от 16.11.2018 – внесены новые, пересмотренные положения в отношении «киберугроз».

Стандарт 4.9.1 Приложения 17: «Каждое Договаривающееся государство обеспечивает, чтобы эксплуатанты или организации, указанные в национальной программе безопасности гражданской авиации или другой соответствующей национальной документации, **определяли свои критически важные системы информационных и связных технологий и данные, используемые для целей гражданской авиации, и в соответствии с оценкой риска разрабатывали и внедряли, по мере необходимости, меры их защиты от незаконного вмешательства.**

Рекомендуемая практика 4.9.2 Приложения 17: *Каждому Договаривающемуся государству следует обеспечивать, чтобы* ***реализуемые меры защищали, по мере необходимости, конфиденциальность, целостность и готовность определяемых критически важных систем и/или данных****. Указанные меры должны предусматривать, по мере необходимости и в соответствии с оценкой риска, проводимой его соответствующими национальными полномочными органами, в частности,* ***учет аспектов безопасности на этапе разработки, обеспечение безопасности цепи поставок, разделение сетей и защиту и/или ограничение любых возможностей дистанционного доступа.***

ИКАО

Doc 10108 — Restricted

Заявление о глобальном контексте риска в области авиационной безопасности

Издание первое, 2018

Утверждено Генеральным секретарем и опубликовано с его санкции

Международная организация гражданской авиации

Кибербезопасность в гражданской авиации - это защита от нападения, направленного против гражданской авиации, совершаемого в «киберпространстве» или с использованием «киберпространства» в отношении взаимозависимой сети инфраструктур информационных технологий, включая Интернет, телекоммуникационные сети, компьютерные системы, встроенные процессоры и управляющие устройства.

Кибератаки в отношении систем управления гражданской авиацией

1. Систем аэропорта;
2. Систем ОрВД;
3. Систем воздушных судов.

Doc 10108, ДСП, 2018 - киберурозы в гражданской авиации носят низкий уровень риска.

Системы аэропорта, которые могут быть подвергнуты кибератакам:

- системы контроля управления доступом;
- системы оформления пропусков;
- системы видеонаблюдения, охраны и сигнализации;
- системы электроснабжения, в том числе и резервных источников питания;
- системы идентификации багажа и груза;
- системы электронного оформления перевозочных документов и предоставления сопутствующих услуг (электронные документы);
- системы передачи данных о пассажирах и членах экипажа и т.д., и т.п.

Системы ОрВД:

«Руководство по безопасности системы организации воздушного движения»
(Doc 9985, ДСП, 2013)

- ресурсы и компоненты системы ОрВД;
- командные, контрольные и диспетчерские системы;
- системы контроля доступа и охранной сигнализации;
- замкнутые телевизионные системы наблюдения;
- базы данных о зарегистрированных агентах и/или известных грузоотправителях;
- портативные и непортативные электронные устройства, используемые для обработки, хранения и передачи критически важной информации ОрВД и т.д., и т.п.

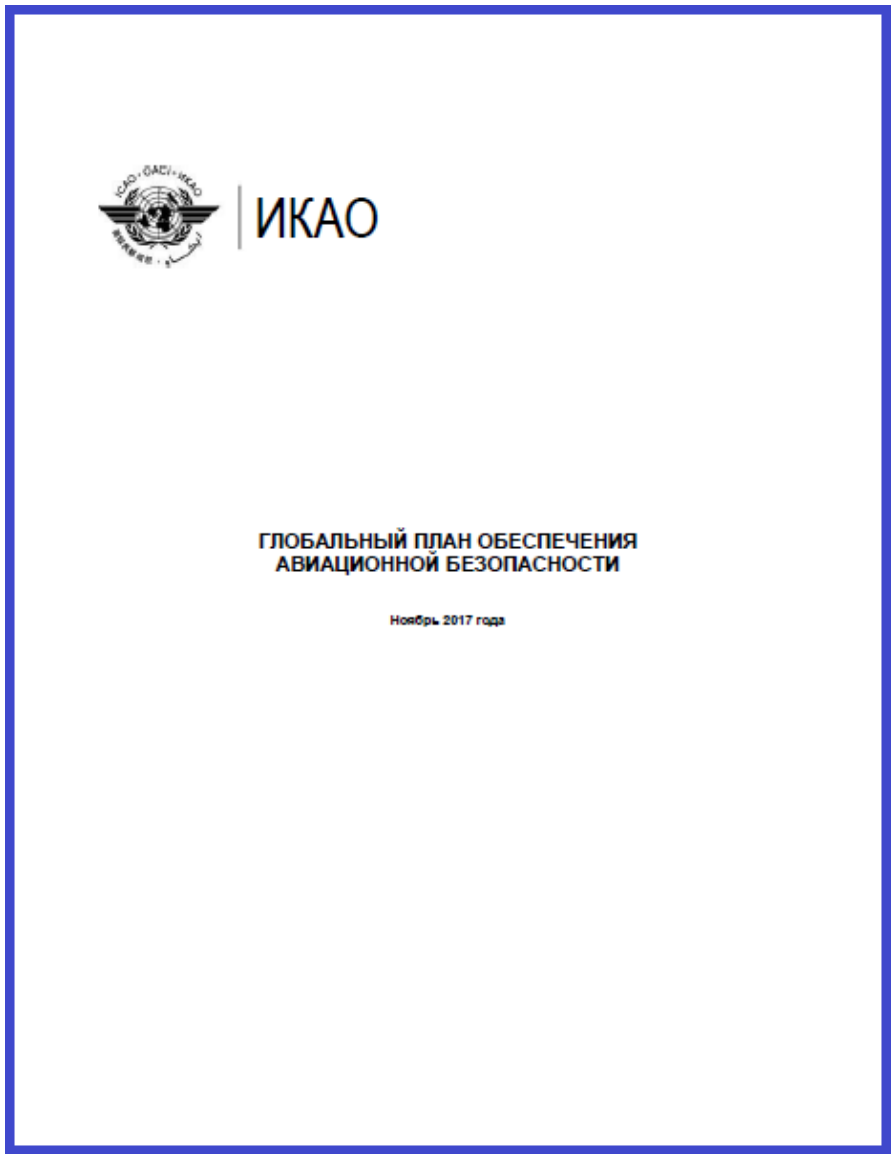
Воздушные суда ГА:

- навигационные системы и электронные полетные планшеты экипажа воздушного судна;
- системы, выполняющие критически важные операции, необходимые для обеспечения безопасности полета ВС (системы управления двигателями, технического обслуживания ВС и т.д.);
- системы бортовых сетей передачи данных ВС, средств связи и навигации;
- системы беспроводных телекоммуникационных и информационно-измерительных устройств на борту ВС;
- системы беспроводных каналов передачи данных, обеспечивающих доступ к бортовой вычислительной сети ВС.
- системы развлечения пассажиров ВС;
- все системы ВС, при наличие в программном обеспечении и в бортовом радиоэлектронном оборудовании незадекларированных возможностей (заранее и умышленно внедренных закладок) и т.д., и т.п.

Системы управления авиационной безопасностью (СУАБ, ДСП, 2015)

СУАБ должна содержать следующие ключевые компоненты кибербезопасности:

а) приверженность руководства по вопросам обеспечения кибербезопасности;
б) ресурсы, выделяемые на кибербезопасность, включая расходы на привлечение внешних поставщиков услуг;
в) угрозы и риски в сфере обеспечения кибербезопасности;
г) контроль за эффективностью мер обеспечения кибербезопасности и их постоянным совершенствованием;
д) информацию по реагированию на киберурозы и кибератаки;
е) информацию по подготовке работников по вопросам обеспечения кибербезопасности;
ж) информационное взаимодействие.



Пять ключевых приоритетных результатов ГПАБ:

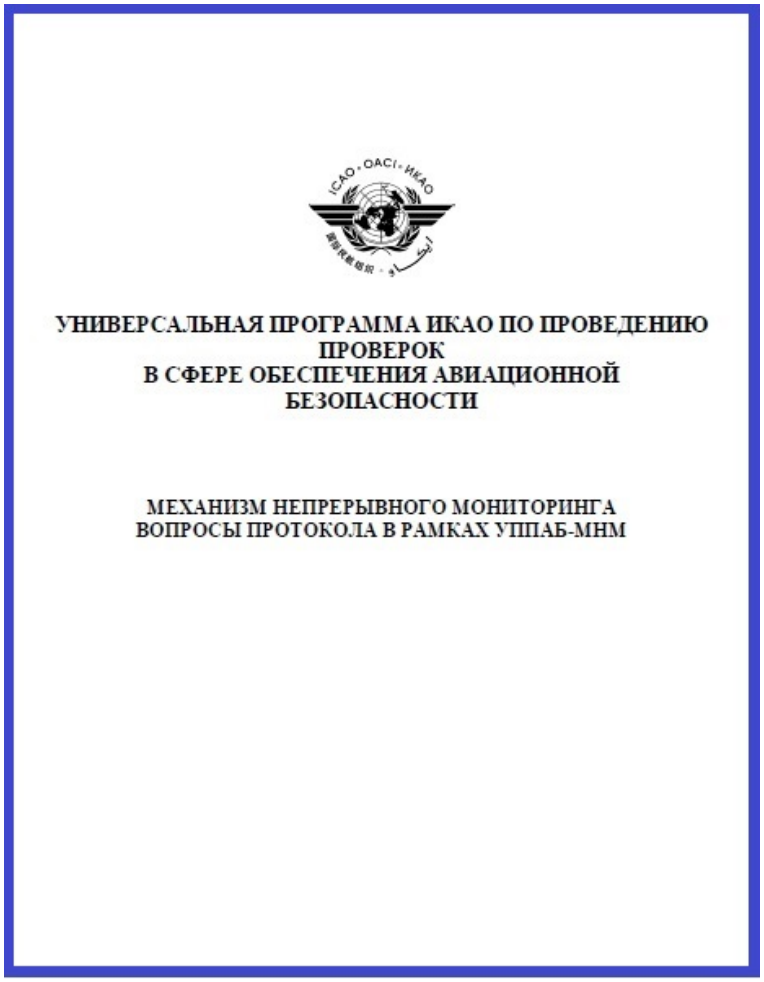
1. Улучшение осведомленности о рисках и реагирования на них.
2. Развитие культуры авиационной безопасности и возможностей человека.
3. Расширение технических ресурсов и инноваций.
4. Усовершенствование надзора и контроля качества.
5. Развитие сотрудничества и поддержки.

Пункт 1.1. «Приоритетные действия» Добавление А: «Дорожная карта реализации глобального плана обеспечения авиационной безопасности» ГПАБ:

- Подпункт 1.A: «Выявление и устранение угроз кибербезопасности критически важных объектов инфраструктуры, данных и информации, и технических систем связи гражданской авиации путем сотрудничества с использованием горизонтального, междисциплинарного и функционального подходов для достижения удовлетворительных и соизмеримых в глобальном масштабе возможностей обеспечения киберустойчивости».

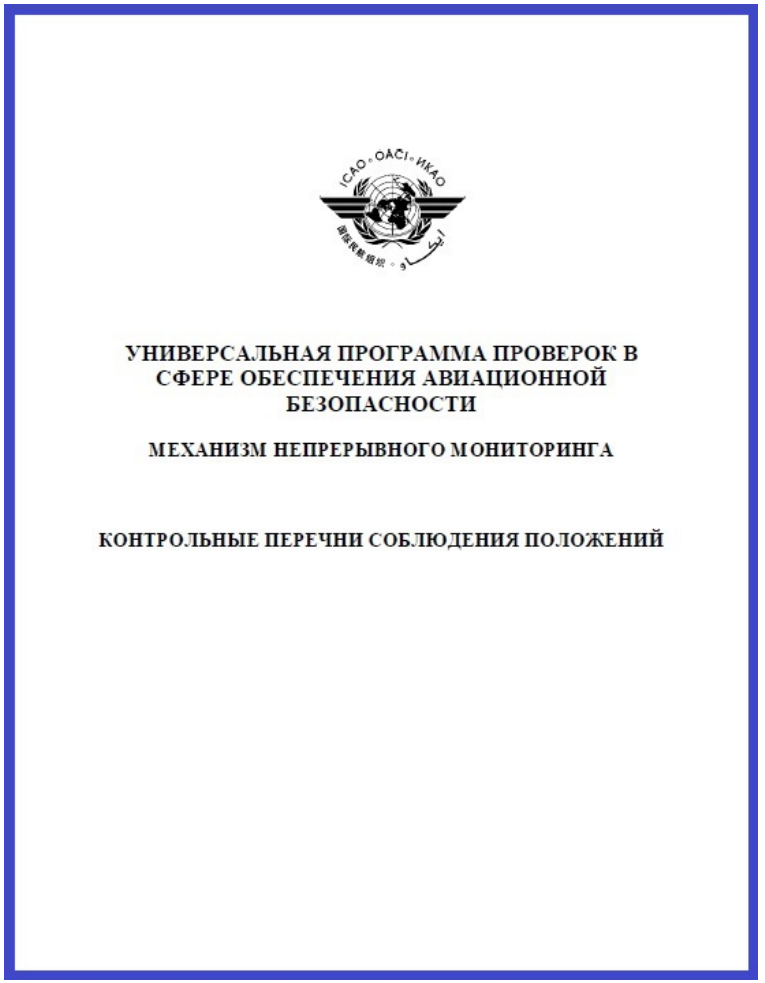
- Подпункт 1.B: «Мониторинг и устранение возникающих и изменяющихся рисков, связанных с кибербезопасностью, дистанционно пилотируемыми авиационными системами (ДПАС), а также рисков, возникающих в зонах конфликтов».

Механизм непрерывного мониторинга в рамках Универсальной программы проверок в сфере авиационной безопасности ИКАО (УППАБ-МНМ)



УНИВЕРСАЛЬНАЯ ПРОГРАММА ИКАО ПО ПРОВЕДЕНИЮ ПРОВЕРОК
В СФЕРЕ ОБЕСПЕЧЕНИЯ АВИАЦИОННОЙ БЕЗОПАСНОСТИ

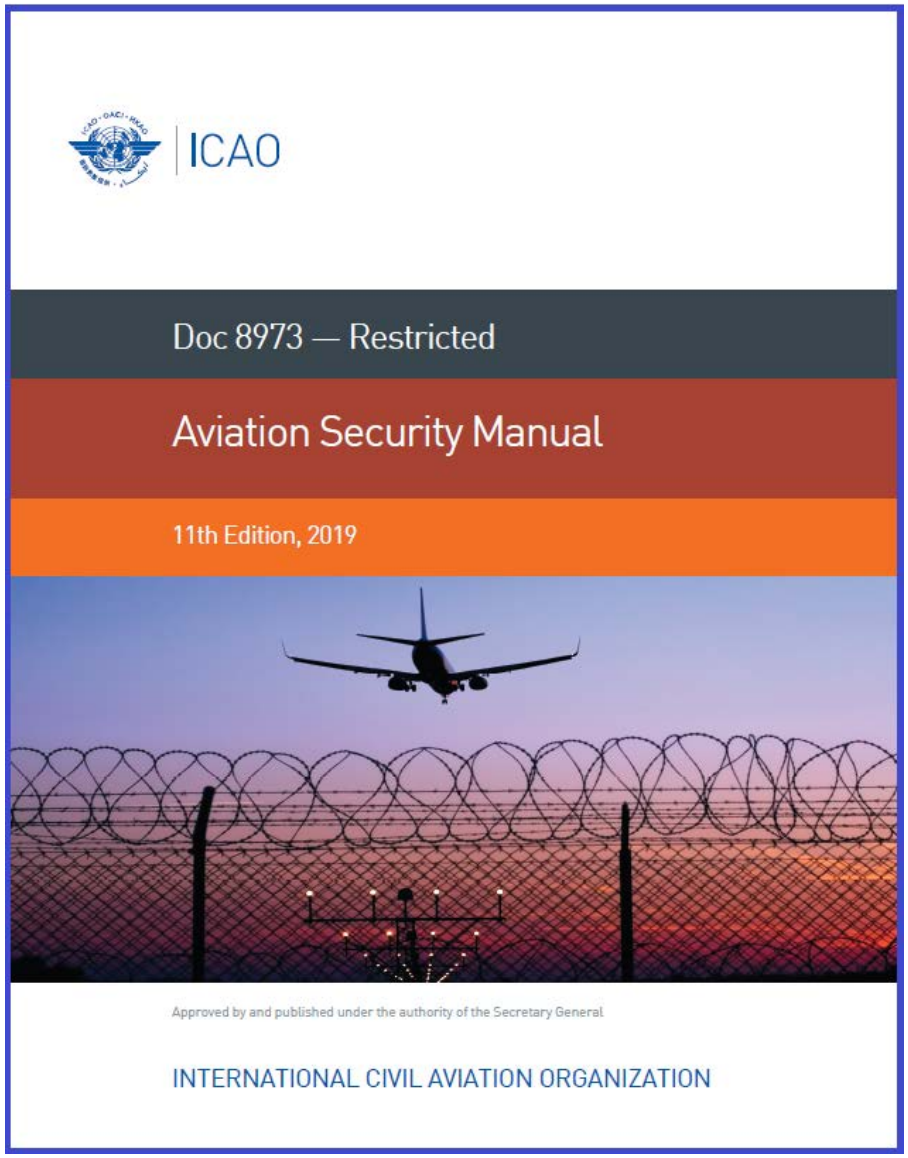
МЕХАНИЗМ НЕПРЕРЫВНОГО МОНИТОРИНГА
ВОПРОСЫ ПРОТОКОЛА В РАМКАХ УППАБ-МНМ



УНИВЕРСАЛЬНАЯ ПРОГРАММА ПРОВЕРОК В СФЕРЕ ОБЕСПЕЧЕНИЯ АВИАЦИОННОЙ БЕЗОПАСНОСТИ

МЕХАНИЗМ НЕПРЕРЫВНОГО МОНИТОРИНГА

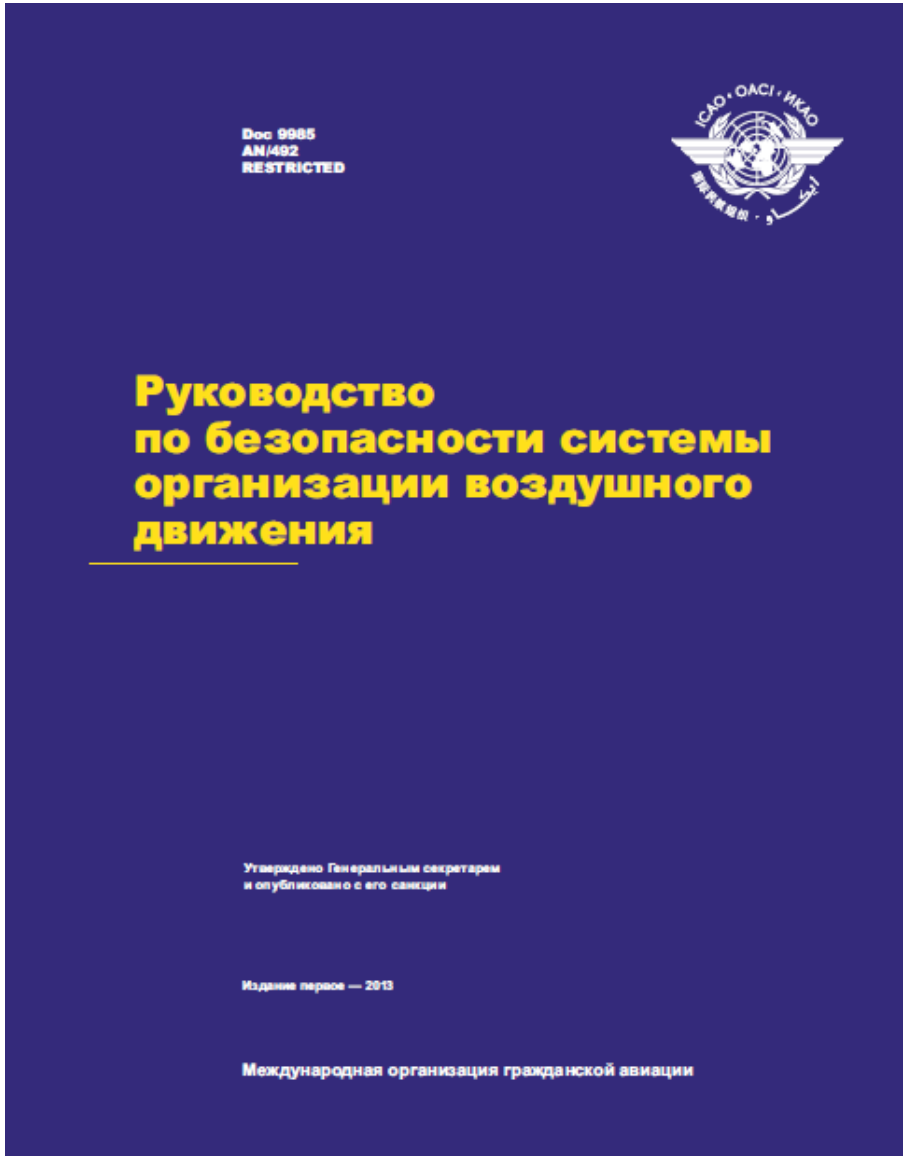
КОНТРОЛЬНЫЕ ПЕРЕЧНИ СОБЛЮДЕНИЯ ПОЛОЖЕНИЙ



Глава 18 Doc 8973 «Руководство по авиационной безопасности» (ДСП, издание 11, ИКАО):

- п. 18.1 «Киберугрозы критически важным авиационным системам информационных и связных технологий»;

- п. 18.2 «Защита критически важных авиационных систем информационных и связных технологий»

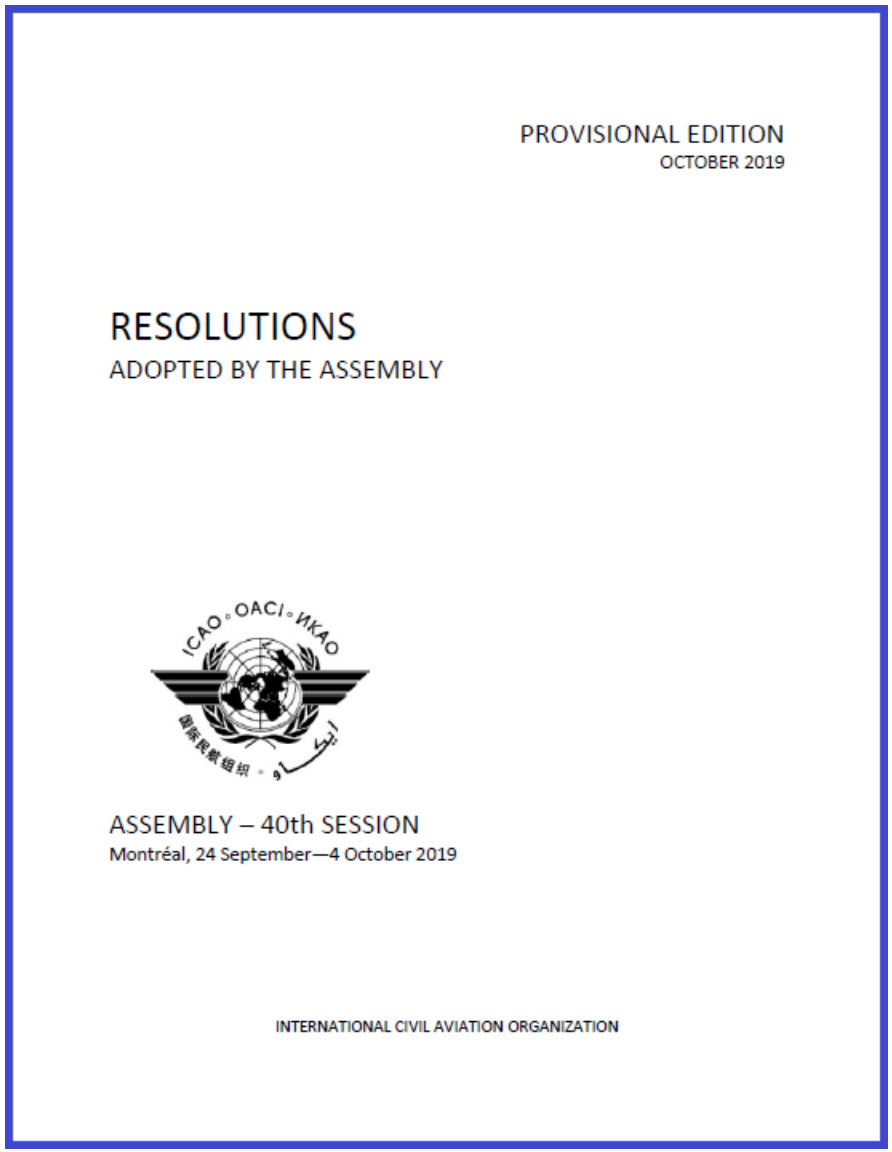


Doc 9985 AN/492

«Руководство по безопасности системы организации воздушного движения» (ДСП, 2013, ИКАО)

- Глава 5: «Обеспечение безопасности систем информационных и связных технологий (включая кибербезопасность)»;

- Добавление B: «Роль кибербезопасности в обеспечении защиты систем информационных и связных технологий».


PROVISIONAL EDITION
OCTOBER 2019

RESOLUTIONS
ADOPTED BY THE ASSEMBLY

ASSEMBLY – 40th SESSION
Montréal, 24 September—4 October 2019

INTERNATIONAL CIVIL AVIATION ORGANIZATION

40-я сессия Ассамблеи ИКАО

(г.Монреаль, 24 сентября – 4 октября 2019 г.)

«Предварительная редакция Ассамблеи» (октябрь 2019):

Резолюция А40-10: «Решение проблемы кибербезопасности в гражданской авиации»

Стратегия в области авиационной кибербезопасности (2019, ИКАО)

Семь основополагающих элементов Стратегии:

1. Международное сотрудничество.
2. Управление.
3. Эффективное законодательство и нормативные положения.
4. Политика в области кибербезопасности.
5. Обмен информацией.
6. Планирование мероприятий на случай инцидентов и действий в чрезвычайных ситуациях.
7. Наращивание потенциала, подготовка персонала и формирование культуры кибербезопасности.

СПАСИБО ЗА ВНИМАНИЕ