



**РАБОЧИЙ ДОКУМЕНТ**

**АССАМБЛЕЯ — 39-Я СЕССИЯ**

**ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ**

**Пункт 16 повестки дня. Авиационная безопасность. Политика**

**РЕШЕНИЕ ПРОБЛЕМ КИБЕРБЕЗОПАСНОСТИ В ГРАЖДАНСКОЙ АВИАЦИИ**

(Представлено Советом ИКАО)

**КРАТКАЯ СПРАВКА**

Эффективность деятельности гражданской авиации, безопасность полетов и авиационная безопасность в значительной степени зависят от наличия систем информационных и связанных технологий (ИТ), а также от точности и конфиденциальности данных. Защита авиационных систем от киберугроз, понижение степени их уязвимости и обеспечение способности систем к восстановлению функций могут быть достигнуты исключительно за счет применения согласованного глобального подхода, основанного на сотрудничестве и включающего коллективную экспертную работу в области авиационной безопасности, аэронавигации, безопасности систем ИТ и участие специалистов из других соответствующих областей.

В 2013 году ИКАО, Международный совет аэропортов (МСА), Организация по аэронавигационному обслуживанию гражданской авиации (КАНСО), Международная ассоциация воздушного транспорта (ИАТА) и Международный координационный совет ассоциаций аэрокосмической промышленности (ИККАИА) учредили Отраслевую группу высокого уровня (IHLG) в качестве механизма сотрудничества на высоком уровне по вопросам, представляющим общий интерес и взаимную важность, к которым относится и кибербезопасность. В этом отношении группа IHLG заключила, что кибербезопасность в гражданской авиации представляет имеющую приоритетное значение проблему общую для всех, требующую согласованных и координированных действий всех соответствующих заинтересованных сторон.

В стремлении оказать дальнейшую поддержку последовательному и согласованному подходу к управлению киберугрозами и факторами риска ИКАО и члены IHLG разработали проект резолюции, приведенный в добавлении к настоящему документу, направленный на решение проблем кибербезопасности в гражданской авиации на основе единого, комплексного и функционального подхода. Резолюция имеет целью вновь подтвердить важность и актуальность защиты критически важных систем инфраструктуры гражданской авиации и данных от киберугроз и добиться глобальной решимости со стороны ИКАО, ее государств-членов и заинтересованных сторон отрасли предпринять активные действия, направленные на совместное и систематическое решение проблем кибербезопасности в гражданской авиации и борьбу с соответствующими угрозами и рисками.

**Действия:** Ассамблее предлагается принять проект резолюции "*Решение проблем кибербезопасности в гражданской авиации*", приведенный в добавлении.

<i>Стратегические цели</i>	Настоящий документ связан со стратегическими целями А "Безопасность полетов", В "Аэронавигационный потенциал и эффективность" и С "Авиационная безопасность и упрощение формальностей"
<i>Финансовые последствия</i>	Деятельность, описанная в данном документе, будет осуществляться при наличии ресурсов в бюджете Регулярной программы на 2017–2019 гг. и/или за счет внебюджетных взносов
<i>Справочный материал</i>	<i>Действующие резолюции Ассамблеи</i> (по состоянию на 4 октября 2013 г.) (Дос 10022)

-----

## ДОБАВЛЕНИЕ

### ПРОЕКТ РЕЗОЛЮЦИИ АССАМБЛЕИ РЕШЕНИЕ ПРОБЛЕМ КИБЕРБЕЗОПАСНОСТИ В ГРАЖДАНСКОЙ АВИАЦИИ

#### Резолюция 16/хх. Решение проблем кибербезопасности в гражданской авиации

Ассамблея,

*принимая во внимание*, что глобальная система авиации представляет собой чрезвычайно сложную и интегрированную систему, включающую в себя информационные и связные технологии, имеющие критически важное значение для безопасности полетов и безопасности гражданской авиации в целом,

*принимая к сведению*, что авиационная отрасль во все большей степени зависит от наличия систем информационных и связных технологий, а также от целостности и конфиденциальности данных,

*учитывая*, что представляемая киберинцидентами угроза для гражданской авиации быстро и постоянно изменяется, что носители такой угрозы лелеют преступные намерения, направленные на нарушение деловой активности и кражу информации, по политическим, финансовым или другим мотивам, а также то, что такая угроза может легко причинить вред критически важным системам гражданской авиации во всем мире,

*признавая*, что не все проблемы в области кибербезопасности, имеющие негативное влияние на безопасность полетов гражданской авиации, носят противоправный и/или злонамеренный характер, а потому должны решаться путем применения систем управления безопасностью полетов;

*подтверждая* важность и актуальность защиты критически важных систем инфраструктуры гражданской авиации и ее данных от киберугроз,

*рассматривая* необходимость совместной работы над разработкой эффективной и координированной глобальной программы для заинтересованных сторон в области гражданской авиации по решению проблем кибербезопасности наряду с краткосрочными мероприятиями по повышению устойчивости глобальной системы авиации к киберугрозам, которые могут представлять угрозу безопасности полетов гражданской авиации,

*признавая* значение соответствующих инициатив, планов действий, публикаций и других вариантов решения проблем кибербезопасности на основе сотрудничества и согласованных действий,

*напоминая* инициативы руководителей Международного совета аэропортов (МСА), Организации по аэронавигационному обслуживанию гражданской авиации (КАНСО), Международной ассоциации воздушного транспорта (ИАТА), Международного координационного совета ассоциаций аэрокосмической промышленности (ИККАИА) и ИКАО, признавших необходимость совместной работы и руководствующихся общностью видения проблемы, стратегией и порядком действий по укреплению защиты глобальной системы авиации от киберугроз и повышению ее устойчивости к таким атакам,

*признавая* многогранность и комплексный характер проблем и решений в сфере кибербезопасности,

1. *призывает* государства и заинтересованные стороны отрасли предпринять следующие меры по противодействию киберугрозам в сфере гражданской авиации:

- a) определить угрозы и факторы риска, представляемые возможными киберинцидентами в отношении полетов и критически важных систем гражданской авиации, а также серьезные последствия, к которым могут привести такие инциденты;
- b) определить круг обязанностей национальных органов и заинтересованных сторон отрасли по отношению к кибербезопасности в гражданской авиации;
- c) поощрять выработку общего понимания государствами-членами киберугроз и факторов риска и общих критериев для определения важности объектов и систем, требующих защиты;
- d) поощрять координацию действий между государственными органами и отраслью по отношению к выработке стратегии, политики и планов обеспечения кибербезопасности, а также обмен информацией, необходимой для выявления критических уязвимых мер, которые требуется устранить;
- e) создавать государственно-отраслевые партнерства и механизмы на национальном и международном уровнях и участвовать в их деятельности по систематическому обмену информацией в области киберугроз, инцидентов, тенденций и мер противодействия;
- f) основываясь на едином понимании киберугроз и факторов риска, использовать гибкий, основанный на оценке рисков подход к защите критически важных авиационных систем путем внедрения систем управления кибербезопасностью;
- g) поощрять развитие в национальных органах и в авиационной отрасли устойчивой культуры кибербезопасности на всех уровнях;
- h) определить юридические последствия действий, ставящих под угрозу безопасность полетов воздушных судов путем использования киберуязвимых мест;
- i) способствовать разработке и внедрению международных стандартов, стратегии и передовой практики в сфере защиты применяемых для целей гражданской авиации критически важных систем информации и связи от актов вмешательства, которые могут угрожать безопасности полетов гражданской авиации;
- j) разработать политику и по необходимости выделять ресурсы для обеспечения следующих требований для критически важных авиационных систем: должна быть обеспечена безопасность архитектуры систем на уровне конструкции; системы должны располагать запасом прочности; способы передачи данных должны быть безопасными, обеспечивающими целостность и конфиденциальность данных; должны быть внедрены методы мониторинга систем и выявления инцидентов и представления сообщений о них; необходимо осуществлять ретроспективный анализ киберинцидентов;

- k) сотрудничать в разработке программы ИКАО в сфере кибербезопасности согласно единому, комплексному и функциональному подходу, включающему области аэронавигации, связи, наблюдения, эксплуатации воздушных судов, летной годности и другие соответствующие дисциплины;
2. *порушает* Генеральному секретарю:
- a) оказать государствам и отрасли помощь и содействие в принятии указанных мер;
  - b) обеспечить всестороннее рассмотрение и координацию решения проблем кибербезопасности в ИКАО во всех соответствующих областях.

— КОНЕЦ —