Международная организация гражданской авиации

A40-WP/219[1]
EX/82
5/8/19

РАБОЧИЙ ДОКУМЕНТ

АССАМБЛЕЯ — 40-Я СЕССИЯ

ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ

Пункт 12 повестки дня. Авиационная безопасность. Политика

ПРЕДЛОЖЕНИЕ В ОТНОШЕНИИ СТРУКТУРЫ УПРАВЛЕНИЯ ИКАО В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

(Представлено Международным координационным советом ассоциаций аэрокосмической промышленности (ИККАИА))

КРАТКАЯ СПРАВКА

Кибербезопасность гражданской авиации является широкой, сложной и междисциплинарной областью, охватывающей аспекты информационных технологий, традиционной авиационной безопасности, управления безопасностью полетов и последствий для производства полетов. Поскольку кибербезопасность носит сквозной характер, группы экспертов и исследовательские группы, которые работают в настоящее время при ИКАО, неэффективны в координации такой деятельности, как кибербезопасность. Необходимо создать орган ИКАО, управляемый государствами-членами при поддержке отрасли, который не будет ограничен существующей организационной структурой ИКАО. Такой орган должен иметь возможность обеспечивать эффективную координацию в ИКАО всей деятельности в области кибербезопасности и надлежащее взаимодействие по вопросам кибербезопасности с другими дисциплинами. Он должен отвечать за общую стратегию ИКАО в области кибербезопасности, а также за согласование и ориентацию работы, выполняемой действующими группами экспертов и исследовательскими группами.

Действия: Ассамблее предлагается:

a) просить Совет учредить орган по кибербезопасности гражданской авиации, управляемый государствами-членами при поддержке отрасли, который будет работать над сквозными вопросами в целях консолидации и гармонизации деятельности, связанной с кибербезопасностью, в масштабе всей ИКАО;

b) просить Совет утвердить стратегию кибербезопасности, разработанную SSGC, признавая при этом, что структурой SSGC не предусматривался горизонтальный и сквозной характер вопроса кибербезопасности;

c) поручить Генеральному секретарю координировать свои действия с государствами и отраслью для гармонизации процессов управления рисками в сфере кибербезопасности, учитывая работу по гармонизации, которая уже осуществляется на региональном или национальном уровне;

d) просить Совет настоятельно призвать государства различных регионов развивать потенциал управления кризисными ситуациями в области кибербезопасности и координировать усилия на международном уровне, чтобы не допустить потерю доверия пассажиров в результате местного инцидента в области авиационной кибербезопасности.

Стратегические цели	Данный рабочий документ связан со стратегическими целями "Безопасность полетов", "Аэронавигационный потенциал и эффективность" и "Авиационная безопасность и упрощение формальностей"
Финансовые последствия	Деятельность, упоминаемая в данном документе, будет осуществляться при наличии ресурсов в бюджете Регулярной программы на 2020–2022 гг. и/или за счет внебюджетных взносов.
Справочный материал	Doc 10075, Действующие резолюции Ассамблеи (по состоянию на 6 октября 2016 года)

[1] Тексты на русском, английском, арабском, испанском, китайском и французском языках представлены ИККАИА.

1. ВВЕДЕНИЕ

1.1 Кибербезопасность гражданской авиации является широкой, сложной и междисциплинарной областью, охватывающей аспекты управления информационными технологиями, традиционной авиационной безопасности, управления безопасностью полетов и последствий для производства полетов.

1.2 Деятельность в сфере кибербезопасности обычно связана с конкретными случаями на местном уровне, и теперь существует необходимость в усилении общей координации, чтобы обеспечить рассмотрение всех аспектов без разрывов и дублирования. Кроме того, учитывая тот факт, что кибербезопасность пересекается со многими видами деятельности ИКАО, необходимо организовать надлежащую координацию между всеми дисциплинами, чтобы обеспечить определение и функционирование единого организационного подхода и процесса принятия решений, принимая во внимание, среди прочего, вопросы безопасности полетов, физической авиационной безопасности и кибербезопасность.

1.3 Поскольку кибербезопасность носит сквозной характер, группы экспертов и исследовательские группы, которые работают в настоящее время при ИКАО, неэффективны в координации такой деятельности, как кибербезопасность. Необходимо создать орган ИКАО, управляемый государствами-членами при поддержке отрасли, который не будет ограничен существующей организационной и политической структурой ИКАО. Такой орган должен иметь возможность обеспечить эффективную координацию в ИКАО всей деятельности в области кибербезопасности и надлежащее взаимодействие по вопросам кибербезопасности с другими дисциплинами. Он должен отвечать за общую стратегию ИКАО в области кибербезопасности, а также за согласование и ориентацию работы, выполняемой действующими группами экспертов и исследовательскими группами.

1.4 Замысел заключается в том, чтобы свести к минимуму накладные расходы и последствия для Организации и максимально использовать существующие структуры для выполнения этой работы, а сам орган будет рассматриваться как структура, определяющая стратегию и концептуальное видение, а также выполняющая руководящую и лидерскую функции. В него войдут представители государств – членов ИКАО, отраслевые и индивидуальные эксперты в области кибербезопасности, которые будут совместно выполнять эту работу и предлагать согласованные ими рекомендации для принятия решения.

2. РАССМОТРЕНИЕ ВОПРОСА

2.1 Централизованный орган по кибербезопасности имеет возможности для решения некоторых проблем, указанных во введении, поскольку он может помочь в удовлетворении потребности в глобальном авиационном междисциплинарном управлении деятельностью в сфере кибербезопасности в ИКАО. Необходимо тщательно проанализировать то, какой тип органа нужен ИКАО для успешного удовлетворения потребностей и достижения целей мирового сообщества гражданской авиации. Плюсы и минусы различных форм организации работы (например, Группа экспертов или Комитет Совета ИКАО) должны быть тщательно взвешены с учетом потребностей и целей, изложенных в настоящем документе.

2.2 При правильном обеспечении ресурсами централизованный орган по кибербезопасности мог бы обеспечить:

- широкий спектр опыта и отраслевых знаний его членов, особенно по вопросу кибербезопасности в гражданской авиации;

- гармонизированный подход к управлению рисками с набором методик, согласованных всеми заинтересованными сторонами, на основе регионального и национального опыта;

- возможность учреждать рабочие группы или распределять работу между существующими органами в целях сосредоточения усилий на разработке Стандартов и Рекомендуемой практики, инструктивных материалов, программ, наращивании потенциала, помощи и подготовке, по мере необходимости;

- рассмотрение всех вопросов кибербезопасности (кибербезопасность для безопасности полетов, производства полетов, технического обслуживания, киберпреступность) в одном органе;

- смешанную группу разных экспертов по кибербезопасности, а также специалистов по безопасности полетов и выполнению полетов, представляющих все заинтересованные стороны в отрасли и разных правительствах. Как минимум, в ней должны быть представлены аэродромы, авиакомпании, производители и поставщики воздушных судов, организации, выполняющие техническое обслуживание, и поставщики навигационного обслуживания.

2.3 Учитывая сквозной и междисциплинарный характер кибербезопасности, рекомендуется развивать всестороннюю координацию с дисциплинами, относящимися к безопасности полетов и авиационной безопасности, на основе прочных связей между Аэронавигационной комиссией, Комитетом по незаконному вмешательству, исследовательскими группами и группами экспертов. Понимая быстро меняющийся характер кибербезопасности и взаимодействия с новыми технологиями, орган по кибербезопасности должен иметь возможность обеспечивать участие всех глобальных экспертов, в том числе отдельных лиц и организаций, не входящих в текущий список "приглашенных организаций" (https://www.icao.int/about-icao/Pages/Invited-Organizations.aspx).

2.4 Признавая, что концепции, которые были представлены в рамках стратегии кибербезопасности, разработанной Исследовательской группой Секретариата по кибербезопасности (SSGC), являются подходящей отправной точкой, на которую следует опираться, этому органу по кибербезопасности следует поручить разработку и реализацию плана действий по всем вопросам, относящимся ко всем направлениям кибербезопасности в гражданской авиации, и поддерживать концептуальное видение, масштаб и стратегию ИКАО в области кибербезопасности. Орган по кибербезопасности ИКАО должен воспользоваться многочисленными и уже осуществляемыми инициативами в области кибербезопасности на региональном и национальном уровнях в качестве средства для ускорения определения и принятия стандартов и инструктивного материала. Данный орган по кибербезопасности должен также, среди прочего:

2.4.1 Консолидировать стратегию SSGC и гармонизировать работу, выполняемую группами и группами экспертов (например, TFSG, Группой экспертов AVSEC и т. д.), чтобы разработать серии принципов, мер и действий в области кибербезопасности, содержащихся в механизме, построенном на восьми главных элементах:

- Международное сотрудничество
- Управление
- Эффективное законодательство и нормативные положения
- Политика
- Обмен информацией
- Заявление о глобальном риске в области кибербезопасности
- Управление инцидентами, а также оперативное воздействие и обеспечение непрерывности
- Наращивание потенциала, подготовка персонала и формирование культуры кибербезопасности

2.4.2 Привлечь Рабочую группу по угрозам и рискам (WGTR) к работе над оценкой рисков кибербезопасности гражданской авиации, возможно, в рамках рабочей группы этого нового органа, или распределить эту работу в соответствующих управлениях ИКАО. Существует острая необходимость в определении руководящих принципов и критериев, чтобы гарантировать сопоставимость результатов анализа при использовании различными государствами-членами и организациями.

2.4.3 Работать с Исследовательской группой по механизму доверия, чтобы содействовать в определении результатов работы, и после двух лет ее существования продолжать гармонизировать и дорабатывать результаты и должным образом распределить последующую работу в соответствующих управлениях ИКАО или действовать по необходимости.

3. ВЫВОДЫ

3.1 Международное сотрудничество и координация необходимы для гармонизации политики и нормативных положений, чтобы обеспечить глобальную интероперабельность кибербезопасности и непрерывность операций. Функционирующие в ИКАО группы экспертов и исследовательские группы неэффективны в координации такой деятельности, как кибербезопасность. Необходимо создать орган ИКАО, управляемый государствами-членами при поддержке отрасли, который не будет ограничен существующей организационной структурой ИКАО. Такой орган должен иметь возможность обеспечивать эффективную координацию всей деятельности в области кибербезопасности в ИКАО и надлежащее взаимодействие по вопросам кибербезопасности с другими дисциплинами.

— КОНЕЦ —