



РАБОЧИЙ ДОКУМЕНТ

АССАМБЛЕЯ — 42-Я СЕССИЯ

ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ

Пункт 13 повестки дня. Авиационная безопасность. Политика

СОЗДАНИЕ РЕГИОНАЛЬНЫХ ГРУПП ПО АВИАЦИОННОЙ КИБЕРБЕЗОПАСНОСТИ В РЕГИОНАЛЬНЫХ БЮРО МЕЖДУНАРОДНОЙ ОРГАНИЗАЦИИ ГРАЖДАНСКОЙ АВИАЦИИ (ИКАО)

(Представлено Венесуэлой (Боливарианская Республика) при поддержке 16 государств – членов
Латиноамериканской комиссии гражданской авиации (ЛАКГА)²).

КРАТКАЯ СПРАВКА

В связи с транснациональным характером авиации и быстрыми темпами ее цифровизации этот сектор превратился в отрасль, включающую значительное число межсетевых элементов и зависящую от разнообразных и сложных ИТ-сетей, которые требуют внедрения новых и более совершенных технологий для повышения эффективности сетей и адаптации к новым глобальным условиям деятельности авиации. Однако в результате такой зависимости авиационный сектор подвергается все более широкому спектру возникающих и сохраняющихся рисков в области кибербезопасности, которые могут создать угрозу для безопасности полетов и авиационной безопасности. Следовательно, обеспечение кибербезопасности уже не является обособленным направлением работы, а включает целый ряд совместных скоординированных мер реагирования, направленных на поиск основанных на индивидуальных возможностях государств решений по противодействию растущему числу киберугроз с учетом региональных реалий.

Действия: Ассамблее предлагается:

- а) поручить Совету дать Секретариату указание создать и сформировать региональные группы по авиационной кибербезопасности в регионах ИКАО. Это является необходимой стратегической мерой по обеспечению целостности, безопасности и надежности воздушного транспорта, а также непрерывности его функционирования, что будет способствовать выработке более устойчивого и упреждающего подхода к киберугрозам в соответствии с Планом действий ИКАО по обеспечению кибербезопасности;
- б) обеспечить включение в состав этих региональных групп по авиационной кибербезопасности квалифицированных экспертов по кибербезопасности, которые будут в состоянии подготовить рекомендации по мерам защиты и передовой практике с учетом результатов работы Группы экспертов по кибербезопасности и региональных потребностей;
- с) признать, что в отличие от других областей авиационная кибербезопасность требует особой технической специализации и координации действий с другими региональными группами в целях обеспечения надлежащего внедрения в каждом регионе стратегий, разработанных Группой экспертов по кибербезопасности.

¹ Текст на испанском языке предоставлен Венесуэлой (Боливарианская Республика).

² Белиз, Боливия (Многонациональное Государство), Бразилия, Гватемала, Гондурас, Доминиканская Республика, Колумбия, Куба, Мексика, Никарагуа, Панама, Парагвай, Сальвадор, Уругвай, Эквадор и Ямайка.

<i>Стратегические цели</i>	Данный рабочий документ связан со стратегической целью <i>"Каждый полет безопасен и защищен"</i>
<i>Финансовые последствия</i>	Упомянутую в настоящем рабочем документе деятельность предлагается осуществлять с использованием ресурсов, имеющихся в бюджете Регулярной программы на текущий трехлетний период, и/или за счет внебюджетных взносов.
<i>Справочный материал</i>	Приложение 17 <i>"Авиационная безопасность"</i> <i>План действий ИКАО по обеспечению кибербезопасности</i> , пп. 5.1.1, 5.8.1, 6.3.1, 9.3.1, 11.1.5 <i>Стратегия ИКАО в области авиационной кибербезопасности</i> (Международное сотрудничество)

1. ВВЕДЕНИЕ

1.1 Гражданская авиация представляет собой отрасль, включающую значительное число межсетевых элементов, которая зависит от целого ряда технологий. Существенная часть глобальной авиационной инфраструктуры в настоящее время опирается на комплексные ИТ-сети, которые способствуют повышению эффективности сектора, однако при этом подвергают его все более широкому спектру сложных и постоянно меняющихся киберугроз, связанных с хищением конфиденциальной информации, нарушением работы критически важных систем навигации, связи и наблюдения и оказанием значительного негативного воздействия на репутацию авиации и степень уверенности в ее безопасности, а также рядом других последствий.

1.2 В этой связи необходимо разработать эффективные механизмы и каналы взаимодействия по вопросам снижения или уменьшения рисков в области кибербезопасности в отрасли, поскольку ее транснациональный характер означает, что кибератака в одной стране может иметь побочные или негативные последствия в масштабе всего региона или всего мира. Следовательно, обеспечение кибербезопасности уже не является обособленным направлением работы, связанным исключительно с авиационной безопасностью, а включает целый ряд совместных скоординированных мер реагирования, выходящих за пределы национальных границ и разработанных с учетом реалий и характерных особенностей каждого региона.

1.3 Киберугрозы имеют характерные особенности, отличающие их от традиционных угроз для безопасности полетов и авиационной безопасности: они развиваются гораздо более стремительно, о чем свидетельствует внезапное появление новых направлений атак и уязвимых мест, которые могут возникать и создаваться в любых регионах мира; как правило, процесс установления личностей правонарушителей и их отличительных признаков является сложным, что иногда позволяет им оставаться анонимными. В этом заключается отличие киберугроз от остальных угроз или рисков, которые обычно требуют физического присутствия или нахождения в непосредственной близости, что кардинально меняет методы обнаружения, реагирования и проведения расследований.

1.4 ИКАО способствует объединению усилий путем обсуждения вопросов кибербезопасности в рамках региональных групп или аналогичных инициатив в области авиационной безопасности; однако при рассмотрении вопросов кибербезопасности важно применять единый межотраслевой подход, призванный обеспечить их включение в различные авиационные дисциплины. Обсуждение вопросов кибербезопасности часто связано со сложными техническими деталями, требующими глубокого понимания ИТ-инфраструктуры и авиационной деятельности.

1.5 Все это свидетельствует о том, что вопросы авиационной кибербезопасности достигли такого уровня сложности и важности, который требует проявления к ним особого отношения и внимания на специализированном форуме квалифицированных специалистов, обладающих конкретными техническими знаниями и координирующих свою работу с аналогичными группами или инициативами в области авиационной безопасности и другими региональными группами, в рамках которых обсуждаются и рассматриваются вопросы, связанные с авиационной кибербезопасностью.

2. АНАЛИЗ

2.1 В соответствии с настоящим предложением основная задача региональных групп экспертов будет заключаться в содействии работе Группы экспертов ИКАО по кибербезопасности (CYSECP) в целях практической реализации глобальной стратегии на региональном уровне, обеспечения должного учета межотраслевого и междисциплинарного вопроса авиационной кибербезопасности в каждом регионе и разработки надлежащего и реалистичного решения данного вопроса. Для этого важно учитывать и наращивать большой объем работы, проделанной членами Группы экспертов, которые приложили значительные усилия для подготовки руководств, рекомендаций и передовой практики, отвечающих условиям сложной авиационной среды.

2.2 Объем и результаты проделанной CYSECP работы часто остаются неизвестными или используются государствами в недостаточной степени. В этой связи региональные группы ИКАО по авиационной кибербезопасности могли бы стать важным каналом распространения, адаптации и внедрения глобальных руководящих принципов в каждом регионе. Это позволило бы государствам извлечь непосредственную пользу из опыта Группы экспертов и предоставляемых ею ресурсов в целях ускорения процесса создания системы обеспечения авиационной кибербезопасности в каждом регионе.

2.3 Официальное создание региональных групп по авиационной кибербезопасности является неотложной задачей. Они будут ориентироваться на организационную структуру и цели Группы экспертов, придерживаясь такой модели сотрудничества, которая будет способствовать укреплению коллективной устойчивости не только посредством содействия обмену информацией и организации специализированной подготовки персонала, но и путем осуществления скоординированных и активных действий. Это позволит внедрить более целенаправленный и эффективный подход, основанный на защите ИТ-инфраструктуры и безопасности полетов, способствуя тем самым обеспечению целостности, безопасности и непрерывности деятельности авиации в наших регионах.