



РАБОЧИЙ ДОКУМЕНТ

АССАМБЛЕЯ – 42-Я СЕССИЯ

ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ

Пункт 13 повестки дня. **Авиационная безопасность. Политика**

СТРАТЕГИЯ В ОБЛАСТИ АВИАЦИОННОЙ КИБЕРБЕЗОПАСНОСТИ В РАМКАХ ПЛАНА СОВМЕСТНОЙ РАБОТЫ ПО ЗАЩИТЕ ГРАЖДАНСКОЙ АВИАЦИИ

(Представлено Колумбией при поддержке 16 государств – членов ЛАКГА²)

КРАТКАЯ СПРАВКА

Авиация переживает беспрецедентную цифровую трансформацию. Такие технологии, как цифровая связь, интеграция интеллектуальных систем, анализ данных, передовое наблюдение, прогнозирующие системы ОрВД и облачные вычисления, преобразуют отрасль. Однако растущая взаимосвязанность увеличивает поверхность для кибератак и уязвимость перед киберугрозами. Все более изощренные атаки ставят под угрозу безопасность полетов, конфиденциальность данных и доверие к системе.

Для противодействия этой проблеме крайне важно укреплять кибербезопасность отрасли. Государствам-членам следует реализовывать рекомендации ИКАО, такие как Стратегия в области авиационной кибербезопасности и План действий по обеспечению кибербезопасности, и адаптировать их к национальным условиям, укрепляя свою организационную культуру, технологическую инфраструктуру и нормативно-правовую базу в области кибербезопасности для решения конкретных проблем, связанных с кибербезопасностью в гражданской авиации.

Кроме того, транзакционный характер киберпространства требует диалога и механизмов технического и операционного сотрудничества между государствами-членами.

Действие: Ассамблее предлагается:

а) поручить Совету ИКАО разработать в рамках ее Стратегического плана на 2026–2050 годы инструмент самооценки для государств, предназначенный для измерения уровня зрелости их систем авиационной кибербезопасности.

Стратегические цели

Данный рабочий документ связан со следующими стратегическими целями "Каждый полет является безопасным и надежным", "Авиация обеспечивает беспрепятственную, доступную и надежную мобильность для всех", "Ни одна страна не остается без внимания"

¹ Версия документа на испанском языке предоставлена Колумбией.

² Белиз, Боливия (Многонациональное Государство), Венесуэла (Боливарианская Республика), Гватемала, Гондурас, Коста-Рика, Куба, Мексика, Никарагуа, Панама, Парагвай, Перу, Сальвадор, Уругвай, Эквадор, Ямайка.

<i>Финансовые последствия</i>	
<i>Справочный материал</i>	Приложение 17 ИКАО "Авиационная безопасность" Документ ИКАО "Стратегия в области авиационной кибербезопасности" Документ ИКАО "Инструктивный материал по политике обеспечения кибербезопасности" Резолюция A41-19 "Решение проблем кибербезопасности в гражданской авиации" Документ ИКАО "План действий по обеспечению кибербезопасности"

1. ВВЕДЕНИЕ

1.1. Глобальная авиация претерпевает беспрецедентную цифровую трансформацию, движимую передовыми технологиями. Однако эта цифровизация увеличивает уязвимость к кибератакам, которые могут поставить под угрозу безопасность и доверие к системе. Таким образом, усиление кибербезопасности крайне важно для защиты информации и поддержания непрерывности воздушных перевозок.

1.2. Государства разработали всеобъемлющую стратегию в области кибербезопасности, которая включает подготовку людских ресурсов, укрепление технологий для обеспечения безопасности, создание нормативно-правовой базы, государственно-частное партнерство и международное сотрудничество. Эта стратегия направлена на всестороннее улучшение подготовки кадров, технологической инфраструктуры и управления рисками на государственном уровне.

1.3. Международное сотрудничество имеет ключевое значение для укрепления устойчивости авиации к киберугрозам. Обмен информацией, координация реагирования и механизмы взаимодействия, важность которых была продемонстрирована инцидентом 19 июля 2024 года, затронувшим системы управления авиакомпаний по всему миру, помогают снижать риски и обеспечивать безопасность полетов.

1.4. Цифровизация повысила уязвимость гражданской авиации к кибератакам, которые ставят под угрозу ее безопасность и инфраструктуру. Укрепление кибербезопасности является стратегическим приоритетом для обеспечения непрерывности и устойчивости.

1.5. Стратегия в области авиационной кибербезопасности и План действий по обеспечению кибербезопасности ИКАО предоставляют прочную основу для решения этих проблем. Однако эффективная реализация этих рекомендаций требует согласованных и непрерывных действий на региональном уровне, а также твердой приверженности всех заинтересованных сторон, включая государства-члены, отрасль и академические круги, в качестве катализатора Стратегических целей ИКАО на 2026–2050 гг.

2. РАССМОТРЕНИЕ

2.1. Цифровизация оптимизировала гражданскую авиацию, улучшив ее процессы и конкурентоспособность. Однако взаимосвязанность систем увеличила риски кибербезопасности, включая несанкционированный доступ к данным и вмешательство в критически важные системы.

Поэтому государства должны укреплять свои национальные возможности и сотрудничать для повышения безопасности полетов и доверия к сектору.

2.2. Гражданская авиация сталкивается с проблемой использования преимуществ цифровизации при одновременном обеспечении кибербезопасности. Это требует внедрения технологий цифровой безопасности, подготовки кадров, обмена опытом, а также разработки политики и стратегий информационной и цифровой безопасности для отраслевых предприятий.

2.3. ИКАО рассматривает кибербезопасность как общую ответственность, требующую международного сотрудничества. Поскольку киберугрозы быстро эволюционируют и не знают границ, государства должны реагировать на них оперативно и скоординированно, обмениваясь информацией, передовой практикой и техническими ресурсами.

2.4. Кибератаки на гражданскую авиацию представляют собой не гипотетическую угрозу, а реальную проблему. Злоумышленники могут угрожать критическим системам, таким как системы управления воздушным движением и системы управления навигацией и полетами, подвергая опасности миллионы пассажиров и членов экипажей. Кроме того, кибератаки могут вызывать значительные нарушения воздушных перевозок, приводя к миллионным финансовым потерям и нанося ущерб репутации отрасли.

2.5. Гражданская авиация сталкивается с киберрисками, включая кражу данных, манипуляции с системами, нарушение работы критически важных служб и потерю общественного доверия. Укрепление кибербезопасности имеет ключевое значение для обеспечения безопасности и защищенности полетов и сохранения стабильности сектора.

2.6. В условиях растущей угрозы кибератак необходимо применять комплексный и совместный подход для усиления кибербезопасности в гражданской авиации путем создания надежного механизма для руководства государствами и заинтересованными сторонами при внедрении эффективных мер безопасности. Этот механизм должен опираться на заинтересованность высшего руководства, эффективное управление и четкую политику в области кибербезопасности для защиты критически важной информации и систем обеспечения полетов.

2.7. Следует создать процесс для укрепления потенциала в области кибербезопасности гражданской авиации. Его стратегия должна строиться на четырех столпах: i) подготовка кадров; ii) укрепление внутренней технологической инфраструктуры; iii) разработка нормативно-правовой базы для содействия обеспечению кибербезопасности в гражданской авиации; и iv) сотрудничество между организациями.

2.8. Эта стратегия направлена на содействие обеспечению безопасности гражданской авиации путем управления целостностью, доступностью и конфиденциальностью информации в критических системах, обеспечивая тем самым эффективное предоставление услуг и защиту чувствительных данных с помощью высококвалифицированных специалистов. Также следует внедрить надежную нормативно-правовую базу для усиления кибербезопасности авиакомпаний, аэропортов, поставщиков и производителей, поддерживающую надежные методы обеспечения безопасности и скоординированное реагирование на киберинциденты, чтобы повысить устойчивость и сохранить доверие пользователей перед лицом растущих цифровых угроз.

2.9. Кроме того, крайне важно развивать специализированные кадры посредством непрерывного обучения в области кибербезопасности. Подготовка квалифицированных специалистов имеет ключевое значение для обеспечения безопасности полетов и снижения рисков, связанных с текучестью кадров. Также существует необходимость создания специализированного центра реагирования на киберинциденты в гражданской авиации для обеспечения быстрого и скоординированного реагирования на киберинциденты. Этот центр должен служить основой для управления инцидентами, координации усилий с отраслевыми заинтересованными сторонами и обучения собственной группы специалистов.

2.10. Международное сотрудничество является другим ключевым элементом для обмена информацией и разработки совместных имитационных учений для эффективного реагирования на трансграничные киберугрозы. Единая технологическая платформа будет способствовать обмену знаниями и передовой практикой.

2.11. Следует поддерживать постоянный диалог с органами власти и отраслевыми предприятиями для координации единообразного реагирования на киберугрозы. Однако киберпространство не знает границ, поэтому такой диалог должен включать государства, которым следует разработать эффективные и надежные механизмы для обмена опытом и рекомендациями по национальным стратегиям в области кибербезопасности.

2.12. Ключевое значение имеет то, что национальные стратегии в области кибербезопасности должны основываться на законах и правилах каждого государства, но они также должны быть совместимыми, чтобы обеспечивать безопасность полетов в глобальном масштабе. Следует поощрять сотрудничество и обмен информацией между экспертами для выявления и устранения уязвимостей и укрепления устойчивости отрасли к кибератакам. Также важно создать постоянный форум, где эксперты могут давать обратную связь по местным стратегиям и совместно работать над устранением пробелов, которые могут быть использованы киберпреступниками или кибертеррористами.

2.13. В этой связи считается необходимым, чтобы ИКАО способствовала принятию мер по укреплению управления кибербезопасностью в гражданской авиации. Создание инструмента самооценки, интегрированного в Стратегический план на 2026–2050 гг., оправдано, поскольку это позволило бы государствам заблаговременно выявлять политические, оперативные и технические пробелы, способствуя упреждающему планированию мер по снижению рисков и развитию национального потенциала. Это помогло бы обеспечить более единообразный уровень защиты в разных государствах, сокращая асимметрию, которая в настоящее время создает уязвимости в глобальной авиационной сети.

2.14. Кроме того, крайне важно, чтобы ИКАО способствовала разработке более конкретных технических и политических руководящих указаний по кибербезопасности, которые направляли бы усилия государств по принятию передовой практики и международных стандартов. Это способствовало бы созданию общей системы, позволяющей более эффективно противостоять цифровым угрозам, укреплять устойчивость авиационной системы и обеспечивать безопасность и непрерывность воздушных перевозок на глобальном уровне.

3. **ВЫВОД**

3.1. Кибербезопасность в гражданской авиации – это проблема, требующая глобального и скоординированного реагирования. ИКАО в сотрудничестве со своими государствами-членами должна взять на себя ведущую роль в повышении защищенности и устойчивости отрасли к киберугрозам. От этого зависит безопасность миллионов пассажиров и стабильность глобальной авиационной системы.

– КОНЕЦ –