



РАБОЧИЙ ДОКУМЕНТ

АССАМБЛЕЯ – 42-Я СЕССИЯ

ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ

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

АЭРОМОБИЛЬНОСТЬ В СЛОЖНЫХ УСЛОВИЯХ И СВЯЗАННЫЕ С НЕЙ РИСКИ ДЛЯ АВИАЦИОННОЙ БЕЗОПАСНОСТИ

(Представлено Саудовской Аравией)

КРАТКАЯ СПРАВКА

Аэромобильность в сложных условиях (ААМ) и новые технологии, такие как беспилотные авиационные системы (БАС), городская воздушная мобильность (UAM) и усовершенствованные воздушные транспортные средства, произвели революцию в авиационной отрасли. Однако эти изменения создают серьезные проблемы для авиационной безопасности, включая угрозы, связанные с несанкционированным доступом, кибератаками и потенциальным использованием террористами. В настоящем документе рассматриваются риски, связанные с аэромобильностью в сложных условиях, дается оценка существующей системы обеспечения авиационной безопасности и подчеркивается необходимость подготовки ИКАО инструктивных материалов для оказания Договаривающимся государствам помощи в обеспечении авиационной безопасности и установлении национальных требований.

Действия: Ассамблее предлагается:

- а) принять к сведению информацию, представленную в настоящем документе;
- б) призвать Договаривающиеся государства обмениваться любой информацией или опытом с Секретариатом в целях создания справочной базы данных, которая поможет Группе экспертов по авиационной безопасности в разработке нормативной базы и предоставлении инструктивных материалов Договаривающимся государствам на основе инициативного подхода к устранению рисков, обеспечивая безопасную интеграцию ААМ в существующие авиационные системы (в рабочий документ включены предлагаемые руководящие принципы и передовая практика для обеспечения авиационной безопасности аэромобильности в сложных условиях);
- с) призвать Договаривающиеся государства сотрудничать с местными заинтересованными сторонами в целях осуществления адаптированных мер авиационной безопасности и поощрения инвестиций в такие технологии, как передовые решения в области организации движения беспилотных летательных аппаратов, средства кибербезопасности для защиты взаимосвязанных систем и обмен информацией об угрозах с другими государствами.

<i>Стратегические цели</i>	Данный рабочий документ связан со стратегической целью "Каждый полет безопасен и защищен"
----------------------------	---

¹ Версии документа на английском и арабском языках предоставлены Саудовской Аравией.

<i>Финансовые последствия</i>	
<i>Справочный материал</i>	Приложение 17 "Авиационная безопасность" Руководство ИКАО по авиационной безопасности (Doc 8973)

1. ВВЕДЕНИЕ

1.1 Благодаря технологическому прогрессу быстро распространяется концепция аэромобильности в сложных условиях (ААМ). Она открывает возможности для роста, но при этом создает новые риски для авиационной безопасности и потенциальные уязвимости, изменяя характер угроз в сети гражданской авиации. Эти риски требуют инициативного подхода со стороны международных регулирующих органов, таких как ИКАО, для обеспечения безопасности полетов и авиационной безопасности авиации в глобальном масштабе. В настоящем документе обсуждаются последствия внедрения ААМ для авиационной безопасности, определяются возникающие риски и предлагаются меры, которые ИКАО и ее Договаривающиеся государства могут принять для решения этих проблем.

1.2 Под аэромобильностью в сложных условиях понимается перемещение пассажиров и грузов с помощью различных средств воздушного транспорта, включая беспилотные авиационные системы (БАС), платформы городской воздушной мобильности (UAM) и электрические воздушные суда вертикального взлета и посадки (eVTOL).

2. ОБСУЖДЕНИЕ

2.1 Хотя ААМ представляет собой значительный шаг вперед в развитии авиации, она также создает новые проблемы в области авиационной безопасности. Поэтому необходимо разработать комплексный подход к обеспечению авиационной безопасности, который позволял бы учитывать потенциальные риски и обеспечивать защиту авиационной экосистемы от угроз, возникающих в результате этой технологической эволюции. К этим рискам относятся:

- а) Несанкционированный доступ и инсайдерские угрозы:
 - 1. Увеличение числа операций БАС и UAM создает уязвимости в зонах ограниченного доступа аэропортов и на траекториях полетов.
 - 2. Системы аэромобильности в сложных условиях могут быть использованы для незаконного вмешательства.
- б) Угрозы кибербезопасности:
 - 1. Интеграция цифровых систем и автоматизации в UAM увеличивает уязвимость к кибератакам.
 - 2. Террористы могут скомпрометировать навигационные системы, сети связи или оперативные данные.
- в) Неправомерное использование систем ААМ:
 - 1. Системы ААМ могут использоваться для наблюдения, контрабанды или транспортировки взрывчатых веществ.
 - 2. Инциденты с системами аэромобильности в сложных условиях вблизи аэропортов могут нарушить воздушное движение и создать риск столкновений.

2.2 СУЩЕСТВУЮЩАЯ ПРАВОВАЯ БАЗА ДЛЯ ОБЕСПЕЧЕНИЯ АВИАЦИОННОЙ БЕЗОПАСНОСТИ

2.2.1 В Приложении 17 изложены международные стандарты, касающиеся защиты гражданской авиации от актов незаконного вмешательства. Однако быстрое развитие ААМ требует обновления этих стандартов, что позволит обеспечить интеграцию беспилотных и автономных транспортных средств и воздушных операций на малых высотах.

2.2.2 Некоторые государства разработали индивидуальную правовую базу для использования беспилотных летательных аппаратов и БАС. Однако соответствующая политика зачастую не согласована с международными стандартами, что приводит к несоответствиям.

2.3 МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО МЕЖДУ ДОГОВАРИВАЮЩИМИСЯ ГОСУДАРСТВАМИ

2.3.1 Обмен данными: содействие своевременному обмену информацией по вопросам авиационной безопасности между государствами.

2.3.2 Совместные семинары: проведение скоординированных учений и учебных мероприятий для противодействия рискам, связанным с аэромобильностью в сложных условиях.

2.3.3 Усилия по стандартизации: согласование правил проведения операций в области аэромобильности в сложных условиях на международном уровне.

2.4 ИНСТРУКТИВНЫЕ МАТЕРИАЛЫ И ПЕРЕДОВЫЙ ОПЫТ В ОБЛАСТИ АВИАЦИОННОЙ БЕЗОПАСНОСТИ

2.4.1 В настоящем документе содержится приложение с инструктивными материалами для Договаривающихся государств по обеспечению авиационной безопасности в рамках новых операций ААМ, включая городскую воздушную мобильность (UAM), доставку грузов с помощью беспилотных летательных аппаратов (RPAS) и автономные воздушные суда (UAS), в соответствии с Приложением 17 и документом Doc 8973 ИКАО.

APPENDIX

GUIDANCE AND BEST PRACTICES FOR AAM SECURITY

1. Purpose and Scope

This document provides guidance for Contracting States on securing AAM operations, including UAM such as air taxis, RPAS cargo and delivery services, and UAS, in accordance with Annex 17 and operational considerations in Doc 8973.

2. Scope of Application

- Civil Aviation Authorities.
- Airport Operators and Air Navigation Service Providers.
- AAM Operators and Service Providers.
- Relevant National Security Agencies.

3. Objectives

- Prevent acts of unlawful interference via AAM systems.
- Protect civil aviation infrastructure from physical and cyber threats related to AAM.
- Ensure safe integration of AAM into national airspace systems.

4. Best Practices for States

4.1 National Civil Aviation Security Regulatory Framework

- Integrate AAM into National Civil Aviation Security Programs (NCASPs).
- Require all AAM operators to establish written security programs/procedures.
- Require registration and licensing of all AAM operations.

4.1.1 Operator Licensing and Security Programs

- All AAM operators (UAM, UAS) must undergo security audits and be licensed by the Civil Aviation Authority.
- Operators must submit and maintain a security program aligned with the NCASP, including:
 - Roles and responsibilities of all personnel.
 - SOPs for normal and emergency conditions.
 - Coordination with local law enforcement, CAA, and ANSPs.

- Security programs should include regular training, recordkeeping, and quality control mechanisms.

4.2 Security Risk Assessments

- Conduct targeted threat and risk assessments for:
 - Low-altitude operations near critical infrastructure.
 - Launch/recovery sites and vertiports.
 - Communication and navigation systems.
- Update risk assessments periodically and post-incident.

4.3 Access Control and Perimeter Security

- Establish security zones around AAM facilities.
- Secure ground control stations and command centers.
- Integrate AAM vertiports into civil airport perimeter control policies.

4.4 Personnel Security

- Conduct regular background checks on remote pilots, engineers, and ground personnel.
- Ensure training on insider threats and cybersecurity awareness.

5. Operational Security Measures

5.1 Secure Launch/Recovery Sites / Vertiports

- Designated launch/recovery sites and vertiports must:
 - Fenced and access-controlled with human or video surveillance and lighting.
 - Equipped with personnel ID verification systems.
 - Integrated with airport security infrastructure, where applicable.
- Clear operational security responsibilities must be assigned.
- Emergency response procedures (e.g., hijacking, cyber breach) must be established and tested regularly.

5.2 Pre-Flight Screening

- Implement screening controls for cargo or passengers aboard AAM vehicles.
- Verify pre-departure data exchange with competent authorities.
- Advanced Air Mobility operations must follow appropriate pre-flight security procedures.
- When used for commercial passenger/cargo transport:
 - Apply security screening consistent with Annex 17.
 - Verify the identity of all passengers and cargo handlers.
- The possibility of implementing a smart verification mechanism as an alternative to manual verification, such as:
 - Developing an electronic platform for digital user identity verification.
 - Benefiting from national information centers or security databases.
 - Two-factor authentication with biometric verification (e.g., facial recognition).

5.3 Security Monitoring and Oversight

- Deploy counter-UAS (C-UAS) near airports.
- Manage AAM and UAS flights to:
 - Ensure real-time tracking and identification.
 - Detect and respond to operational interference.

5.4 Real-Time Communication and Command

- Operators of Advanced Air Mobility (AAM) systems, such as Urban Air Mobility (UAM) vehicle operators and unmanned aircraft (drone) operators, are required to:
 - Use encrypted communication between aircraft and control stations.
 - Establish a direct communication line with airspace authorities to redirect the aircraft or return it to the ground in emergency situations.

5.5 Cybersecurity Protocols

- Assess cybersecurity vulnerabilities in:

- Autonomous flight software.
- Remote control stations.
- Communication networks.
- Ensure alignment with ICAO's Cybersecurity Strategy.

6. Incident Response and Coordination

6.1 Reporting and Notification

- Integrate AAM systems into national aviation security incident reporting systems.
- Establish a point of contact for coordination with:
 - Air traffic services.
 - Intelligence and law enforcement agencies.

6.2 Response to Unlawful Interference

- Develop emergency response plans for unauthorized interference scenarios.
- Train aviation security staff in response procedures.

7. International and Regional Cooperation

- Data Sharing: Facilitate timely exchange of threat intelligence among States.
- Joint Exercises: Conduct coordinated training and simulation exercises.
- Standardization: Harmonize standards for AAM operations.

8. Capacity Building and Training

- Develop specialized aviation security training modules for:
 - Operators.
 - Security screening personnel.
 - Cybersecurity and risk managers.
- Promote use of ICAO Aviation Security Training Centers (ASTCs) for AAM simulations.

9. Continuous Monitoring and Quality Assurance

- Include AAM systems in national quality control programs.
- Ensure internal compliance monitoring aligns with national and ICAO standards.