



РАБОЧИЙ ДОКУМЕНТ

АССАМБЛЕЯ – 42-Я СЕССИЯ

ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ

Пункт 13 повестки дня. Авиационная безопасность. Политика

НЕОБХОДИМОСТЬ УКРЕПЛЕНИЯ МЕР ПО УПРАВЛЕНИЮ АСПЕКТАМИ ЧЕЛОВЕЧЕСКОГО ФАКТОРА И КИБЕРБЕЗОПАСНОСТЬЮ ПРИ ОБЕСПЕЧЕНИИ АВИАЦИОННОЙ БЕЗОПАСНОСТИ

(Представлено Кубой при поддержке 17 государств – членов ЛАКГА²)

КРАТКАЯ СПРАВКА

В данном документе рассматривается человеческий фактор и его воздействие на развитие и эффективность работы персонала служб авиационной безопасности – принципиально важная область, в которой могут быть разработаны стратегии и приняты дальнейшие меры для привлечения специалистов в области авиационной безопасности и в целом для обеспечения стабильности работы персонала, прошедшего подготовку по исполнению данных функций. В целях дальнейшего укрепления авиационной безопасности, ключевого элемента устойчивого развития воздушного транспорта, необходимы согласованные усилия в области найма и удержания квалифицированных и владеющих должными навыками сотрудников, обеспечивающих управление этой системой и поддерживающих ее эффективность и результативность.

Действия: Ассамблее предлагается:

а) принять к сведению представленную информацию;
б) настоятельно призвать государства к укреплению мер по управлению аспектами человеческого фактора и кибербезопасностью при обеспечении авиационной безопасности, таких как:

- разработка всесторонних планов управления аспектами человеческого фактора и кибербезопасностью, согласованных с Приложением 17 к Чикагской конвенции и стратегией ИКАО в области авиационной безопасности;
- периодическое проведение оценки риска и обновление мер защиты;
- содействие сотрудничеству в целях обмена информацией и передовой практикой на национальном и международном уровне;
- проведение постоянной подготовки персонала по вопросам кибербезопасности и человеческого фактора;
- содействие формированию организационной культуры, ориентированной на обеспечение безопасности и устойчивости в цифровой сфере.

Стратегические цели

Данный рабочий документ связан со стратегической целью "Каждый полет безопасен и защищен"

¹ Версия документа на испанском языке предоставлена Кубой

² Белиз, Боливия (Многонациональное Государство), Бразилия, Венесуэла (Боливарианская Республика), Гватемала, Гондурас, Колумбия, Мексика, Никарагуа, Панама, Парагвай, Перу, Сальвадор, Уругвай, Чили, Эквадор и Ямайка

<i>Финансовые последствия</i>	Ресурсы для найма и подготовки персонала, а также инвестиции в технологии
<i>Справочный материал</i>	Дос 10118 <i>"Глобальный план авиационной безопасности"</i> (ГПАБ), второе издание Резолюция A41-18 <i>"Сводное заявление о постоянной политике ИКАО в области авиационной безопасности"</i> Резолюция A41-19 Ассамблеи <i>"Решение проблем кибербезопасности в гражданской авиации"</i> Приложение 17 <i>"Авиационная безопасность"</i> Дос 8973 <i>"Руководство по авиационной безопасности"</i> Стратегия в области авиационной кибербезопасности Маскатская декларация по авиационной безопасности и авиационной кибербезопасности

1. ВВЕДЕНИЕ

1.1 Авиационная безопасность является основой устойчивого и эффективного развития воздушного транспорта во всем мире. Для обеспечения безопасной и надежной деятельности этого сектора, играющего принципиальную роль в достижении глобальной связности и экономического роста, необходимы высокие стандарты безопасности. Человеческий фактор имеет в этом контексте решающее значение, поскольку предотвращение инцидентов и авиационных происшествий в значительной степени зависит от подготовки сотрудников, эффективности их работы и принимаемых ими решений на всех этапах производства полетов. Кроме того, успешная реализация международных стандартов и процедур может быть достигнута только путем эффективного управления аспектами человеческого фактора, области, требующей дальнейшего изучения и применения полученных данных в целях повышения безопасности и обеспечения устойчивости авиационной системы.

1.2 Сложность авиационной системы, возрастающая в результате развития технологий и возникновения новых угроз, обусловила создание международным сообществом надежных нормативно-правовых механизмов. В этом отношении Приложение 17 ИКАО является основным сводом правил защиты гражданской авиации от актов незаконного вмешательства в ее деятельность, включая угрозы как в физической, так и в цифровой сфере. В этом Приложении признается, что обеспечение авиационной безопасности предусматривает не только физические барьеры и процедуры, но и всестороннее управление человеческим фактором и кибербезопасностью. Оба этих элемента стали необходимы для обеспечения устойчивости авиации в противостоянии нынешним и будущим вызовам.

2. РАССМОТРЕНИЕ ВОПРОСА

2.1 Человеческий фактор охватывает все аспекты поведения, показателей эффективности работы, навыков и ограничений, присущих сотрудникам служб безопасности. Сюда входит отбор и подготовка персонала, управление стрессом и усталостью, коммуникация и принятие решений в экстренных ситуациях. Персонал служб безопасности должен проходить основательную техническую и профессиональную подготовку, специальную сертификацию и иметь опыт управления подобными ситуациями. Чрезвычайно важно обеспечивать постоянную

подготовку такого персонала, с тем чтобы соответствовать темпам постоянного видоизменения угроз и развития технологий обеспечения безопасности.

2.2 Среди существующих в настоящее время проблем следующие:

- a) **Дефицит квалифицированного персонала.** Отрасль испытывает проблемы, связанные с привлечением и удержанием перспективных сотрудников, прошедших специальную подготовку, что может сказаться на эффективности мер обеспечения безопасности и ограничить возможности реагирования на инциденты.
- b) **Усталость и избыточная рабочая нагрузка.** Дефицит людских ресурсов может приводить к продлению рабочего дня, усталости и падению уровня эффективности работы, что повышает риск возникновения ошибок и опасных ситуаций.
- c) **Адаптация к технологиям.** Быстрое внедрение новых технологий требует от персонала адаптации и развития навыков работы в цифровой среде для управления сложными системами и защиты конфиденциальной информации.
- d) **Управление конфиденциальной информацией.** Персонал должен быть способен обрабатывать конфиденциальные данные и реагировать на инциденты в сфере безопасности, в том числе на киберугрозы.
- e) **Многообразие и работа в группе.** Работа в группах, состав которых характеризуется культурным и возрастным многообразием, требует развитых навыков коммуникации и лидерства, позволяющих предотвратить недопонимание и содействовать совместной работе.

2.3 Нехватка персонала служб безопасности может вести к возникновению ошибок, задержкам в процессах и уменьшению способности реагировать на инциденты. Она может также воздействовать на реализацию мер безопасности и вызвать увеличение рабочей загрузки, что может привести к возникновению опасных ситуаций. Результатом этого может стать повышенный уровень эксплуатационных рисков и невыявленные угрозы.

2.4 Среди стратегий предотвращения возникновения дефицита людских ресурсов и смягчения его последствий следующие:

- a) кадровое планирование;
- b) наем и удержание сотрудников;
- c) постоянная подготовка персонала;
- d) поддержка средствами технологий;
- e) улучшение условий труда;
- f) контроль и постоянное совершенствование.

2.5 С появлением цифровой среды возникли новые риски и проблемы в области авиационной безопасности. В Приложении 17 ИКАО признается важность обеспечения кибербезопасности для защиты от актов незаконного вмешательства. Чтобы подготовить персонал служб безопасности к выявлению, предотвращению и реагированию на киберугрозы, эта подготовка должна включать следующее:

- a) **подготовка по вопросам кибербезопасности:** специальная подготовка по выявлению цифровых угроз и выполнению протокола реагирования;

- b) **урегулирование киберинцидентов:** отработка навыков реагирования на инциденты, способные негативно повлиять на безопасность;
- c) **осведомленность и культура в вопросах кибербезопасности:** содействие применению передовой практики и повышению уровня осведомленности персонала на всех уровнях.

2.6 В Приложении 17 содержится требование выявлять критические системы в области информационных и связанных технологий и применять основанные на оценке риска меры по их защите. Для этого необходима интеграция кибербезопасности в национальные программы обеспечения авиационной безопасности, межотраслевое взаимодействие и постоянный мониторинг реализуемых мер.

3. ВЫВОД

3.1 Авиационная безопасность представляет собой сложную динамическую систему, где человеческий фактор является основой, поддерживающей эффективность всех действующих мер и процедур. Способность государств и организаций прогнозировать, предотвращать и эффективно реагировать на уже распространенные и новые риски и угрозы, в том числе киберугрозы, в значительной степени определяется надлежащим управлением этим фактором.

3.2 Кибербезопасность является новым вызовом в сфере управления человеческим фактором. Благодаря цифровой среде расширился спектр угроз в сфере авиационной безопасности. Персонал должен быть подготовлен к работе не только с физическими, но и с цифровыми рисками. Это требует прочной культуры кибербезопасности, специальной подготовки и четких протоколов реагирования на цифровые инциденты. Включение кибербезопасности в сферу управления аспектами человеческого фактора сейчас является обязательным условием обеспечения всесторонней защиты гражданской авиации.

— КОНЕЦ —