

**РАБОЧИЙ ДОКУМЕНТ****АССАМБЛЕЯ — 41-Я СЕССИЯ****ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ****Пункт 14 повестки дня. Авиационная безопасность. Политика****СЛОЖНЫЙ ХАРАКТЕР ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ В ГРАЖДАНСКОЙ
АВИАЦИИ**

(Представлено Объединенными Арабскими Эмиратами)

КРАТКАЯ СПРАВКА

Авиационная отрасль все сильнее полагается на цифровые средства, и кибербезопасность стала одним из важнейших компонентов устойчивости системы гражданской авиации. В данном документе описывается сложная и комплексная сфера кибербезопасности, которая затрагивает все аспекты гражданской авиации, включая безопасность полетов, авиационную безопасность, а также аэронавигационный потенциал и эффективность. Она распространяется также на коммерческие и экономические интересы государств и заинтересованных сторон в том, что касается обеспечения бесперебойной работы воздушного транспорта. В данном документе представлены результаты обсуждения на Форуме по кибербезопасности, организованного в рамках "Всемирного правительственного саммита 2022" и Международной программы высокого уровня для руководителей гражданской авиации 28–30 марта 2022 года на выставке Expo 2020 в Дубае, Объединенные Арабские Эмираты.

Действия: Ассамблее предлагается:

а) признать необходимость того, чтобы ИКАО, государства-члены и все соответствующие заинтересованные стороны продолжали совместно решать сложные вопросы, связанные с обеспечением кибербезопасности в гражданской авиации;

б) призвать заинтересованные авиационные стороны в области кибербезопасности к дальнейшей разработке стратегий наращивания потенциала в целях повышения компетентности и квалификации людских ресурсов для обеспечения наличия достаточного количества специалистов как в области кибербезопасности, так и в области гражданской авиации.

| | |
|-------------------------------|--|
| <i>Стратегические цели</i> | Настоящий рабочий документ связан со стратегическими целями: "Аэронавигационный потенциал и эффективность", "Безопасность полетов", а также "Авиационная безопасность и упрощение формальностей" |
| <i>Финансовые последствия</i> | Данный рабочий документ не имеет прямых финансовых последствий |
| <i>Справочный материал</i> | Приложение 17, <i>Безопасность</i> Дос 10118, <i>Глобальный план обеспечения авиационной безопасности</i> <i>Стратегия в области авиационной кибербезопасности</i> <i>План действий по обеспечению кибербезопасности</i> Инструктивный материал по политике в области кибербезопасности Культура кибербезопасности в гражданской авиации Руководство по протоколу "Светофор" A40-10, <i>Решение проблем кибербезопасности в гражданской авиации</i> |

1. ВВЕДЕНИЕ

1.1 Авиационная кибербезопасность носит глобальный и комплексный характер, затрагивая все аспекты гражданской авиации, включая безопасность полетов, авиационную безопасность, а также аэронавигационный потенциал и эффективность. Она также распространяется на коммерческие и экономические интересы государств и заинтересованных сторон в гражданской авиации в том, что касается обеспечения бесперебойности функционирования воздушного транспорта. Обеспокоенность по поводу кибербезопасности в гражданской авиации возрастает по мере увеличения количества и повышения серьезности атак, причем не обязательно в секторе гражданской авиации, но и в различных секторах по всему миру, а также по причине повышения зависимости авиационной отрасли от цифровых средств. Поэтому кибербезопасность стала одним из важнейших компонентов устойчивой системы гражданской авиации.

1.2 В целях оказания поддержки государствам и заинтересованным сторонам в решении вопросов авиационной кибербезопасности ИКАО разработала Стратегию в области авиационной кибербезопасности; План действий по обеспечению кибербезопасности; Инструктивный материал по политике в области кибербезопасности; Культуру кибербезопасности в гражданской авиации; Руководство ИКАО по протоколу "Светофор". Впрочем, сложный характер кибербезопасности порождает множество проблем на национальном, региональном и глобальном уровнях, которые необходимо решать в целях внедрения комплексного, согласованного и последовательного подхода к обеспечению авиационной кибербезопасности в секторе гражданской авиации.

2. ОБСУЖДЕНИЕ

2.1 В целях улучшения понимания актуальных проблем, связанных с обеспечением кибербезопасности в гражданской авиации, Главное управление гражданской авиации Объединенных Арабских Эмиратов организовало Форум по вопросам кибербезопасности, который прошел 28–30 марта 2022 года на полях "Всемирного правительственного саммита 2022" в рамках Международной программы высокого уровня для руководителей гражданской авиации на выставке Ехро 2020 в Дубае, Объединенные Арабские Эмираты. Следует отметить, что данный Форум по вопросам кибербезопасности был проведен до первого заседания Группы экспертов ИКАО по кибербезопасности, которое состоялось в мае 2022 года.

2.2 В рамках этого мероприятия по кибербезопасности был организован круглый стол по теме "Согласованный на глобальном уровне подход к обеспечению авиационной кибербезопасности" и Форум высокого уровня по кибербезопасности гражданской авиации: "Важность кибербезопасности в гражданской авиации". В круглом столе и форуме высокого уровня принимали участие высокопоставленные должностные лица и эксперты по вопросам кибербезопасности, представляющие многочисленные государства (включая министров, директоров ВГА и/или соответствующих секторов, руководителей отделов кибербезопасности и т. д.), ИКАО, региональные организации гражданской авиации (включая Африканскую комиссию гражданской авиации (АКГА), Арабскую организацию гражданской авиации (АрКГА), Европейскую конференцию гражданской авиации (ЕКГА) и т. д.), международные организации (включая Международный совет аэропортов (МСА) и т. д.), отрасль и другие важные заинтересованные стороны.

2.3 В ходе этих мероприятий на стратегическом уровне рассматривались и обсуждались различные проблемы, такие как: сложный характер проблемы кибербезопасности в гражданской авиации; цифровизация и быстро меняющаяся среда, обусловленная техническим развитием; связанные с традиционным подходом ограничения и необходимость изменения привычных

принципов при решении вопросов кибербезопасности в гражданской авиации; ограничения на международном и национальном уровнях, связанные с правовыми положениями для предотвращения киберинцидентов, уголовного преследования и своевременного реагирования на них; действия, которые необходимо предпринять правительствам на национальном уровне, поскольку обеспечение кибербезопасности необходимо для всех секторов, включая гражданскую авиацию; надлежащее распределение ролей и обязанностей между различными государственными структурами по решению комплексной задачи по обеспечению кибербезопасности, включая аспект гражданской авиации и соответствующую координацию деятельности; управление кибербезопасностью в гражданской авиации; разработка национальной стратегии кибербезопасности в гражданской авиации в качестве одной из составляющих национальной стратегии кибербезопасности; эволюция угроз авиационной кибербезопасности и снижение степени риска; меры реагирования на инциденты в области кибербезопасности на национальном, региональном и международном уровнях; важность развития культуры кибербезопасности; обмен информацией об угрозах кибербезопасности между государствами и заинтересованными сторонами (включая авиастроительные компании); важность партнерства, наращивания потенциала, обучения и развития людских ресурсов; определение обязательств и возможностей по контролю за обеспечением авиационной кибербезопасности и их реализация; и т. д.

2.4 Участники поделились своими достижениями, опытом, подходами, мнениями, опасениями и предложениями относительно дальнейших действий. Подчеркивалось, что применение комплексного, согласованного и последовательного подхода к обеспечению кибербезопасности в гражданской авиации по-прежнему является сложной задачей для многих заинтересованных сторон гражданской авиации, включая государственные структуры, органы власти, отрасль и заинтересованные стороны. Для развития сотрудничества и партнерских отношений, комплексного решения сложных межотраслевых проблем кибербезопасности и дальнейшего развития потенциала и квалификации людских ресурсов в секторе гражданской авиации необходимо провести дополнительную работу и добиться координации действий для последовательного и согласованного обеспечения защиты от киберугроз для гражданской авиации, смягчения их последствий и реагирования на них, а также для обеспечения киберустойчивости системы гражданской авиации.

3. ВЫВОД

3.1 Важно, чтобы все заинтересованные стороны продолжали совместно решать связанные с кибербезопасностью проблемы в гражданской авиации. Вопросы авиационной кибербезопасности должны рассматриваться на межотраслевой основе и решаться при помощи скоординированных действий. Комплексный характер проблемы авиационной кибербезопасности требует широкого сотрудничества между: ИКАО, государствами, организациями, отраслью и заинтересованными сторонами во всех соответствующих авиационных областях в целях защиты гражданской авиации от киберугроз. Государствам следует оказывать дальнейшую поддержку в продолжении разработки национальных стратегий авиационной кибербезопасности на основе Стратегии ИКАО в области авиационной кибербезопасности и с учетом ситуации с кибербезопасностью в их стране. Этого невозможно достичь без разработки стратегий наращивания потенциала и повышения компетенции и квалификации людских ресурсов как в области кибербезопасности, так и в области гражданской авиации.