Международная организация гражданской авиации

A41-WP/374
EX/170
2/8/22

РАБОЧИЙ ДОКУМЕНТ

АССАМБЛЕЯ — 41-Я СЕССИЯ

ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ

Пункт 14 повестки дня. Авиационная безопасность. Политика

ГОТОВНОСТЬ ПЕРСОНАЛА К ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ АЭРОНАВИГАЦИОННЫХ СЛУЖБ В ОБЫЧНОЕ И КРИЗИСНОЕ ВРЕМЯ

(Представлено Африканской комиссией гражданской авиации (АКГА) от имени 54 государств-членов[1])

КРАТКАЯ СПРАВКА

Со временем важность кибербезопасности и киберустойчивости в авиации резко возросла, и неотложный характер вопроса обеспечения кибербезопасности подчеркивался снова и снова в связи с новыми атаками до и во время пандемии COVID-19. Кроме того, помимо катастрофического воздействия COVID-19 на мировую экономику в целом и на авиацию в частности, во время пандемии было зафиксировано большее число кибератак. Наращивание потенциала, обучение и развитие культуры кибербезопасности представляют собой одни из основных принципов стратегии кибербезопасности ИКАО, и необходимо принимать во внимание важность аэронавигационной инфраструктуры для авиационного сектора. В связи с этим в данном рабочем документе подчеркивается важность решения вопросов наращивания потенциала, обучения и развития культуры кибербезопасности в обычное и кризисное время.

Действия: Ассамблее предлагается:

a) принять к сведению информацию, приведенную в данном рабочем документе;

b) поручить ИКАО включить в список задач Группы экспертов по кибербезопасности разработку инициатив по наращиванию потенциала, обучению и формированию культуры кибербезопасности в кризисные периоды.

Стратегические цели	Данный рабочий документ связан со стратегической целью *"Авиационная безопасность и упрощение формальностей"*
Финансовые последствия	
Справочный материал	*Стратегия авиационной кибербезопасности* *План действий по обеспечению кибербезопасности* Резолюция Ассамблеи 40-10. Решение проблем кибербезопасности в гражданской авиации Doc 9985, *Руководство по безопасности системы организации воздушного движения*

[1] Алжир, Ангола, Бенин, Ботсвана, Буркина-Фасо, Бурунди, Габон, Гамбия, Гана, Гвинея, Гвинея-Бисау, Демократическая Республика Конго, Джибути, Египет, Замбия, Зимбабве, Кабо-Верде, Камерун, Кения, Коморские Острова, Кот-д'Ивуар, Лесото, Либерия, Ливия, Маврикий, Мавритания, Мадагаскар, Малави, Мали, Марокко, Мозамбик, Намибия, Нигер, Нигерия, Республика Конго, Руанда, Сан-Томе и Принсипи, Сейшельские Острова, Сенегал, Сомали, Судан, Сьерра-Леоне, Танзания, Того, Тунис, Уганда, Центральноафриканская Республика, Чад, Экваториальная Гвинея, Эритрея, Эсватини, Эфиопия, Южная Африка и Южный Судан.

1. ВВЕДЕНИЕ

1.1 Технологии и киберсистемы стали неотъемлемой частью современного общества и используются во многих видах деятельности, которые стали зависеть от информационных технологий. В связи с этим со временем важность кибербезопасности и киберустойчивости в авиации резко возросла, и неотложный характер вопроса обеспечения кибербезопасности подчеркивался снова и снова в связи с новыми атаками, происходившими до и во время пандемии COVID-19.

1.2 Признавая многогранность и комплексный характер вопросов кибербезопасности и отмечая способность кибератак одновременно воздействовать на широкий круг областей и быстро распространяться, необходимо выработать общую концепцию и определить глобальную стратегию обеспечения кибербезопасности. В связи с этим ИКАО разработала и опубликовала Стратегию авиационной кибербезопасности, чтобы создать устойчивую и надежную систему обеспечения кибербезопасности.

1.3 Стратегия кибербезопасности ИКАО включает семь основных направлений: международное сотрудничество, механизмы управления, действенное законодательство и нормы, политика кибербезопасности, обмен информацией, управление инцидентами и планирование на случай экстренных ситуаций, а также **наращивание потенциала, обучение и культура кибербезопасности**.

1.4 На 40-й сессии Ассамблеи ИКАО была принята резолюция Ассамблеи A40-10 *"Решение проблемы кибербезопасности в гражданской авиации"*. В резолюции кибербезопасность рассматривается через призму горизонтального, сквозного и функционального подхода, подтверждается важность и срочная необходимость защиты систем и данных критической инфраструктуры гражданской авиации от киберугроз и содержится призыв к государствам реализовать Стратегию кибербезопасности ИКАО.

1.5 План действий ИКАО по кибербезопасности (ПДоК) был разработан с целью предложить ряд принципов, мер и действий для достижения целей по семи основным направлениям стратегии. Он закладывает основу для совместной работы государств, отрасли, заинтересованных сторон и ИКАО по развитию способности выявлять, предотвращать, обнаруживать кибератаки на объекты гражданской авиации, реагировать на них и восстанавливаться после них, а также служит прочной основой для сотрудничества.

1.6 Недавно была создана Группа по кибербезопасности как часть нового механизма управления для решения вопросов кибербезопасности в ИКАО. Круг ведения Группы по кибербезопасности включает деятельность, ведущуюся в соответствии с Программой работы в области авиационной кибербезопасности в целях разработки положений, которые могут включать Стандарты и Рекомендуемую практику (SARPS) и/или процедуры защиты гражданской авиации от киберугроз с должным учетом экономических, эксплуатационных и других последствий таких положений.

1.7 ИКАО разработала инструктивный материал по культуре кибербезопасности ("Культура кибербезопасности в гражданской авиации").

2. ХОД ОБСУЖДЕНИЯ

2.1 Пандемия коронавирусного заболевания (COVID-19), начавшаяся в 2019 году, безвозвратно изменила наш образ жизни. Государствами было принято множество мер по ограничению физического контакта между людьми и, таким образом, по борьбе с распространением COVID-19, среди которых социальное дистанцирование, дистанционное обучение и удаленная работа. Это привело к резкому росту объемов удаленной работы и числа видеоконференций, ускорению цифровизации, внедрению инноваций и других онлайн-технологий, в результате чего сформировалась "новая реальность". Помимо катастрофических последствий COVID-19 для международной экономики и общества, во время пандемии было зафиксировано более высокое число кибератак, что также повлияло на общество и бизнес.

2.2 Сектор аэронавигации считается одной из критически важных частей авиационной инфраструктуры, в связи с чем ему необходимо уделять особое внимание в свете перехода средств аэронавигации от аналоговых наземных систем к цифровым космическим системам для обеспечения стремительного роста плотности воздушного движения.

2.3 Наращивание потенциала, обучение и культура кибербезопасности являются одними из основных столпов стратегии кибербезопасности, которая позволяет обеспечить киберустойчивость авиационной системы. Вместе с тем существующими механизмами ИКАО не охвачены вопросы кибербезопасности во время кризисов, таких как пандемия COVID-19 или другие будущие пандемии или кризисы.

3. ВЫВОД

3.1 Наращивание потенциала, обучение и культура кибербезопасности считаются одними из основных направлений обеспечения киберустойчивости авиационных систем в обычное и кризисное время. Поэтому в резолюции ИКАО по кибербезопасности следует учесть этот важный вопрос. Кроме того, недавно созданная Группа экспертов по кибербезопасности должна заниматься этим вопросом в числе своих задач.

— КОНЕЦ —