

**РАБОЧИЙ ДОКУМЕНТ****АССАМБЛЕЯ – 42-Я СЕССИЯ****ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ**

Пункт 18 повестки дня. Нарращивание потенциала и поддержка внедрения. Политика и деятельность

**ПРЕДЛОЖЕНИЕ О РАЗРАБОТКЕ ПРОГРАММЫ ОБУЧЕНИЯ В ОБЛАСТИ
КИБЕРБЕЗОПАСНОСТИ В СООТВЕТСТВИИ С НОВЫМИ РУКОВОДЯЩИМИ
ПРИНЦИПАМИ**

(Представлено Республикой Корея)

КРАТКАЯ СПРАВКА

Анализ статистических данных о недавних киберинцидентах в авиации показывает, что киберугрозы превратились в **реальную опасность**. В этой связи Группа экспертов по кибербезопасности разрабатывает и публикует соответствующие инструктивные материалы на основе **пункта 4.9 Приложения 17 "Авиационная безопасность" ИКАО**. Однако в настоящее время существует только один официальный учебный курс ИКАО по кибербезопасности. Для наращивания потенциала в целях противодействия этим реальным угрозам требуются образование и учебная подготовка. Поэтому необходимо побуждать государства-члены к разработке учебных программ на основе руководящих принципов в области кибербезопасности, а ИКАО необходимо **стандартизировать** эти усилия.

Действия: Ассамблее предлагается:

- признать эволюционный характер киберугроз в сфере гражданской авиации;
- рассмотреть руководящие принципы в области кибербезопасности, разработанные на основе требований, содержащихся в п. 4.9 Приложения 17 "Авиационная безопасность";
- инициировать разработку новых учебных программ ИКАО под руководством ИКАО на основе этих руководящих принципов в области кибербезопасности.

<i>Стратегические цели</i>	Данный рабочий документ связан со стратегической целью "Каждый полет безопасен и защищен"
<i>Финансовые последствия</i>	Деятельность ИКАО, упомянутая в настоящем документе, как ожидается, будет осуществляться в рамках ресурсов, имеющихся в бюджете Регулярной программы на 2026–2028 гг., и/или за счет внебюджетных взносов в соответствии с бизнес-планом ИКАО на 2026–2028 гг.
<i>Справочный материал</i>	Дос 10184 "Действующие резолюции Ассамблеи" (по состоянию на 7 октября 2022 года) A42-WP/12 "Кибербезопасность в гражданской авиации" A42-WP/13 "Итоги этапа заседаний высокого уровня с участием министров в рамках Недели ИКАО по авиационной безопасности 2024 года, проведенного в Маскате, Оман"

1. ВВЕДЕНИЕ

1.1 В последнее время цели кибератак меняются. В прошлом злоумышленники занимались кражей личной информации, такой как имена пассажиров, номера телефонов и данные кредитных карт. В настоящее время они все чаще ставят перед собой цель создать прямые и ощутимые сбои в работе гражданской авиации, например, парализовать услуги воздушного транспорта или вывести из строя системы аэронавигации.

1.2 Согласно данным, опубликованным EATM-CERT за год, предшествующий первой половине 2025 года, наиболее распространенным типом кибератак было использование программ-вымогателей, на которые пришлось 15 из 33 инцидентов (около 45 %); далее следовали взлом (7 случаев) и DDoS-атаки (5 случаев). Основными целями были авиакомпании (16 инцидентов, т. е. примерно 48 %), за которыми следовали аэропорты (7 инцидентов), цепочки поставок (7 инцидентов) и ведомства гражданской авиации (ВГА) (3 инцидента).

1.3 Ожидается, что число таких случаев будет расти, и, учитывая значительное количество инцидентов, о которых не сообщается, киберугрозы должны быть признаны реальной и насущной опасностью для авиационного сектора.

2. ОБСУЖДЕНИЕ

2.1 В пункте 4.9 Приложения 17 "Авиационная безопасность" ИКАО содержится требование определять критически важные системы информационно-коммуникационных технологий и данные, используемые для целей гражданской авиации, и в соответствии с оценкой риска разрабатывать и внедрять, в случае необходимости, меры их защиты от актов незаконного вмешательства.

2.2 В прошлом году Республика Корея реализовала соответствующие требуемые стандарты по линии МНМ-УППАБ (механизм непрерывного мониторинга в рамках Универсальной программы проверок в сфере обеспечения авиационной безопасности) с помощью своих национальных правил в области кибербезопасности, и ожидается, что многие государства-члены также смогут в достаточной степени выполнить эти стандарты.

2.3 Кроме того, за последние четыре года Группа экспертов по кибербезопасности разработала и частично опубликовала ряд инструктивных материалов для укрепления потенциала в области авиационной кибербезопасности; в них содержатся руководящие указания для государств-членов по упрощению их применения в отрасли гражданской авиации.

2.4 В этой связи представляется, что сейчас настал подходящий момент для разработки учебных курсов ИКАО по этим руководящим принципам; кроме того, необходимо разработать образовательные и учебные программы по руководящим принципам в области кибербезопасности, которые находятся на этапе разработки или уже опубликованы. (В настоящее время среди учебных курсов ИКАО имеется одна программа по кибербезопасности.)

3. ЗАКЛЮЧЕНИЕ

3.1 Анализ статистических данных за последние пять лет и недавних данных показывает, что мы должны признать, что сейчас настало время в инициативном порядке сделать упор на укрепление устойчивости авиационной кибербезопасности, поскольку киберугрозы для гражданской авиации стали реальностью.

3.2 Под руководством Группы экспертов по кибербезопасности разрабатываются и публикуются руководящие принципы по кибербезопасности, учитывающие рекомендации в п. 4.9 Приложения 17 "Авиационная безопасность". Всем государствам-членам необходимо ознакомиться с этими руководящими принципами и подготовить меры по их адаптации в конкретных организациях.

3.3 Для достижения этой цели наиболее важной является разработка образовательных и учебных программ в области кибербезопасности. Хотя Группа экспертов по кибербезопасности разрабатывает руководящие принципы в сфере учебной подготовки, существует только один официальный учебный курс ИКАО. ИКАО следует побуждать многие государства-члены к разработке учебных курсов в области кибербезопасности, а затем работать над их стандартизацией.

— КОНЕЦ —