Международная организация гражданской авиации

A40-WP/243[1]
EX/95
5/8/19

РАБОЧИЙ ДОКУМЕНТ

АССАМБЛЕЯ — 40-Я СЕССИЯ

ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ

Пункт 12 повестки дня. Авиационная безопасность. Политика

КИБЕРБЕЗОПАСНОСТЬ

(Представлено Международным советом аэропортов (МСА))

КРАТКАЯ СПРАВКА

Угрозы кибербезопасности стали реальными факторами рисками для авиационного сектора и в обозримом будущем ожидается рост количества и последствий этих факторов риска. Таким образом, заинтересованным сторонам в сфере авиации необходимо разработать программу киберустойчивости и поддерживать надежные и эффективные средства защиты от киберугроз. Все предприятия, включая аэропорты, подвержены киберугрозам, как предприятия с простым комплектом систем, так и имеющие наиболее развитые цифровые технологии в сфере ИТ.

Существует острая необходимость в международном сотрудничестве для решения проблем в сфере кибербезопасности, объединенного управления и последовательной и практичной политики, в сочетании с практическими решениями для обмена информацией, надзора, наращивания потенциала и подготовки. Применяемый в настоящее время обособленный подход не может эффективно решить данную проблему. Необходимы четкое концептуальное видение и стратегия ИКАО, а также совместная работа по всем дисциплинам, которая будет учитывать вопросы безопасности полетов, авиационной безопасности, эксплуатации и устойчивости.

Действия: Ассамблее предлагается:

a) поддержать стратегию ИКАО в области авиационной кибербезопасности и требовать, чтобы ИКАО работала с государствами и отраслью над разработкой плана действий в поддержку данной стратегии;

b) признать насущную необходимость междисциплинарного подхода к кибербезопасности;

c) просить ИКАО оперативно завершить оценку существующей структуры управления вопросами кибербезопасности, уделив особое внимание Группе экспертов, отвечающей за кибербезопасность и рассматривающей одновременно вопросы безопасности полетов, авиационной безопасности, устойчивости и непрерывности перевозок. Данная Группа должна включать в себя обладающих надлежащими навыками экспертов от государств и отрасли, чтобы проделать работу, указанную в Стратегии ИКАО в области кибербезопасности, и находиться в совместном ведении Аэронавигационной комиссии и Комитета по незаконному вмешательству или Авиатранспортного комитета;

d) просить Совет привлекать отрасль и государства к процессу определения политики, стратегии, планов и стандартов в области авиационной кибербезопасности.

[1] Документы на русском, английском, арабском, испанском, китайском и французском языках представлены МСА.

Стратегические цели	Данный рабочий документ связан со следующими стратегическими целями: *"Безопасность полетов", "Потенциал и эффективность", "Авиационная безопасность и упрощение формальностей"*
Финансовые последствия	Деятельность, упоминаемая в данном документе, будет осуществляться при наличии ресурсов в бюджете Регулярной программы на 2020–2022 гг. и/или за счет внебюджетных взносов
Справочный материал	A40-WP/28 EX/13, *Стратегия ИКАО в области кибербезопасности* Приложение 17, *Безопасность* Doc 8973, *Руководства по авиационной безопасности*

1. ВВЕДЕНИЕ

1.1 Авиационные системы становятся все более взаимосвязанными. Системы аэропортов, эксплуатантов воздушных судов, ПАНО, организаций наземного обслуживания и пассажирские системы зависят друг от друга в обмене цифровой информацией.

1.2 Угрозы кибербезопасности превратились в реальные факторы риска для авиационного сектора, и в обозримом будущем ожидается рост количества и последствий этих факторов риска. Поэтому для заинтересованных сторон в авиации жизненно важно создать надежные и эффективные средства киберзащиты и поддерживать программу киберустойчивости. Все предприятия, включая аэропорты, подвержены киберугрозам, как предприятия с простым комплектом систем, так и имеющие наиболее развитые цифровые технологии в сфере ИТ.

1.3 Необходимо подчеркнуть, что наиболее важным обстоятельством является то, что кибербезопасность – это проблема не "только" информационных и связных технологий (ICT). Кибербезопасность – это ответственность всей организации, а эффективная киберустойчивость зависит от всеобщей поддержки, надежного контроля качества и надзора, четких рамок политики и эффективного сотрудничества между заинтересованными сторонами. Крайне важно, чтобы в авиационном секторе развивалась сильная культура информационной безопасности.

1.4 Угрозы и инциденты, связанные с кибербезопасностью, могут влиять на всю систему воздушного транспорта, приводить к проблемам в сфере безопасности полетов и авиационной безопасности, сбоям в эксплуатации и финансовым потерям, а их последствия могут быстро пересекать границы и иметь глобальный характер.

1.5 Понимание того, что представляет собой киберугроза, будет иметь решающее значение для понимания и управления этим риском. Необходимо сотрудничество всех в авиационной отрасли, чтобы способствовать диалогу, в рамках которого ценятся разные точки зрения и согласовывается общий набор действий.

1.6 Авиационная отрасль имеет многолетний опыт решения проблем, связанных с безопасностью полетов и авиационной безопасностью, однако проблема кибербезопасности является сравнительно новой. Авиационная отрасль и аэропорты приобретают опыт устранения рисков кибербезопасности. Таким образом, отрасль должна на равных правах с государствами принимать участие в принятии решений, а также в разработке политики и стандартов в соответствующих органах ИКАО. На разработку и замену авиационных систем может уйти больше времени, чем потратят злоумышленники на развитие своих возможностей, поэтому необходим подход, позволяющий отрасли продолжать внедрение передовой практики в

соответствии с существующими международными стандартами, например, ИСО, одновременно содействуя более широкому внедрению во всем мире.

1.7 Необходим всеобъемлющий подход, учитывающий аспекты авиационной безопасности, безопасности полетов, устойчивости системы воздушного транспорта, защитных мер, механизмов реагирования, обмена информацией, наращивания потенциала и надзора.

2. РАССМОТРЕНИЕ ВОПРОСА

2.1 Последние несколько лет ИКАО рассматривала вопросы кибербезопасности и устойчивости к кибератакам на различных форумах.

2.2 Группа экспертов AVSEC в настоящее время рассматривает кибербезопасность с точки зрения авиационной безопасности, сосредоточив свое внимание главным образом на кибербезопасности в контексте замысла террористов нанести вред авиации. Три рабочие группы в составе данной Группы экспертов более подробно рассмотрели эту тему.

2.3 Рабочая группа по угрозам и рискам провела (в 2015 году) анализ риска преднамеренной кибератаки, способной повлиять на системы авиакомпании, аэропорта и аэронавигационного обслуживания. В частности, для аэропортов был сделан акцент на преднамеренном вмешательстве в системы безопасности, например, системы контроля доступа и досмотровое оборудование.

2.4 Рабочая группа AVSEC по инструктивному материалу (WGGM) подготовила главу по кибербезопасности для *Руководства по авиационной безопасности* ИКАО (Doc 8973). В этой главе для государств представлены общие сведения и инструктивный материал по разработке оценки рисков и политики, предлагаемым рамкам политики, структуре управления, подготовке, практике проектирования, закупочной деятельности, обнаружению, реагированию на инциденты, восстановлению и отчетности.

2.5 Рабочая группа по Приложению 17 в составе Группы экспертов AVSEC подробно обсудила SARPS. Кульминацией этой работы стало то, что Группа экспертов AVSEC, первоначально поддержавшая две Рекомендованные практики в поправке 15 к Приложению 17, решила заменить их на Стандарт и Рекомендуемую практику и включить в поправку 16 к Приложению 17 (ноябрь 2018 года).

2.6 Для изучения возможности создания надежной сети аэронавигационного обслуживания Секретариат ИКАО учредил в структуре Аэронавигационного управления группу "INNOVA", чтобы найти средство, обеспечивающее безопасный, устойчивый и "бесшовный" обмен информацией в цифровом пространстве в поддержку текущих и будущих операций. Для достижения этой цели в структуре Аэронавигационного управления была создана Исследовательская группа по рамкам доверия (TFSG) для разработки общего набора принципов, политики и руководящих указаний, а также стратегии перехода к согласованной на глобальном уровне структуре, которая будет обеспечивать надежный обмен данными и информацией в форматах "земля-земля", "воздух-земля" и "воздух-воздух" между соответствующими заинтересованными сторонами в авиации и обладать устойчивостью и функциональной совместимостью, которые необходимы для повышения пропускной способности и эффективности в целях обеспечения непрерывной и безопасной деятельности системы гражданской авиации.

2.7 ИКАО учредила Исследовательскую группу Секретариата по кибербезопасности (SSGC) под руководством заместителя директора по авиационной безопасности и упрощению формальностей (DD/ASF). Эта группа работает над рекомендациями для ИКАО по стратегии, юридической политике и общим потребностям государств и отрасли, связанным с кибербезопасностью, но у нее ограничены сфера охвата и состав.

2.8 Группа по дистанционно пилотируемым авиационным системам (ДПАС) разработала стандарты для обмена информацией между дистанционно пилотируемыми воздушными судами и удаленными пилотными станциями, чтобы сделать минимальной вероятность любого несанкционированного контроля и смягчить его последствия.

2.9 Юридический комитет рассматривает адекватность существующих документов международного воздушного права для противодействия киберугрозам гражданской авиации.

2.10 МСА признает ИКАО как наиболее подходящую организацию для принятия мер в области авиационной кибербезопасности. Однако описанное выше текущее разделение усилий в структуре ИКАО, связанных с кибербезопасностью, не позволяет применять эффективный и целостный подход.

2.11 Наоборот, они могут оказаться контрпродуктивными, поскольку этот стремительно меняющийся, нестабильный вопрос требует гибких и динамичных ответных мер. Разные государства имеют также разные подходы, и обязанности распределены по-разному между разными учреждениями. Это делает набор исключительно авиационных стандартов сложным и трудным с точки зрения внедрения.

2.12 Однако существует острая необходимость в международном сотрудничестве для решения проблем в сфере кибербезопасности, объединенного управления и последовательной и практичной политики. Помимо практических решений для обмена информацией, надзора, наращивания потенциала и подготовки, срочно требуется стратегия и план действий для гражданской авиации.

2.13 Этот план действий должен поощрять и поддерживать выработку общих руководящих принципов, стандартов, показателей, информированность и обмен знаниями по кибербезопасности для авиационной экосистемы. Кроме того, следует поддерживать инициативы по повышению осведомленности и взаимный обмен ноу-хау и практическим опытом среди заинтересованных сторон в авиации, чтобы использовать извлеченные уроки и существующую передовую практику.

3. ВЫВОДЫ

3.1 МСА полностью поддерживает рабочий документ Секретариата о стратегии ИКАО в области кибербезопасности и будет продолжать играть активную роль в ее дальнейшей разработке и реализации.

3.2 Крайне важно, чтобы ИКАО, государства и отрасль ускорили работу в этой области и при рассмотрении вопроса кибербезопасности работали совместно во всех дисциплинах. Это не тот вопрос, который можно естественным образом отнести к сфере безопасности полетов, авиационной безопасности, производству полетов, аэронавигации и упрощению формальностей, поскольку он затрагивает все сферы. Оценка рисков, инструктивный материал, разработка политики и надзор будут применяться ко всем этим сферам.

3.3 Группа экспертов по кибербезопасности, если она будет надлежащим образом укомплектована, потенциально могла бы решить некоторые из указанных выше вопросов, предлагая:

a) широкий диапазон экспертных знаний и опыта среди членов группы, особенно по теме кибербезопасности;

b) целостный подход к оценке рисков на основе методик, согласованных и обоюдно понимаемых всеми заинтересованными сторонами, опираясь на региональный и национальный опыт;

c) возможности учреждать рабочие группы, чтобы посвящать больше времени и ресурсов разработке инструктивных материалов, программ, наращиванию потенциала, помощи и подготовке, если необходимо;

d) совместное рассмотрение вопросов аэронавигации, безопасности полетов и авиационной безопасности.

— КОНЕЦ —