Международная организация гражданской авиации

A40-WP/427
EX/176
2/8/19

РАБОЧИЙ ДОКУМЕНТ

АССАМБЛЕЯ — 40-Я СЕССИЯ

ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ

Пункт 12 повестки дня. Авиационная безопасность. Политика

ПРЕДЛОЖЕНИЕ ИКАО ПО УПРАВЛЕНИЮ КИБЕРБЕЗОПАСНОСТЬЮ И ОТКАЗОУСТОЙЧИВОСТЬЮ

(Представлено Соединенными Штатами Америки)

КРАТКАЯ СПРАВКА

Кибербезопасность и отказоустойчивость авиационной экосистемы – это многодисциплинарная проблема, которая затрагивает или будет затрагивать почти все аспекты глобальной авиации. Ввиду сложности системы авиации и зависимости от обмена цифровой информации и процесса коммуникации потребность в обеспечении кибербезопасности и отказоустойчивости по мере развития технологий и непрерывной модернизации авиационной экосистемы становится все более насущной.

ИКАО, государства-члены и отрасль усердно работают над решением проблем кибербезопасности и отказоустойчивости, но нынешний подход в ИКАО характеризуется отсутствием надлежащего управления и вниманием отдельным секторам и различному опыту вместо того, чтобы отражать целостную глобальную авиационную экосистему.

Для решения этих вопросов Соединенные Штаты Америки рекомендуют ИКАО учредить при Совете технический комитет по вопросам кибербезопасности и отказоустойчивости для централизации управления и надлежащего решения проблем кибербезопасности и отказоустойчивости на основе комплексного подхода. Комитет будет управлять политикой и интеграцией отраслевых стандартов, а также заниматься оценкой потенциала разработки технических стандартов и рекомендуемой практики.

Действия: Ассамблее предлагается:

a) дать указание Совету ИКАО учредить при Совете новый технический комитет по вопросам кибербезопасности и отказоустойчивости, как предлагается в настоящем документе;

b) призвать государства поддержать предлагаемую стратегию ИКАО в области кибербезопасности, разработанную Исследовательской группой Секретариата по кибербезопасности;

c) призвать государства оказать поддержку работе Исследовательской группы по механизму доверия.

Стратегические цели	Настоящий рабочий документ связан со стратегическими целями "Авиационная безопасность и упрощение формальностей" и "Аэронавигационный потенциал и эффективность"
Финансовые последствия	Не имеется
Справочный материал	Doc 10075 *"Действующие резолюции Ассамблеи"*, A39-18 и A39-19 Рекомендация 5.4/1 13-й Аэронавигационной конференции ИКАО A40-WP/28 *"Стратегия ИКАО в области кибербезопасности"* Doc 7559/10 *"Правила процедуры Совета"*, раздел III, правило 17 a)

1. ВВЕДЕНИЕ

1.1 Кибербезопасность и отказоустойчивость авиационной экосистемы – это многодисциплинарная проблема, которая затрагивает или будет затрагивать почти все аспекты глобальной авиации. Как указано в резолюциях A39-18 и A39-19 39-й Сессии Ассамблеи ИКАО, глобальная авиационная система становится все более сложной и интегрированной с помощью информационно-коммуникационных технологий. Ввиду этих сложностей и зависимости от обмена цифровой информацией и процесса коммуникации потребность в обеспечении кибербезопасности и отказоустойчивости по мере развития технологий и непрерывной модернизации авиационной экосистемы становится все более насущной.

1.2 О важности вопросов кибербезопасности и отказоустойчивости свидетельствует также рекомендация 5.4/1, вынесенная по итогам 13-й Аэронавигационной конференции ИКАО, в которой, в частности, содержится призыв к государствам и ИКАО сотрудничать с отраслью в целях повышения осведомленности об угрозах и принятия совместных мер по уменьшению угроз. Вторая конференция высокого уровня ИКАО по авиационной безопасности также рекомендовала ИКАО разработать всеобъемлющую стратегию кибербезопасности и провести работу по технико-экономическому обоснованию для учреждения группы экспертов по кибербезопасности.

1.3 Несмотря на то, что ИКАО добивается определенного прогресса в разработке стратегии ИКАО в области кибербезопасности (см. документ A40-WP/28), управление кибербезопасностью и отказоустойчивостью в рамках Организации по-прежнему остается недостаточным. Отсутствие надлежащего управления снижает эффективность и приводит к отсутствию обмена информацией, что делает невозможным надлежащее решение проблем кибербезопасности и отказоустойчивости в рамках целостного подхода, характеризуемого централизованным управлением политикой, интеграцией отраслевых стандартов и потенциальной разработкой технических Стандартов и Рекомендуемой практики (SARPS).

2. ОБСУЖДЕНИЕ

2.1 Практикуемая в настоящее время руководящая деятельность ИКАО по вопросам, связанным с киберпространством, предусматривает разделение функций между Авиатранспортным управлением (ATB), которое контролирует кибербезопасность, и Аэронавигационным управлением (ANB), которое занимается вопросам киберустойчивости.

2.2 ATB отвечает за разработку SARPS и внесение поправок в Приложение 17 *"Безопасность"*. ATB также поддерживает работу Группы экспертов по авиационной безопасности и Комитета по незаконному вмешательству (UIC), включая создание Исследовательской группы Секретариата по кибербезопасности (SSGC). SSGC служит координационным центром для работы в области кибербезопасности, готовит обзоры, такие как обзор приложений ИКАО для консолидации SARPS, связанных с кибербезопасностью, и занимается общим содействием обмену информацией в рамках авиационного сообщества.

2.3 Подход ATB хорошо работает, когда кибербезопасность рассматривается как отдельная тема, подразумевающая защиту критических систем от незаконного вмешательства, как это определено в разделе 4.9 Приложения 17. Однако глобальная авиация представляет собой целостную экосистему, включающую множество взаимосвязанных систем, непосредственно влияющих на процесс эксплуатации, которые не входят в компетенцию ATB и UIC по решению проблем кибербезопасности.

2.4 ANB отвечает за разработку и внесение поправок в SARPS в 17 различных Приложениях, касающихся безопасности полетов и аэронавигационного потенциала и эффективности. ANB также поддерживает работу Аэронавигационной комиссии и ее технических групп, включая создание Рабочей группы INNOVA и Исследовательской группы по механизму доверия. Исследовательская группа по механизму доверия служит координационным центром для разработки киберустойчивых сетевых взаимосвязей через доверенную структуру, чтобы обеспечить глобальную передачу авиационных данных и информации, имеющих особо важное значение для осуществления полетов.

2.5 Подход ANB хорошо работает только в отношении оперативных данных и передачи информации. Однако он не учитывает безопасность систем, не подключенных к операционной сети, но способных оказывать влияние в других областях, значимых для безопасности или эффективности.

2.6 Несмотря на то, что ИКАО очевидно занимается вопросами как кибербезопасности, так и отказоустойчивости, нынешняя структура управления создает разделение между безопасностью и отказоустойчивостью, что негативно сказывается на целостности авиационной экосистемы. Государства-члены и отрасль признали существование такой проблемы и представили рекомендации по созданию новой "группы экспертов" по вопросам, связанным с киберпространством. Однако перед группой экспертов ИКАО ставится конкретная задача по ускорению решений специальных проблем или разработке SARPS (см. Doc 7984 *"Директивы группам экспертов Аэронавигационной комиссии"*). Кибербезопасность и отказоустойчивость являются более многодисциплинарными и всеобъемлющими областями, чем "специальная проблема", и в настоящее время ИКАО, вместо разработки новых SARPS ИКАО или нового Приложения, следует использовать отраслевые стандарты для кибербезопасности.

2.7 С учетом этого следует признать, что кибербезопасность и отказоустойчивость оказывают воздействие на всю авиационную экосистему, и поэтому к ним необходимо относиться как к проблемам более высокого уровня, а осуществлять централизованное управление ими должен Совет ИКАО через созданный для этой цели технический комитет.

2.8 В соответствии с правилом 17 a) раздела III документа Doc 7559/10 *"Правила процедуры Совета"*, Соединенные Штаты Америки предлагают сформировать технический комитет Совета по кибербезопасности и отказоустойчивости. В Doc 7559/10 говорится, что Совет может учреждать другие комиссии, комитеты или рабочие группы, как постоянные, так и временные. Новый комитет Совета может быть создан для решения проблем, связанных с техническими, экономическими, социальными и правовыми аспектами международной гражданской авиации, которые для их развития или решения требуют специальных знаний и опыта, которые не могут быть предоставлены Совету другими средствами.

2.9 Предлагаемый технический комитет будет работать под непосредственным контролем Совета, который также разработает круг полномочий и членский состав предлагаемого комитета на основе *"Директив для Комитета по кибербезопасности и отказоустойчивости"*. SSGC и Исследовательская группа по механизму доверия будут реорганизованы в рамках нового технического комитета с полным учетом задач, усилий и затрат, связанных с обеспечением надлежащего управления новым комитетом. Благодаря этому подходу предлагаемый комитет будет надлежащим образом использовать экспертов по данной тематике из различных областей, в том числе из рабочей структуры ИКАО, избегая при этом неэффективности и проблем в области коммуникации, возникающих в результате распределения сложных, взаимоувязанных вопросов между множеством управлений и ведомств с различными приоритетами.

3. ЗАКЛЮЧЕНИЕ

3.1 Кибербезопасность и отказоустойчивость в значительной степени влияют на всю глобальную авиационную экосистему. Предлагаемый подход, обсуждаемый в настоящем документе, позволит повысить статус работы над этой критически важной проблемой до уровня технического комитета Совета, который может работать на основе междисциплинарных мер и использовать опыт многочисленных управлений ИКАО и всего авиационного сообщества, сохраняя при этом темпы инноваций перед лицом постоянно растущих угроз.

3.2 Ассамблее предлагается одобрить действия, указанные в краткой справке.

— КОНЕЦ —