



РАБОЧИЙ ДОКУМЕНТ

АССАМБЛЕЯ — 42-Я СЕССИЯ

ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ

Пункт повестки дня № 13. Авиационная безопасность. Политика

ПОВЫШЕНИЕ НАДЕЖНОСТИ МЕХАНИЗМА УПРАВЛЕНИЯ И БОРЬБА С ЦИФРОВЫМИ И КИБЕРУГРОЗАМИ ГРАЖДАНСКОЙ АВИАЦИИ

(Подготовлено Международным координационным советом ассоциаций аэрокосмической промышленности (ИККАИА) и Международной федерацией ассоциаций линейных пилотов (ИФАЛПА))

КРАТКАЯ СПРАВКА

В гражданской авиации все шире внедряются взаимосвязанные цифровые технологии и системы, в том числе такие, которые напрямую управляют физическими и рабочими процессами или оказывают на них влияние. Несмотря на то, что эти технологии обеспечивают значительные преимущества, они также делают отрасль менее защищенной перед лицом преднамеренных, непреднамеренных и вызванных природными факторами цифровых угроз, а также уязвимостей, которые могут усиливать такие угрозы и поставить под угрозу критически важные операции.

Большая часть концепций ИКАО в сферах безопасности, защиты и операционной деятельности были изначально разработаны без учета системного и всеобъемлющего воздействия и распространения цифровых угроз, подвергающих риску внедряемые в отрасли цифровые технологии и взаимозависимости. Наиболее актуальная проблема касается умышленных и злонамеренных действий, совершаемых на стыке границ между безопасностью и защитой.

Данный документ призывает ИКАО, в качестве первого шага, создать концепцию внутреннего координированного управления и борьбы с цифровыми угрозами, чтобы сосредоточиться в сфере безопасности, защиты и операционной деятельности на преднамеренных и злонамеренных угрозах. В качестве дополнительной меры документ призывает ИКАО ускорить разработку руководств и глобальных стандартов, необходимых для формирования упорядоченной и эффективной защиты во всей экосистеме авиационных перевозок

Действия: Ассамблее предлагается:

а) подтвердить, что все категории цифровых угроз – будь то преднамеренные, непреднамеренные или вызванные природными факторами – представляют опасность для гражданской авиации, и с ними нужно бороться в рамках комплексного подхода к управлению, который следует сначала выработать в рамках ИКАО, чтобы организовать согласованную и эффективную поддержку странам и отрасли;

¹ Тексты документа на английском, арабском, испанском, китайском, русском и французском языках представлены ИККАИА и ИФАЛПА.

b) предложить Совету ИКАО начать разработку внутренней межотраслевой и междисциплинарной системы для борьбы с цифровыми угрозами в рамках ИКАО; c) призвать ИКАО ускорить разработку руководств и, где необходимо, Стандартов и Рекомендуемой практики (SARPS) по созданию системной, гармонизированной и адаптивной основы цифровой безопасности для всех стран и заинтересованных сторон; d) рекомендовать ИКАО усилить информирование и коммуникацию в области координации борьбы с цифровыми угрозами в рамках региональных сетей, поддерживать принятие гармонизированных мер и мероприятий по обеспечению безопасности в глобальном масштабе.	
<i>Стратегические цели</i>	Настоящий рабочий документ связан со стратегической целью: <i>"Каждый рейс безопасен и защищен"</i>
<i>Финансовые последствия</i>	Нет.
<i>Справочные документы</i>	A41-19 "Обеспечение кибербезопасности в гражданской авиации", Приложение 17 "Авиационная безопасность" Приложение 19 "Управление безопасностью полетов"

1. ВВЕДЕНИЕ

1.1 Цифровая трансформация позволила улучшить работу гражданской авиации. Однако рост зависимости от цифровых технологий открывает — и создает — новые уязвимости, вызванные ростом взаимосвязанности и сложностью систем.

1.2 Эта эволюция порождает организационные и управленческие проблемы, связанные с разделением по сферам деятельности ИКАО таких областей ответственности, как защита, безопасность, потенциал и эффективность, что демонстрирует растущую потребность в комплексном и координированном управлении.

1.3 Среди различных категорий цифровых угроз особенно важно бороться с преднамеренными и злонамеренными действиями (обычно именуемыми кибератаками) из-за их способности нарушить работу важнейших авиационных систем, а также недостаточно четкого распределения обязанностей в сфере защиты и безопасности.

1.4 Это изменение также подчеркивает отсутствие глобальной концепции для систематического внедрения "безопасности на этапе проектирования" и подхода, основанного на специализированном управлении и стандартах для всех сфер деятельности, учитывающего угрозы. В отсутствие согласованных подходов для поддержки на начальных этапах могут потребоваться промежуточные механизмы координации, особенно в контексте операций с высоким уровнем риска.

1.5 Цифровые угрозы, — определяемые как любые события потенциально или фактически вредоносного характера, исходящие от цифровых ресурсов или осуществляемые с их помощью, — начинают привлекать внимание экспертных и рабочих групп ИКАО. Однако многим из этих угроз, особенно если они не соответствуют стандартным определениям незаконного вмешательства или угроз безопасности людей или оборудования, пока что уделяется недостаточно внимания. Это особенно верно в отношении преднамеренных и злонамеренных угроз, действующих на стыке сфер деятельности ИКАО, что приводит к неопределенности в плане подотчетности, контроля и координации мероприятий по реагированию.

2. ОБСУЖДЕНИЕ

2.1 Цифровые угрозы для гражданской авиации охватывают широкий спектр событий. Такие угрозы могут носить преднамеренный (злонамеренный или нет), непреднамеренный (человеческая ошибка, ошибка в настройке оборудования) или природный характер (явления окружающей среды). Они могут иметь цифровое, физическое или комбинированное происхождение и оказывать влияние на цифровые элементы и физические системы, с которыми они взаимодействуют, тем самым ставя под угрозу безопасность полетов и бесперебойность работы авиации. Понимание этих широких категорий — это только первый шаг; также необходимо понимать, каким образом происходящая цифровая трансформация повышает их сложность.

2.2 Цифровая трансформация меняет экосистему авиации, внедряя не только новые технологии, но и новые виды отказов, уязвимостей и зависимостей. Многие из этих рисков не находят адекватного отражения в традиционных концепциях сфер деятельности ИКАО — начиная с тех, что связаны с защитой и безопасностью, но не только. Отсутствие глобальной структуры порождает несогласованность мер реагирования, дробление ответственности и отсутствие общего понимания — факторы, которые подрывают возможности защиты и противодействия.

2.3 Помимо роста уязвимости к злонамеренным действиям, цифровая трансформация порождает сложности структурного характера, которые создают проблемы для действующих систем управления и реагирования на события и факторы риска. Она создает непрозрачные взаимозависимости между информационными (ИТ) и операционными технологиями (ОТ), риски для цепочек поставок и порождает скорость изменений, для которой существующие сроки сертификации недостаточны. Традиционная авионика теперь зависит от связей с облачной инфраструктурой, искусственным интеллектом (AI) и протоколом интернета (IP), чьи компоненты сторонних производителей обновляются каждый месяц и создают уязвимости, не поддающиеся традиционным средствам управления. Нововведения появляются каждый месяц, в то время как стандарты меняются не чаще одного раза в год, из-за чего устаревают меры по снижению рисков и ширится разрыв на уровне стран. В отсутствие общей классификации и механизма обмена информацией об угрозах сообщество видит только отдельные части проблемы, и это тормозит разработку соответствующих мер защиты.

2.4 Отсутствие специализированного глобального механизма управления и SARPS, основанных на принципе "безопасности на этапе проектирования" и учете угроз, означает отсутствие согласованного системного подхода к борьбе с цифровыми угрозами во всех сферах деятельности. Такое отсутствие общих рабочих критериев для стран создает системную уязвимость и закладывает основу для угроз, созданных специально с учетом этой сложности.

2.5 В связи с этим особого внимания требуют преднамеренные и злонамеренные угрозы. Часто сложные, динамические и трудно выявляемые угрозы этих типов используют цифровые зависимости для того, чтобы спровоцировать ухудшение или прерывание работы систем. Обладая уникальными особенностями, они могут классифицироваться как традиционные авиационные категории, находиться на их стыке или за их пределами, что создает трудности с обнаружением, отчетностью и реагированием.

2.6 Опыт работы показывает, что некоторые виды злонамеренного цифрового вмешательства не укладываются в рамки существующих концепций по сферам деятельности. Ярким примером является преднамеренная подмена сигнала GNSS, при этом передаются поддельные сигналы позиционирования, которые вводят в заблуждение навигационные системы воздушного судна без необходимости физического доступа или очевидного вмешательства.

Несмотря на то, что такие действия являются преднамеренными и могут напрямую повлиять на осуществление полетов, они могут не подпадать под определение незаконного вмешательства в Приложении 17 и не требовать обязательного отчета о нарушении безопасности согласно Приложению 19.

2.7 Пробелы в нормативном регулировании не только ограничивают понимание обстановки и координацию мер реагирования, но, что более важно, демонстрируют насущную необходимость формирования концепции управления, которая учитывает эти новые формы цифрового вмешательства, устанавливает четкие пороги отчетности и однозначно определяет задачи различных институтов в сферах защиты и безопасности.

2.8 В текущих условиях отсутствия согласованной международной системы Страны и региональные органы власти начали внедрять разнообразные нормативные подходы к регулированию. Это растущее расхождение создает сложности для заинтересованных сторон в авиации, в том числе производителей комплектного оборудования, поставщиков товаров и услуг, которые должны разбираться в разнородных требованиях законодательства.

Для решения этой проблемы нужно действовать в двух направлениях:

- единая комплексная стратегия, которая может охватить весь спектр цифровых угроз — преднамеренные, непреднамеренные и вызванные природными факторам;
- расстановка приоритетов и целенаправленная борьба с преднамеренными и злонамеренными угрозами с учетом их приоритета, возможных последствий и несогласованности существующего законодательства.

3. ЗАКЛЮЧЕНИЕ

3.1 Усиление защиты от цифровых угроз жизненно важно для обеспечения защиты, безопасности, структуры и эффективности работы гражданской авиации. По мере роста цифровых зависимостей в различных системах и сферах деятельности растет потребность в согласованном управлении с учетом перспективы в будущем.

3.2 Для решения этой проблемы ИКАО и ее соответствующие заинтересованные стороны должны стремиться к осуществлению двух четких целей:

- реализовать комплексный подход ко всему спектру цифровых угроз — преднамеренных, непреднамеренных и вызванных природными факторам;
- уделить основное внимание борьбе с преднамеренными и злонамеренными угрозами, которые в настоящее время представляют наибольшую опасность в условиях неопределенности ролей и отсутствия согласованности между соответствующими сферами деятельности ИКАО.

3.3 Формируя согласованность в различных сферах деятельности, применяя промежуточные средства оценки и строя взаимопонимание, ИКАО может играть ведущую роль в выработке единого, адаптивного и единообразного ответа на эволюционирующие цифровые риски на глобальном уровне.

3.4 Этой деятельностью может руководить действующий Специальный координационный комитет по кибербезопасности (АНССС) путем закрепления за этой структурой конкретных полномочий в области управления (в настоящее время у него такой задачи нет).

— КОНЕЦ —