Международная организация гражданской авиации

A41-WP/64[1]
EX/33
22/7/22

РАБОЧИЙ ДОКУМЕНТ

АССАМБЛЕЯ — 41-Я СЕССИЯ

ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ

Пункт 14 повестки дня. **Авиационная безопасность. Политика**

ИНТЕГРАЦИЯ И КООРДИНАЦИЯ СТРАТЕГИЙ И РАБОЧИХ ПЛАНОВ ИКАО В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

(Представлено Международной ассоциацией воздушного транспорта (ИАТА))

КРАТКАЯ СПРАВКА

Кибербезопасность в гражданской авиации остается областью повышенного интереса со стороны ИКАО, государств и отрасли. Основное внимание по-прежнему уделяется не только выявлению и снижению уровня киберугроз и рисков, направленных на вмешательство в цифровые системы, но и созданию международной основы для обеспечения безопасных технологических инноваций, опирающейся на ключевые принципы, такие как обеспечение безопасности на этапе проектирования, для цепочки поставок аэрокосмической отрасли.

В настоящем документе представлена необходимость комплексного и скоординированного подхода к обеспечению кибербезопасности со стороны нового созданного Специального координационного комитета по кибербезопасности (AHCCC). Отметим, что предложения, исходящие от технических групп экспертов и подгрупп, которые могут повлиять на Стандарты и рекомендуемую практику (SARPS), а также другие требования, отражают всеобъемлющий характер этой дисциплины в рамках множества Приложений, документов и руководств ИКАО.

Действия: Ассамблее предлагается обратиться с просьбой, чтобы Совет:

a) обратиться к Совету с просьбой обеспечить совместную работу всех рабочих органов ИКАО по созданию междисциплинарного и многоэтапного согласованного подхода к интеграции положений о кибербезопасности и других требований, основанных на обеспечении безопасности на этапе проектирования;

b) обратиться к Совету с просьбой признать потенциальное воздействие внедрения нового поколения взаимосвязанных и инновационных технологий и связанных с ними цепочек поставок, которые не ограничены правилами в сфере гражданской авиации или SARPS.

Стратегические цели	Данный рабочий документ связан со стратегическими целями: *"Безопасность полетов", "Авиационная безопасность и упрощение формальностей"* и *"Аэронавигационный потенциал и эффективность"*
Финансовые последствия	Расходы на разработку, координацию и подготовку новых положений и инструктивных материалов, которые будут предоставлены отраслью ИКАО
Справочный материал	Doc 10140, *Действующие резолюции Ассамблеи (по состоянию на 4 октября 2019 года)* Doc 10108, *Заявление о глобальном контексте риска в области авиационной безопасности* Резолюция A40-10 по *Решению проблем кибербезопасности в гражданской авиации* *Стратегия в области авиационной кибербезопасности* *План действий по обеспечению кибербезопасности*

[1] Тексты на русском, английском, арабском, испанском, китайском и французском языках представлены ИАТА.

1. ВВЕДЕНИЕ

1.1 На 40-й сессии Генеральной Ассамблеи ИКАО (2019 год) была принята резолюция A40-10 "*Решение проблем кибербезопасности в гражданской авиации*". По сути, резолюция уполномочила Генерального секретаря продолжать обеспечивать комплексное рассмотрение и координацию вопросов кибербезопасности с помощью соответствующих механизмов в духе Стратегии ИКАО в области авиационной кибербезопасности (2019 год).

1.2 В Стратегии ИКАО в области авиационной кибербезопасности предложен ряд принципов, мер и мероприятий, а также прагматически определенные четкие действия по координации в рамках Плана действий ИКАО по обеспечению кибербезопасности (СуАР) (2019 год) для устранения киберугроз и создания элементов, необходимых для укрепления позиции международной гражданской авиации с точки зрения цифровой безопасности, авиационной безопасности и доверия.

1.3 В 2022 году Совет ИКАО принял решение о создании нового Специального координационного комитета по кибербезопасности (AHCCC) и двух отдельных групп экспертов в рамках двух разных комитетов. Это особенно подчеркивает пристальное внимание ИКАО и Совета к критическому состоянию стратегической авиационной кибербезопасности. Новая Группа экспертов по кибербезопасности (CYSECP), одобренная Комитетом по авиационной безопасности 24 января 2022 года в рамках 225-й сессии, провела своё первое заседание в мае 2022 года. Группа экспертов CYSECP отметила предыдущие достижения SSGC и предложила рабочий план, отвечающий потребности во внутренней и международной координации. Кроме того, для усиления перспектив координации между бюро, комитетами и техническими группами экспертов ИКАО Аэронавигационная комиссия (АНК) создала Группу экспертов по доверенным системам (TSP).

2. ОБСУЖДЕНИЕ

Координация в области кибербезопасности в ИКАО

2.1 Широко известно, что авиационная кибербезопасность по своей природе является трансверсальной и комплексной дисциплиной. Таким образом, роль AHCCC в будущем имеет решающее значение для обеспечения скоординированного стратегического движения, связывающего воедино рабочие планы и мероприятия разных рабочих органов ИКАО, в направлении обеспечения полной защиты авиации от всех форм цифровых помех при одновременной поддержке безопасных технологических инноваций.

2.2 По сути, SARPS и руководящие указания, имеющие в своей основе документы, часто связаны с обеспечением соблюдения государствами международных обязательств, изложенных в 19 Приложениях. Поэтому крайне важно, чтобы AHCCC обеспечивал координацию посредством структурированного и эффективного управления.

2.3 Ниже описывается ряд усилий, имеющих отношение к AHCCC:

a) деятельность Группы экспертов по доверенным системам основана на принципах, определенных для следующего поколения аэромобильности, и касается разработки концепции функционирования и управления такой структурой;

b) Группа экспертов по кибербезопасности проводит работу, в рамках которой рассматривается введение или предложения по изменению/модификации существующих Приложений, документов и руководств в части, касающейся обеспечения кибербезопасности;

c) Группа экспертов по управлению информацией в Правилах аэронавигационного обслуживания. Управление информацией (PANS-IM) формулирует определенные требования к информационной безопасности, а также предпринимает другие усилия, такие как работа над текущей редакцией документа 9896 изд. 3 об использовании пакета протоколов Интернет в сети аэронавигационной электросвязи, которая также связана с включением требований к кибербезопасности в данное руководство;

d) также предлагается внести изменения в Руководство по управлению безопасностью полетов (Doc 9859);

e) отмечена координация результатов Универсальной программы аудита авиационной безопасности (USAP) для SARPS, связанных с кибербезопасностью, согласно Приложению 17, как указано в документе A41-WP/22, представленном Советом ИКАО;

f) Отмечена работа Исследовательской подгруппы по правовым аспектам (RSGLA) и координация Секретариата с Юридическим комитетом, как указано в документе A41-WP/22, представленном Советом ИКАО.

2.4 Со временем интеграция требований и положений по кибербезопасности в различные Приложения и документы станет сложной задачей. В результате может возникнуть необходимость в оценке создания нового Приложения для упрощения интеграции и обеспечения того, чтобы SARPS разрабатывались трансверсально для создания мер, которые смягчают преднамеренные и/или непреднамеренные события и, более того, угрозы, способные привести к вторичному / кумулятивному воздействию на безопасность полетов или авиационную безопасность, которое не всегда немедленно определяется как форма цифровых помех.

Интеграция цифровой трансформации

2.5 Происходит непрерывная эволюция цифровой трансформации в разных областях, что приводит к появлению более взаимосвязанных технологий, таких как прогнозируемое техническое обслуживание воздушных судов, принятие решений на основе искусственного интеллекта и/или машинного обучения, передовые вычисления, открытая архитектура и беспроводные обновления критически важных телекоммуникационных систем.

2.6 Новейшие концепции аэромобильности приводят к появлению новых и эффективных технологий. Однако цепочки поставок в аэрокосмической отрасли не обязательно регулируются традиционными национальными регулирующими нормами и стандартами в сфере гражданской авиации. Новые цепочки поставок создают непрозрачные возможности для внедрения потенциальных уязвимостей в и без того сложную операционную среду, где область кибератак, когда-то ограниченная устаревшими системами, теперь распространяется на неизвестные взаимосвязанные технологии. В целом, возникающая взаимосвязь и растущая зависимость требуют четкой структуры регулирования аэрокосмической отрасли, которая обеспечит постоянную летную годность и сертификацию воздушных судов.

2.7 Принципы обеспечения безопасности на этапе проектирования являются частью подхода к политике в сфере кибербезопасности, который был отмечен в Стратегии ИКАО в области авиационной кибербезопасности. В этой связи рабочие планы, направленные на цифровую защиту отрасли и поддержку технологий следующего поколения, инновационных продуктов и услуг, должны быть независимыми и охватывать всю систему гражданской авиации. Это сводится не только к поддержке концепции Trust Framework или предложению поправок к Приложениям и документам, но включает также общий междисциплинарный рабочий план в рамках многоэтапного подхода.

3. ВЫВОДЫ

3.1 Международная политика и обязательства в области авиационной кибербезопасности, позволяющие эксплуатантам в условиях регулирования достигать эффективной отдачи от инвестиций внутри цепочек поставок, имеют решающее значение для устойчивости авиационного сектора. Кроме того, существует потребность в поддержке со стороны ИКАО и государств международных усилий, позволяющих отрасли внедрять инновации и повышать устойчивость гражданской авиации относительно новых цепочек поставок. Крайне необходимо продвигать подход, направленный на обеспечение безопасности на этапе проектирования, который по своему характеру является междисциплинарным и многоэтапным, и, таким образом, интегрировать положения и требования в универсальный рабочий план, в рамках компетенции АНССС, групп экспертов, рабочих и исследовательских групп ИКАО.

3.2 План работы, в основе которого – идея обеспечения безопасности на этапе проектирования, заложит основу для создания интегрированной, киберустойчивой, гибкой и инновационной экосистемы, с целью уменьшения частоты способных повлиять на безопасность полетов и на международную гражданскую авиацию в целом кибератак и снижения их воздействия на государства и отрасль.

— КОНЕЦ —