

**РАБОЧИЙ ДОКУМЕНТ****ТРИНАДЦАТАЯ АЭРОНАВИГАЦИОННАЯ КОНФЕРЕНЦИЯ****Монреаль, Канада, 9–19 октября 2018 года****КОМИТЕТ А****Пункт 5 повестки дня. Возникающие проблемы****5.4 Киберустойчивость****КИБЕРУСТОЙЧИВОСТЬ**

(Представлено Секретариатом)

КРАТКАЯ СПРАВКА

Важность надлежащего подхода к обеспечению киберустойчивости в гражданской авиации признана на глобальном уровне и является значимым вопросом для рассмотрения в *Глобальном аэронавигационном плане* (ГАНП, Doc 9750) издания 2019 года. Успешное управление киберустойчивостью во все более взаимосвязанной авиационной системе требует подхода, глобально согласованного между всеми заинтересованными сторонами. Без скоординированной в глобальном масштабе структуры доверия, обеспечивающей обмен информацией в направлениях "земля – земля", "воздух – земля" и "воздух – воздух", и приверженности построению культуры доверия, ведущей к обмену информацией об киберинцидентах, киберустойчивость не может быть гарантирована. Также признано, что, несмотря на возрастающий уровень зависимости от информационных технологий, участие людей одновременно является главной причиной возникновения киберугроз и первой линией защиты от них, и поэтому эксплуатационный персонал должен пройти подготовку по распознаванию общих аспектов киберугроз и сообщению информации о любой предполагаемой киберугрозе или киберинциденте.

Действия: Конференции предлагается согласиться с рекомендацией 5.4/х "Киберустойчивость", приведенной в п. 3.

<i>Стратегические цели</i>	Данный рабочий документ связан со стратегическими целями "Безопасность полетов" и "Аэронавигационный потенциал и эффективность".
<i>Финансовые последствия</i>	<i>Воздействие на авиационное сообщество:</i> Внедрение политики, технологий и процедур в целях гарантированного обеспечения киберустойчивости может оказать значимое финансовое воздействие на некоторые заинтересованные стороны. Это воздействие, однако, будет зависеть от масштаба авиационной деятельности и соответствующей инфраструктуры. Возможно также воздействие на безопасность полетов, эффективность, финансовое положение и репутацию в том случае, если нельзя будет обеспечить киберустойчивость аэронавигационной системы.

	<i>Воздействие на ИКАО (относительно уровней ресурсов в текущем бюджете Регулярной программы):</i> Поскольку процесс планирования, разработки и внедрения на государственном уровне глобальной структуры доверия и дальнейшей деятельности, направленной на повышение уровня осведомленности в вопросах киберустойчивости, будет продолжаться в течение следующего трехлетнего периода, необходимы дополнительные ресурсы, как финансовые, так и людские, в поддержку усилий ИКАО в узкоспециальных областях, связанных с киберустойчивостью и структурой доверия.
<i>Справочный материал</i>	Приложение 1, <i>Выдача свидетельств авиационному персоналу</i> Приложение 6, <i>Метеорологическое обеспечение международной аэронавигации</i> Приложение 8, <i>Летная годность воздушных судов</i> Приложение 10, <i>Авиационная электросвязь</i> Приложение 11, <i>Обслуживание воздушного движения</i> Приложение 14, <i>Аэродромы</i> Приложение 15, <i>Службы аэронавигационной информации</i> Приложение 17, <i>Безопасность. Защита международной гражданской авиации от актов незаконного вмешательства</i> Приложение 19, <i>Управление безопасностью полетов</i> Дос 9854, <i>Глобальная эксплуатационная концепция ОрВД</i> Дос 9750, <i>Глобальный аэронавигационный план</i> Дос 9896, <i>Руководство по сети авиационной электросвязи (ATN), использующей стандарты и протоколы пакета протоколов Интернет (IPS)</i> Дос 10022, <i>Действующие резолюции Ассамблеи (по состоянию на 4 октября 2013 года)</i> Дос 10039, <i>Руководство по общесистемному управлению информацией (SWIM)</i>

1. ВВЕДЕНИЕ

1.1 Авиация представляет собой сложную систему, составленную из разнообразных сетей и устройств, которые при обмене цифровыми данными и информацией становятся все более взаимосвязанными и взаимозависимыми. Заинтересованные стороны авиационного сектора, такие как государства, эксплуатанты воздушных судов и аэродромов, поставщики аэронавигационного обслуживания (ПАНО) и другие стали зависеть в своей повседневной деятельности от взаимосвязанных и взаимодействующих систем в области информационных и связанных технологий (ICT), став частью цифровой экосистемы гражданской авиации. Такие события, как разработка общесистемного управления информацией (SWIM), внедрение дистанционно пилотируемых авиационных систем (ДПАС), а также появление будущих пользователей воздушного пространства и заинтересованных сторон, которые еще не начали свою деятельность, только укрепляют эту взаимозависимость.

1.2 Развитие в направлении взаимосвязанных и взаимодействующих информационных систем, о котором упоминалось выше, приводит также к возникновению новых уязвимых мест. События, связанные с кибербезопасностью, могут оказывать многоуровневое воздействие на авиацию и создавать угрозу работе системы аэронавигации. Эти события могут влиять на обмен информацией между заинтересованными сторонами, напрямую затрагивая безопасность полетов, потенциал и эффективность, что может привести к серьезным последствиям.

1.3 В полностью взаимосвязанной авиационной среде киберустойчивость становится критически важным фактором обеспечения безопасности деятельности. Поэтому необходимо повысить устойчивость авиационной системы к киберугрозам. Киберустойчивость можно определить как способность авиационной системы выдерживать состояние сниженных рабочих характеристик, возникшее в результате киберугроз и киберинцидентов, в том числе утраты или порчи данных и системных нарушений, таких как потеря возможности установления связи или интероперабельности, а также способность выходить из этого состояния.

1.4 Киберустойчивость можно обеспечить путем применения сочетания стандартов, процедур и методов, способствующих уменьшению киберугроз в отношении систем, критически важных для безопасности и эффективности авиации.

1.5 Вопрос о важности надлежащего подхода к обеспечению киберустойчивости в гражданской авиации будет включен в *Глобальный аэронавигационный план* (Дос 9750) издания 2019 года и является главным элементом реализации идей, изложенных в документе *Глобальная эксплуатационная концепция ОрВД* (Дос 9854). Соответственно, повышение уровня осведомленности заинтересованных сторон о киберугрозах, уязвимых местах и рисках для авиационной системы необходимо для дальнейшего развития комплекса глобально согласованных подходов к обеспечению киберустойчивости в гражданской авиации.

1.6 Признавая срочность и значимость вопроса защиты критически важных систем инфраструктуры, информационных и связанных технологий гражданской авиации от киберугроз, 39-я сессия Ассамблеи ИКАО призвала к применению скоординированного подхода для достижения приемлемых и адекватных возможностей обеспечения киберустойчивости в глобальном масштабе. В этой связи и в целях содействия улучшению осведомленности в вопросах киберустойчивости всего авиационного сообщества ИКАО создала Исследовательскую группу Секретариата по кибербезопасности (SSGC), с тем чтобы охватить все аспекты системы международной авиации, которые могут быть затронуты киберинцидентами.

2. ОБСУЖДЕНИЕ

2.1 Киберустойчивая система необходима для обеспечения информационно насыщенной среды с данными в режиме реального времени, позволяющей осуществлять прогнозный анализ и моделирование. Вместе с рядом автоматизированных инструментов для принятия решений и осуществления вспомогательных функций это позволит развивать обслуживание как предусмотрено в документе Дос 9854.

2.2 Обеспечение системной взаимосвязанности и киберустойчивости посредством структуры доверия

2.2.1 Успешное управление киберустойчивостью требует подхода, глобально согласованного между всеми заинтересованными сторонами. Необходимо согласие в вопросе о том, каким образом должны взаимодействовать цифровые информационные системы, чтобы обеспечить общую информационно насыщенную среду для авиационного сообщества в целом. Защищенный и устойчивый обмен информацией, требуемый для удовлетворения потребностей развивающейся деятельности авиационного сектора, может быть обеспечен посредством структуры доверия, состоящей из согласованных стандартов, процедур, методов и соглашений в области цифрового обмена информацией в системах "земля – земля", "воздух – земля" и "воздух – воздух" и регулирования системы идентификации.

2.2.2 Для повышения уровня киберустойчивости требуется также улучшение защиты обмена информацией между заинтересованными сторонами и ее передачи от системы к системе.

Модели, принятые в других отраслях и основанные на открытых и проверенных стандартах информационных и связанных технологий, таких как концепция структур доверия, цифровые сертификаты и виртуальные частные сети, работающие поверх общедоступной инфраструктуры Интернета, могут служить примером возможной защиты глобального обмена информацией гражданской авиации.

2.2.3 Прежде всего, критически важные с точки зрения обеспечения безопасности системы и каналы, используемые для обмена цифровой информацией, следует разрабатывать и непрерывно анализировать с использованием подхода "изначальной надежности", при котором киберустойчивость обеспечивается методами как технологического, так и процедурного характера.

2.2.4 Глобальная структура доверия позволяет улучшить интероперабельность и возможности установления связи цифровых систем, таким образом повышая уровень киберустойчивости. При разработке структуры доверия в авиации на глобальном уровне следует сосредоточиться на требованиях в области управления, политики и общих технических характеристик, которые будут выполняться заинтересованными сторонами в авиационном секторе, желающими обмениваться цифровой информацией. Фрагментарные и нескоординированные подходы на государственном или региональном уровне были бы неэффективны, привели бы к высоким затратам для всех заинтересованных сторон и в конечном итоге ограничили бы возможности цифровых систем в отношении установления связи и взаимодействия, а также снизили бы уровень киберустойчивости авиационной системы.

2.2.5 Глобальная структура доверия может быть создана только устанавливающим стандарты органом, заслужившим доверие значительного большинства заинтересованных сторон в авиации и по своей сути способным служить опорой в деле глобального согласования политики, процедур и методов в целях обеспечения безопасности и эффективности гражданской авиации.

2.2.6 Проект концепции функционирования структуры доверия в поддержку защищенного обмена информацией размещен по адресу (<https://www4.icao.int/ganpportal/trustframework>). Этот предварительный проект служит источником дополнительной информации о структуре доверия и подлежит доработке.

2.3 **Обмен информацией и осведомленность в области кибербезопасности**

2.3.1 Ни одна отдельная заинтересованная сторона в авиации не может защитить себя от всех киберугроз своими силами. Обмен информацией помог бы всем заинтересованным сторонам в авиации лучше подготовиться к более широкому ряду киберинцидентов и повысить уровень своих возможностей в сфере уменьшения воздействия таких инцидентов и снижения рисков. Обмен информацией в области кибербезопасности, затрагивающей эксплуатационную безопасность, вызвал бы дальнейшее развитие культуры доверия между заинтересованными сторонами в авиационном секторе, которая в конечном итоге повышает уровень киберустойчивости авиационной системы и улучшает осведомленность всех заинтересованных сторон о киберугрозах.

2.3.2 Всем заинтересованным сторонам также настоятельно рекомендуется признать, что, несмотря на возрастающий уровень зависимости от информационных технологий, участие людей одновременно является главной причиной возникновения киберугроз и первой линией защиты от них. Эксплуатационный персонал на всех уровнях должен пройти подготовку по распознаванию общих аспектов киберугроз и сообщению информации о любой предполагаемой угрозе или инциденте в области кибербезопасности, сколь бы незначительными они ни были.

3. ВЫВОД

3.1 Степень взаимосвязанности авиационных систем продолжит расти, а цифровая авиационная система продолжит расширяться. Без согласованной в глобальном масштабе структуры доверия, состоящей из требований в области управления, политики и общих технических характеристик для обеспечения системной взаимосвязанности и интероперабельности, киберустойчивость авиации гарантировать нельзя. Обмен информацией об угрозах и инцидентах в области кибербезопасности в сочетании с надлежащей подготовкой персонала содействует дальнейшему повышению уровня киберустойчивости. Сохранение безопасности и эффективности авиации во все более взаимосвязанной и интероперабельной цифровой авиационной системе требует согласованных многоуровневых подходов к обеспечению киберустойчивости, приносящих прямую выгоду всем заинтересованным сторонам сейчас и в будущем.

3.2 С учетом важности борьбы с киберугрозами и ввиду их воздействия на устойчивость авиационной системы Конференции предлагается согласиться со следующей рекомендацией:

Рекомендация 5.4/х. Киберустойчивость

Конференции рекомендуется:

- а) обратиться к ИКАО с просьбой проводить работу с государствами, отраслью и международными организациями в целях разработки глобально согласованной структуры доверия в авиации, включающей требования в области управления, политики, подготовки персонала и общих технических характеристик, с тем чтобы позволить создать информационно насыщенную и устойчивую авиационную систему;
- б) обратиться к ИКАО с просьбой проводить работу с государствами, отраслью и международными организациями в целях распространения информации о структуре доверия, разъяснения ее преимуществ и улучшения осведомленности о ее роли в повышении уровня киберустойчивости;
- с) настоятельно призвать государства, отрасль и международные организации к сотрудничеству с ИКАО в целях повышения уровня осведомленности о киберугрозах и процессах, связанных с системной устойчивостью, а также координирования деятельности по обмену информацией о киберинцидентах и по подготовке персонала.

— КОНЕЦ —