



РАБОЧИЙ ДОКУМЕНТ

ЧЕТЫРНАДЦАТАЯ АЭРОНАВИГАЦИОННАЯ КОНФЕРЕНЦИЯ

Монреаль, Канада, 26 августа – 6 сентября 2024 года

Пункт 4 повестки дня. Гиперсвязность аэронавигационной системы

4.2. Кибербезопасность и устойчивость информационных систем

ВНЕДРЕНИЕ ОСНОВНЫХ ЭЛЕМЕНТОВ МЕХАНИЗМА ОБЕСПЕЧЕНИЯ АВИАЦИОННОЙ КИБЕРБЕЗОПАСНОСТИ

(Представлено Секретариатом)

КРАТКАЯ СПРАВКА

Цифровизация всех областей гражданской авиации делает все более насущной необходимость решения вопросов кибербезопасности в гражданской авиации для обеспечения безопасности полетов, авиационной безопасности, потенциала и эффективности сектора. В настоящем документе представлен ряд основных элементов высокого уровня, которые государствам и заинтересованным сторонам следует рассмотреть для комплексного и согласованного обеспечения авиационной кибербезопасности во всех соответствующих областях. В нем также указывается на необходимость подготовки ИКАО дополнительного инструктивного материала для оказания поддержки государствам и заинтересованным сторонам с повышением уровня защищенности и устойчивости сектора перед киберугрозами и источниками риска. В нем также содержатся рекомендации, позволяющие обеспечить дальнейшую согласованность и последовательность шагов на региональном уровне.

Действия: Конференции предлагается согласиться с рекомендацией 4.2/x "Авиационная кибербезопасность", изложенной в п. 3.

<i>Стратегические цели</i>	Данный рабочий документ связан со стратегическими целями "Безопасность полетов", "Аэронавигационный потенциал и эффективность", а также "Авиационная безопасность и упрощение формальностей"
<i>Финансовые последствия</i>	<i>Последствия для авиационного сообщества:</i> Реализация шагов, рассматриваемых в данном документе, потребует определенных затрат. Однако их реализация даст возможность выработать четкий подход к обеспечению авиационной кибербезопасности, четко определив роли и обязанности всех заинтересованных сторон. <i>Последствия для ИКАО (относительно текущего объема ресурсов бюджета Регулярной программы):</i> Деятельность ИКАО, о которой идет речь в данном рабочем документе, будет продолжаться в течение следующих трех лет. Потребуется дополнительные ресурсы на поддержку этих мероприятий, а также на информационную поддержку и содействие реализации.

<i>Справочный материал</i>	Дос 8973, <i>Руководство по авиационной безопасности (Restricted)</i> Дос 9750, <i>Глобальный аэронавигационный план</i> Дос 10004, <i>Глобальный план обеспечения безопасности полетов</i> Дос 10118, <i>Глобальный план обеспечения авиационной безопасности</i> Дос 10184, <i>Действующие резолюции Ассамблеи (по состоянию на 7 октября 2022 года)</i> Стратегия ИКАО в части, касающейся авиационной кибербезопасности План действий по обеспечению кибербезопасности Инструктивный материал по политике обеспечения кибербезопасности Культура кибербезопасности в гражданской авиации
----------------------------	--

1. ВВЕДЕНИЕ

1.1 На 40-й сессии Ассамблеи ИКАО была подтверждена важность и острая необходимость выполнения глобального обязательства по принятию мер всеми заинтересованными сторонами для совместного решения проблем кибербезопасности в гражданской авиации, путем принятия резолюции А40-10 "*Решение проблем кибербезопасности в гражданской авиации*" и одобрения Стратегии в области авиационной кибербезопасности ИКАО¹. На 41-й сессии Ассамблеи ИКАО важность решения проблем кибербезопасности в гражданской авиации была подтверждена в обновленной резолюции А41-19.

1.2 Ассамблея призвала ИКАО также разработать План действий по поддержке реализации государствами и заинтересованными сторонами Стратегии в области авиационной кибербезопасности. Второе издание Плана действий по кибербезопасности², опубликованное в январе 2022 года, закладывает основу для совместной работы ИКАО, государств и заинтересованных сторон, и в нем изложен ряд принципов, мер и действий для достижения целей семи основополагающих элементов Стратегии кибербезопасности³.

1.3 В соответствии с Планом действий по обеспечению кибербезопасности ИКАО уже опубликовала инструктивный материал по темам, связанным с авиационной кибербезопасностью. ИКАО также изучила соответствие поставленным в них целям международно-правовым документам, посвященным борьбе с кибератаками на гражданскую авиацию, а также необходимость включения Стандартов и Рекомендуемой практики по авиационной кибербезопасности в Приложения к Конвенции о международной гражданской авиации (Чикагской конвенции), разработки материалов для содействия обеспечению доверия на оперативном уровне в различных областях авиации, повышения осведомленности о важности устранения киберугроз и рисков для гражданской авиации, разработки инициатив по наращиванию возможностей обеспечения авиационной кибербезопасности и проведения теоретических учений по международной авиационной кибербезопасности.

¹ <https://www.icao.int/aviationcybersecurity/Pages/Aviation-Cybersecurity-Strategy.aspx>

² <https://www.icao.int/aviationcybersecurity/Pages/Cybersecurity-Action-Plan.aspx>

³ Основополагающими элементами Стратегии в области авиационной кибербезопасности являются: международное сотрудничество, управление, эффективное законодательство и нормативные положения, политика в области кибербезопасности, обмен информацией, планирование мероприятий на случай инцидентов и действий в чрезвычайных ситуациях, а также наращивание потенциала, подготовка персонала и формирование культуры кибербезопасности.

2. РАССМОТРЕНИЕ ВОПРОСА

2.1 Поскольку в сфере гражданской авиации для повышения потенциала и эффективности при сохранении оговоренного уровня безопасности полетов и авиационной безопасности продолжают использоваться технологические инновации, вопросы кибербезопасности рассматриваются в каждой области авиации отдельно. С годами это привело к тому, что авиация превратилась в своего рода "систему систем" (SoS), где средства контроля и процессы обеспечения защиты от кибератак и устойчивости разрабатывались и внедрялись без использования комплексного подхода, что привело к потенциальным пробелам на макроуровне.

2.2 В этой связи важно, чтобы авиационная кибербезопасность обеспечивалась в сфере гражданской авиации на национальном, региональном и международном уровнях скоординированным, согласованным и целостным образом. Это позволит устранять киберугрозы и снижать риск для гражданской авиации без ущерба для требований к обеспечению безопасности полетов, авиационной безопасности, пропускной способности и эффективности.

2.3 Была проделана значительная работа по решению вопросов кибербезопасности в гражданской авиации, однако требуются дополнительные рекомендации для поддержки внедрения государствами требований по обеспечению авиационной кибербезопасности в существующие контрольно-регуляторные режимы, а также в их региональные и национальные планы, касающиеся соответствующих областей гражданской авиации, и, прежде всего, безопасности полетов, авиационной безопасности и упрощения формальностей, а также аэронавигации.

2.4 Более того, как в резолюции Совета Безопасности ООН 2341 (2017) о защите критической инфраструктуры от террористических актов, так и в резолюции Генеральной Ассамблеи ООН (A/RES/77/298) о восьмом обзоре Глобальной контртеррористической стратегии ООН (A/RES/60/288) подчеркивается важность многостороннего сквозного сотрудничества международных, региональных и субрегиональных организаций, частного сектора и гражданского общества для решения проблем кибербезопасности.

2.5 В соответствии с действующими резолюциями Ассамблеи ИКАО, Стратегией в области авиационной кибербезопасности, предусмотренным ею Планом действий и различными инструктивными материалами, разработанными ИКАО, в настоящем документе предлагаются основные базовые элементы, которые следует рассмотреть государствам и заинтересованным сторонам для противодействия киберугрозам и рискам для гражданской авиации. Эти основные элементы должны включать:

а) Нормативные аспекты государственного уровня:

- 1) **Управление авиационной кибербезопасностью на государственном уровне:** этот элемент включает аспекты, связанные с определением профильного органа по вопросам авиационной кибербезопасности, включением требований к обеспечению авиационной кибербезопасности в государственные программы безопасности полетов и национальные программы авиационной безопасности для гражданской авиации, распределением ролей и обязанностей авиационных и неавиационных органов (например, национальных органов по кибербезопасности) и координацией их деятельности в части регулирования и контроля обеспечения кибербезопасности в гражданской авиации, использованием национальных ресурсов обеспечения кибербезопасности для поддержки организаций, занимающихся мониторингом, обнаружением, реагированием на киберинциденты и восстановлением после них, но не исчерпывается ими.

- 2) **Национальная правовая база:** этот элемент включает в себя аспекты, связанные с национальной правовой базой государств, дающей возможность судебного преследования за кибератаки на объекты гражданской авиации. Сюда также относятся аспекты, связанные с ратификацией *Конвенции о борьбе с незаконными актами в отношении международной гражданской авиации* (Пекин, 2010) и *Протокола, дополняющего Конвенцию о борьбе с незаконным захватом воздушных судов* (Пекин, 2010), как инструментами борьбы с кибератаками на объекты гражданской авиации в глобальном масштабе.
 - 3) **Политика авиационной кибербезопасности:** этот элемент включает аспекты, связанные с политикой авиационной кибербезопасности на государственном уровне.
 - 4) **Надзорные функции:** этот элемент включает в себя аспекты, связанные с возможностями государств по осуществлению мер контроля за обеспечением авиационной кибербезопасности, которые могут быть реализованы с помощью существующих механизмов контроля за обеспечением безопасности полетов и авиационной безопасности на скоординированной основе.
- b) Аспекты, касающиеся государств и заинтересованных сторон:
- 1) **Управление рисками в плане кибербезопасности:** этот элемент включает аспекты, связанные с определением критических объектов авиационной инфраструктуры и интеграцию оценки рисков в плане кибербезопасности в существующие программы оценки рисков для безопасности полетов и авиационной безопасности этой инфраструктуры.
 - 2) **Представление данных о киберинцидентах:** этот элемент включает в себя аспекты, связанные с внедрением механизма представления данных о киберинцидентах организациями в профильные органы власти, которое может осуществляться с использованием отдельных или уже существующих механизмов представления данных о безопасности полетов или авиационной безопасности.
 - 3) **Обмен информацией по кибербезопасности:** этот элемент включает аспекты, связанные с внедрением механизмов обмена информацией между государствами и заинтересованными сторонами на национальном, региональном и международном уровнях.
 - 4) **Реагирование на киберинциденты и восстановление после них:** этот элемент включает аспекты, связанные с реализацией планов и возможностей реагирования на киберинциденты и восстановления после них. Сюда также относятся аспекты, связанные с интеграцией этих планов в авиационные планы действий и управления в чрезвычайных и кризисных ситуациях.
 - 5) **Управление цепочками поставок с точки зрения кибербезопасности:** этот элемент включает аспекты, связанные с управлением рисками с точки зрения кибербезопасности в цепочках поставок авиационных и неавиационных товаров и услуг. Сюда относятся несколько типов цепочек поставок, например, сертифицированное авиационное оборудование и системы, услуги авиационных систем (например, системы планирования

полетов, аэропортовые сети), поставщики неавиационных услуг (например, поставщики облачных услуг, поставщики спутниковой связи).

- 6) **Культура кибербезопасности:** этот элемент включает в себя аспекты, связанные с формированием устойчивой культуры кибербезопасности в гражданской авиации с использованием опыта отрасли по формированию культуры обеспечения безопасности полетов и авиационной безопасности.
- 7) **Программы подготовки специалистов по авиационной кибербезопасности:** этот элемент включает аспекты, связанные с разработкой и проведением программ подготовки специалистов по авиационной кибербезопасности, ориентированных на различную аудиторию (например, общая подготовка или подготовка к выполнению конкретных функций).

2.6 Учитывая, что во многих государствах авиационный сектор считается национальной критической инфраструктурой, необходим поэтапный и многоуровневый подход к обеспечению кибербезопасности и обеспечению устойчивости этого сектора. Задача состоит в реализации стратегии "глубокоэшелонированной обороны"⁴, которая охватывает все заинтересованные стороны, прямо или косвенно участвующие в устранении киберугроз и рисков для гражданской авиации. Перечисленные выше элементы не являются полным перечнем областей, которые должны быть рассмотрены в рамках системы авиационной кибербезопасности, однако они служат основой для обеспечения надежного и эффективного управления авиационной кибербезопасностью, включая обеспечение защиты и устойчивости авиационных объектов, находящихся в ведении государств и заинтересованных сторон.

2.7 В регионах ИКАО создаются группы по обеспечению кибербезопасности для поддержки региональных обсуждений вопросов обеспечения защиты от кибератак и устойчивости к внешним воздействиям в различных областях авиации. Эти мероприятия весьма важны для решения конкретных задач, связанных с киберугрозами и рисками в каждом регионе, однако существует потенциальный риск дублирования и даже конфликта, если эти мероприятия не скоординировать в рамках различных региональных групп и планов. Такая координация позволит выработать целостный, согласованный и скоординированный подход к устранению киберугроз и рисков в различных регионах, а также обеспечит последовательность и взаимодополняемость региональных планов аэронавигации, безопасности полетов, авиационной безопасности и упрощения формальностей в отношении авиационной кибербезопасности, что в дальнейшем положительно скажется на деятельности государств-членов по планированию и реализации мероприятий на национальном уровне. Государства могут также использовать эти форумы, чтобы сообщать ИКАО о проблемах, с которыми они сталкиваются при решении вопросов кибербезопасности в гражданской авиации, что ляжет в основу деятельности ИКАО, связанной с разработкой положений и инструктивного материала.

3. ВЫВОД

3.1 Цифровизация всех областей гражданской авиации высвечивает все более насущную необходимость решения вопросов кибербезопасности в гражданской авиации для обеспечения безопасности полетов, авиационной безопасности, потенциала и эффективности работы сектора. Признавая проблемы, связанные с обеспечением авиационной кибербезопасности,

⁴ "Глубокоэшелонированная оборона" – это многоуровневое или поэтапное применение различных контрмер для достижения целей обеспечения безопасности. Эта методика предполагает использование на нескольких уровнях различных технологий обеспечения защиты от общих направлений атак, с тем чтобы гарантировать, что атаки, пропущенные одной технологией, будут нейтрализованы при помощи другой (ISO/IEC 62443 1-1).

государства и заинтересованные стороны должны учитывать основные базовые элементы на нормативном и оперативном уровнях.

3.2 В свете вышесказанного Конференции предлагается согласиться со следующей рекомендацией:

Рекомендация 4.2/х. Авиационная кибербезопасность

Государствам рекомендуется:

- a) разработать и реализовать национальный план устранения киберугроз и рисков для гражданской авиации на основе целостного подхода, охватывающего все сферы авиации и в координации с соответствующими заинтересованными не связанными с авиацией сторонами, используя основные элементы в качестве ориентира;
- b) согласовать мероприятия по обеспечению авиационной кибербезопасности с региональными аэронавигационными планами, планами обеспечения безопасности полетов, авиационной безопасности и упрощения формальностей в рамках процессов координации деятельности региональных групп планирования и осуществления проектов (PIRG), региональных групп по обеспечению безопасности полетов (RASG) и региональных групп по авиационной безопасности и упрощению формальностей (AVSEC/FAL);
- c) сообщать ИКАО о своем опыте реализации положений и инструктивного материала ИКАО, касающихся авиационной кибербезопасности по линии соответствующих групп экспертов или в рамках работы PIRG, RASG и региональных групп AVSEC/FAL; и рекомендовать

ИКАО:

- d) предоставить инструктивный материал по основным элементам для оказания поддержки государствам и заинтересованным сторонам в решении вопросов авиационной кибербезопасности, а также последовательно и скоординированным образом интегрировать все мероприятия по обеспечению авиационной кибербезопасности в единую систему.

— КОНЕЦ —