Международная организация гражданской авиации

A41-WP/22
EX/10
7/7/22

РАБОЧИЙ ДОКУМЕНТ

АССАМБЛЕЯ — 41-Я СЕССИЯ

ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ

Пункт 14 повестки дня. Авиационная безопасность. Политика

КИБЕРБЕЗОПАСНОСТЬ В ГРАЖДАНСКОЙ АВИАЦИИ

(Представлено Советом ИКАО)

КРАТКАЯ СПРАВКА

Осознание сектором гражданской авиации важности решения проблемы киберугроз в сфере гражданской авиации с годами постоянно повышается, несмотря на некоторые проблемы, главным образом относимые, прямо и косвенно, к кризису, вызванному пандемией COVID-19. Хотя много изменений происходит на национальном, региональном и глобальном уровнях, необходимо приступить к выполнению еще большего объема работ, особенно на национальном уровне, чтобы обеспечить целостный, согласованный и последовательный подход к обеспечению кибербезопасности авиации во всем секторе гражданской авиации.

В данном документе представлен обзор действий, связанных с кибербезопасностью в авиации, включая мероприятия, предписанные Ассамблеей, и в нем предлагается обновить резолюцию A40-10 *"Решение проблем кибербезопасности в гражданской авиации"*, чтобы подчеркнуть важность повышения уровня кибербезопасности и киберустойчивости сектора гражданской авиации.

Действия: Ассамблее предлагается:

a) принять к сведению информацию о развитии событий в области обеспечения кибербезопасности в авиации;

b) принять представленную в добавлении пересмотренную резолюцию Ассамблеи *"Решение проблем кибербезопасности в гражданской авиации"*, которая заменит резолюцию Ассамблеи A40-10.

Стратегические цели:	Данный рабочий документ связан со следующими стратегическими целями: *"Аэронавигационный потенциал и эффективность", "Безопасность полетов"* и *"Авиационная безопасность и упрощение формальностей"*
Финансовые последствия:	Указанная в прилагаемом рабочем документе Ассамблеи деятельность ИКАО будет, руководствуясь положениями бизнес-плана ИКАО на 2023–2025 гг., осуществляться в рамках ресурсов регулярного бюджета на 2023–2025 годы и/или за счет внебюджетных взносов.
Справочный материал:	Doc 10140, Действующие резолюции Ассамблеи (по состоянию на 4 октября 2019 года) Doc 10118, *Глобальный план обеспечения авиационной безопасности* Doc 9750, *Глобальный аэронавигационный план* *Стратегия кибербезопасности в авиации* *План действий по обеспечению кибербезопасности*

1. ВВЕДЕНИЕ

1.1 39-я сессия Ассамблеи ИКАО поручила ИКАО обеспечить детальное рассмотрение проблемы киберугроз в сфере гражданской авиации и оказать содействие государствам и отрасли в принятии необходимых мер. В 2017 году была создана Исследовательская группа Секретариата по кибербезопасности (SSGC) для проведения этой работы.

1.2 40-я сессия Ассамблеи ИКАО вновь подтвердила важность и безотлагательность глобальных обязательств всех заинтересованных сторон предпринять действия в целях совместного решения проблемы кибербезопасности в авиации и приняла Стратегию кибербезопасности в авиации. Она также призвала ИКАО разработать план действий по внедрению Стратегии кибербезопасности в авиации и продолжить междисциплинарное рассмотрение и координацию вопросов кибербезопасности. Кроме того, она отметила ряд недостатков в структуре рассмотрения вопросов кибербезопасности в ИКАО и обсудила ряд критериев, которые могут укрепить пересмотренную структуру кибербезопасности.

1.3 Стоит отметить, что пандемия COVID-19 сказалась на ходе работы ИКАО по обеспечению кибербезопасности в авиации в связи с тем, что ресурсы были перенаправлены на решение критически важных задач кризисного управления и на поддержку процесса возобновления и восстановления деятельности гражданской авиации, а также в связи с финансовыми ограничениями, с которыми столкнулась Организация в течение первых восьми месяцев 2020 года, приведшими к отсутствию ресурсов в области обеспечения кибербезопасности.

2. ОБСУЖДЕНИЕ

2.1 План действий по обеспечению кибербезопасности

2.1.1 В соответствии с резолюцией A40-10 Ассамблеи, ИКАО разработала и опубликовала в ноябре 2020 года План действий по обеспечению кибербезопасности (ПДОК) в поддержку государств и заинтересованных сторон в деле осуществления стратегии кибербезопасности в авиации. ПДОК создает основу для сотрудничества ИКАО, государств и заинтересованных сторон и содержит ряд принципов, мер и действий по достижению целей семи основополагающих элементов стратегии кибербезопасности (международное сотрудничество; управление, эффективное законодательство и нормативные положения; политика в области кибербезопасности; обмен информацией; планирование мероприятий на случай инцидентов и действий в чрезвычайных ситуациях; наращивание потенциала, подготовка персонала и формирование культуры кибербезопасности).

2.1.2 Принимая во внимание меняющиеся приоритеты государств-членов из-за продолжающейся пандемии COVID-19 и опыт государств и заинтересованных сторон в осуществлении инициатив в области авиационной кибербезопасности в своих государствах и организациях, ИКАО пересмотрела ПДОК и опубликовала второе издание документа в январе 2022 года. Пересмотр включал в себя оптимизацию документа с целью сделать его более кратким и ясным, и в пункты действий были внесены уточнения, касающиеся действий, показателей и сроков.

2.2 Укрепление механизма обеспечения кибербезопасности в ИКАО

2.2.1 40-я сессия Ассамблеи ИКАО отметила наличие нескольких органов, занимающихся вопросами кибербезопасности в ИКАО, и выразила обеспокоенность возможностью возникновения пробелов, дублирования, непоследовательности и отсутствия прозрачности. Для устранения такой обеспокоенности Ассамблея призвала ИКАО объединить работу этих групп в рамках комплексной структуры и обсудила ряд критериев, которые могут лечь в основу пересмотренной структуры управления деятельностью в области кибербезопасности.

2.2.2 Совет в ходе своей 218-й сессии одобрил методику разработки технико-экономического обоснования и анализа недостатков механизма по решению проблем кибербезопасности. Результаты двух первых этапов исследования были представлены во время 219-й сессии. Совет поручил Секретариату продолжить рассмотрение и обновление технико-экономического обоснования и делегировал Президенту Совета полномочия рассмотреть вопрос об учреждении небольшой рабочей группы в составе представителей Совета и членов Аэронавигационной комиссии (АНК) для разработки с помощью Секретариата этапа 3 технико-экономического обоснования. Небольшая рабочая группа активно проводила совещания в период с ноября 2020 года по январь 2021 года, рассмотрела несколько вариантов структуры управления и рекомендовала решение, которое было одобрено Советом в ходе его 222-й сессии. Новая структура управления вопросами кибербезопасности в ИКАО включает в себя:

a) преобразование Исследовательской группы Секретариата по кибербезопасности в Группу экспертов по кибербезопасности, отчитывающуюся перед Комитетом по авиационной безопасности Совета ИКАО;

b) интеграцию Исследовательской группы по механизму доверия в структуру Групп экспертов АНК;

c) создание Специального координационного комитета Совета по кибербезопасности (АНССС). В членский состав Комитета входят по одному члену Авиатранспортного комитета, Комитета по авиационной безопасности, Аэронавигационной комиссии и каждой Группы экспертов ИКАО и экспертной группы, занимающейся отдельными аспектами кибербезопасности в своих программах работы. Ожидается что для Совета и всех занимающихся вопросами кибербезопасности в ИКАО Комитет станет единым координатором всех направлений деятельности ИКАО, связанных с кибербезопасностью, что повысит таким образом уровень ответственности, прозрачности, эффективности и координации работы ИКАО в области авиационной кибербезопасности и киберустойчивости. Совет в ходе 224-й сессии одобрил круг полномочий АНССС.

2.2.3 После принятия Советом решения о новой структуре управления в ходе 225-й сессии была учреждена Группа экспертов по кибербезопасности, которая провела свое первое совещание в мае 2022 года. АНК в ходе своей 219-й сессии одобрила преобразование Исследовательской группы по механизму доверия в новую Группу экспертов АНК для продолжения работы в рамках международного авиационного механизма доверия.

2.3 Разработка международного авиационного механизма доверия

2.3.1 Начиная со своей 223-й сессии Совет обсуждает разработку международного авиационного механизма доверия. Он продолжит заниматься этой работой, в том числе концепцией функционирования и вопросами управления таким механизмом.

2.4 Достаточность инструментов международного воздушного права для решения вопроса о кибератаках на гражданскую авиацию

2.4.1 Стратегия авиационной кибербезопасности призывает к анализу соответствующих международных правовых документов, чтобы выявить существующие или недостающие основные правовые положения, касающиеся предотвращения, судебного преследования и своевременной реакции на кибер-инциденты. Эта задача была соответственно отражена в Плане действий по обеспечению авиационной кибербезопасности как вопрос, требующий от ИКАО принятия мер. Поэтому SSGC учредила Исследовательскую подгруппу по правовым аспектам (RSGLEG). В состав Подгруппы вошли эксперты по юридическим вопросам и вопросам кибербезопасности, чтобы обеспечить наличие всех экспертных знаний, необходимых для достижения целей подгруппы. Как было договорено на последнем совещании RSGLEG в январе 2022 года, Секретариат представил доклад о работе, проведенной Подгруппой, 38-й сессии Юридического комитета, которая прошла в марте 2022 года.

2.5 **Инструктивный материал**

2.5.1 В соответствии с Планом действий по обеспечению авиационной кибербезопасности ИКАО подготовила инструктивный материал для оказания поддержки государствам и заинтересованным сторонам в решении вопросов кибербезопасности в гражданской авиации, в который вошли следующие документы (опубликованные на сайте ICAO-NET в подразделе "Others" раздела "Publications"):

a) Инструктивный материал относительно протокола "Светофор" (TLP), который предоставляет государствам и заинтересованным сторонам указания по использованию TLP с тем, чтобы упростить совместное пользование информацией в области кибербезопасности.

b) Стратегический инструктивный материал по кибербезопасности, в котором рассматриваются вопросы защиты и устойчивости критически важной инфраструктуры международной гражданской авиации от киберугроз и потребности в многостороннем сотрудничестве в гражданской авиации, в том числе с участием внешних полномочных органов. Кроме того, в инструктивном материале говорится о необходимости назначения органа, компетентного в вопросах авиационной кибербезопасности и в него также включен шаблон для оказания содействия государствам и заинтересованным сторонам в разработке политики в области кибербезопасности.

c) Культура кибербезопасности в гражданской авиации, которая поддерживает разработку и реализацию надежной культуры кибербезопасности, основываясь на успехе гражданской авиации в реализации культуры безопасности полетов и культуры авиационной безопасности.

2.6 **Наращивание потенциала**

2.6.1 В 2020 году ИКАО разработала Дорожную карту подготовки кадров в сфере кибербезопасности, чтобы поддержать усилия Организации по созданию потенциала в области предоставления государствам и заинтересованным сторонам надлежащего, последовательного и профильного обучения по вопросам кибербезопасности в авиации. Дорожная карта подготовки кадров в сфере кибербезопасности обеспечивает выполнение Стратегии кибербезопасности в авиации и Плана действий по обеспечению авиационной кибербезопасности. Ее разработка также поддерживает резолюцию A40-25 Ассамблеи "*Реализация стратегий подготовки авиационных специалистов и наращивания потенциала",* в которой говорится о том, как ИКАО посредством действий по подготовке персонала должна помогать и поддерживать государства в процессе развития достаточных человеческих ресурсов и потенциала. Вслед за Дорожной картой подготовки кадров ИКАО начала создавать комплект учебных программ по кибербезопасности, в который к настоящему моменту входят следующие курсы:

2.6.1.1 Основы руководства и технического управления деятельностью по обеспечению авиационной кибербезопасности. Курс был разработан в сотрудничестве с Авиационным университетом имени Эмбри-Риддла и впервые проведен в октябре 2021 года. Это комплексный ознакомительный курс, который охватывает все аспекты кибербезопасности, рассматриваемые в Стратегии кибербезопасности в авиации.

2.6.1.2 Управление факторами риска авиационной безопасности в системе организации воздушного движения (ОрВД). Курс был разработан в сотрудничестве с ЕВРОКОНТРОЛЕМ. Он охватывает вопросы безопасности в системе ОрВД и включает элементы физической безопасности и кибербезопасности. Первая сессия курса будет проведена в ноябре 2022 года.

2.6.1.3 Контроль за обеспечением кибербезопасности в гражданской авиации. Курс разрабатывается в партнерстве с Управлением гражданской авиации Соединенного Королевства. Он охватывает ключевые аспекты, которые помогут государствам при установлении и выполнении своих обязательств по контролю за обеспечением авиационной кибербезопасности.

2.7 Повышение уровня осведомленности и информационно-разъяснительной деятельности

2.7.1 Повышение уровня осведомленности государств и заинтересованных сторон относительно важности решения вопросов кибербезопасности в гражданской авиации является основным видом деятельности ИКАО. Организация продолжает прилагать значительные усилия к организации и/или участию в национальных, региональных и международных конференциях, совещаниях и вебинарах с тем, чтобы способствовать сотрудничеству всех заинтересованных сторон в области обеспечения кибербезопасности и киберустойчивости, а также внедрению Стратегии кибербезопасности в авиации и Плана действий по обеспечению авиационной кибербезопасности.

2.8 Проверка обязательств в сфере кибербезопасности в рамках (МНМ-УППАБ)

2.8.1 Цель механизма непрерывного мониторинга в рамках Универсальной программы проверок в сфере авиационной безопасности (МНМ-УППАБ) состоит в том, чтобы улучшить глобальную авиационную безопасность посредством проведения проверок и непрерывного мониторинга показателей авиационной безопасности государств-членов. Проверяющие определяют документацию, требующую от эксплуатантов или предприятий указать свои критически важные системы информационно-коммуникационных технологий и данные, используемые в целях гражданской авиации. Они также гарантируют охват таким требованием вопросов оценки, разработки и внедрения мер по защите такой информации и систем от незаконного вмешательства. При наличии такого требования проверяющие обеспечивают четкое распределение обязанностей, касающихся мер обеспечения кибербезопасности.

2.8.2 Из 136 государств, проверенных по состоянию на 31 декабря 2021 года, в 54 государствах были проверены связанные с документацией аспекты готовности в области кибербезопасности. Результаты проверок, проведенных в этих государствах, свидетельствуют о следующем:

a) пятнадцать процентов государств не установили требований к эксплуатантам или организациям указать свои критически важные системы информационных и связных технологий и данные, используемые для целей гражданской авиации, и в соответствии с результатами оценки факторов риска разрабатывать и внедрять, по мере необходимости, меры их защиты от незаконного вмешательства;

b) двадцать шесть процентов государств не определили обязанности эксплуатантов или организаций в отношении кибербезопасности в гражданской авиации;

c) сорок один процент государств не разработали критерии защиты от незаконного вмешательства критически важных систем информационных и связных технологий и данных, используемых для целей гражданской авиации.

2.8.3 Эти результаты не обязательно являются показателем глобальной картины обеспечения защиты авиации от киберугроз, поскольку в некоторых государствах проверки проводились удаленно по причине пандемии, и результаты таких проверок не являются полными. Кроме того, общий размер выборки недостаточно представительный, чтобы обеспечить высокую степень достоверности. Однако эти результаты четко показывают, что сектор гражданской авиации должен активизировать свои усилия по решению проблемы киберугроз на таком уровне, который предусматривает последовательную и согласованную защиту от них, снижение остроты киберугроз для гражданской авиации и реакцию на них.

— — — — — — — — —

ДОБАВЛЕНИЕ

ПРОЕКТ РЕЗОЛЮЦИИ АССАМБЛЕИ
"РЕШЕНИЕ ПРОБЛЕМ КИБЕРБЕЗОПАСНОСТИ В ГРАЖДАНСКОЙ АВИАЦИИ"

~~A40-10~~ A41-xx: Решение проблем кибербезопасности в гражданской авиации

Ассамблея,

принимая во внимание, что глобальная система авиации представляет собой чрезвычайно сложную и интегрированную систему, включающую в себя ~~информационные и связные технологии, а также системы эксплуатационных технологий, некоторые из которых~~ ~~имеющие~~ системы, которые имеют критически важное значение для безопасности полетов и безопасности гражданской авиации,

принимая к сведению, что авиационная отрасль все больше зависит от наличия, целостности и конфиденциальности~~, целостности и наличия~~ информации, данных и систем ~~систем информационных и связных технологий~~, ~~а также от целостности и конфиденциальности данных~~,

учитывая, что ~~представляемая~~ ~~киберинцидентами угроза~~ киберугрозы для гражданской авиации быстро и постоянно изменяются, что ~~носители такой угрозы вынашивают преступные намерения, ставят целью по политическим, финансовым или другим мотивам нарушение деловой активности и кражу информации~~, авиация по-прежнему представляет собой ~~привлекательную~~ цель для правонарушителей как в киберпространстве, так и в физическом пространстве, а также то, что масштаб такой киберугрозы может ~~легко~~ достичь уровня, на котором может быть нанесен вред критически важным системам гражданской авиации во всем мире,

признавая, что не все ~~проблемы~~ события в области кибербезопасности, имеющие негативное воздействие на безопасность полетов гражданской авиации, носят противоправный и/или злонамеренный характер~~, а потому должны решаться путем применения систем управления безопасностью полетов~~,

признавая многогранность и комплексный характер вызовов и решений в области кибербезопасности и отмечая способность киберрисковатак одновременно воздействовать на широкий круг авиационных областей и быстро распространяться,

подтверждая обязательства по обеспечению безопасности полетов, авиационной безопасности и непрерывности деятельности гражданской авиации, предусмотренные *Конвенцией о международной гражданской авиации* (Чикагской конвенцией),

учитывая, что *Конвенция о борьбе с незаконными актами в отношении международной гражданской авиации* (Пекинская конвенция) и *Протокол, дополняющий Конвенцию о борьбе с незаконным захватом воздушных судов* (Пекинский протокол), укрепят глобальные международные правовые рамки в целях борьбы с кибератаками на международную гражданскую авиацию как с преступлениями, и, следовательно, широкая ратификация государствами этих документов обеспечит предотвращение таких нападений и наказание за них в любой точке мира,

подтверждая важность и безотлагательность ~~защиты~~ решения проблем кибербезопасности и киберустойчивости критически важных систем ~~инфраструктуры~~ гражданской авиации и ее данных и информации от киберугроз и опасностей, в том числе в контексте гражданской и военной авиации,

рассматривая необходимость совместной работы по созданию ~~для заинтересованных сторон в области гражданской авиации~~ эффективной и координированной глобальной ~~программы по~~ основы для решения проблем кибербезопасности в авиации ~~наряду с краткосрочными мероприятиями по повышению~~ и поддержки кибербезопасности и киберустойчивости глобальной системы авиации к киберугрозам, которые могут подрывать основы безопасности полетов и/или авиационной безопасности гражданской авиации,

признавая ~~работу Исследовательской группы Секретариата~~ руководящую роль и деятельность ИКАО в области авиационной кибербезопасности~~, которая внесла~~ и киберустойчивости, ~~и ее~~ вносящих значительный вклад в комплексный ~~формат стратегии кибербезопасности, объединив связанные с кибербезопасностью характеристики безопасности полетов и авиационной безопасности,~~ подход к этому вопросу в рамках различных авиационных дисциплин,

признавая, что авиационная кибербезопасность должна быть согласована на глобальном, региональном и национальном уровнях в целях ~~содействия глобальной упорядоченности и~~ обеспечения последовательности и полной функциональной совместимости мер защиты и систем управления факторами риска,

признавая важность разработки четких национальных процессов управления и подотчетности в отношении кибербезопасности гражданской авиации, включая назначение компетентного национального органа, отвечающего за авиационную кибербезопасность и действующего в координации с соответствующими национальными органами и учреждениями,

признавая значение соответствующих инициатив, планов действий, публикаций и других средств решения проблем кибербезопасности на основе сотрудничества и ~~согласованных действий и~~ целостного подхода,~~;~~

1. *настоятельно призывает* государства-члены ~~и ИКАО способствовать всеобщему принятию и претворению в жизнь~~ принять и ратифицировать *Конвенци~~и~~ю о борьбе с незаконными актами в отношении международной гражданской авиации* (Пекинская конвенция) и *Протокол~~а~~, дополняющ~~его~~ий Конвенцию о борьбе с незаконным захватом воздушных судов* (Пекинский протокол) как способ~~а~~ противостоять кибератакам на гражданскую авиацию;

2. *призывает* государства и заинтересованные стороны отрасли предпринять следующие меры по ~~противодействию~~ решению проблемы киберугроз~~ам~~ в сфере гражданской авиации:

   a) осуществлять стратегию авиационной кибербезопасности ИКАО и использовать план действий ИКАО по обеспечению кибербезопасности в качестве инструмента поддержки процесса реализации стратегии кибербезопасности в авиации;

   b) назначить компетентный полномочный орган по кибербезопасности в авиации и определить порядок взаимодействия между таким органом и соответствующими национальными учреждениями;

   ~~c) определить создаваемые возможными киберинцидентами угрозы и факторы риска для полетов и критически важных систем гражданской авиации, а также серьезные последствия, к которым могут привести такие инциденты~~;

   c) определить круг обязанностей национальных органов и заинтересованных сторон отрасли применительно к кибербезопасности в гражданской авиации;

d) подготовить и внедрить надёжную систему управления факторами риска кибербезопасности, основанную на соответствующей практике управления факторами риска для безопасности полетов и авиационной безопасности, и принять основанный на оценке рисков подход к защите от киберугроз критически важных систем, информации и данных гражданской авиации;

~~j~~e) разработать принципы и инструменты и~~, при необходимости,~~ выделять ресурсы для обеспечения следующих требований к критически важным авиационным системам: должна быть обеспечена структурная безопасность систем; системы должны быть устойчивыми; ~~способы передачи данных~~ данные должны быть защищенными и доступными при хранении и в процессе передачи~~безопасными, обеспечивающими целостность и конфиденциальность данных~~; должны быть внедрены методы мониторинга систем и выявления инцидентов и представления сообщений о них; должны быть разработаны и использоваться планы действий по восстановлению после инцидентов; необходимо проводить судебно-криминалистический анализ киберинцидентов;

~~d) поощрять выработку общего понимания государствами-членами киберугроз и факторов риска, а также общих критериев для определения степени важности объектов и систем, требующих защиты~~;

~~e~~f) поощрять координацию действий между государственными органами и отраслью при выработке стратегии, политики и планов обеспечения кибербезопасности, а также при обмене информацией, необходимой для выявления наиболее уязвимых мест, которые требуется устранить;

g) поощрять сотрудничество гражданских/военных органов в целях определения, защиты и мониторинга общих уязвимых мест и потоков данных в процессе взаимосвязи гражданских и военных авиационных систем и сотрудничать в деле реагирования на общие киберугрозы и восстановления после киберинцидентов;

~~f~~h) создавать государственно-отраслевые партнерства и механизмы на национальном и международном уровнях и участвовать в их деятельности по систематическому обмену информацией в области киберугроз, инцидентов, тенденций и мер противодействия;

~~g) основываясь на общем понимании киберугроз и факторов риска, использовать гибкий, основанный на оценке факторов риска подход к защите критически важных авиационных систем путем внедрения систем управления кибербезопасностью;~~

~~h~~i) ~~поощрять развитие в национальных органах~~ создавать и внедрять ~~и~~ в ~~авиационной~~ отрасли гражданской авиации жизнестойк~~ой~~ую культур~~ы~~у кибербезопасности ~~на всех уровня~~х;

j) рекомендовать государствам продолжать вносить вклад в деятельность ИКАО по разработке международных стандартов, стратегий и передовой практики для содействия повышению уровня авиационной кибербезопасности и киберустойчивости;

i) ~~способствовать разработке и внедрению международных стандартов, стратегий и передовой практики в сфере защиты применяемых для целей гражданской авиации критически важных систем информации и связи от актов вмешательства, которые могут угрожать безопасности полетов гражданской авиации~~;

k) продолжать сотрудничать в разработке программы ИКАО в сфере кибербезопасности согласно единому, комплексному и функциональному подходу, включающему области безопасности полетов, авиационной безопасности, упрощения формальностей, аэронавигации, связи, наблюдения, организации воздушного движения, эксплуатации воздушных судов, ~~и~~ летной годности и другие соответствующие дисциплины;

3. *поручает* ИКАО:

a) продолжать пропагандировать всеобщее принятие и ратификацию Конвенции о борьбе с незаконными актами в отношении международной гражданской авиации (Пекинская конвенция) и Протокола, дополняющего Конвенцию о борьбе с незаконным захватом воздушных судов (Пекинский протокол);

~~а) разработать план действий для оказания государствам и отрасли поддержки в принятии стратегии кибербезопасности~~;

b) продолжать обеспечивать междисциплинарный подход к рассмотрению и координации вопросов кибербезопасности и киберустойчивости с помощью ~~соответствующих~~ нового механизма~~ов в духе стратегии~~ ИКАО для решения проблемы авиационной кибербезопасности.

— КОНЕЦ —