



РАБОЧИЙ ДОКУМЕНТ

АССАМБЛЕЯ – 42-Я СЕССИЯ

ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ

Пункт 13 повестки дня. **Авиационная безопасность. Политика**

КИБЕРБЕЗОПАСНОСТЬ В ГРАЖДАНСКОЙ АВИАЦИИ

(Представлено Советом ИКАО)

КРАТКАЯ СПРАВКА

Информированность и активность сектора гражданской авиации в деле устранения киберугроз и рисков для гражданской авиации постоянно повышаются. За прошедший трехлетний период в ИКАО, а также в государствах на национальном, региональном и глобальном уровнях произошло множество изменений. Однако необходимо проделать еще больше работы, особенно на национальном уровне, чтобы обеспечить целостный, согласованный и последовательный подход к обеспечению авиационной кибербезопасности во всем секторе гражданской авиации.

В данном документе представлен обзор действий по обеспечению авиационной кибербезопасности, в том числе санкционированных Ассамблеей, и содержится предложение обновить резолюцию A41-19 *"Решение проблем кибербезопасности в гражданской авиации"*, чтобы подчеркнуть важность повышения защищенности и устойчивости сектора гражданской авиации в условиях киберугроз и рисков, принимая во внимание наработки ИКАО по этой теме.

Действия: Ассамблее предлагается:

- а) принять к сведению информацию об изменениях в области обеспечения кибербезопасности в авиации;
- б) принять резолюцию Ассамблеи *"Решение проблем кибербезопасности в гражданской авиации"*, представленную в добавлении.

Стратегические цели	Данный рабочий документ связан со стратегическими целями <i>"Каждый полет безопасен и защищен"</i> и <i>"Авиация обеспечивает беспрепятственную, доступную и надежную мобильность для всех"</i>
Финансовые последствия	Указанная в настоящем рабочем документе деятельность будет осуществляться при наличии ресурсов в бюджете Регулярной программы на 2026–2028 гг. и/или за счет внебюджетных взносов, в соответствии с бизнес-планом на 2026–2028 гг.
Справочный материал	Дос 10184 <i>"Действующие резолюции Ассамблеи (по состоянию на 7 октября 2022 года)"</i> <i>Стратегия в области авиационной кибербезопасности</i> <i>План действий по обеспечению кибербезопасности</i>

1. ВВЕДЕНИЕ

1.1 В секторе гражданской авиации наблюдается стремительная эволюция в использовании информационных и новых технологий для удовлетворения потребностей в автоматизации, взаимосвязанности и интероперабельности, а также для внедрения новых эксплуатационных концепций на земле и в воздухе и интеграции новых участников, таких как беспилотные авиационные системы (БАС), в систему воздушного транспорта. Конечной целью этих разработок является поддержка роста сектора гражданской авиации при обеспечении его безопасности, надежности, эффективности, пропускной способности и устойчивости.

1.2 Однако эта тенденция привела к росту киберугроз для операционных систем, данных и информации. Этот рост еще более усугубляется геополитической напряженностью, наблюдаемой во всем мире. Несмотря на отсутствие сообщений о кибератаках, оказавших существенное влияние на безопасность полетов или авиационную безопасность, в секторе наблюдается тенденция к увеличению числа сообщений о киберинцидентах, которые, как представляется на сегодняшний день, в основном мотивированы финансовой выгодой, хищением информации или хактивизмом¹.

1.3 Усложнение характера киберугроз и их потенциального воздействия на гражданскую авиацию свидетельствует о необходимости выработки глобального, надежного и согласованного подхода к повышению уровня защиты и устойчивости гражданской авиации к киберугрозам. В этой связи ИКАО продолжает сотрудничать с государствами-членами, международными организациями и отраслью, оказывая им поддержку в снижении киберрисков для сектора гражданской авиации

1.4 На своей 41-й сессии Ассамблея ИКАО с удовлетворением отметила работу, проделанную ИКАО в области авиационной кибербезопасности в течение прошедшего трехлетнего периода (2019–2022 гг.), и выразила признательность ИКАО и ее группам экспертов за их работу. В частности, Ассамблея приветствовала принятие и внедрение в ИКАО усовершенствованной структуры внутреннего управления в области авиационной кибербезопасности, а также непрерывную разработку политики, положений, инструктивных материалов и мер по укреплению потенциала и инициатив по повышению осведомленности в области авиационной кибербезопасности. Кроме того, на 41-й сессии Ассамблеи ИКАО была принята резолюция A41-19 Ассамблеи *"Решение проблем кибербезопасности в гражданской авиации"*, которая заменила собой резолюцию A40-10 Ассамблеи.

2. РАССМОТРЕНИЕ ВОПРОСА

2.1 Стандарты и Рекомендуемая практика по авиационной кибербезопасности

2.1.1 В соответствии с пунктом действий ПДоК 3.4 Плана действий по обеспечению кибербезопасности (ПДоК), в котором ИКАО предлагается "рассмотреть существующие Стандарты и Рекомендуемую практику (SARPS) ИКАО для определения необходимости их обновления на предмет кибербезопасности", в 2022 году ИКАО провела углубленный индивидуальный анализ 16 Приложений к *Конвенции о международной гражданской авиации* (Чикагская конвенция) в целях выявления в SARPS ИКАО потенциальных областей, представляющих интерес с точки зрения авиационной кибербезопасности, в поддержку всеобъемлющего междисциплинарного подхода к обеспечению авиационной кибербезопасности в соответствии с положениями ИКАО.

2.1.2 Результаты анализа были переданы Группе экспертов по кибербезопасности, которая учредила Целевую группу по Стандартам и Рекомендуемой практике в области кибербезопасности (TF-CYSARPS) для продолжения работы путем проведения перекрестного анализа потенциальных

¹ Дополнительную информацию о киберугрозах и рисках для сектора гражданской авиации можно найти в документе ИКАО "Глобальные соображения по киберрискам" (*Doc 10213 – Restricted*)

областей, представляющих интерес с точки зрения авиационных дисциплин, как это отражено в соответствующих Приложениях. Работа Целевой группы направлена на изучение того, насколько адекватно вопросы авиационной кибербезопасности охватываются существующими SARPS (как прямо, так и косвенно), на выявление потенциальных пробелов в системе SARPS ИКАО и координацию с соответствующими экспертными группами для устранения этих пробелов в случае необходимости. Работа по этому вопросу по-прежнему идет и, как ожидается, будет продолжена в течение предстоящего трехлетнего периода.

2.2 Международно-правовые документы

2.2.1 В исследовании о применимости инструментов международного воздушного права к киберугрозам против гражданской авиации, представленном на 38-й сессии Юридического комитета, сделан вывод о том, что *Конвенция о борьбе с незаконными актами, связанными с международной гражданской авиацией*² (Пекин, 2010 г., Пекинская конвенция 2010 года) и *Протокол, дополняющий Конвенцию о борьбе с незаконным захватом воздушных судов*³ (Пекин, 2010 г., Пекинский протокол 2010 года), содержат в себе важные усовершенствования по сравнению с более старыми документами, что служит достаточным основанием для того, чтобы государства могли рассматривать кибератаки на гражданскую авиацию как преступления.

2.2.2 По состоянию на 1 апреля 2024 года Пекинскую конвенцию 2010 года ратифицировали 53 государства-члена, а Пекинский протокол 2010 года – 54 государства-члена. Учитывая, что эти документы содержат положения, имеющие отношение к борьбе с кибератаками на гражданскую авиацию, настоятельно рекомендуется широкое принятие и ратификация этих документов государствами-членами, что подчеркивается в резолюциях Ассамблеи по решению проблем кибербезопасности в гражданской авиации, чтобы обеспечить сдерживание киберугроз для гражданской авиации и преследование за совершение кибератак на этот сектор.

2.3 Второе издание Глобального плана обеспечения авиационной безопасности (ГПАБ)

2.3.1 В соответствии с пунктом действий ПДоК 2.5 Плана действий по обеспечению кибербезопасности, в котором ИКАО предлагается "включить вопросы кибербезопасности в региональные и глобальные планы в целях обеспечения безопасности полетов, авиационной безопасности и устойчивости авиации", и в связи с обновлением ГПАБ, второе издание которого было опубликовано в июне 2024 года (<https://www.icao.int/Security/Pages/Global-Aviation-Security-Plan.aspx>), ИКАО включила вопросы авиационной кибербезопасности в положения Плана в рамках Глобальных приоритетов 1, 2 и 4.

2.4 Инструктивный материал

2.4.1 В соответствии с Планом действий по обеспечению кибербезопасности ИКАО разработала инструктивный материал⁴ с целью оказать поддержку государствам и заинтересованным сторонам при решении проблем кибербезопасности в гражданской авиации, в том числе по управлению и политике в области авиационной кибербезопасности на государственном уровне, культуре кибербезопасности в гражданской авиации и планированию и осуществлению обмена киберинформацией. ИКАО опубликовала также документ *"Глобальный обзор рисков в области кибербезопасности"* (*Doc 10213 – Restricted*) – руководство, в котором представлена методика управления рисками в области кибербезопасности в рамках управления рисками, связанными с безопасностью полетов и авиационной безопасностью, эффективностью и пропускной способностью аэронавигации, а также обзор глобальных киберугроз и рисков высокого уровня:

² [Конвенция о борьбе с незаконными актами в отношении международной гражданской авиации](#)

³ [Протокол, дополняющий Конвенцию о борьбе с незаконным захватом воздушных судов](#)

⁴ <https://www.icao.int/aviationcybersecurity/Pages/Guidance-material.aspx>

2.4.2 В соответствии с рекомендацией 4.2/1 14-й Аэронавигационной конференции относительно авиационной кибербезопасности, в настоящее время работа над инструктивным материалом включает разработку комплексного набора руководств, посвященных различным аспектам авиационной кибербезопасности. Сюда также относится план по объединению всех инструктивных материалов в *Руководство по авиационной кибербезопасности*, охватывающее все аспекты, связанные с защитой и обеспечением устойчивости критически важной авиационной инфраструктуры и служб в условиях киберугроз и рисков.

2.5 Механизмы доверия

2.5.1 На своей 220-й сессии, прошедшей в июне 2022 года, Аэронавигационная комиссия одобрила создание Группы экспертов по механизму доверия (TFP). С этого момента TFP поддерживает разработку инструктивного материала для создания следующих совместимых механизмов доверия:

- a) подготовленное техническое руководство по совместимым механизмам обеспечения доверия и предоставления идентификационной информации в условиях эксплуатации, включая руководство по информационной безопасности (Doc 10204 "*Руководство по авиационной информационной безопасности*");
- b) политика общих авиационных сертификатов для поддержки совместимых цифровых идентификаторов, аутентичности и достоверности информации в гражданской авиации, включая, в частности, поддержку аутентификации спутниковых систем функционального дополнения (SBAS) для глобальных навигационных спутниковых систем (GNSS);
- c) разработанный и обновляемый список примеров целесообразного использования механизмов доверия в условиях эксплуатации. Недавно началась разработка руководства, призванного помочь заинтересованным авиационным сторонам в создании правил для использования механизмов доверия;
- d) в тесной координации между соответствующими экспертными группами завершается подготовка инструктивного материала по защищенной воздушной/наземной связи с помощью сети авиационной электросвязи в рамках пакета протоколов Интернета (ATN/IPS) для непосредственной поддержки поправки 93 к тому III "Системы связи" Приложения 10 "Авиационная электросвязь".

2.6 Программа работы ИКАО в области обеспечения авиационной кибербезопасности

2.6.1 Совет на своей 228-й сессии в 2023 году утвердил создание, членский состав и круг полномочий АНССС после определения ресурсов Секретариата, достаточных для обеспечения функционирования АНССС. В состав АНССС входят по одному члену от Авиатранспортного комитета, Комитета по авиационной безопасности (ASC) и Аэронавигационной комиссии и 11 членов от каждой экспертной группы, на постоянной основе занимающейся вопросами кибербезопасности в рамках своей программы работы.

2.6.2 Основные функции Комитета заключаются в координации всей работы ИКАО по вопросам авиационной кибербезопасности путем разработки и поддержания актуальности всеобъемлющей Программы работы ИКАО в области обеспечения авиационной кибербезопасности. Он также служит главным консультативным органом Совета по определению приоритетности элементов работы в соответствии с Программой работы.

2.6.3 С момента своего создания АНССС провел три совещания и продолжает совершенствовать Программу работы ИКАО в области обеспечения авиационной кибербезопасности по мере продвижения работы в области кибербезопасности, выступая в качестве платформы для сотрудничества экспертных групп в целях обмена информацией и поддержания согласованного и последовательного подхода к обеспечению авиационной кибербезопасности в рамках их соответствующих областей работы.

2.7 Подготовка специалистов и наращивание потенциала

2.7.1 На сегодняшний день комплект учебных программ ИКАО по кибербезопасности включает два курса по обеспечению авиационной кибербезопасности:

- а) Основные принципы руководства и технического управления в области авиационной кибербезопасности. Курс был разработан ИКАО в партнерстве 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 в области авиационной кибербезопасности. В предыдущем трехлетнем периоде, с сентября 2022 года по апрель 2025 года, этот курс прошли 88 участников;
- б) Контроль за обеспечением кибербезопасности в гражданской авиации. Курс был разработан ИКАО в партнерстве с ведомством гражданской авиации Соединенного Королевства и впервые проведен в марте 2023 года. В нем рассматриваются ключевые аспекты, которые могут помочь государствам в разработке и внедрении системы контроля за обеспечением авиационной кибербезопасности на примере опыта Соединенного Королевства. В предыдущем трехлетнем периоде, с марта 2023 года по апрель 2025 года, этот курс прошли 34 участника.

2.8 Повышение уровня осведомленности и информационно-разъяснительная деятельности

2.8.1 В соответствии с призывами 41-й сессии Ассамблеи к ИКАО активизировать свои кампании по повышению осведомленности и проводить теоретические учения по авиационной кибербезопасности, Организация использовала добровольные взносы Португалии и Сингапура на реализацию программы по обеспечению авиационной кибербезопасности, что позволило в течение трехлетнего периода разработать и провести серию из пяти региональных семинаров по обеспечению авиационной кибербезопасности.

2.8.2 В семинарах приняли участие представители всех авиационных и соответствующих неавиационных специальностей (безопасность полетов, авиационная безопасность, аэронавигация, кибербезопасность, национальные CERT/CSIRT, национальные органы по обеспечению кибербезопасности, правоохранительные органы, военные и т. д.). В общей сложности семинары посетили более 450 участников.

2.8.3 Помимо теоретических учений (ТТХ), проводимых в рамках региональных семинаров по обеспечению авиационной кибербезопасности, ИКАО провела ТТХ на полях четвертого совещания Группы экспертов по кибербезопасности (CYSECP/4) 5 июня 2025 года, в ходе Недели авиационной безопасности в 2023 году, а также четыре отдельных ТТХ, в результате чего общее число международных ТТХ, проведенных ИКАО в течение трехлетнего периода, достигло десяти учений по обеспечению авиационной кибербезопасности.

3. Пересмотр резолюции A41-19 Ассамблеи

3.1 С учетом принятия Маскатской декларации и итогов 14-й Аэронавигационной конференции в прилагаемом добавлении приводятся предлагаемые обновления резолюции A41-19 Ассамблеи. Обновленная резолюция была согласована с Группой экспертов ИКАО по кибербезопасности для обеспечения ее соответствия содержанию Декларации и итогам Конференции, касающимся авиационной кибербезопасности, а также приведена к единообразию с определениями терминов по авиационной кибербезопасности, одобренными на третьем совещании Группы экспертов по кибербезопасности, и с наработками ИКАО по этому вопросу.

— — — — —

ДОБАВЛЕНИЕ

Резолюция A41-19 A42-XX "Решение проблем кибербезопасности в гражданской авиации"

Ассамблея,

принимая во внимание, что глобальная система авиации представляет собой чрезвычайно сложную и интегрированную взаимосвязанную систему, включающую в себя данные, информацию и системы, которые имеют критически важное значение для безопасности полетов и, авиационной безопасности, эффективности и потенциала гражданской авиации,

принимая к сведению, что авиационная отрасль все больше зависит от наличия и целостности и конфиденциальности данных, информации, данных и систем, а в определенных обстоятельствах и от их конфиденциальности,

признавая, что авиационная кибербезопасность имеет решающее значение для устойчивого и эффективного развития воздушного транспорта, в связи с чем ей необходимо уделять первоочередное внимание и выделять на ее обеспечение надлежащие ресурсы,

учитывая, что киберугрозы для гражданской авиации быстро и постоянно изменяются и становятся все более масштабными, сложными и частыми, что авиация по-прежнему представляет собой цель для злоумышленников правонарушителей как в киберпространстве, так и в физическом пространстве, а также то, что масштаб киберугрозы может достичь уровня, на котором может быть нанесен вред критически важным системам могут представлять значительный риск для критической инфраструктуры гражданской авиации, что может поставить под угрозу безопасность полетов, авиационную безопасность, эффективность или потенциал гражданской авиации во всем мире,

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

признавая, что не все события в области кибербезопасности киберинциденты, имеющие негативное воздействие на безопасность полетов, авиационную безопасность, эффективность или потенциал гражданской авиации, носят противоправный и/или злонамеренный характер по отношению к гражданской авиации,

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 введения уголовной ответственности за совершение борьбы с кибератаками на международную гражданскую авиацию как с преступлениями, и, следовательно, широкая ратификация и внедрение государствами-членами этих документов обеспечит повсеместное предотвращение таких нападений и наказание за них в любой точке мира,

подтверждая важность и безотлагательность ~~решения проблем~~ повышения кибербезопасности защищенности и киберустойчивости критически важных данных, информации и систем гражданской авиации ~~и ее данных и информации~~ от киберугроз и рисков ~~опасностей~~, в том числе в контексте гражданской ~~и военной~~ авиации и других связанных с ней секторов;

рассматривая необходимость совместной работы по созданию эффективной и координированной глобальной основы ~~для решения проблем~~ по кибербезопасности в авиации ~~и поддержки кибербезопасности и киберустойчивости глобальной системы авиации~~ в целях согласованного и непрерывного обеспечения защиты и устойчивости этого сектора к киберугрозам и рискам, ~~которые могут подрывать основы безопасности полетов и/или авиационной безопасности гражданской авиации,~~

признавая руководящую роль и деятельность ИКАО в области авиационной кибербезопасности ~~и киберустойчивости~~, вносящих значительный вклад в комплексный подход к этому вопросу в рамках различных авиационных дисциплин,

признавая, что авиационная кибербезопасность должна быть согласована на глобальном, региональном и национальном уровнях ~~в целях~~ *поддержку* обеспечения последовательности и ~~полной~~ функциональной совместимости мер защиты и *сохранения* устойчивости и соответствующих процессов ~~систем управления факторами риска,~~

признавая важность разработки и внедрения государствами четких *комплексных планов* обеспечения авиационной кибербезопасности, ~~национальных процессов управления и подотчетности~~ определяющих законодательство, правила, политику, процедуры и меры 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 *положений, инструктивного материала и инициатив;* ~~планов действий, публикаций и других средств~~ для решения проблем кибербезопасности на основе сотрудничества и целостного подхода,

принимая во внимание итоги 14-й Аэронавигационной конференции, прошедшей в Монреале 26 августа – 6 сентября 2024 года, а также положения Маскатской декларации по авиационной безопасности и авиационной кибербезопасности, которая была принята в Маскате (Оман) 11 декабря 2024 года,

1. *настоятельно призывает* государства-члены принять, ~~и~~ ратифицировать и *выполнять* Конвенцию о борьбе с незаконными актами в отношении международной гражданской авиации (Пекинская конвенция) 2010 года и Протокол, дополняющий Конвенцию о борьбе с незаконным захватом воздушных судов (Пекинский протокол) 2010 года, как способ противостоять кибератакам на гражданскую авиацию;
2. *призывает* государства и заинтересованные стороны отрасли предпринять следующие меры по решению проблемы киберугроз в сфере гражданской авиации:
 - a) осуществлять стратегию авиационной кибербезопасности ИКАО и использовать план действий ИКАО по обеспечению кибербезопасности в качестве инструмента поддержки процесса ~~ее реализации стратегии кибербезопасности в авиации;~~
 - b) разработать и внедрить национальные планы обеспечения авиационной кибербезопасности, которые касаются стратегических целей по обеспечению авиационной кибербезопасности,

управления и ответственности, политики, коммуникаций, управления киберрисками, реагирования на инциденты и восстановления, наращивания потенциала и подготовки кадров, соблюдения нормативных требований и проверок, наблюдения и постоянного совершенствования, документации и ведения учета, в целях устранения киберугроз и рисков для гражданской авиации на основе целостного подхода, охватывающего все сферы авиации;

- c) разработать и внедрить процессы и механизмы в поддержку реализации планов по обеспечению авиационной кибербезопасности и контроля за их выполнением;
- d) ~~б)~~ в рамках национального плана по обеспечению авиационной кибербезопасности назначить компетентный полномочный орган по кибербезопасности в авиации и определить порядок взаимодействия между таким органом и соответствующими национальными учреждениями из авиационной отрасли и за ее пределами;
- e) ~~е)~~ определить круг обязанностей национальных органов и заинтересованных сторон отрасли применительно к кибербезопасности в гражданской авиации;
- f) привлечь достаточные ресурсы для обеспечения наличия и постоянной подготовки квалифицированных и компетентных специалистов в области авиации и кибербезопасности в целях регулирования, налаживания, администрирования, поддержания и мониторинга эффективного выполнения соответствующих законов, положений, политики, процедур и мер в области авиационной кибербезопасности;
- g) ~~д)~~ подготовить и внедрить надежную систему управления факторами риска в области кибербезопасности, ~~основанную на~~ которая включает процесс управления такими факторами риска в соответствующую практику управления факторами риска для безопасности полетов, ~~и~~ авиационной безопасности, эффективности и потенциала, и принять основанный на оценке рисков подход к ~~защите~~ повышению защищенности и устойчивости ~~от~~ в условиях киберугроз и рисков критически важных данных, информации и систем, ~~информации и данных~~ гражданской авиации;
- h) ~~е)~~ разработать соответствующие законы, нормы, принципы, процедуры и меры ~~и инструменты~~ и выделять достаточные ресурсы для обеспечения следующих требований к критически важным авиационным системам: должна быть обеспечена структурная безопасность систем; системы должны быть устойчивыми; данные должны быть защищенными и доступными при хранении, использовании и в процессе передачи; должны быть внедрены методы мониторинга систем и выявления киберинцидентов и представления сообщений о них; должны быть разработаны и использоваться планы действий по реагированию и восстановлению ~~но не~~ в случае киберинцидентов в координации с установленными планами реагирования на чрезвычайные ситуации и управления кризисными ситуациями; необходимо проводить судебно-криминалистический анализ киберинцидентов;
- i) ~~создавать и внедрять в отрасли гражданской авиации жизнестойкую~~ разработать и внедрить практические меры по развитию культуры кибербезопасности во всех учреждениях гражданской авиации;

~~ф) 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;~~

- j) ~~h)~~ создавать межгосударственные и государственно-отраслевые партнерства и механизмы на национальном и международном уровнях и участвовать в их деятельности по систематическому обмену информацией в области киберугроз, инцидентов, факторов уязвимости, показателей компрометации, тенденций, ~~и мер~~ противодействия, передовой практики и полученного опыта;
- k) ~~g)~~ ~~поощрять~~ разработать механизмы сотрудничества гражданских/военных с соответствующими национальными органами, включая в том числе военные, правоохранительные органы и органы по обеспечению кибербезопасности, в целях определения, защиты и мониторинга общих уязвимых мест и потоков данных информации в процессе взаимодействия гражданских и военных авиационных, которые могут повлиять на системы гражданской авиации и сотрудничать в деле реагирования на предотвращения общих киберугроз и обеспечения готовности к ним, а также реагирования и восстановления ~~ноеле~~ в случае киберинцидентов;
- ~~a)~~ рекомендовать государствам продолжать вносить вклад в деятельность ИКАО по разработке международных стандартов, стратегий и передовой практики для содействия повышению уровня авиационной кибербезопасности и киберустойчивости;
- l) ~~k)~~ продолжать сотрудничать и вносить вклад в отношении разработки программы ИКАО в сфере авиационной кибербезопасности согласно единому, комплексному и функциональному подходу, включающему области безопасности полетов, авиационной безопасности, упрощения формальностей, аэронавигации, связи, наблюдения, организации воздушного движения, эксплуатации воздушных судов, летной годности и другие все соответствующие авиационные дисциплины в целях комплексного устранения киберугроз и рисков для безопасности полетов, авиационной безопасности, эффективности и потенциала.

3. поручает ИКАО:

- a) продолжать пропагандировать всеобщее принятие и ратификацию *Конвенции о борьбе с незаконными актами в отношении международной гражданской авиации* (Пекинская конвенция) 2010 года и *Протокола, дополняющего Конвенцию о борьбе с незаконным захватом воздушных судов* (Пекинский протокол) 2010 года;
- b) продолжать обеспечивать междисциплинарный комплексный подход к рассмотрению и координации вопросов авиационной кибербезопасности ~~и киберустойчивости~~ ~~е помощью нового механизма ИКАО для решения проблемы авиационной кибербезопасности~~ путем сотрудничества между всеми соответствующими органами ИКАО.

— КОНЕЦ —