Международная организация гражданской авиации

A40-WP/28
EX/13
25/6/19

РАБОЧИЙ ДОКУМЕНТ

АССАМБЛЕЯ — 40-Я СЕССИЯ

ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ

Пункт 12 повестки дня. Авиационная безопасность. Политика

СТРАТЕГИЯ ИКАО В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

(Представлено Советом ИКАО)

КРАТКАЯ СПРАВКА

В данном документе представлена комплексная стратегия в области кибербезопасности, и, с тем чтобы подчеркнуть ее срочный характер и важность, в него включена измененная резолюция A39-19 Ассамблеи *"Решение проблем кибербезопасности в гражданской авиации"*, поддерживающая ее реализацию государствами-членами. Эта стратегия основана на концептуальном видении ИКАО глобальной кибербезопасности, которое состоит в том, что авиационный сектор должен быть устойчив к кибератакам, сохраняя надежность и глобальное доверие к себе, продолжая при этом внедрять инновации и развиваться. Ее необходимо будет поддержать планом действий, который будет разработан в рамках надлежащих структур. Эта стратегия является результатом обсуждений в Исследовательской группе Секретариата по кибербезопасности.

Действия: Ассамблее предлагается:

a) принять предлагаемую резолюцию Ассамблеи, которая приводится в добавлении A, заменяющую резолюцию A39-19;

b) утвердить стратегию кибербезопасности, приведенную в добавлении B;

c) призвать государства ратифицировать *Конвенцию 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).

Стратегические цели	Данный рабочий документ связан со следующими стратегическими целями: *"Потенциал и эффективность", "Безопасность полетов", "Авиационная безопасность и упрощение формальностей"*
Финансовые последствия	Деятельность, упоминаемая в данном документе, будет осуществляться при наличии ресурсов в бюджете Регулярной программы на 2020–2022 гг. и/или за счет внебюджетных взносов.
Справочный материал	Doc 10075, *Действующие резолюции Ассамблеи* (по состоянию на 6 октября 2016 года)

1. ВВЕДЕНИЕ

1.1 39-я сессия Ассамблеи ИКАО вновь подтвердила важность и крайнюю необходимость защиты критически важных систем инфраструктуры гражданской авиации и данных от кибератак и получения глобальных обязательств со стороны ИКАО, ее государств-членов и заинтересованных сторон отрасли по проведению активных действий, направленных на совместное и системное решение проблем кибербезопасности в гражданской авиации и устранение соответствующих угроз и факторов риска. В резолюции A39-19 *"Решение проблем кибербезопасности в гражданской авиации"* были определены действия, которые должны предпринять государства и другие заинтересованные стороны в этой связи. 39-я сессия Ассамблеи ИКАО также поручила ИКАО подготовить всеобъемлющий рабочий план и структуру управления кибербезопасностью.

1.2 Для достижения этих целей ИКАО учредила Исследовательскую группу Секретариата по кибербезопасности (SSGC) под руководством заместителя директора по вопросам авиационной безопасности и упрощения формальностей (DD/ASF). Группа SSGC состоит из представителей 20 государств, 13 международных организаций и Секретариата ИКАО, а за ее деятельностью наблюдает Группа старших руководителей Секретариата по общим вопросам безопасности полетов и авиационной безопасности под председательством Генерального секретаря ИКАО.

1.3 После своего создания в августе 2017 года SSGC собиралась шесть раз и подготовила комплект рекомендаций, касающихся решения возникающей проблемы кибербезопасности в авиации. Основным результатом стала разработка комплексной стратегии в области кибербезопасности. Эта стратегия призвана направлять работу государств и ИКАО в целях обеспечения безопасности полетов, авиационной безопасности и непрерывности деятельности гражданской авиации посредством применения надежного механизма обеспечения кибербезопасности. Совет на своей 217-й сессии утвердил стратегию в области авиационной кибербезопасности в принципе и согласился представить измененную резолюцию A39-19 Ассамблеи *"Решение проблем кибербезопасности в гражданской авиации"* 40-й сессии Ассамблеи ИКАО.

2. РАССМОТРЕНИЕ ВОПРОСА

2.1 Стратегия в области авиационной кибербезопасности учитывает и дополняет другие инициативы ИКАО, связанные с кибербезопасностью. Стратегия согласована с существующими Стандартами и Рекомендуемой практикой (SARPS) по обеспечению безопасности полетов и авиационной безопасности, связанными с кибербезопасностью и защитой критически важной авиационной информации, в частности относящимися к Приложению 17 *"Безопасность"*.

2.2 В стратегии подчеркивается важность признания кибербезопасности общей проблемой, затрагивающей все сегменты авиационного сектора. Существующие положения, относящиеся к проблемам кибербезопасности и рассеянные по различным Приложениям, объединены в ней в единый механизм, ориентированный на управление факторами риска кибербезопасности и повышение уровня кибербезопасности в целом. Стратегия обеспечивает государства концептуальным видением сектора гражданской авиации как устойчивого к кибератакам, при этом продолжающего внедрять инновации и развиваться.

2.3 Стратегия нацелена на:

a) защиту гражданской авиации и пассажиров от угроз кибербезопасности, которые могут повлиять на безопасность полетов, авиационную безопасность системы воздушного транспорта и доверие к ней;

b) сохранение или повышение уровня безопасности полетов и авиационной безопасности в авиационной системе при сохранении непрерывности воздушных перевозок;

c) признание государствами своих обязательств в рамках *Конвенции о международной гражданской авиации* (Чикагской конвенции) по обеспечению безопасности полетов, авиационной безопасности и непрерывности деятельности гражданской авиации с учетом угроз кибербезопасности;

d) согласование мер по обеспечению кибербезопасности между государственными органами в целях обеспечения эффективного и результативного управления факторами риска кибербезопасности.

2.4 Цели стратегии будут достигаться посредством применения серии принципов, мер и действий, содержащихся в механизме, построенном на семи основополагающих элементах: 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.

2.5 Необходимым условием для реализации стратегии является формулирование и применение государствами-членами национального законодательства и нормативных положений в соответствии с положениями ИКАО. При этом следует определить целесообразность обновления или принятия нового национального законодательства для того, чтобы предусмотреть преследование в судебном порядке за киберугрозы, связанные с терроризмом, а также за совершение кибератак, имеющих негативные последствия для гражданской авиации. Процесс оценки и возможное обновление законодательства на государственном уровне могут задержать эффективное внедрение стратегии и создать проблему для согласованного обеспечения кибербезопасности на глобальном уровне.

2.6 Стратегия учитывает потребность в наращивании потенциала и популяризации культуры кибербезопасности. В этой связи государствам потребуется прошедший надлежащую подготовку персонал, обладающий широкими экспертными знаниями в области авиации и кибербезопасности. Для достижения этой цели могут потребоваться полностью новые или обновленные учебные планы, и необходимо будет учесть время и ресурсы для их подготовки.

2.7 Для обеспечения упорядоченного принятия и реализации мер, поддерживающих достижение целей стратегии, потребуется комплексный план действий. ИКАО в сотрудничестве с государствами и отраслью следует незамедлительно приступить к подготовке такого плана, используя соответствующие механизмы решения вопросов кибербезопасности.

2.8 Кибербезопасность представляет собой быстро изменяющуюся проблему, при решении которой необходимо учитывать ее срочный характер и важность. Следовательно, а также с тем чтобы подчеркнуть обязанности и обязательства государств и ИКАО по совместному

обеспечению кибербезопасности, в измененной резолюции Ассамблеи подчеркиваются достижения государств и ИКАО в решении вопросов в области кибербезопасности и необходимость принятия и осуществления стратегии в области кибербезопасности добавлением к существующей резолюции A39-19, которая была отправной точкой в работе ИКАО по обеспечению кибербезопасности.

2.9 Представленный в добавлении к настоящему рабочему документу проект резолюции Ассамблеи вносит еще один элемент в существующую резолюцию по кибербезопасности, подчеркивая необходимость глобального всеобщего принятия и осуществления *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) как способа противостоять кибератакам на гражданскую авиацию.

2.10 Далее в ней признается необходимость продолжения работы SSGC в более официальном ключе, что позволит осуществлять упорядоченную координацию деятельности с другими группами экспертов ИКАО.

3. **ВЫВОД**

3.1 В духе Чикагской конвенции глобальная стратегия ИКАО в области кибербезопасности обеспечит основу для дальнейшей работы, взаимоприемлемую для всех государств. Она будет способствовать синхронизации работы международных, региональных и национальных механизмов обеспечения кибербезопасности и поддерживать соответствующие механизмы обмена информацией, которые обеспечат дополнительные преимущества для управления факторами риска кибербезопасности.

3.2 Стратегия обеспечит создание гибкого механизма, подготавливая гражданскую авиацию к эффективному решению проблем кибербезопасности в предстоящие десятилетия. Стратегия имеет модульную структуру, что позволяет адаптировать ее к возникающим киберугрозам и учитывать любые будущие события в сфере гражданской авиации. Это гарантирует, что все сегменты авиационного сектора будут охвачены, а проблемы будут рассматриваться в широком комплексном ключе.

3.3 Стратегию в области кибербезопасности будет необходимо поддержать планом действий, включая конкретные шаги к созданию развитого механизма кибербезопасности. Этот план действий будет опираться на руководящие принципы реализации существующих SARPS, связанных с кибербезопасностью, но будет расширять и объединять их, с тем чтобы обеспечить всеобъемлющие руководящие принципы достижения высшего уровня кибербезопасности.

3.4 В стратегии учтены существующие глобальные планы и далее принята во внимание потребность в подготовленном и компетентном персонале с опытом работы в области авиации и кибербезопасности.

— — — — — — — — —

ДОБАВЛЕНИЕ А

ПРОЕКТ РЕЗОЛЮЦИИ АССАМБЛЕИ "РЕШЕНИЕ ПРОБЛЕМ КИБЕРБЕЗОПАСНОСТИ В ГРАЖДАНСКОЙ АВИАЦИИ"

Резолюция A~~39-19~~40-XX *"Решение проблем кибербезопасности в гражданской авиации"*

принимая во внимание, что глобальная система авиации представляет собой чрезвычайно сложную и интегрированную систему, включающую в себя информационные и связные технологии, имеющие критически важное значение для безопасности полетов и безопасности гражданской авиации,

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

учитывая, что представляемая киберинцидентами угроза для гражданской авиации быстро и постоянно изменяется, что носители такой угрозы вынашивают преступные намерения, ставят целью по политическим, финансовым или другим мотивам нарушение деловой активности и кражу информации, а также то, что масштаб такой угрозы может легко достичь уровня, на котором может быть нанесен вред критически важным системам гражданской авиации во всем мире,

признавая, что не все проблемы 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 киберрисков одновременно воздействовать на широкий круг 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 правовые рамки, в которых кибератаки на международную гражданскую авиацию считаются 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 критически важных систем инфраструктуры гражданской авиации и ее данных от киберугроз,

рассматривая необходимость совместной работы по созданию для заинтересованных сторон в области гражданской авиации эффективной и координированной глобальной программы по решению проблем кибербезопасности наряду с краткосрочными мероприятиями по повышению устойчивости глобальной системы авиации к киберугрозам, которые могут подрывать основы безопасности полетов гражданской авиации,

признавая работу Исследовательской группы Секретариата по кибербезопасности, которая внесла значительный вклад в формат стратегии кибербезопасности, объединив связанные с кибербезопасностью характеристики безопасности полетов и авиационной безопасности,

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

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

~~*напоминая* об инициативах руководителей Международного совета аэропортов (МСА), Организации по аэронавигационному обслуживанию гражданской авиации (КАНСО), Международной ассоциации воздушного транспорта (ИАТА), Международного координационного совета ассоциаций аэрокосмической промышленности (ИККАИА) и ИКАО, признающих необходимость совместной работы, руководствуясь общностью видения проблемы, стратегией и порядком действий по укреплению защиты глобальной системы авиации от киберугроз и повышению ее устойчивости к ним,~~

~~*признавая* многогранность и комплексный характер проблем и решений в сфере кибербезопасности~~,

Ассамблея:

1. *Настоятельно призывает* государства-члены и ИКАО способствовать всеобщему принятию и претворению в жизнь *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) как способа противостоять кибератакам на гражданскую авиацию;

2. *Призывает* государства и заинтересованные стороны отрасли предпринять следующие меры по противодействию киберугрозам в сфере гражданской авиации:

   a) осуществлять стратегию кибербезопасности, представленную в добавлении;

   ~~a)~~b) 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;

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

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

   ~~d)~~e) 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;

~~e)~~ f) 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;

~~f)~~ 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;

~~g)~~ h) поощрять развитие в национальных органах и в авиационной отрасли жизнестойкой культуры кибербезопасности на всех уровнях;

~~h) определить правовые последствия действий, подрывающих безопасность полетов воздушных судов за счет использования киберуязвимых мест~~;

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;

j) разработать принципы 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 должны быть безопасными, обеспечивающими целостность и конфиденциальность данных; должны быть внедрены методы мониторинга систем и выявления инцидентов и представления сообщений о них; необходимо проводить судебно-криминалистический анализ киберинцидентов;

k) сотрудничать в разработке программы ИКАО в сфере кибербезопасности согласно единому, комплексному и функциональному подходу, включающему области аэронавигации, связи, наблюдения, эксплуатации воздушных судов, летной годности и другие соответствующие дисциплины.

3. *Поручает* Генеральному секретарю:

a) разработать план действий для оказании государствам и отрасли поддержки в принятии стратегии кибербезопасности; ~~оказать государствам и отрасли помощь и содействие в принятии указанных мер~~;

b) продолжать обеспечивать междисциплинарный подход к рассмотрению и координации вопросов кибербезопасности с помощью соответствующих механизмов в духе стратегии.. ~~обеспечить всестороннее рассмотрение и координацию действий по решению проблем кибербезопасности во всех соответствующих сферах деятельности ИКАО~~.

— — — — — — — —

ДОБАВЛЕНИЕ В

СТРАТЕГИЯ В ОБЛАСТИ АВИАЦИОННОЙ КИБЕРБЕЗОПАСНОСТИ

1. КОНЦЕПТУАЛЬНОЕ ВИДЕНИЕ ГЛОБАЛЬНОЙ СТРАТЕГИИ АВИАЦИОННОЙ КИБЕРБЕЗОПАСНОСТИ

1.1 Сектор гражданской авиации все в большей степени зависит от наличия систем информационных и связных технологий, а также от целостности и конфиденциальности данных. Представляемая возможными киберинцидентами угроза для гражданской авиации постоянно изменяется, а носители такой угрозы вынашивают преступные намерения, ставя целью нарушение деловой активности и кражу информации по политическим, финансовым или другим мотивам.

1.2 Признавая многогранную и междисциплинарную природу кибербезопасности и отмечая, что кибератаки могут одновременно затрагивать широкий спектр областей и быстро распространяться, необходимо разработать общее концептуальное видение и определить глобальную стратегию кибербезопасности.

1.3 Концептуальное видение ИКАО глобальной кибербезопасности состоит в том, что авиационный сектор должен быть устойчив к кибератакам, сохраняя надежность и глобальное доверие к себе, продолжая при этом внедрять инновации и развиваться.

1.4 Это может быть достигнуто следующими действиями:

- признание государствами своих обязательств в рамках *Конвенции о международной гражданской авиации* (Чикагской конвенции) по обеспечению безопасности полетов, авиационной безопасности и непрерывности деятельности гражданской авиации с учетом кибербезопасности;
- согласование мер по обеспечению кибербезопасности между государственными органами в целях обеспечения эффективного и результативного управления факторами риска кибербезопасности;
- все заинтересованные стороны в сфере гражданской авиации берут на себя обязательства по дальнейшему развитию киберустойчивости и защите от кибератак, которые могут повлиять на безопасность полетов, авиационную безопасность и непрерывность деятельности системы воздушного транспорта.

1.5 Стратегия согласуется с другими инициативами ИКАО, связанными с обеспечением кибербезопасности, и координируется с соответствующими положениями по управлению безопасностью полетов и авиационной безопасностью. Цели стратегии будут достигаться посредством применения серии принципов, мер и действий, содержащихся в механизме, построенном на семи основополагающих элементах:

I. Международное сотрудничество
II. Управление
III. Эффективное законодательство и нормативные положения
IV. Политика в области кибербезопасности
V. Обмен информацией

VI. Планирование мероприятий на случай инцидентов и действий в чрезвычайных ситуациях
VII. Наращивание потенциала, подготовка персонала и формирование культуры кибербезопасности

2. МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО

2.1 В силу своей природы кибербезопасность и авиация не знают границ. Они в одинаковой степени требуют сотрудничества на национальном и международном уровне и требуют взаимного признания усилий по развитию, поддержанию и повышению кибербезопасности с целью защиты сектора гражданской авиации от всех киберугроз для безопасности полетов и авиационной безопасности.

2.2 Авиационная кибербезопасность должна быть согласована на глобальном, региональном и национальном уровнях в целях содействия глобальной упорядоченности и обеспечения полной функциональной совместимости мер защиты и систем управления факторами риска.

2.3 ИКАО является надлежащим всемирным форумом для привлечения государств к рассмотрению вопросов кибербезопасности в международной гражданской авиации. С этой целью ИКАО будет организовывать, поддерживать и способствовать проведению международных мероприятий, служащих платформой для обмена знаниями между государствами, международными организациями и отраслью. Государствам рекомендуется принимать участие в обсуждениях вопросов кибербезопасности в гражданской авиации.

3. УПРАВЛЕНИЕ

3.1 Всем государствам-членам ИКАО рекомендуется поддерживать и развивать стратегию авиационной кибербезопасности ИКАО для обеспечения безопасности полетов и авиационной безопасности гражданской авиации в мире, который подвергается все большему количеству киберугроз.

3.2 Государствам рекомендуется разработать четкие структуры национального управления и подотчетности в области авиационной кибербезопасности. Ведомствам гражданской авиации рекомендуется обеспечивать координацию со своим компетентным национальным органом в области кибербезопасности, признавая, что общая ответственность за обеспечение кибербезопасности во всех секторах может выходить за рамки ведомства гражданской авиации. Также необходимо установить соответствующие каналы координации деятельности различных государственных органов и заинтересованных сторон от отрасли.

3.3 Кроме того, государствам-членам рекомендуется включать кибербезопасность в свои национальные программы обеспечения безопасности полетов и авиационной безопасности. С этой целью ИКАО следует также включить вопросы кибербезопасности в региональные и глобальные планы и работать над общими исходными параметрами для Стандартов и Рекомендуемой практики в области кибербезопасности (SARPS).

4. ЭФФЕКТИВНОЕ ЗАКОНОДАТЕЛЬСТВО И НОРМАТИВНЫЕ ПОЛОЖЕНИЯ

4.1 Основной целью международного, регионального и национального законодательства и нормативных положений о кибербезопасности для гражданской авиации является оказание поддержки в осуществлении комплексной стратегии кибербезопасности для защиты гражданской авиации и пассажиров от последствий кибератак.

4.2 Руководствуясь положениями ИКАО, государства-члены должны разработать и применять соответствующее законодательство и нормативные положения до реализации своей национальной политики в области кибербезопасности для гражданской авиации. Необходимо продолжать разработку соответствующего инструктивного материала для государств и отрасли, связанного с выполнением положений по кибербезопасности. С этой целью ИКАО обязуется разрабатывать, пересматривать и по необходимости изменять инструктивный материал, связанный с включением аспектов кибербезопасности в меры по обеспечению безопасности полетов и авиационной безопасности.

4.3 Следует проанализировать соответствующие документы международного права, чтобы выявить существующие или отсутствующие ключевые правовые положения в воздушном праве, связанные с предотвращением, преследованием в судебном порядке и своевременным реагированием на киберинциденты, чтобы сформировать основу для последовательного и упорядоченного применения законодательства и нормативных положений в области кибербезопасности во всем мировом авиационном секторе. Тем временем государствам предлагается ратифицировать документы ИКАО, в том числе *Конвенцию о борьбе с незаконными актами в отношении международной гражданской авиации* (Пекинскую конвенцию) и *Протокол, дополняющий Конвенцию о борьбе с незаконным захватом воздушных судов* (Пекинский протокол).

4.4 Государствам рекомендуется рассмотреть вопрос о необходимости обновления их национального законодательства или принятия нового национального законодательства, обеспечивающего преследование в судебном порядке связанных с терроризмом киберугроз, а также кибератак, имеющих отрицательные последствия для гражданской авиации. Одновременно государствам предлагается создать соответствующие механизмы для сотрудничества с "добросовестными" исследованиями в области безопасности, представляющих собой исследовательскую деятельность, которая осуществляется в условиях, позволяющих избегать последствий для безопасности полетов, авиационной безопасности и непрерывности деятельности гражданской авиации.

5. ПОЛИТИКА КИБЕРБЕЗОПАСНОСТИ

5.1 Кибербезопасность должна быть включена в государственные системы контроля над обеспечением авиационной безопасности и безопасности полетов как часть комплексной системы управления факторами риска.

5.2 Признавая существование различных методик оценки факторов риска, следует отдавать приоритет возможной разработке и изменениям инструктивного материала, связанного с оценками угроз кибербезопасности и факторов риска, чтобы достичь сопоставимости результатов таких оценок.

5.3 В секторе гражданской авиации политика кибербезопасности может охватывать весь жизненный цикл авиационной системы и включать следующие элементы: культура кибербезопасности, популяризация безопасных конструкторских решений, безопасность цепочек поставок для программного и аппаратного обеспечения, целостность данных, надлежащий контроль доступа, упреждающее управление уязвимостями, повышение гибкости процесса обновления систем безопасности без ущерба безопасности полетов, а также включение систем и процессов мониторинга данных, относящихся к кибербезопасности.

6. ОБМЕН ИНФОРМАЦИЕЙ

6.1 Поскольку сектор гражданской авиации - это глобальная, взаимозависимая система, охватывающая множество общих систем, кибератаки могут легко распространяться и приводить к глобальным последствиям. Задачами обмена информацией являются предотвращение, раннее обнаружение и смягчение воздействия соответствующих событий в сфере кибербезопасности до того, как они приведут к более широким последствиям для безопасности полетов или авиационной безопасности. Культура обмена информацией, доказавшая свою значимость для безопасности полетов и авиационной безопасности, значительно снизит уровень системного киберриска в авиационном секторе.

6.2 Обмен информацией по таким аспектам, как уязвимости, угрозы, события и передовая практика, осуществляемый в рамках налаженных и доверительных отношений, способен снизить воздействие постоянных атак. В соответствии с существующими положениями ИКАО должны быть признаны надлежащие механизмы обмена информацией.

7. ПЛАНИРОВАНИЕ МЕРОПРИЯТИЙ НА СЛУЧАЙ ИНЦИДЕНТОВ И ДЕЙСТВИЙ В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ

7.1 В соответствии с существующими механизмами управления инцидентами существует потребность в наличии надлежащих и масштабируемых планов, обеспечивающих непрерывность деятельности воздушного транспорта во время киберинцидентов. Государствам и авиационному сектору рекомендуется применять уже разработанные планы действий в чрезвычайных ситуациях и внести в них поправки, включив положения о кибербезопасности.

7.2 Учения в области кибербезопасности являются полезным инструментом для проверки существующей киберустойчивости и поиска улучшений, поэтому настоятельно рекомендуется их проведение. Такие учения могут иметь разные формы (например, штабные учения, моделирование ситуаций или учения в реальном времени) и разные уровни (международный, национальный, организационный).

8. НАРАЩИВАНИЕ ПОТЕНЦИАЛА, ПОДГОТОВКА ПЕРСОНАЛА И ФОРМИРОВАНИЕ КУЛЬТУРЫ КИБЕРБЕЗОПАСНОСТИ

8.1 Человеческий элемент заложен в саму основу кибербезопасности. Для сектора гражданской авиации чрезвычайно важно предпринять ощутимые шаги по увеличению количества квалифицированного персонала, обладающего экспертными знаниями в области авиации и кибербезопасности. Это может быть сделано повышением осведомленности о кибербезопасности, а

также образованием, наймом и подготовкой. Учебные планы по кибербезопасности и, если это практически возможно, по авиационной кибербезопасности на всех уровнях должны быть включены в структуру национального образования, а также в соответствующие международные программы подготовки. Следует искать инновационные решения для совмещения и перекрестного взаимодействия традиционных информационных технологий, киберпрофессий и специалистов, имеющих отношение к авиации.

8.2 Поддержка и стимулирование развития навыков существующей и новой рабочей силы должны способствовать инновациям в области кибербезопасности и соответствующим научным исследованиям и разработкам в авиационном секторе. Для поддержки персонала в выполнении его повседневных обязанностей должна постоянно проводиться соответствующая профессиональная подготовка.

8.3 Кибербезопасность может быть включена в стратегию следующего поколения авиационных специалистов, поскольку ИКАО лучше всего подходит для сотрудничества с государствами и отраслью в разработке требований к компетентности авиационных специалистов, исходя из их повседневных ролей.

8.4 Сектору гражданской авиации удалось достичь завидного уровня безопасности полетов, который основан на культуре упреждающих мер обеспечения безопасности полетов, являющихся обязанностью каждого. Принципы этой культуры безопасности полетов должны применяться в разработке и поддержании культуры кибербезопасности во всем авиационном секторе.

— КОНЕЦ —