Международная организация гражданской авиации

РАБОЧИЙ ДОКУМЕНТ

A40-WP/395[1]
EX/161
30/7/19
(Information paper)

АССАМБЛЕЯ — 40-Я СЕССИЯ

ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ

Пункт 12 повестки дня. Авиационная безопасность. Политика

АВИАЦИОННАЯ КИБЕРБЕЗОПАСНОСТЬ – ДВИЖЕНИЕ ВПЕРЕД

(Представлено Международной ассоциацией воздушного транспорта)

КРАТКАЯ СПРАВКА

В документе представлены мнения Международной ассоциации воздушного транспорта (ИАТА) о необходимости скоординированного, активного и ощутимого прогресса в определении рисков в сфере авиационной кибербезопасности и управления ими.

Стратегические цели	Настоящий информационный документ связан со стратегической целью "*Авиационная безопасность*"
Финансовые последствия	Отсутствуют
Справочный материал	

1. ВВЕДЕНИЕ

1.1 Авиационная кибербезопасность (кибербезопасность, которая касается обеспечения безопасного, надежного и устойчивого выполнения полетов) остается ключевым приоритетом для сектора. Рост цифровизации и возможностей подключения помогает преобразовать сервисы, доступные клиентам, а также улучшить всё от показателей эффективности до показателей надежности для эксплуатантов. Но эта трансформация не просто дает новые возможности авиационному сектору, она дает потенциальную возможность тем, кто желает ему вреда. На базовом уровне авиационный сектор, возможно, находится в лучшем положении, чем многие сектора, благодаря тому, что в центре его внимания - культура безопасности, видение риска, а также разработка решений и профессиональное обучение для подготовки резерва или на случай ошибки. Но сложность и взаимозависимость сервисов и систем, часто на международном уровне, потенциально влияет на способность понимать риски в сфере кибербезопасности и управлять ими.

[1] Тексты на русском, английском, арабском, испанском, китайском и французском языках представлены ИАТА.

1.2 ИАТА решительно поддерживает позицию ИКАО как наиболее подходящей организации для проведения согласованного глобального диалога и действий, касающихся авиационной кибербезопасности. Без четкого международного лидерства в области авиационной кибербезопасности мы рискуем получить фрагментацию глобальных стандартов, сложный регулирующий режим, который сдерживает рост и инновации, а также ограничивает способность оценивать риски для авиационной кибербезопасности и управлять ими как внутри стран, так и за из их пределами.

1.3 Разработка стратегии ИКАО в области авиационной кибербезопасности является похвальным и давно назревшим шагом, который полностью поддерживается ИАТА. Теперь потребуются руководство, действия и надлежащее управление для одобрения стратегии путем внесения поправки в существующую резолюцию A39-19 Ассамблеи *"Решение проблем кибербезопасности в гражданской авиации",* с тем чтобы включить соответствующую ссылку. Поэтому необходимо обеспечить надлежащие ресурсы, время и усилия всех заинтересованных сторон, в том числе безопасность полётов и авиационную безопасность. Кроме того, в свете вышеизложенного важно поощрить ратификацию государствами *Конвенции о борьбе с незаконными актами, направленными против безопасности гражданской авиации*, и *Протокола, дополняющего Конвенцию о борьбе с незаконным захватом воздушных судов.* Это сотрудничество должно привести к разработке передовой практики и инструктивных материалов, на основании которых ИАТА поддерживает создание, в качестве первоисточника, связанных с кибербезопасностью SARPS, их последующее внедрение и контроль за их выполнением.

1.4 В более широком смысле, в наших усилиях обезопасить отрасль мы не можем забывать о движущей силе нашей отрасли, которой являются наши пассажиры и клиенты. Мы должны гарантировать, что на протяжении всего путешествия, их кибербезопасность, конфиденциальность, данные и права будут защищены. Кроме того, гарантия того, что мы как отрасль, будем прозрачны в этих вопросах, обеспечит создание и сохранение доверительных отношений с теми, кто это поддерживает.

1.5 ИАТА принимает активное участие в повышении осведомленности и диалоге заинтересованных сторон о глобальных вызовах авиационной кибербезопасности. ИАТА создала Целевую группу по кибербезопасности воздушных судов (ACSTF), которая работает с целью углубления понимания, развития диалога и обобщения передового опыта среди заинтересованных сторон авиационного сектора. Зрелость ACSTF создала среду высокого доверия, в которой разделяют и изучают идеи обмена конкретной информацией по множеству смежных тем. Кроме того, ИАТА также провела с заинтересованными сторонами, представляющими весь авиационный сектор, новаторский круглый стол по авиационной кибербезопасности в Сингапуре (в апреле 2019 года). В рамках этого круглого стола заинтересованные стороны изучили текущие проблемы, стоящие перед авиационной отраслью, обсудили вопросы о том, как должно выглядеть кибербезопасное будущее и как его достичь. В выводах подчеркивается, что, хотя немало уже сделано, многое еще предстоит сделать.

1.6 Кроме того, ИАТА начала процесс разработки стратегии кибербезопасности в авиационной отрасли наряду с дорожной картой по ее реализации. Цель этой стратегии состоит в том, чтобы позволить ИАТА от имени своих членов и отрасли уделять повышенное внимание, как вызовам, так и возможностям, связанным с вопросами кибербезопасности, с которыми мы сталкиваемся, вести ощутимую деятельность, которая приведет к изменениям, а также в сотрудничестве, направленном на достижение результата.

2. ОБСУЖДЕНИЕ

2.1 При текущих показателях роста к 2037 году мы могли бы увидеть двукратное увеличение числа пассажиров, при этом большая часть этого роста приходится на Азиатско-Тихоокеанский регион[2]. Существует много проблем и рисков для развития, и в качестве одного из этих рисков следует добавить авиационную кибербезопасность. Нельзя недооценивать важность обеспечения безопасности полетов, авиационной безопасности и надежности, от которых зависит этот рост.

2.2 Авиационное кибер-событие не просто создает риски для безопасности полетов, авиационной безопасности, эксплуатации, риски финансовых потерь или риски для развития. Это – риск критически подорвать доверие пассажиров – доверие к самим услугам, которые мы предоставляем. На протяжении многих лет авиационная отрасль доказывала, что она устойчива к инцидентам в сфере безопасности и способна восстановить доверие пассажиров с помощью наглядных мер и взаимодействия. После неблагоприятного авиационного кибер-события восстановить доверие будет на порядок сложнее, чем это было ранее, поэтому нам нужно не только повысить кибербезопасность, но и вести открытый диалог о стоящих перед нами задачах и предпринимаемых нами усилиях.

2.3 В нашем стремлении к технологическому прогрессу необходимо также найти баланс между повышением эффективности и уровнем сервиса за счет более широкого использования связанных технологий, гарантирующих кибербезопасность, безопасность полетов, авиационную безопасность и устойчивость своей работы на протяжении всего срока существования. В авиационной отрасли мы больше не можем позволить себе внедрять какие-либо новые технологии, если они не будут спроектированы кибербезопасными, если они будут вводиться в действие без упреждающего и динамичного управления уязвимостями и без возможности прозрачного взаимодействия в отношении киберрисков между поставщиком и конечным пользователем.

2.4 Наряду с межотраслевыми действиями по повышению кибербезопасности необходимо также предпринять усилия по снижению затрат на кибербезопасность. В международной отрасли с широким спектром организаций, все, что может быть сделано для снижения уровня сложности, стоимости или решения проблемы надлежащего управления рисками кибербезопасности, гарантирует, что ни одна страна (или компания) не останется в стороне.

2.5 Отрасль также должна делать больше, чтобы заблаговременно определять риски и уязвимости, связанные с кибербезопасностью. Это означает быть открытым и активно стремиться к сотрудничеству между заинтересованными сторонами, включая коллег, страны, многонациональные организации, другие сектора и исследовательское сообщество. Как отрасль, мы должны четко понимать, кто наши противники, а кто нет; те, кто хочет помочь нам понять, где мы рискуем, не являются нашими противниками. Межотраслевые, юридические, частные исследования уязвимостей аппаратного и программного обеспечения привели к созданию преуспевающего и активного исследовательского сообщества тех, кто действует добросовестно, чтобы помочь разным отраслям быть более кибербезопасными

2.6 Авиационный сектор обязан выслушивать, оценивать и принимать соответствующие меры по любой потенциальной проблеме безопасности; не зависимо от того, как о них было сообщено, мы должны относиться к уведомлениям о потенциальных уязвимостях

[2] Пресс-релиз ИАТА от 24 октября 2018 года. ИАТА прогнозирует 8,2 млрд авиапутешественников в 2037 году. Доступно по ссылке https://www.iata.org/pressroom/pr/Pages/2018-10-24-02.aspx.

кибербезопасности одинаково. Авиационная отрасль должна предпринять шаги для укрепления доверия и взаимоотношений с исследовательским сообществом, с тем, чтобы с обеих сторон было достигнуто взаимопонимание. ИАТА дополнительно поддерживает эти усилия, а также разработку мер и законодательства, которые поощряют и защищают способность добросовестных исследователей поддерживать авиационную отрасль.

2.7 В ходе круглого стола ИАТА по авиационной кибербезопасности в Сингапуре в апреле 2019 года международные участники, представляющие весь сектор, подчеркнули, те аспекты, где достигается прогресс, а также те, где требуется больше усилий. Основные моменты изложены ниже.

2.7.1 Были предложены следующие взгляды на текущее состояние авиационной кибербезопасности:

a) Понять масштаб и сложный характер рисков для авиационной кибербезопасности, расставить приоритеты и предпринять действия оказывается сложной задачей для некоторых организаций.

b) В силу взаимозависимого и глобального характера авиационной отрасли, по текущим оценкам, количество инцидентов в сфере кибербезопасности будет быстро увеличиваться и вызывать последствия на международном уровне.

c) В авиационной отрасли сохраняются несоответствия и недостатки в поиске, управлении и распространении информации об уязвимостях кибербезопасности, что приводит к плохому выявлению реальных рисков в сфере кибербезопасности.

2.7.2 Были предложены следующие взгляды на то, что участники представляют в качестве идеального "Видения будущего" для авиационной кибербезопасности в 2030 году и как его достичь:

a) Культура кибербезопасности. Подобно культуре безопасности полетов и физической безопасности, вся авиационная отрасль нуждается в культуре кибербезопасности.

b) Прозрачность и доверие. Отношения между всеми заинтересованными сторонами в авиационной отрасли должны стать более прозрачными и, следовательно, должно возрасти доверие по вопросам кибербезопасности, начиная от доступа к соответствующим данным, касающимся кибербезопасности, до надежных методов развития и управления уязвимостью. Для этого авиационная отрасль может применять подходы аналогичные тем, которые она уже использует в рамках культуры безопасности полетов и культуры авиационной безопасности, привнося общность подхода и моральных целей таким образом, чтобы это понимали все.

c) Формирование консенсуса и последовательности. Во всей мировой авиационной отрасли нам необходимо продолжать укреплять согласованность, стандартизацию и регулирование в области кибербезопасности. Это потребует формирования лидерства на корпоративном и индивидуальном уровнях, а также готовности к открытому диалогу между всеми заинтересованными сторонами.

d) Взаимодействие и сотрудничество. Для более эффективного управления рисками авиационной кибербезопасности в глобальном масштабе необходимо установить более прочные отношения как внутри авиационной отрасли, так и за её пределами с теми, кто может помочь. Это будет способствовать более тесному сотрудничеству во всем, от разработки передовых методов до управления потенциальными уязвимостями.

e) Трудовые ресурсы. Посредством диалога о проблемах и возможностях в области кибербезопасности, с которыми сталкивается авиационная отрасль, мы должны вдохновить новое поколение людей и организаций, способных оказать поддержку в решении проблем авиационной кибербезопасности. Кроме того, авиационный персонал должен быть обучен распознавать риски для кибербезопасности и управлять ими, что приведет к повышению бдительности и надежности.

2.8 В рамках круглого стола ИАТА по авиационной кибербезопасности обсуждались еще две темы.

2.8.1 Расследование аспектов кибербезопасности происшествий или инцидентов. При расследовании авиационных происшествий и инцидентов в настоящее время очень мало внимания уделяется потенциальным проблемам кибербезопасности. Во время, когда многие авиационные системы связаны и оцифрованы, было сочтено, что необходимо приложить больше усилий для понимания того, как собирать, надежно защищать и анализировать данные, имеющие отношение к кибербезопасности. Не делать этого означает, что отрасль будет иметь очень мало возможностей, чтобы заверить себя и своих клиентов о своей способности управлять рисками в сфере кибербезопасности.

2.8.2 Таким образом, многое предстоит сделать для повышения кибербезопасности, авиационной безопасности и отказоустойчивости авиационной отрасли. Но наряду с этой проблемой существует большой потенциал для межотраслевого сотрудничества и действий в тесном партнерстве между всеми заинтересованными сторонами. Сейчас нам нужны приверженность, лидерство и действия.

— КОНЕЦ —