Международная организация гражданской авиации

A41-WP/74
EX/36
26/7/22

РАБОЧИЙ ДОКУМЕНТ

АССАМБЛЕЯ — 41-Я СЕССИЯ

ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ

Пункт 14 повестки дня. Авиационная безопасность. Политика

РАЗРАБОТКА РАМОЧНОГО МЕХАНИЗМА ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

(Представлено Чехией от имени Европейского Союза и его государств-членов[1], а также других государств – членов Европейской конференции гражданской авиации[2], государств – членов Африканской комиссии гражданской авиации[3] и ЕВРОКОНТРОЛя)

КРАТКАЯ СПРАВКА

Значение кибербезопасности продолжает возрастать, так как в связи с появлением новых технологий и все большей зависимости авиации от информационных технологий и цифровых операционных систем возникают как новые уязвимости, так и новые возможности. С лучшим пониманием специфики киберсреды приходит также осознание ряда конкретных проблем, при этом возникает необходимость продвижения и последовательного осуществления отдельного подхода, направленного на уменьшение рисков. Растущее значение кибербезопасности еще больше высвечивает необходимость того, чтобы государства и ИКАО активизировали усилия в поддержку разработки рамочного механизма обеспечения кибербезопасности, а также культуры обеспечения кибербезопасности и подготовки по соответствующим вопросам.

Действия: Ассамблее предлагается:

a) поручить ИКАО рассмотреть необходимые шаги по дальнейшей разработке инструктивного материала по оценке рисков кибербезопасности для авиации, учитывая при этом действующих лиц, необходимость комплексного и сквозного подхода и отличительные факторы, описанные в настоящем рабочем документе;

b) поручить ИКАО завершить составление сборника соответствующих существующих Стандартов и Рекомендуемой практики (SARPS) и других международно-правовых норм, на которые могут опереться государства и организации при учете рисков, связанных с кибербезопасностью, в своих авиационных системах;

[1] Австрия, Бельгия, Болгария, Венгрия, Германия, Греция, Дания, Ирландия, Испания, Италия, Кипр, Латвия, Литва, Люксембург, Мальта, Нидерланды, Польша, Португалия, Румыния, Словакия, Словения, Финляндия, Франция, Хорватия, Чехия, Швеция и Эстония.

[2] Албания, Армения, Азербайджан, Босния и Герцеговина, Грузия, Исландия, Молдова, Монако, Черногория, Северная Македония, Норвегия, Сан-Марино, Сербия, Швейцария, Турция, Украина и Соединенное Королевство.

[3] Алжир, Ангола, Бенин, Ботсвана, Буркина-Фасо, Бурунди, Габон, Гамбия, Гана, Гвинея, Гвинея-Бисау, Демократическая Республика Конго, Джибути, Египет, Замбия, Зимбабве, Кабо-Верде, Камерун, Кения, Коморские Острова, Конго, Кот-д'Ивуар, Лесото, Либерия, Ливия, Маврикий, Мавритания, Мадагаскар, Малави, Мали, Марокко, Мозамбик, Намибия, Нигер, Нигерия, Объединенная Республика Танзания, Руанда, Сан-Томе и Принсипи, Сейшельские Острова, Сенегал, Сомали, Судан, Сьерра-Леоне, Того, Тунис, Уганда, Центральноафриканская Республика, Чад, Экваториальная Гвинея, Эритрея, Эсватини, Эфиопия, Южная Африка и Южный Судан.

c) просить ИКАО и ее договаривающиеся государства активизировать усилия по продвижению особой культуры кибербезопасности и мероприятий в поддержку подготовки достаточного количества людских ресурсов и развития потенциала для решения вопросов кибербезопасности и киберустойчивости в гражданской авиации; d) поручить ИКАО рассмотреть вопрос об организации учений по вопросам кибербезопасности на глобальном и региональном уровнях.	
Стратегические цели	Данный рабочий документ связан со стратегическими целями *"Авиационная безопасность"* и *"Упрощение формальностей"*.
Финансовые последствия	
Справочный материал	

1. ВВЕДЕНИЕ

1.1 На 40-й сессии Ассамблеи ИКАО была принята резолюция Ассамблеи A40-10 *"Решение проблем кибербезопасности в гражданской авиации"*. В резолюции кибербезопасность рассматривается сквозь призму горизонтального, сквозного и функционального подхода, подтверждается важность и срочность вопроса о необходимости защиты систем и данных критической инфраструктуры гражданской авиации от киберугроз и содержится призыв к государствам реализовать Стратегию ИКАО в области авиационной кибербезопасности (октябрь 2019 года). Стратегия реализуется посредством выполнения Плана действий по обеспечению кибербезопасности (ПДоК) и при поддержке недавно созданной Группы экспертов по кибербезопасности, которая будет опираться на работу Исследовательской группы Секретариата по кибербезопасности.

1.2 По мере все более глубокого влияния цифровизации на экономику и изменения авиационного сектора вопрос кибербезопасности приобретает все большую актуальность. Обеспечение кибербезопасности также продолжает оставаться серьезной задачей для всех секторов на этапе восстановления после пандемии COVID-19. Предприятия все чаще используют дистанционные методы работы, что может повысить их уязвимость к киберугрозам. Это требует активизации усилий по разработке системы кибербезопасности с учетом ее специфики.

2. ХАРАКТЕРНЫЕ ОТЛИЧИТЕЛЬНЫЕ ЭЛЕМЕНТЫ КАРТИНЫ КИБЕРБЕЗОПАСНОСТИ ПРИ ОПРЕДЕЛЕНИИ ПОДХОДА К УПРАВЛЕНИЮ РИСКАМИ

2.1 Сфера кибербезопасности отличается уникальной картиной угроз. Невозможно сконцентрироваться исключительно на террористических группах, стремящихся к прямым нападениям и массовым жертвам, поскольку следует также принимать во внимание и целый ряд других возможных субъектов и мотивов. К ним можно отнести крупные организованные структуры, активистов и хакеров-преступников, например, преследующих цель создания сбоев в работе, принуждения, демонстрации силы, привлечения внимания СМИ или финансовой наживы. Нападения также могут намеренно или случайно приводить к последствиям для гражданской авиации, возможно даже угрожая безопасности полетов, и оказывать прямое или косвенное воздействие на весь сектор.

2.2 К другим элементам, которые необходимо учитывать при управлении рисками в плане кибербезопасности, относятся значительное количество не связанных с авиацией поставщиков услуг для авиационной системы, которые могут по-разному понимать потребности и риски в области кибербезопасности.

2.3 Кроме того, для сферы кибербезопасности характерно государственное регулирование, которое может применяться к различным секторам, не имеющим отношения к авиации.

2.4 Вышеперечисленные соображения указывают на необходимость определения конкретного подхода к оценке рисков кибербезопасности, в рамках которого:

a) требуются специалисты с особой компетенцией, особенно в части знания уязвимостей и мер по их устранению, обладающие знаниями и опытом и в области авиации, и в области информационных технологий;
b) сфера оценки должна быть четко определена и прежде всего включать вопросы безопасности полетов, авиационной безопасности и стабильности осуществления критически важных функций всеми эксплуатантами/субъектами и во всех областях;
c) оценка рисков может выявить потенциальные возможности для единичного отказа с точки зрения (глобальной) информационной безопасности, с тем чтобы затем устранить их надлежащим образом.

3. РАЗРАБОТКА МЕХАНИЗМА ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ С УЧЕТОМ СПЕЦИФИКИ РАБОТЫ

3.1 При разработке механизма обеспечения кибербезопасности авиационный сектор должен разработать подходы, которые не только выходят за рамки традиционных авиационных вопросов (например, предусмотреть необходимость как макро-подхода (например, для ОрВД), так и подхода к отдельным полетам), но и учитывают отличия неавиационных секторов и единые (не связанные с авиацией) требования государственного регулирования, как описано выше в пп 2.2 и 2.3. Крайне важно обеспечить согласованность, а также избегать дублирования, пробелов и чрезмерно обременительного регулирования или надзора для государств и эксплуатантов при внедрении системы кибербезопасности.

3.2 Авиационный сектор имеет все необходимое для использования существующих в мире функций, обязанностей и процедур в области авиации и выстраивания своей дальнейшей работы на их основе. SARPS ИКАО в области авиационной безопасности и безопасности полетов служат прочной основой, на которую можно опираться на уровне как правительств, так и отдельных организаций. То же самое относится и к механизмам обмена информацией и представления отчетности. Имеются также существующие международные договоры о воздушном праве, предусматривающие уголовную ответственность за действия, ставящие под угрозу безопасность, и которые следует использовать в максимально возможной степени.

3.3 Государствам и организациям рекомендуется изучить и рассмотреть соответствующие документы ИКАО по кибербезопасности и внедрить существующие SARPS по кибербезопасности. Важно также, чтобы государства и организации переосмыслили существующие структуры обеспечения авиационной безопасности и безопасности полетов, а также авиационного

уголовного права с точки зрения цифровых технологий, с тем чтобы обеспечить их актуальность в будущем и добиться надлежащей координации функций и обязанностей.

4. КРИТИЧЕСКОЕ ЗНАЧЕНИЕ ЧЕЛОВЕЧЕСКОГО ФАКТОРА В ВОПРОСАХ КИБЕРБЕЗОПАСНОСТИ

4.1 Человеческий фактор лежит в основе кибербезопасности, что признается в Стратегии ИКАО в области авиационной кибербезопасности (2019).

4.2 Ускоряющаяся цифровизация и все большая взаимосвязанность авиационной системы требует активизации усилий по удовлетворению растущего спроса на повышение осведомленности, профессиональную подготовку, обновление учебных программ и соответствующим образом подготовленных сотрудников с междисциплинарным опытом и в вопросах авиации, и в вопросах кибербезопасности.

4.3 Секретариат ИКАО приступил к проведению первого курса ИКАО по кибербезопасности и киберустойчивости "Основы лидерства и управления техническими аспектами авиационной кибербезопасности", а также курса "Управление рисками безопасности при ОрВД", разработанного в партнерстве с ЕВРОКОНТРОЛем. Важно продолжать эту востребованную работу и накапливать опыт.

4.4 Как отмечается в Стратегии ИКАО в области авиационной кибербезопасности, учения по кибербезопасности являются полезным инструментом для проверки текущего уровня киберустойчивости и выявления требующих доработки областей, в связи с чем их проведение настоятельно рекомендуется. Помимо учений, проводимых на уровне отдельных европейских государств, Европа обладает региональным опытом в этой области, которым может поделиться на благо международного авиационного сообщества.[4] ИКАО рекомендуется изучить возможности проведения таких учений.

4.5 Как подчеркивалось в ходе *Года культуры безопасности* ИКАО (ГКАБ), жизненно важно расширить понятие культуры авиационной безопасности и безопасности полетов за пределы физической сферы. Государствам и организациям рекомендуется развивать достижения ГКАБ путем внедрения культуры кибербезопасности и обмена передовым опытом. ИКАО следует содействовать усилиям в этом направлении, в том числе посредством разработки соответствующего инструктивного материала.

— КОНЕЦ —

[4] В учениях "Кибер-Европа 2018", организованных Агентством Европейского Союза по сетевой и информационной безопасности (ENISA), приняли участие отдельные специалисты и организации, занимающиеся вопросами информационной безопасности в авиационном секторе; в 2018 году Европейское подразделение по координированию кризисных ситуаций в сфере авиации (EACCC) организовало учения по управлению кризисной ситуацией, вызванной кибератакой на программное обеспечение для устройств слежения за полетами, а на 2022 год готовятся учения по управлению кризисной ситуацией, имитирующей крупномасштабное отключение инфраструктуры европейской цифровой сети в результате кибератаки; Европейское агентство по безопасности полетов также организовало учения по кибербезопасности.