Международная организация гражданской авиации

A39-WP/187[1]
EX/72
10/08/16

РАБОЧИЙ ДОКУМЕНТ

АССАМБЛЕЯ — 39-Я СЕССИЯ

ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ

Пункт 16 повестки дня. Авиационная безопасность. Политика

СТРАТЕГИЯ В ОБЛАСТИ ЗАЩИТЫ КИБЕРБЕЗОПАСНОСТИ

(Представлено Организацией аэронавигационного обслуживания гражданской авиации (КАНСО))

КРАТКАЯ СПРАВКА

Кибербезопасность – один из наиболее важных вопросов и самая обсуждаемая тема в гражданской авиации. Развитие авиационных систем рождает новые риски, которые могут повлиять на безопасность и непрерывность вследствие возрастающей зависимости от информационных технологий. Инциденты в сфере кибербезопасности, связанные не только с конфиденциальностью, но главным образом с доступностью и непрерывностью, могут оказать влияние на системы организации воздушного движения (ОрВД), авиационные системы, системы управления аэропортами, системы бронирования, аэронавигационную и метеорологическую информацию.

Действия Ассамблее предлагается согласовать рекомендацию, изложенную в разделе 5.

Стратегические цели	Настоящий рабочий документ относится к стратегической цели C *"Авиационная безопасность и упрощение формальностей"*
Финансовые последствия	Снижение затрат на страхование, снижение угроз и опасных факторов в свете устойчивости и безопасности, а также снижение затрат, связанных с антикризисным управлением и социальными последствиями
Справочный материал	Приложение 17 *"Безопасность"* к Чикагской конвенции; Doc. 8973; Doc. 9985; Doc. 9854; Руководство КАНСО по оценке рисков в области безопасности

1. ВВЕДЕНИЕ

1.1 Гражданская авиация по-прежнему является приоритетной целью для преступников и террористов. Обязательство защищать гражданскую авиацию от актов незаконного вмешательства означает предотвращать комплексные угрозы, включая угрозы технологического характера. Общество всегда будет ожидать полного отсутствия несчастных случаев и инцидентов в связи с

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

нарушениями безопасности в сфере гражданской авиации. Эта концепция обеспечит уверенность конечного пользователя в сфере воздушных перевозок. Воздушная транспортная сеть играет ключевую роль для мировой экономики и является основой для международной торговли, туризма, инвестиций и процветания. Любые нарушения ее эффективности могут привести к значительным экономическим и социальным нарушениям по всему миру. Разработка комплексных систем, взаимосвязанных по своему характеру, в глобальной и международной среде требует методологического подхода к управлению безопасностью с целью обеспечения постоянного контроля ресурсов, интеграции процессов в сфере информационных технологий (ИТ), логической и физической безопасности. Это необходимо реализовать путем постоянной оценки уровня угроз и потенциальной уязвимости с целью предотвратить незаконное вмешательство и реализовать меры реагирования на такое вмешательство. Эта задача также требует тесного взаимодействия между всеми действующими лицами авиационной системы, государствами и соответствующими заинтересованными сторонами. Простого соблюдения нормативных положений недостаточно, несмотря на то что это необходимо для демонстрации должной осмотрительности при защите человеческих жизней в воздухе и на земле, а также для обеспечения безопасности, непрерывности, устойчивости и регулярности работы системы. Рабочая группа ИКАО по устранению угроз и рисков также подчеркнула, что глобальная система воздушных перевозок при своей информационной и коммуникационной сложности определенно является потенциальной целью для серьезных кибератак. Цель по обеспечению взаимосвязи и открытия сетей для сетецентрических операций путем распространения информации и операционных данных в режиме реального времени делают систему еще более уязвимой.

1.2 ИКАО уже выразила обеспокоенность тем, что кибербезопасность может стать препятствием для реализации Глобального аэронавигационного плана (ГАНП) и поддержала инициативу, разработанную совместно с крупнейшими заинтересованными сторонами в сфере авиации, с целью систематической оценки существующей схемы обеспечения кибербезопасности (Отраслевая рабочая группа высокого уровня по вопросам кибербезопасности подписала документ в Монреале 5 декабря 2014 г.).

1.3 Во время заседания Группы экспертов ИКАО по авиационной безопасности (AVSECP/27), которое проводилось в марте 2016 г., большое количество государств-членов подчеркнуло необходимость обновления текущей рекомендуемой практики в Приложении 17 ("Безопасность") в отношении кибербезопасности до стандарта. Однако большинство членов выразили мнение, что кибербезопасность не ограничивается только системой авиационной безопасности. Члены подчеркнули особую важность надлежащей координации, включая согласование с другими приложениями, а именно 3, 6, 10, 11, 14 и 15. Кроме того, координация с другими соответствующими группами экспертов необходима до обновления текущей рекомендуемой практики до стандарта; существует четкая необходимость в консультировании с Комитетом по аэронавигации ИКАО.

1.4 КАНСО желает подчеркнуть важность защиты всей цифровой информации и систем в рамках авиационной системы. Важно обеспечить защиту и безопасность общественности, пассажиров, экипажей, наземного персонала, судов и строений от незаконного вмешательства как на земле, так и в воздухе. Для расширения этой концепции в менее развитых странах необходимы конкретные действия в соответствии с инициативой "Ни одна страна не остается без внимания" (NCLB).

2. НЕОБХОДИМОСТЬ УТОЧНЕНИЯ ТЕРМИНА КИБЕРБЕЗОПАСНОСТЬ

2.1 КАНСО отмечает наличие некоторой степени неопределенности касательно термина "кибербезопасность". Он используется для обозначения угроз со стороны врагов, а также при необходимости оценки и выявления уязвимостей в системах ИТ. Кроме того, данный термин используется для описания способов реализации эффективного планирования непрерывности в свете устойчивости.

2.2 КАНСО подчеркивает, что четкая стратегия по обеспечению безопасности гражданской авиации должна учитывать не только технологический уровень зрелости, но главным образом методологический защитный подход для достижения основной цели в сфере безопасности авиации. Это может быть достигнуто с помощью принципа восходящего подхода, включая всю организацию, с учетом человеческого фактора.

2.3 Эта цель четко изложена в *Глобальной эксплуатационной концепции ОрВД* (Doc. 9854 ИКАО), в которой указана важнейшая роль безопасности и дано новаторское определение:

> *"Под авиационной безопасностью понимается защита от опасности, которую несут с собой преднамеренные (например, террористические) или непреднамеренные (например, ошибка человека, природные бедствия) акты, затрагивающие воздушные суда, людей или объекты на земле. Обеспечение такой безопасности является одним из главных ожиданий сообщества ОрВД и населения. Поэтому система ОрВД должна способствовать авиационной безопасности, а вся система и связанная с ней информация должны быть защищены от незаконного вмешательства".*

2.4 С этой точки зрения, связанной с основными стандартами безопасности в сфере ИТ, цель по обеспечению доступности, целостности и конфиденциальности связана с общим обязательством принимающих на себя такие обязательства государств по обеспечению защиты основных элементов гражданской авиации в соответствии с Чикагской конвенцией и особенно Приложением 17 ИКАО ("Безопасность").

3. НОВЫЙ ПОДХОД

3.1 КАНСО подчеркивает, что защита соответствующих активов, важных для обеспечения безопасности гражданской авиации, может отличаться у заинтересованных сторон в сфере авиации в соответствии с их целями, например правительства, поставщики аэронавигационного обслуживания, авиакомпании, аэропорты, производители, военные структуры и т. д. Можно определить некоторые темы в области кибербезопасности авиации, общие для всех членов общественности, с учетом специальных потребностей:

a) обеспечивать доступ к критической информации только уполномоченным лицам с целью предотвращения актов незаконного вмешательства изнутри независимо от ключевых услуг оператора;

b) выполнять обязательство, основываясь на здравом смысле и *принципах добросовестности*, выявлять уязвимые области в критических системах и устранять тщательно и предусмотрительно;

c) расширить управление рисками, включив в него те риски, которые обусловлены возрастающей зависимостью от ресурсов в области ИТ, принадлежащих одному оператору;

d) предусмотреть надлежащие меры реагирования на случай инцидентов и с целью антикризисного управления, включая план действий в чрезвычайной ситуации;

e) оценивать влияние нарушений (кибер)безопасности не только на одного оператора, но и на всю отрасль в целом в рамках Национальной программы по обеспечению безопасности гражданской авиации.

3.2 Другими словами, кибербезопасность предполагает такой же подход, что и обеспечение стандартной авиационной безопасности; это естественное расширение базовых принципов, предусмотренных в Приложении 17 ("Безопасность") и указаниях по наиболее распространенным факторам опасности и уязвимости в области физической безопасности.

3.3 Киберугрозы в сфере авиации, скорее всего, станут главной проблемой, учитываемой в новых программах модернизации, например Single European Sky (SES), программах исследования ОрВД (SESAR), Next Generation (NEXTGEN) и других программах на региональном уровне. Это один из наиболее важных факторов развития в других областях авиационной отрасли. Будучи критическим источником, информация должна восприниматься как любой другой актив, важный для выживаемости и успеха систем ОрВД. Все подобные программы, в том числе ОрВД и другие программы, затрагивающие операторов воздушных судов, аэропорты, военные структуры и других лиц, будут основаны на концепции Общесистемного управления информацией (SWIM), которая ускоряет сетецентрический операционный обмен информацией и услугами в рамках всей системы. Концепция SWIM улучшит процесс совместного принятия решений и повысит качество информации, предоставляемой в нужное время необходимому получателю, который нуждается в такой информации для исполнения своих обязанностей. SWIM – ключевой фактор для будущей технологической среды авиации; при проектировании связанной с ней инфраструктуры безопасность должна быть ключевым требованием этого важнейшего элемента.

3.4 В этом отношении, учитывая, что общая безопасность является обязательством принимающих на себя соответствующие обязательства государств и предполагает последствия для национального суверенитета, обороны, получения информации и контроля исполнения законодательства, необходимость учитывать специфический характер авиационной среды вызывает необходимость более эффективных действий.

3.4.1 Соответствующие инициативы на региональном уровне находятся в процессе реализации или уже реализованы. Среди недавних результатов следует отметить следующие. Позиция Европейского союза о кибербезопасности в ОрВД четко отражает в принятом Положении ЕС № 1035/2011 связь между уязвимыми факторами и предусматривает обязательные требования в связи с кибербезопасностью. Федеральное управление гражданской авиации США в предложении, представленном Сенату, заявляет о цели в области кибербезопасности (раздел 4109), направленной на выполнение сложных задач, включая широкий спектр действий по решению проблем в области кибербезопасности. Другие государства уделяют такое же пристальное внимание усилиям по регулированию кибербезопасности в области авиации.

3.4.2 Признавая важность кибербезопасности для гражданской авиации, КАНСО полностью поддерживает инициативу, направленную на полную интеграцию вопроса кибербезопасности в программы национальной и региональной авиационной безопасности и заявляет о своей полной готовности принимать активное участие.

4. ЗАКЛЮЧЕНИЕ

4.1 Кибербезопасность – тема, которая требует методологического и реалистичного рассмотрения с учетом последствий и влияния на общую отрасль и уверенность общественности.

4.2 КАНСО продвигает обновленную международную инициативу под руководством ИКАО, реализуемую в соответствии с принципами эффективности и устойчивости согласно положениям инициативы "Ни одна страна не остается без внимания".

4.3 Отраслевая рабочая группа высокого уровня по вопросам кибербезопасности после подписания плана действий в области кибербезопасности в декабре 2014 года разрабатывает схему добровольного взаимодействия в этой области. Эта отраслевая программа должна быть дополнена и одобрена регуляторными органами. Следует также более глубоко рассмотреть многопрофильную проблему гражданской авиации, касающуюся кибербезопасности.

5. РЕКОМЕНДАЦИИ

5.1 Ассамблее предлагается поставить перед ИКАО безотлагательную задачу по включению кибербезопасности в перечень вопросов авиационной безопасности на постоянной основе. Ассамблее предлагается одобрить следующие рекомендации:

Ассамблее:

a) рассмотреть содержание настоящего документа и одобрить его, а также признать актуальность для гражданской авиации и возможное влияние на эту отрасль;

b) одобрить разработку ИКАО новой стратегии в области авиационной кибербезопасности в качестве вертикальной области авиационной безопасности и выпустить руководящие документы, нацеленные на приведение к единообразию существующих инициатив на региональном и национальном уровне;

c) рекомендовать государствам-членам сфокусировать свое внимание на уязвимых факторах систем и сетей, а не на опасных факторах и учесть последствия для всей отрасли гражданской авиации;

d) рекомендовать проведение форума для авиакомпаний с целью обмена передовыми методами создания безопасной/надежной среды, а также обмена информацией об эффективных инструментах и методиках для усиления безопасности текущих и будущих технологических систем;

e) рекомендовать государствам-членам рассмотреть последние инициативы, представленные на AVSECP/27, с целью пересмотра текущих рекомендуемых практик в пунктах 4.9.1 и 4.9.2 Приложения 17 до стандарта;

f) ознакомиться с *Руководством КАНСО по оценке рисков в области безопасности*[2].

— КОНЕЦ —

[2] https://www.canso.org/canso-cyber-security-and-risk-assessment-guide