Международная организация гражданской авиации

A39-WP/175
EX/64
9/8/16

РАБОЧИЙ ДОКУМЕНТ

АССАМБЛЕЯ — 39-Я СЕССИЯ

ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ

Пункт 16 повестки дня. Авиационная безопасность. Политика

КИБЕРБЕЗОПАСНОСТЬ ГРАЖДАНСКОЙ АВИАЦИИ. ВОЗМОЖНЫЕ ДЕЙСТВИЯ РЕГУЛИРУЮЩИХ ОРГАНОВ И ЗАИНТЕРЕСОВАННЫХ СТОРОН

(Представлено Аргентиной, Бельгией, Бывшей югославской Республикой Македония, Гайаной, Лаосской Народно-Демократической Республикой, Намибией, Науру, Непалом, Нигерией, Нидерландами, Объединенными Арабскими Эмиратами, Республикой Молдова, Российской Федерацией, Саудовской Аравией, Сенегалом, Сент-Люсией, Сингапуром, Соединенным Королевством, Сьерра-Леоне, Тринидадом и Тобаго, Францией, Швейцарией и Южной Африкой)

КРАТКАЯ СПРАВКА

Киберугрозы, стоящие перед системой гражданской авиации, являются предметом серьезной озабоченности заинтересованных сторон во всем мире. Критическое значение имеет сотрудничество между ИКАО, полномочными органами авиационной безопасности, авиационной отраслью и другими заинтересованными сторонами гражданской авиации в целях повышения осведомленности об угрозах и разработки практической и устойчивой политики, подходов и мер, в том числе в части, касающейся подготовки персонала и наращивания потенциала, с тем чтобы обеспечить защиту от киберугроз и смягчить их последствия. Ввиду взаимозависимости различных частей глобальной экосистемы гражданской авиации тесное сотрудничество играет ключевую роль в решении данных задач.

Действия: Ассамблее предлагается:

a) принять к сведению содержание настоящего документа, в особенности возможные действия регулирующих органов и заинтересованных сторон по борьбе с киберугрозами для гражданской авиации;

b) призвать ИКАО создать глобальную программу кибербезопасности для заинтересованных сторон гражданской авиации;

c) поручить одному из органов ИКАО работу по созданию глобальной концепции и координации с другими соответствующими органами ИКАО и заинтересованными сторонами.

Стратегические цели:	Настоящий рабочий документ связан со стратегическими целями A *"Безопасность полетов"*, B *"Аэронавигационный потенциал и эффективность"* и C *"Авиационная безопасность и упрощение формальностей"*
Финансовые последствия:	Дополнительные финансовые последствия отсутствуют
Справочный материал:	A39-WP/14 *"Всеобъемлющая стратегия ИКАО в сфере обеспечения авиационной безопасности (ICASS)"* A39-WP/15 *"Разработка глобального плана обеспечения авиационной безопасности"* A39-WP/16 *"Сводное заявление о постоянной политике ИКАО в области авиационной безопасности"* A39-WP/17 *"Решение проблем кибербезопасности в гражданской авиации"* Резолюция A38-15 Ассамблеи *"Сводное заявление о постоянной политике ИКАО в области авиационной безопасности"* AVSECP/27, Доклад в желтой обложке. Для ограниченного распространения (*только на английском языке*)

1. ВВЕДЕНИЕ

1.1 Как и в других областях, киберугрозы вызывают серьезную озабоченность в системе гражданской авиации. У террористов и лиц, имеющих преступные намерения, есть множество способов для совершения кибератак, направленных против заинтересованных сторон и инфраструктуры в сфере гражданской авиации. Они могут нарушить работу гражданской авиации, в том числе путем взлома систем навигации и управления воздушного судна, вмешательства в работу радиолокационной системы и системы связи, а также повреждения различных систем аэропорта. Хотя до сих пор большинство подобных атак, направленных против авиационного сектора, осуществлялись на невысоком уровне, и их негативное воздействие было ограниченным, кибератака, целью которой является нарушение деятельности гражданской авиации, потенциально может иметь катастрофические последствия, повлечь за собой значительные жертвы, нарушение обслуживания гражданской авиации и/или повреждение критически важных объектов инфраструктуры. Эта озабоченность усугубляется тем фактом, что в своей деятельности авиакомпании, аэропорты, поставщики аэронавигационного обслуживания и другие заинтересованные стороны (например, компании по наземному обслуживанию, поставщики технического обслуживания, поставщики услуг по обеспечению безопасности, топливные компании, грузовые агенты и т. д.) все в большей степени зависят от информационных систем связи и компьютерных технологий (ICT).

2. БОРЬБА С КИБЕРУГРОЗАМИ

2.1 В последние годы заинтересованные стороны гражданской авиации уделяют все большее внимание киберугрозам. В 2014 году ИКАО, Международная ассоциация воздушного транспорта (ИАТА), Международный совет аэропортов (МСА), Организация по аэронавигационному обслуживанию гражданской авиации (КАНСО) и Международный координационный совет ассоциаций аэрокосмической промышленности (ИККАИА) выпустили совместный план действий по борьбе с этими угрозами. ИАТА также разработала инструментарий для обеспечения кибербезопасности для авиакомпаний, а многие аэропорты, поставщики аэронавигационного обслуживания и изготовители воздушных судов приняли различные меры для повышения уровня защиты своей работы от кибератак.

2.2 На международном уровне регулирующие органы, отвечающие за авиационную безопасность гражданской авиации, работают над решением проблем кибербезопасности в рамках Группы экспертов ИКАО по авиационной безопасности (AVSECP). Рабочая группа AVSECP по угрозам и рискам (WGTR) представила Группе экспертов ряд оценок и рекомендаций по риску кибератак, а также был начат процесс координации работы AVSECP и соответствующих Групп экспертов ИКАО по безопасности полетов, с тем чтобы упорядочить работу по общей для них теме.

2.3 Несмотря на эти действия, многим заинтересованным сторонам все еще сложно справиться с данными проблемами. Повышение осведомленности и стимулирование диалога между заинтересованными сторонами в части, касающейся киберугроз, было бы полезно для улучшения понимания. Проведение подробной оценки риска позволит заинтересованным сторонам выявить пробелы в области авиационной безопасности, с тем чтобы в дальнейшем предпринять необходимые шаги по их устранению. В июле 2015 года Сингапур в сотрудничестве с ИКАО и ИАТА и при поддержке различных государств и заинтересованных представителей отрасли организовал конференцию по кибербезопасности, на которой для обсуждения киберугроз собрались специалисты из различных частей экосистемы гражданской авиации. Среди участников

были эксплуатанты аэропортов, авиакомпании, изготовители авиационных двигателей, компании по наземному обслуживанию, поставщики услуг по обеспечению безопасности, поставщики оборудования для обеспечения безопасности, организации, имеющие отношение к международной гражданской авиации, и регулирующие органы. Среди прочего на ней обсуждались следующие ключевые вопросы:

a) угрозы и факторы риска кибератак, направленных против глобальной системы гражданской авиации: периодическая оценка данных угроз и факторов риска силами WGTR может быть использована ИКАО и заинтересованными сторонами для разработки эффективных профилактических и ответных мер;

b) анализ мер предупреждения, реагирования, а также действий в чрезвычайных ситуациях и экстренных действий в случае кибератаки, целью которой является деятельность гражданской авиации;

c) действия, предпринятые некоторыми заинтересованными сторонами для борьбы с киберугрозами;

d) риск для авиационного сектора особенно велик, поскольку вероятность успешного совершения кибератак выше в секторе, чьи составные части отличаются высокой взаимозависимостью, а также потому что механизмы защиты от кибератак, которыми в данный момент располагает авиационный сектор пока недостаточны для борьбы с данной стремительно видоизменяющейся угрозой;

e) необходим сквозной подход, охватывающий весь авиационный сектор, с тем чтобы обеспечить скоординированное, соразмерное и эффективное внедрение.

3. ВОЗМОЖНЫЕ ДЕЙСТВИЯ РЕГУЛИРУЮЩИХ ОРГАНОВ И ЗАИНТЕРЕСОВАННЫХ СТОРОН

3.1 Был определен ряд возможных действий регулирующих органов и заинтересованных сторон, в том числе:

a) Необходимо как можно скорее разграничить ответственность за данный вопрос, начиная с **<u>глобального уровня</u>**, где **ИКАО было бы полезно создать глобальную программу борьбы с киберугрозами для заинтересованных сторон гражданской авиации**. Данная программа, которая должна быть основана на существующей передовой практике в области информационной безопасности и разрабатываться в тесном взаимодействии со специалистами по авиационной безопасности и безопасности полетов, могла бы включать в себя набор принципов, инструктивный материал и подходы для использования регулирующими органами и отраслью.

b) **На <u>уровне государств</u> для борьбы с киберугрозами важно разработать механизм нормативного надзора со стороны органов обеспечения авиационной безопасности (координирующих свои действия с другими полномочными органами, отвечающими за кибербезопасность на**

национальном уровне) и обеспечить его применение. Режим нормативного надзора должен быть комплексным и распространяться на сектор гражданской авиации и всех участников системы гражданской авиации с учетом их взаимозависимости.

c) **На уровне отдельных заинтересованных сторон, каждой из них необходимо разработать свой собственный набор действий для защиты от киберугроз, особенно если речь идет о системах, имеющих отношение к безопасности полетов и авиационной безопасности**.

d) Заинтересованным сторонам необходимо как можно раньше реагировать на киберугрозы. Поэтому для сектора гражданской авиации важно **разрабатывать меры раннего обнаружения, координации и оперативной ликвидации последствий**. Представление информации об инцидентах в области кибербезопасности групп реагирования на компьютерные угрозы (CERT) или центрам по обмену информацией и анализу (ISAC) позволит своевременно предупреждать остальные заинтересованные стороны и должно поощряться на национальном уровне, в то время как международная координация должна осуществляться под руководством ИКАО.

e) Поскольку движущими факторами повышения уровня кибербезопасности являются эволюция угроз и новые технологические тенденции, **требуется согласование работы людей, процессов, технологий и систем, с тем чтобы обеспечить наличие у каждого из этих компонентов соответствующих возможностей для выявления угроз и борьбы с ними**.

f) **Обмен информацией и передовой практикой между ведомствами, отвечающими за обеспечение кибербезопасности гражданской авиации, играет важнейшую роль**. Это поможет государствам и заинтересованным сторонам совместно и сообща выявлять тенденции, определять угрозы и разрабатывать эффективные меры противодействия. Также важно, чтобы разведывательные и прочие соответствующие службы продолжали работу по получению более полного представления о киберугрозах для гражданской авиации.

g) В силу взаимосвязанности информационных систем гражданской авиации **необходимо общее понимание того, какие именно системы и данные считаются критически важными или являются ключевыми для безопасности полетов, авиационной безопасности и бесперебойного функционирования системы гражданской авиации**. Авиационным регулирующим органам следует совместно определить критерии систем, считающихся критически важными (с глобальной, региональной и/или национальной точек зрения), с тем чтобы указать основные направления в сфере внедрения.

h) **Важное значение имеет подготовка персонала гражданской авиации в рамках всей системы гражданской авиации для повышения его осведомленности об угрозах и факторах риска кибератак, а также оперативного и адекватного реагирования на них**. Выявление внештатных ситуаций и своевременное оповещение о любых подозрительных событиях или

деятельности способствовало бы предотвращению или сдерживанию кибератаки и помогло бы свести к минимуму нарушения деятельности. Важно включать проблематику кибербезопасности в программы подготовки в области авиационной безопасности, а также нанимать специалистов по авиационной безопасности и аудиторов, знакомых с вопросами кибербезопасности.

i) **Важно также развивать культуру авиационной безопасности, что должно включать лучшее понимание киберугроз**. Если высшее руководство осознает необходимость борьбы с этими угрозами и будет оказывать активную поддержку в деле подготовки персонала и инвестирования в средства борьбы с киберугрозами, сектор гражданской авиации будет в состоянии более эффективно противодействовать им.

— КОНЕЦ —