



РАБОЧИЙ ДОКУМЕНТ

АССАМБЛЕЯ — 40-Я СЕССИЯ

ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ

Пункт 12 повестки дня. **Авиационная безопасность. Политика**

СТРАТЕГИЧЕСКИЙ ПОДХОД К АВИАЦИОННОЙ КИБЕРБЕЗОПАСНОСТИ

(Представлено Францией)

КРАТКАЯ СПРАВКА

В условиях возрастающей опасности киберугроз многие государства уже разработали стратегический национальный межотраслевой подход. В то же время вырабатываются или должны быть выработаны специфические подходы в области авиационной кибербезопасности, обеспечивающие безопасность полетов, авиационную безопасность и устойчивое развитие воздушного транспорта. Эти два подхода не должны вступать в противоречие между собой; напротив, они должны дополнять друг друга.

Более того, для эффективной реализации стратегии авиационной кибербезопасности крайне важно, чтобы деятельность в области кибербезопасности не трансформировалась в монодисциплинарную практику, что со временем может вылиться в потенциальную избыточность, дублирование или несоответствия.

Для обеспечения эффективности такой координации Франция, например, учредила Совет по кибербезопасности воздушного транспорта, который уже предлагает ключевые решения по защите гражданской авиации от кибератак.

Построение стратегии ИКАО по этому вопросу в таком же духе, с созданием специализированного органа, обеспечивающего взаимную координацию подходов, может только приветствоваться и было бы крайне полезно.

Действия: Ассамблее предлагается:

а) рекомендовать всем государствам создать на национальном уровне эффективную систему координации действий между полномочными органами по делам гражданской авиации и соответствующими органами, отвечающими за кибербезопасность, включая механизмы координации как на стратегическом, так и на оперативном уровнях с участием всех поставщиков услуг и заинтересованных сторон авиационной отрасли;

б) подчеркнуть важность эффективного междисциплинарного сотрудничества и координации действий между подразделениями Секретариата ИКАО, отвечающими за авиационную безопасность и за безопасность полетов, а также относящимися к ним рабочими группами и группами экспертов;

с) призвать Совет ИКАО учредить и сформировать в рамках ИКАО междисциплинарный орган по кибербезопасности гражданской авиации, например, в виде группы экспертов, создаваемой в соответствии с Директивами группам экспертов (Дос 9482), для консолидации и согласования всей деятельности и документации, относящихся к кибербезопасности, включая механизм доверия.

<i>Стратегические цели</i>	Настоящий рабочий документ относится к стратегическим целям <i>"Безопасность полетов", "Аэронавигационный потенциал и эффективность", "Авиационная безопасность и упрощение формальностей"</i>
<i>Финансовые последствия</i>	Действия, упомянутые в настоящем документе, будут предприняты за счет ресурсов, имеющихся в бюджете Регулярной программы на 2020–2022 гг., и/или за счет внебюджетных поступлений
<i>Справочные материалы</i>	A40-WP/28, EX/13 <i>"Стратегия ИКАО в области кибербезопасности"</i>

1. ИСХОДНАЯ ИНФОРМАЦИЯ

1.1 На национальном уровне государства-члены несут ответственность за обеспечение безопасности полетов, авиационной безопасности и устойчивое развитие гражданской авиации, принимая во внимание вопросы обеспечения кибербезопасности, как это уже требуется в Приложении 17 ИКАО *"Авиационная безопасность"*. Однако защита воздушного транспорта от кибератак подразумевает очень широкий спектр тематик и требует привлечения самых разнообразных ресурсов. Поэтому наиважнейшей задачей является определить рамки действий полномочных органов гражданской авиации и, как следствие, роль ИКАО в этой деятельности.

1.2 Кибербезопасность не является понятием, характерным только для авиации, и многие государства уже разработали стратегический национальный межотраслевой подход и соответствующие правила. Управление кибербезопасностью очень часто происходит на межминистерском уровне и осуществляется через какую-либо специализированную организацию или специальный орган в рамках министерства. Такой "национальный" или регулирующий подход применяется к авиации, как к одному из секторов экономики, имеющему жизненно важное значение.

1.3 Одновременно с этим, и особенно в отношении международной гражданской авиации, различные государства применяют меры по защите отраслевых эксплуатантов (аэропортов, авиакомпаний, поставщиков аэронавигационных услуг и т. д.), а также изготовителей воздушных судов, стараясь обеспечить их оперативную совместимость, сбалансированность с общими процессами управления безопасностью полетов и авиационной безопасностью и соответствие им. В этом заключается цель "подхода к обеспечению кибербезопасности в авиации".

1.4 Для того чтобы решать проблемы кибербезопасности в авиации и уменьшить соответствующие угрозы и факторы риска, ИКАО на своем уровне учредила Исследовательскую группу Секретариата по кибербезопасности (SSGC), создала механизм доверия и разработала внятную стратегию кибербезопасности в авиации.

2. ОБСУЖДЕНИЕ

2.1 Понятие кибербезопасности в авиации может заставить рассматривать все стороны деятельности воздушного транспорта, включая такие потенциальные аспекты, как экономический, репутационный, воздействие на окружающую среду и конфиденциальность личной информации. Некоторые из них не являются специфичными для авиационной области и регулируются другими полномочными органами в рамках различных программ. Таким образом, необходимо не замыкаться внутри монодисциплинарной практики, которая со временем может привести к потенциально избыточным мерам или несоответствиям, а сконцентрироваться на управлении авиационной безопасностью и безопасностью полетов, что само по себе важно и потребует

привлечения значительных ресурсов. Решение остальных аспектов кибербезопасности в авиации должно таким образом быть в компетенции национальных регулирующих органов, либо находиться под внутриотраслевым управлением.

2.2 Подходы к авиационной кибербезопасности на национальном уровне должны правильно сочетаться с независимыми подходами и обеспечивать равномерную и последовательную реализацию. Необходимо использовать обратную связь с авиационным сектором для внесения необходимых изменений и поправок в положения и практику национального подхода к решению проблем кибербезопасности. В свою очередь, информация и данные, касающиеся кибербезопасности, получаемые из других областей, могут помочь в идентификации потенциальных угроз для авиации.

2.3 Наконец, на национальном уровне подход к авиационной кибербезопасности должен принимать во внимание потребности всей системы авиации и в полной мере управлять всеми киберрисками, свойственными авиационной деятельности, не игнорируя небольшие аэродромы или эксплуатантов, обращая в то же время внимание на пропорциональность требований к уровню риска. Это можно, таким образом, рассматривать как способ достижения целей национального подхода во всем авиационном секторе.

2.4 На глобальном уровне ИКАО должна стремиться выстроить необходимую структуру взаимодействия таким образом, чтобы обеспечивалось должное сочетание национального и отраслевого подходов. В соответствии с приоритетами, определенными выше для ведомств гражданской авиации, такая структура ИКАО в особенности должна поддерживать такие качества глобальной системы авиации как безопасность полетов, авиационная безопасность и функциональная совместимость. Она должна вести к системному подходу к кибербезопасности в синергетической связи с существующими процессами управления безопасностью полетов, используемыми по всему миру.

2.5 ИКАО должна представлять авиационный сектор на форумах ООН, касающихся национального подхода к кибербезопасности, чтобы избежать ситуации, когда плохо координированные национальные меры в области кибербезопасности начнут оказывать негативное влияние на работоспособность всей системы авиации.

3. ОПЫТ КООРДИНАЦИИ: ПРИМЕР ФРАНЦИИ

3.1 В апреле 2018 года Франция учредила Совет по кибербезопасности на воздушном транспорте (ССТА). Совет возглавляет генеральный директор гражданской авиации, в него также входят представители всех заинтересованных сторон из государственного и частного сектора (таких как национальное агентство по вопросам кибербезопасности, министерства обороны и внутренних дел, производители воздушных судов и электронного оборудования, а также поставщики услуг для аэропортов, воздушных судов, аэронавигации), и он является компетентным органом для решения всех вопросов по кибербезопасности в гражданской авиации.

3.2 В этом контексте становится ясно, что для того, чтобы получить все возможное синергетическое взаимодействие и справиться с возможными противоречиями, к авиационной кибербезопасности следует относиться как к целостному и вместе с тем комплексному явлению вне зависимости от классических разграничений между авиационной безопасностью и безопасностью полетов.

3.3 Комплексная деятельность ССТА также показала важность точного определения общей терминологии и взаимно используемой методики для проработки других сценариев. Такие сценарии выражаются в классических целях кибербезопасности (доступность, комплексность,

аутентичность и конфиденциальность), применяемых к критически важным авиационным активам, и оцениваются по 4-балльной шкале, совместимой с оценкой факторов риска для безопасности полетов.

3.4 В настоящее время на основе анализа риска ведется работа над динамичным отображением информации, служащим питательной средой для всех процессов эксплуатации (обслуживание воздушных судов, эксплуатация аэропортов, выполнение полетов, наземные операции). Такое системное отображение информации позволит ССТА определять потоки критической информации, информационные системы, границы информационных систем, характерные для каждого из сценариев. Ожидаемым значимым результатом станет построение иерархии сценариев согласно их важности.

3.5 Следующим шагом станет оценка мер по снижению угрозы и/или ликвидации последствий в целях коллективного выбора наиболее эффективного способа борьбы с угрозой, представляемой конкретным сценарием.

4. ЗАКЛЮЧЕНИЕ

4.1 Национальные стратегии кибербезопасности и стратегия ИКАО должны сосредоточиться на укреплении безопасности полетов и авиационной безопасности всей системы авиации и сохранении устойчивости услуг воздушного транспорта.

4.2 На национальном уровне всем государствам следует координировать управление авиационной кибербезопасностью, а также соответствующие программы регулирования и процессы управления с процессами обеспечения безопасности полетов и авиационной безопасности. Должна быть организована действенная координация между национальным полномочным органом гражданской авиации и соответствующими организациями, отвечающими за управление кибербезопасностью, а также механизмы координации на стратегическом и оперативном уровнях со всеми поставщиками авиационных услуг и заинтересованными участниками отрасли.

4.3 Подходы в области авиационной кибербезопасности должны четко согласовываться на глобальном, региональном и национальном уровнях с национальными подходами для обеспечения полной согласованности мер по защите от угроз и их снижению, а также систем управления риском.

4.4 На международном уровне представляется необходимым создание в рамках ИКАО межотраслевого органа по обеспечению кибербезопасности гражданской авиации, аналогичного группе экспертов, учрежденной согласно положениям документа *"Директивы для групп экспертов Авиатранспортного комитета и Комитета по незаконному вмешательству"* (Doc 9482). При координации его действий с подразделениями Секретариата ИКАО, отвечающими за авиационную безопасность и за безопасность полетов, он мог бы распространить свою деятельность на все области в компетенции ИКАО, чтобы обеспечить консолидацию и согласование всех действий и документации, имеющих отношение к кибербезопасности, включая механизм доверия. До этого момента продолжать работу по данному предмету должна Исследовательская группа Секретариата по кибербезопасности.