



РАБОЧИЙ ДОКУМЕНТ

АССАМБЛЕЯ — 42-Я СЕССИЯ

ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ

Пункт 13 повестки дня. Авиационная безопасность. Политика

ПЛАНЫ ДЕЙСТВИЙ НА СЛУЧАЙ НЕПРЕДВИДЕННЫХ ОБСТОЯТЕЛЬСТВ И УЧЕНИЯ В КИБЕРПРОСТРАНСТВЕ КАК СРЕДСТВО ПОВЫШЕНИЯ УСТОЙЧИВОСТИ К КИБЕРУГРОЗАМ

(Представлено Бразилией)

КРАТКАЯ СПРАВКА

В рабочем документе подчеркивается необходимость разработки планов действий на случай непредвиденных обстоятельств для критически важных систем гражданской авиации, как указано в Плане действий ИКАО в области кибербезопасности в соответствии с элементом 6 Стратегии ИКАО в области авиационной кибербезопасности, а также совершенствования планов по итогам учений по моделированию кибератак на основе реальных характеристик систем и уже выявленных фактов, которые могут привести к таким атакам, как указано в Плане действий ИКАО в области кибербезопасности в соответствии с элементом 7 Стратегии. В нем описывается эволюция кибератак в гражданской авиации, а также подчеркивается важность соответствующих учений и планов действий в чрезвычайных ситуациях.

Действия: Ассамблее предлагается призвать государства-члены:

- а) содействовать разработке планов управления кибер-инцидентами, связанными с критически важной авиационной инфраструктурой;
- б) проводить регулярные кибер-учения с участием государственных и частных заинтересованных сторон.

Стратегические цели	Настоящий рабочий документ связан со стратегической целью <i>"Каждый полет является безопасным и надежным"</i>
Финансовые последствия	Неприменимо.
Справочный материал	Элемент 6 (Планирование мероприятий на случай инцидентов и действий в чрезвычайных ситуациях) и элемент 7 (Наращивание потенциала, подготовка персонала и формирование культуры кибербезопасности) Стратегии ИКАО в области авиационной кибербезопасности.

1. ВВЕДЕНИЕ

1.1 Киберугрозы представляют собой серьезную и растущую проблему для сектора гражданской авиации, который по своей сути является взаимосвязанной глобальной системой, в которой наличие уязвимых мест может способствовать быстрому распространению вредоносных программ, вызывая широкомасштабные и глобальные последствия. Несмотря на то, что технологические достижения принесли авиации множество преимуществ, они также привели к появлению постоянно меняющейся среды киберугроз в связи с глубокой зависимостью от цифровых инфраструктур. Признавая эту настоятельную необходимость обеспечения киберзащиты и устойчивости важнейших авиационных систем, в Стратегии ИКАО в области авиационной кибербезопасности излагаются принципы, меры и действия, основанные на семи основополагающих элементах.

1.2 В связи с этим в настоящем рабочем документе дано описание некоторых мер, принятых Бразилией для достижения большей киберустойчивости в ситуациях, когда элемент 6 (Планирование мероприятий на случай инцидентов и действий в чрезвычайных ситуациях) и элемент 7 (Наращивание потенциала, подготовка персонала и формирование культуры кибербезопасности)) Стратегии ИКАО по авиационной кибербезопасности могут способствовать киберзащите важных активов, используемых в управлении воздушным движением. Объединяя эти два элемента, гражданская авиация может создать комплексную и адаптируемую оборону, не только реагируя на угрозы, но и активно предотвращая их и смягчая их воздействие, обеспечивая постоянную безопасность и надежность авиаперевозок.

1.3 Элемент 6 включает в себя надежные процедуры восстановления, наличие четких и проверенных планов действий на случай непредвиденных обстоятельств для незамедлительного начала процедур восстановления скомпрометированных систем и данных, сводя к минимуму нарушение процессов управления воздушным движением, наземными операциями и обслуживанием пассажиров. Это включает в себя резервное копирование, альтернативные системы и детально прописанные действия по восстановлению.

1.4 Элемент 7 направлен на повышение осведомленности и подготовку всех заинтересованных сторон, участвующих в управлении воздушным движением, предоставляя всем, от диспетчеров УВД до персонала по наземному обслуживанию, возможность реагировать на киберинцидент и играть свою роль в поддержании безопасной и защищенной среды. Хорошо развитая культура кибербезопасности означает, что каждый человек понимает, что он является потенциальной первой линией обороны. Так же, постоянное обучение и адаптация имеют важное значение, признавая постоянное изменение среды киберугроз и готовность адаптироваться к новым стратегиям и технологиям обеспечения кибербезопасности. Это означает никогда не останавливаться на достигнутом и всегда стремиться к совершенствованию.

1.5 Эти принципы имеют важное значение для укрепления сотрудничества между органами обеспечения кибербезопасности гражданской авиации и другими заинтересованными сторонами в целях реагирования на кибератаки и подготовки надежного сценария, при котором планы действий на случай непредвиденных обстоятельств являются способом реагирования на эти злонамеренные действия. В документе будет рассмотрен вопрос координации действий между всеми участниками с указанием всех механизмов, которые будут доступны для восстановления нормальной работы после компрометации каждой системы, и подчеркиванием важнейших требований для выполнения ответных действий, способствующих созданию более безопасной и более устойчивой глобальной авиационной экосистемы.

2. РАССМОТРЕНИЕ ВОПРОСА

2.1 Ежедневно СМИ сообщают о попытках кибератак, некоторые из которых являются успешными, а о других даже не сообщается, потому что они были предотвращены различными защитными мерами, которые внедряют компании и организации для борьбы с этими ежедневными атаками. Ситуация в авиационном секторе практически такая же. Злоумышленники ищут, в основном, незащищенные уязвимые места, чтобы попытаться вторгнуться и украсть информацию и модифицировать системы, с целью, как правило, извлечь финансовую выгоду.

2.2 Бразилия в рамках Департамента контроля воздушного пространства (DECEA) подготавливает меры по повышению устойчивости бразильской системы контроля воздушного движения к киберугрозам, количество которых нарастает с каждым днем. Таким образом, подтверждая понимание этой темы в ИКАО и отражая два основных элемента, упомянутых в стратегии Организации в области кибербезопасности, DECEA занимается организацией учений по подготовке групп реагирования на инциденты из числа сотрудников органов по контролю воздушного пространства. Эти учения не только способствуют обучению групп, но и помогают выявить пробелы в кибербезопасности, возникающие в результате сочетания систем и приложений, разработанных для удовлетворения требований по контролю за воздушным движением. Результаты этих учений обобщаются в отчетах, адресованных группам, отвечающим за совершенствование систем и плана действий в чрезвычайных ситуациях.

2.3 Каждая смоделированная в ходе учений ситуация сопровождается детальным описанием, предоставляемым специалистами по обслуживанию каждой системы, для создания достоверности ситуаций, основанных на реальных событиях. Таким образом действия приближены к реальной ситуации и позволяют получить более точную оценку для совершенствования принимаемых мер по каждой системе (выявленным пробелам) и самому плану.

2.4 Еще один элемент стратегии ИКАО в области кибербезопасности, который касается управления инцидентами и планов действий на случай непредвиденных обстоятельств, служит основой для подготовки планов действий в чрезвычайных ситуациях применительно к каждой критически важной системе, используемой для контроля за воздушным пространством Бразилии. В документе приведена вся информация, необходимая для того, чтобы направить усилия на восстановление функциональных возможностей каждой системы на различных уровнях управления воздушным движением, а также различных субъектов, участвующих в действиях по реагированию, при должной координации действий в целях сведения к минимуму нарушения доступности и последствия для пользователей воздушного транспорта.

2.5 Планы на случай непредвиденных обстоятельств разрабатываются на основе международных стандартов, таких как ISO/IEC 27031, и корректируются с учетом специфики каждого места. Это позволяет агрегировать подробную информацию о функциональных возможностях систем в каждом месте для поддержания этих функциональных возможностей даже в случае кибератак, сохраняя устойчивость среды и контроль за ней.

2.6 Важно уточнить, что DECEA также участвует в бразильском национальном учении по кибербезопасности под эгидой министерства обороны, которые направлены на защиту важнейших систем страны. В этих национальных учениях DECEA для обеспечения безопасности воздушного транспорта предоставляет экспертные знания, накопленные в подразделениях управления по контролю за воздушным пространством, и получает информацию из других областей, в которых также имеются критически важные системы, требующие мер защиты и устойчивости. Мероприятия, разработанные в рамках этого крупного национального учения,

помогают подтвердить и улучшить планы действий на случай непредвиденных обстоятельств, которые необходимо постоянно обновлять перед лицом ежедневных новых угроз.

2.7 Бразилия призывает государства - члены ИКАО и авиационную отрасль поддерживать и организовывать учения по кибербезопасности, с тем чтобы собрать вместе правительственных и отраслевых экспертов для обмена передовым опытом и знаниями при подготовке экспертов в области кибербезопасности к реагированию на кибератаки и при разработке более надежных планов действий в киберпространстве в целях защиты критически важной авиационной инфраструктуры и систем.

3. **ВЫВОДЫ**

3.1 Киберугрозы представляют собой постоянную проблему, и сектор гражданской авиации с его сложной глобальной сетью также уязвим. Проактивная позиция Бразилии, о чем свидетельствуют инициативы DECEA, согласуется со Стратегией ИКАО в области авиационной кибербезопасности, в частности с элементами 6 и 7. Уделение внимания надежности планов действий в чрезвычайных ситуациях, основанных на международных стандартах, таких как ISO/IEC 27031, и адаптированных к местным особенностям, в сочетании с регулярными реалистичными киберучениями значительно повышает уровень киберустойчивости. Эти усилия не только обеспечивают подготовку групп реагирования на инциденты и выявляют уязвимые места, но и способствуют формированию устойчивой культуры кибербезопасности у всех заинтересованных сторон. Обмениваясь опытом и сотрудничая в рамках национальных и международных учений, Бразилия подчеркивает острую необходимость постоянной адаптации и коллективных действий для защиты глобальной авиационной экосистемы от возникающих киберугроз.

— КОНЕЦ —