Международная организация гражданской авиации

A41-WP/488[1]
EX/235
2/8/22

РАБОЧИЙ ДОКУМЕНТ

АССАМБЛЕЯ – 41-Я СЕССИЯ

Пункт 15 повестки дня. Программы проверок. Механизм непрерывного мониторинга

УКРЕПЛЕНИЕ ГРУПП ПРОВЕРЯЮЩИХ ПО ЛИНИИ УППАБ-МНМ ДЛЯ ОЦЕНКИ И ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ ПРИЛОЖЕНИЯ 17 ПО КИБЕРБЕЗОПАСНОСТИ

(Представлено Венесуэлой (Боливарианской Республикой) при поддержке Боливии (Многонационального Государства), Колумбии, Коста-Рики, Панамы, Перу и Уругвая[2])

КРАТКАЯ СПРАВКА

В соответствии с Универсальной программой проверок в сфере обеспечения авиационной безопасности (УППАБ) в настоящее время в государствах действуют руководящие принципы, позволяющие проводить общую оценку функционирования государственной системы надзора за обеспечением авиационной безопасности. Это позволило разработать рекомендации по совершенствованию использования общих принципов авиационной безопасности. Такая оценка проводится группой проверяющих, которые следят за тем, чтобы эта деятельность охватывала важнейшие элементы системы надзора за авиационной безопасностью в дополнение к соблюдению положений и определению уровня соблюдения Стандартов Приложения 17 *"Авиационная безопасность"*. В Приложении 17 указаны способы разработки и осуществления мер по защите систем информационно-коммуникационных технологий, а также важнейших данных, используемых для целей гражданской авиации. С учетом этого необходимо укрепить группы проверяющих путем разработки руководящих указаний или учебных материалов, которые позволят им оценивать и выполнять требования в области кибербезопасности, изложенные в Приложении 17.

Действия: Ассамблее предлагается:

a) принять к сведению информацию, представленную в настоящем рабочем документе;

b) поручить Совету разработать инструменты или учебные материалы для предоставления группе проверяющих по линии УППАБ полных инструкций и подготовки по вопросам кибербезопасности, с тем чтобы назначенные группы могли проводить объективную и техническую оценку вопросов протокола (ВП) в соответствии со специализированными аспектами кибербезопасности в гражданской авиации.

Стратегические цели	Настоящий рабочий документ связан со стратегической целью Авиационная безопасность и упрощение формальностей
Финансовые последствия	Мы предлагаем, чтобы деятельность, упомянутая в настоящем документе, осуществлялась с использованием ресурсов, имеющихся в рамках Регулярной программы на текущий трехгодичный период, и/или за счет внебюджетных взносов
Справочный материал	Рекомендуемая практика 4.9.1 Приложения 17 и Протокол по УППАБ-МНМ

[1] Текст на испанском языке представлен Венесуэлой (Боливарианской Республикой).
[2] Государства – члены Южноамериканского региона (SAM) и Латиноамериканской комиссии гражданской авиации (ЛАКГА).

1. ВВЕДЕНИЕ

1.1 В рамках Универсальной программы проверок в сфере обеспечения авиационной безопасности (УППАБ) государствам предоставляются руководящие принципы, позволяющие проводить общую оценку функционирования государственной системы надзора за обеспечением авиационной безопасности. Это позволило разработать рекомендации по совершенствованию использования общих принципов авиационной безопасности. Согласно Протоколу по механизму непрерывного мониторинга УППАБ (УППАБ-МНМ), в настоящее время существуют конкретные ВП (1345, 1350, 1360 и 3278), связанные с оценкой общих или основных аспектов разработки и осуществления мер по защите систем информационно-коммуникационных технологий, а также критически важных данных, используемых для целей гражданской авиации.

1.2 Такая оценка проводится группой проверяющих по линии УППАБ, которые обеспечивают, чтобы такая деятельность охватывала наиболее важные элементы системы надзора за обеспечением авиационной безопасности, а также соблюдение положений и определение уровня соблюдения Стандартов Приложения 17 *"Авиационная безопасность"*. В Приложении 17 содержится обязательство каждого государства распределять обязанности, устанавливать национальные критерии защиты систем, связанных с авиационной деятельностью, посредством осуществления защитных мер, выявлять критически важные системы, осуществлять постоянный мониторинг, обеспечивать обнаружение, анализ и реагирование на кибератаки, а также оценивать деятельность по контролю качества, проводимую государством в соответствии с оценками рисков.

2. АНАЛИЗ

2.1 Учитывая важность мероприятий, проводимых в рамках УППАБ-МНМ в отношении кибербезопасности важно обеспечить, чтобы группа проверяющих по линии УППАБ располагала инструктивными материалами, позволяющими им проводить объективную и техническую оценку осуществления международных стандартов, стратегий и передовой практики, разработанных и осуществляемых государствами в целях выявления и защиты важнейших информационных технологий и систем связи от любого вмешательства, которое может поставить под угрозу безопасность полетов, целостность или функционирование системы гражданской авиации.

2.2 В настоящее время на глобальном уровне мы располагаем нормативными документами и существующей практикой, которые позволили различным организациям эффективно управлять ситуацией и снижать риски в области кибербезопасности. В качестве примеров можно привести стандарты серии ISO/IEC-2700, разработанные с целью внедрения передовой практики в отношении различных аспектов управления информационной безопасностью, постоянного совершенствования и снижения рисков; Руководство по контрольным целям для информационных технологий (COBIT); Методологию анализа и управления рисками MAGERIT для информационных систем; и другие международные стандарты, руководящие принципы и передовую практику.

2.3 Вышеупомянутые нормативные документы отражают значительный прогресс в сотрудничестве и глобальной интеграции в области кибербезопасности, обеспечивая порядок действий и ориентиры, которые применимы и являются общими для всех типов критической инфраструктуры. Такие ориентиры относятся конкретно к отраслевым стандартам, руководящим принципам и практике, которые делают возможным внедрение и оценку кибербезопасности не только на уровне организации и документации, но и на уровне операционной деятельности и реализации.

2.4 С учетом этого мы предлагаем разработать стандартизированные инструктивные материалы, позволяющие создать справочную основу, использующую передовую отраслевую практику и методологию, а также опыт государств для достижения гармонизированного подхода. Это будет не статичный документ, а скорее инструктивный материал, который позволит группе проверяющих по линии УППАБ провести техническую и объективную оценку уровня соблюдения Стандартов с учетом специфики и потребностей каждого государства, как это изложено в ВП 1345, 1350, 1355, 1360 и 3278.

2.5 В добавлении к настоящему рабочему документу представлена предлагаемая модель содержания для областей знаний и инструктивных материалов. Предложение основано на критериях, взятых из различных стандартов, руководств и существующей практики управления информационной безопасностью, опыта постоянного совершенствования и смягчения последствий в организациях с международной критической инфраструктурой. В добавлении особо отмечено следующее:

a) области знаний и опыта, потенциально необходимые для оценки мер в области кибербезопасности, осуществляемых государствами (в соответствии с ВП);

b) предложенное содержание для составления текста или инструктивных материалов, с тем чтобы группа проверяющих по линии УППАБ могла оценить и выполнить требования по кибербезопасности, изложенные в Приложении 17.

3. ЗАКЛЮЧЕНИЕ

3.1 Важно, чтобы группы проверяющих, назначенные для проверки осуществления УППАБ-МНМ, обладали инструментами и знаниями, необходимыми для точной и объективной оценки выполнения государствами задач по подготовке, разработке и реализации задач по защите гражданской авиации в области кибербезопасности в соответствии с требованиями, изложенными в Стандартах и Рекомендуемой практике Приложения 17 ИКАО *"Авиационная безопасность"*.

— — — — — — — —

ДОБАВЛЕНИЕ

ПРЕДЛАГАЕМОЕ СОДЕРЖАНИЕ ДЛЯ ОБЛАСТЕЙ ЗНАНИЙ И МЕТОДИЧЕСКИХ МАТЕРИАЛОВ

a) Области знаний и опыта, необходимые для оценки мер кибербезопасности, осуществляемых государствами

Знание процедур и методов управления информационными ресурсами и критическими процессами; идентификация и оценка технологических ресурсов или информации, связанной с авиацией; политика, процедуры и меры информационной безопасности; управление рисками и инцидентами; управленческий контроль или гарантии, позволяющие смягчить последствия в области кибербезопасности; экспертные, сетевые, кодовые проверки, аудит уязвимости и физические проверки, веб-анализ и прочее.

Технические возможности для оценки защитных мер путем проведения испытаний, таких как, например: сбор, классификация и идентификация имеющихся средств, проверка работоспособности сервисов, анализ и проверка уязвимости; проверка работоспособности системы электроснабжения, оборудования, зависимых ресурсов или систем при выходе из строя системы электроснабжения; тестирование оборудования для управления информационной системой и ИТ-платформой; тестирование аппаратного, операционного и инфраструктурного программного обеспечения и/или программных приложений; тестирование производительности ИТ-платформы (в условиях полного нарушения деятельности); тестирование резервного интернет-сервиса (отключение от первичного канала, проверка подключения вторичного канала, балансировка нагрузки и т. д.); тестирование системы восстановления информации и прочее.

b) Предлагаемое содержание для подготовки текста или инструктивных материалов в целях оценки и осуществления требований в области кибербезопасности, изложенных в Приложении 17.

1. Инструктивный материал по общим критически важным процессам в гражданской авиации, касающимся авиакомпаний (управление пассажиропотоком, багажом, грузами, наземное обслуживание, отправка рейсов, техническое обслуживание воздушных судов и т. д.); критически важные процессы в аэропортах (безопасность аэропортов, полеты и инфраструктура аэропортов, управление и чрезвычайные ситуации в аэропортах, в частности); важнейшие процессы управления воздушным движением (голосовая связь, передача аэронавигационных сообщений и радиолокационных данных, аэронавигация и т. д.).

2. Стандартизированная методология оценки рисков для авиационного сектора, которая включает определение контекста, политики и ответственности, определение оперативных процессов, выявление и оценку имеющихся средств, выявление уязвимостей и угроз, определение вероятности их возникновения и оценку воздействия (последствий).

3. Инструктивный материал по контролю или защите, включая управление сетевым оборудованием, управление авторизованным и неавторизованным программным обеспечением, базовую конфигурацию для мобильных устройств, портативных компьютеров, настольных компьютеров, серверов, непрерывный процесс идентификации и устранения уязвимостей, процессы и инструменты для идентификации, предотвращения и корректировки использования и настройки административных полномочий (сети/приложения), обслуживание, мониторинг и анализ результатов аудита, процедуры защиты электронной почты и маршрутизаторов, управление портами, протоколами и услугами в сетевых устройствах; процедуры, основанные

на соответствующих методологиях и инструментах для резервного копирования критически важной информации и тестирования восстановления; процедуры безопасного конфигурирования сетевых устройств (брандмауэров, маршрутизаторов и коммутаторов), защиты периметра; процедуры и инструменты защиты данных для предотвращения потери информации, смягчения последствий инцидентов и обеспечения конфиденциальности и целостности конфиденциальной информации; процедуры управления инцидентами и реагирования на них, а также другие средства контроля.

– КОНЕЦ –