Международная организация гражданской авиации

A41-WP/122[1]
TE/37
1/8/22

РАБОЧИЙ ДОКУМЕНТ

АССАМБЛЕЯ — 41-Я СЕССИЯ

ТЕХНИЧЕСКАЯ КОМИССИЯ

Пункт 31 повестки дня. Стандартизация в области безопасности полетов и аэронавигации

ОБНОВЛЕНИЕ СУЩЕСТВУЮЩИХ ЦЕЛЕЙ ОБУЧЕНИЯ ПО КИБЕРБЕЗОПАСНОСТИ ПЕРСОНАЛА ATSEP (ЭРТОС) И РАЗРАБОТКА НОВЫХ ЦЕЛЕЙ ОБУЧЕНИЯ ПО КИБЕРБЕЗОПАСНОСТИ ATSEP

(Представлено Международной федерацией ассоциаций по электронным средствам для обеспечения безопасности воздушного движения)

КРАТКАЯ СПРАВКА

В настоящем документе описывается предложение по обновлению существующих целей обучения кибербезопасности персонала по электронным средствам для обеспечения безопасности воздушного движения (ATSEP) и разработке новых целей обучения кибербезопасности в *Руководстве по основанной на компетенциях системе подготовки и оценки персонала по электронным средствам обеспечения безопасности воздушного движения (ATSEP)* (Doc10057).

Действия: Ассамблее предлагается:

a) обратить внимание на растущие роли и обязанности персонала ATSEP как части киберзащиты в интерфейсах со смежными зонами ответственности и новыми архитектурами ATM (УВД) и бизнес-моделями;

b) обратить внимание на постоянно меняющийся и динамичный характер киберугроз;

c) расставить приоритеты и предпринять все необходимые шаги в рамках процесса *Правил аэронавигационного обслуживания. Подготовка персонала* (PANS-TRG, Doc 9868) для обновления существующих целей обучения по кибербезопасности и разработки новых целей обучения кибербезопасности ATSEP как для базовых, так и для квалификационных целей подготовки персонала в документе Doc 10057, добавление B.

Стратегические цели	Данный рабочий документ касается стратегических целей "Безопасность полетов", "Аэронавигационный потенциал и эффективность", "Авиационная безопасность и упрощение формальностей"
Финансовые последствия	Возникнут некоторые расходы, связанные с обновлением и разработкой целей обучения по кибербезопасности в документе Doc 10057. Учебным подразделениям, отвечающим за базовую и квалификационную подготовку персонала ATSEP, возможно, придется адаптировать содержание учебных курсов с учетом обновленных или новых целей
Справочный материал	A39-WP/370, *Архитектурный подход к кибербезопасности для устаревших систем CNS/ATM, а также систем на базе SWIM* Приложение 10, *Авиационная электросвязь*, тома I, II, III и IV Doc 10057, *Руководство по основанной на компетенциях системе подготовки и оценки персонала по электронным средствам обеспечения безопасности воздушного движения (ATSEP)* Doc 9868, *Правила аэронавигационного обслуживания. Подготовка персонала (PANS-TRG)*

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

1. ВВЕДЕНИЕ

1.1 Системы CNS/ATM претерпевают смену парадигмы с внедрением новых технологий, концепций и бизнес-моделей. Интегрированная модель ANS будет заменена распределенной сервис-ориентированной архитектурой (SOA), а обмен информацией будет осуществляться вне сетей, таких как SWIM. Аэронавигационные системы. Сервис будет осуществляться на земле и в космическом пространстве, и даже обработка данных ATM (УВД) может проводиться в системах, развернутых в распределенных архитектурах и разделенных географически (например, европейские ADSP и виртуальные центры УВД). Гибридные конфигурации систем CNS быстро вступают в строй во всей авиационной экосистеме. Если интерфейсы взаимосвязи систем авиаотрасли между заинтересованными сторонами не будут должным образом рассмотрены с точки зрения кибербезопасности, могут возникнуть уязвимости в системе или элементе системы у одного из участников авиаотрасли. Хотя эти уязвимости не представляют серьезного риска для самой системы, они могут легко перерасти в угрозу, которая представляет риск для системы другого участника отрасли, с негативными последствиями. Требуется создать слой данных ATM (УВД) между участниками авиаотрасли в сфере ANS и внешними заинтересованными сторонами.

1.2 В главе 7 Стратегии ИКАО по авиационной кибербезопасности от октября 2019 г., относительно вопросов подготовки персонала, содержится следующая информация: "Надлежащая профессиональная подготовка должна предоставляться на постоянной основе для поддержания персонала в его повседневной роли", и "Кибербезопасность может быть включена в стратегию для следующего поколения авиационных специалистов, поскольку ИКАО имеет все возможности для работы с государствами и отраслью в целях развития требований компетентности авиационных специалистов на базе ролей". Так, в проекте доклада ИКАО A40-WP/577, пункт 30.36, говорится, что "специальное Руководство по кибербезопасности может быть рассмотрено для будущих обновлений документа Doc 10057".

1.3 Персонал ATSEP представляет собой основных специалистов в рамках ANSP, которые тактически решают проблемы кибербезопасности в случае удаленных сетевых угроз или угроз через спутниковые сигналы. В этом случае они несут ответственность за определение и разграничение технических сбоев и кибератак. Общим для этих служб является ввод и вывод из эксплуатации, принятие в работу и списание аппаратного и программного обеспечения персоналом ATSEP (ЭРТОС). Для обеспечения лучшей защиты систем ATM (УВД), как описано выше, эти специалисты также имеют авторизованный доступ к техническим системам ATM/ANS, и должны находиться в местах расположения интерфейсов.

1.4 Работники ATSEP играют все более важную роль в защите этих критически важных интерфейсов (ИКАО A39. WP17 EX / 5). Например, большинство стран создали или начинают создавать компьютеризированные группы реагирования на чрезвычайные ситуации (CERT), ответственность за которые несет персонал ATSEP. Тем не менее, условия подготовки ATSEP, содержащиеся в текущей версии документа ИКАО Doc 10057, главным образом рассматривают требования объектовой безопасности, в то время как кибербезопасность, особенно в отношении изменений парадигмы, выдвинутых программами SESAR и NextGen, включая видение системы ATM (УВД) со стороны CANSO, не рассматривается. По вышеуказанным причинам, существует явная необходимость в расширении программы подготовки ATSEP в контексте кибербезопасности, чтобы персонал мог приобрести соответствующий уровень квалификации для тактического и стратегического реагирования на киберсобытия.

1.5 Как известно по опыту Европы, обеспечение безопасности требует не только системы управления безопасностью у провайдеров ATS. NPA 2019/07 требует наличия интегрированной системы ISMS (Integrated Security Management System) для всех ATM /ANS и сопутствующих сервисов, есть много дополнительных интерфейсов, что также правильно, поскольку речь идет о различной нормативной документации и действиях по обслуживанию систем/оборудования. Тем не менее, появление темы кибербезопасности и отношение к данной теме при подготовке персонала ATSEP во всем мире, в лучшем случае является недостаточным, а в худшем – необходимые действия не предпринимаются.

1.6 Чтобы понять влияние кибератак на отдельные части сети ATM (УВД), недостаточно иметь профессиональные знания IT-технологии и IP-сетей. Поскольку различные сети представляют собой не только физические подключения, но и информацию, элементы управления и сигналы, вызванные различными факторами и использующие различные способы передачи, такие как радио, VoIP, сети, человеческие команды, световые знаки и сигналы, звуки и т. д., также требуется глубокое понимание действий по управлению кибербезопасностью и их влияния на безопасность ATM (УВД). Также персоналу необходимо иметь опыт работы в аэронавигации.

1.7 Поэтому, предлагается переориентировать и расширить содержание программы подготовки персонала ATSEP (ЭРТОС) в документе Doc 10057 внутри систем ATM/ANS, которая предусматривает наличие у подготовленного персонала достаточного опыта в области аэронавигации и владения компьютерной техникой, для противостояния угрозам кибератак на тактическом и стратегическом уровне.

2. ОБСУЖДЕНИЕ

2.1 Существующие цели подготовки персонала, содержащиеся в Руководстве по подготовке ATSEP (ИКАО DOC 10057, второе издание, 2020) в отношении кибербезопасности, должны быть пересмотрены, обновлены, и, при необходимости, созданы новые цели обучения, на уровне как базовой, так и квалификационной подготовки, с акцентом на элементы кибербезопасности самой информации и ICT (информационно-коммуникационных технологий), основанные на современных реалиях и, в некоторых случаях, на противостоянии комбинированным атакам в области IT и спутниковых сигналов.

2.2 IFATSEA готова оказать помощь ИКАО в разработке программы подготовки по кибербезопасности для персонала ATSEP.

— КОНЕЦ —