Международная организация гражданской авиации

РАБОЧИЙ ДОКУМЕНТ

A40-WP/105[1]
TE/33
30/7/19

АССАМБЛЕЯ — 40-Я СЕССИЯ

ТЕХНИЧЕСКАЯ КОМИССИЯ

Пункт 30 повестки дня. Прочие вопросы для рассмотрения Технической комиссией

ВНЕДРЕНИЕ ЦИФРОВОЙ АВИАЦИИ ПОСРЕДСТВОМ РАЗВИТИЯ КИБЕРСРЕДСТВ ПЕРСОНАЛА ПО ЭЛЕКТРОННЫМ СРЕДСТВАМ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ВОЗДУШНОГО ДВИЖЕНИЯ (ATSEP)

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

КРАТКАЯ СПРАВКА

Новое поколение оперативного персонала, экипажей и диспетчеров УВД (ATCO) будет в значительной степени полагаться на технические и управленческие возможности ATSEP для противостояния киберугрозам информационным системам и инфраструктурам связи, навигации и наблюдения (CNS), защищающим путешественников. Обязательства со стороны государств по определению критических инфраструктур и созданию Группы быстрого компьютерного реагирования частично покрываются личной ответственностью авиадиспетчеров и персонала ATSEP. Это также прикрывается на стыках критически важных инфраструктур. Если происходит кибератака на более широкую инфраструктуру, поддерживающую организацию воздушного движения (ОрВД), персонал ATSEP выполняет четкую роль по координации восстановления систем, обеспечивая безопасность ОрВД.

Действия: ИФАТСЕА призывает Ассамблею отметить информацию, содержащуюся в настоящем рабочем документе, и просит Совет ИКАО предпринять необходимые шаги для развития нового направления в работе ATSEP по безопасности и противодействию киберугрозам, наряду с соответствующими программами подготовки.

Стратегические цели	Настоящий документ относится к вопросам безопасности полетов, возможностям, эффективности и безопасности аэронавигации, а также к вопросу способствования достижению стратегических целей
Финансовые последствия	Стоимость развития нового направления работы ATSEP ожидается минимальной, поскольку просто расширяет действующее внедрение программы подготовки персонала, описанной в документе Doc 10057
Справочный материал	Приложение 10 *"Авиационная электросвязь"*, тома I, II, III и IV Doc 8071, *Руководство по испытаниям радионавигационных средств* Doc 9683, *Руководство по обучению в области человеческого фактора* Doc 9868, *Правила аэронавигационного обслуживания. Подготовка персонала* (PANS-TRG) Doc 10057, *Руководство по квалификационной системе подготовки и оценки персонала по электронным средствам для обеспечения безопасности воздушного движения*

[1] Документы на русском, английском, арабском, испанском, китайском и французском языках представлены ИФАТСЕА.

1. ВВЕДЕНИЕ

1.1 По всему миру существуют планы развития новых инфраструктур, поддерживающих организацию воздушного движения; включая, но, не ограничиваясь, авиатранспортную систему нового поколения (NextGen) и ОрВД в условиях единого европейского неба (SESAR). Все эти планы базируются на сильно зависимом процессе цифровой обработки данных и методологии связи. Безопасное и успешное развитие этих крупных и сложных инфраструктур ставит многочисленные вызовы перед отраслью, включая необходимость интеграции новых технологий в устаревшие системы. Эти великолепные совместимые технологии, основанные на цифровых системах ОрВД, по своей сути опираются на кибербезопасность, чтобы обеспечить целостность и безопасность воздушного движения. Это, в свою очередь, требует наличие персонала по электронным средствам для обеспечения безопасности воздушного движения (ATSEP) с новым развивающимся набором навыков. Понятно, что природа киберугроз в авиации со временем изменится. Настоящий документ предлагает практический, системный подход к развитию программ подготовки, педагогики, и оценки компетенции, с задействованием нового поколения персонала, способного реализовать наше совместное видение цифровой авиации.

2. РАССМОТРЕНИЕ ВОПРОСА

Безопасность полетов и авиационная безопасность при ОрВД/ANS

2.1 Новые регулятивные документы (US PPD-21, EU 2016/1148) в большей степени требуют от государств определения их критически важных инфраструктур, и определения растущей взаимозависимости между ними. Например, между цифровыми телекоммуникациями и системами УВД.

2.2 В настоящее время многие поставщики аэронавигационного обслуживания (ПАНО) испытывают недостаток с опытом работы в области кибербезопасности; это естественно, принимая во внимание, что в прошлом уровень угроз был очень низким. Часто у них не было достаточного количества квалифицированного персонала. Многие ПАНО решали этот вопрос, нанимая в аутсорсинг консультантов по кибербезопасности. Зачастую такие контракты доставались компаниям, не имеющим отношения к авиации, и не обладающим соответствующим уровнем понимания специфики отрасли, который необходим для поддержки уровня безопасности и стабильности работы. Сторонним консультантам может быть сложно убедить авиадиспетчеров в потенциальной угрозе работе из-за вирусного ПО, пересекающего "воздушный слой" по пути к системам, изолированным от общественного Интернета. Поэтому, аутсорсинг-компании часто оказывают очень ограниченное воздействие на надежность защиты многих стран от киберугроз. Более того, развитие сильной культуры безопасности наиболее эффективно, когда является "домашней" разработкой. В структуре поставщиков обслуживания воздушного движения (ОВД) аутсорсинг-компаниям не хватает влияния на ATSEP, который отвечает за технические системы, и на авиадиспетчеров, которые зависят от систем, обеспечивающих воздушное движение.

2.3 Персонал ATSEP обладает исключительно важной ролью в защите этих критических интерфейсов (ICAO A39.WP17 EX/5). Например, большинство стран развивают или начинают развитие групп реагирования на случаи нарушения безопасности компьютерных сетей (CERT), которые попадают в зону ответственности диспетчеров и ATSEP. Однако отношение к вопросам кибербезопасности в программе подготовки персонала ATSEP в лучшем случае является недостаточным, а в худшем – носит случайный характер.

Политические и регулятивные основания

2.4 Важность этих вопросов была признана и закреплена в ряде инструментов. Они включают аспекты сервисов Федерального авиационного управления (Соединенные Штаты Америки) (FAA) (FENS), а также регулятивные требования EC No 300/2008 Европарламента и Совета Европы от 11 марта 2008 года, об общих требованиях в сфере безопасности гражданской авиации. В других регионах мира существует опасность, связанная с тем, что страны могут даже отставать в области кибербезопасности. Есть потребность в более широком руководстве по соответствующим мерам защиты нашего общего будущего в инфраструктурах цифровой авиации, особенно когда регулятивные требования EC No 1254/2009 позволяют государствам – членам Евросоюза частично уйти от общих стандартов в гражданской авиации, и принять альтернативные меры безопасности. Важность такого четкого видения также была упомянута Генеральным Секретарем ИКАО д-ром Фан Лю на форуме ICAO-EASA 21 сентября 2018 года.

3. ВЫВОДЫ

3.1 Предложение концепции по направлению работы ATSEP в сфере безопасности, кибербезопасности, и соответствующей подготовки персонала.

3.2 Мы предлагаем создать новое направление в работе ATSEP, посвященное вопросам безопасности и кибербезопасности, для усиления существующих знаний персонала об авиационных инфраструктурах с четким базовым пониманием угроз и средств защиты этих инфраструктур от этих угроз. Мы предвидим уровень компетенции, который захватывает перекрестные сферы в других критически важных инфраструктурах; это повысит устойчивость авиации к угрозам; эта устойчивость основывается на расширенных схемах безопасности, использующих цифровые технологии массового рынка, хорошо известные хакерам и государственным агентствам.

3.3 Мы поднимаем этот вопрос потому, что различные государства – члены ЕС предпринимают радикально отличающиеся подходы к инженерии кибербезопасности в отрасли ОрВД, даже с учетом того, что все мы полагаемся на соседние страны в поддержании функционирования транспортных сетей.

3.4 Более того, ИФАТСЕА предлагает учредить новую ветвь программ подготовки в сфере кибербезопасности, где стартовая квалификация должна быть определена в сотрудничестве между странами или провайдерами аэронавигационных услуг, с общей целью повышения доверия и надежности авиационных инфраструктур соседних государств, поскольку они будут защищены высококвалифицированным персоналом ATSEP.

3.5 В дополнение, ИФАТСЕА предлагает ИКАО свою помощь в вопросах, касающихся подготовки ATSEP, внедрения и эксплуатации технического функционала и систем.

— КОНЕЦ —