Международная организация гражданской авиации

A41-WP/421[1]
TE/161
2/8/22

РАБОЧИЙ ДОКУМЕНТ

АССАМБЛЕЯ — 41-Я СЕССИЯ

ТЕХНИЧЕСКАЯ КОМИССИЯ

Пункт 33 повестки дня. Прочие вопросы, подлежащие рассмотрению Технической комиссией

РАЗРАБОТКА СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ПРИМЕНИТЕЛЬНО К АЭРОНАВИГАЦИОННОМУ ОБСЛУЖИВАНИЮ В ВЕНЕСУЭЛЕ

(Представлено Венесуэлой (Боливарианская Республика) при поддержке Доминиканской Республики, Коста-Рики и Панамы[2])

КРАТКАЯ СПРАВКА

Цель настоящего рабочего документа – представить краткую информацию о достижениях в области разработки и применения системы управления информационной безопасностью (СУИБ) в сфере аэронавигационного обслуживания (ANS), ходе работы и запланированных последующих шагах.

Действия: Ассамблее предлагается:

a) принять к сведению представленную информацию;

b) распространить информацию об инициативах по анализу факторов риска одновременно с информацией об инициативах по разработке СУИБ;

c) изучить вопрос о создании подгруппы по обмену знаниями, эксплуатационными характеристиками систем и опытом внедрения СУИБ применительно к ANS.

Стратегические цели	Данный рабочий документ связан со стратегическими целями "Безопасность полетов" и "Аэронавигационный потенциал и эффективность"
Финансовые последствия	

[1] Текст на испанском языке представлен Венесуэлой (Боливарианская Республика).
[2] Государства – члены Латиноамериканской комиссии гражданской авиации (ЛАКГА).

Справочный материал	Приложение 17 *"Безопасность. Защита международной гражданской авиации от актов незаконного вмешательства"* (пп. 4.9.1–4.9.2) Doc 10075, *Действующие резолюции Ассамблеи (по состоянию на 6 октября 2016 года)* (резолюция A39-19, стр. 91–93) CSA 43-107 и 45-107 Национальный план обеспечения безопасности полетов гражданской авиации (PNSAC) Стандарты ИСО серии 27000 Законы и правила Венесуэлы

1. ВВЕДЕНИЕ

1.1 В соответствии с рекомендациями ИКАО, изложенными в Приложении 17, а также согласно другой передовой практике, установленной стандартами ИСО серии 27000 в отношении внедрения системы управления информационной безопасностью (СУИБ), технического обслуживания этой системы и управления ею, была начата оценка информационно-коммуникационных систем и критически важных данных, используемых в сфере ANS, направленная на определение факторов риска и мер, которые необходимо принять с учетом конкретных характеристик и местоположения каждой из этих систем. Таким образом было установлено, какие элементы являются наиболее важными и в каких местах имеются пробелы, с тем чтобы можно было принять соответствующие меры для предотвращения неправомерного использования этих пробелов.

1.2 В рамках разработки СУИБ была создана целевая группа в составе представителей каждой оперативно-технической области (радиолокаторы, электросвязь, радионавигационные средства и аэронавигационные сообщения) для изучения любых/возможных уязвимых мест и обсуждения наиболее эффективных способов их уменьшения и предотвращения тем самым возможных инцидентов. В этих целях был проведен обмен знаниями и были созваны совещания исследовательских групп по наращиванию потенциала в области сетевых технологий и кибербезопасности.

2. РАССМОТРЕНИЕ ВОПРОСА

2.1 Одним из основных аспектов СУИБ является процесс формирования культуры кибербезопасности, адаптированной к системам аэронавигационного обслуживания, которая формируется одновременно с анализом технических рисков, проводимым не только на основе выхода из строя аппаратных средств, но также и с учетом возможных системных атак, обусловленных цифровизацией и интеграцией систем и видов обслуживания.

2.2 Кроме того, крайне важно использовать людские ресурсы соответствующих служб (инженеров в области электросвязи, компьютерной техники, электроники и т. д.), которые должны быть готовы разрабатывать, совершенствовать и изучать меры кибербезопасности, адаптированные к видам обслуживания. Целевая группа должна провести повторную оценку многих стратегий обеспечения безопасности полетов, чтобы определить, какие из них являются эффективными и должны быть реализованы для поэтапного усовершенствования существующих стратегий.

2.3 Группы экспертов должны подтвердить важность проведения информационно-просветительских кампаний по кибербезопасности (семинары, инфографика и т. д.) не только для

технического персонала, но и для пользователей системы. Это будет способствовать дальнейшему формированию культуры кибербезопасности, призванной обеспечить осведомленность технических и оперативных рабочих групп о новых факторах риска.

2.4 Конечная цель разработки СУИБ заключается в создании подразделения по кибербезопасности, которое будет функционировать под административным управлением специалистов системы ANS и будет состоять из сотрудников, прошедших подготовку и курсы повышения квалификации в этой области знаний. Такой персонал будет играть ведущую роль в содействии решению вопросов обеспечения кибербезопасности системы и разработке соответствующих инструктивных указаний после того, как системы начнут взаимодействовать с другими сетями.

2.5 Одним из первых шагов, которые необходимо предпринять, является назначение руководителя среднего звена по информационно-коммуникационным технологиям (ICT), которому будет поручено создать рабочую группу и собрать необходимую информацию о разработке СУИБ и о документах, которые должны быть подготовлены. Однако важно отметить, что успешность фактического применения вышеупомянутых мер зависит от активной совместной работы с участием старших руководителей подразделений ANS, руководителей по техническому обслуживанию, специалистов по техническим аспектам системы и руководителя по вопросам ITC.

2.6 Внедрение СУИБ должно сопровождаться информационно-разъяснительной кампанией по кибербезопасности для технического, оперативного и административного персонала аэронавигационных служб.

2.7 Еще одним важным фактором после установления процессов и процедур является моделирование сценариев возможных атак, что позволяет техническим специалистам изучать эти явления, экспериментировать и применять необходимые меры безопасности для предотвращения или уменьшения последствий. Такое моделирование будет проводиться в безопасной среде, изолированной от основных систем.

3. ЗАКЛЮЧЕНИЕ

3.1 Разработка СУИБ предполагает признание критической важности каждой области в целях надлежащего распределения ресурсов и усилий по созданию основы для обеспечения непрерывности обслуживания.

3.2 Анализ рисков позволяет выявить уязвимые места, связанные не только с техническими аспектами, но также с человеческим фактором/эксплуатационными аспектами, что подтверждает важность проведения такого анализа. Полученные результаты могут использоваться для выявления скрытых факторов риска и разработки более эффективных мер по проведению такого анализа, в основном касающихся каждого отдельного вида обслуживания или объекта.

3.3 Создание многопрофильной группы специалистов ANS имеет основополагающее значение для передачи знаний о соответствующих стратегиях обеспечения безопасности полетов, распространения информации о таких стратегиях и их реализации с уделением особого внимания вопросу уменьшения факторов риска. Кроме того, информационно-разъяснительные кампании помогут повысить уровень информированности о кибербезопасности, поскольку этот вопрос оказывает воздействие не только на организации/предприятия, но также и на повседневную жизнь.

3.4 Создание региональных/международных групп по кибербезопасности будет способствовать оказанию поддержки государствам и получению информации об их опыте благодаря обмену информацией о закупках оборудования, поставщиках услуг по обеспечению кибербезопасности, выявленных уязвимых местах и методах их устранения. В настоящее время, когда число кибератак ежедневно растет, эта мера рассматривается в качестве важной возможности для развития этой области и укрепления отношений сотрудничества и взаимопомощи между государствами.

— КОНЕЦ —