Международная организация гражданской авиации

AN-Conf/14-WP/124[1]
29/6/24

РАБОЧИЙ ДОКУМЕНТ

ЧЕТЫРНАДЦАТАЯ АЭРОНАВИГАЦИОННАЯ КОНФЕРЕНЦИЯ

Монреаль, Канада, 26 августа – 6 сентября 2024 года

Пункт 4 повестки дня. Гиперсвязность аэронавигационной системы
4.2. Кибербезопасность и устойчивость информационных систем

НОРМАТИВНЫЕ ИНСТРУКТИВНЫЕ МАТЕРИАЛЫ ПО КИБЕРБЕЗОПАСНОСТИ ДЛЯ ОБСЛУЖИВАНИЯ ВОЗДУШНОГО ДВИЖЕНИЯ (ОВД)

(Представлено Аргентиной при поддержке 19 государств – членов Латиноамериканской комиссии гражданской авиации (ЛАКГА)[2])

КРАТКАЯ СПРАВКА

В этом документе представлены соображения по согласованию нормативных положений по обслуживанию воздушного движения (ОВД) с целью включения спецификаций, методов и процедур, касающихся возможных сценариев вредоносных атак на органы ОВД, чтобы обеспечить постоянный мониторинг первоначального обучения и переподготовки персонала.

Конференции предлагается:

a) поддерживать инициативы, представленные в настоящем рабочем документе, запросив при этом анализ целесообразности включения правил и методов обеспечения кибербезопасности для ОВД в глобальную авиационную систему;

b) рекомендовать государствам согласовать свои национальные стратегии в области кибербезопасности со стратегиями ИКАО в области гражданской авиации в целях формирования культуры кибербезопасности в области ОВД, включающей политику, стратегии и механизмы обеспечения кибербезопасности, посредством разработки предлагаемых нормативных положений.

1. ВВЕДЕНИЕ

1.1 Растущее использование современных и глобально взаимосвязанных технологий в гражданской авиации привело к заметному увеличению риска киберугроз.

1.2 41-я сессия Ассамблеи Международной организации гражданской авиации (ИКАО) признала важность этой проблемы, включив резолюцию A41-19 Ассамблеи, озаглавленную *Решение проблем кибербезопасности в гражданской авиации*, в *действующие резолюции Ассамблеи (по состоянию на 7 октября 2022 года)* (Doc 10184), часть VII *Незаконное вмешательство; Прочие вопросы, относящиеся к незаконному вмешательству*. Резолюция призывает государства принять ряд мер; к некоторым из этих действий следует подходить с использованием инструментов регулирования, тем самым решая текущие проблемы в авиационном сообществе, касающиеся эффективности существующих стандартов, процедур и процессов, когда речь идет о поддержании приемлемого уровня риска в цифровой среде.

[1] Текст на испанском языке предоставлен Аргентиной.

[2] Аргентина, Аруба (Королевство Нидерландов), Белиз, Венесуэла (Боливарианская Республика), Гватемала, Гондурас, Колумбия, Коста-Рика, Куба, Мексика, Никарагуа, Панама, Парагвай, Перу, Сальвадор, Уругвай, Чили, Эквадор и Ямайка.

1.3 Согласно статье, опубликованной в 2019 году группой ALLIANZ под названием "Risk Barometer: Top Business Risks" ("Барометр рисков: Основные риски для бизнеса") (цитируется в седьмом издании Глобального аэронавигационного плана (ГАНП, Doc 9750)), самыми серьезными видами *нарушения деятельности* (BI) являются кибератаки *с использованием программ-вымогателей*[3]. *WannaCry* и *Petya* – это два примера *программ-вымогателей*, используемых для атак на цифровые системы в Евросоюзе. Однако следует отметить, что согласно этой статье только 12 % киберинцидентов типа BI происходят в результате преступных кибератак, тогда как 88 % происходят из-за технических сбоев или ошибок, вызванных взаимодействием человека с системами.

1.4 Все заинтересованные стороны гражданской авиации прилагают значительные совместные усилия для обеспечения безопасности и защиты аэронавигационной системы от актов незаконного вмешательства, уделяя первостепенное внимание управлению рисками и киберустойчивости системы. В этом контексте органы регулирования гражданской авиации играют основополагающую роль, которая должна постоянно развиваться. Иными словами, помимо действующих правил, было бы полезно предложить масштабируемые, гибкие инновации, особенно с учетом новых разрабатываемых бизнес-моделей, в которых основное внимание должно уделяться бизнесу для бизнеса и/или бизнесу для потребителей[4]. Соответственно, правила должны устанавливать стандарты эффективности, необходимые для этого нового контекста, а не сохранять их предыдущую функцию детального определения отдельных технических компонентов.

1.5 Поэтому правила должны содействовать инновациям и поощрять их, соответствовать требованиям к характеристикам и поддерживать развитие аэронавигационной системы, а также обеспечивать мониторинг и контроль. С этой точки зрения новая парадигма регулирования во многих отношениях представляет собой переход от централизованной системы, предназначенной только для двух субъектов (государственного регулирующего органа и поставщика аэронавигационного обслуживания (ПАНО)), к распределенной скоординированной системе регулирования, которая предоставляет обслуживание, адаптированное к потребностям киберустойчивой инфраструктуры и выявленным потребностям пользователей.

2. РАССМОТРЕНИЕ ВОПРОСА

2.1 Учитывая вышесказанное, мы предлагаем ряд соображений, которые способствуют согласованию и гармонизации нормативных положений в области ОВД. Наша цель состоит в том, чтобы проанализировать предложение о включении спецификаций и процедур, относящихся к возможным сценариям вредоносных атак на информационные системы, при одновременном удовлетворении потребностей всех заинтересованных сторон и обеспечении постоянного надзора за первоначальным обучением и переподготовкой персонала, чтобы гарантировать, что сотрудники сохраняют необходимые навыки.

2.1.1 Сценарий кибератаки против гражданской авиации классифицируется как незаконное вмешательство в соответствии с резолюцией Ассамблеи A41-19 *Решение проблем кибербезопасности в гражданской авиации* и по причине ее криминального характера.

2.1.2 Технологические достижения и взаимосвязь аэронавигационных систем направлены на обеспечение безопасности полетов, но потенциально они создают условия, при которых незаконное вмешательство может затронуть не только воздушное судно, но и смежные системы ОВД.

---

[3] *Программы-вымогатели – разновидность вредоносных программ, которые шифруют архивы пользователя, а затем требуют выкуп для их восстановления.*

[4] *ГАНП онлайн. Новые и адаптированные бизнес-модели, ИКАО:* https://www4.icao.int/ganpportal/GanpDocument#/lessons/WWfUWzbjlhwCVRRkMTd9NRWaFjpHfZxp

2.1.3 Стандарты и Рекомендуемая практика (SARPS) Приложения 11 *Обслуживание воздушного движения* и методы, изложенные в документе *Правила аэронавигационного обслуживания. Организация воздушного движения* (PANS-ATM, Doc 4444), рассматривают проблему незаконного вмешательства как комплекс действий или процедур, которые применяются, если воздушное судно является или предположительно является объектом незаконного вмешательства.

2.1.4 В вышеупомянутых документах не рассматривается случай потенциальной атаки на смежные системы ОВД. Поэтому может быть важно включить в эти документы нормативные или технические инструктивные материалы ИКАО в отношении смежных систем ОВД, затронутых кибератаками, чтобы обеспечить адекватные процедуры для надлежащего реагирования на такие события. Мы предлагаем изучить сценарий незаконного вмешательства в системы ОВД, чтобы выработать конкретные меры противодействия кибератакам.

2.1.5 Учитывая это и в соответствии с Планом действий ИКАО по обеспечению кибербезопасности, мы предлагаем проанализировать, целесообразно ли включать спецификации и/или процедуры для информирования уполномоченного государством компетентного органа в тех случаях, когда подозревается или подтверждается кибератака на смежные системы ОВД, что позволит обеспечить своевременный обмен соответствующей информацией между всеми заинтересованными сторонами, особенно эксплуатантами воздушных судов.

2.1.6 Более того, мы считаем, что важно создать механизмы обмена информацией о кибербезопасности между военными полномочными органами и органами ОВД, чтобы можно было обмениваться соответствующими данными. Такой совместный подход способствовал бы снижению риска кибератак на системы ОВД.

2.2 Кроме того, исходя из того, что в Плане действий по обеспечению кибербезопасности указывается задача *добиваться регуляторной гармонизации на глобальном, региональном и национальном уровне с целью способствовать глобальной согласованности и обеспечить интероперабельность мер защиты*[5], мы отмечаем необходимость включения конкретных нормативных положений, без ущерба для принятия других положений, связанных с этим вопросом, в том числе следующих:

a) процедуры, касающиеся киберугроз и сценариев кибератак на региональном уровне, поскольку такие процедуры позволят устранить экономические и технологические различия, которые некоторые государства не могут устранить самостоятельно, особенно с учетом того, что последствия кибератак или киберугроз обычно выходят за пределы государственных границ;

b) надлежащие инструменты для обеспечения связи между государственной стратегией в области обеспечения кибербезопасности и инструктивными материалами ИКАО, изложенными в *Стратегии в области авиационной кибербезопасности,* что позволит включить политику, стратегию, обучение и расходы, связанные с реализацией, в сферу национальной гражданской авиации. Кроме того, будет предусмотрено назначение компетентного органа по кибер-безопасности гражданской авиации и определен порядок его взаимодействия с национальными организациями и другими заинтересованными сторонами;

c) положения, касающиеся авиационной безопасности государственных аэронавигационных систем, архитектура которых обеспечивает их целостность

[5] *План действий по обеспечению кибербезопасности*, глава 3, Стратегический план действий, основополагающий элемент 1: Международное сотрудничество, ИКАО, издание 2022 года.

и защиту. Это может включать методы отчетности, контроля и проведения криминалистического анализа[6] киберинцидентов, характерных для гражданской авиации;

d) положения о подготовке кадров для продвижения культуры кибербезопасности в области ОВД и обеспечения надлежащей подготовки всего персонала, задействованного в аэронавигационной системе. В этой связи было бы важно предусмотреть проекты по подготовке указанного персонала;

e) конкретные меры в области ОВД, предпринимаемые в чрезвычайных ситуациях для преодоления этих ситуаций и обеспечения быстрого восстановления деятельности, включая действия по восстановлению в случае киберинцидентов и определение ключевых заинтересованных сторон для эффективной коммуникации и координации во время кризиса;

f) протоколы обнаружения и оповещения о киберинцидентах, устанавливающие четкие процедуры раннего обнаружения и своевременного оповещения о любом инциденте в области кибербезопасности, затрагивающем системы ОВД. Это обеспечило бы быстрое и скоординированное реагирование на любую угрозу, тем самым снизив потенциальное влияние кибератак на безопасность полетов и непрерывность воздушных перевозок.

3. ВЫВОД

3.1 Обеспечение кибербезопасности в области ОВД является проблемой, требующей скоординированных действий на национальном, региональном и глобальном уровнях. Внедрение предложений, изложенных в этом документе, представляет собой значительный шаг к повышению авиационной безопасности и снижению рисков, связанных с кибератаками на системы ОВД. Приняв эти подходы, государства стали бы лучше подготовлены к решению возникающих проблем кибербезопасности, одновременно обеспечивая непрерывность и целостность воздушных перевозок. Кроме того, международное сотрудничество и гармонизация нормативных актов будут способствовать продвижению надежной и устойчивой культуры кибербезопасности во всем мировом авиационном сообществе.

3.2 Поэтому Конференции предлагается утвердить следующие действия:

a) поддержать инициативы, представленные в настоящем рабочем документе, запросив при этом анализ целесообразности включения правил и методов обеспечения кибербезопасности для ОВД в глобальную авиационную систему;

b) рекомендовать государствам согласовать свои национальные стратегии в области кибербезопасности со стратегиями ИКАО в области гражданской авиации в целях формирования культуры кибербезопасности в области ОВД, включающей политику, стратегии и механизмы обеспечения кибербезопасности, посредством разработки предлагаемых нормативных положений.

— КОНЕЦ —

[6] Криминалистический анализ в области кибербезопасности – это дисциплина, используемая для расследования и анализа инцидентов в области информационной авиационной безопасности. К ним относятся кибератаки, хищение данных и взлом систем.