Международная организация гражданской авиации

РАБОЧИЙ ДОКУМЕНТ

AN-Conf/13-WP/270
28/9/18
English, Arabic, Chinese[1], French, Russian and Spanish only[2]

ТРИНАДЦАТАЯ АЭРОНАВИГАЦИОННАЯ КОНФЕРЕНЦИЯ

Монреаль, Канада, 9–19 октября 2018 года

КОМИТЕТ A

Пункт 5 повестки дня. Возникающие проблемы
5.4 Киберустойчивость

КОНЦЕПЦИЯ СИСТЕМЫ СИСТЕМ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В АВИАЦИИ

(Представлено Канадой, Австрией от имени Европейского союза и его государств-членов[3] и других государств – членов Европейской конференции гражданской авиации[4], ЕВРОКОНТРОЛем, Сингапуром и поддержано Австралией и Новой Зеландией)

КРАТКАЯ СПРАВКА

Данный документ коротко представляет концепцию системы систем, а также обоснование, почему такой подход был бы предпочтителен в контексте относящимся к вопросам кибербезопасности в гражданской авиации. Этот документ также предлагает подход по безопасному дизайну и интеграцию такой концепции в авиационных системах, улучшающую их защиту.

Действия: Конференции предлагается согласиться с рекомендациями, содержащимися в п. 3.1.

1. ВВЕДЕНИЕ

1.1 Наличие точной информации и правильное функционирование систем критических в смысле безопасности являются исходной позицией для безопасности и надежности авиационной системы как сектора, включающего дальнейшее развитие цифровой техники. Авиационная

[1] Документ на китайском языке представлен Сингапуром.
[2] Документы на русском, английском, арабском, испанском и французском языках представлены Канадой.
[3] Австрия, Бельгия, Болгария, Венгрия, Германия, Греция, Дания, Ирландия, Испания, Италия, Кипр, Латвия, Литва, Люксембург, Мальта, Нидерланды, Польша, Португалия, Румыния, Словакия, Словения, Соединенное Королевство, Финляндия, Франция, Хорватия, Чешская Республика, Швеция и Эстония.
[4] Албания, Армения, Азербайджан, Босния и Герцеговина, Грузия, Исландия, Республика Молдова, Монако, Черногория, Норвегия, Сан-Марино, Сербия, Швейцария, Бывшая югославская Республика Македония, Турция и Украина.

система является глубоко интегрированной, и информация распределяется глобально. Исходя из этого, инициативы в авиационном секторе должны быть всеобъемлющими и законченными.

1.2 Всеобъемлемость, завершенность могут быть только успешными если авиация видится как "система систем", для которой все члены авиационного сообщества разделяют ответственность. Авиационная система развивается на многообразии цифровых сетей и компонентов, которые становятся все более взаимосвязанными и взаимозависимыми в смысле обмена цифровыми данными и информациями, в то время как члены авиационного сообщества такие как страны, авиакомпании и аэропорты, аэронавигационные службы и прочие должны доверять доступной информации и коммуникационным технологиям систем для их ежедневной работы.

1.3 Развитие управления систем обширной информации, появление авиационных систем дистанционного управления и сложные ситуации для будущих пользователей авиационного пространства и заинтересованных сторон, – все это является будущим дальнейшим усилением этой всеобъемлющей зависимости. Авиационная система будущего предполагает более нацеленный дизайн и менее индивидуальную эволюцию, включая киберзащиту.

1.4 Эволюция навстречу взаимосвязанным и взаимоиспользуемым информационным системам, упомянутая до этого, откроет новые уязвимые области. Киберсобытия могут коснуться многих сторон авиации и могут угрожать корректному функционированию аэронавигационных систем и препятствовать общей безопасности авиационного сектора. Такие события могут повлиять на обмен информацией между заинтересованными сторонами напрямую, влияя на безопасность, защиту и эффективность с возможными различными последствиями.

2. РАССМОТРЕНИЕ ВОПРОСА

2.1 **Авиация как система систем.** В авиа секторе многие заинтересованные партии прямо и косвенно участвуют в функционировании и техобслуживании различных субсистем и систем как единое целое в том смысле, что под системой можно понимать продукты, людей и процессы. Каждая из этих субсистем связана напрямую с субсистемами, с тем чтобы они функционировали корректно и эффективно; и наоборот, каждая из этих субсистем также имеет существенное влияние на другие, если она функционирует неправильно.

2.2 Сегодня такие субсистемы сконструированы, интегрированы, используемы и управляемы независимо одна от другой, и развиваются индивидуальными путями, что ведет к общему эволюционному процессу, который очень сложно предвидеть и представить предсказуемо. Начиная с того времени, когда авиационные партии взяли на себя общую ответственность по системе всего продукта и, принимая во внимание авиацию как систему систем, – все это становиться намного важнее. Ответственность за функционирование авиационной системы, исходя из того, затрагивает все напрямую заинтересованные стороны, такие как владельцы/операторы самолетов и аэропортов, аэронавигационные службы, а также, косвенно, такие заинтересованные стороны, как государства и производители/конструкторы оборудования.

2.3 Исходя из того, что эти субсистемы служат индивидуальным функциям, которые объединены для достижения общих целей (например, коммуникация между авиадиспетчером и пилотом или передача данных траектории полета между центром управления и самолетом), ложное функционирование любой из этих субсистем могло бы негативно затронуть общее функционирование всей цепи таковых. Следовательно, киберриск менеджмент должен быть

направлен на использование общего подхода, с тем чтобы уменьшить доступность неавторизованным элементам к ключевым функциям.

2.4 **Кибербезопасность: современная, развивающиеся область требующая внимания.** Упомянутая выше эволюционная природа системы систем показывает, что кибербезопасность должна быть соответствующим образом учтена среди заинтересованных партий в авиационной системе систем. Также необходимо, чтобы авиационная система систем имела свои предписанные киберусловия, предоставляя необходимую гибкость и способность к адаптации, когда ее компоненты непрерывно влияют различным образом друг на друга (например, самолет взаимодействует с различными представителями аэронавигационной информации постольку-поскольку он пролетает различные регионы полетно-информационного сервиса).

2.5 Исходя из ранее упомянутого, разработка и техобслуживание киберподдержки во всей системе систем предписывает постоянную координацию среди всех заинтересованных сторон (см. п. 2.2) с целью иметь желаемую гибкость и способность к адаптации, с тем, чтобы авиационная система систем функционировала правильно.

2.6 Важный вызов, чтобы соответствовать выполнению этой задачи, является концепция "быть способным подходить" – способность интегрировать многочисленные элементы (отдельные компоненты для систем или же субсистемы в систему систем) в большие безопасные технические образования. Главная проблема при этом – уйти от привычного представления в отношении безопасности, при котором интегрирование элементов сконцентрировано на первом плане на их работоспособности и взаимной работе с другими элементами дизайна через общие интерфейсы. С точки зрения кибербезопасности, установка отдельных элементов также требует внимательного учета принципов кибербезопасности в отношении каждого элемента, от которого зависит состояние кибербезопасности в целом. Ключевой вопрос, который будет поставлен в достижении этой цели, как поддержать страны и регионы (и других отдельных участников авиационного сообщества) в их процессах по разработке технического дизайна таким образом, чтобы система систем могла быть эффективно защищена от кибератак, несмотря на возможные критические элементы дизайна, что существуют между субсистемами.

2.7 Для достижения ранее упомянутой цели, интегрирование отдельных субсистем должно обязательно предусматривать и интеграцию присущих условий безопасности специфических для каждой субсистемы в такой полноте, чтобы учесть всеобщую и киберзащищенную среду от опасных воздействий. Некоординированный подход к кибербезопасности мог бы также привести к существованию ненаблюдаемых незащищенных зон в дизайне защиты; избыточности функций защиты в общей системе защиты - и это только опасности начиная с того времени, когда сценарий становился бы потенциально возможным как область для атаки авиационной системы систем.

2.8 Поэтому глобально координированный подход по управлению системных воздействий является существенным, и ядром этой задачи является общее видение на то, как эти системы и субсистемы взаимодействуют.

2.9 **Интегрирующая безопасность посредством технического дизайна для авиационных систем.** Для того чтобы достичь желаемого уровня киберзащиты в авиационной системе систем для учета кибербезопасности, важно принимать участие уже в начале проектирования системы, или же альтернативно, быть учтенным позже, уже после начала проектирования. Это также позволило бы принять во внимание интерфейсы между субсистемами так, чтобы их взаимное влияние могло бы также быть учтено правильно и эффективно.

2.10 Большинство теперешних стандартов по безопасности сосредоточены на мероприятиях по уменьшению влияния, взятых и примененных в организационном контексте – существует насущная необходимость перевести фокус таких мероприятий на включение и принятие во внимание мер, которые должны быть предприняты также с точки зрения международной организационной перспективы. Это позволит поддержать всеобъемлющую безопасность системы систем, превосходящую безопасность существующую при смешивании субсистем, которые имеют индивидуальную защиту.

2.11 Без соответствующего менеджмента, нескоординированные подходы к кибербезопасности авиационных субсистем могут образовать риск для системы в целом. Такой недостаток координации также потенциально исходит от недостаточной коммуникации между менеджерами субсистем и другими важными "игроками" в процессе разработки и определения подходов по кибербезопасности.

2.12 Теперешние многочисленные участники координации (например, между государствами как руководителями своих национальных субсистем, и т. д.) по различным уровням субсистем, а также по установлению того, что каждая отдельно взятая субсистема эффективно защищена в смысле национальных предписаний, эти государства могли бы вносить больше в такую авиационную систему систем, которая имеет более высокую степень защиты, что было бы естественным результатом таковой работы.

2.13 **Будущая работа.** Такая работа по созданию безопасности предусмотренной в техническом дизайне как части базового дизайна системы не заменяла бы лучший опыт накопленный авиационным сообществом в течении длительного времени по работам в создании авиасистем и по деятельности в отношении вызовов, которые выдвигает кибербезопасность. При внедрении таких принципов наряду с тем и дополнительно к традиционным приоритетам по степени резервирования системы, а также с акцентом на простоту доступа к операционным данным и системам, заинтересованные партии будут в дальнейшем делать более сильной авиационную систему систем в отношении ее политики по уровню нагрузок, выдерживаемых киберзащитой, в то время как их операционная эффективность сохраняется.

2.14 Как часть многогранности операционных концепций и решений, дискутируемых на различных авиационных форумах, в настоящее время, важно для государств и индустрии принять во внимание ранее приведенные соображения в процессах разработки и конструирования. В дальнейшем сообщество может также привлечь к своей совместной работе установленных представителей субсистем, а также исследователей, с которыми поделятся результатами, базируясь на проведенных мероприятиях и лучшем опыте, они могут быть переданы другим субсистемам с целью улучшения кибербезопасности всей технической популяции.

2.15 Похожим образом, следуя успеху на этой арене, авиационное сообщество может принять инициативу по дальнейшей разработке растущих больших субсистем, которые учитывают информационную безопасность уже на начальном этапе проектирования. В процессе прогресса и роста зрелости такой работы, заинтересованные стороны могут начать коллективные исследования, существуют ли в наличии доверительные кандидаты, кто нес бы ответственность за разработку и поддержание таких систем, которые учитывают аспекты безопасности в своем дизайне и возможность внедрения таковых процессов в авиационной системе будущего.

2.16 В период участия и деятельности по усилиям на сцене улучшения киберзащиты системы, авиационное общество будет эффективно вносить вклад в безопасность и продуктивную деятельность авиационной экологической системы ("системы систем") также и в будущем.

3. ВЫВОД

3.1 Конференция приглашается поддержать следующие рекомендации:

Конференции предлагается:

а) настоятельно просить ИКАО и государства принять во внимание, что улучшение киберзащиты авиационных систем зависит от непрерывной координации между всеми важными заинтересованными сторонами;

б) просить ИКАО учесть концепцию системы систем, требующую необходимость совместной деятельности и координации среди менеджеров субсистем, в особенности, когда происходит разработка, интеграция, операционное использование и техподдержка субсистем, которые учитывают аспекты безопасности в своем дизайне;

в) настоятельно просить ИКАО создать рабочую сеть, которая обязует и ведет государства к внедрению мероприятий по ослаблению киберугрозы и риска для гражданских авиационных систем. Это может быть отражено в развитии Стандартов и Рекомендуемой практики (SARPS) в некоторых затронутых Приложениях ИКАО;

г) просить признать концепцию, содержащуюся в информационном листе *"Учитывание кибербезопасности в авиации"*.

— КОНЕЦ —