Международная организация гражданской авиации

AN-Conf/14-WP/125[1]
29/6/24

РАБОЧИЙ ДОКУМЕНТ

ЧЕТЫРНАДЦАТАЯ АЭРОНАВИГАЦИОННАЯ КОНФЕРЕНЦИЯ

Монреаль, Канада, 26 августа – 6 сентября 2024 года

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

КИБЕРБЕЗОПАСНОСТЬ ПРИ ОБСЛУЖИВАНИИ ВОЗДУШНОГО ДВИЖЕНИЯ (ОВД)

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

КРАТКАЯ СПРАВКА

В этом документе изложены соображения о разработке механизмов поддержки поставщиков обслуживания воздушного движения (ОВД) в управлении киберугрозами и киберсобытиями, а также в разработке эффективных стратегий смягчения последствий.

Действия: Конференции предлагается:

a) разработать руководящие механизмы для оказания помощи поставщикам обслуживания воздушного движения в управлении киберрисками, связанными с безопасностью полетов, в рамках их системы управления безопасностью полетов;

b) разрабатывать и/или внедрять технологии, процедуры и механизмы, позволяющие авиадиспетчерам безопасно предоставлять обслуживание воздушного движения (ОВД) и оперативно восстанавливать деятельность в случае киберсобытия;

c) определить компетенции и навыки, которые необходимы авиадиспетчерам для оценки киберсобытий и устранения последствий их влияния на предоставление ОВД в целях достижения киберустойчивости.

1. ВВЕДЕНИЕ

1.1 Ввиду роста киберугроз и кибератак в авиационной отрасли и поскольку одним из семи основополагающих принципов *Стратегии ИКАО в области авиационной кибербезопасности* и лежащей в ее основе *Политики в области кибербезопасности* является учет *вопросов кибербезопасности* в управлении авиационными рисками, как никогда важно определить и измерить то влияние, которое такие события оказывают на обслуживание воздушного движения (ОВД), несмотря на развитие новых технологий в области аэронавигации, которые позволяют лучше справляться с *киберсобытиями*.

[1] Текст на испанском языке предоставлен Аргентиной.

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

1.2 Поскольку авиационные системы тесно связаны друг с другом и с другими внешними системами, киберсобытия стали более далеко идущими и действенными и имеют потенциал для создания глобальных *разрушительных событий*[3]. Поэтому важно рассматривать *киберсобытия* как угрозы безопасности полетов или, по крайней мере, как источники и факторы, способствующие возникновению глобальных событий категории высокого риска (G-HRC), упомянутых в *Глобальном плане обеспечения безопасности полетов на 2023–2025 гг.* (Doc 10004, ГПБП). Более того, в документе *"Глобальная эксплуатационная концепция ОрВД"* (Doc 9854) отмечено, что решения, в том числе решения в отношении безопасности полетов, часто принимаются на основе различных критериев. Эта ситуация требует принятия соответствующих мер для достижения одного из ожидаемых результатов, упомянутых в добавлении E к документу 9854: *"за счет* [...] *расширенного определения опасных факторов появится возможность использования более стабильных траекторий"*.

1.3 Обслуживание воздушного движения осуществляется в более автоматизированной, цифровой и взаимосвязанной среде, которая делает его более уязвимым для *киберугроз* и *кибератак*. Использование связи "диспетчер-пилот" по каналу линии данных (CPDLC), интеграция беспилотных летательных аппаратов в контролируемое воздушное пространство, удаленные цифровые командно-диспетчерские пункты и аэродромные автоматизированные системы полетной информации (A-AFIS) – это лишь некоторые из изменений, которые свидетельствуют в пользу повышения осведомленности и принятия мер по устранению последствий *киберсобытий* при обеспечении ОВД.

1.4 Действительно, были достигнуты значительные успехи в предотвращении и/или смягчении последствий *киберсобытий*. Однако, по определению, такие события напрямую связаны с организацией воздушного движения / связью, навигацией и наблюдением (ОрВД/CNS) и информационными системами, и поэтому необходимы дополнительные усилия для срочного устранения воздействия киберсобытий на ОрВД.

1.5 Если подразделения ОВД не имеют системы адекватного контроля риска и защитных барьеров, они могут столкнуться с частичным нарушением обслуживания, "нулевыми" условиями управления воздушным движением (УВД) или даже инцидентами в области безопасности полетов, такими как потеря эшелонирования между воздушными судами в полете, что может привести к столкновению в воздухе (МАС) – происшествию, относящемуся к одной из пяти глобальных категорий высокого риска.

1.6 В разделе 4 *"Разработка политики в области кибербезопасности" Плана действий по кибербезопасности* (CyAP), подготовленного Исследовательской группой по кибербезопасности Секретариата ИКАО (SSGC), предусматриваются меры по управлению киберрисками. Исходя из этого, стоит переосмыслить способы управления рисками в области безопасности полетов в рамках УВД в глобальном контексте, который характеризуется как изменчивый, неопределенный, сложный и неоднозначный, а также все более уязвимый и нелинейный[4].

[3] Разрушительное событие: необычное и серьезное событие в национальном, региональном или глобальном масштабе, которое негативно влияет на авиацию. Такие события обычно не возникают из-за авиационной деятельности, но тем не менее могут оказать существенное влияние на полеты.

[4] Это определение взято из моделей для социальных наук, известных как *VUCA* (изменчивый, неопределенный, сложный, неоднозначный) и *BANI* (хрупкий, тревожный, нелинейный, непонятный), которые используются для объяснения текущих глобальных событий и которые могут применяться к любым областям исследования.

2. РАССМОТРЕНИЕ ВОПРОСА

2.1 В свете вышесказанного важно определить возможности для повышения потенциала и наращивания деятельности по обеспечению *кибербезопасности* при предоставлении ОВД.

2.2 Во-первых, важно еще раз посмотреть на растущую сложность эксплуатационного контекста, в котором предоставляется обслуживание воздушного движения, и пересмотреть роль и функции подразделений ОВД, особенно на стыке четырех комплексных систем управления, в которых требуется принятие мер: управление киберрисками, управление рисками для безопасности полетов, управление авиационной безопасностью и управление информационной авиационной безопасностью.

2.3 Кроме того, существует три аспекта, связанных с ОВД, для которых необходимо разработать и реализовать меры по смягчению последствий *киберсобытий:*

a) управление рисками для безопасности полетов в контексте обеспечения ОВД;

b) технические/эксплуатационные средства[5], используемые подразделениями ОВД для предоставления обслуживания;

c) навыки и компетенции, необходимые авиадиспетчерам (ATCO) для достижения киберустойчивости в своих подразделениях ОВД.

2.4 Что касается управления рисками для безопасности полетов в контексте ОВД, *киберугрозы* и *кибератаки* должны быть включены в систему управления безопасностью полетов (СУБП) поставщика обслуживания воздушного движения (ATSP). Компонент 2 СУБП, естественно, приобретает особую актуальность, поскольку опасности должны быть логически идентифицированы для управления связанными с ними рисками. Следовательно, важно понимать, что *киберугрозы* и *кибератаки* должны быть идентифицированы как таковые в качестве первого шага для регистрации их возникновения, измерения их воздействия на ОВД и оценки связанных с ними рисков.

2.5 Данный подход не должен ограничиваться выявлением опасностей, традиционно связанных с ОВД, а должен охватывать также опасности, связанные с информационными технологиями (ИТ), такими как сети, поддерживающие системы ATM/CNS подразделения ОВД, используемое программное обеспечение, серверы и аппаратные средства, а также другие соответствующие элементы. Поскольку технологии меняются скачкообразно, такой подход должен рассматриваться не как статичный, а как динамичный и адаптивный. Это повлечет за собой постоянный пересмотр и корректировку в соответствии с быстрым развитием технологий не только в эксплуатационной сфере, но и в контексте всей системы. Поэтому необходимо понимать, что как киберсобытие, так и инцидент могут превратиться в нарушение безопасности при обеспечении ОВД и выполнении полетов.

2.6 Что касается эксплуатационных инструментов, используемых подразделениями ОВД, то под ними понимаются технологии, процедуры и правила, которые необходимы авиадиспетчерам для безопасного обеспечения ОВД, а также для достижения киберустойчивости и быстрого восстановления деятельности после киберсобытия. По этой причине очень важно разработать механизмы, помогающие авиадиспетчерам быстро выявлять киберугрозы и принимать соответствующие меры.

[5] К ним относятся оперативные процедуры, компьютерные системы и другие средства ICT, наблюдение ОВД, связь и т. д.

2.7 Роль авиадиспетчеров изменилась, и способы их взаимодействия с элементами модели SHELL меняются в соответствии с новыми нормами. Симбиоз между людьми, аппаратным и программным обеспечением усилился и повысил подверженность воздействию *киберсобытий*. Поэтому необходимо развивать необходимые компетенции и навыки, чтобы диспетчеры в подразделениях ОВД могли обеспечить киберустойчивость и быть в состоянии справиться с различными сценариями *киберсобытий*.

3. ВЫВОД

3.1 С учетом вышеизложенного и принимая во внимание сквозной характер кибербезопасности в обеспечении ОВД, существует необходимость в механизмах для предоставления рекомендаций ATSP по включению *киберугроз* и методов управления *киберсобытиями* в их СУБП, а также в создании аналитических инструментов для разработки стратегий смягчения последствий и процедур раннего обнаружения, а также инструментов, помогающих диспетчерам принимать оперативные решения в ответ на *киберсобытия*.

3.2 Также целесообразно определить компетенции и навыки для авиадиспетчеров, чтобы они могли оценивать события в области кибербезопасности, которые могут повлиять на предоставление ОВД, и реагировать на них, а также повышать их ситуационную осведомленность о возможных последствиях и человеческом факторе.

3.3 Конференции предлагается:

a) разработать руководящие механизмы для оказания помощи поставщикам обслуживания воздушного движения в управлении киберрисками, связанными с безопасностью полетов, в рамках их системы управления безопасностью полетов;

b) разрабатывать и/или внедрять технологии, процедуры и механизмы, позволяющие авиадиспетчерам безопасно предоставлять обслуживание воздушного движения (ОВД) и оперативно восстанавливать деятельность в случае киберсобытия;

c) определить компетенции и навыки, которые необходимы авиадиспетчерам для оценки киберсобытий и устранения последствий их влияния на предоставление ОВД в целях достижения киберустойчивости.

— КОНЕЦ —