Международная организация гражданской авиации

AN-Conf/13-WP/42
28/8/18

РАБОЧИЙ ДОКУМЕНТ

ТРИНАДЦАТАЯ АЭРОНАВИГАЦИОННАЯ КОНФЕРЕНЦИЯ

Монреаль, Канада, 9–19 октября 2018 года

КОМИТЕТ A

Пункт 5 повестки дня. Возникающие проблемы
5.4. Киберустойчивость

СОВЕРШЕНСТВОВАНИЕ КОНЦЕПЦИЙ КИБЕРБЕЗОПАСНОСТИ В АВИАЦИИ

(Представлено Австрией от имени Европейского союза и его государств – членов[1], других государств – участников Европейской конференции гражданской авиации[2]; и ЕВРОКОНТРОЛем)

КРАТКАЯ СПРАВКА

В настоящем документе кратко представлены соображения, почему организациям следует управлять своими индивидуальными факторами риска, продуктами и услугами в области кибербезопасности на основе системы управления информационной безопасностью (ISMS), позволяющей учитывать факторы риска, связанные со взаимодействием данной организации с другими организациями или эксплуатируемыми ими системами.

В этом документе также затрагивается вопрос доверия, почему оно необходимо, и какие преимущества оно дает организациям, использующим ISMS. Кроме того, в этом документе также приводится объяснение важности обеспечения эквивалентного уровня кибербезопасности для систем связи независимо от времени и места, и предлагаются возможные способы решения этой задачи применительно к операциям "земля – земля" или "воздух – земля".

В этом документе также излагается общий взгляд на параметр критичности для авиации и изложены преимущества обмена информацией.

Действия:
Конференции предлагается согласиться с рекомендациями, приведенными в п. 3.

[1] 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.

[2] Азербайджан, Албания, Армения, Босния и Герцеговина, Бывшая югославская Республика Македония, Грузия, Исландия, Монако, Норвегия, Республика Молдова, Сан-Марино, Сербия, Турция, Украина, Черногория и Швейцария.

1. ВВЕДЕНИЕ

1.1 Наличие точной информации и надлежащее функционирование критически важных для безопасности полетов систем являются необходимым условием обеспечения безопасной деятельности гражданской авиации в связи с дальнейшим внедрением цифровых технологий в этом секторе. Авиационная система является высокоинтегрированной, и информация передается по всему миру. Следовательно, к инициативам по обеспечению кибербезопасности в авиационном секторе надлежит применять комплексный и всеобъемлющий подход.

1.2 В настоящем документе указаны преимущества внедрения систем управления информационной безопасностью (ISMS) в авиационном секторе. Такие системы управления, которые рекомендуется совмещать или объединять с имеющимися системами управления факторами риска для авиации, помогают отдельным организациям и сектору в целом лучше подготовиться к возникновению угроз в области информационной безопасности и более эффективно реагировать на них.

1.3 Общий подход к системе управления позволяет координировать меры в масштабе всего сектора с учетом факта осуществления обмена информацией, использования одних и тех же систем разными участниками сектора и наличия общих факторов риска.

1.4 Помимо ISMS в настоящем документе также рассматривается доверие как понятие. В авиационном секторе первостепенное значение имеет не только уверенность в каждом партнере, но и доверие к каждому партнеру. Как правило, придать всем партнерам уверенность в добросовестном и надлежащем выполнении каждым из них своих функций применительно к каждому полету позволяет надежная система подготовки персонала, сертификации, контроля и двойных проверок.

2. РАССМОТРЕНИЕ ВОПРОСА

2.1 **Принципы использования ISMS.** Существующие концепции ISMS по определению ограничены отдельными организациями. Однако гражданская авиация представляет собой такой комплекс тесно переплетенных систем, в который входят взаимосвязанные продукты, люди и процессы, включая даже связь с военными системами[3], и который нельзя рассматривать с точки зрения одной отдельной организации. В связи с этим в гражданской авиации необходимо внедрять ISMS на основе межорганизационного управления кибербезопасностью.

2.2 Таким образом, согласованный на глобальном уровне механизм на основе ISMS является одним из основных факторов, обеспечивающих функционирование гражданской авиации. Внедрение подобного глобального подхода будет способствовать последовательному осуществлению ряда вспомогательных концепций, включая глобальную интероперабельную и защищенную инфраструктуры связи, структуру доверия или другие концепции, обеспечивающие работу будущей системы на основе доверительного обмена информацией. Поскольку на строительство такой системы уйдет некоторое время, необходимо содействовать эволюционным изменениям в отдельных организациях, государствах или регионах. Непременным условием реализации этих концепций является внедрение ISMS во всех организациях. В ходе внедрения ISMS следует принять меры по обеспечению ее совместимости с существующими системами управления безопасностью полетов (например, предусмотренными в Приложении 19 *"Управление безопасностью полетов")* и системами управления факторами риска для авиационной безопасности, положениями ИКАО и отраслевыми стандартами, а также эффективными механизмами контроля.

[3] См. документ AN-Conf/13-WP/39

2.3 **Концепция доверия.** За несколько десятилетий в гражданской авиации была создана надежная структура доверия. В настоящее время структура доверия является официальной концепцией, согласно которой одна организация или эксплуатируемая ею система может полагаться на систему обеспечения кибербезопасности, принадлежащую другой организации или эксплуатируемой ею системе[4]. Поскольку доверие никогда не бывает абсолютным, в этой концепции предусмотрено несколько уровней доверия, которые зависят от воздействия (с точки зрения безопасности полетов или непрерывности обслуживания, например, оперативного управления воздушным движением в регионе) на доверяющую сторону.

2.4 Например, в области сертификации воздушных судов максимальная уверенность в летной годности достигается с помощью гарантий выполнения соответствующих действий для получения приемлемых результатов. Эти действия направлены на смягчение воздействия факторов риска для безопасности полетов. Более серьезным факторам требуется уделять более пристальное внимание в процессе разработки. В отношении систем обеспечения кибербезопасности предлагается применять аналогичную концепцию. Она должна обеспечивать эффективную защиту от киберугроз. В сущности, уверенность в отсутствии ошибок или уязвимых мест в разработанных системах или обеспечении организациями надлежащей защиты гражданской авиации имеет основополагающее значение для будущей деятельности по обеспечению безопасности полетов. Концепцию доверия следует включить в ISMS, которую, в свою очередь, рекомендуется совмещать или объединять с существующими системами управления.

2.5 **Условия эксплуатации средств обеспечения кибербезопасности.** В целях максимально эффективного использования концепции доверия необходимо учитывать также динамику эволюции отдельных организаций и эксплуатируемых ими систем, принадлежащих к глобальной интероперабельной защищенной инфраструктуре. Один из способов решения этой задачи заключается в предварительном определении условий эксплуатации средств обеспечения кибербезопасности. В каждом случае установления связи между равными пользователями основополагающее значение имеет их совместимость с точки зрения степени доверия, что обуславливает необходимость определения понятия "совместимая пара". Отдельные варианты соотношения степеней доверия отвечают критериям допустимости установления связи, поскольку они соответствуют требованиям в отношении кибербезопасности и приемлемых уровней риска. Другие варианты могут не соответствовать этим требованиям. Это обстоятельство станет стимулом для достижения пользователями соглашений об условиях совместимости для разного уровня доверия, что в итоге приведет к выработке сбалансированных подходов. Необходимо проводить различие между двумя уровнями установления связи между равными пользователями: к одному уровню относятся случаи установления связи между системами организаций, а ко второму – случаи установления связи между воздушными судами или космическими аппаратами и наземными системами, которые характеризуются быстрыми переключениями. Их основным отличительным признаком является скорость изменения условий в области кибербезопасности.

2.6 Медленные изменения. С одной стороны, все наземные системы, и в частности системы организации воздушного движения (ОрВД)/аэронавигационного обслуживания (ANS), развиваются относительно медленно. Изменение условий их эксплуатации в значительной степени определяется изменениями в их собственных механизмах обеспечения кибербезопасности или в подобных механизмах систем, к которым они подключаются. Это позволяет осуществлять тесное взаимодействие по адаптации средств обеспечения кибербезопасности, с тем чтобы все участники сеанса связи соответствовали общим требованиям в отношении кибербезопасности. В концепции

[4] Объяснение этих концепций и принципов ISMS, концепций доверия и условий эксплуатации средств обеспечения кибербезопасности, а также преимуществ обмена информацией будет представлено в информационном документе (AN-Conf/13-WP/160).

условий эксплуатации предусмотрено обеспечение надлежащего соотношения уровней доверия между устанавливающими связь организациями.

2.7 Быстрые изменения. С другой стороны, воздушные суда перемещаются из одного пункта в другой с относительно высокой скоростью и при этом динамично устанавливают связь со множеством систем в течении короткого периода времени. В принципе, однажды воздушные суда или системы ОрВД/ANS перестанут соответствовать друг другу с точки зрения кибербезопасности. Их дальнейшая эксплуатация потребует перехода на условия одной из сторон. В области кибербезопасности возможным решением этой проблемы является адаптация концепции условий эксплуатации. Например, согласно существующей концепции условий эксплуатации применимые в пределах одного воздушного пространства требования в отношении горизонтального эшелонирования обуславливают необходимость использования определенных наземных и бортовых систем, отвечающих этим требованиям. Таким образом, концепция условий эксплуатации могла бы служить основой для разработки системы обеспечения кибербезопасности с учетом предъявляемых к ней требований в отношении уровня доверия. Надлежащее соотношение уровней доверия между системами ОрВД/ANS и бортовыми системами позволит использовать воздушное пространство безопасным образом.

2.8 **Обмен информацией по вопросам кибербезопасности.** Еще одним важным аспектом ISMS является обмен информацией. Наличие глобальной ISMS могло бы также способствовать созданию более слаженного механизма обмена информацией о факторах риска для кибербезопасности. В мире информационных технологий (ИТ) была разработана концепция центра кибербезопасности, в задачи которого входит "обработка" информации об инцидентах в области кибербезопасности, включая составление и обновление баз данных об инцидентах, угрозах и уязвимых местах, а также предоставление членам этой организации аналитической поддержки и инструктивного материала по успешной практике в области реагирования на фактические инциденты. Эти задачи связаны с обменом информацией.

2.9 На международном уровне группами быстрого реагирования на компьютерные инциденты (CERT) и группами реагирования на инциденты в области компьютерной безопасности (CSIRT) было создано сообщество, которое называется Форум групп реагирования на инциденты и обеспечения безопасности (FIRST). Этот форум мог бы служить авиационному сообществу примером согласованного подхода к глобальному обмену информацией, ориентированного не только на реагирование на инциденты, но и на предотвращение будущих атак. В связи с выявлением новых уязвимых мест собранная CSIRT информация позволит с определенной точностью прогнозировать возникающие факторы риска и впоследствии принимать предупредительные меры по смягчению неблагоприятных последствий для гражданской авиации. Основная цель этой деятельности заключается в повышении осведомленности о киберугрозах и уязвимых местах авиационных систем. Необходимым условием осуществления согласованных на международном уровне мер по уменьшению киберугроз и защите от них является координация действий авиационных CSIRT и их членов.

2.10 Киберугрозы характерны не только для гражданской авиации, но и для других транспортных и нетранспортных секторов (например, для банковской системы, атомной отрасли). В этих секторах широко распространены обмены технологиями и способами их внедрения, что является причиной возникновения угроз и уязвимых мест. Следовательно, важно обмениваться стратегиями, оперативной информацией и передовой практикой с организациями из этих секторов. Таким образом, в целях разработки подхода к обеспечению кибербезопасности в гражданской авиации следует использовать национальные или региональные подходы и практические знания, применяемые в других секторах. Кроме того, для содействия повышению эффективности деятельности ведомств гражданской авиации государств предлагается наладить тесное взаимодействие с государственными учреждениями, занимающимися обеспечением кибербезопасности в других секторах.

3. ВЫВОД

3.1 Конференции предлагается согласиться со следующими рекомендациями:

Конференции предлагается:

a) настоятельно рекомендовать ИКАО оказать поддержку государствам в установлении требований для организаций по управлению факторами риска для кибербезопасности, связанными с их операциями, продуктами и услугами, включая их взаимодействие с партнерами, посредством системы управления информационной безопасностью (ISMS), основанную на международных отраслевых стандартах, которую рекомендуется совмещать или объединять с имеющимися системами управления;

b) поручить ИКАО предложить государствам принять надлежащие меры по внедрению глобальной интероперабельной инфраструктуры, способной противодействовать кибератакам. Она должна соответствовать требованиям в отношении интероперабельности и кибербезопасности в целях содействия достижению комплексных целей более высокого уровня в области обеспечения безопасности полетов и оперативного управления воздушным движением;

c) настоятельно рекомендовать ИКАО, придерживаясь многодисциплинарного подхода, разработать положения о доверии между организациями в рамках более широкой структуры доверия и содействовать их внедрению;

d) поручить ИКАО предложить государствам принять меры по стимулированию эксплуатантов воздушных судов к налаживанию обмена оперативной информацией по вопросам кибербезопасности по соответствующим каналам, таким как глобальная сеть "пользующихся доверием организаций", а также содействию такому обмену информацией;

e) настоятельно рекомендовать ИКАО содействовать разработке положений о структуре доверия и условиях эксплуатации средств обеспечения кибербезопасности в целях безопасной эксплуатации такой глобальной интероперабельной инфраструктуры;

f) поручить ИКАО предложить государствам расширить существующие или создать новые каналы для передачи сообщений об инцидентах в области кибербезопасности в целях более эффективного противодействия новым факторам риска для безопасности полетов и авиационной безопасности и оперативного управления воздушным движением;

g) поручить ИКАО призвать государства содействовать развитию межотраслевого сотрудничества по вопросам кибербезопасности среди государственных и негосударственных структур авиационной отрасли и других отраслей.

— КОНЕЦ —