Международная организация гражданской авиации

РАБОЧИЙ ДОКУМЕНТ

A39-WP/99
EX/45, TE/26
27/7/16
Revision No. 1

АССАМБЛЕЯ — 39-Я СЕССИЯ

ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ
ТЕХНИЧЕСКАЯ КОМИССИЯ

Пункт 16 повестки дня. Авиационная безопасность
Пункт 36 повестки дня. Безопасность полетов и поддержка внедрения в области аэронавигации

КИБЕРУСТОЙЧИВОСТЬ В ГРАЖДАНСКОЙ АВИАЦИИ

(Представлено Словакией от имени Европейского союза и его государств-членов[1], а также других государств – членов Европейской конференции гражданской авиации[2], и ЕВРОКОНТРОЛем)

КРАТКАЯ СПРАВКА

Система гражданской авиации состоит из множества взаимосвязанных компонентов, систем и сетей. За многие годы возросла возможность киберинцидентов, которые могут поставить под угрозу связь и обмен информацией между различными заинтересованными сторонами авиации, повлиять на безопасность полетов и авиационную безопасность и нарушить непрерывность авиационной деятельности. Несмотря на признание ИКАО важности определения соответствующего подхода к кибербезопасности в гражданской авиации, необходимо предпринять дополнительные усилия по повышению глобальной осведомленности и дальнейшей разработке согласованных подходов к киберустойчивости авиационной системы.

Действия: Ассамблее предлагается:

a) просить ИКАО всесторонним образом рассмотреть вопрос киберустойчивости в гражданской авиации;

b) просить ИКАО и его Договаривающиеся государства способствовать повышению осведомленности о киберугрозах и уязвимых местах в гражданской авиации посредством включения аспекта киберустойчивости в соответствующие процессы и такую деятельность, как проектирование систем, управление процедурами ОрВД и безопасностью полетов и обеспечение авиационной безопасности;

c) просить ИКАО безопасным образом способствовать обмену информацией между государствами и заинтересованными сторонами, касающейся киберугрозы, уязвимых мест и мер снижения риска;

d) просить ИКАО рассмотреть необходимые шаги по разработке руководящих указаний относительно управления текущими и будущими киберугрозами и уязвимыми местами с момента идентификации до принятия мер по снижению риска с учетом существующих в государствах соответствующих мер и отраслевых стандартов;

e) просить ИКАО поручить существующим группам экспертов учитывать в соответствующих случаях эти директивные указания при выполнении своей работы.

[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.

Стратегические цели	Данный рабочий документ связан со стратегическими целями "Безопасность полетов", "Аэронавигационный потенциал и эффективность", "Безопасность полетов и упрощение формальностей"
Финансовые последствия	Деятельность, упоминаемая в прилагаемом документе Ассамблеи, будет осуществляться при наличии ресурсов в бюджете Регулярной программы на 2017–2019 гг. и/или за счет внебюджетных взносов
Справочный материал	Doc 10022, *Действующие резолюции Ассамблеи (по состоянию на 4 октября 2013 года)* Приложение 17*"Безопасность. Защита международной гражданской авиации от актов незаконного вмешательства"*

1. ВВЕДЕНИЕ

1.1 Авиационная система состоит из множества взаимосвязанных компонентов, систем и сетей. Такие новые тенденции, как прогрессивное введение ДПАС и постоянная эволюция системы ОрВД (например, SWIM), укрепляют взаимосвязь и интеграцию систем. Несмотря на принятые до сих пор превентивные меры авиационной безопасности, подверженность авиационной системы киберинцидентам возрастает.

1.2 Важность применения соответствующего подхода к обеспечению кибербезопасности в авиации признана на глобальном уровне. Тем не менее, по-прежнему необходимо предпринять усилия по повышению глобальной осведомленности и дальнейшей разработке глобально связанных подходов к киберустойчивости авиационной системы.

1.3 Киберинциденты могут влиять на глобальное авиационное сообщество или отдельные системы на многих уровнях. Эти инциденты могут поставить под угрозу связи и обмен информацией между различными заинтересованными сторонами авиации, повлиять на безопасность полетов и авиационную безопасность и нарушить непрерывность авиационной деятельности. Способность обмениваться информацией, касающейся киберугроз, и применение надежных стандартных методов обеспечения безопасности обмена данными и информацией повысят способность авиационного сообщества к самозащите и ограничат последствия киберинцидентов.

2. РАССМОТРЕНИЕ ВОПРОСА

2.1 Несмотря на ряд разработанных инициатив на местном, национальном, региональном и глобальном уровнях, риски, возникающие в результате эволюции среды киберугроз в авиации, могут снижаться за счет более стандартизированного, последовательного и связанного подхода.

2.2 Содействовать повышению глобальной осведомленности о киберустойчивости в авиации

2.2.1 В некоторых экономических сферах, таких как банковское дело, киберугрозы и уязвимые места хорошо известны, и для снижения выявленных рисков внедрены контрмеры. В области авиации, однако, риски, связанные с кибератаками, не всегда хорошо понимаются всеми государствами и заинтересованными сторонами и не рассматриваются последовательным и системным образом.

2.2.2 Необходимо повысить осведомленность о киберугрозах и уязвимых местах авиационного сектора на глобальном уровне в целях обеспечения выявления появляющихся рисков государствами и заинтересованными сторонами и их уменьшения.

2.2.3 Такое повышение осведомленности может быть в значительной степени формализовано путем адаптации существующих процессов, в частности посредством разработки подхода к обеспечению конструктивной безопасности или внедрения методов специальной подготовки персонала. В дополнение и в координации с инициативами, касающимися авиационной безопасности (например, системы управления авиационной безопасностью, если таковые имеются, или национальные программы безопасности гражданской авиации), следует принимать во внимание аспекты киберустойчивости в контексте деятельности по управлению безопасностью полетов на организационном уровне (в рамках своей системы управления безопасностью полетов – СУБП), а также на государственном или региональном уровне (в рамках Государственной программы по безопасности полетов – ГосПБП) и в соответствующих случаях в контексте региональной программы по обеспечению безопасности полетов.

2.3 Способствовать обмену информацией о киберинцидентах, угрозах и стандартных подходах

2.3.1 Ни одна организация или группа заинтересованных сторон не в состоянии защитить себя собственными силами от преднамеренных несанкционированных электронных помех. К тому же киберугрозы постоянно эволюционируют и никто не может заявить о том, что он не подвержен никаким связанным с ними возможным рискам. Поэтому эффективное устранение киберинцидентов требует от государств и заинтересованных сторон обмена соответствующей информацией и гармонизации методов сохранения целостности обмена данными и информацией. Обмен информацией помогает государствам и заинтересованным сторонам лучше подготавливаться к киберинцидентам и принимать соответствующие меры по смягчению их последствий. Совместная информация может включать случаи возникновения инцидентов, уязвимые места, угрозы, тенденции и наблюдаемые особенности, оценки общих рисков, планы устранения рисков, успешные средства смягчения последствий (технические, эксплуатационные или организационные) или мероприятия по обеспечению безопасности, зарекомендовавшие себя как эффективная защита.

2.3.2 В авиации уже существует ряд инициатив, направленных на содействие обмену информацией о безопасности полетов (нередко конфиденциальной), в том числе на региональном и глобальном уровнях, однако они требуют дальнейшей разработки и дополнения в поддержку киберустойчивости всей авиационной системы. Такие инициативы могут базироваться на существующих платформах обмена информацией, таких как ISAC (центр обмена информацией и ее анализа) или CERT (группа реагирования на компьютерные происшествия), и могут потребовать создания общих протоколов обмена информацией, касающихся киберинцидентов, в соответствии с национальными и региональными правилами защиты конфиденциальной информации.

2.3.3 Необходимо также усовершенствовать методы защиты данных и обмена информацией между всеми заинтересованными сторонами. Следует поощрять стандартизацию технических средств контроля, которые обеспечат более прочные методы аутентификации и авторизации данных для глобального авиационного сообщества.

2.4 Содействовать применению "совместного подхода к управлению авиационными рисками"

2.4.1 В авиации существует много методик оценки рисков, большинство которых направлены на характеризацию и оценку угроз и уязвимых мест. Несмотря на возможное согласие относительно того, какие элементы необходимы для характеризации рисков (например, вероятность возникновения риска и размеры последствий), оценки конкретных деталей довольны разнообразны, чтобы можно было достигнуть сопоставимых, связанных или даже последовательных результатов. Однако, при столкновении с повторяющимися киберинцидентами, в рамках которых могут использоваться аналогичные схемы, полезно определить "общие принципы" и методы установления, оценки и снижения рисков.

2.4.2 Такие "общие принципы" должны способствовать идентификации угроз и уязвимых мест, позволять оценивать риски и предоставлять средства их снижения. Одним из примеров было бы формальное определение сферы авиационной безопасности, описывающее контекст, в котором осуществляются оценки риска, и определение этой сферы помогло бы идентифицировать критически важные авиационно-информационные системы, предусмотренные соответствующими положениями Приложения 17 ИКАО. Другим примером было бы рассмотрение "сценариев угрозы" от начала до конца, включающих угрозы, рассматриваемую архитектуру системы и активы, вызывающие нежелательные эффекты. Оно также включает известные уязвимые места в рамках сценариев угрозы, которые могут требовать уменьшения последствий соразмерно степени серьезности воздействия.

2.4.3 После определения и принятия "общие принципы" оценки риска в авиации будут идеально применяться в структуре ИКАО при разработке или изменении Стандартов и Рекомендуемой практики (SARPS).

— КОНЕЦ —