Международная организация гражданской авиации

A40-WP/295
TE/119
1/8/19

РАБОЧИЙ ДОКУМЕНТ

АССАМБЛЕЯ — 40-Я СЕССИЯ

ТЕХНИЧЕСКАЯ КОМИССИЯ

Пункт 30 повестки дня. Прочие вопросы, подлежащие рассмотрению Технической комиссией

ПРИМЕНЕНИЕ В АВИАЦИИ МЕТОДОВ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ, ИСПОЛЬЗУЕМЫХ ГОСУДАРСТВОМ

(Представлено Новой Зеландией)

КРАТКАЯ СПРАВКА

В настоящем документе обсуждается вопрос разработки принципов ИКАО по обеспечению кибербезопасности в авиации в контексте существующих, не привязанных к какой-либо отрасли методов обеспечения кибербезопасности, применяемых государствами. В документе предлагается ИКАО сосредоточить свои усилия на разработке надежных и согласованных принципов, которые государства могли бы положить в основу своего подхода к решению проблем кибербезопасности.

Действия: Ассамблее предлагается:

a) принять к сведению, что реализация глобальных, согласованных и имеющих избыточно предписывающий характер стандартов в области кибербезопасности может вступать в конфликт с национальными механизмами обеспечения кибербезопасности и ограничивать возможности государств по соблюдению SARPS ИКАО;

b) призвать ИКАО сосредоточиться на разработке принципиальных инструктивных указаний по обеспечению кибербезопасности в авиационной отрасли, призванных помочь государствам интегрировать авиацию в национальные механизмы обеспечения безопасности, принимая во внимание существующие стандарты в области информационной безопасности, такие как ИСО 27000;

c) призвать ИКАО предоставить инструктивные указания в отношении выработки цели и реализации механизма доверия.

Стратегические цели	Настоящий рабочий документ связан со стратегическими целями "Авиационная безопасность и упрощение формальностей" и "Безопасность полетов"
Финансовые последствия	Отсутствуют
Справочные материалы	AN-Conf/13-WP/270: "Концепция системы систем обеспечения кибербезопасности в авиации" (28/09/2018)

1. ВВЕДЕНИЕ

1.1 В условиях непрерывного технического прогресса и возрастающего уровня сложности авиационных систем безопасность полетов и авиационная безопасность глобальной авиационной системы все более зависят от эффективности методов обеспечения кибербезопасности.

1.2 Необходимость эффективных методов обеспечения кибербезопасности является общей для широкого круга различных сфер деятельности и ни в коем случае не является уникальной для авиации. В отсутствие эффективной кибербезопасности организациям будет сложно предоставлять цифровые продукты и услуги таким образом, чтобы сохранить доверие и уверенность своих клиентов и заинтересованных сторон.

1.3 Государства должны играть ведущую роль в обеспечении достижения национально значимыми организациями и отраслями стабильно высокого уровня кибербезопасности. Применяемый подход будет варьироваться от государства к государству в зависимости от различий в характере угроз, возможностях и интересах национальной безопасности.

1.4 Несмотря на то, что методы обеспечения безопасности, применяемые конкретными организациями, в целом будут выбираться в соответствии с их потребностями и возможностями, равно как и потребностями сектора, в котором они работают, определяющие требования будут диктоваться интересами национальной безопасности. Национальные интересы государства всегда будут иметь приоритет над интересами отдельной отрасли или организации.

1.5 Глобальная авиация в значительной степени зависит от безопасной и надежной цифровой передачи информации между членами авиационного сообщества, в том числе между государствами. В документе AN-Conf/13-WP/270, представленном на Тринадцатой Аэронавигационной конференции, была изложена концепция подхода к кибербезопасности под названием "Система систем". В рамках этого подхода делается вывод, что общая авиационная система состоит из некоторого количества подсистем, управляемых целым рядом заинтересованных сторон, и для создания безопасной операционной среды их необходимо рассматривать в целостности.

1.6 Для обеспечения возможности установления доверенных коммуникационных связей между заинтересованными сторонами был разработан механизм доверия ИКАО. Этот механизм предусматривает применение следующих принципов:

1.6.1 Взаимодействие между всеми заинтересованными сторонами обеспечивается путем использования общего механизма доверия и архитектуры, предназначенной для бесперебойного и эффективного обмена сообщениями в глобальном масштабе.

1.6.2 Устойчивость коммуникаций в максимальной степени достигается за счет использования конструктивных решений, ограничивающих количество потенциальных уязвимых мест. Это включает в себя разделение на части сети и приложений, а также иерархическое построение защиты в инфраструктуре и ограничение числа участвующих систем.

1.6.3 Строгая идентификация, аутентификация, авторизация, целостность и конфиденциальность.

1.7 Несмотря на то, что концепция механизма доверия имеет определенную ценность, отсутствует ясность в отношении ее цели и потенциального применения. Дальнейшее развитие механизма для обеспечения четкого определения его роли потребует тщательного учета интересов национальной безопасности государств.

2. ОБСУЖДЕНИЕ

2.1 Национальные интересы государства накладывают ограничения на характер систем кибербезопасности, которые могут быть реализованы отдельными секторами и организациями. Там где имеются государственные нормативные требования и стандарты в области безопасности информации, они будут иметь приоритет над отраслевыми и корпоративными стандартами.

2.2 Как таковая, способность государства соблюдать предписывающие SARPS ИКАО в области авиационной кибербезопасности, вероятно, будет ограничена его собственными механизмами национальной безопасности. Степень этого ограничения будет значительно варьироваться от государства к государству и зависеть от строгости предписания в самих SARPS.

2.3 Так же маловероятно, что строго предписывающий и строго стандартизированный подход будет эффективно регулировать область, в которой технологии и среда угроз развиваются быстрыми темпами. Глобальные требования, носящие чрезмерно предписывающий характер, могут препятствовать способности государства реагировать на изменения и в равной степени могут не подходить к различным типам операций.

2.4 Несмотря на различия в потребностях отдельных государств в области кибербезопасности и проблемы, связанные с введением строго предписывающих международных требований, существует необходимость в последовательном и согласованном наборе принципов, регулирующих безопасную передачу информации между заинтересованными сторонами.

2.5 Для поддержки реализации этих принципов следует разработать инструктивный материал ИКАО, где уделялось бы особое внимание оказанию государствам помощи в обеспечении авиационной кибербезопасности в качестве неотъемлемой части национальных механизмов безопасности. Для достижения этой цели наиболее действенным, вероятно, будет подход, основанный на эффективности или на принципах.

2.6 Путем принятия принципиального подхода инструктивный материал ИКАО может быть адаптирован отдельными государствами таким образом, чтобы глобальный механизм доверия был реализован в согласии с национальными требованиями. Основой для такого руководства служат существующие принципиальные стандарты информационной безопасности, такие как ИСО 27000. В идеале следует рассмотреть четыре основные области:

2.6.1 **Управление**: содействие кибербезопасности на уровне высшего руководства для защиты наиболее важных цифровых активов организации. Советы директоров и руководители в конечном счете несут ответственность за результаты любого киберинцидента, включая его влияние на доверие заинтересованных сторон и клиентов.

2.6.2 **Инвестиции**: инвестиции в кибербезопасность для минимизации рисков и максимизации прибыли. Согласование допустимого уровня рисков и определение ключевых активов организации на уровне управляющего звена являются важнейшими первыми шагами для обеспечения надлежащей целенаправленности и сбалансированности инвестиций.

2.6.3 **Готовность**: подготовленность организации к обнаружению инцидента в области кибербезопасности, реагированию на него и последующему восстановлению работоспособности. Вопрос в данном случае ставится в форме не "если", а "когда" организация будет переживать инцидент с кибербезопасностью. Готовность к инциденту позволяет организациям снизить общий риск в области кибербезопасности за счет быстрого и эффективного восстановления работоспособности.

2.6.4 **Цепочка поставок**: осуществление постоянного надзора и поддержание осведомленности о рисках кибербезопасности в цепочке поставок организации. Эта область особенно важна в авиационном секторе, поскольку его зачастую отличают длинные цепочки, связанные с поставкой оборудования и услуг. Это включает в себя такие аспекты, как техническую составляющую проектирования систем и человеческий фактор проектирования процессов.

2.7 Должным образом сформулированные руководящие указания, основанные на эффективности и принятых стандартах информационной безопасности, будут представлять ценность для отдельных организаций авиационного сектора и будут способствовать применению последовательного подхода, распространяющегося на важнейшие элементы эффективного контроля в области кибербезопасности.

2.8 При разработке принципов таких указаний следует также учитывать, где существует необходимость в определенных минимальных мерах по обеспечению безопасности и как к ним следует подходить с учетом механизмов, применяемых различными государствами.

2.9 Разработка механизма доверия ИКАО дает возможность выработать протоколы по обмену информацией между заинтересованными сторонами, однако необходимо дальнейшее разъяснение его цели и видов применения.

2.10 Разработка механизма доверия должна рассматриваться в сочетании с механизмами кибербезопасности, реализуемыми заинтересованными сторонами. Безопасность обмена данными надежна ровно в той же степени, что и безопасность источника данных, а это зависит от эффективности методов обеспечения безопасности, предпринимаемых организациями и государствами.

— КОНЕЦ —