Международная организация гражданской авиации

HLCAS/2-WP/18
16/10/18

РАБОЧИЙ ДОКУМЕНТ

ВТОРАЯ КОНФЕРЕНЦИЯ ВЫСОКОГО УРОВНЯ ПО АВИАЦИОННОЙ БЕЗОПАСНОСТИ (HLCAS/2)

Монреаль, 29–30 ноября 2018 года

Пункт 2 повестки дня. Будущие подходы к управлению факторами риска для авиационной безопасности

РАЗРАБОТКА ГЛОБАЛЬНОЙ СТРАТЕГИИ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

(Представлено Румынией)

АННОТАЦИЯ

В настоящем документе государствам и отрасли представлены рекомендации по активной поддержке разработки глобальной стратегии обеспечения кибербезопасности в гражданской авиации.

Действия Конференции высокого уровня по авиационной безопасности указаны в п. 4.

1. ВВЕДЕНИЕ

1.1 С 7 по 9 мая 2018 года в Бухаресте, Румыния, был проведен Саммит по вопросам кибербезопасности в гражданской авиации в Европе, на Ближнем Востоке и в Африке (EMEA). На саммите присутствовали 416 делегатов из 55 государств и 19 международных организаций. На саммите обсуждались пути содействия разработке единообразных механизмов обеспечения кибербезопасности.

1.2 На саммите была упомянута *Дубайская декларация о кибербезопасности в гражданской авиации*, первоначально представленная в Дубае 5 апреля 2017 года. Кроме того, на нем была отмечена деятельность Исследовательской группы Секретариата по кибербезопасности (SSGC) и ее текущая работа по всем элементам международной авиационной системы, которые могут быть затронуты киберинцидентами.

2. РАССМОТРЕНИЕ ВОПРОСА

2.1 Десять лет назад международной проблеме обеспечения кибербезопасности в авиации уделялось незначительное внимание. С начала текущего десятилетия авиационные эксперты предупреждали, что злонамеренная кибератака на гражданскую авиацию может привести к катастрофическим последствиям. Технические достижения обуславливают необходимость кардинального изменения методов обеспечения безопасности полетов и авиационной безопасности на этапах проектирования, производства, эксплуатации и технического обслуживания.

2.2 Киберпространство стало одним из важных основополагающих факторов экономического, социального и политического взаимодействия. Однако повышение уровня независимости и появление новых экономических возможностей сопровождалось появлением уязвимых мест и проблем в области безопасности. По мнению некоторых экспертов, в связи с обработкой больших объемов данных, компьютерным обучением и "Интернетом вещей" к 2035 году число подключенных к Интернету устройств может возрасти почти до одного триллиона. Резко возрастет число потенциальных объектов атак, совершаемых частными и государственными субъектами, и в него войдут всевозможные объекты, от промышленных систем управления до кардиостимуляторов, транспортных средств с системой автоматического управления, дронов и, наконец, что не менее важно, гражданской авиации.

2.3 По аналогии с другими отраслями, затронутыми "цифровой революцией", авиации необходимо сохранять доверие заинтересованных сторон за счет точного распознавания уязвимых мест и возможностей, а также понимания враждебных угроз. Ниже указаны проблемы, стоящие перед взаимосвязанной и "оцифрованной" гражданской авиацией.

2.3.1 По мере подключения авиационных систем и служб к компьютерным сетям растет число потенциальных объектов возможной атаки и их составных частей, в результате чего они превращаются в более крупную мишень.

2.3.2 Поскольку авиационная отрасль в значительной степени полагается на технические средства и в ней все активнее используется киберсреда, то понимание и преодоление культурных различий между двумя отраслями потребует глобальных изменений. Совместную деятельность по развитию общей культуры, рассмотрению проблем и поиску возможных решений необходимо осуществлять на основе междисциплинарного сотрудничества.

2.3.3 Осознание киберугрозы будет играть решающую роль в понимании этого фактора риска и борьбе с ним. В целях противодействия потенциальному фактору риска и развития конструктивного диалога с учетом множества точек зрения необходимо обеспечить единый уровень осознания и понимания киберугрозы в масштабе всей отрасли.

2.3.4 В авиационной отрасли накоплен многолетний опыт работы в области обеспечения безопасности полетов и авиационной безопасности, однако проблема обеспечения кибербезопасности является относительно новой. Точная оценка факторов риска и борьба с угрозами осложняются тем, что на разработку и замену авиационных систем может уйти больше времени, чем требуется правонарушителям на наращивание своих возможностей.

2.3.5 Инвестиции в организацию воздушного движения (ОрВД) уже окупаются, однако при использовании передовых технологий, таких как глобальная система определения местоположения (GPS), цифровая связь и радиовещательное автоматическое зависимое наблюдение (ADS-B), необходимо предпринимать действия по устранению уязвимых мест, возникающих в результате применения этих технологий, а также способствовать обеспечению киберустойчивости.

2.3.6 Аэропорты представляют собой объединения нескольких отдельных организаций, которые могут придерживаться различных подходов, однако киберуязвимость одной из них может сказываться на всех остальных. Крайне важно гарантировать надлежащую защиту систем обеспечения физической безопасности в аэропортах от киберугроз.

2.3.7 Существуют согласованные на национальном и международном уровнях стратегии и правила по обеспечению безопасности полетов и физической безопасности, однако до сих пор четко не определены подходы к разработке аналогичных стратегий по обеспечению кибербезопасности в авиации. В связи с этим ИКАО, Европейскому агентству по безопасности полетов (ЕАБП), ЕВРОКОНТРОЛю, Европейской конференции гражданской авиации (ЕКГА), а также другим многосторонним организациям надлежит действовать плечом к плечу в целях разработки политики и правил, единых интеллектуальных систем, механизмов управления и отчетности, методов укрепления доверия и безопасного процесса принятия решений людьми в рамках общей многофункциональной и трансграничной киберсреды.

2.3.8 ИКАО обладает благоприятными возможностями для объединения многочисленных глобальных инициатив в области обеспечения кибербезопасности в авиации, а также укрепления доверия, управления и установления Стандартов. В целях повышения уровня согласованности действий различных стран по разработке стандартов в области обеспечения кибербезопасности и содействия развитию диалога и сотрудничества между отдельными заинтересованными сторонами необходимо провести критический анализ Приложений (8, 10, 17, 18 и т. д.) к Чикагской конвенции и внести в них соответствующие поправки с точки зрения кибербезопасности. Настало время признать потенциальную возможность незаконного вмешательства в авиационную деятельность с помощью киберсредств, а также внедрить положения по кибербезопасности по аналогии с действующими положениями по физической безопасности.

2.3.9 В обозримом будущем устойчивость гражданской авиации будет гарантирована путем наращивания потенциала в области обеспечения кибербезопасности в рамках слаженного взаимодействия между людьми, технологиями и процессами по внедрению основанного на информационных сетях оперативного подхода и созданию средств обнаружения, защиты, охраны, анализа, определения и реагирования, а также восстановления.

2.3.10 Всесторонний и своевременный обмен информацией позволит свести к минимуму воздействие факторов риска, а дополнительная польза такого сотрудничества заключается в оказании содействия заинтересованным сторонам в повышении уровня кибербезопасности. В качестве примеров организаций, оказывающих помощь государствам-членам в обеспечении кибербезопасности, можно привести новый Европейский центр по обеспечению кибербезопасности в авиации, связанный с группой ЕС по быстрому реагированию на компьютерные инциденты (CERT), авиационный центр по совместному использованию и анализу информации или оперативные центры по вопросам безопасности.

2.3.11 Обмен информацией между гражданскими и военными органами также имеет большое значение. Гражданская авиация могла бы извлечь уроки из опыта военной авиации в области обеспечения безопасности воздушных судов и систем в условиях создания радиотехнических помех и уводящих помех, а также киберугроз.

2.3.12 ЕАБП разработало документ под названием "Бухарестская декларация об усилиях в области обеспечения кибербезопасности гражданской авиации на высоком уровне", в котором основное внимание уделяется нескольким направлениям работы, таким как координация действий на европейском уровне, международное сотрудничество, оценка факторов риска, повышение

осведомленности, обмен информацией, научно-исследовательские и опытно-конструкторские работы. Кроме того, было предложено согласовать соответствующие правила на международном уровне с учетом необходимости разработки более широкого комплексного подхода.

3. ВЫВОД

3.1 В целях обеспечения устойчивой кибербезопасности путем принятия мер по борьбе с факторами риска для кибербезопасности на этапах концептуального моделирования, проектирования, контроля качества, поставки, строительных работ, сдачи в эксплуатацию, эксплуатации и технического обслуживания необходимо разработать общий всеобъемлющий комплексный подход. Деятельность по изменению текущего положения и достижению желаемых результатов в области борьбы с факторами риска и угрозами надлежит начать как можно скорее.

3.2 На Саммите ИКАО по вопросам обеспечения кибербезопасности в гражданской авиации в Европе, на Ближнем Востоке и в Африке, который проходил 7-9 мая 2018 года в Бухаресте, Румыния, должностные лица и представители государств, региональных и международных организаций и отрасли обсудили проблемы международной гражданской авиации, создаваемые киберугрозами.

3.3 С учетом необходимости упорядоченного обеспечения безопасности полетов, авиационной безопасности и непрерывности деятельности гражданской авиации рекомендуем:

3.3.1 государствам и отрасли разработать как можно более единообразные механизмы обеспечения кибербезопасности;

3.3.2 государствам и отрасли развивать региональное сотрудничество в области разработки общих стратегий, обмена информацией и передовой практикой по примеру уже существующих инициатив;

3.3.3 способствовать разработке механизмов доверия в целях безопасного обмена информацией по мере целесообразности;

3.3.4 государствам и отрасли сотрудничать в определении долгосрочных потребностей в людских ресурсах и разрабатывать стратегии по привлечению, обучению и удержанию следующего поколения авиационных специалистов;

3.3.5 государствам и отрасли оказать активную поддержку процессу разработки глобальной стратегии обеспечения кибербезопасности под эгидой Международной организации гражданской авиации.

4. ДЕЙСТВИЯ КОНФЕРЕНЦИИ ВЫСОКОГО УРОВНЯ

4.1 Конференции высокого уровня по авиационной безопасности предлагается одобрить выводы и подтвердить необходимость разработки общего всеобъемлющего комплексного подхода в области кибербезопасности.

— КОНЕЦ —