Международная организация гражданской авиации

AN-Conf/13-WP/62
27/8/18

РАБОЧИЙ ДОКУМЕНТ

ТРИНАДЦАТАЯ АЭРОНАВИГАЦИОННАЯ КОНФЕРЕНЦИЯ

Монреаль, Канада, 9–19 октября 2018 года

КОМИТЕТ A

Пункт 5 повестки дня. Возникающие проблемы
5.4 Киберустойчивость

СОДЕЙСТВИЕ УКРЕПЛЕНИЮ КИБЕРУСТОЙЧИВОСТИ ПУТЕМ ПОВЫШЕНИЯ ГЛОБАЛЬНОЙ ОСВЕДОМЛЕННОСТИ И ПРОВЕДЕНИЯ РЕГИОНАЛЬНЫХ УЧЕНИЙ

(Представлено Соединенными Штатами Америки)

КРАТКАЯ СПРАВКА

В соответствии с резолюцией A39-19 Ассамблеи ИКАО *"О киберустойчивости в гражданской авиации"* Федеральное авиационное управление (ФАУ) совместно с ИКАО и региональными партнерами провело работу по определению создаваемых возможными киберинцидентами угроз и рисков для безопасности полетов гражданской авиации и критических систем, а также по содействию выработке среди своих партнеров единого понимания киберугроз, рисков и мер по минимизации последствий киберинцидентов.

В этой связи ФАУ предложило модель региональных штабных учений по киберустойчивости упрощенным обсуждением различных сценариев, построенных таким образом, чтобы способствовать открытому и дающему пищу для размышлений обмену идеями по различным вопросам, касающимся гипотетических или смоделированных киберинцидентов. Такие учения могут быть использованы для повышения общей осведомленности, проверки существующих планов и процедур, а также для оценки систем и действий по реагированию на киберинциденты и для восстановления деятельности.

Действия: Конференции предлагается согласиться со следующими действиями:

a) утвердить концепцию региональных штабных учений по киберустойчивости, проводимых совместно с региональными бюро ИКАО и государствами – членами ИКАО, в соответствии с п. 2.6;

b) поручить ИКАО создать архив сценариев и извлеченных уроков, доступный государствам-членам для разработки региональных штабных учений по киберустойчивости.

1. ВВЕДЕНИЕ

1.1 Пассажиры, авиационная отрасль, поставщики аэронавигационного обслуживания (ПАНО) и ведомства гражданской авиации (ВГА) все больше полагаются на технологии связи и сетецентрические операции, а значит государства должны провести модернизацию вычислительной и сетевой инфраструктуры, обеспечить связь пользователей, систем и данных для того, чтобы обеспечить бесперебойный и защищенный от киберинцидентов доступ.

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

1.3 Для укрепления позиций гражданской авиации в области авиационной безопасности Федеральное авиационное управление (ФАУ) провело работу по определению рисков, связанных с киберугрозой, которые могут повлиять на безопасность полетов и вызвать сбои в работе национальной аэрокосмической системы (NAS), и разработке соответствующих стратегий по снижению их последствий для всей авиационной экосистемы. Такая многопрофильная стратегия позволяет компонентам NAS работать как единой системе, нацеленной на обеспечение безопасного и эффективного обслуживания пассажиров, авиакомпаний, военной авиации США, авиации общего назначения и аэропортов.

1.4 Помимо разработки местных стратегий кибербезопасности по снижению последствий и в соответствии с резолюцией A39-19 Ассамблеи ИКАО *"О киберустойчивости в гражданской авиации"* ФАУ совместно с ИКАО и региональными партнерами провело работу по определению угроз и рисков, создаваемых вероятными киберинцидентами, влияющими на безопасность полетов гражданской авиации и критические системы, а также по содействию выработки единого понимания среди партнеров в вопросах киберугроз, рисков и мер по минимизации последствий киберинцидентов.

1.5 ФАУ предложило модель региональных штабных учений по киберустойчивости упрощенным обсуждением различных сценариев, построенных таким образом, чтобы способствовать открытому и дающему пищу для размышлений обмену идеями по различным вопросам, касающимся гипотетических или смоделированных киберинцидентов. Такие учения могут быть использованы для повышения общей осведомленности, проверки существующих планов и процедур, а также для оценки систем и действий по реагированию на киберинциденты и для восстановления деятельности.

2. РАССМОТРЕНИЕ ВОПРОСА

2.1 В своей резолюции A39-19 39-я сессия Ассамблеи ИКАО, помимо прочего, призвала государства:

a) определить угрозы и риски для безопасности полетов гражданской авиации и критических систем от возможных киберинцидентов, а также серьезные последствия таких инцидентов;

b) способствовать выработке единого понимания киберугроз и рисков среди государств - членов, а также общих критериев определения критичности тех объектов и систем, которые необходимо защитить;

c) способствовать укреплению взаимодействия между правительством и отраслью в отношении стратегий, политики и планов авиационной кибербезопасности, а также обмена информацией для определения уязвимых мест, которые должны быть устранены;

d) развивать сотрудничество между правительством и отраслью (на национальном и международном уровне) и методы регулярного обмена информацией о киберугрозах, инцидентах, тенденциях и мерах по снижению последствий, а также становиться участниками такого процесса сотрудничества;

e) разрабатывать политику и выделять ресурсы, необходимые критическим авиационным системам в целях обеспечения следующего: защиты архитектуры системы еще на этапе проектирования; устойчивости системы; защиты методов передачи данных и обеспечения целостности и конфиденциальности данных; внедрения методов мониторинга системы, выявления инцидентов и составления отчетности; и проведения ретроспективного анализа киберинцидентов.

2.2 В то время как работа ИКАО по созданию единых, согласованных методов защиты авиационного сообщества от рисков кибербезопасности путем интеграции нормативных требований продвигается благодаря Рабочей группе INNOVA, отдельные государства высказали озабоченность в отношении создания и реализации программ кибербезопасности.

2.3 Для решения этих вопросов и с учетом большого объема переписки и обмена информацией и данными между ФАУ, ведомствами гражданской авиации и поставщиками аэронавигационного обслуживания в Карибском регионе, а также в целях поддержки разработки региональной практики в отношении авиационных киберугроз ФАУ провело штабные учения по киберустойчивости. Эти учения могут рассматриваться как модель для проведения других региональных штабных учений в будущем.

2.4 Штабные учения по киберустойчивости представляли собой упрощенное обсуждение сценариев в официальной, но непринужденной обстановке. Это был открытый и дающий пищу для размышлений обмен идеями по различным вопросам, касающимся гипотетических или смоделированных киберинцидентов, который может проводиться в Карибском регионе для повышения общей осведомленности, проверки существующих планов и процедур, а также для оценки систем и действий по реагированию на киберинциденты и ликвидации последствий. Внимание в рамках учений было также уделено политике, планам, работе с персоналом, обмену информацией, взаимодействию с правительством, а также определению каких-либо пробелов и нечетких или дублирующих обязанностей.

2.5 Штабные учения по киберустойчивости проведены ФАУ и государствами Карибского региона для обеспечения успешной киберустойчивой работы независимых или совместно используемых информационных систем и сетей.

2.6 Штабные учения по киберустойчивости представляли собой интенсивное обсуждение политики и практики. Цели данных учений заключались в том, чтобы:

a) выработать и продвигать в рамках авиационной экосистемы единое понимание киберугроз, уязвимых мест и итогового риска;

b) определить пробелы в государственной политике и оперативной деятельности;

c) определить принципы и способствовать укреплению регионального взаимодействия и механизмов обмена информацией о возникающих угрозах и реагировании на инциденты.

3. ВЫВОД

3.1 В то время как в ИКАО продолжается работа по созданию единых принципов нормативных требований, в целях повышения уровня кибербезопасности необходимо провести обширную работу на региональном и государственном уровнях. Государства могут приступить к разработке основных принципов повышения уровня кибербезопасности и снижения последствий от киберинцидентов путем совместной работы в рамках региональных партнерств, используя успешную модель выработки единого понимания.

— КОНЕЦ —