Международная организация гражданской авиации

A41-WP/158
EX/72
2/8/22

РАБОЧИЙ ДОКУМЕНТ

АССАМБЛЕЯ — 41-Я СЕССИЯ

ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ

Пункт 14 повестки дня. Авиационная безопасность. Политика

НАРАЩИВАНИЕ ПОТЕНЦИАЛА И ПОДГОТОВКА ГОСУДАРСТВ В ВОПРОСАХ КИБЕРБЕЗОПАСНОСТИ

(Представлено Гайаной и поддержано Аргентиной, Боливией, Бразилией, Венесуэлой, Гватемалой, Доминиканской Республикой, Колумбией, Панамой, Перу, Сальвадором, Уругваем и Эквадором)

КРАТКАЯ СПРАВКА

Обеспечение кибербезопасности – это междисциплинарный вопрос, который по-прежнему сопряжен с угрозами для гражданской авиации. ИКАО признает эту угрозу безопасности международной гражданской авиации и в качестве ответной меры разработала Стратегию обеспечения кибербезопасности и План действий по обеспечению кибербезопасности. Хотя эта политика и инструктивный материал полезны для государств, крайне важно, чтобы государства обладали соответствующими знаниями, возможностями, подготовкой и ресурсами для реального снижения киберугроз и рисков на национальном, региональном и международном уровнях.

В связи с этим в данном рабочем документе содержится просьба к ИКАО выделить ресурсы на наращивание потенциала государств для достижения целей приведенных ниже семи основных направлений стратегии обеспечения кибербезопасности:

a) международное сотрудничество;
b) создание структур управления;
c) действенное законодательство и нормативные положения;
d) политика обеспечения кибербезопасности;
e) обмен информацией;
f) управление инцидентами и планирование на случай чрезвычайных ситуаций;
g) наращивание потенциала, подготовка и культура кибербезопасности.

Действия: Ассамблее предлагается:

a) поручить Совету дать Секретариату задание выделить ресурсы на обеспечение киберустойчивости и наращивание потенциала малых государств. К требующим внимания областям относятся: повышение осведомленности по вопросам кибербезопасности; управление инцидентами в плане кибербезопасности и профессиональная подготовка по реагированию в чрезвычайных ситуациях и программа подготовки и сертификации инструкторов по кибербезопасности;

b) поручить ИКАО развивать и создавать механизмы сотрудничества для развития программ авиационного наставничества и обмена техническим опытом между государствами.

Стратегические цели	Данный рабочий документ связан со стратегической целью "Авиационная безопасность и упрощение формальностей".
Справочный материал	Приложение 17, *Авиационная безопасность* *Стратегия обеспечения кибербезопасности в авиации* *План действий по обеспечению кибербезопасности*

ВВЕДЕНИЕ

1.1 Прогнозируется, что объем воздушных перевозок гражданской авиации будет расти, а вместе с ним будет расти и зависимость от технологий. Большая зависимость от технологий ведет к увеличению угроз и рисков, что делает кибербезопасность и необходимость повышения устойчивости к киберугрозам важным вопросом для государств. Обеспечение кибербезопасности в авиации крайне необходимо, поскольку оно представляет собой широкий спектр вопросов, включающий аспекты безопасности полетов, авиационной безопасности, аэронавигации, систем ИКТ и полетов авиации общего назначения. В Стратегии обеспечения кибербезопасности ИКАО и Плане действий по обеспечению кибербезопасности содержатся необходимые рекомендации для государств, позволяющие начать закладывать фундамент надежной инфраструктуры обеспечения кибербезопасности. Вместе с тем для этого потребуется наращивание потенциала, подготовка, создание культуры кибербезопасности, а также межведомственное и межрегиональное сотрудничество.

1.2 Для создания надежной инфраструктуры кибербезопасности государства должны следовать семи основным принципам Стратегии обеспечения кибербезопасности авиации ИКАО и принять План действий ИКАО по обеспечению кибербезопасности, которые закладывает основу для сотрудничества государств, заинтересованных сторон в отрасли и ИКАО в целях развития способности выявлять, предотвращать и обнаруживать кибератаки на объекты системы гражданской авиации, реагировать на них и восстанавливаться после них, а также для создания основ сотрудничества. В Плане действий по обеспечению кибербезопасности предлагается ряд мер и действий, которые государства должны принять для достижения целей по семи основным направлениям. Они включают в себя международное и межгосударственное сотрудничество, создание структур управления, разработку эффективного национального законодательства и нормативных положений, разработку политики обеспечения кибербезопасности, обмен соответствующей информацией между государствами, управление инцидентами и планирование на случай чрезвычайных ситуаций, наращивание потенциала, подготовка и развитие культуры кибербезопасности, с тем чтобы, в конечном счете, повысить устойчивость к этому глобальному явлению.

1.3 Наращивание потенциала является ключевым элементом надежной глобальной инфраструктуры обеспечения кибербезопасности. Это основа, с опорой на которую можно развивать остальные шесть направлений. В связи с этим ИКАО настоятельно рекомендуется содействовать наращиванию государствами, особенно малыми государствами, необходимого потенциала и обеспечивать его.

2. РАССМОТРЕНИЕ ВОПРОСА

2.1 Гайана выдвинула ряд инициатив по борьбе с кибератаками и повышению киберустойчивости, которые соответствуют семи основным направлениям стратегии обеспечения авиационной кибербезопасности. Руководит этой миссией Национальный орган по управлению данными (NDMA), который является уполномоченным органом Гайаны по мониторингу и защите данных. NDMA приступил к разработке Национальной политики, стандартов, законодательства и нормативных актов в области кибербезопасности, которые будут представлены на обсуждение межведомственным комитетам. Это циклический процесс, требующий участия профильных ведомств, особенно тех из них, что имеют критически важную инфраструктуру. Учитывая ограничения и проблемы малых государств, существует необходимость в предоставлении сторонних рекомендаций и организации обучения для комплексного решения вопросов кибербезопасности. Несмотря на то, что обмен информацией между ведомствами осуществляется

на национальном уровне, а запросы на обучение подаются через межведомственный комитет, необходимо наращивать государственный потенциал.

2.2 Наращивание потенциала подразумевает соответствующую подготовку авиационного персонала для повышения уровня знаний, квалификации, развития навыков и расширения возможностей в области обеспечения кибербезопасности. Оно подразумевает также предоставление соответствующих людских и капитальных ресурсов для создания надежной инфраструктуры обеспечения кибербезопасности. Для разработки соответствующих законодательных и нормативных актов нужны квалифицированные и опытные специалисты по обеспечению кибербезопасности. Этот потенциал может быть создан путем проведения национальных, региональных и международных практикумов. Это требует актуальных и дающихся в необходимом объеме программ подготовки для укрепления возможностей государств по управлению инцидентами в области кибербезопасности и планированию мер реагирования на чрезвычайные ситуации. Это крайне важно, поскольку кибератаки невозможно остановить полностью, но с помощью надежных систем можно смягчить их последствия. Следовательно, кибератаки будут происходить и впредь, но важно, чтобы государства обладали киберустойчивостью для обеспечения бесперебойной деятельности.

2.3 Проведение тренингов, практикумов, программ стажировок и наставничества и т. д. является необходимым условием для наращивания потенциала малых государств. В зависимости от ситуации они могут организовываться для конкретных государств и регионов.

3. ВЫВОД

3.1 В данном рабочем документе признается необходимость наращивания потенциала и укрепления устойчивости государств перед лицом угроз в сфере кибербезопасности.

— КОНЕЦ —