Международная организация гражданской авиации

LC/39-WP/2-5[1]
10/5/24

РАБОЧИЙ ДОКУМЕНТ

ЮРИДИЧЕСКИЙ КОМИТЕТ — 39-Я СЕССИЯ

(Монреаль, 25–28 июня 2024 года)

Пункт 2 повестки дня. Рассмотрение общей программы работы Юридического комитета

АКТЫ ИЛИ НАРУШЕНИЯ, ВЫЗЫВАЮЩИЕ ОЗАБОЧЕННОСТЬ СООБЩЕСТВА МЕЖДУНАРОДНОЙ ГРАЖДАНСКОЙ АВИАЦИИ, ВКЛЮЧАЯ КИБЕРУГРОЗЫ, КОТОРЫЕ МОГУТ БЫТЬ В НЕДОСТАТОЧНОЙ СТЕПЕНИ ОХВАЧЕНЫ СУЩЕСТВУЮЩИМИ ДОКУМЕНТАМИ В СФЕРЕ ВОЗДУШНОГО ПРАВА

(Представлено Доминиканской Республикой)

1. СПРАВОЧНАЯ ИНФОРМАЦИЯ

1.1 Ассамблея ИКАО на своей 41-й сессии определила, что некоторые акты или преступления, вызывающие озабоченность сообщества международной гражданской авиации, включая киберугрозы, могут быть в недостаточной степени охвачены существующими документами в сфере воздушного права, в связи с чем необходимо провести правовую работу в области кибербезопасности. Как мы понимаем, усилия, предпринимаемые в этом направлении в последние десятилетия, всегда были связаны с адаптацией к текущим проблемам. В 2022 году Секретариат на 38-й сессии Юридического комитета, проходившей в Монреале, представил доклад подгруппы по изучению правовых аспектов, в котором говорилось, что существующие рамки международного воздушного права отчасти пригодны для противодействия киберугрозам, с которыми сталкивается гражданская авиация.

1.2 Впоследствии в ходе Форума консультантов по правовым аспектам деятельности гражданской авиации (16–17 мая 2019 года) Сингапур представил выводы и рекомендации, согласно которым "проблемы и уязвимости, связанные с кибербезопасностью, являются побочным результатом наступления цифровой эры. Они касаются не только авиационной отрасли, но и всех видов деятельности в нашем обществе. Следовательно, с юридической точки зрения проблемы авиации могут решаться таким же образом, как и проблемы других отраслей". Для решения проблем в сфере кибербезопасности, стоящих перед гражданской авиацией, не следует экономить ресурсы. Необходимо сосредоточиться на комплексном подходе, чтобы меры были приняты во всех областях, связанных с отраслью. В противном случае возникнут новые правовые пробелы.

1.3 Мы согласны со Стратегией в области авиационной кибербезопасности ИКАО 2019 года: "Основной целью международного, регионального и национального законодательства и нормативных положений о кибербезопасности для гражданской авиации является оказание поддержки в осуществлении комплексной стратегии кибербезопасности для защиты гражданской авиации и пассажиров от последствий кибератак". Стратегия также предусматривает, что государства "должны обеспечить разработку и применение соответствующего законодательства и нормативных положений, руководствуясь положениями ИКАО, до реализации своей национальной политики в области кибербезопасности для гражданской авиации". Очевидно, что в сфере технологий и, следовательно, в

[1] Версия на испанском языке предоставлена Доминиканской Республикой.

авиации достигнут значительный прогресс. Из этого следует, что каждое государство приняло меры, связанные с цифровой трансформацией, кибератаками, киберугрозами, конфиденциальностью и защитой данных; из этого также следует, что в некоторых случаях может не потребоваться вносить изменения в национальные и международные инструктивные материалы, руководства, политику и нормативные акты, охватывающие аспекты, связанные с кибербезопасностью, в частности, эксплуатационную безопасность и безопасность полетов.

1.4 В свою очередь, в Плане действий ИКАО по обеспечению кибербезопасности 2022 года говорится, что "государствам рекомендуется провести оценку существующей национальной правовой базы в области кибербезопасности и гражданской авиации, с тем чтобы выявить имеющиеся пробелы, а также обеспечить наличие соответствующего законодательства и нормативных актов в связи с конкретными элементами кибербезопасности гражданской авиации. Еще одним ключевым компонентом является механизм правоприменения, который государствам рекомендуется внедрить, если он еще не существует в их национальной правовой базе, с тем чтобы была введена уголовная ответственность и предусмотрено судебное преследование в связи с незаконными актами против гражданской авиации, совершенными с использованием киберсредств".

2. АНАЛИЗ

2.1 В 2019 году в рамках Стратегии ИКАО в области кибербезопасности государствам было предложено рассмотреть вопрос о необходимости обновления их соответствующего национального законодательства и принятия нового национального законодательства, предусматривающего судебное преследование за кибератаки, связанные с терроризмом, и атаки, негативно влияющие на гражданскую авиацию. Соответствующие законы и нормативные акты, несомненно, существуют. Однако с учетом того, что для правильного применения соответствующих санкций в законодательстве крайне важно определить составы преступлений, государствам срочно необходимо разработать четкие и единообразные руководящие принципы. Недостаточно просто признать важность кибербезопасности в международной гражданской авиации. Руководящие принципы были опубликованы, но технологии развиваются быстрее, чем мы к ним адаптируемся, и мы все еще пытаемся приспособиться к современным разработкам. Пришло время установить юридические обязательства и ответственность государств в этой области.

2.2 Хотя существуют добровольные, необязательные стандарты и недобровольные, обязательные стандарты, такие как приведенные в Приложении 17, необходимо определить, как применять соответствующие принципы международного права и при этом обеспечивать более тщательное соблюдение национальных норм. Нынешние ограничения в каждой стране – будь то законодательные или технологические – не позволяют нам оценивать вероятность угроз в ситуациях, которые, как считается, требуют принятия надлежащих мер.

2.3 В Доминиканской Республике законодательство, такое как Закон № 53-07 (2007 год), охватывает преступления и правонарушения в сфере высоких технологий. Однако мы считаем, что киберугрозы для гражданской авиации, которые возникают или могут возникнуть в будущем, не всегда охватываются или определяются в этом законе или в нашем Уголовном кодексе. Имеются в виду кибертерроризм и кибершпионаж, а также атаки на критически важную инфраструктуру. Кроме того, большинство дел, рассматриваемых прокуратурой, предполагают правоприменение в сфере публичного права в связи с частными жалобами, то есть пострадавшему лицу приходится подавать жалобу и взаимодействовать с прокуратурой на протяжении всего разбирательства, при этом обвиняемый может остаться безнаказанным. Определения должны быть такими, чтобы любое принятое к рассмотрению дело относилось исключительно к сфере публичного права.

2.4 Регулирующие органы, как правило, классифицируют угрозы и/или уязвимости в области информационно-коммуникационных (ИКТ) или эксплуатационных технологий. Безусловно, в последние десятилетия безопасности ИКТ уделяется особое внимание при решении всех административных и технических вопросов. Однако с эксплуатационными технологиями дело обстоит иначе, поскольку внедрение определенных мер защиты происходит в ущерб их эффективному функционированию в таких областях, как аэронавигация и правила полетов; вопрос баланса между эффективностью и безопасностью полетов является предметом постоянных дискуссий.

2.5 Доминиканская Республика приняла меры в соответствии со своей Конституцией, в частности статьей 260, для обеспечения того, чтобы технологические достижения и их влияние на гражданскую авиацию не ставили под угрозу авиационную безопасность, указав, что "приоритетными национальными целями являются: борьба с транснациональной преступностью, которая ставит под угрозу интересы Республики и ее жителей; организация и поддержание эффективных систем, предотвращающих или смягчающих ущерб, причиненный стихийными бедствиями и технологическими катастрофами".

2.6 Впоследствии согласно Указу № 230-18, опубликованному 19 июня 2018 года, была разработана Национальная стратегия кибербезопасности на 2018–2021 гг. и создан Национальный центр кибербезопасности. Группа реагирования на киберинциденты (CSIRT-RD) служит общенациональным координационным центром для предотвращения инцидентов, затрагивающих государственные информационные системы и критическую инфраструктуру, обнаружения таких инцидентов и управления мерами реагирования на них.

2.7 Законопроект 2024 года о комплексном управлении кибербезопасностью в Доминиканской Республике, который в настоящее время находится на рассмотрении Конгресса Республики, направлен на укрепление нормативно-правовой базы для управления кибербезопасностью ИКТ-инфраструктуры органов государственной управления и критически важных объектов инфраструктуры по всей стране. После утверждения этого законопроекта будет создан Национальный совет по кибербезопасности, который станет коллегиальным органом и высшей инстанцией Национального центра кибербезопасности, отвечающей за разработку и руководство политикой по обеспечению кибербезопасности ИКТ-инфраструктуры органов государственного управления и критически важных объектов инфраструктуры.

2.8 В данном законопроекте признаются принципы, изложенные 12 ноября 2018 года в Парижском призыве к доверию и безопасности в киберпространстве и в итоговом докладе Глобальной комиссии по стабильности киберпространства, опубликованном в ноябре 2019 года. Он охватывает, среди прочего, принципы взаимопомощи, предотвращения незаконной деятельности, обмена информацией, защиты прав человека и защиты критически важных объектов инфраструктуры.

2.9 Важно отметить, что, хотя Национальный центр кибербезопасности существует с 2018 года, согласно законопроекту он будет присоединен к Министерству президентства в качестве субъекта публичного права, являющегося юридическим лицом и обладающего функциональной, бюджетной, административной, технической и фискальной автономией; цель состоит в том, чтобы предоставить Центру бóльшую независимость в выполнении его функций.

2.10 Кроме того, в законопроекте рассматриваются критически важные объекты инфраструктуры и информация об инцидентах в сфере кибербезопасности, в частности, порядок их признания, рамки, в соответствии с которыми они будут обозначаться, соответствующие административные процедуры и анализ рисков. В нем дается определение значительного кибервоздействия и системы наказаний. Законопроект призван охватить вопросы, которые до сих пор не рассматривались.

3. ЗАКЛЮЧЕНИЕ

3.1 Очевидно, что успешные действия перед лицом угроз и инцидентов в области кибербезопасности должны основываться на системе, регулирующей принятие превентивных мер, управление эффективными ответными действиями и функционирование соответствующей инфраструктуры. Мы столкнулись с ситуацией, которая затронет всех без исключения, и противостоять ей необходимо также сообща. Доминиканская Республика рассматривает кибербезопасность как вопрос национальной безопасности и поэтому приняла соответствующие меры.

3.2 Мы призываем другие государства, которые еще не приняли таких мер, сделать это столь же энергично. Мы рекомендуем всем государствам, которые еще не задумывались над этим вопросом, пересмотреть свое уголовное, уголовно-процессуальное и процессуальное законодательство, рассматривая этот вид преступления как публичный акт, направленный против национальной безопасности. Мы также настоятельно призываем обновить законодательство и предусмотреть в нем такие уголовные преступления, как кибертерроризм и кибершпионаж, чтобы их можно было преследовать в судебном порядке и надлежащим образом определять в целях обеспечения авиационной безопасности как на национальном, так и на международном уровне. Терминология также должна быть дополнена путем включения новых видов кибератак и киберугроз, возникших в последнее десятилетие.

— КОНЕЦ —