Международная организация гражданской авиации

LC/40-WP/2-7
12/9/26

РАБОЧИЙ ДОКУМЕНТ

ЮРИДИЧЕСКИЙ КОМИТЕТ – 40-Я СЕССИЯ

(Монреаль, 26–30 октября 2026 года)

Пункт 2 повестки дня. Рассмотрение общей программы работы Юридического комитета

УЯЗВИМОСТИ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ, НЕ ПОДПАДАЮЩИЕ ПОД ПОЛОЖЕНИЯ ДЕЙСТВУЮЩЕГО ВОЗДУШНОГО ПРАВА

(Представлено Южной Африкой)

1. ВВЕДЕНИЕ

1.1 Учитывая рост числа кибератак, а также связанных с ними угроз для гражданской авиации и сложностей, присущих организации работы с действующими документами международного права, обеспечению их соблюдения и применимости, критически важно, чтобы государства ускорили анализ действующих документов международного права и закрыли юридические пробелы, снижающие эффективность мер, которые могут быть приняты для обеспечения их соблюдения и предупреждения правонарушений в области кибербезопасности.

1.2 Хотя кибератаки широко распространены, существует несколько проблем, затрудняющих идентификацию правонарушителей, сдерживание и предотвращение их действий и применение необходимых правовых мер. В настоящем документе анализируются эти проблемы, решение которых потребует разностороннего подхода и взятых государствами на себя обязательств предоставить для этого ресурсы.

2. РАССМОТРЕНИЕ ВОПРОСА

2.1 Механизм международного воздушного права подвергается испытаниям угрозами, справляться с которыми изначально не входило в его задачи. Проблема не в том, что международное воздушное право перестало соответствовать реальности; а скорее в том, что имеются поддающиеся выявлению пробелы, связанные с атрибуцией, юрисдикцией, обеспечением соблюдения норм, ответственностью, распространением информации и категоризацией кибератак. Это связано со все большей подверженностью действию среды комбинированных угроз, к которой относится следующее:

a) спонсируемые кибероперации и политически мотивированные действия, нарушающие работу систем;
b) программы-вымогатели и атаки на аэропортовые системы регистрации пассажиров, обработки багажа, системы авиакомпаний и наземного обслуживания;
c) помехи и спуфинг в глобальных навигационных спутниковых системах (GNSS);
d) использование дронов, ракет и систем противовоздушной обороны рядом с маршрутами гражданской авиации;

e) нарушение работы аэронавигационных служб, систем связи и цепочек поставок в авиации;
f) действия хактивистов и зависимых исполнителей, результаты определения спонсоров которых могут быть труднодоказуемы;
g) быстрые изменения доступности воздушного пространства в периоды кризисных ситуаций.

2.2 ИКАО рассматривает эти риски как взаимосвязанные, а не отдельные вопросы "безопасности полетов", "авиационной безопасности" и "кибербезопасности". Взаимосвязанность этих рисков надлежащим образом представлена в документе ИКАО "Глобальный обзор рисков в области кибербезопасности" (Doc 10213).

2.3 Обеспокоенность, вызванная правовыми вопросами более общего характера, также отражена в докладе по итогам недавно проведенного анализа пробелов в отношении потребности в Стандартах и Рекомендуемой практике по авиационной кибербезопасности, в котором дается высокая оценка проделанной работе и результатам, полученным Целевой группой по Стандартам и Рекомендуемой практике в области кибербезопасности, которая сообщила, что самой по себе существующей правовой защиты недостаточно для того, чтобы защитить гражданские воздушные суда в периоды кризисных ситуаций, связанных с кибератаками. Это обусловлено срочной необходимостью в быстром распространении информации, более точной оценке риска и координации действий различных заинтересованных сторон на национальном и международном уровнях в случае кибератаки.

2.4 **Выявленные пробелы**

2.4.1 Кибератаки не всегда четко категоризуются на основе документов международного права как акты незаконного вмешательства. Кибератаки, оказывающие воздействие на безопасность полетов и авиационную безопасность гражданской авиации, часто вызывают следующие вопросы:

a) Когда нарушение работы систем аэронавигации или аэропортов достаточно серьезно, чтобы считаться атакой на гражданскую авиацию, а не обычным киберпреступлением?
b) Какой уровень нарушений работы систем представляет собой угрозу безопасности полетов и авиационной безопасности?
c) Как следует категоризовать кибератаку, которая ведет к негативным экономическим последствиям, но не вызывает физических повреждений или авиационных происшествий?

2.5 Положения действующего международного правового механизма определены с ориентацией на традиционные физические акты, такие как угон воздушного судна, разрушение воздушного судна или атаки на авиационные объекты, а не на кибератаки, которые могут изначально затронуть целостность данных или обработку данных пассажиров.

2.6 **Атрибуция остается основным слабым местом**

2.6.1 Хотя расследователи могут определить инфраструктуру, семейство вредоносной программы или паттерн действий, использованные при атаке, значительно сложнее и тяжелее доказать, кто является стороной, ответственной за атаку. Это создает практический пробел в области ответственности, когда:

a) операция осуществляется группой, являющейся зависимым исполнителем;
b) инфраструктура расположена в нескольких странах;
c) группа использует взломанные системы, принадлежащие невиновным третьим сторонам;
d) некоторое государство предоставляет поддержку, но открыто не руководит конкретной операцией;
e) государство, к которому относится жертва, не может публично раскрыть разведывательные данные, подтверждающие сделанный им вывод;
f) лицо, совершившее атаку, отрицает причастность и выгоду.

2.7 Кибератаки характеризуются сложной организацией и не соответствуют обычным формам атак, нацеленных на нарушение безопасности полетов или авиационной безопасности.

2.8 **Юрисдикция фрагментирована**

2.8.1 С одним авиационным киберинцидентом может быть связано следующее:

a) аэропорты или авиакомпании в различных затронутых государствах;
b) поставщик облачного обслуживания в другой стране;
c) поставщик программного или аппаратного обеспечения в другой стране;
d) инфраструктура для атаки в нескольких территориальных юрисдикциях;
e) пассажиры, имеющие гражданство разных государств;
f) атакующий правонарушитель или зависимая группа, действующие из государства, не желающего сотрудничать.

2.9 **Ответственность и компенсация**

2.9.1 Хотя *Конвенцией для унификации некоторых правил международных воздушных перевозок* (Монреаль, 1999 год) установлены важные правила, касающиеся ответственности авиакомпаний, она не предназначена для того, чтобы служить всесторонним инструментом распределения киберрисков. Среди сложных вопросов, возникающих в связи с кибератаками, следующие:

a) Кто должен возмещать пассажирам убытки, нанесенные в результате кибератаки на аэропорт?
b) Относится ли отмена рейса в результате действия программы-вымогателя к чрезвычайным обстоятельствам?
c) В каких случаях авиакомпания несет ответственность за неспособность поддерживать киберустойчивость?
d) Какую ответственность несут аэропорт, поставщик аэронавигационного обслуживания, поставщик облачного обслуживания или поставщик оборудования?
e) Как следует распределять ответственность, если к возникновению уязвимости причастны несколько организаций?
f) Имеет ли кибератака, затрагивающая системы обработки багажа или регистрации пассажиров, те же правовые последствия, что и атака, затрагивающая системы обеспечения безопасности полетов?

2.10 Отсутствие согласованного международного правового механизма, охватывающего вопросы, связанные с ответственностью в цепочках поставок и нарушениями в эксплуатационной деятельности вследствие проблем с обеспечением кибербезопасности, может приводить к непоследовательным исходам в разных территориальных юрисдикциях.

3. ЗАКЛЮЧЕНИЕ

3.1 Существующие документы международной гражданской авиации не образуют полной, централизованной и включающей разные юрисдикции системы для расследования трансграничных авиационных киберинцидентов, преследования виновных и выплаты компенсации их жертвам. На практике ответственность может разделяться между национальным уголовным законодательством, авиационными нормативно-правовыми механизмами, законодательством о защите данных, законодательством о связи и нормами договорного и международного права.

3.2 ИКАО необходимо через государства принять меры по мобилизации ресурсов в целях разработки всестороннего правового механизма, в котором будут учтены все сочетания факторов и проблемы, связанные с инцидентами в области кибербезопасности.

4. ДЕЙСТВИЯ КОМИТЕТА

4.1 Юридическому комитету предлагается:

a) принять к сведению осуществляемую в настоящее время работу в области анализа применимости действующих документов международного права к решению проблем, связанных с инцидентами в области кибербезопасности, воздействующими на безопасность полетов и авиационную безопасность гражданской авиации;

b) продолжить работу по оценке международного правового механизма, который будет не только охватывать традиционные угрозы безопасности полетов и авиационной безопасности, но и учитывать менее заметные и все более сложные риски, связанные с кибератаками.

— КОНЕЦ —