Правовые аспекты обеспечения безопасности полетов в условиях киберугроз: на примере гражданской авиации

Петрова Р. Е.[*]

Ключевые слова: *цифровые технологии, кибератаки, авиационный транспорт, борт самолета, аэропорт, национальная безопасность, пассажир, необходимость, устройства, уязвимость, рекомендации, эксперты, злоумышленники, террористические организации, хакер, риски, расходы.*

Аннотация.

Статья посвящена анализу современной проблемы правового обеспечения кибербезопасности в авиационной сфере с учетом возрастающего развития информационных технологий, развлекательной индустрии в киберпространстве. Автором рассматриваются существующие рекомендации международного уровня по необходимости внедрения комплексного подхода к использованию новейших разработок на борту самолета и в инфраструктуре современных аэропортов. Кроме того, приводятся мнения экспертов о выявлении потенциальных уязвимостей и видение решения указанных проблем. Автор придерживается точки зрения относительно необходимости соблюдения баланса между современным оснащением и необходимостью поддержания безопасности, с одной стороны, и обеспечением комфортной среды для пассажиров, доступа к гаджетам, с другой. Анализируется соответствие национального законодательства в области обеспечения безопасности полетов в условиях киберугроз международным требованиям и рекомендациям.

DOI: 10.21681/2226-0692-2020-1-56-60

В условиях глобального информационного взаимодействия общества вопросы кибербезопасности рассматриваются учеными как важнейший элемент обеспечения национальной безопасности, детерминирующий приоритеты государственной правовой политики в условиях рисков и угроз [1; 6; 7; 9]. В этих условиях особую актуальность приобретают вопросы кибербезопасности как отклик на современную «цифровую революцию», которая находит свое выражение в создании и бурном развитии современных цифровых, информационно-коммуникационных технологий, их широкого использования в различных сферах деятельности [4, с. 18]. Стремительное развитие современных технологий в информационной сфере можно рассматривать в двух аспектах. С одной стороны, информационные технологии, прежде всего, направлены на поддержание и улучшение жизнедеятельности человека, общества и государства в целом. Однако, с другой стороны, возникает вопрос поддержания качественного уровня безопасности непосредственного использования воздушного судна.

Цифровые технологии формируют новую технологическую среду, в которой действует такой социальный феномен, как право. Более того, цифровые технологии начинают диктовать свои условия, к которым необходимо адаптировать правовые институты, в том числе институты гражданского права [2, с. 25], которые не всегда поспевают за стремительным ростом инноваций.

Принципам правового обеспечения информационной безопасности посвящаются работы, где отмечается актуальность изучения принципов правового обеспечения информационной безопасности в различных аспектах (по сфере их распространения, характеру, функциональному назначению и объекту отображения, по нормативному закреплению, способу выражения в источниках права) [2, с. 39]. Соединение нормативности как свойства того или иного принимаемого в определенном легально установленном порядке акта и концептуальных основ назначения и реализации программ, доктрин стратегического уровня свойственно большинству документов, так или иначе опосредующих регулирование информационных отношений [8, с. 71].

Справедливо утверждение, что за последние годы специалистам удалось добиться высокой отказоустойчивости воздушной техники и наземных систем управления, но, по мнению экспертов, должного внимания вопросам кибербезопасности не уделяется, что само по себе представляет угрозу [3]. Авиатранспортная отрасль характеризуется сочетанием сложности и взаимообусловленности, что делает ее уязвимой и привлекательной мишенью для кибератак. По мере того как авиация подвергается глобальной цифровой трансформации,

[*] ***Петрова Роза Есеновна,*** кандидат юридических наук, доцент кафедры КБ-13 «Гражданско-правовое обеспечение национальной безопасности» ФГБОУ ВО «МИРЭА — Российский технологический университет», г. Москва, Российская Федерация.

E-mail: petrova_r_@mail.ru

возрастает риск просчитанных и преднамеренных кибератак со стороны потенциально расширяющегося количества субъектов, несущих угрозы в своей идеологии, одержимых желанием совершения преступных действий либо дестабилизации жизненного уклада.

Кибератака может привести к крупномасштабному хаосу на крупных транспортных узлах по всему миру и к огромному количеству задержек, отмен рейсов и повышенных предупреждений о безопасности. Нарушение глобальной транспортной сети может привести к всплескам экономических и социальных потрясений. Авиационные инциденты оказывают непропорциональное влияние на общественное сознание, делая потерю доверия пассажиров и деловой репутации предметом озабоченности как для авиакомпаний, так и для аэропортов. Неудивительно, что «Европейская Комиссия считает кибербезопасность проблемой номер один в отрасли воздушного транспорта» — сообщает Майкл Шелленберг, директор по интеграции и услугам SITA[1].

По указанным причинам отрадно видеть, что мировая авиаиндустрия предпринимает шаги по улучшению своей оборонительной позиции. В отчете SITA за 2017 год "AIR TRANSPORT IT Trends Insights" говорится, что приоритетным направлением инвестиций авиакомпаний и аэропортов в информационные технологии является кибербезопасность, причем 95% авиакомпаний и 96% аэропортов планируют инвестировать в крупные программы кибербезопасности или пилотные исследования в течение следующих трех лет. Тем не менее, только 35% авиакомпаний и 30% аэропортов считают, что они уже готовы бороться с любыми киберугрозами сегодня.

Отрасль воздушного транспорта сталкивается с растущим числом путешественников и, соответственно, с увеличенным числом взаимодействий между людьми, устройствами и услугами, а также созданием интеллектуальных аэропортов, внедрением более сложных воздушных судов и информационных технологий.

Слияние информационных и операционных технологий создало новые возможности для преднамеренных кибератак, причем со стороны злоумышленников возможно использование пробелов сначала в сетях информационных технологий, а затем в операционных. С учетом трансформации отрасли, операционная технологическая среда не в состоянии справиться с такими атаками. Кроме того, отрасль сталкивается с двумя противоположными проблемами. С одной стороны — необходимость защитить системы надежной многоуровневой безопасностью, а с другой стороны, обеспечить возможность пассажирам продолжать взаимодействовать с устройствами.

Несомненно, с киберугрозами невозможно справиться, действуя в одностороннем порядке. Авиатранспортная отрасль должна объединить усилия и найти взаимосогласованные способы борьбы с этой реальностью, делясь информацией о реальных угрозах сообщества. Недавние глобальные кибератаки демонстрируют риски и необходимость активного подхода. Отрасль воздушного транспорта очень тесно связана с партнерами и зависит от них. Мы должны работать как сообщество для борьбы с глобальной угрозой кибербезопасности. Расходы на кибербезопасность растут ежегодно. Уровень расходов на кибербезопасность на воздушном транспорте сопоставим с другими сферами. В среднем авиакомпании тратят около 7% их общегодового IT-бюджета по сравнению с аэропортами, которые выделяют около 10% на эти цели. На сегодняшний день кибербезопасность не получает тех инвестиций, которые заслуживает, по сравнению с увеличившимися расходами в 9% и выше в последующие годы. Эти показатели отражают растущее значение защиты баз данных и систем от несанкционированного доступа. 73% респондентов отметили соблюдение нормативных требований и регулирование защиты личных баз данных среди наивысших приоритетов. Это считается важнейшим двигателем инвестиций в безопасность в течении последних трех лет. Расходы на безопасность, как ожидается, будут наблюдаться в сферах по обнаружению и принятию ответных мер в предстоящие годы[2].

При решении проблемы кибербезопасности отрасль воздушного транспорта сталкивается с проблемами, характерными и для других отраслей: нехватка ресурсов, бюджета и навыков. Самым большим барьером на пути внедрения новейших разработок в области кибербезопасности выступает именно нехватка ресурсов, а также набора и удержания квалифицированного персонала в области отражения кибератак.

Основы безопасности создаются с целью постоянного совершенствования. Важным компонентом защиты от кибератак считается осведомленность сотрудников. Построение хорошей базы в IT-безопасности против кибератак становится главным приоритетом авиаиндустрии.

В 2018 в силу вступили правила GDPR[3] — это новый Общий регламент защиты данных Европейского союза (далее — ЕС), который регулирует обработку персональных данных физических лиц, относящихся к компаниям или организациям в ЕС. Этот регламент предусматривает расходы на инструменты безопасности, в частности, на системы идентификации и доступа к технологии управления. Регламентом не охватываются вопросы обработки персональных данных умерших лиц или юридических лиц, а также на данные физического лица, которые собираются им исключительно в личных целях в своем собственном доме, при условии отсутствия коммерческой, профессиональной и иной связи, не относящейся к личным нуждам. В случае же, если указанные персональные данные будут им исполь-

[1] Let's tackle the cyber threat in aviation. URL: https://www.sita.aero/air-transport-it-review/articles/lets-tackle-the-cyber-threat-in-aviation (дата обращения — 12.11.2019).

[2] SITA Air Transport cybersecurity insights, 2018. URL: https://www.icao.int/NACC/Documents/Meetings/2018/ CSEC/D12b-AirTransportCybersecurityInsights2018-SITA.pdf (дата обращения — 10.12.2019).

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1). URL:. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en#_ftn1 (дата обращения — 13.12.2019).

зованы вне своих личных нужд, например, при ведении социокультурной деятельности, Регламентом предписывается неукоснительное соблюдение законодательства о защите персональных данных.

Применение высокотехнологичной продукции стимулирует вовлечение в гражданский оборот имущественных прав на сложные объекты и технологии, включающих множество результатов интеллектуальной деятельности (программы для ЭВМ и базы данных, патенты на изобретения, промышленные образцы и полезные модели, секреты производства, товарные знаки и др.) [3, с. 45].

На сегодняшний день общество стоит перед необходимостью разработки согласованных мер и процедуры принятия решений по защите глобальной системы авиационной отрасли от кибератак. Указанные меры необходимо сочетать с периодическими мероприятиями, направленными на защиту компонентов авиационной отрасли от внешних воздействий. Кроме того, на наш взгляд, обязательно следует руководствоваться рекомендуемой практикой ИКАО, а также актами международного и национального правового регулирования при разработке перспективных IT-технологий в сфере обеспечения кибербезопасности.

Особенно актуально урегулировать и внедрить технологии по решению проблемы кибербезопасности в гражданской авиационной сфере. Эта деятельность требует согласованных усилий всех участников авиационной отрасли. Можно говорить о том, что качественная защита от кибератак в авиации должна стать стратегическим приоритетом в национальной безопасности.

Еще в 2013 году путем многостороннего объединения усилий ИКАО, Международного совета аэропортов (МСА), Организации по аэронавигационному обслуживанию гражданской авиации (КАНСО), Международной ассоциации воздушного транспорта (ИАТА) и Международного координационного совета ассоциаций аэрокосмической промышленности (ИККАИА) была создана Отраслевая группа высокого уровня (IHLG) в целях реализации сотрудничества по вопросам взаимной важности, к которым была отнесена и кибербезопасность. На международном уровне было подчеркнуто, что кибербезопасность представляет проблему приоритетного значения для абсолютно всех заинтересованных сторон, причастных к авиационной сфере.

Основным нормативным актом в области авиационной кибербезопасности можно считать Резолюцию А39-19 «Решение проблем кибербезопасности в гражданской авиации», принятой в ходе 39-й сессии Ассамблеи Международной организации гражданской авиации (ИКАО)[4], а также принятую в ходе 40-й сессии Ассамблеи на её основе Стратегию ИКАО в области кибербезопасности[5]. В данной стратегии отражено отношение ИКАО к обеспечению глобальной кибербезопасности, обеспечении устойчивости авиационного сектора к кибератакам в условиях постоянного развития и внедрения инноваций. Стратегия затрагивает все сегменты авиационной отрасли.

На национальном уровне во исполнение рекомендаций международных актов в Российской Федерации принят Федеральный закон от 26 июля 2017 г. ФЗ-187 «О безопасности критической информационной инфраструктуры Российской Федерации»[6], согласно которому под безопасностью критической информационной инфраструктуры (далее — КИИ, то есть объектов информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления субъектов критической информационной инфраструктуры) понимается состояние защищенности КИИ, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак.

Для целей указанного федерального закона разрабатываются средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные происшествия, в том числе для поиска признаков подобного рода атак в сетях электросвязи, используемых для организаций взаимодействия объектов КИИ, предупреждения и ликвидации последствий кибератак, криптографические средства защиты информации. Уполномоченным центром в указанной области назначается Национальный координационный центр по компьютерным инцидентам.

Одним из объектов КИИ является комплекс информационных систем гражданской авиации. Воздушные суда, аэропортовая инфраструктура оснащаются с каждым днем все более сложным аэронавигационным и иным техническим электронным оборудованием, все больше зависят от компьютеризированных систем, которые потенциально могут быть взломаны хакерами[7], поэтому киберугрозы и атаки как представляли, так и будут представлять реальную опасность для авиации, что подтверждается и рекомендациями ИКАО.

Ведущие авиационные предприятия признают в качестве основной производственной функции эффективное управление безопасностью полетов как баланс интересов целей безопасности полетов и производственного процесса. Несомненно, что эксплуатационные потребности авиаорганизаций отличаются и зависят от организационных, финансовых возможностей. Но все сходятся в одном: при надлежащем внедрении мер по управлению безопасностью полетов повышается не только уровень безопасности, но и качество и результативность работы предприятия в целом.

Эксперты обращают внимание на следующие выявленные виды авиауязвимостей:

- интернет-доступ на борту самолета. Для злоумышленника, владеющего минимальными навыками в сфере IT, не составит труда взломать через эту ин-

[4] Размещена на официальном сайте ИКАО. URL: https://www.icao.int/Meetings/a39/Pages/RU/resolutions_RU.aspx (дата обращения — 09.12.2019).

[5] Размещена на официальном сайте ИКАО. URL: https://www.icao.int/Meetings/a40/Pages/RU/resolutions_RU.aspx (дата обращения — 09.12.2019).

[6] Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства РФ. 2017. № 31 (часть I). Ст. 4736.

[7] Основы кибербезопасности для авиации» — новый курс в рамках программы ИКАО TRAINAIR PLUS. URL: https://avianews.info/osnovy-kiberbezopasnosti-dlya-aviatsii-novyj-kurs-v-ramkah-programmy-ikao-trainair-plus/ (дата обращения — 09.12.2019).

формационно-развлекательную сеть систему управления полетом, к примеру, изменить высоту полета, что в свою очередь, может привести к столкновению с другими воздушными судами. Неоднократно звучали предложения о необходимости разделения этих взаимосвязанных систем: управления самолетом и информационно-развлекательной сетью;

- системы автоматического зависимого наблюдения, вещания, которые позволяют как находящимся на борту пилотам, так и авиадиспетчерам наблюдать за движением всех судов. Эдуард Фальков, главный конструктор Государственного научно-исследовательского института авиационных систем, в интервью отметил, что любой, у кого имеется доступ к данным системам, может «стереть» самолет, а значит, создать угрозу столкновения, либо, наоборот, «дорисовать» несуществующий самолет [10]. Для устранения данной угрозы предлагается создать систему шифрования данных.

Проблемой правового поля является неурегулированость вопроса подключения злоумышленников, находящихся в существенном удалении от борта, к устройствам пассажиров без их на то согласия и ведения, а затем через информационно-развлекательную сеть самолета к устройствам управления полетом.

Обеспечение безопасности полетов в условиях возможных кибератак представляет собой национальный интерес в связи с тем, что воспользоваться такими уязвимостями могут не просто «хакеры-шутники», взламывающие системы безопасности из спортивного интереса, но и радикально настроенные и террористические организации, чтобы создать панику на борту самолета, изменить параметры его полета, что может повлечь за собой человеческие жертвы.

Защита авиационных систем от киберугроз, снижение их уязвимости и обеспечение способности систем к восстановлению функций могут быть достигнуты исключительно за счет применения согласованного глобального подхода, основанного на сотрудничестве и включающего коллективную экспертную работу в области авиационной безопасности, аэронавигации, безопасности систем ICT и участие специалистов из других соответствующих областей[8].

Для обеспечения безопасности существует множество руководств, содержащих рекомендации и инструкции, но все осложняется их зарубежным характером. Так, например, зарубежные авиакомпании руководствуются рекомендациями по оценке безопасности и качества программного обеспечения, согласно которым все бортовые системы должны носить разделенный характер и не пересекаться с процессом управления полетом — RTCA DO-178B, Software Considerations in Airborne Systems and Equipment Certification[9]. Есть требования и по шифрованию, криптографии, которые рекомендованы в авиационной сфере (ISO/IEC 27002 — Code of practice for information security management), однако в России они не используются.

Таким образом, можно сделать следующие выводы. Необходимо привести

- национальную нормативно-правовую базу в соответствие с международными требованиями и рекомендациями, в том числе для защиты от кибератак,
- требования ГОСТ Р ИСО/МЭК 15408 и КТ-178С в соответствие рекомендациям ИКАО для защиты от угроз кибератак в различных типах линий передачи данных.

Назрела необходимость разработать единые рекомендации по защите информации при осуществлении межсистемного информационного обмена не только на борту самолета, но и между бортом самолета и наземными системами.

В заключение отметим, что нам видится целесообразным разработать единый комплексный документ, посвященный сертификации программных и аппаратных средств, обеспечивающих кибербезопасность и обработку информации на борту воздушного судна гражданской авиации, в целях определения возникающих информационных угроз и принятия необходимых и действенных мер по их отражению. Для этого следует объединить усилия не только авиакомпаниям, но и всем заинтересованным в поддержании качества и безопасности полетов.

Цифровизация позволяет авиатранспортной отрасли предоставлять более качественные услуги своим клиентам, но в то же время, как мы увидели, повышает подверженность угрозам, в том числе кибератакам. Крайне важно сегодня объединить усилия заинтересованных сторон для предотвращения вредоносных событий во благо развития промышленности, экономики и общества в целом. Кибербезопасность должна стать не просто вопросом вовлечения в гонку информационных технологий в авиасфере, а средством покрытия перспективных бизнес-рисков для всех субъектов авиатранспортной отрасли.

[8] Решение проблем кибербезопасности в гражданской авиации (Представлено Советом ИКАО) A39-WP/17 EX/5 30/5/16 Ассамблея — 39-я сессия Исполнительный комитет. Пункт 16 повестки дня. Авиационная безопасность. Политика. URL: https://www.icao.int/Meetings/a39/Documents/WP/wp_017_ru.pdf (дата обращения — 13.12.2019).

[9] Document No. RTCA/DO-178B. Software considerations in airborne systems and equipment certification. 1992. URL: https://www.patmos-eng.com/do-254-training-do-178c-training/178c-certification-software .

Литература

1. Атагимова Э.И., Макаренко Г.И., Федичев А.В. Информационная безопасность // Терминологический словарь в определениях действующего законодательства / Федеральное бюджетное учреждение «Научный центр правовой информации при Министерстве юстиции Российской Федерации» (издание 3-е). 448 с.
2. Карцхия А.А. Цифровая трансформация права // Мониторинг правоприменения. 2019. № 1 (30). С. 25—29. DOI: 10.21681/2226-0692-2019-1-25-29.
3. Карцхия А.А. Цифровые права и правоприменение // Мониторинг правоприменения. 2019. № 2 (31). С. 44—46. DOI: 10.21681/2226-0692-2019-2-44-46.
4. Карцхия А.А., Макаренко Г.И., Сергин М.Ю. Современные тренды киберугроз и трансформация понятия кибербезопасности в условиях цифровизации системы права // Вопросы кибербезопасности. 2019. № 3 (31). С. 18—23. DOI: 10.21681/2311-3456-2019-3-18-23.
5. Костюченко Юрий. Кибербезопасность: как защитить авиацию? URL: http://avia.pro/blog/kiberbezopasnost-kak-zashchitit-aviaciyu .
6. Общество: пространство, риски, ценности / Устьянцев В.Б., Гобозов И.А., Пигров К.С. и др., монография / под ред. профессора А. Н. Чумакова. Саратов, 2012. 268 с.
7. Полякова Т. А. Базовые принципы как основные начала правового обеспечения информационной безопасности // Труды Института государства и права Российской академии наук. 2016. № 3 (55). С. 17—40.
8. Рыбаков О.Ю. Приоритеты развития информационного общества в России: правовое обеспечение // Мониторинг правоприменения. 2017. № 3 (24). С. 71—76. DOI: 10.21681/2226-0692-2017-3-71-76.
9. Рыбаков О.Ю., Тихонова С.В. Информационные риски и эффективность правовой политики // Журнал российского права. 2016. № 3 (231). С. 88—95.
10. Шадрина Т. Чтобы никто не смог «стереть» самолет. Системы гражданских самолетов защитят от взломов // Российская газета — Столичный выпуск № 34 (7200). URL: https://rg.ru/2017/02/15/v-rossii-poiavitsia-sistema-zashchity-grazhdanskoj-aviacii-ot-kiberugroz.html .

Рецензент: Морозов Андрей Витальевич, *доктор юридических наук, профессор, заведующий кафедрой Всероссийского университета юстиции (РПА Минюста России), г. Москва, Россия.*
E-mail: av_morozov@list.ru