

АДМИНИСТРАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ТРАНСПОРТНЫХ ОТНОШЕНИЙ

УДК 631.95

Химченко Алексей Игоревич,

кандидат юридических наук, доцент,

Московский государственный юридический университет

имени О. Е. Кутафина (МГЮА)

Беспилотные летательные аппараты:

вопросы безопасности и доверенного использования

Аннотация. Процессы цифровизации способствуют изменению подхода к организации многих технологических процессов. Развитие отрасли беспилотных летательных аппаратов, будучи среди характерных примеров реализации таких преобразований, качественно меняет подход к организации процесса полета. При этом помимо основного происходит преобразование и множества смежных и обеспечивающих процессов, имеющих критическое значение для конечного результата. Развитие технологических решений и усложнение архитектурных подходов по их реализации, увеличение числа субъектов и периметра информационного взаимодействия требуют отдельного подхода к вопросам безопасности информационной инфраструктуры, обеспечивающей реализацию полета. В статье рассматриваются особенности развития беспилотных летательных аппаратов, анализируются тенденции и подходы к обеспечению информационной безопасности, формируются предложения по повышению защищенности информационной инфраструктуры.

Ключевые слова: цифровая среда; информационная инфраструктура; доверие; кибербезопасность; беспилотные летательные аппараты.

Aleksey Ig. Khimchenko,

Candidate of Law, associate professor,

Kutafin Moscow State Law University (MSAL)

Unmanned aerial vehicles: issues of security and trusted use

Abstract. Digitalization processes contribute to changing the approach to the organization of many technological processes. The development of the unmanned aerial vehicle industry, being among the typical examples of the

implementation of such transformations, can qualitatively change the approach to organizing the flight process. At the same time, there is also a transformation of many related and supporting processes that are crucial for the result. The development of technological solutions and the complication of architectural approaches for their implementation, the increase in the number of subjects and the perimeter of information interaction require a separate approach to the security of the information infrastructure that ensures the implementation of the flight. In the current paper there have been considered the features of the development of unmanned aerial vehicles, analyzed trends and approaches to information security enforcement, and developed proposals for improving information infrastructure security.

Keywords: digital environment; information infrastructure; confidence; cybersecurity; unmanned aerial vehicles.

Введение

Стремительное развитие технологий и цифровизация оказывают кардинальное влияние на многие сферы и отрасли промышленности, формируя новые технологические уклады и виды техники, варианты ее применения и способы эксплуатации. Среди таких отраслей особенно выделяется авиационная, беспилотный вариант выполнения которой формирует принципиально новый подход к реализации авиации, расширяя сферу применения и использования, создавая дополнительный потенциал экономического развития.

Возможность использования беспилотных летательных аппаратов (БПЛА) рассматривалась в различных сферах и государственных институтах, что в определенные этапы находило отражение в соответствующих концептуальных и стратегических документах. Например, тенденции развития отрасли связи предусматривают возможности гибридных орбитально-наземных сетей по управлению беспилотными летательными аппаратами в режиме реального времени [распоряжение Правительства РФ от 24 ноября 2023 г. № 3339-р «Об утверждении Стратегии развития отрасли связи Российской Федерации на период до 2035 года»].

В интересах оборонно-промышленного комплекса отмечается необходимость развития «комплексов БПЛА» [Указ Президента РФ от 7 мая 2012 г. № 603 «О реализации планов (программ) строительства и развития Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов и модернизации оборонно-промышленного комплекса»]. МВД России рассматривает возможность использовать информацию, полученную с применением БПЛА, при наблюдении за дорожным движением [приказ МВД России от 2 мая 2023 г. № 264 «Об утверждении Порядка осуществления надзора за соблюдением участниками дорожного движения требований законодательства

Российской Федерации о безопасности дорожного движения»], ФТС России — в части «товаров, перемещаемых беспилотным транспортом» [распоряжение Правительства РФ от 23 мая 2020 г. № 1388-р «Стратегия развития таможенной службы Российской Федерации до 2030 года»]. Допускается возможность взаимодействия с беспилотными воздушными судами при регламентации действий сотрудников органов государственной охраны [постановление Правительства РФ от 11 мая 2020 г. № 654 «Об утверждении Правил применения сотрудниками органов государственной охраны боевой техники»].

Одновременно на концептуальном уровне фиксируется целесообразность совершенствования регулирования использования беспилотных воздушных судов [распоряжение Правительства РФ от 19 августа 2020 г. № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года»].

Вместе с тем, разработка и утверждение Стратегии развития беспилотной авиации [утверждена распоряжением Правительства РФ от 21.06.2023 № 1630-р] ознаменовало новый этап комплексного развития указанной сферы.

Описание

Стратегией на горизонте до 2030 г. предусматривается формирование новой отрасли экономики, ориентированной на создание и использование гражданских БПЛА. Согласно оценкам, объем рынка к 2035 г. может превысить 1 млн БПЛА. Наибольший потенциал их применения сосредоточен в отраслях сельского хозяйства, сфере геопространственных данных, логистике и строительстве.

Концептуальной идеей рассматриваемой технологии является качественное изменение подхода к выполнению полета, не предполагающего наличия пилота, а сама беспилотная авиационная система реализована посредством воздушного средства и соответствующих средств обеспечения движения, управления полетом и контроля.

При этом отрасль беспилотной авиации состоит как непосредственно из беспилотных авиационных систем, так и потенциального спектра оказываемых с их использованием услуг, значительную часть среди которых занимают основанные на сборе и передаче данных.

Указанные виды деятельности подразумевают новые технологические подходы и решения, в том числе принципы взаимодействия между участниками, программное обеспечение, создание и обслуживание информационной инфраструктуры.

Вместе с тем в число профильных технологий, обеспечивающих функционирование, входят системы обнаружения и идентификации объектов, автоматического управления и принятия решений, навигации, контроля состояния обеспечивающих систем, системы оценки угроз.

Столь высокотехнологичная специфика и комплексность элементов системы беспилотной авиации предопределяет необходимость решений по снижению уязвимостей информационной инфраструктуры с учетом существующих рисков.

При этом случаи использования БПЛА в целях разрушения объектов инфраструктуры [1, стр. 24] отражают масштаб критических последствий, и вне зависимости от исходных условий, было ли нанесение ущерба изначально целью или произошло в результате противоправного вмешательства в процесс гражданского полета, указывают на высокий потенциал риска в целом.

Очевидно, что реализовавшиеся риски использования БПЛА в противоправных целях (использования в террористических целях, против общественной опасности и общественного порядка, недобросовестной конкуренции и многие другие) должны быть учтены при поиске и выработке решений по защите информационной инфраструктуры, обеспечивающей их функционирование.

Постановка проблемы

Развитие технологических процессов, обеспечивающих возможность полета, способствует усложнению их архитектуры и расширению инфраструктурного периметра, включающего как сами беспилотные аппараты, так и транспортные и цифровые алгоритмы, системы и сервисы участников движения, пользовательские устройства. В связи с чем, а также принимая во внимание общий рост напряженности в цифровой среде и потенциальную опасность противоправного использования БПЛА, обеспечение их кибербезопасности можно выделить среди наиболее значимых отраслевых вопросов развития.

Указанная проблематика ввиду своей актуальности часто находится в фокусе внимания, в том числе обозначалась в профильных поручениях по развитию отрасли [перечень поручений по вопросам развития беспилотных авиационных систем (утвержден Президентом РФ 30 декабря 2022 г. № Пр-2548)], а также становится предметом изучения научного сообщества.

В исследованиях признается, что обеспечивающие информационные системы подвержены опасности крупномасштабных, автоматизированных и вредоносных атак, реализация которых сопровождается возможным причинением вреда и нанесением материального ущерба [2, стр. 8], отмечается необходимость уделить внимание вопросам правового обеспечения информационной безопасности информационной инфраструктуры беспилотного движения и обрабатываемых данных [3, стр. 125], рассматривается возможность введения в уголовное законодательство квалификации последствий несанкционированного доступа к беспилотному средству [4, стр. 134].

Очевидно, что развитие отрасли подразумевает создание системы правового регулирования беспилотной авиации, подразумевающей

решение многих фундаментальных задач, среди которых разработка понятийного аппарата, определение субъектного состава отношений, решение вопросов распределения и страхования ответственности, определение степени автономности средств и многие другие.

При этом динамика развития отрасли зависит от поиска баланса в решении многих межотраслевых вопросов, достижения безопасности информационной инфраструктуры и соответствующего контроля в условиях оптимизации административных, технических и иных препятствующих развитию ограничений.

Зарождающаяся отрасль при всей инновационности подхода к выполнению полета, функционально реализована посредством технологических решений, подразумевающих вполне определенные подходы к обеспечению безопасности. В связи с чем при наличии определенной специфики информационного взаимодействия составляющих беспилотную систему элементов в целом наследует общие тенденции сферы информационной безопасности, выраженные в отсутствии систематизации и рассредоточении специализированных норм по отдельным нормативным актам [5, стр. 115], необходимости решения системных вопросов в национальной системе права [6, стр. 39], отсутствии правовых средств функционирования института кибербезопасности [7, стр. 173], отсутствии системной координации и централизованного планирования.

Меры и реализация

Не ставя целью в рамках настоящего исследования детально рассмотреть их все, остановимся на тенденциях и подходах к обеспечению кибербезопасности БПЛА, находящих в настоящий момент отражение в законодательных инициативах, концептуальных документах, организации экспериментальных режимов.

Нормами Федерального закона от 4 августа 2023 г. № 487-ФЗ «О внесении изменений в Воздушный кодекс Российской Федерации» с 1 марта 2024 г. Кодекс был дополнен ст. 78.3, установившей требования и порядок оснащения обеспечивающего полет оборудования средствами криптографической защиты информации. При этом реализован подход, при котором указанное оснащение осуществляется владельцами пилотируемых воздушных судов и беспилотных авиационных систем.

Необходимо отметить, что ранее вопрос кибербезопасности уже поднимался законодателем в законопроекте о высокоавтоматизированных транспортных средствах [подготовлен Минтрансом России, ID проекта 02/04/06-21/00116763, текст по состоянию на 10 июня 2021 г.], согласно ст. 6 которого предусматривалось требование к программному обеспечению беспилотных автомобилей противостоять хакерским и террористическим атакам.

Активное внимание проблематике кибербезопасности БПЛА уделяется в концептуальных документах Российской Федерации. Так, подход к

интеграции беспилотных воздушных судов в единое воздушное пространство предусматривает формирование требований по кибербезопасности, а также необходимость обеспечения средствами защиты информации в соответствии с установленными требованиями [распоряжение Правительства РФ от 5 октября 2021 г. № 2806-р «Об утверждении Концепции интеграции беспилотных воздушных судов в единое воздушное пространство Российской Федерации и плана реализации Концепции в части развития технологий»].

Кроме того, на концептуальном уровне рассматривается вопрос применения квантовых коммуникаций в системах высоко- и полностью автоматизированного транспорта, предусматривается возможность оперативной замены алгоритмов защиты информации на квантовобезопасные технологии [распоряжение Правительства РФ от 11 июля 2023 г. № 1856-р «Об утверждении Концепции регулирования отрасли квантовых коммуникаций в Российской Федерации до 2030 года»].

Вместе с тем ведется активное применение БПЛА в рамках экспериментальных правовых режимов (ЭПР), тематика и содержание которых подчеркивает актуальность вопросов обеспечения кибербезопасности. Так, программой ЭПР в сфере цифровых инноваций «Аэрологистика», направленной на проектирование, производство и эксплуатацию в том числе беспилотных воздушных судов [утверждена постановлением Правительства РФ от 2 ноября 2023 г. № 1840], предусмотрена возможность разработки требований по применению средств криптографической защиты информации.

Реализация программы, предусмотренной ЭПР в сфере цифровых инноваций по эксплуатации сельскохозяйственных беспилотных авиационных систем [утверждена постановлением Правительства РФ от 16 сентября 2023 г. № 1510] и направленной на развитие технологий информационно-управляющих систем летательных аппаратов, предусматривает тестирование средств защиты от их противоправного применения, в том числе криптографических.

Кроме того, проводится тестовое использование БПЛА в отдельных регионах в рамках ЭПР в Томской области [постановление Правительства РФ от 24 марта 2022 г. № 458 «Об установлении экспериментального правового режима в сфере цифровых инноваций и утверждении Программы экспериментального правового режима в сфере цифровых инноваций по эксплуатации беспилотных авиационных систем в Томской области»], ЭПР в Камчатском крае, Ханты-Мансийском автономном округе — Югре, Чукотском и Ямало-Ненецком автономных округах [постановление Правительства РФ от 24 марта 2022 г. № 462 «Об установлении экспериментального правового режима в сфере цифровых инноваций и утверждении Программы экспериментального правового режима в сфере цифровых инноваций по эксплуатации беспилотных

авиационных систем в Камчатском крае, Ханты-Мансийском автономном округе — Югре, Чукотском автономном округе и Ямало-Ненецком автономном округе»].

Приоритетные вопросы

Проведенное исследование позволяет отметить активную тенденцию по поиску решений в вопросе достижения кибербезопасности БПЛА. При этом определенные моменты требуют детализации и дополнительной проработки.

1. Необходимо определить состав цифровой инфраструктуры и функциональных сервисов для развития отраслевых решений по информационной безопасности, систем обнаружения и противодействия их противоправному применению.

Также следует предусмотреть развитие системы мониторинга, оценки и управления кибербезопасности в беспилотных авиационных системах, инструментов практической оценки защищенности.

Необходимо разработать реестр потенциальных отраслевых угроз кибербезопасности, выработать ситуационный порядок (при нештатных/аварийных ситуациях), оперативного и стратегического реагирования на инциденты.

2. Вопросом приоритетного внимания является реализация системы обеспечения доверия. Проблематика обусловлена тем, что созданные на основе иностранного оборудования системы обеспечения полетов БПЛА наследуют соответствующие решения безопасности и наложенные в условиях низкого доверия к среде функционирования решения не достигают эффективности.

Необходимо формирование системы обеспечения доверия к оборудованию и программному обеспечению систем управления и контроля БПЛА, использование сертифицированных решений.

3. Разработка юридических механизмов фиксации инцидентов, установления причин и мотивов, оценки и компенсации последствий.

4. Детализация ответственности между разработчиками, операторами и лицами, эксплуатирующими инфраструктуру и сервисы, критериев ее наступления, разработка механизмов страхования ответственности.

Разработка механизма страхования киберриска, включающего методики оценки предварительного состояния защищенности.

5. Отдельным вопросом становится разработка мер оперативного вмешательства в ситуацию, законодательное закрепление подходов к противодействию противоправному использованию беспилотных средств в случае наступления критической ситуации.

Заключение

Беспилотные транспортные средства становятся передовым результатом технологического развития. Формирование актуальной нормативно-правовой среды необходимо для их продуктивного и безопасного функционирования и получения экономического эффекта.

При этом качественное обеспечение кибербезопасности всего цикла технологического процесса их функционирования является критическим фактором успешного функционирования всей зарождающейся отрасли.

Формирование таких решений может осуществляться с учетом рассмотренных факторов.

Литература

1. Корякин, В. М. Правовое обеспечение деятельности подразделений транспортной безопасности по пресечению функционирования беспилотных комплексов: проблемные вопросы / В. М. Корякин // Транспортное право и безопасность. — 2024. — № 1 (49). — С. 23—31.
2. Грачева, Ю. В. Высокоавтоматизированные транспортные средства: угрозы информационной системе безопасности и правовая ответственность / Ю. В. Грачева [и др.] // Государственная власть и местное самоуправление. — 2020. — № 12. — С. 3—9.
3. Полякова, Т. А. Формирование системы беспилотного транспорта: проблемы реализации государственной политики обеспечений информационной безопасности и правового регулирования / Т. А. Полякова, А. И. Химченко // Транспортное право и безопасность. — 2020. — № 2 (34). — С. 118—126.
4. Кочои, С. М. Уголовно-правовые риски использования беспилотных транспортных средств / С. М. Кочои // Актуальные проблемы российского права. — 2021. — № 7. — С. 125—135.
5. Полякова, Т. А. Новые векторы развития системы правового обеспечения информационной безопасности как одного из приоритетов безопасности (к 30-летию принятия Закона Российской Федерации «О безопасности») / Т. А. Полякова, Г. Г. Камалова. // Правовое государство: теория и практика. — 2022. — № 2(68). — С. 112—122.
6. Четвертые Бачиловские чтения: материалы Международной научно-практической конференции / ответственные редакторы Т. А. Полякова, А. В. Минбалеев, В. Б. Наумов. // Институт государства и права РАН. — Москва ; Саратов : Амирит, 2022.
7. Формирование системы правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе: монография / под общей редакцией Т. А. Поляковой. — Москва ; Саратов : Амирит, 2022.
8. Публично-правовые проблемы транспортного права : материалы Пятого международного транспортно-правового форума / под редакцией А. А. Чеботаревой, В. Е. Чеботарева, Л. М. Малёшиной. — Москва : Изд-во Юридического института РУТ (МИИТ), 2023.

References

1. Koryakin, V. M. Pravovoye obespecheniye deyatel'nosti podrazdeleniy transportnoy bezopasnosti po presecheniyu funktsionirovaniya bespilotnykh kompleksov: problemnyye voprosy [Legal support for the activities of transport security units to suppress the functioning of unmanned systems: problematic issues] / V. M. Koryakin // 'Transportnoye pravo i bezopasnost'. — 2024. — № 1 (49). — S. 23—31.
2. Gracheva, YU. V. Vysokoavtomatizirovannyye transportnyye sredstva: ugrozy informatsionnoy sisteme bezopasnosti i pravovaya otvetstvennost' [Highly automated vehicles: threats to the information security system and legal liability] /

- YU. V. Gracheva [i dr.] // Gosudarstvennaya vlast' i mestnoye samoupravleniye. — 2020. — № 12. — S. 3—9.
3. Polyakova, T. A. Formirovaniye sistemy bespilotnogo transporta: problemy realizatsii gosudarstvennoy politiki obespecheniy informatsionnoy bezopasnosti i pravovogo regulirovaniya [Formation of an unmanned transport system: problems of implementing state policy of ensuring information security and legal regulation] / T. A. Polyakova, A. I. Khimchenko // Transportnoye pravo i bezopasnost'. — 2020. — № 2 (34). — S. 118—126.
 4. Kochoi, S. M. Ugolovno-pravovyye riski ispol'zovaniya bespilotnykh transportnykh sredstv [Criminal legal risks of using unmanned vehicles] / S. M. Kochoi // Aktual'nyye problemy rossiyskogo prava. — 2021. — № 7. — S. 125—135.
 5. Polyakova, T. A. Novyye vektory razvitiya sistemy pravovogo obespecheniya informatsionnoy bezopasnosti kak odnogo iz prioritetrov bezopasnosti (k 30-letiyu prinyatiya Zakona Rossiyskoy Federatsii «O bezopasnosti») [New vectors for the development of the system of legal support for information security as one of the security priorities (to the 30th anniversary of the adoption of the Law of the Russian Federation “On Security”)] / T. A. Polyakova, G. G. Kamalova. // Pravovoye gosudarstvo: teoriya i praktika. — 2022. — № 2(68). — S. 112—122.
 6. Chetvertyye Bachilovskiye chteniya: materialy Mezhdunarodnoy nauchno-prakticheskoy konferentsii [Fourth Bachilov Readings: materials of the International Scientific and Practical Conference] / otvetstvennyye redaktory T. A. Polyakova, A. V. Minbaleyev, V. B. Naumov. // Institut gosudarstva i prava RAN. — Moskva ; Saratov : Amirit, 2022.
 7. Formirovaniye sistemy pravovogo regulirovaniya obespecheniya informatsionnoy bezopasnosti v usloviyakh bol'shikh vyzovov v global'nom informatsionnom obshchestve: monografiya [Formation of a system of legal regulation for ensuring information security in the face of great challenges in the global information society] / pod obshchey redaktsiyey T. A. Polyakovoy. — Moskva ; Saratov : Amirit, 2022.
 8. Publichno-pravovyye problemy transportnogo prava : materialy Pyatogo mezhdunarodnogo transportno-pravovogo foruma [Public legal problems of transport law: materials of the Fifth International Transport Legal Forum] / pod redaktsiyey A. A. Chebotarevoy, V. Ye. Chebotareva, L. M. Maloshinoy. — Moskva : Izd-vo Yuridicheskogo instituta RUT (MIIT), 2023.