DOI: 10.17803/1994-1471.2026.185.4.161-175

М. Е. Мунтян*

От национальных стратегий к глобальному консенсусу: международно-правовые аспекты кибербезопасности космической деятельности

Аннотация. Проблема безопасности космической деятельности с каждым годом становится всё острее в связи с достижениями научно-технического прогресса. В поддержании бесперебойного функционирования спутниковых систем особую роль играет кибербезопасность, правовое обеспечение которой является одним из наиболее дискуссионных вопросов в мировом сообществе. Космическая инфраструктура уязвима для киберугроз как технического, так и социально-инженерного характера. В статье рассмотрены инициативы по решению проблемы обеспечения кибернетической безопасности космических систем на национальном, региональном и международно-правовом уровнях; проанализированы основные проблемы, подлежащие разрешению на начальном этапе формирования соответствующей правовой базы; проведена оценка влияния кибербезопасности космической инфраструктуры на управление космическим движением. В завершение подчеркивается необходимость разрешения вопросов обеспечения кибербезопасности космической деятельности преимущественно на уровне многосторонних переговоров, предложены варианты решения поставленной задачи.

Ключевые слова: космос; международное космическое право; кибербезопасность; космическая деятельность; управление космическим движением; космическая безопасность; международное право; спутниковые системы; Комитет ООН по космосу; Будапештская конвенция

Для цитирования: *Мунтян М. Е.* От национальных стратегий к глобальному консенсусу: международно-правовые аспекты кибербезопасности космической деятельности // Актуальные проблемы российского права. — 2026. — Т. 21. — № 4. — С. 161–175. — DOI: 10.17803/1994-1471.2026.185.4.161-175

From National Strategies to Global Consensus: International Legal Aspects of Cybersecurity in Outer Space Activities

Marina E. Muntyan, Head of the Competitions and Grants Department, Autonomous Non-Commercial Organization Research Center for Space Economics and Policy, Postgraduate Student, Department of International Law, MGIMO University, Moscow, Russian Federation
m.e.muntyan@yandex.ru

Abstract. The issue of security in space activities is becoming increasingly acute due to scientific and technological advancements. Cybersecurity plays a crucial role in maintaining the smooth operation of satellite systems, and its

* *Мунтян Марина Евгеньевна*, руководитель направления «Конкурсы и гранты» автономной некоммерческой организации «Исследовательский центр “Космическая экономика и политика”», аспирант кафедры международного права Московского государственного института международных отношений (университета) Министерства иностранных дел Российской Федерации (МГИМО МИД России) Красноармейская ул., д. 4, г. Москва, Российская Федерация, 125167
m.e.muntyan@yandex.ru

legal framework is one of the most controversial issues in the global community. Space infrastructure is vulnerable to cyber threats of both technical and social engineering nature. This paper examines initiatives to address the issue of ensuring cybersecurity of space systems at the national, regional, and international legal levels. It also analyzes the key issues to be addressed at the initial stage of developing the relevant legal framework. It also assesses the impact of cybersecurity of space infrastructure on space traffic management. In conclusion, the need to resolve issues of ensuring cybersecurity in space activities primarily at the level of multilateral negotiations is emphasized, and options for solving this problem are proposed.

Keywords: space; international space law; cybersecurity; space activities; space traffic management; space security; international law; satellite systems; UN Committee on Outer Space; Budapest Convention

Cite as: Muntyan ME. From National Strategies to Global Consensus: International Legal Aspects of Cybersecurity in Outer Space Activities. *Aktual'nye problemy rossijskogo prava*. 2026;21(4):161-175. (In Russ.). DOI: 10.17803/1994-1471.2026.185.4.161-175

В соответствии с данными ABI Research[1], по состоянию на декабрь 2024 г. в космическом пространстве функционировало более 10 тыс. искусственных спутников из более чем 100 стран[2]. Реестр космических объектов ООН говорит о наличии на начало 2025 г. на орбите более 13 тыс. спутников, и речь идет только о тех космических объектах, которые были непосредственно в нем зарегистрированы[3]. При этом практически вся критически важная инфраструктура, к числу которой относятся телекоммуникации, воздушный и морской транспорт, финансовые системы, онлайн-банкинг, системы военной связи и обороны, научный мониторинг, а также интеллектуальные сети, зависит от спутниковых систем. Это понятие включает в себя не только отдельные спутники и их группировки (satellite constellations), но и наземные системы. Космические операции полностью зависят от безопасности киберпространства, через которое проходят восходящие (передача сигнала от наземной станции к спутнику) и нисходящие (от спутника к наземной станции) линии связи, передается информация непосредственно между космическими объектами, а также осуществляется сообщение между наземными станциями, поддерживающими космическую деятельность[4].

Спутниковая система, как правило, включает 3 операционных компонента, а именно космический, наземный и пользовательский сегменты, причем оценка уязвимости спутника для киберугроз по большей части сосредоточена на первых двух[5]. Сами кибернетические угрозы космической деятельности можно разделить на две основные категории: технические и социально-инженерные, заключающиеся в обмане или давлении на ответственных лиц с целью

[1] Международная аналитическая компания, проводящая маркетинговые исследования, стратегический анализ и предоставляющая консультационные услуги по трансформационным технологиям в различных отраслях промышленности.

[2] Over 480 Orbital Launches and 43 000 Active Satellites Expected by 2032 // ABI Research. December 19, 2024. URL: https://www.abiresearch.com/press/over-480-orbital-launches-and-43000-active-satellites-expected-by-2032?utm_source=chatgpt.com (дата обращения: 23.07.2025).

[3] Online Index of Objects Launched into Outer Space // United Nations Office for Outer Space Affairs. URL: https://www.unoosa.org/oosa/osoindex/search-ng.jspx?lf_id=#?c=%7B%22filters%22:%5B%5D,%22sortings%22:%5B%7B%22fieldName%22:%22object.launch.dateOfLaunch_s1%22,%22dir%22:%22desc%22%7D%5D%7D (дата обращения: 23.07.2025).

[4] *Housen-Couriel D.* IAC-21-E-9 (Paper ID: 67116) information sharing for the mitigation of outer space — related cybersecurity threats // Acta Astronautica. 2023. Vol. 203. P. 548.

[5] *Breda P.*, *Markova R.*, *Abdin A. F.,* et al. An extended review on cyber vulnerabilities of AI technologies in space applications: Technological challenges and international governance of AI // Journal of Space Safety Engineering. 2023. Vol. 10. Iss. 4. P. 449.

проникновения в систему[6]. Технические киберугрозы для космической инфраструктуры включают в себя создание помех и, как следствие, ухудшение качества связи, манипулирование данными и взлом действующих систем[7]. Такие вредоносные действия могут быть направлены как против самих спутников, так и против систем управления ими, в том числе наземных центров контроля. Среди конкретных способов осуществления подобных атак особое место занимает смена IP-адреса с целью сокрытия шпионажа, а также создание помех в функционировании навигационных спутниковых систем (например, GPS или ГЛОНАСС). Социально-инженерные кибернетические угрозы, например фишинг[8], направлены на операторов спутниковых систем и предполагают различные способы манипулирования поведением и психологией жертвы с целью получения необходимых для авторизации в системе данных или ее непосредственного взлома.

Несмотря на столь широкий круг угроз, стоящих перед спутниковыми системами и их операторами, обеспечение кибербезопасности современной космической деятельности на данный момент осуществляется исключительно в соответствии с актами национального и регионального характера, т.к. международно-правовые нормы, регулирующие данные отношения, отсутствуют. Первая попытка унифицировать требования к кибербезопасности спутниковых систем на национальном уровне была предпринята лишь в 2013 г., когда Aerospace Industries Association[9] опубликовала Стандарты аэрокосмической кибербезопасности (Aerospace Cybersecurity Standards), предназначенные для обеспечения «динамической оценки рисков и принятия на ее основании соответствующих решений» с целью устранения угроз кибербезопасности и выступающие в качестве дополнения к требованиям Министерства обороны США[10].

Определения понятий «космическое пространство» и «киберпространство» всё еще находятся в процессе разработки как в большинстве национальных правовых систем, так и на международно-правовом уровне. Ни одно из международных соглашений, касающихся космической деятельности (Договор о принципах деятельности государств по исследованию и использованию космического пространства, включая Луну и другие небесные тела, 1967 г., Соглашение о спасании космонавтов, возвращении космонавтов и возвращении объектов, запущенных в космическое пространство, 1968 г., Конвенция о международной ответственности за ущерб, причиненный космическими объектами, 1972 г., Конвенция

---

6 *Carlo A., Manti N. P., Bintang A. S. W. A. M.,* et al. The importance of cybersecurity frameworks to regulate emergent AI technologies for space applications // Journal of Space Safety Engineering. 2023. Vol. 10. Iss. 4. P. 476.

7 *Carlo A.*, *Veazoglou N.* ASAT Weapons: Enhancing NATO's Operational Capabilities in the Emerging Space Dependent Era // Modelling and Simulation for Autonomous Systems: 6th International Conference, MESAS, 2019, Palermo, Italy, October 29–31, 2019, Revised Selected Papers / J. Mazal, A. Fagiolini, P. Vasik (eds.). Springer, 2019.

8 Фишинг (phishing, от fishing — «рыбная ловля, выуживание» и password — «пароль») — вид интернет-мошенничества, цель которого — получить идентификационные данные пользователей информационных систем. См.: Энциклопедия: проект «Лаборатории Касперского». URL: https://encyclopedia.kaspersky.ru/knowledge/what-is-phishing/ (дата обращения: 23.07.2025).

9 Американская торговая ассоциация, представляющая производителей и поставщиков гражданских, военных и бизнес-самолетов, вертолетов, беспилотных летательных аппаратов, спутниковых систем, авиационных двигателей, ракет, материалов и сопутствующих компонентов, оборудования, услуг и информационных технологий в США.

10 *Falco G.* Cybersecurity Principles for Space Systems // Journal of Aerospace Information Systems. 2019. Vol. 16. Iss. 2. P. 1.

о регистрации объектов, запускаемых в космическое пространство, 1975 г. и Соглашение о деятельности государств на Луне и других небесных телах 1979 г.[11]), не затрагивает напрямую вопросы ограничения кибероружия или обеспечения кибербезопасности в рамках космической деятельности. Причина очевидна: во время принятия данных договоров государства если даже и предполагали, насколько частыми будут кибератаки на космическую инфраструктуру в ближайшем будущем, то уж точно не намеревались заложить правовую основу для их предотвращения в рамках фундаментальных соглашений по космосу.

Существует мнение, что не все киберугрозы в отношении спутниковых систем, например взлом наземных систем контроля за спутником с целью хищения данных, подпадают под действие международного космического права, т.к. бóльшая их часть направлена против наземного сегмента космической инфраструктуры[12] и не преследует целей космической деятельности[13]. Классическим примером кибератаки, на которую будут распространяться нормы международного космического права, является вмешательство в управление полетом космического объекта, которое впоследствии приводит к причинению ущерба на поверхности Земли или воздушному судну в полете. В соответствии со ст. II Конвенции о международной ответственности за ущерб, причиненный космическими объектами, в данном случае запускающее государство будет нести абсолютную ответственность за такой ущерб, что, по мнению ряда исследователей, налагает на него «непропорциональное бремя ответственности за кибератаки, которые оно не планировало»[14].

В соответствии со ст. IV Договора о принципах деятельности государств по исследованию и использованию космического пространства, включая Луну и другие небесные тела, 1967 г. государства «обязуются не выводить на орбиту вокруг Земли любые объекты с ядерным оружием или любыми другими видами оружия массового уничтожения, не устанавливать такое оружие на небесных телах и не размещать такое оружие в космическом пространстве каким-либо иным образом»[15]. Из этого следует, что запрет на вывод оружия на орбиту не распространяется на виды вооружений, отличных от оружия массового уничтожения, а также на использование кибероружия как в отношении самих спутников, так и против наземных систем управления ими. Ввиду того что целый ряд спутников, принадлежащих России, США, Китаю и ЕС, имеют двойное назначение, различие между гражданскими и военными целями становится всё более размытым как в киберпространстве, так и в космосе. Это во многом препятствует разработке ключевой терминологии, которая, по сути, стала бы отправной точкой на пути к урегулированию проблем в рассматриваемой области. Например, в рамках универсальных международных соглашений не раскрываются такие понятия, как «кибертерроризм», «кибероружие», «космическое оружие», «кибератака», «киберугроза» и пр. Даже термин «оружие» довольно широк и не поддается универсальному толкованию. Тем не менее официальные испытания систем, в перспективе подпадающих под категорию «кибероружие», уже проводятся. Так, в 2021 г. в рамках программы AsterX Франция совместно с Германией, Италией и США провела первые военные учения, предназначенные для подготов-

[11] *Колосов Ю. М.* Борьба за мирный космос: правовые вопросы. 2-е изд., стер. М. : Статут, 2014. С. 6.

[12] *Li D.* Upgrading space debris mitigation measures to cope with proliferating cyber threats to space activities // Advances in Space Research. 2023. Vol. 71. Iss. 10. P. 4186.

[13] К таким целям относят, например, исследование космоса, разработку космической техники, применение космической техники и внедрение результатов исследования космоса и технологий.

[14] *Suwijak C.* Global Internet Access from the Low Earth Orbit: Legal Issues regarding Cybersecurity in Outer Space // Journal of East Asia and International Law. 2022. Vol. 15. Iss. 1. P. 102.

[15] URL: https://www.un.org/ru/documents/decl_conv/conventions/outer_space_governing.shtml (дата обращения: 23.07.2025).

ки так называемых космических комбатантов[16]. В рамках миссии были отработаны не менее 18 различных космических событий и сценариев, в том числе и подавление спутниковой связи с использованием кибернетических технологий. Официальная цель учений заключается в «подготовке подразделений Космического командования Франции[17] в максимально приближенной к реальной, комплексной, имитируемой среде к решению задач, возникающих в связи с постоянно растущими угрозами различной природы» в космическом пространстве[18]. Программа уже приобрела характер ежегодной, и к ней присоединилась Бельгия. Учения AsterX, проведенные в феврале — марте 2023 г., включали уже 23 космические ситуации, в том числе одну в киберпространстве.

Первым международным договором о преступлениях, совершенных через Интернет и другие компьютерные сети, является Конвенция о преступности в сфере компьютерной информации от 23.11.2001 ETS № 185 (вступила в силу 1 июля 2004 г., далее — Будапештская конвенция)[19], заключенная с целью выработки общей правоохранительной политики для защиты общества от киберпреступности. Тем не менее Конвенция не получила широкого распространения. По состоянию на июнь 2025 г. ее участниками являются 80 государств, среди которых наиболее значимы в области исследования и использования космического пространства США, Япония, Франция, Германия, Великобритания, Италия и Канада[20]. Российская Федерация в Конвенции не участвует. Будапештская конвенция признает в качестве преступлений против конфиденциальности, целостности и доступности компьютерных данных и систем такие действия, как неправомерный доступ к компьютерной системе в целом или любой ее части (ст. 2); неправомерный перехват не предназначенных для общего пользования компьютерных данных (ст. 3); воздействие на компьютерные данные, заключающееся в их умышленном повреждении, удалении, ухудшении качества, изменении или блокировке (ст. 4); воздействие на функционирование компьютерной системы посредством умышленного создания неправомерно серьезных помех ее функционированию путем ввода, передачи, повреждения, удаления, ухудшения качества, изменения или блокировки компьютерных данных (ст. 5); неправомерное использование устройств, включая компьютерные программы, и компьютерных паролей, кодов доступа или иных аналогичных данных, с помощью которых может быть получен доступ к компьютерной системе в целом или любой ее части, с намерением использовать их в целях совершения упомянутых ранее правонарушений (ст. 6).

В 2005 г. Российская Федерация сделала заявление о возможном участии в Будапештской конвенции лишь при условии пересмотра п. «b» статьи 32, положения которой могли быть истолкованы как способные «нанести ущерб суверенитету и национальной безопасности государств-участников, правам и законным интересам их граждан и юридических лиц»[21]. Указанная статья Конвенции предусматривает

---

16 *Delaporte M.* ASTERX 2021: French Space Forces Reach For Higher «Orbit» // Breaking Defense. April 9, 2021. URL: https://breakingdefense.com/2021/04/asterx-2021-french-space-forces-reach-for-higher-orbit/ (дата обращения: 23.07.2025).

17 Созданное в 2019 г. формирование Воздушно-космических сил Франции, которое занимается вопросами обеспечения безопасности космической деятельности.

18 French Space Exercise AsterX Builds on Realistic Scenario and Integration // NATO Allied Air Command. 2023. URL: https://ac.nato.int/archive/2023/FRA_AsterX23 (дата обращения: 23.07.2025).

19 Council of Europe Convention on Cybercrime ETS No. 185 // Council of Europe. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention (дата обращения: 23.07.2025).

20 Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY // Council of Europe. URL: https://www.coe.int/en/web/cybercrime/parties-observers (дата обращения: 21.07.2025).

21 Распоряжение Президента РФ от 15.11.2005 № 557-рп «О подписании Конвенции о киберпреступности» (утратило силу) // СЗ РФ. 2005. № 47. Ст. 4929.

право одной из сторон «получать через компьютерную систему на своей территории доступ к хранящимся на территории другой Стороны компьютерным данным или получать их, если эта Сторона имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой Стороне через такую компьютерную систему» без согласия второй стороны. Положения ст. 32 остались неизменными, в связи с чем в 2008 г. Российской Федерацией было принято решение об отказе от участия в ней[22]. В июне 2021 г. отечественной делегацией был представлен проект Конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях[23] в качестве альтернативы Будапештской конвенции.

Уже 24 декабря 2024 г. резолюцией 79/243 Генеральной Ассамблеи ООН была принята Конвенция ООН против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям[24]. Отмечается, что вопрос создания данного документа стал для российской стороны еще более актуальным «с учетом того, что в 2022 г. Россия перестала быть государством — членом Совета Европы»[25], по большей части в рамках которого действует Будапештская конвенция. Конвенция ООН против киберпреступности, однако, также не содержит положений об особой защите космических систем от киберпреступлений и является актом общего характера.

В 2017 г. Международная группа экспертов под руководством профессора Майкла Н. Шмитта подготовила Таллинское руководство 2.0[26], целью которого являлась оценка применения международного права к кибератакам. Руководство содержит 154 правила проведения кибероперaций, в том числе и в отношении космического пространства, а также подробные комментарии к каждому из них. Под кибератакой авторы Таллинского руководства понимают «кибероперацию как наступательного, так и оборонительного характера, которая, как обоснованно ожидается, может привести к травмам или смерти людей, повреждению или уничтожению объектов»[27]. Таллинское руководство не относит к кибератакам такие виды деятельности, как «психологические кибероперации и кибершпионаж», т.к. они являются ненасильственными[28]. Кибершпионаж, с точки зрения авторов, при его проведении в мирное время не нарушает международное право per se, однако неправомерным может признаваться способ его осуществления (например, если органы одного государства с целью извлечения данных взламывают киберинфраструктуру, расположенную в другом государстве, что приводит к потере ее

[22] Распоряжение Президента РФ от 22.03.2008 № 144-рп «О признании утратившим силу распоряжения Президента РФ от 15 ноября 2005 г. № 557-рп “О подписании Конвенции о киберпреступности”» // СЗ РФ. 2008. № 13. Ст. 1295.

[23] Проект Конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях, 29.06.2021 // Организация Объединенных Наций. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_R.pdf (дата обращения: 23.07.2025).

[24] Организация Объединенных Наций. URL: https://www.un.org/ru/documents/treaty/A-RES-79-243 (дата обращения: 23.07.2025).

[25] *Штодина Д. Д.* Конвенция Организации Объединенных Наций против киберпреступности 2024 г. — итог «киберкомпромисса»? // Московский журнал международного права. 2025. № 1. С. 115.

[26] *Schmitt M.* Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, 2017.

[27] «…A cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects» (*Schmitt M.* Op. cit. P. 415).

[28] *Schmitt M.* Op. cit. P. 415.

функциональности и, следовательно, представляет собой нарушение государственного суверенитета)[29].

В отношении кибернетических операций применительно к космическим деятельности и пространству Руководство предусматривает следующие правила: их проведение должно ограничиваться исключительно мирными целями в понимании «неагрессивных» (п. «a» правила 58)[30]; на них распространяются международно-правовые ограничения на применение силы (п. «b» правила 58); они должны проводиться с должным учетом необходимости избегать вмешательства в мирную космическую деятельность других государств (п. «b» правила 59); другие государства обязаны уважать право государства регистрации на осуществление юрисдикции и контроля над космическими объектами, включенными в его регистры (п. «a» правила 59); государства несут обязательства по санкционированию и контролю за кибернетической деятельностью в космическом пространстве, осуществляемой их неправительственными юридическими лицами (п. «a» правила 60); на кибероперации с участием космических объектов распространяется режим ответственности, предусмотренный нормами международного космического права (п. «b» правила 60)[31]. Указанные правила предлагается распространить на все виды кибероперации, проводимых в космическом пространстве, из него или через него[32].

Еще одной инициативой в данной области является приглашение к столу переговоров, опубликованное Учебным и научно-исследовательским институтом ООН под названием «Право киберпространства»[33]. В отличие от Будапештской конвенции, по большей части затрагивающей чувствительные для любого государства вопросы юрисдикции, оно сосредоточено не только на концепции киберпреступности, но и на таком широком спектре вопросов, как право на доступ к данным, их защита, интеллектуальная собственность и пр. Однако обозначенные акты и документы относительно международно-правового обеспечения кибербезопасности либо носят научный или рекомендательный характер, либо не находят поддержки значительного количества государств, что препятствует формированию единого подхода к вопросам кибербезопасности. Более того, лишь малая их часть напрямую затрагивает проблемы, связанные с кибербезопасностью непосредственно космической деятельности.

Тем не менее определенный прогресс в данной области всё же наблюдается. По вопросу обеспечения кибербезопасности Генеральной Ассамблеей ООН принимаются резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» и «Противодействие использованию информационно-коммуникационных технологий в преступных целях». Еще с 1958 г. в качестве специального, а с 1959 г. в качестве постоянного при ООН функционирует Комитет по использованию космического пространства в мирных целях (далее — Комитет ООН по космосу), а также с 2012 г. работает Группа правительственных экспертов ООН по мерам транспарентности и укрепления доверия в космосе. По результатам деятельности этих органов Генеральной Ассамблеей ООН принимаются такие резолюции, как «Международное сотрудничество в использовании космического пространства в мирных целях» и «Меры по обеспечению транспарентности и укреплению доверия

[29] *Schmitt M.* Op. cit. P. 170.

[30] В самом правиле не употребляется термин «неагрессивные цели», однако соответствующее толкование дано в п. 7 разъяснений к правилу 58. О различии понятий «мирные цели» и «неагрессивные цели» см.: *Колосов Ю. М.* Указ. соч. С. 51–56.

[31] *Schmitt M.* Op. cit. P. 270–283.

[32] *Schmitt M.* Op. cit. P. 270.

[33] *Kamal A.* The Law of Cyber-Space: An Invitation to the Table of Negotiations / United Nations Institute of Training and Research. Geneva, 2005. P. 197.

в космической деятельности»[34]. Ряд проблемных аспектов обеспечения кибербезопасности космической деятельности были рассмотрены первой Рабочей группой по долгосрочной устойчивости космической деятельности, созданной в 2010 г. при Научно-техническом подкомитете Комитета ООН по космосу[35].

В 2021 г. Международный союз электросвязи (МСЭ) выпустил второе издание Справочного руководства по разработке национальной стратегии кибербезопасности[36], участие в работе над которым приняли как межправительственные организации, так и представители частного сектора. Целью Справочного руководства является «помощь ответственным за проведение внешней политики лицам в разработке национальной стратегии кибербезопасности»[37]. Документ, однако, содержит лишь общие рекомендации в отношении обеспечения кибербезопасности, умалчивая о проблемных аспектах ее поддержания в рамках космической деятельности. МСЭ также развивает объявленную еще в 2007 г. Глобальную программу по кибербезопасности[38], в рамках которой был подготовлен и опубликован в марте 2022 г. проект Руководящих принципов, где в качестве первоосновы отдельно обозначена потребность в разработке соответствующей правовой базы[39].

В 2021 г. на площадке Комитета ООН по космосу прозвучало предложение о включении в повестку его Юридического подкомитета проблематики кибербезопасности космической деятельности с целью «анализа касающихся обеспечения кибербезопасности космической деятельности политики, принципов, правил и передового опыта государств» в качестве первого этапа работы и «подготовки материалов (сборника, руководства и т.д.) и их распространения среди государств в качестве рекомендаций для выработки общих подходов к управлению угрозами кибербезопасности космической деятельности»[40], однако ряд государств выразили мнение о том, что круг вопросов, поднимаемых в данном предложении, выходит за рамки деятельности подкомитета[41]. В повестке Научно-технического подкомитета Комитета ООН по космосу подобный пункт также отсутствует.

Во многом более эффективными в решении вопросов кибербезопасности в космической деятельности оказались двусторонние и регио-

[34] *Себекин С.* Кибербезопасность космической инфраструктуры: векторы развития международного сотрудничества // ПИР-Центр. URL: https://pircenter.org/editions/kiberbezopasnost-kosmicheskoj-infrastruktury-vektory-razvitija-mezhdunarodnogo-sotrudnichestva/ (дата обращения: 23.07.2025).

[35] Report of the Scientific and Technical Subcommittee on its Forty-Seventh Session, Held in Vienna from 8 to 19 February 2010. UN Doc. A/AC.105/958 // United Nations Office for Outer Space Affairs. URL: https://www.unoosa.org/oosa/oosadoc/data/documents/2010/aac.105/aac.105958_0.html (дата обращения: 21.07.2025).

[36] Guide to Developing a National Cybersecurity Strategy. 2nd edition // NCS Guide. URL: https://ncsguide.org/the-guide/ (дата обращения: 21.07.2025).

[37] Guide to Developing a National Cybersecurity Strategy. P. 8.

[38] Global Cybersecurity Agenda (GCA) // International Telecommunication Union. URL: https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx (дата обращения: 21.07.2025).

[39] Guidelines for Utilization of the Global Cybersecurity Agenda by the ITU // International Telecommunication Union. URL: https://www.itu.int/en/action/cybersecurity/Documents/Guidelines%20for%20utilization%20of%20the%20GCA.pdf (дата обращения: 23.07.2025).

[40] The Proposal of the Ukrainian Delegation on the Establishment of a New Item on the Agenda of the Legal Subcommittee on the Cybersecurity of Space Activities, Submitted to United Nations Committee on the Peaceful Uses of Outer Space, Legal Subcommittee, 60th Session, Vienna, 2021. UN Doc. A/AC.105/C.2/2021/CRP.27 // United Nations Office for Outer Space Affairs. URL: https://www.unoosa.org/oosa/en/oosadoc/data/documents/2021/aac.105c.22021crp/aac.105c.22021crp.27_0.html (дата обращения: 21.07.2025).

[41] Доклад Юридического подкомитета о работе его шестидесятой сессии, проведенной в Вене 31 мая — 11 июня 2021 г. // Организация Объединенных Наций. URL: https://documents.un.org/doc/undoc/gen/v21/047/19/pdf/v2104719.pdf (дата обращения: 23.07.2025). П. 267.

нальные соглашения. Например, еще в 2013 г. США и Россия создали постоянную Рабочую группу по вопросам безопасности киберпространства, двусторонние переговоры в рамках которой привели к принятию ряда мер по обеспечению транспарентности и укреплению доверия в указанной сфере[42]. В 2015 г. Россия и Китай подписали двустороннее соглашение, содержащее взаимный запрет на проведение кибероперациий друг против друга[43]. Государства также договорились совместно реагировать на технологии, которые, по их мнению, могут оказать дестабилизирующее воздействие на политическую и социально-экономическую сферы или позволяют вмешиваться во внутренние дела государств.

Всё бóльшую популярность получает заключение соглашений по кибербезопасности на региональном уровне. Например, в рамках ЕС действует Директива Совета Европы 2008/114/ЕС об идентификации и обозначении европейских критических инфраструктур и оценке необходимости улучшения их защиты (Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection), принятая 8 декабря 2008 г. Она интересна тем, что в ней к критической причисляется и так называемая цифровая инфраструктура. Несмотря на то что космические объекты и системы сами по себе не признаются в рамках Директивы критически важной инфраструктурой, в ряде исследований отмечается, что они могут рассматриваться как таковая, поскольку прямо или косвенно обеспечивают функционирование всех непосредственно признаваемых критическими инфраструктур (в том числе в сфере энергетики, транспорта, банковского дела, здравоохранения, цифровых технологий и т.д.)[44].

В 2019 г. Европейское космическое агентство запустило проект «Финансирование и поддержка космических служб кибербезопасности» (Cyber security and space based services), задействующий компании, которые занимаются разработкой инновационных продуктов и услуг в области информационно-коммуникационных технологий. Программа сосредоточена на инициативах по обеспечению устойчивости служб, инфраструктур и операций, вовлеченных в осуществление космической деятельности и подверженных возможным киберугрозам. Ключевыми областями являются транспорт (морской, наземный и воздушный, включая автономные транспортные средства), энергетика, коммунальные услуги, финансы и общественная безопасность.

Стремительный рост объема данных, собираемых и предоставляемых спутниками, требует использования новых технологий для их быстрого и точного анализа, в связи с чем в космической деятельности всё чаще используются системы искусственного интеллекта (ИИ)[45]. Так, НАСА (National Aeronautics and Space Administration, NASA) уже на протяжении нескольких лет активно внедряет ИИ в космические системы, а 18 мая 2022 г. марсоход Perseverance впервые использовал ИИ AEGIS с целью обнаружения, фокусировки изображения и самостоятельного изучения определенного камня без команды с Земли[46]. Двумя годами ранее был запущен первый европейский спутник с использованием ИИ в целях наблюдения за Землей под названием Phi-Sat-1 (ϕ-Sat-1)[47]. В декабре 2023 г. Европейский парламент и Европейский совет

[42] *Bilodeau M.* The risk that cyber-attacks pose to outer space assets: how can international dialogue and cooperation help? McGill University, Institute of Air and Space Law, 2020. P. 47.

[43] *Roth A.* Russia and China Sign Cooperation Pacts // New York Times. May 8, 2015. URL: https://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html (дата обращения: 20.01.2025).

[44] *Bilodeau M.* Op. cit. P. 53.

[45] *Carlo A.*, *Manti N. P.*, *Bintang A. S. W. A. M.,* et al. Op. cit. P. 475.

[46] Perseverance's SuperCam Uses AEGIS for the First Time // NASA Science. May 31, 2022. URL: https://mars.nasa.gov/resources/26782/perseverances-supercam-uses-aegis-for-the-first-time/ (дата обращения: 21.07.2025).

[47] ϕ-sat. Artificial intelligence for Earth observation // European Space Agency. URL: https://www.esa.int/Applications/Observing_the_Earth/Ph-sat (дата обращения: 21.07.2025).

достигли предварительного соглашения по проекту Закона ЕС об искусственном интеллекте[48], положения которого в зависимости от сферы действия вступят в силу в 2025, 2026 и 2027 гг.[49] Его целями являются гармонизация правил размещения на рынке, ввода в эксплуатацию и использования систем ИИ; установление запретов на определенные системы ИИ; особых требований к системам ИИ высокого риска; правил мониторинга и надзора за рынком и пр.[50] Вопрос о применимости Закона к космическим системам, функционирующим с помощью ИИ, неоднозначен. Закон устанавливает ряд правил в отношении различных категорий систем ИИ, кроме систем ИИ, разработанных или используемых исключительно в военных целях, в целях обороны или национальной безопасности, независимо от типа организации, осуществляющей эту деятельность[51]. Закон также предъявляет особые требования к системам ИИ высокого риска, перечень которых представлен в приложении III к Закону, где, однако, космические системы не перечислены[52].

Государства Северной и Южной Америки также провели определенную работу в области обеспечения кибербезопасности, в частности в рамках Организации американских государств (ОАГ). Под ее эгидой действует Группа правительственных экспертов по киберпреступности, главными направлениями работы которой являются анализ преступной деятельности, связанной с компьютерными сетями, сравнение национальных законодательств и выявление национальных и международных организаций, обладающих соответствующим опытом. По итогам работы данной группы Генеральная Ассамблея ОАГ одобрила Межамериканскую комплексную стратегию борьбы с угрозами кибербезопасности. В 2012 г. ОАГ также была одобрена Декларация об укреплении кибербезопасности в Северной и Южной Америке, призывающая к разработке национальных стратегий в области кибербезопасности и укреплению механизмов международного сотрудничества.

Вопросы обеспечения кибербезопасности в Азиатском регионе рассматривались на уровне Ассоциации государств Юго-Восточной Азии (АСЕАН). Совет по сотрудничеству в области безопасности в Азиатско-Тихоокеанском регионе в Меморандуме № 20 «Обеспечение более безопасной киберсреды» (Ensuring a Safer Cyber Security Environment) рекомендовал интеграционному объединению осуществить меры по наращиванию кибернетического потенциала и оказанию технической помощи. В рамках АСЕАН принят также План действий по борьбе с транснациональной преступностью, рассчитанный на 2016–2025 гг. и рассматривающий в том числе вопросы кибербезопасности. Однако в настоящее время какого-либо целостного акта, регулирующего вопросы кибербезопасности в космической деятельности, нет. Это объясняется довольно существенным разрывом в экономическом развитии между государствами Азии, а также тем, что среди азиатских стран активным освоением космического пространства занимаются в основном Китай и Япония.

Наконец, обратимся к национальным стратегиям в области кибербезопасности и космической деятельности. Так, за последнее деся-

[48] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance) // EUR-Lex. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32024R1689 (дата обращения: 20.07.2025).

[49] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. Document 52021PC0206 // EUR-Lex. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206 (дата обращения: 20.07.2025).

[50] Artificial Intelligence Act. Art. 1.

[51] Artificial Intelligence Act. Art. 2(3).

[52] *Breda P.*, *Markova R.*, *Abdin A. F.,* et al. Op. cit. P. 454.

тилетие в США были разработаны различные стратегические документы, касающиеся улучшения кибербезопасности в космической области, включая Национальную киберстратегию 2018 г. и Директиву по космической политике — 5 (Space Policy Directive-5, SPD-5)[53]. Как и прочие директивные документы, принятые во время первого срока президента Дональда Трампа, указанная Директива подчеркивает его стремление создать комплексную систему защиты американских интересов в космическом пространстве[54].

В разделе 1 Директивы подчеркивается приверженность США принципу неограниченной свободы действий в космосе для обеспечения безопасности, экономического процветания и научных знаний нации, что сразу вызывает ряд вопросов, в особенности в отношении словосочетания «неограниченная свобода действий». Там же делается отсылка к Стратегии национальной безопасности США от 18.12.2017, где отмечается особая роль США в сохранении лидерства и свободы действий в космосе. На данный момент в государстве идет активная работа по созданию Системы координации движения в космосе (Traffic Coordination System for Space, TraCSS), которая, как предполагается, возьмет на себя функции по управлению гражданским космическим движением посредством сбора данных из Министерства обороны и других источников и их использования для предупреждения о потенциальных близких подходах к операторам спутниковой связи[55]. Данная информация, как и сами каналы ее передачи, потенциально подпадает под понятие космических систем, к которым в соответствии с Директивой должны применяться меры киберзащиты. В общем и целом Директива, как и иные подобные документы, преисполнена убежденностью в «первенстве и превосходстве американской нации» в космическом и киберпространстве, но не содержит каких-либо значительных новшеств в регулировании рассматриваемой деятельности. В Российской Федерации такие документы отсутствуют.

Ряд государств, активно занимающихся исследованием и использованием космоса, опираются в своей деятельности на технические руководства по обеспечению кибербезопасности космической инфраструктуры. Так, в 2023 г. Япония представила обновленные Руководящие принципы по мерам кибербезопасности коммерческих космических систем[56], в которых «обозначены факторы риска и описаны необходимые меры по смягчению последствий атак на уровне подсистемы»[57]. Аналогичный документ был принят в том же году в Германии: Базовый профиль IT-защиты для космической инфраструктуры (IT-Grundschutz-Profil für Weltrauminfrastrukturen)[58] определяет минимальные требования к кибербезопасности

[53] Memorandum on Space Policy Directive-5 — Cybersecurity Principles for Space Systems // Trumpwhitehouse.gov. September 4, 2020. URL: https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/ (дата обращения: 20.07.2025).

[54] *Уваров В. Б.* Космическое наследие Дональда Трампа // Россия в глобальной политике. 2021. Т. 19. № 2 (108).

[55] *Уваров В.* Космические штрафы и «американский ЦОДД» // Россия в глобальной политике. 04.09.2023. URL: https://globalaffairs.ru/articles/kosmicheskie-shtrafy/ (дата обращения: 20.07.2025).

[56] Cybersecurity Guidelines for Commercial Space Systems. Ver. 1.1 / Space Industry Office, Manufacturing Industries Bureau, Ministry of Economy, Trade and Industry (METI) // URL: https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_uchu_sangyo/pdf/20230331_1e.pdf (дата обращения: 20.07.2025).

[57] *Falco G.*, *Henry W.*, *Aliberti M.,* et al. An International Technical Standard for Commercial Space System Cybersecurity — A Call to Action // ASCEND, 24–26 October 2022, Las Vegas, Nevada & Online. AIAA 2022-4302. Session: Methods and Considerations for Cyber Protection of Space Assets. ASCEND, 2022. P. 4.

[58] IT-Grundschutz-Profil für Weltrauminfrastrukturen. 30.06.2022 // Bundesamt für Sicherheit in der Informationstechnik. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Profil_Weltrauminfrastrukturen.html (дата обращения: 20.07.2025).

спутников, предусматривает установление особых требований к защите спутниковых группировок (Zahlreiche Satellitensysteme) и предлагает различные варианты защиты в случае кибернетических атак против космической инфраструктуры[59]. Оба акта носят рекомендательный характер.

В общем контексте обеспечения безопасности космической деятельности необходимо обратиться и к такому аспекту, как управление космическим движением. Несмотря на то что на данный момент существуют широкомасштабные проекты по мониторингу космического пространства, которые осуществляются в основном Системой контроля космического пространства РФ, Сетью космического наблюдения США (Space Surveillance Network) и Системой космического наблюдения и слежения ЕС (Space Surveillance and Tracking), они зачастую работают независимо и разрозненно. На данный момент не существует единой всеобъемлющей системы мониторинга космических объектов, направленной на предотвращение столкновения космических объектов друг с другом и с космическим мусором. Российская Федерация, выступающая за разрешение вопросов космической безопасности исключительно на международном уровне, в 2016 г. представила в Комитете ООН по космосу рабочий документ «Дополнительные идеи относительно совокупности целей достижения Венского консенсуса по безопасности в космосе и необходимости в серьезном осмыслении модальностей рассмотрения сложных проблем, связанных с управлением движением в космосе, и оправданности больших ожиданий скорых решений в этой области»[60], в котором отражена позиция государства относительно международно-правового режима управления космическим движением. В нем отечественная делегация предложила создать единую информационную платформу в рамках ООН в качестве механизма, объединяющего усилия государств, международных межправительственных организаций, операторов космических аппаратов, специализированных национальных агентств и международных неправительственных организаций по сбору, систематизации, обмену и анализу информации о мониторинге объектов и явлений в космическом пространстве. Предложение, однако, до сих пор не нашло широкой поддержки у западных государств.

Довольно известным примером столкновения космических аппаратов в связи с невозможностью единовременного отслеживания каждого из них всеми заинтересованными государствами является авария с участием спутников «Космос-2251» и Iridium 33 в 2009 г. Уже не функционирующий к тому моменту российский спутник «Космос-2251» столкнулся с Iridium 33, который, несмотря на отслеживание именно американскими военными, не был зарегистрирован в Реестре космических объектов ООН. В соответствии с п. «с» ст. I Конвенции о международной ответственности за ущерб, причиненный космическими объектами, под непосредственно запускающим государством понимается:

«i) государство, которое осуществляет или организует запуск космического объекта,

ii) государство, с территории или установок которого осуществляется запуск космического объекта»[61].

---

[59] *Falco G.*, *Henry W.*, *Aliberti M.,* et al. Op. cit. P. 4.

[60] Рабочий документ, представленный Российской Федерацией, A/AC.105/2016/CRP.13 «Дополнительные идеи относительно совокупности целей достижения Венского консенсуса по безопасности в космосе и необходимости в серьезном осмыслении модальностей рассмотрения сложных проблем, связанных с управлением движением в космосе, и оправданности больших ожиданий скорых решений в этой области» // Committee on the Peaceful Uses of Outer Space, Fifty-ninth session, Vienna, 8–17 June 2016. URL: https://www.unoosa.org/res/oosadoc/data/documents/2016/aac_1052016crp/aac_1052016crp_13_0_html/AC105_2016_CRP13E.pdf (дата обращения: 20.07.2025).

[61] Конвенция о международной ответственности за ущерб, причиненный космическими объектами, от 29.11.1971 (вступила в силу 1 сентября 1972 г.) // Организация Объединенных Наций. URL: https://www.un.org/ru/documents/decl_conv/conventions/damage.shtml (дата обращения: 21.07.2025).

В соответствии с данными положениями, а также с требованиями о регистрации космического объекта в Реестре ООН[62] запускающим государством спутника «Космос-2251» являлась Российская Федерация, в то время как ситуация с Iridium 33 не была достаточна ясной, поскольку он не был зарегистрирован в указанном Реестре. Несмотря на то что оба спутника отслеживались компетентными представителями военных подразделений соответствующих государств, столкновение всё же произошло, в связи с чем и были впоследствии созданы вышеуказанные системы контроля и наблюдения. Данный шаг во многом поспособствовал усилению безопасности в космическом пространстве. Тем не менее наличие автономных систем мониторинга, не находящихся в достаточно тесном взаимодействии, поднимает ряд других вопросов.

Во-первых, ни одна система не является совершенной и не может отследить каждый космический объект. Данные существенно разнятся, в особенности в отношении спутников, не зарегистрированных в национальных регистрах или же в Реестре ООН. Ситуацию осложняет возрастающая популярность группировок спутников, действующих взаимосвязанно и зачастую обладающих сравнительно малым размером и весом, что делает их отслеживание затруднительным. Кроме того, существуют спутники, в принципе лишенные маневренности и, следовательно, представляющие бóльшую опасность с точки зрения столкновения с другими космическими объектами.

Во-вторых, данные системы также подвержены кибератакам, причем не с одной лишь целью кражи. Наиболее опасным представляется перехват управления спутником или целой системой спутников, в особенности если они осуществляют управление воздушными, наземными и морскими вооружениями, а также транспортной, банковской и иной инфраструктурой. Например, еще 1998 г., проникнув в систему Центра космических полетов Годдарда в США, хакеры взяли под контроль американо-немецкий исследовательский спутник ROSAT X-Ray и направили его солнечные батареи прямо на солнце, что привело к выведению спутника из строя[63].

Правила в отношении обеспечения кибербезопасности космических систем находят отражение по большей части в актах национального и регионального характера. При этом наблюдается тенденция невключения космической инфраструктуры в критическую и, следовательно, подлежащую особой защите, что вызывает опасения относительно направления развития нормативного регулирования в данной области. Тем временем ученые прогнозируют увеличение в будущем таких обусловленных политическими тенденциями киберугроз, как «перехват, подмена информации и глушение сигналов при растущей зависимости наземной критически важной инфраструктуры от систем космического базирования»[64]. Высказываются предложения о разработке международных стандартов кибербезопасности космической инфраструктуры в рамках Института инженеров электротехники и электроники (Institute of Electrical and Electronics Engineers)[65] или Международной организации по стандартизации (International Organization for Standardization)[66]; об обсуждении на мировом уровне проблем защиты не только самих космических объектов и систем,

[62] Ст. III Конвенции о регистрации объектов, запускаемых в космическое пространство, от 12.11.1974 (вступила в силу 15 сентября 1976 г.) // Организация Объединенных Наций. URL: https://www.un.org/ru/documents/decl_conv/conventions/objects_registration.shtml (дата обращения: 20.07.2025).

[63] *Tucker P.* The NSA Is Studying Satellite Hacking // Defense One. September 20, 2019. URL: https://www.defenseone.com/technology/2019/09/nsa-studying-satellite-hacking/160009/ (дата обращения: 20.07.2025).

[64] *Housen-Couriel D.* Op. cit. P. 549.

[65] Некоммерческая профессиональная ассоциация, целью которой является содействие развитию и продвижению технических и технологических инноваций во всех областях, связанных с применением электроэнергии.

[66] *Falco G.*, *Henry W.*, *Aliberti M.,* et al. Op. cit. P. 5.

но и спутниковых данных[67]; о распространении принципов особой защиты критической инфраструктуры на космические системы на уровне национального законодательства[68] и т.д.

Впрочем, решение обозначенных проблем кроется прежде всего в обеспечении многосторонних переговоров и готовности государств пойти на взаимные уступки с целью поддержания не только национальной, но и глобальной безопасности. Представляется, что на данный момент разработка единого международно-правового акта, предметом которого являлась бы кибербезопасность в космической деятельности, маловероятна и даже нецелесообразна. Во-первых, к настоящему времени не существует единого и согласованного подхода мирового сообщества к проблемам киберпреступности. Для создания более детального, узконаправленного документа сначала необходимо принять общее соглашение по вопросам кибербезопасности в целом, а также оценить его эффективность. Во-вторых, техническая составляющая во многом опережает правовую базу, что в том числе касается и космической отрасли. В связи с этим оптимальным видится следующий порядок действий: продолжение многосторонних переговоров по вопросам кибербезопасности в целом; разработка рекомендательных норм с их последующей детализацией с целью применения в космической деятельности; создание рабочей группы по вопросам кибербезопасности в космическом пространстве. Возможны также работа над текстом универсальной конвенции по вопросам кибербезопасности с включением космической отрасли в перечень критической инфраструктуры, подлежащей особой защите, или включение положений о кибербезопасности и киберугрозах в отношении космической деятельности в новое всеобъемлющее соглашение по космическому праву, вероятность принятия которого, однако, в текущих условиях также находится под большим сомнением. Однако ни первый, ни второй вариант решения проблемы не получит развития вне согласованной работы всего международного сообщества, что потребует постепенных, порой кажущихся незначительными шагов в сторону консенсуса.

БИБЛИОГРАФИЯ

1. *Колосов Ю. М.* Борьба за мирный космос: правовые вопросы. — 2-е изд., стер. — М. : Статут, 2014. — 176 с.
2. *Уваров В. Б.* Космическое наследие Дональда Трампа // Россия в глобальной политике. — 2021. — Т. 19. — № 2 (108). — С. 131–146.
3. *Штодина Д. Д.* Конвенция Организации Объединенных Наций против киберпреступности 2024 г. — итог «киберкомпромисса»? // Московский журнал международного права. — 2025. — № 1. — С. 110–124.
4. *Bilodeau M.* The risk that cyber-attacks pose to outer space assets: how can international dialogue and cooperation help? — McGill University, Institute of Air and Space Law, 2020. — 129 p.
5. *Breda P.*, *Markova R.*, *Abdin A. F.*, *Manti N. P.*, *Carlo A.*, *Jha D.* An extended review on cyber vulnerabilities of AI technologies in space applications: Technological challenges and international governance of AI // Journal of Space Safety Engineering. — 2023. — Vol. 10. — Iss. 4. — P. 447–458.
6. *Carlo A.*, *Manti N. P.*, *Bintang A. S. W. A. M.*, *Casamassima F.*, *Boschetti N.*, *Breda P.*, *Rahloff T.* The importance of cybersecurity frameworks to regulate emergent AI technologies for space applications // Journal of Space Safety Engineering. — 2023. — Vol. 10. — Iss. 4. — P. 474–482.
7. *Carlo A.*, *Veazoglou N.* ASAT Weapons: Enhancing NATO's Operational Capabilities in the Emerging Space Dependent Era // Modelling and Simulation for Autonomous Systems: 6th International Conference, MESAS, 2019, Palermo, Italy, October 29–31, 2019, Revised Selected Papers / J. Mazal, A. Fagiolini, P. Vasik (eds.). — Springer, 2019. — P. 417–426.

[67] *Carlo A.*, *Manti N. P.*, *Bintang A. S. W. A. M.,* et al. Op. cit. P. 478.

[68] *Falco G.* Op. cit. P. 7.

8. *Falco G.* Cybersecurity Principles for Space Systems // Journal of Aerospace Information Systems. — 2019. — Vol. 16. — Iss. 2. — P. 1–10.
9. *Falco G.*, *Henry W.*, *Aliberti M.,* et al. An International Technical Standard for Commercial Space System Cybersecurity — A Call to Action // ASCEND, 24–26 October 2022, Las Vegas, Nevada & Online. AIAA 2022-4302. Session: Methods and Considerations for Cyber Protection of Space Assets. — ASCEND, 2022. — P. 1–8.
10. *Housen-Couriel D.* IAC-21-E-9 (Paper ID: 67116) information sharing for the mitigation of outer space — related cybersecurity threats // Acta Astronautica. — 2023. — Vol. 203. — P. 546–550.
11. *Kamal A.* The Law of Cyber-Space, An Invitation to the Table of Negotiations / United Nations Institute of Training and Research. — Geneva, 2005. — 269 p.
12. *Li D*. Upgrading space debris mitigation measures to cope with proliferating cyber threats to space activities // Advances in Space Research. — 2023. — Vol. 71. — Iss. 10. — P. 4185–4195.
13. *Schmitt M.* Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. — Cambridge University Press, 2017. — 648 p.
14. *Suwijak C.* Global Internet Access from the Low Earth Orbit: Legal Issues regarding Cybersecurity in Outer Space // Journal of East Asia and International Law. — 2022. — Vol. 15. — Iss. 1. — P. 93–108.

Материал поступил в редакцию 23 июля 2025 г.

REFERENCES (TRANSLITERATION)

1. Kolosov Yu. M. Borba za mirnyy kosmos: pravovye voprosy. — 2-e izd., ster. — M.: Statut, 2014. — 176 s.
2. Uvarov V. B. Kosmicheskoe nasledie Donalda Trampa // Rossiya v globalnoy politike. — 2021. — T. 19. — № 2 (108). — S. 131–146.
3. Shtodina D. D. Konventsiya Organizatsii Obedinennykh Natsiy protiv kiberprestupnosti 2024 g. — itog «kiberkompromissa»? // Moskovskiy zhurnal mezhdunarodnogo prava. — 2025. — № 1. — S. 110–124.
4. Bilodeau M. The risk that cyber-attacks pose to outer space assets: how can international dialogue and cooperation help? — McGill University, Institute of Air and Space Law, 2020. — 129 p.
5. Breda P., Markova R., Abdin A. F., Manti N. P., Carlo A., Jha D. An extended review on cyber vulnerabilities of AI technologies in space applications: Technological challenges and international governance of AI // Journal of Space Safety Engineering. — 2023. — Vol. 10. — Iss. 4. — P. 447–458.
6. Carlo A., Manti N. P., Bintang A. S. W. A. M., Casamassima F., Boschetti N., Breda P., Rahloff T. The importance of cybersecurity frameworks to regulate emergent AI technologies for space applications // Journal of Space Safety Engineering. — 2023. — Vol. 10. — Iss. 4. — P. 474–482.
7. Carlo A., Veazoglou N. ASAT Weapons: Enhancing NATO's Operational Capabilities in the Emerging Space Dependent Era // Modelling and Simulation for Autonomous Systems: 6th International Conference, MESAS, 2019, Palermo, Italy, October 29–31, 2019, Revised Selected Papers / J. Mazal, A. Fagiolini, P. Vasik (eds.). — Springer, 2019. — P. 417–426.
8. Falco G. Cybersecurity Principles for Space Systems // Journal of Aerospace Information Systems. — 2019. — Vol. 16. — Iss. 2. — P. 1–10.
9. Falco G., Henry W., Aliberti M., et al. An International Technical Standard for Commercial Space System Cybersecurity — A Call to Action // ASCEND, 24–26 October 2022, Las Vegas, Nevada & Online. AIAA 2022-4302. Session: Methods and Considerations for Cyber Protection of Space Assets. — ASCEND, 2022. — P. 1–8.
10. Housen-Couriel D. IAC-21-E-9 (Paper ID: 67116) information sharing for the mitigation of outer space — related cybersecurity threats // Acta Astronautica. — 2023. — Vol. 203. — P. 546–550.
11. Kamal A. The Law of Cyber-Space, An Invitation to the Table of Negotiations / United Nations Institute of Training and Research. — Geneva, 2005. — 269 p.
12. Li D. Upgrading space debris mitigation measures to cope with proliferating cyber threats to space activities // Advances in Space Research. — 2023. — Vol. 71. — Iss. 10. — P. 4185–4195.
13. Schmitt M. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. — Cambridge University Press, 2017. — 648 p.
14. Suwijak C. Global Internet Access from the Low Earth Orbit: Legal Issues regarding Cybersecurity in Outer Space // Journal of East Asia and International Law. — 2022. — Vol. 15. — Iss. 1. — P. 93–108.