УДК 34 **DOI: 10.34670/AR.2026.38.71.020**

Правовое регулирование использования цифровых технологий при обеспечении кибербезопасности цепочек поставок

Аликина Светлана Викторовна

Преподаватель кафедры информатики и математики
Волгоградская академия Министерства
внутренних дел Российской Федерации
400075, Российская Федерация, Волгоград, Историческая ул, 130;
e-mail: mail@law-books.ru

Охотников Илья Викторович

Кандидат экономических наук, доцент,
Российский университет транспорта (МИИТ),
127994, Российская Федерация, Москва, ул Образцова, 9/9;
e-mail: roat.miit@mail.ru

Спектор Асия Ахметовна

Доктор юридических наук, доцент,
Профессор кафедры экономической теории и менеджмента
Российский университет транспорта (МИИТ),
127994, Российская Федерация, Москва, ул Образцова, 9/9;
e-mail: analitikarodis@yandex.ru

Аннотация

Внедрение интернета вещей, блокчейна, больших данных, облачных вычислений и искусственного интеллекта в повседневную и профессиональную жизнь общества неизбежно влияет на логистические и управленческие процессы, генерируя новые риски. Объект исследования - общественные отношения, складывающиеся в процессе обеспечения кибербезопасности цепочек поставок посредством применения цифровых технологий. Предмет исследования - нормы международного и национального права, регулирующие использование цифровых технологий для обеспечения кибербезопасности, а также доктринальные подходы и практические модели такого регулирования. Цель исследования - комплексный анализ современного состояния правового регулирования использования цифровых технологий для обеспечения кибербезопасности цепочек поставок, выявлении системных пробелов и коллизий, а также в разработке научно обоснованных предложений по совершенствованию соответствующего правового инструментария. Уточнено содержание ключевых понятий «цифровые технологии», «кибербезопасность цифровой среды» и «кибербезопасность цепочки поставок» в правовом контексте. Реализован критический анализ существующих регуляторных подходов (отраслевого, риск-ориентированного и технологически-нейтрального).

Выявлены ключевые недостатки, такие как фрагментарность законодательства, экстерриториальность правовых актов, отсутствие единых международных стандартов и норм в цифровой сфере, сложность атрибуции киберинцидентов в распределенных сетях. Разработаны предложения, направленные на эффективность законодательства в рамках концепции «безопасности по дизайну», внедрения обязательных стандартов киберустойчивости для критически важных звеньев цепочек поставок, развития международно-правовых механизмов взаимного признания сертификатов соответствия и создание трансграничных платформ обмена информацией об угрозах на базе доверенных технологий.

Для цитирования в научных исследованиях

Аликина С.В., Охотников И.В., Спектор А.А. Правовое регулирование использования цифровых технологий при обеспечении кибербезопасности цепочек поставок // Вопросы российского и международного права. 2026. Том 16. № 1А. С. 142-149. DOI: 10.34670/AR.2026.38.71.020

Ключевые слова

Правовое регулирование, кибербезопасность цепочек поставок, цифровые технологии, трансграничные риски, гармонизация законодательства, киберустойчивость.

Введение

Объективная необходимость адекватного правового регулирования использования цифровых технологий в контексте кибербезопасности цепочек поставок исходит из самой цифровой природы современных экономических и логистических процессов, которые существуют в гибридном физико-цифровом пространстве, характеризующемся высокой степенью взаимозависимости и уязвимости. Правовое регулирование в данной сфере выступает не просто инструментом минимизации IT-рисков, но конкретные нормативно-правовыми нормами для обеспечения предсказуемости, стабильности и устойчивости глобальных товарно-финансовых потоков, поскольку оно устанавливает границы допустимого поведения, распределяет ответственность за киберинциденты, формирует стандарты поведения заинтересованных лиц и создает правовые стимулы для инвестиций в защищенную инфраструктуру. В отсутствие четкого и сбалансированного правового режима возрастают системные риски каскадных сбоев, когда компрометация одного, даже периферийного участника цепочки поставок через уязвимости в цифровых интерфейсах или слабые протоколы обмена данными может привести к масштабным экономическим, экологическим и социальным последствиям, что и актуализирует потребность в разработке механизма правового регулирования, способного интегрировать технические требования кибербезопасности в сферу договорного, корпоративного и административного права.

Материалы и методы

Под цифровыми технологиями мы, как и зарубежные и отечественные исследователи понимаем совокупность аппаратных и программных средств, алгоритмов и протоколов, основанных на двоичном коде и обеспечивающих создание, обработку, хранение, передачу и

использование данных в электронной форме [Уголовный кодекс РФ, 1996], [Козлов, 2002]. К цифровым технологиям, прежде всего, относятся - интернет вещей (IoT), обеспечивающий подключение физических объектов к сети; блокчейн и распределенные реестры, предлагающие децентрализованные модели верификации транзакций; облачные вычисления, предоставляющие масштабируемые вычислительные ресурсы; большие данные и аналитика; искусственный интеллект (ИИ) и машинное обучение; а также роботизированные системы автоматизации процессов (RPA) [Птицына, 2023]. Их интеграция в цепочки поставок приводит к возникновению киберфизических систем, в которых физические процессы неразрывно связаны с цифровым управлением и обратной связью, что неизбежно генерирует новые несистемные риски.

Кибербезопасность в цифровой среде представляет собой состояние защищенности информации, информационных систем и информационно-телекоммуникационных сетей от внутренних и внешних угроз, направленных на нарушение конфиденциальности, целостности и доступности данных, а также устойчивости и нормального функционирования связанных с ними процессов [Питецкий, 2025]. В правовом измерении «устойчивое состояние киберфизических систем» [Подборка судебных решений..., 2024] обеспечивается комплексом нормативных требований, технических стандартов, направленных на предотвращение, обнаружение и нейтрализацию киберугроз. Само понятие «киберугроза» [Кассационное определение ВС РФ № 83-УДП25-4-К1, 2025] эволюционирует от защиты периметра сетей к обеспечению безопасности данных на всем их жизненном цикле и устойчивости систем в условиях продолжающейся атаки. В узкоспециализированном контексте кибербезопасность цепочек поставок определяется как практика управления киберрисками, возникающими во всей экосистеме взаимосвязанных организаций, участвующих в создании и поставке продукции или услуг (от первоначальных поставщиков сырья до конечного потребителя), с учетом их хозяйствования в цифровой среде [Постановление Пленума ВС РФ № 48, 2019]. Системные угрозы включают компрометацию программного обеспечения для управления цепочками поставок (SCM), атаки на системы IoT в логистике (умные контейнеры, датчики), внедрение вредоносного кода через обновления от сторонних поставщиков, кражу критически важных данных (интеллектуальной собственности, коммерческой тайны) и атаки на системы критической информационной инфраструктуры, от которой зависят логистические узлы.

Результаты исследования и обсуждение

Можно выделить несколько основных регуляторных парадигм к правовому регулированию: 1. отраслевой и секторальный подход, при котором требования фокусируются на конкретных отраслях, признанных критически важными (энергетика, финансы, транспорт, здравоохранение). Его примером служит законодательство США в области защиты критической инфраструктуры или европейские директивы NIS и NIS2, обязывающие сетевых операторов принимать технические и организационные меры безопасности и уведомлять о инцидентах; 2. риск-ориентированный подход, закрепленный, в частности, в российском законодательстве (ФЗ-187 «О безопасности критической информационной инфраструктуры»), который предполагает категорирование объектов и применение дифференцированных мер защиты в зависимости от значимости возможного ущерба; 3. технологически-нейтральное регулирование, устанавливающее общие рамки и принципы (как GDPR в части безопасности обработки персональных данных), но оставляющее конкретный выбор технологий на

усмотрение самого оператора; 4. современный подход, который связан с прямым регулированием безопасности цифровых продуктов (кибербезопасность «по дизайну»), что находит отражение в таких инициативах, как Европейский Акт о кибербезопасности (EU Cybersecurity Act), устанавливающий условия для сертификации и проект директивы ЕС об ответственности за программное обеспечение (Cyber Resilience Act). Сведём в таблицу 1 подходы и проведём эвристический анализ их преимуществ и недостатков.

Таблица 1 - Подходы к правовому регулированию использования цифровых технологий при обеспечении кибербезопасности цепочек поставок

Подход	Сущность подхода	Примеры правового закрепления	Ключевые преимущества	Основные недостатки
Секторальный (отраслевой) подход	Регулирование фокусируется на конкретных секторах экономики, признанных критически важными, с установлением специфических требований к их кибербезопасности.	Директива ЕС NIS2 (сети и информационные системы); отраслевые стандарты в США для энергетики, финансов, транспорта; регулирование в сфере телекоммуникаций и финансов в РФ.	Позволяет учесть уникальные риски и операционную специфику конкретной отрасли. Повышает релевантность требований.	Приводит к фрагментации регулирования. Не учитывает взаимозависимость отраслей в единой цепочке поставок. Создает регуляторное неравенство.
Риск-ориентированный подход	Требования к мерам безопасности и их строгость дифференцируются в зависимости от категории объекта (значимости), определяемой через оценку потенциального ущерба от киберинцидента.	Федеральный закон РФ № 187-ФЗ «О безопасности критической информационной инфраструктуры»; элементы в Директиве NIS2; подходы Банка России.	Позволяет оптимизировать ресурсы, направляя их на защиту наиболее значимых активов. Способствует гибкости регулирования.	Сложность и субъективность процедур категорирования и оценки рисков. Проблема каскадных эффектов при недооценке рисков у «менее значимых» звеньев цепочки.
Технологически-нейтральный подход	Регулирование устанавливает общие цели, принципы и обязательные результаты в области безопасности, не предписывая использование конкретных технологий или технических решений.	Общие принципы безопасности обработки данных в GDPR; многие национальные рамочные законы в области информационной безопасности.	Стимулирует инновации и конкуренцию среди поставщиков решений. Обеспечивает долгосрочную актуальность правовых норм.	Требует высокой экспертизы от регулируемых организаций для интерпретации. Может приводить к неоднозначности правоприменения и различию в уровнях реальной безопасности.

Подход	Сущность подхода	Примеры правового закрепления	Ключевые преимущества	Основные недостатки
Подход, основанный на безопасности «по умолчанию и по проекту»	Законодательное закрепление обязанности производителей и разработчиков внедрять необходимые меры кибербезопасности на этапе проектирования и разработки продукта/услуги, а также обеспечивать безопасные настройки по умолчанию.	Европейский акт о киберустойчивости (Cyber Resilience Act, проект); положения GDPR о защите данных по умолчанию и проектированию; концепция в стандартах ISO.	Устраняет уязвимости на самом раннем этапе. Снижает нагрузку на конечных пользователей (в т.ч. участников цепочек). Создает единый базовый уровень безопасности для цифровых продуктов.	Сложность контроля и верификации выполнения требований на этапе разработки. Потенциальное увеличение стоимости и времени вывода продукта на рынок.
Обязательная сертификация и стандартизация	Установление законодательных требований о подтверждении соответствия цифровых продуктов, услуг или процессов определенным стандартам кибербезопасности через процедуры независимой оценки.	Схемы сертификации в рамках Европейского акта о кибербезопасности (EU Cybersecurity Act); обязательные стандарты ФСТЭК и ФСБ России для определенных классов продуктов; отраслевые стандарты платежных карт PCI DSS.	Повышает доверие и обеспечивает проверяемость соответствия. Упрощает выбор безопасных решений для участников цепочек поставок.	Риск бюрократизации и формального подхода. Быстрое устаревание стандартов в условиях динамичного технологического развития. Затратность процедур для малого бизнеса.

Источник: разработано авторами

Правовой анализ действующих правовых режимов позволяет выявить ряд системных недостатков и пробелов: 1. наблюдается фрагментарность и коллизионность регулирования, особенно в трансграничном контексте. Требования разных юрисдикций могут налагать на участника глобальной цепочки поставок противоречащие друг другу обязанности; 2. проблема экстерриториальности законодательства и сложности его правоприменения в отношении иностранных поставщиков цифровых решений и субподрядчиков; 3. отсутствие единых международно-признанных стандартов кибербезопасности в отношении поставщиков, что приводит к правовой неопределённости в части договорного распределения рисков через односторонние оценочные анкеты безопасности; 4. крайняя сложность атрибуции киберинцидентов в распределенных системах создает правовой вакуум в вопросах установления вины и возмещения ущерба; 5. регуляторный фокус зачастую смещен на крупных операторов, в то время как уязвимость зачастую возникает на уровне малых и средних предприятий – субпоставщиков, не обладающих ресурсами для полноценного противодействия киберугрозам; 6. наблюдается правовое отставание от темпа технологических изменений:

регулирование не успевает адаптироваться к рискам, порождаемым ИИ, автономными системами и квантовыми вычислениями.

В качестве предложений по совершенствованию правового регулирования представляется целесообразным развитие следующих направлений. Первое - это продвижение на международном уровне (через UNIDROIT, UNCITRAL или специализированные организации типа ISO) модельных стандартов контрактных кибер-клауз для цепочек поставок, предусматривающих прозрачное распределение обязанностей по безопасности, взаимное принятие сертификатов, порядок уведомления об инцидентах и механизмы разрешения споров. Второе - это гармонизация национальных законодательств в сторону имплементации принципа «безопасности и устойчивости по дизайну», как обязательного требования для цифровых технологий, внедряемых в критически важные процессы цепочек поставок, с сопутствующей разработкой систем обязательной сертификации для ключевых категорий продуктов (SCM-системы, промышленный IoT). Третье - это создание на межгосударственном или отраслевом уровне (например, для транспортных коридоров) защищенных платформ обмена информацией об угрозах и уязвимостях, функционирующих на доверенных технологиях (например, конфиденциальные вычисления) и обеспеченных правовыми гарантиями защиты обменивающейся стороны от антимонопольных и иных исков. И последнее - это введение в законодательство о корпоративном управлении обязанностей советов директоров по надзору за киберрисками в цепочке поставок, что повысит ответственность топ-менеджмента. Пятое – стимулирование через государственные закупки и налоговые механизмы внедрения технологий повышенной доверенности, таких как блокчейн для отслеживания происхождения компонентов и неизменности логистических записей, что одновременно повышает прозрачность и безопасность.

Заключение

Правовое регулирование использования цифровых технологий при обеспечении кибербезопасности цепочек поставок представляет собой динамично развивающуюся, но пока недостаточно правовую область релевантную окружающей действительности. Эффективный правовой режим в данной сфере должен преодолевать традиционную национальную фрагментацию и эволюционировать в сторону комплексного, риск-ориентированного, но технологически осознанного подхода, который бы органично сочетал императивные требования безопасности для критически важных элементов цепочек с гибкими стимулами для повсеместного внедрения лучших практик. Ключевыми векторами развития правового регулирования цепочек поставок в цифровой среде видятся международная гармонизация национальных стандартов, легальное закрепление принципа «безопасности по дизайну» для цифровых продуктов, используемых в логистике и создание трансграничных доверенных платформ для совместного использования цифровых технологий.

Библиография

1. Timotheou S. et al. Impacts of digital technologies on education and factors influencing schools' digital capacity and transformation: A literature review //Education and information technologies. – 2023. – Т. 28. – №. 6. – С. 6695-6726.- DOI 10.1007/s10639-022-11431-8
2. Караваева Ю. И. Современные цифровые технологии и проблема обеспечения прав человека //Вестник Университета имени ОЕ Кутафина. – 2025. – №. 9 (133). – С. 170-176.- URL: https://cyberleninka.ru/article/n/sovremennye-tsifrovye-tehnologii-i-problema-obespecheniya-prav-cheloveka
3. Elia G., Margherita A., Passiante G. Digital entrepreneurship ecosystem: How digital technologies and collective intelligence are reshaping the entrepreneurial process //Technological forecasting and social change. – 2020. – Т. 150.

– С. 119791.- DOI 10.1016/j.techfore.2019.119791
4. Лазарь, К. К. Кибербезопасность и суверенитет в киберпространстве: вызовы и перспективы международного права / К. К. Лазарь // Московский журнал международного права. – 2025. – № 1. – С. 125-137. – DOI 10.24833/0869-0049-2025-1-125-137. – EDN HLNRTE.
5. Ma S. et al. Cloud-integrated cyber-physical systems: Reliability, performance and power consumption with shared-servers and parallelized services //Frontiers of Engineering Management. – 2025. – Т. 12. – №. 2. – С. 272-290.- DOI 10.1007/s42524-023-0272-2
6. Язов Ю. К. Об определении понятия «кибербезопасность» и связанных с ним терминов //Вопросы кибербезопасности. – 2025. – №. 1 (65). – С. 2-6.- URL: https://cyberleninka.ru/article/n/ob-opredelenii-ponyatiya-kiberbezopasnost-i-svyazannyh-s-nim-terminov
7. Ромашкина, Н. П. Стратегические риски и проблемы кибербезопасности / Н. П. Ромашкина, Д. В. Стефанович // Вопросы кибербезопасности. – 2020. – № 5(39). – С. 77-86. – DOI 10.21681/2311-3456-2020-05-77-86. – EDN TYCIVU.

Legal Regulation of the Use of Digital Technologies in Ensuring Cybersecurity of Supply Chains

Svetlana V. Alikina

Lecturer, Department of Informatics and Mathematics,
Volgograd Academy of the Ministry
of Internal Affairs of the Russian Federation,
400075, 130, Istoricheskaya str., Volgograd, Russian Federation;
e-mail: mail@law-books.ru

Il'ya V. Okhotnikov

PhD in Economics, Associate Professor,
Russian University of Transport (MIIT),
127994, 9/9, Obraztsova str., Moscow, Russian Federation;
e-mail: roat.miit@mail.ru

Asiya A. Spector

Doctor of Law, Associate Professor,
Professor of the Department of Economic Theory and Management,
Russian University of Transport (MIIT),
127994, 9/9, Obraztsova str., Moscow, Russian Federation;
e-mail: analitikarodis@yandex.ru

Abstract

The introduction of the Internet of Things, blockchain, big data, cloud computing, and artificial intelligence into the daily and professional life of society inevitably affects logistical and managerial processes, generating new risks. The object of the study is the social relations that develop in the process of ensuring cybersecurity of supply chains through the application of digital technologies. The subject of the study is the norms of international and national law regulating the use of digital technologies to ensure cybersecurity, as well as doctrinal approaches and practical models of such

regulation. The purpose of the study is a comprehensive analysis of the current state of legal regulation of the use of digital technologies to ensure cybersecurity of supply chains, identifying systemic gaps and conflicts, as well as developing scientifically based proposals for improving the relevant legal toolkit. The content of the key concepts "digital technologies," "cybersecurity of the digital environment," and "supply chain cybersecurity" in the legal context is clarified. A critical analysis of existing regulatory approaches (sectoral, risk-oriented, and technologically neutral) is carried out. Key shortcomings are identified, such as the fragmentation of legislation, the extraterritoriality of legal acts, the lack of uniform international standards and norms in the digital sphere, and the difficulty of attributing cyber incidents in distributed networks. Proposals are developed aimed at the effectiveness of legislation within the framework of the "security by design" concept, the introduction of mandatory cyber resilience standards for critical links in supply chains, the development of international legal mechanisms for the mutual recognition of conformity certificates, and the creation of cross-border platforms for exchanging threat information based on trusted technologies.

For citation

Alikina S.V., Okhotnikov I.V., Spector A.A. (2026) Pravovoye regulirovaniye ispol'zovaniya tsifrovykh tekhnologiy pri obespechenii kiberbezopasnosti tsepochek postavok [Legal Regulation of the Use of Digital Technologies in Ensuring Cybersecurity of Supply Chains]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 16 (1A), pp. 142-149. DOI: 10.34670/AR.2026.38.71.020

Keywords

Legal regulation, supply chain cybersecurity, digital technologies, cross-border risks, harmonization of legislation, cyber resilience.

References

1. Timotheou S. et al. Impacts of digital technologies on education and factors influencing schools' digital capacity and transformation: A literature review // Education and information technologies. - 2023. - Vol. 28. - No. 6. - Pp. 6695-6726.- DOI 10.1007/s10639-022-11431-8
2. Karavaeva Yu. I. Modern digital technologies and the problem of ensuring human rights // Bulletin of the OE Kutafin University. - 2025. - No. 9 (133). – P. 170-176.- URL: https://cyberleninka.ru/article/n/sovremennye-tsifrovye-tehnologii-i-problema-obespecheniya-prav-cheloveka
3. Elia G., Margherita A., Passiante G. Digital entrepreneurship ecosystem: How digital technologies and collective intelligence are reshaping the entrepreneurial process // Technological forecasting and social change. – 2020. – Vol. 150. – P. 119791.- DOI 10.1016/j.techfore.2019.119791
4. Lazar, K. K. Cybersecurity and sovereignty in cyberspace: challenges and prospects of international law / K. K. Lazar // Moscow Journal of International Law. – 2025. – No. 1. – P. 125-137. – DOI 10.24833/0869-0049-2025-1-125-137. – EDN HLNRTE.
5. Ma S. et al. Cloud-integrated cyber-physical systems: Reliability, performance and power consumption with shared-servers and parallelized services //Frontiers of Engineering Management. – 2025. – Vol. 12. – No. 2. – Pp. 272-290.- DOI 10.1007/s42524-023-0272-2
6. Yazov Yu. K. On the definition of the concept of "cybersecurity" and related terms // Cybersecurity Issues. – 2025. – No. 1 (65). – P. 2-6.- URL: https://cyberleninka.ru/article/n/ob-opredelenii-ponyatiya-kiberbezopasnost-i-svyazannyh-s-nim-terminov
7. Romashkina, N. P. Strategic risks and problems of cybersecurity / N. P. Romashkina, D. V. Stefanovich // Issues of cybersecurity. – 2020. – No. 5(39). – P. 77-86. – DOI 10.21681/2311-3456-2020-05-77-86. – EDN TYCIVU.