ОСОБЕННОСТИ ПРАВОВОГО РЕГУЛИРОВАНИЯ КИБЕРБЕЗОПАСНОСТИ В ЭПОХУ ГЛОБАЛЬНОГО ПРОТИВОСТОЯНИЯ

Баландин А.Ю.[1]

Ключевые слова: *киберугрозы, информационная безопасность, киберпространство, национальная безопасность, критическая информационная инфраструктура, цифровые технологии, юридические акты, хакерские группы, ИКТ-среда.*

Аннотация

В статье рассматривается место правового обеспечения кибербезопасности в системе национальной безопасности Российской Федерации. При исследовании автором предложен системный подход, основанный на формулировании четких юридических определений, направленный на разработку международных и национальных юридических норм, а также интеграцию правовых, технических и организационных мер в целях формирования единого комплексного подхода. В статье уделено внимание необходимости соблюдения баланса между обеспечением безопасности и защитой прав человека в ИКТ-среде, формированию отвечающих общественному запросу правовых механизмов. Содержащиеся в статье предложения могут быть использованы для повышения эффективности правового регулирования, способного адаптироваться к вызовам цифровой эпохи, и необходимого для развития международного сотрудничества в области обеспечения информационной, в том числе кибербезопасности.

Цель работы: обосновать ключевые проблемы правового обеспечения информационной безопасности включая вопросы кибербезопасности.

Методы: системный анализ и сравнительное моделирование, позволяющее обеспечить точность юридических критериев, применяемых в моделях правового регулирования информационных правоотношений. Их применение обосновано необходимостью концептуальной оценки эффективности существующего правового регулирования в национальной и международной правовых системах.

Результаты: выявлены ключевые правовые и организационные проблемы обеспечения безопасности информационной инфраструктуры в условиях глобальных вызовов и угроз. Проанализированы принципы реализации основных типов угроз в киберсреде, включая трансграничные атаки и информационно-психологическое воздействие, что позволило определить их стратегическое значение для национальной безопасности. Обоснована необходимость развития инструментов правового регулирования сферы обеспечения кибербезопасности на национальном и наднациональном уровнях, включая унификацию подхода к регулированию трансграничных аспектов. На основе системного анализа и сравнительного моделирования выработаны предложения, связанные с формированием правовой базы, включая вопросы унификации юридических терминов и правовых категорий, взаимную интеграцию правовых, технических и организационных мер.

Кроме того, обосновано, что правовое обеспечение кибербезопасности является в условиях реализации национального проекта экономики данных и цифровой трансформации государства в Российской Федерации одним из приоритетных направлений реализации государственной политики и разработки международных юридически закрепленных стандартов. Указанные выводы свидетельствуют о том, что системный подход к правовому регулированию необходим для повышения устойчивости критической информационной инфраструктуры и укрепления международного сотрудничества в данной области. Практическая значимость работы заключается в формировании предложений для разработки адаптивных правовых механизмов, способных минимизировать риски в условиях появления новых киберугроз.

DOI: 10.24412/1994-1404-2025-1-50-56

[1] ***Баландин Артур Юрьевич,*** *аспирант кафедры информационного права и цифровых технологий Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), г. Москва, Российская Федерация.*

E-mail: 365inttech@gmail.com

Введение и постановка задачи

Высокая интенсивность развития цифровых технологий в сочетании с нарастающими геополитическими угрозами придают особую значимость вопросу обеспечения безопасности национальной информационной инфраструктуры. На государственном уровне поставлены стратегические задачи на достижение доминирования в таких высокотехнологичных областях, как искусственный интеллект и квантовые вычисления, потенциал которых способен радикально трансформировать киберпространство [1]. Повсеместное применение инновационных технологий ознаменовало зарождение так называемой цифровой цивилизации [2], а противостояние в ИКТ-среде становится одним из ключевых элементов современной геополитики, оказывающих существенное влияние как на развитие международных отношений, так и на проведение внутренней политики государств. При таких обстоятельствах представляется необходимым определить область правового регулирования вопросов безопасности информационной инфраструктуры, сформировать критерии для разработки и совершенствования соответствующих правовых механизмов, отвечающих вызовам сегодняшнего дня и тенденциям общественного развития.

Информационная безопасность и кибербезопасность: соотношение правовых категорий и норм правового регулирования

Использование информационных технологий в качестве инструмента распространения деструктивной информации [3, с. 286], оказывающей негативное информационно-психологическое воздействие на человеческое сознание, приводит к компрометации информационных систем и отдельных объектов информатизации, причинению ущерба объектам критической информационной инфраструктуры, репутационного ущерба органам публичной власти, имущественного вреда физическим и юридическим лицам. По мнению экспертов, отдельной категорией подобного рода субъектов являются привлеченные специализированными структурами недружественных государств проправительственные хакерские группы, специализирующиеся на совершении таргетированных продолжительных кибератак, характеризующихся высокой степенью технологичности и скрытности протекающих процессов [4].

Повсеместность применения инновационных сервисов и средств информационного обмена ставит в качестве приоритетной задачу обеспечения персональных данных и иной информации конфиденциального характера, обрабатываемой в информационных системах. Учитывая, что кибератаки могут быть компонентом гибридных войн, направленных на подрыв доверия к государственным институтам и дестабилизацию функционирования системы органов публичной власти, кибербезопасность является важным направлением обеспечения информационной безопасности, в соответствии со Стратегией национальной безопасности, утвержденной Указом Президента Российской Федерации от 29.10.2024 № 920 в качестве стратегического национального приоритета государственной политики.

Несмотря на актуальность рассматриваемого вопроса, сегодня отмечается острый дефицит эффективных правовых норм, регулирующих деятельность субъектов информационных правовых отношений на государственном и международном уровнях, включая закрепленные на законодательном уровне и обязательные к исполнению меры обеспечения кибербезопасности. Возрастающая агрессивность интернет-пространства, недооценка значения необходимости реализации эффективных мер обеспечения индивидуальной и коллективной безопасности, а также отсутствие консолидированного правового противодействия делают как государственные структуры, так и бизнес, а также отдельных граждан максимально уязвимыми перед организованным целенаправленным вмешательством.

В связи с этим очевидна необходимость формирования информационно- правового пространства, реализующего применение информационных технологий на основании объективно сформулированных правовых норм, защищающих права граждан и общественные интересы, отвечающие требованиям обеспечения государственной безопасности в цифровой среде. Важен комплексный подход к решению поставленных проблем, связанных с формированием правовых инструментов обеспечения кибербезопасности как на международном, так и на национальном уровне, что требует интеграции правовых, технических, технологических и организационных мер для создания эффективных механизмов защиты информационных систем и данных.

Ключевым вопросом достижения консенсуса представляется разработка и унификация применяемых в национальных правовых системах юридических терминов. Киберугрозы все чаще носят трансграничный характер, что требует от субъектов международных правовых отношений в области применения информационных технологий конструктивного сотрудничества. Унификация межотраслевого понятийно-категориального аппарата видится отправной точкой для последующего успешного сотрудничества в сфере обеспечения кибербезопасности информационных систем на международном уровне и формирования перспективы применения международных правовых стандартов в данной области в целях обеспечения государственного суверенитета.

Достаточно острую дискуссию вызывает применение самого термина «кибербезопасность», до настоящего времени не нашедшего закрепления в российской правовой системе. Вместе с тем исследование позволяет выделить несколько подходов к формулированию данной юридической дефиниции.

Так, кибербезопасность рассматривается в контексте обеспечения защищенности от деструктивной

информации, распространяемой при помощи информационных технологий. При этом объектом деструктивного воздействия является человек, в сознании которого под влиянием транслируемой информации возникают когнитивные процессы, а результатом непосредственного воздействия — когнитивные процессы, порождаемые в человеческом сознании в результате восприятия вредоносного контента [5, с. 157].

В качестве альтернативы предлагается рассматривать ограничение сферы обеспечения кибербезопасности ИКТ-средой, при этом объектом деструктивного воздействия остается исключительно компьютерная инфраструктура, а недопустимые события в виде материального вреда либо репутационного ущерба, возникающие в реальном мире в результате подобного воздействия, выходят за рамки предметной области вопросов правового обеспечения кибербезопасности и подлежат рассмотрению в парадигме иных отраслей права [6]. Данный подход, на наш взгляд, достаточно радикален по отношению к первому и характеризуется строго определенными предметной областью, объектом правового регулирования и специфическими субъектами правовых отношений. При этом пресечение попыток распространения деструктивной информации в ИКТ-среде предлагается рассматривать в рамках необходимости обеспечения информационно-психологической безопасности с учетом специфики применяемых инструментов.

Вместе с тем, несомненно, кибербезопасность сегодня должна найти свое место в структуре российского информационного и, соответственно, публично-правового (государственного) регулирования, поскольку в приведенных позициях данное направление рассматривается как специализированный сегмент информационной безопасности в системе информационного права Российской Федерации.

Представляется, что юридическое закрепление данной категории будет способствовать достижению урегулирования спорных ситуаций, структурированию и совершенствованию действующих правовых норм и институционализации этих вопросов в системе информационного права и правового обеспечения информационной безопасности. Отсутствие общепринятых и юридически закрепленных на национальном и международном уровнях терминов в области обеспечения кибербезопасности является сегодня одной из ключевых проблем не только информационного права, но и смежных отраслей, а разработка новых юридических дефиниций необходима для развития доктрины информационного права.

Для обеспечения принципа преемственности вопрос унификации понятийно-категориального аппарата целесообразно рассматривать в общей концепции кодификации информационного законодательства, а необходимость разработки отдельного раздела, посвящённого вопросам кибербезопасности, объясняется особой значимостью данного направления как приоритетного направления государственной безопасности. Отсутствие единства юридических терминов и в связи с этим вынужденно субъективное толкование новых правовых категорий, а также потенциально возможные пробелы в соотношении новых юридических норм с уже существующими могут создать предпосылки для снижения уровня правовой определенности в развитии общественных отношений, что для сферы обеспечения национальной безопасности является недопустимым [7, с. 42].

Процесс кодификации нормативных правовых актов в определенной степени основывается как на переоценке существующих юридических норм, так и на формировании новых правовых конструкций, их объединении в единый структурированный документ. Особое значение процесс кодификации приобретает для развития информационного права, поскольку позволяет систематизировать и интегрировать в существующую нормативную базу российского законодательства нормативные правовые акты в области обеспечения кибербезопасности, имеющие комплексный характер и воплощающие межотраслевой подход, подлежащий применению при их формировании.

Упорядоченность правовых норм позволит сформировать единую систему, объективно оптимизирующую законотворческие и правоприменительные процессы, информационно-правовую деятельность. Таким образом, в рамках научной дискуссии о развитии национальной правовой системы внедрение кодификации видится не просто желательным, но и вполне закономерным шагом, отвечающим общественному вызову и продиктованным стремлением к повышению эффективности правового регулирования в области развития информационных технологий и обеспечения кибербезопасности национальной информационной инфраструктуры.

Не менее важной задачей правового обеспечения кибербезопасности является решение проблем юридической атрибуции. Установление субъектов, совершивших правонарушение или готовящихся к его совершению, включая подтверждение их принадлежности национальным юрисдикциям, представляется одним из наиболее эффективных правовых механизмов предотвращения и пресечения деструктивной хакерской деятельности. В контексте возможности эксплуатации уязвимостей как элементов тактик, применяемых при совершении кибератак, вместе с вопросами субъектной идентификации непосредственных исполнителей несанкционированного вмешательства в защищаемую инфраструктуру отмечается целесообразность репутационной оценки производителей программного обеспечения и программно-аппаратных платформ, ранее уличенных в производстве технических решений с большим количеством уязвимостей, содержащих скомпрометированные элементы, и не принимающих должных мер по их устранению.

Вопрос необходимости преодоления различий и восполнения правовых лакун в национальных правовых актах заслуживает особого внимания. Подходы

к регулированию рассматриваемых правовых отношений могут иметь существенные различия в зависимости от национальных приоритетов, что усложняет процесс достижения унифицированной международной правовой структуры. Следует согласиться, что при таких обстоятельствах, с учетом специфики и трансграничного характера киберпространства унификация правовых норм должна основываться на общности интересов субъектов международных правовых отношений, исключая приоритет интересов и технологическую гегемонию отдельных государств [8]. Ещё одной критически важной задачей является нахождение баланса между обеспечением безопасности и защитой прав человека. Правовое регулирование должно учитывать фундаментальные права и свободы, такие как право на неприкосновенность личной жизни и свободу слова, и при разрешении противоречий подход к применяемым ограничениям должен быть сбалансированным, а пределы вмешательства государства в частную жизнь — обоснованными. Это свидетельствует о сложности правового регулирования кибербезопасности и необходимости применения комплексного подхода к решению возникающих проблем.

В условиях современности стремительное развитие цифровых технологий требует от правового регулирования гибкости и адаптивности. Правовое регулирование закономерно не успевает за технологическими инновациями (наукоемкими технологиями) и новыми формами киберугроз, что ведет к возникновению правовых лакун. В современном мире компьютерные технологии все чаще используются как инструмент геополитического влияния и даже агрессивных действий между государствами. В связи с этим следует признать справедливость позиции относительно того, что «правовые рамки, регулирующие вопросы кибероружия и стратегий предотвращения кибервойны, остаются недоработанными и требуют дальнейшего совершенствования» [9]. Это подчеркивает необходимость динамичного правового подхода, способного оперативно реагировать на изменяющуюся цифровую среду и обеспечивать надлежащую защиту от возникающих киберугроз и совершенствующихся тактик их реализации. Такие особенности подчеркивают необходимость комплексного и согласованного подхода к правовому регулированию кибербезопасности, а также постоянного диалога между государствами, технологическими компаниями и гражданским обществом.

Основные приоритеты и направления государственной политики в области информационной безопасности определены в Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 02.07.2021 № 400, и Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 05.12.2016 № 646, в которых к числу основных угроз информационной безопасности в системе обеспечения национальной безопасности Российской Федерации относятся распространение ложной информации и деструктивное информационно-техническое воздействие, нарушения защищенности информационно-коммуникационной инфраструктуры и утечки конфиденциальной информации и персональных данных. В связи с этим нормативные правовые акты, вопросы защищенности информации направлены в том числе и на защиту данных в цифровом виде. Стратегия развития информационного общества в Российской Федерации на 2017—2030 годы, утвержденная Указом Президента Российской Федерации от 09.05.2017 № 203, определяет информационную безопасность как одно из стратегических направлений для обеспечения национальной безопасности. В связи с этим правовые аспекты информационной безопасности являются приоритетными, поскольку правовые механизмы способны формировать устойчивую правовую основу для защиты от киберугроз и предотвращения их влияния на экономическую и политическую стабильность.

Как отмечают исследователи, в настоящее время правовое обеспечение цифровизации общества осуществляется через развитие базовых информационно-правовых норм, регулирующих ключевые аспекты цифровых отношений. Эти нормы включают принципы регулирования цифровых взаимодействий, режим управления цифровыми данными и другими объектами цифровой среды, определение правового статуса субъектов, функционирующих в цифровой среде, а также другие правовые элементы, отражающие сущность цифровой формы; нормы обладают универсальным характером и могут быть интегрированы в систему права в целом. Кроме того, правовое обеспечение цифровизации связано с появлением отраслевых цифровых норм. Указанные нормы разрабатываются и принимаются в различных отраслях права и отражают специфику реализации цифровых процессов в разных сферах общественных отношений, регулируемых соответствующими отраслями права, что позволяет учитывать уникальные особенности каждой сферы и эффективнее адаптировать правовое регулирование к потребностям цифровой эпохи [10].

В качестве предмета правового обеспечения информационной безопасности научную обоснованность получило представление о нем как об области правового воздействия на поведение людей в целях недопущения проявления угроз объектам национальных интересов в информационной сфере или минимизация негативных последствий проявления этих угроз [11]. Иная формулировка раскрывает данную дефиницию через влияние информации и информационной инфраструктуры на обеспечение национальных интересов [12].

В российской юридической науке предмет правового обеспечения информационной безопасности определен как *область правового воздействия на поведение людей в целях недопущения проявления угроз объектам национальных интересов в информационной сфере или минимизации негативных последствий проявления этих угроз* [11].

Требование защиты информационных и коммуникационных технологий приводит к необходимости

формирования специализированного понятия. Принимая во внимание специфику развития общественных отношений, темпы развития информационных технологий, а также общественный запрос на трансформацию информационных правовых отношений, представляется обоснованным определить предметную область правового регулирования кибербезопасности как **область нормативного правового воздействия, направленного на исключение вредоносного воздействия на информационно-технические ресурсы, реализуемого при помощи программно-аппаратных средств в информационно-коммуникационных системах либо посредством таковых, и/или ликвидации последствий проявления этих угроз.**

Вывод

На современном этапе информационное законодательство, находясь под влиянием цифровой трансформации, выступает в качестве формирующей правовой системы и комплексной правовой отрасли, требующей современных теоретических подходов к урегулированию законодательства в России на основе научного анализа [13—16]. Создание и закрепление новых терминов в юридическом дискурсе позволит не только повысить точность правового регулирования, но и обеспечить соответствие норм права требованиям современного информационного общества. В этой связи для достижения высокоэффективного правового обеспечения безопасности национальной информационной инфраструктуры Российской Федерации необходимо определение кибербезопасности как одного из приоритетных векторов информационной безопасности сегодня в системе информационного права с четко определенной предметной областью, объектом правового регулирования и характеристиками субъектного состава.

Литература

1. Полякова Т.А., Минбалеев А.В., Кроткова Н.В. Развитие доктрины российского информационного права в условиях перехода к экономике данных // Государство и право. 2023. № 9. С. 158—171.
2. Троян Н.А. Современные подходы к эффективному правовому регулированию в целях обеспечения цифрового суверенитета России // Мониторинг правоприменения. 2024. № 1. С. 63—72.
3. Смирнов А.А. Формирование системы правового обеспечения информационно психологической безопасности в Российской Федерации : дисс. … д-ра юрид. наук. М., 2022. С. 286.
4. Шариков П.А. Военные аспекты кибербезопасности в контексте специальной военной операции ФПР на территории Украины // Аналитические записки Института Европы РАН. 2022. № 2. С. 5—12.
5. Саликов М.С., Несмеянова С.Э., Колобаева Н.Е., Кузнецова С.С., Мочалов А.Н. Государственное регулирование Интернета и права человека / Под ред. д-ра юрид. наук, профессора М.С. Саликова. Екатеринбург : изд-во УМЦ УПИ, 2022. 220 с.
6. Козлова Н.Ш., Довгаль В.А. Кибербезопасность и информационная безопасность: сходства и отличия // Вестник Адыгейского государственного университета. Серия: Естественно-математические и технические науки. 2021. № 3 (286). С. 88—97.
7. Полякова Т.А. Развитие понятийного аппарата в области обеспечения информационной безопасности в Российской Федерации // Понятийный аппарат в информационном праве: сборник научных работ / ИГП РАН, отв. ред. И.Л. Бачило, Т.А. Полякова, В.Б. Наумов. М. : Канон-Плюс, 2017. 264 с.
8. Дегтерев Д.А., Рамич М.С., Пискунов Д.А. Подходы США и КНР к глобальному управлению киберпространством: «новая биполярность» в «сетевом обществе» // Вестник международных организаций: образование, наука, новая экономика. 2021. Т. 16. № 3. С. 7—33.
9. Макаров В.А., Коротков В.Г. Подходы к обеспечению безопасности энергетических систем в условиях возможного применения кибероружия // Вестник НИЦ ВА РВСН. 2020. № 1. С. 47—55.
10. Полякова Т.А., Минбалеев А.В., Кроткова Н.В. Трансформация науки информационного права и информационного законодательства: новый этап в условиях научно-технологического развития России // Государство и право. 2024. № 9. С. 166—179.
11. Полякова Т.А. Правовое обеспечение информационной безопасности при построении информационного общества в России: дисс. … д-ра юрид. наук. М., 2008. С. 111.
12. Стрельцов А.А. Предмет правового обеспечения информационной безопасности // Российский юридический журнал. 2003. № 2 (38). С. 24—35.
13. Полякова Т.А., Минбалеев А.В., Наумов В.Б. К вопросу о кодификации информационного законодательства в условиях цифровой трансформации // Государство и право. 2024. № 1. С. 81—91.
14. Карцхия А.А., Макаренко Г.И. Правовые аспекты современной кибербезопасности и противодействия киберпреступности // Вопросы кибербезопасности. 2023. № 1 (53). С. 58—74. DOI: 10.21681/2311-3456-2023-1-58-74 .
15. Карцхия А.А., Макаренко Г.И., Сергин М.Ю. Современные тренды киберугроз и трансформация понятия кибербезопасности в условиях цифровизации системы права // Вопросы кибербезопасности. 2019. № 3 (31). С. 18—23. DOI: 10.21681/2311-3456-2019-3-18-23 .

16. Карцхия А.А., Макаренко Г.И. Правовые проблемы искусственного интеллекта в России // Правовая информатика. 2024. № 1. С. 4—19. DOI: 10.21681/1994-1404-2024-1-4-19 .

SECTION:
CONSTITUTIONAL LAW

SPECIFIC FEATURES OF LEGAL REGULATION OF CYBERSECURITY IN THE TIMES OF GLOBAL CONFRONTATION

Artur Balandin, *Ph.D. student at the Department of Information Technology Law and Digital Technologies of the Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation.*
E-mail: 365inttech@gmail.com

Keywords: *cyber threats, information security, cyberspace, national security, critical information infrastructure, digital technologies, legal acts, hacker groups, ICT environment.*

Abstract

The paper examines the place of legal provision of cybersecurity in the national security system of the Russian Federation. In the study, the author proposed a systematic approach based on the formulation of clear legal definitions aimed at the development of international and national legal norms, as well as the integration of legal, technical and organizational measures in order to form a single integrated approach. The article focuses on the need to maintain a balance between ensuring security and protecting human rights in the ICT environment, and the formation of legal mechanisms that meet public demand. The proposals contained in the article can be used to improve the effectiveness of legal regulation that can adapt to the challenges of the digital age and is necessary for the development of international cooperation in the field of information security, including cybersecurity.

Purpose of the study: identifying key problems of legal provision of information security, including cybersecurity issues.

Methods used in the study: system analysis and comparative modeling, which allows to ensure the accuracy of legal criteria used in models of legal regulation of information legal relations. Their application is justified by the need for a conceptual assessment of the effectiveness of existing legal regulation in national and international legal systems.

Study findings: within the framework of the conducted research, the key legal and organizational problems of ensuring the security of information infrastructure in the context of global challenges and threats have been identified. The principles of the implementation of the main types of threats in the cyber environment, including cross-border attacks and information and psychological impact, have been analyzed, which made it possible to determine their strategic importance for national security. As a result of the study, the need for the development of legal regulation tools for cybersecurity at the national and supranational levels, including the unification of the approach to regulating cross-border aspects, is substantiated. Based on system analysis and comparative modeling, proposals related to the formation of a legal framework have been developed, including issues of unification of legal terms and legal categories, mutual integration of legal, technical and organizational measures.

In addition, the study substantiates that the legal provision of cybersecurity is one of the priorities for the implementation of state policy and the development of international legally established standards in the context of the implementation of the national project of data economy and digital transformation of the state in the Russian Federation. These conclusions indicate that a systematic approach to legal regulation is necessary to increase the stability of critical information infrastructure and strengthen international cooperation in this area. The practical significance of the work lies in the formation of proposals for the development of adaptive legal mechanisms that can minimize risks in the face of new cyber threats.

References

1. Poliakova T.A., Minbaleev A.V., Krotkova N.V. Razvitie doktriny rossiiskogo informatsionnogo prava v usloviiakh perekhoda k ekonomike dannykh. Gosudarstvo i pravo. 2023. No. 9. Pp. 158–171.
2. Troian N.A. Sovremennye podkhody k effektivnomu pravovomu regulirovaniiu v tseliakh obespecheniia tsifrovogo suvereniteta Rossii. Monitoring pravoprimeneniia. 2024. No. 1. Pp. 63–72.
3. Smirnov A.A. Formirovanie sistemy pravovogo obespecheniia informatsionno psikhologicheskoi bezopasnosti v Rossiiskoi Federatsii : diss. ... d-ra iurid. nauk. M., 2022. P. 286.

4. Sharikov P.A. Voennye aspekty kiberbezopasnosti v kontekste spetsial'noi voennoi operatsii FPR na territorii Ukrainy. Analiticheskie zapiski Instituta Evropy RAN. 2022. No. 2. Pp. 5–12.
5. Salikov M.S., Nesmeianova S.E., Kolobaeva N.E., Kuznetsova S.S., Mochalov A.N. Gosudarstvennoe regulirovanie Interneta i prava cheloveka. Pod red. d-ra iurid. nauk, professora M.S. Salikova. Ekaterinburg : izd-vo UMTs UPI, 2022. 220 pp.
6. Kozlova N.Sh., Dovgal' V.A. Kiberbezopasnost' i informatsionnaia bezopasnost': skhodstva i otlichiia. Vestnik Adygeiskogo gosudarstvennogo universiteta. Seriia: Estestvenno-matematicheskie i tekhnicheskie nauki. 2021. No. 3 (286). Pp. 88–97.
7. Poliakova T.A. Razvitie poniatiinogo apparata v oblasti obespecheniia informatsionnoi bezopasnosti v Rossiiskoi Federatsii. Poniatiinyi apparat v informatsionnom prave: sbornik nauchnykh rabot. IGP RAN, otv. red. I.L. Bachilo, T.A. Poliakova, V.B. Naumov. M. : Kanon-Plius, 2017. 264 pp.
8. Degterev D.A., Ramich M.S., Piskunov D.A. Podkhody SShA i KNR k global'nomu upravleniiu kiberprostranstvom: "novaia bipoliarnost'" v "setevom obshchestve". Vestnik mezhdunarodnykh organizatsii: obrazovanie, nauka, novaia ekonomika. 2021. T. 16. No. 3. Pp. 7–33.
9. Makarov V.A., Korotkov V.G. Podkhody k obespecheniiu bezopasnosti energeticheskikh sistem v usloviiakh vozmozhnogo primeneniia kiberoruzhiia. Vestnik NITs VA RVSN. 2020. No. 1. Pp. 47–55.
10. Poliakova T.A., Minbaleev A.V., Krotkova N.V. Transformatsiia nauki informatsionnogo prava i informatsionnogo zakonodatel'stva: novyi etap v usloviiakh nauchno-tekhnologicheskogo razvitiia Rossii. Gosudarstvo i pravo. 2024. No. 9. Pp. 166–179.
11. Poliakova T.A. Pravovoe obespechenie informatsionnoi bezopasnosti pri postroenii informatsionnogo obshchestva v Rossii: diss. ... d-ra iurid. nauk. M., 2008. P. 111.
12. Strel'tsov A.A. Predmet pravovogo obespecheniia informatsionnoi bezopasnosti. Rossiiskii iuridicheskii zhurnal. 2003. No. 2 (38). Pp. 24–35.
13. Poliakova T.A., Minbaleev A.V., Naumov V.B. K voprosu o kodifikatsii informatsionnogo zakonodatel'stva v usloviiakh tsifrovoi transformatsii. Gosudarstvo i pravo. 2024. No. 1. Pp. 81–91.
14. Kartskhiia A.A., Makarenko G.I. Pravovye aspekty sovremennoi kiberbezopasnosti i protivodeistviia kiberprestupnosti. Voprosy kiberbezopasnosti. 2023. No. 1 (53). Pp. 58–74. DOI: 10.21681/2311-3456-2023-1-58-74 .
15. Kartskhiia A.A., Makarenko G.I., Sergin M.Iu. Sovremennye trendy kiberugroz i transformatsiia poniatiia kiberbezopasnosti v usloviiakh tsifrovizatsii sistemy prava. Voprosy kiberbezopasnosti. 2019. No. 3 (31). Pp. 18–23. DOI: 10.21681/2311-3456-2019-3-18-23 .
16. Kartskhiia A.A., Makarenko G.I. Pravovye problemy iskusstvennogo intellekta v Rossii. Pravovaia informatika. 2024. No. 1. Pp. 4–19. DOI: 10.21681/1994-1404-2024-1-4-19 .