Дата поступления рукописи в редакцию: 14.11.2025 г.
Дата принятия рукописи в печать: 14.12.2025 г.
DOI: 10.24412/2076-1503-2025-11-641-648

ПЕКАРЕВА Виктория Владимировна,
Магистрант юридического факультета
Российский государственный педагогический университет им. А. И. Герцена,
г. Санкт-Петербург,
e-mail: viktoria.pekareva@yandex.ru

ПРАВОВЫЕ МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ»

Аннотация. *В условиях необходимости достижения идеальной модели состояния «посередине» в теоретическом, и практическом представлении между требованиями по локализации данных и контролируемом обеспечением возможности их трансграничной передачи в рамках свободного пользования гражданами сети «Интернет», а также при существовании не менее важных обстоятельств — динамичного прогресса преступлений в сфере компьютерной информации, исследование динамичной области — правового регулирования Интернета с его уникальными свойствами является одним из приоритетных научных знаний. Кроме обозначения специфики и проблем существующего нормативно-правового упорядочения общественных взаимодействий в сети «Интернет», одной из которых, например, является своевременная адаптивность норм права под текущие общественные отношения и существующие использующиеся невсегда в законных целях в них возможности цифровой сети, технические средства и решения, производится сравнительный анализ правового регулирования информационной безопасности информационно-телекоммуникационной сети «Интернет» некоторых из зарубежных стран.*

Ключевые слова: *информационная безопасность, национальная безопасность, информационно-телекоммуникационная сеть, сеть общего пользования, интернет, цифровизация, права человека, цифровая среда.*

PEKAREVA Victoria Vladimirovna,
Master's student of Law Faculty
Herzen Russian State Pedagogical University,
St. Petersburg, Russia

LEGAL MECHANISMS FOR ENSURING THE SECURITY OF THE INFORMATION AND TELECOMMUNICATIONS NETWORK «INTERNET»

Annotation. *Given the need to achieve an ideal model of a 'middle ground' in theoretical and practical terms between the requirements for data localisation and controlled provision of cross-border data transfer within the framework of free use of the Internet by citizens, as well as the existence of equally important circumstances, such as the dynamic progress of crimes in the field of computer information, research into the dynamic field of legal regulation of the Internet with its unique properties is one of the priorities of scientific knowledge. In addition to identifying the specifics and problems of the existing regulatory framework for social interactions on the Internet, one of which, for example, is the timely adaptability of legal norms to current social relations and the existing possibilities of the digital network, technical means and solutions that are not always used for legal purposes, a comparative analysis of the legal regulation of information security of the Internet information and telecommunications network in some foreign countries is carried out.*

Key words: *information security, national security, information and telecommunications network, public network, internet, digitalisation, human rights, digital environment.*

Потребность в теоретико-правовой идентификации и необходимости в решении вопроса о критериях включения той или иной новой категории в число юридических и теоретико-правовых для последующего правоприменения в целях регламентации и урегулирования общественных отношений, в которых существует, используется и (или) функционирует техническое нововведение, инновации в принципе, в частности все области, связанные так или иначе с информационно-телекоммуникационной сетью «Интернет», основана на том, чтобы гарантировать правовую регламентацию общественных взаимодействий в информационной среде на принципе равноправия всех субъектов и на конституционно закрепленной свободе граждан осуществлять поиск, получение, создание и распространение сведений любыми не противоречащими законодательству способами, при одновременной защите их прочих законных прав, а главное – организовать разрабатываемыми, имеющимися и совершенствующимися нормами права конструктивное взаимодействие государственных органов, организаций и граждан при решении задач по обеспечению информационной безопасности. Также важнейшей функцией правового регулирования сети «Интернет» выступает установление и поддержание соразмерного равновесия, а именно, необходимо гармонизировать естественную потребность общества в беспрепятственном информационном обмене с объективной необходимостью введения ограничений для защиты суверенитета и обеспечения национальной безопасности государства. Шевко Н.Р. [8] и Верютин В.Н. [3] справедливо замечают, что развитие информационных технологий только усиливает взаимосвязь между информационной и национальной безопасностью, что влечёт за собой необходимость пересмотра приоритетов и модернизации как технических, так и правовых инструментов защиты.

На самом деле достижение баланса между контролем и свободой в такой глобальной и динамичной цифровой среде как Интернет можно по праву считать утопической идей. Однако попытаться достичь равновесия при выборе правильного подхода к правовому регулированию сложно, но вполне возможно.

Прежде всего, следует отметить фундаментальный разрыв между статичной природой законодательства и экспоненциальной скоростью технологической эволюции. Нормы, актуальные на момент их принятия, рискуют стремительно устареть под натиском новых технологических решений, что в большей степени касается сети «Интернет» из-за его структурной и функциональной специфики. Авакьян С.А. замечает недостаток норм права в плане неспешки в изменениях своей терминологии, понятийного аппарата, основных концепций[1], что в теории является вполне логичным, потому что право призвано обеспечить стабильность, предсказуемость принимаемых решений и действий. Не каждое техническое нововведение требует кардинальных изменений в правовой среде его регламентирующего, но каждое нововведение способствует приближению и необходимости к трансформации норм права. Также стоит обратить внимание на то, что даже если какие-либо определения технического характера находят свое место в нормах права, их регламентация не всегда происходит безупречно. В большинстве случаев может наблюдаться отсутствие унификации в формулировках понятий, а также несоответствие общепринятым профессиональным и научным определениям, связанным с информационной безопасностью государства, организаций и членов общества.

Не менее важным фактором являются обстоятельства, при которых осуществляются попытки применения национального законодательства по отношению к глобальным цифровым платформам и потокам данных, а также разворачиваются усилия по противодействию преступлений в информационно-цифровой среде, распространению «фейковых» сведений, и данный процесс неизбежно сталкивается с проблемой экстерриториальности, что приводит к конфликту правовых режимов различных государств. Возникает вопрос о соотношении государственного суверенитета и власти негосударственных акторов – транснациональных технологических корпораций, чьи внутренние политики и пользовательские соглашения фактически формируют собственную квазиправовую систему.

Разделяя точку зрения Чапис М.А. о правовом содержании информационной безопасности государства и о том, что юридические основания информационного правопорядка – это точки опоры на нормы действующего законодательства в области обеспечения информационной безопасности Российской Федерации, содержащиеся в Конституции России, законах и подзаконных актах, которые, несмотря на отсутствие единого закона, делают юридическую защиту интересов субъектов права информационной безопасности Российской Федерации с правовой точки зрения допустимой, а с юридической точки зрения – возможной и обоснованной[7], рассмотрим и проведем анализ отечественного законодательства, распространяющего свое действие на информационно-телекоммуникационную сеть «Интернет».

Детальной характеристике и структурированному исследованию подвергнется правовое регулирование как функционирования, так и взаи-

модействия задействованных в глобальной сети участников соответствующего типа общественных отношений. Внимание концентрируется на технических и организационных способностях Интернета в правовой среде.

Не будем останавливаться на основополагающих нормах права, содержащихся в Конституции Российской Федерации (например, статьях 2, 8, 13, 23,24,29) , которые бесспорно гарантируют охрану и защиту общественных отношений, прав граждан в самых разнообразных областях, причем их действие распространяется и на такую специфическую область, как информационная сфера, особый статус которой регламентирован в статье 71 Конституции РФ. Обратим свое внимание на такие нормативно-правовые акты, регулирующие функционирование и взаимодействие в информационно-телекоммуникационной сети «Интернет» как:

1. Ключевые в вопросах регулирования и обеспечения информационной безопасности являются: Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 №149-ФЗ и Федеральный закон «О персональных данных» от 27 июля 2006 №152-ФЗ;
2. Постановление Правительства Российской Федерации от 15 января 2024 г. №4 «Об утверждении правил установки, эксплуатации и модернизации в точках обмена трафиком технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования»: кто и как отвечает за установку, эксплуатацию и модернизацию технических средств противодействия угрозам (радиочастотная служба совместно с владельцами точек обмена трафиком); какой порядок взаимного обмена и обновления информации между радиочастотной службой и владельцами точек обмена трафиком (подача и ответ на запросы, сроки и форма взаимодействия), указаны требования к техническим характеристикам средств; обозначены строгие сроки для обмена информации и для уведомления о различных событиях (установка, модернизация, изменения подключения); оформление актов передачи и возврата технических средств и т.д.
3. Постановление Правительства РФ от 24 июля 2025 г. «1092 «О государственной информационной системе “Интеграционный шлюз национального сегмента Российской Федерации интегрированной информационной системы Евразийского экономического союза» (вместе с «Положением о государственной информационной системе „Интеграционный шлюз национального сегмента Российской Федерации интегрированной информационной системы Евразийского экономического союза“)» - основные положения связаны с регламентацией обеспечения обмена электронными документами и сообщениями между информационными системами, входящими в интегрированную информационную систему Евразийского экономического союза (ЕАЭС), реализуемыми по законодательству РФ и актам Евразийской экономической комиссии; унификация и маршрутизация электронных сообщений между пользователями и оператором шлюза. Одним из главных положений в данном правовом документе - утверждение требований к программно-техническим средствам, размещение на территории России, информация доступна на государственном русском языке, наличие сертификатов ФСБ и ФСТЭК по безопасности информации, ведение электронных журналов учёта операций с фиксированием времени и участников, а также обеспечение аутентификации и авторизации администраторов, защита от несанкционированного доступа;
4. Постановление Правительства РФ от 30 августа 2025 г. №1333 «Об утверждении правил установки, эксплуатации и модернизации в сети связи оператора связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования. Можно проиллюстрировать для общего понимания такими положениями как: в план мероприятий включаются планируемые даты ввода в эксплуатацию (модернизации) узлов связи операторов связи с указанием мест их размещения, количества планируемых каналов передачи данных с указанием их технологии и пропускной способности, планируемая дата начала установки технических средств противодействия угрозам, сведения о среднестатистической и максимальной загрузке каналов, к которым планируется подключать технические средства противодействия угрозам. Пропускная способность технических средств противодействия угрозам должна соответствовать или превышать пропускную способность сети связи, в которой установлены технические средства про-

тиводействия угрозам. При эксплуатации технических средств не допускается негативное влияние на функционирование сети связи общего пользования (потеря скорости, качества услуг связи, ухудшение других параметров) в связи с работой технических средств противодействия угрозам, в том числе их недостаточной пропускной способностью, за исключением случаев ограничения доступа к информации, распространяемой посредством сети «Интернет», доступ к которой должен быть ограничен в соответствии с законодательством Российской Федерации и многие другие указывающие на обязательный порядок по обеспечению целостности , безопасности и устойчивости функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования операторами связи;

5. Согласно Указу Президента РФ от 01 мая 2022 г. №250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» с 1 января 2025 г. органам (организациям) запрещается использовать средства защиты информации, странами происхождения которых являются иностранные государства, совершающие в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия, либо производителями которых являются организации, находящиеся под юрисдикцией таких иностранных государств, прямо или косвенно подконтрольные им либо аффилированные с ними, а также пользоваться сервисами (работами, услугами) по обеспечению информационной безопасности, предоставляемыми (выполняемыми, оказываемыми) этими организациями, а также в каждом таком органе должен быть ответственный и подразделение по информационной безопасности, для работы следует привлекать только лицензированные и аккредитованные российские компании, обеспечивать должностным лицам органов федеральной службы безопасности беспрепятственный доступ (в том числе удаленный) к принадлежащим органам (организациям) либо используемым ими информационным ресурсам, доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети «Интернет», в целях осуществления мониторинга данных;
6. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 31 июля 2024 г. №677 «Об утверждении требований о защите информации при предоставлении вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к информационно-телекоммуникационной сети «Интернет», операторам государственных информационных систем, муниципальных информационных систем, информационных систем государственных и муниципальных унитарных предприятий, государственных и муниципальных учреждений».
7. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 16 сентября 2024 г. n 773 «Об утверждении перечня индикаторов риска нарушения обязательных требований при осуществлении федерального государственного контроля (надзора) в сфере идентификации и (или) аутентификации» и другие.

Невозможно указать все нормативно-правовые акты от регулирующих до устанавливающих деятельность в рамках информационно-цифровой сети, их разрабатывается, существует и планируется огромное количество для поддержания стабильности в одной из сложных постоянно совершенствующейся технологической системой. Были приведены одни из последних с указанием определенных особенностей регламентации тех или иных сегментов, связанных с информационно-телекоммуникационной сетью «Интернет».

Также стоит обратить свое внимание на нововведения в порядок урегулирования отношений, существующих в информационно-телекоммуникационной сети «Интернет», с 1 марта 2026 года. Так, согласно Постановлению Правительства «Об утверждении Правил централизованного управления сетью связи общего пользования» за органом исполнительной власти будет законодательно закреплены права для полного оперативного управления интернет-трафиком в стране. Согласно новому правительственному постановлению, ведомство в лице РКН сможет напрямую отдавать предписания операторам связи, что фактически формирует систему централизованного контроля над российским сегментом Интернета.

Согласно данным правилам, Роскомнадзору предоставляются следующие возможности: мгновенное блокирование любых интернет-ресурсов; перенаправление интернет-трафика через специализированные технические средства; изменение маршрутов передачи данных и внедрение механизмов фильтрации с последующим ограничением доступа.

В дополнение к этому, ведомство имеет право переводить всю сеть связи в особый режим ручного управления при возникновении определённых угроз. Среди таких угроз следует понимать следующие ситуации: перебои или полное отсутствие связи, вызванные авариями или перегрузкой сети; сбои в работе объектов, которые имеют критически важное значение; доступ к интернет-ресурсам, чьё использование ограничено на территории Российской Федерации; проведение компьютерных атак.

Основная задача инициативы заключается в обеспечении устойчивой работы, защиты и сохранения целостности российского сегмента Интернета, особенно в условиях возникновения внешних и внутренних угроз.

Восприятие подобных регуляторных мер в обществе не может быть чем-то однозначным, как и формирование отношения к любому явлению, которое обычно носит амбивалентный характер. С позиции рядового пользователя, не погруженного в геополитические и технические нюансы, на первый план могут выходить преимущественно отрицательные аспекты и возможные ограничения, связанные с реализацией указанных целей.

Тем не менее, подобная перспектива не охватывает всей полноты картины. Следует признать, что у данного начинания существуют и определенные преимущества, рассмотрение которых требует более взвешенного и комплексного анализа, выходящего за рамки обыденного восприятия. Однако надо понимать, что одними ограничениями и контролем решить главные проблемы в цифровой среде невозможно, поскольку то, что можно запретить никуда не исчезнет, поэтому эффективной можно признать работу по преодолению негативных сторон такой глобальной сети как «Интернет» за счет изучения подноготной, например, тех же киберпреступлений, чтобы понимать, как работает то или иное действие/бездействие, перестающее в противоправное, как отслеживать цифровой след во всех формах и попытках злоумышленником скрыть его и т.д.

В рамках сравнения и возможного выбора направления совершенствования существующих норм права, регулирующих различные типы взаимодействия в сети «Интернет», проведем характеристику осуществляющего регламентацию процессов, происходящих в цифровой среде, законодательства Китайской Народной Республики.

Позицию о правовой модели цифровой среды в КНР можно понять по рассуждениям в опубликованной Информационном бюро Государственного совета «Белой книге» о «Совместной работе по созданию сообщества судьбы в киберпространстве»: «Следует уважать права всех стран на выбор собственного пути развития сети и модели управления, а также на равноправное участие в международном управлении в киберпространстве. Все страны имеют право формулировать государственную политику, законы и положения о киберпространстве в контексте своих национальных условий и международного опыта. Ни одна страна не должна стремиться к кибергегемонии; использовать Интернет для вмешательства во внутренние дела других стран; участвовать, подстрекать или поддерживать кибердеятельность, которая ставит под угрозу национальную безопасность других стран или нарушает критическую информационную инфраструктуру других стран»[2].

Правовая система КНР гибридная, неоднородная, развивающаяся в тенденциях юридического плюрализма. Поэтому представлять систему законодательства КНР, регулирующего как использование технических средств, искусственного интеллекта, иных инноваций, так и информационно-телекоммуникационной сети «Интернет», довольно затруднительно. К тому же в рассматриваемой стране существует многочисленное количество законов и подзаконных актов, которые в совокупности охватывают вопросы регулирования, стандартизации и обеспечения национальной и личной безопасности все новых сфер цифровой действительности. Одни из основных законов и иных правовых положений с их особенностями изложены в *таблице 1.*

Система государственного надзора за цифровой средой в Китайской Народной Республике представляет собой одну из наиболее развитых и всеобъемлющих структур по мониторингу и фильтрации сетевого контента в глобальном масштабе. Ключевым элементом данной системы является повсеместное внедрение процедуры обязательной верификации личности на всех онлайн-ресурсах, что фактически исключает для граждан возможность сохранять анонимность при осуществлении деятельности в интернете. Примечательно, что функции правового регулирования значительной части национального сегмента сети не сконцентрированы исключительно в руках центральных государственных органов. Полномочия по надзору активно передаются на исполнение различным децентрализованным структурам.

Признавая, что динамичное внедрение информационно-коммуникационных технологий кардинально меняет глобальный ландшафт, правительства Российской Федерации и Республики Сербии выражают обеспокоенность их возможным деструктивным использованием. В частности, речь идет о рисках вмешательства во внутренние дела суверенных государств, нарушениях суверенитета, безопасности и прав граждан на частную жизнь, а также о попытках разжигания

Таблица 1. Законы КНР, регулирующие отношения в цифровой среде.

Наименование нормативно-правого акта	Особенности его функционирования	
Закон Китайской Народной Республики о кибербезопасности от 2016 г. *(разработан в целях: обеспечения кибербезопасности; защиты суверенитета и национальной безопасности в киберпространстве, а также социальных и общественных интересов; защиты законных прав и интересов граждан, юридических лиц и других организаций; содействия здоровому развитию информатизации экономики и общества)*	Глава I: Общие положения Глава II. Поддержка и продвижение кибербезопасности Глава III. Безопасность сетевых операций Раздел 1. Общие положения Раздел 2. Безопасность операций в критически важной информационной инфраструктуре Глава IV. Сетевая информационная безопасность Глава V: Мониторинг, раннее оповещение и реагирование на чрезвычайные ситуации Глава VI: Юридическая ответственность Глава VII: Дополнительные положения Например, статья 21: Государство внедряет многоуровневую систему защиты кибербезопасности [MLPS]. Операторы связи	должны выполнять определенные обязанности по обеспечению безопасности в соответствии с требованиями многоуровневой системы защиты кибербезопасности, чтобы гарантировать отсутствие помех, повреждений или несанкционированного доступа к сети, а также предотвратить утечку, кражу или фальсификацию сетевых данных. Например, внедрить технические средства для мониторинга и регистрации рабочего состояния сети и инцидентов, связанных с кибербезопасностью, а также обеспечить хранение сетевых журналов в течение как минимум шести месяцев; принять меры по классификации данных, созданию резервных копий важных данных и их шифрованию и т.д.
Постановление Государственного совета Китайской Народной Республики № 745 от 2021 года «Правила защиты критически важной информационной инфраструктуры»	Статья 2: Критически важная информационная инфраструктура, как указано в настоящем постановлении, относится к важной сетевой инфраструктуре, информационным системам и т. д. в таких значимых отраслях и секторах, как государственные телекоммуникационные и информационные службы, энергетика, транспорт, водоснабжение, финансы, государственные услуги, электронное правительство, национальная оборонная наука, технологии, промышленность и т. д., а также к тем сферам, где их разрушение, потеря функциональности или утечка данных могут нанести серьёзный ущерб национальной безопасности, национальной экономике и благосостоянию населения или общественным интересам. Регламентирована защита и продвижение, а также установлены дополнительные виды ответственности, например *статья 40* (несообщение о возникновении крупного инцидента кибербезопасности в критически важной информационной инфраструктуре или обнаружении серьезной угрозы кибербезопасности не сообщают об этом в департамент работы по защите и орган общественной безопасности), *статья 41* (приобретение операторами сетевых продуктов	и услуг, которые могут повлиять на национальную безопасность, и не проведение проверку безопасности в соответствии с национальными правилами кибербезопасности, *статья 42* (не обеспечивание сотрудничества с отделами защиты, выполняющими работы по проверке кибербезопасности критической информационной инфраструктуры и мониторингу, а также с общественной безопасностью, государственной безопасностью, административным управлением по защите тайны, управлением шифрованием и другими такими соответствующими подразделениями, законно выполняющими работы по проверке кибербезопасности критической информационной инфраструктуры), *статья 43*(лица, осуществляющие незаконное вторжение в критически важную информационную инфраструктуру, вмешательство в ее работу или разрушение, наносящие ущерб ее безопасности, но не являющиеся преступлением, должны, согласно соответствующим положениям «Закона Китайской Народной Республики о кибербезопасности», быть конфискованы органами общественной безопасности за незаконный доход, задержаны на срок до пяти дней и дополнительно может быть наложен штраф.
Правила управления информационным push-сервисом во всплывающем окне Интернета от 30 сентября 2022 года.	Лица, предоставляющие услуги по распространению информации во всплывающих окнах в Интернете, должны соответствовать перечню требований. Например, запрещается распространять незаконную и нежелательную информацию, предусмотренную "Правилами экологического управления информационным контентом в Интернете", особенно контент, нарушающий общественный порядок и добрые обычаи, такой как злонамеренное спекулирование развлекательными сплетнями, неприкосновенность частной жизни, расточительность богатства, уродство и безобразничанье, и не допускается злонамеренное перемещивание	с целью сосредоточения внимания на определенной теме; также там, где рекламная информация размещается во всплывающих окнах, она должна быть идентифицируемой, с четко обозначенными надписями "реклама" и "закрытие", гарантирующими закрытие всплывающей рекламы одним щелчком мыши;Ссылки сторонних производителей, QR-коды и другая информация, которая злонамеренно сливается и переходит, не должны предоставляться посредством всплывающей информационной рассылки, и пользователей нельзя побуждать нажимать на всплывающие информационные рассылки для совершения мошенничества с трафиком или перехвата трафика.
Правила управления информацией об учетных записях пользователей Интернета от 09.06.2022 года	Регистрация пользователей Интернета, использование и управление информацией учетной записи пользователя Интернета поставщиками информационных услуг Интернета должны соответствовать законам и нормативным актам, общественному порядку и добрым обычаям, быть честными и заслуживающими доверия и не должны наносить ущерб национальной безопасности, социальным и общественным интересам или законным правам и интересам других лиц, должны соответствовать истинной профессиональной информации пользователя. Поставщики информационных услуг Интернета должны отображать информацию об атрибуции адресов учетных записей пользователей Интернета по интернет-протоколу (IP) в разумных пределах на странице информации об учетной записи пользователя Интернета для облегчения общественного контроля в общественных интересах.	
Положение об управлении Информационными сервисами мобильных интернет-приложений	Помимо установления правил функционирования и регулирования в правовой среде, определены следующие дефиниции: **«мобильное интернет-приложение»** - прикладное программное обеспечение, которое приобретается и запускается на мобильном интеллектуальном терминале путем предварительной установки, загрузки и т.д. для предоставления информационных услуг пользователям.	**«поставщик мобильных интернет-приложений»** - владелец или оператор мобильного интернет-приложения, предоставляющего информационные услуги. **«Интернет-магазин приложений»** - платформа, которая предоставляет просмотр, поиск, загрузку прикладного программного обеспечения или инструменты разработки и услуги по выпуску продукта через Интернет.

межнациональной и религиозной розни. Страны придают важное значение информационной безопасности как ключевому элементу международной стабильности, поддерживают разработку под эгидой ООН норм ответственного поведения государств в информационном пространстве и подтверждают распространение государственного суверенитета и юрисдикции на информационную инфраструктуру на их территории. Кроме того, Сербия выражает заинтересованность в развитии сотрудничества с Российской Федерацией в сфере цифровизации. Основываясь на резолюции ГА ООН 73/27, принципах взаимного уважения и будучи убежденными в необходимости углубления доверия, вышеуказанные страны согласовали правовые и организационные основы сотрудничества в сфере информационной безопасности, не направленного против интересов третьих лиц, о чем свидетельствует Распоряжение Правительства РФ от 26 февраля 2022 г. №332-р «О подписании Соглашения между Правительством Российской Федерации и Правительством Республики Сербии о сотрудничестве в области обеспечения информационной безопасности». Одни из механизмов реализации сотрудничества: координирующие органы от России – аппарат Совета Безопасности РФ; от Сербии – Министерство внутренних дел Республики Сербии, также практическое

взаимодействие осуществляется через компетентные органы государств, которые определяются сторонами; регулярные межведомственные консультации проводятся не реже одного раза в год, а также по мере необходимости, страны могут заключать дополнительные договоры по конкретным направлениям.

Международное сотрудничество в принципе всегда сталкивается с множеством препятствий – будь то политические разногласия, экономические вызовы или культурные различия. Однако, даже в таких непростых условиях, диалог с многими странами продолжается, а желание находить общие точки соприкосновения не угасает, тем более в плане обеспечения информационной безопасности.

Президент Российской Федерации Владимир Путин направил приветствие участникам проводимой 23 октября 2025 г. IX Международной научно-практической конференции «Проблемы защиты прав человека: обмен лучшими практиками омбудсменов», в которой отметил требующие особого внимания обстоятельства, а именно: «...стремительное развитие информационно-коммуникационных технологий, в том числе искусственного интеллекта, не только открывает новые возможности для экономического роста и повышения уровня жизни, но и сопряжено с весьма серьёзными рисками. В нашей стране последовательно реализуется комплекс мер по защите цифровых прав граждан, осуществляется системная работа по совершенствованию законодательных норм, регулирующих сбор, передачу, обработку и хранение персональных данных, внедряются передовые методы обеспечения кибербезопасности. Хотел бы подтвердить, что Россия открыта к обмену опытом и самому активному взаимодействию с зарубежными партнёрами на данном направлении». Учитывая, что и сама информация может быть источником существенной угрозы, поэтому безопасность рассматривается не только преимущественно с точки зрения защиты ее количественно-качественных характеристик[5], но со стороны состояния сохранности, надежности, что автоматически предполагает поддержание определенного баланса между негативным воздействием на субъект окружающей его среды и его способностью преодолеть это воздействие либо собственными ресурсами, либо при помощи соответствующих, специально для этого созданных органов или механизмов[4].

Таким образом, дальнейший анализ правового механизма обеспечения информационной безопасности цифровой среды, в частности информационно-телекоммуникационной сети «Интернет», должен выйти за пределы догматического толкования норм среди юристов и перейти к прогностическому моделированию и междисциплинарному синтезу, объединяющему юриспруденцию, информатику, криптографию и социологию. Ключевой задачей становится не просто кодификация существующего положения общественных отношений и имеющихся проблем, а главное – разработка соответствующих техническим характеристикам и адаптивных, «гибких» регуляторных моделей, способных динамично реагировать на технологические вызовы, обеспечивая при этом защиту фундаментальных прав человека в новую цифровую эпоху.

Список литературы:

[1] Авакьян С. А. Информационное пространство знаний, цифровой мир и конституционное право // Конституционное и муниципальное право. 2019. № 7. С. 23—24.

[2] Белая Книга // Центральное народное правительство Китайской Народной Республики URL: https://www.gov.cn/zhengce/2022-11/07/content_5725117.htm (дата обращения: 09.11.2025).

[3] Верютин В.Н. Административно-правовой механизм обеспечения информационной безопасности как составной части национальной безопасности // Вестник Краснодарский университета МВД России. 2009. №1. С. 138-141

[4] Зеленков М. Ю. Теоретико-методологические проблемы теории национальной безопасности РФ. М. : Юридический институт МИИТа, 2013. 210 с.

[5] Некрасов, Д. Е. Информационная безопасность как криминологическая проблема / Д. Е. Некрасов, А. А. Брюхнов, И. П. Напханенко // Юристъ-Правоведъ. – 2025. – № 1(112). – С. 158-164. – EDN XDWJMU.

[6] Участникам IX Международной научно-практической конференции «Проблемы защиты прав человека: обмен лучшими практиками омбудсменов» // Официальный сайт Президента России URL: http://www.kremlin.ru/events/president/letters/78270 (дата обращения: 01.11.2025).

[7] Чапис М. А. Информационная безопасность государства как правовой порядок обеспечения национальной безопасности в информационной сфере / М. А. Чапис // Наукосфера. – 2024. – № 6-1. – С. 551-557. – DOI 10.5281/zenodo.11638587. – EDN JKTRGZ.

[8] Шевко Н.Р. Актуальные проблемы обеспечения информационной безопасности современного общества // Вестник Казанского юридического института МВД России. 2012. №8. С. 57–59.

References:

[1] Avakyan S. A. Information about the space of knowledge, the digital world and constitutional law// Constitutional and municipal law. 2019. № 7. S. 23-24.

[2] White Paper//Central People's Government of the People's Republic of China URL: https://www.gov.cn/zhengce/2022-11/07/content_5725117.htm (Accessed: 09.11.2025).

[3] Veryutin V.N. Administrative and legal mechanism for ensuring information security as an integral part of national security//Bulletin of the Krasnodar University of the Ministry of Internal Affairs of Russia. 2009. №1. S. 138-141

[4] Zelenkov M. Yu. Theoretical and methodological problems of the theory of national security of the Russian Federation. M.: MIIT Law Institute, 2013. 210 s.

[5] Nekrasov, D. E. Information security as a criminological problem/D. E. Nekrasov, A. A. Bryukhnov, I. P. Napkhanenko//Lawyer-Pravod. – 2025. – № 1(112). - S. 158-164. – EDN XDWJMU.

[6] Participants of the IX International Scientific and Practical Conference "Problems of Protecting Human Rights: Exchange of Best Practices of Ombudsmen "//Official website of the President of Russia URL: http://www.kremlin.ru/events/president/letters/78270 (date of appeal: 01.11.2025).

[7] Chapis M. A. Information security of the state as a legal procedure for ensuring national security in the information sphere/M. A. Chapis//Naukosphere. – 2024. – № 6-1. - S. 551-557. – DOI 10.5281/zenodo.11638587. – EDN JKTRGZ.

[8] Shevko N.R. Actual problems of ensuring information security of modern society//Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. 2012. №8. S. 57-59.