ПРАВОВЫЕ АСПЕКТЫ РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННОЙ СРЕДЫ

Карцхия А.А.[1]

Ключевые слова: *киберпространство, национальная безопасность, информационное право, цифровое право, персональные данные, кибербезопасность, защита информации.*

Аннотация

Цель исследования: правовой анализ информационной среды, ее содержания и особенностей формирования при использовании современных информационно-коммуникационных и цифровых технологий, которые находят свое отражение в национальном и международном праве.

Методы исследования: сравнительно-правовой анализ действующего российского и международного законодательства в сфере информационной цифровой среды и практики применения, а также формально-логическое исследование понятийного аппарата, содержания и структуры предмета исследования.

Результаты исследования: сформулированы особенности информационной цифровой среды и ее содержания, в т. ч. с точки зрения кибербезопасности и национальной безопасности в информационной сфере. Автор полагает закономерным формирование информационной среды, цифрового технологического пространства в новом, не аналоговом физическом измерении как новой сферы правового регулирования, что обусловливает формирование специального законодательства в данной сфере и специального правового регулирования.

Научная новизна исследования: выявление понятия и качественных характеристик, особенностей содержания информационной цифровой среды, ее элементов и степени влияния на реальные отношения.

DOI: 10.24412/1994-1404-2025-1-19-31

Введение

XX век стал свидетелем масштабных социальных преобразований, а 1950-е годы ознаменовались сменой парадигмы — «информационной революцией», связанной с формированием «информационного общества», или общества, основанного на знаниях. Мир изменился и тогда, когда Интернет в 1993 году стал общедоступным пространством, создав цифровую параллель с повседневной «аналоговой» жизнью. За последние два десятилетия цифровые технологии коренным образом изменили восприятие информации и взаимодействие с ней. Интернет позволил создавать контент и делиться им с широкой аудиторией с минимальными затратами, социальные сети стерли границы между личной и массовой коммуникацией, а поисковые системы сделали огромные объемы информации широко, мгновенно и свободно доступными. Однако первоначальный оптимизм по поводу позитивного преобразующего потенциала цифровых технологий уступил место критическому осознанию связанных с ними рисков, включая риски поляризации общества по идеологическим воззрениям и фрагментации политического дискурса, возрастающие риски недобросовестного распространения дезинформации в Интернете с использованием противоправных способов. В общий лексикон вошел термин «киберпреступность», которая затрагивает уже всех, а не только беспечных граждан или «небрежный» бизнес. Каждый человек и организация могут стать потенциальной мишенью, сталкивались с киберпреступностью в той или иной форме. Информационная безопасность приобретает первостепенное значение как для граждан, так и для компаний. Конфиденциальность все чаще рассматривается как основополагающее требование как для деловой практики, так и для отношений частного характера, а защита конфиденциальной информации стала неотъемлемой частью коммерческой деятельности. В то же время кибербезопасность стала стратегическим приоритетом не только государственной политики, но и предпринимательства и частной жизни. Нарушение конфиденциальности может привести к значительному юридическому, финансовому и репутационному ущербу, что подтверждает необходимость комплексного подхода к защите данных. Соблюдение всемирно признанных

[1] ***Карцхия Александр Амиранович,*** *доктор юридических наук, профессор РГУ нефти и газа (НИУ) им. И.М. Губкина, г. Москва, Российская Федерация.*

E-mail: arhz50@mail.ru

стандартов безопасности обес-печивает прозрачность и всестороннюю ИТ-защиту. Соблюдение глобальных стандартов безопасности, отслеживаемость и подотчетность приобретают решающее значение, особенно в трансграничных контактах или международных сделках, где безопасность обработки данных имеет решающее значение. Соответствие мировым стандартам безопасности должно демонстрировать приверженность компаний и отдельных лиц информационной безопасности, а также обеспечивает структурированные подходы к управлению рисками кибербезопасности.

Технический прогресс, как отмечается в рекомендациях ООН[2], за несколько коротких десятилетий произвел революцию в сфере коммуникаций, объединив отдельных людей и сообщества в немыслимых ранее масштабах и предоставив беспрецедентные возможности для распространения знаний, культурного обогащения и устойчивого развития. Они во многом повысили стремление к целостности информационной экосистемы, где в полной мере обеспечивается свобода выражения мнений и где точная, надежная информация, свободная от дискриминации и ненависти, доступна всем в открытой, инклюзивной, безопасной информационной среде. Хотя эти достижения позволили массово распространять информацию, они также способствовали распространению дезинформации и разжиганию ненависти многими субъектами с беспрецедентными в истории объемами, скоростью и вирусностью, ставя под угрозу целостность информационной экосистемы. Такие риски включают в себя целый ряд текущих, возникающих и будущих угроз в условиях стремительного развития технологий искусственного интеллекта (ИИ). Такое нарушение целостности информационного пространства может подорвать способность людей осуществлять права человека и помешать усилиям по достижению мира, процветания и достойного будущего на нашей планете. Таким образом, задача укрепления информационной целостности представляет собой одну из наиболее актуальных задач нашего времени. Информационная целостность предполагает плюралистическое информационное пространство, которое защищает права человека, мирные общества и устойчивое будущее. Оно несет в себе обещание цифровой эры, которая способствует доверию, знаниям и индивидуальному выбору для всех. Обеспечение целостности информации предполагает предоставление людям возможности осуществлять свое право искать, получать и распространять информацию и идеи любого рода, а также беспрепятственно придерживаться своего мнения. Во все более сложной цифровой информационной среде это означает предоставление людям возможности безопасно перемещаться в информационном пространстве, сохраняя конфиденциальность и свободу. Усилия по повышению целостности информации имеют решающее значение для сохранения и дальнейшего продвижения целей в области устойчивого развития.

Разрушительные возможности манипулирования информацией как один из указанных WEF 2025 глобальных рисков[3] стремительно возрастают по мере распространения открытого доступа ко всё более совершенным технологиям и снижения доверия к информации и институтам. Число пользователей Интернет и соцсетей неуклонно растет из года в год (см. табл. 1 и табл. 2). Вместе с тем дезинформация — новый лидер топ-10 рейтинга глобальных рисков. Простые в использовании интерфейсы для крупномасштабных моделей ИИ, которые больше не требуют специальных навыков, уже привели к резкому росту количества фальсифицированной информации и так называемого «синтетического» контента — от сложного клонирования голоса до поддельных веб-сайтов. Для борьбы с растущими рисками правительства начинают внедрять новые и постоянно меняющиеся нормативные акты, нацеленные как на владельцев, так и на создателей онлайн-дезинформации и незаконного контента. Зарождающееся регулирование генеративного ИИ сможет дополнить эти усилия. Например, в КНР требования о нанесении водяных знаков на контент, созданный с помощью ИИ, могут помочь идентифицировать ложную информацию, включая непреднамеренную дезинформацию с помощью контента, созданного с помощью ИИ. В течение следующих двух лет искусственный контент будет манипулировать людьми, наносить ущерб экономике и разрушать общество различными способами. Фальсифицированная информация может быть использована для достижения различных целей, от борьбы за изменение климата до эскалации конфликтов. Также будут распространяться новые виды преступлений, такие как подделка порнографии без согласия пользователя или манипулирование фондовым рынком. Существует риск нарушения баланса между предотвращением дезинформации и защитой свободы слова, усиления нормативного контроля со стороны государства за информацией для нарушения прав человека, широкое использование дезинформации и средств ее распространения для разжигания публичных беспорядков и насильственных протестов, преступлений на почве ненависти и даже гражданской конфронтации и терроризма.

[2] United Nations Global Principles for Information Integrity. Recommendations for Multi-Stakeholder Action. URL: https://www.un.org/sites/un2.un.org/files/un-global-principles-for-information-integrity-en.pdf

[3] Global Risks Report 2024, WEF 2025, p. 18. URL: https://trendsunplugged.io/wp-content/uploads/2024/01/The-Global-Risks-Report-2024.pdf

Таблица 1

Число пользователей Интернет в мире (млрд человек)

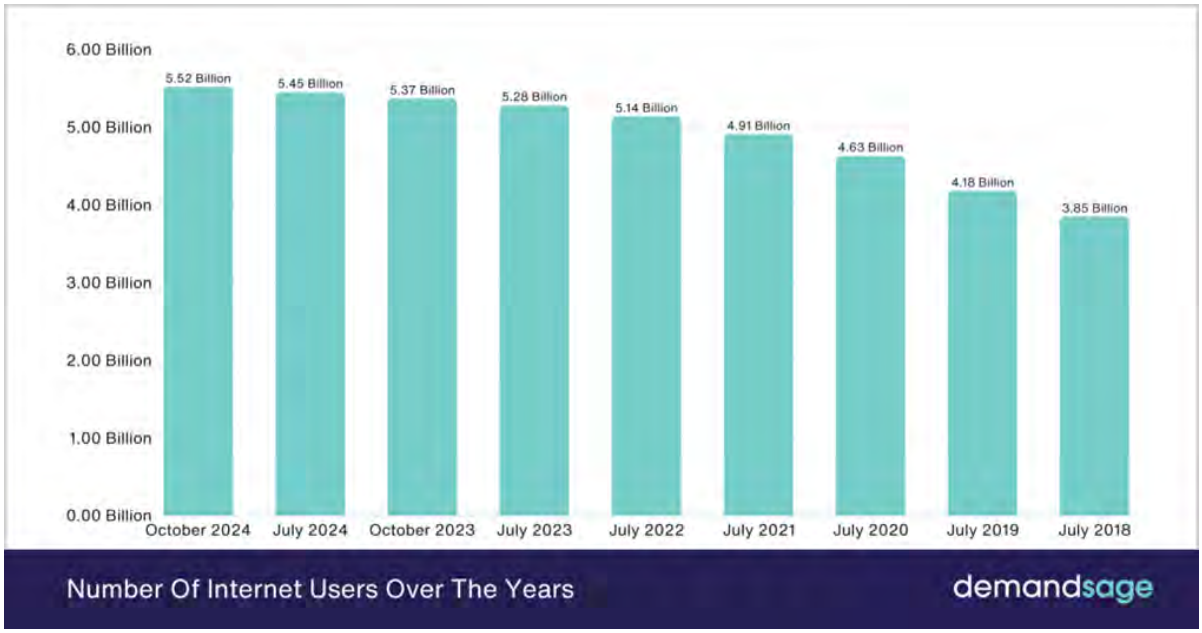
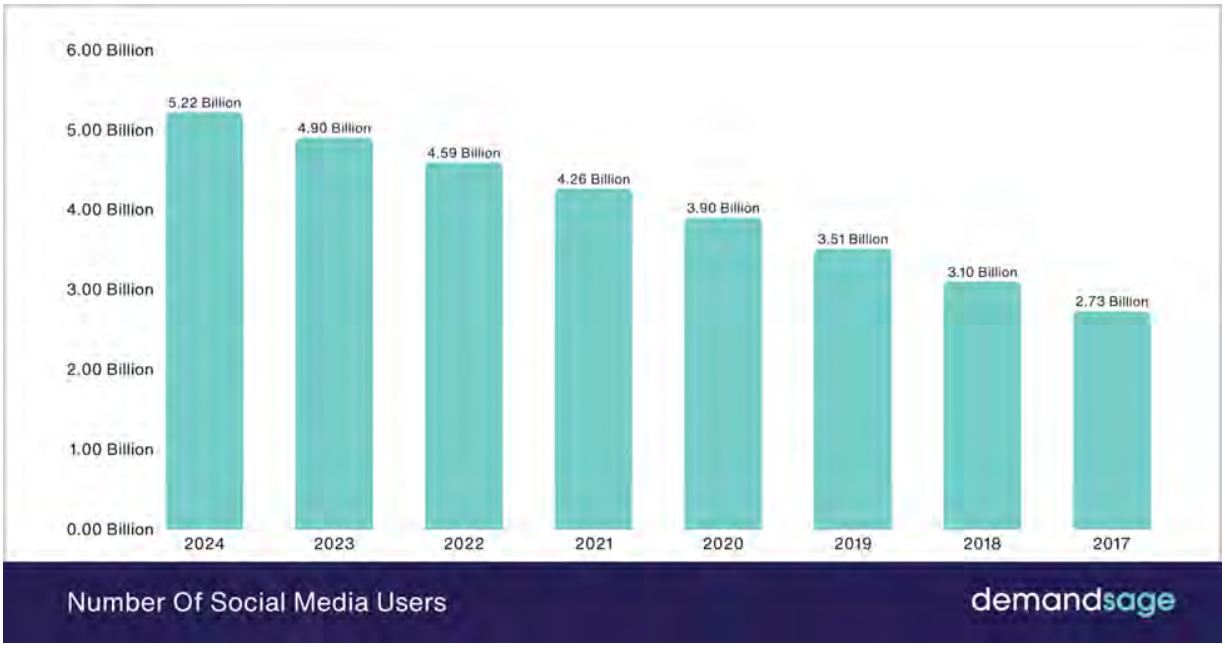


Таблица 2

Число пользователей социальных сетей в мире (млрд человек)



Источник: https://www.demandsage.com/internet-user-statistics

Информационная среда: понятие и особенности

Часто информационная среда понимается как пространство, где сходятся человеческое познание, технологии и контент, где информация обрабатывается людьми и, все чаще, машинами и которое включает технологии, используемые для обработки этой информации и доступа к ней, в том числе мобильные телефоны, Интернет и дополненная реальность, а также сопутствующий контент. Иными словами, информационная среда представляется адаптивной системой, сложность которой возрастает с появлением новых социальных норм и технологий, которая подвергается негативным влияниям, угрожающим целостности такой среды, психологическому и физическому здоро-

вью ее участников, даже общественной безопасности и государственному строю[4].

Термин «информация» преимущественно используется как абстрактное массовое понятие и обозначает любой объем данных, кода или текста, который хранится, отправляется, принимается или обрабатывается любым способом. Точное значение термина «информация» в разных философских традициях различно, а его разговорное употребление варьируется географически и в разных прагматических контекстах. Хотя анализ понятия информации был темой западной философии с самого ее зарождения, явный анализ информации как философской концепции появился недавно и восходит ко второй половине XX века. Исторически сложилось так, что изучение концепции информации можно рассматривать как попытку сделать измеримыми обширные свойства человеческого знания. Информация включает в себя широкий спектр понятий и явлений. Они относятся как к процессам, так и к материальным состояниям, которые тесно взаимосвязаны. Информация может быть продуктом, который включает в себя информацию как вещь, как объект, как ресурс, как товар, или то, что передается по каналу, включая сам канал, или даже фактическое содержание носителя. Информация имеет множество различных абстракций. Данные могут быть как отдельными наблюдениями, так и примитивными сообщениями низкого уровня. Информация представляется как отсортированные, классифицированные или проиндексированные данные в организованные наборы. В то же время информация — это отличный товар, которым обычно обмениваются люди-операторы, стремящиеся приобрести достаточно знаний о рассматриваемой проблеме. Понимание информации (знание) обеспечивает определенную степень понимания как статических, так и динамических взаимосвязей объектов данных и способность моделировать структуру и поведение этих объектов в прошлом (и будущем). Знания включают в себя как статическое содержимое, так и динамические процессы. Экспертные знания представляют собой совокупность знаний по определенной теме, предмету или процессу, которое позволят достичь информационного превосходства, т. е. способности собирать, обрабатывать и распространять непрерывный поток информации, одновременно используя или лишая противника возможности делать то же самое[5].

Последние десятилетия отечественными исследователями активно развивались воззрения, согласно которым жизнь человека развёртывается не только в физической среде, мире природы, но и в им же созданном искусственном мире, который делится на два основных компонента — техносферу (мир науки, техники, технологий) и информационную среду[6]. Техносфера рассматривается как часть биосферы, коренным образом преобразованная человеком в технические и техногенные объекты, становящиеся частью ноосферы. Информационная среда общества не представляется статичной, наполняемость ее изменяется по мере развития технических средств.

Изменение взаимодействия участников с информационной средой, беспрецедентный масштаб и уровень детализации при анализе огромных объемов данных в любых сферах жизнедеятельности позволяют с новых позиций рассматривать преимущества и риски цифровых преобразований, оценивать фундаментальные когнитивные механизмы взаимодействия с информацией и выдвигать новые гипотезы о функционировании этих механизмов в эпоху цифровых технологий. Такой подход объективно нуждается в определении термина «информационная среда», который часто используется без предварительного определения и приобретает различные значения в зависимости от контекста, в котором он используется.

Как отмечают современные исследования [3; 8], термин «информация» сам по себе не имеет единого определения. Одна из интересных концепций сформулирована в семиотике, науке о знаках и сигналах в широком спектре биологических, инженерных и социальных систем. Специалисты этой области понимают информацию как неожиданное, новое содержание знака, означающее, что существует двоякое понимание информации, поскольку оно относится как к объекту, служащему знаком, так и к когнитивному процессу распознавания новизны в нем. Так, широко используется общее определение информации[7], основанное на семиотической концепции информации как «текст + контент» (*text* + *content*)[8] либо как «данные + значение» (*data* + *meaning*). Такой концептуальный подход основан на том, что информационное наполнение состоит из данных, которые являются правильно сформированными, т. е. синтаксически корректными, и значимыми (семантически корректными). Данные, в свою очередь, могут быть поняты как неинтерпретируемое отсутствие единообразия в реальном мире, между сигналами или символами. К примеру, новостная статья представляет собой информацию, поскольку она состоит из данных (букв), следует грамматическим пра-

[4] Alicia Wanless and Jacob N. Shapiro. A CERN Model for Studying the Information Environment, 2022 Carnegie Endowment for International Peace and Princeton University. URL: https://carnegie-production-assets.s3.amazonaws.com/static/files/ Wanless_Shapiro_CERN_final.pdf

[5] Michel J. Menou, Richard D. Taylor. A "Grand Challenge": Measuring Information Societies. Inf. Soc. 22(5):261–267; Birger Hjørland. Theory and metatheory of information science: A new interpretation. Journal of Documentation, December 1998. URL: https://www.researchgate.net/publication/228717437; R. Mathar. Information Theory. URL: https://ti.rwth-aachen.de/teaching/InformationTheory/ws1819/data/InformationTheory.pdf

[6] Дружилов С.А. Современная информационная среда и экология человека: психологические аспекты // Hygiene & Sanitation (Russian Journal). 2018. № 97. С. 597—602.

[7] Floridi, Luciano (2005). Semantic conceptions of information, Stanford Encyclopedia of Philosophy; Floridi, Luciano (2010). Information: A Very Short Introduction. Oxford University Press, 2010.

[8] Raber, Douglas and John M Budd (2003). Information as sign: semiotics and information science. Journal of Documentation. 2003. 59(5): 505—522. DOI: 10/1108/00220410310499564 .

вилам и доносит смысл до читателя. Упрощенно можно определить окружающую среду как физическое, социальное и цифровое окружение индивида, в частности, те аспекты этого окружения, которые могут влиять на поведение индивида.

Следуя этому концепту, информационную среду можно определить как состоящую из всех информационных процессов, услуг и сущностей, включая, таким образом, информационных агентов, а также их свойства, взаимодействия и взаимоотношения. Примечательно, что термин «агент» охватывает как отдельных лиц, так и организации. Отдельные лица могут обрабатывать информацию, которую они получают, и взаимодействовать с ней посредством социальных сетей или средств массовой информации. Они также могут формировать свою информационную среду и вносить в нее свой вклад, самостоятельно создавая информационный контент или делясь им. Они могут действовать в одиночку или группой, скоординированно или нескоординированно. С другой стороны, организации включают в себя новостные агентства и другие учреждения, которые создают и распространяют информацию, а также, в частности, цифровые платформы и социальные сети, которые облегчают обмен информацией между отдельными лицами, а также между отдельными лицами и организациями. Информационная среда динамична и меняется в зависимости от технологических инноваций, а также социальных и политических обстоятельств. Анализ влияния информационной среды на индивидов и группы означает анализ фактических данных о том, как эта среда влияет на индивидуальное и коллективное поведение, а также о том, как индивиды и группы взаимодействуют с ней и друг с другом, находясь в ней[9].

Такое определение информационной среды наиболее близко к тому, которое используется в политологии или науке о коммуникациях. Но оно формулируется в расширенном контексте в качестве синонима новостной медиасреды, в частности, печати и телевидения, которая охватывает передачу социальной информации, цифровые информационные платформы и социальные медиа, а также политически значимой информации. Такое понимание информации тем не менее исключает описание информации на финансовых рынках, которая позволяет корпорациям принимать решения, или информации, используемой в корпорациях для руководства и организационной структуры. Однако информационная среда не является внутренне сплоченной и универсальной областью. Так, имеются географические различия в информационной среде, связанные с глубокими экономическими и социальными различиями между развитыми и развивающимися странами, которые отражаются в явных различиях в том, как люди воспринимают информацию по всему миру. Например, доступ в Интернет, который радикально изменил информационную среду, предоставив доступ к онлайн-новостным сайтам и социальным сетям, расширяется во всем мире, но еще не полностью охватил страны Глобального Юга. Так, в 2019 году Международный союз электросвязи ООН сообщил, что уровень использования Интернета в странах Глобального Севера приближается к уровню насыщения: 80,1% и 74,6% пользователей в Европе и Северной и Южной Америке находятся в Сети, в то время как в Африке только 26,3% людей пользовались Интернетом, а в арабских государствах и Азиатско-Тихоокеанском регионе — 49,5% и 46,2% людей соответственно. Помимо географических различий, демографические характеристики являются ключевым фактором, определяющим индивидуальную информационную среду. Возраст, в частности, имеет большое значение, который в первую очередь касается потребления новостей, а не информации в целом. Так, молодое поколение в подавляющем большинстве случаев потребляет новости со своих смартфонов, особенно через социальные сети, в то время как старшие поколения в бóльшей степени полагаются на телевидение, радио и печатные издания. Примечательно, что среди пользователей социальных сетей существует разделение по поколениям, например: 93% подростков в возрасте от 16 до 24 лет имели профиль в социальных сетях, в то время как 58% людей в возрастной категории 55—64 года и 34% — в возрастной группе 65—74 года [8].

Информационная среда и информационная безопасность

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 23.11.2024) (далее — Закон об информации)[10] содержит определение «информация» как сведения (сообщения, данные) независимо от формы их представления, а также понятие «информационно-телекоммуникационная сеть», которая представляет собой технологическую систему, предназначенную для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. Информация может носить ограниченный характер доступа и распространения в соответствии с установленным правовым режимом. Так, к охраняемой законом тайне относятся любые сведения, доступ к которым ограничен федеральными законами и указами Президента РФ. К ней, в частности, относится конфиденциальная информация, включая персональные данные, информацию, составляющая профессиональную (адвокатскую, банковскую, аудиторскую и др.), коммерческую, служебную тайну. Особый правовой режим и категорию информации составляет охраняемая законом гостайна. В некоторых случаях для придания информации статуса конфиден-

[9] Habermas, Jürgen (2015). The Theory of Communicative Action: Lifeworld and Systems, a Critique of Functionalist Reason. Vol. 2. John Wiley & Sons.

[10] Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448.

циальной требуется ограничить доступ к сведениям, обладающим коммерческой ценностью, и установить в отношении них режим коммерческой тайны.

В предусмотренных законом случаях установлен запрет на распространение информации (ч. 6 ст. 10 Закона об информации), в т. ч. если эта информация направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, либо за ее распространение предусмотрена уголовная или административная ответственность (напр., административная ответственность за оскорбление, совершенное публично, в том числе с использованием сети Интернет (ч. 2 ст. 5.61 КоАП РФ), незаконное распространение информации о несовершеннолетнем (ч. 3 ст. 13.15 КоАП РФ), за распространение порнографических материалов или предметов среди несовершеннолетних (ч. 2 ст. 242 УК РФ). В п. 1 ч. 5 ст. 15.1 Закона об информации также приведен перечень запрещенной к распространению информации, при выявлении которой в сети Интернет уполномоченные госорганы вправе обращаться для включения страниц сайтов в соответствующий Единый реестр. Запрещается распространять материалы, производимые и (или) распространяемые иностранным агентом в связи с осуществлением им вида деятельности, установленного ст. 4 Закона об иностранном влиянии, а также информацию о таком виде деятельности без указания на то, что эти материалы (информация) произведены и (или) распространены иностранным агентом (ч. 7 ст. 10 Закона об информации, ч. 3 ст. 9 Закона об иностранном влиянии).

Вместе с тем Закон об информации не содержит понятия «информационная среда (сфера)», но дает определение информационной системы как совокупности содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

В ***Доктрине информационной безопасности Российской Федерации***[11] под информационной сферой понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет» (сеть «Интернет»), сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений. Обеспечение информационной безопасности означает осуществление взаимоувязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления.

В то же время ***Основы государственной культурной политики***[12] определяют понятие «информационная среда» как совокупность средств массовой информации, радио- и телевещание, информационно-телекоммуникационная сеть «Интернет» (сеть «Интернет»), распространяемые с их помощью текстовые и визуальные материалы, информацию, а также созданные и создаваемые цифровые архивы, библиотеки, оцифрованные музейные фонды.

Реализация стратегического национального приоритета «Защита традиционных российских духовно-нравственных ценностей, культуры и исторической памяти» предполагает решение ряда задач государственной политики по сохранению и укреплению традиционных ценностей, в т. ч. поддержку проектов, направленных на продвижение традиционных ценностей в информационной среде в соответствии с ***Основами государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей***[13].

Следует особо выделить значение информационного пространства во внешнеполитической сфере. Так, в ***Концепции внешней политики Российской Федерации*** (далее — Концепция)[14] отмечается, что в международных отношениях используется широкий набор противоправных инструментов и методов, включая применение принудительных мер (санкций) в обход Совета Безопасности ООН, провоцирование государственных переворотов, вооруженных конфликтов, угрозы, шантаж, манипулирование сознанием отдельных социальных групп и целых народов, наступательные и подрывные операции в информационном пространстве, допускается использование информационно-коммуникационных технологий в противоправных целях (п. 9). Концепция выделяет среди современных тенденций развития международных отношений повышение роли фактора силы в международных отношениях, использование военной силы в нарушение международного права, освоение космического и информационного пространства в качестве новых сфер военных действий, стирание грани между военными и невоенными средствами межгосударственного противоборства (п. 11). С учетом этого определены сферы национальных интересов Российской Федерации во внешнеполитической сфере, к которым, в частности, относятся развитие безопасного информационного пространства, защита российского общества от деструктивного иностранного информационно-психологического воздействия, формирование объективного восприятия

[11] Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

[12] Указ Президента РФ от 24.12.2014 № 808 (ред. от 25.01.2023) «Об утверждении Основ государственной культурной политики».

[13] Указ Президента РФ от 09.11.2022 № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей».

[14] Указ Президента РФ от 31.03.2023 № 229 «Об утверждении Концепции внешней политики Российской Федерации».

России за рубежом, укрепление ее позиций в мировом информационном пространстве.

Концепция особо оговаривает право Российской Федерации в случае совершения иностранными государствами или их объединениями недружественных действий, представляющих угрозу её суверенитету и территориальной целостности, в том числе связанных с применением ограничительных мер (санкций) политического или экономического характера либо с использованием современных информационно-коммуникационных технологий, принять симметричные и асимметричные меры, необходимые для пресечения таких недружественных действий, а также для предотвращения их повторения в будущем (п. 26).

В целях обеспечения международной информационной безопасности, противодействия угрозам в ее отношении, укрепления российского суверенитета в глобальном информационном пространстве Российская Федерация намерена уделять приоритетное внимание:

(1) укреплению и совершенствованию международно-правового режима предотвращения и разрешения межгосударственных конфликтов и регулирования деятельности в глобальном информационном пространстве;

(2) формированию и совершенствованию международно-правовых основ противодействия использованию информационно-коммуникационных технологий в преступных целях;

(3) обеспечению безопасного и стабильного функционирования и развития информационно-телекоммуникационной сети Интернет на основе равноправного участия государств в управлении данной сетью и недопущению установления иностранного контроля над ее национальными сегментами;

(4) принятию политико-дипломатических и иных мер, направленных на противодействие политике недружественных государств по милитаризации глобального информационного пространства, по использованию информационно-коммуникационных технологий для вмешательства во внутренние дела государств и в военных целях, а также по ограничению доступа других государств к передовым информационно-коммуникационным технологиям и усилению их технологической зависимости.

Стратегия противодействия экстремизму в Российской Федерации[15] констатирует, что наиболее опасным проявлением экстремизма является терроризм, представляющий глобальную угрозу международному миру и безопасности. Современному росту экстремистских и террористических угроз в мире способствует стремительное распространение экстремистской идеологии (включая неонацизм и радикальный национализм), в том числе в информационном пространстве. Информационно-телекоммуникационные сети, включая сеть «Интернет», мультимедийные и онлайн-технологии все шире используются в экстремистских целях — для вербовки новых членов, организации и координации совершения преступлений экстремистской направленности, распространения экстремистской идеологии, а также финансирования экстремистской деятельности, распространения призывов к насильственным действиям. Все чаще применяются различные методы манипулирования общественным мнением и распространения недостоверной информации, в т. ч. дискредитация использования Вооруженных Сил Российской Федерации, исполнения государственными органами Российской Федерации своих полномочий. В целях дестабилизации общественно-политической и социально-экономической обстановки в Российской Федерации специальные службы и организации иностранных государств наращивают деструктивное информационно-психологическое воздействие на население России, прежде всего на молодежь. В связи с этими угрозами основными направлениями государственной политики в сфере противодействия экстремизму предусмотрены, в частности: совершенствование законодательства Российской Федерации в части, касающейся пресечения производства экстремистских материалов и их распространения, в том числе на электронных носителях информации, а также в информационно-телекоммуникационных сетях, включая сеть «Интернет»; противодействие пропаганде идей экстремизма в средствах массовой информации и информационно-телекоммуникационных сетях, включая сеть «Интернет».

В соответствии с Федеральным законом от 26.07.2017 № 187-ФЗ (ред. от 10.07.2023) «О безопасности критической информационной инфраструктуры Российской Федерации» субъекты критической информационной инфраструктуры (государственные органы и учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления), функционирующие в критически важных отраслях здравоохранения, науки, транспорта, связи, энергетики, государственной регистрации прав на недвижимое имущество и сделок с ним, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей, переведены на преимущественное использование доверенных программно-аппаратных комплексов.

В целях обнаружения, предупреждения и ликвидации последствий компьютерных атак на информа-

[15] Указ Президента РФ от 28.12.2024 № 1124 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации».

ционные ресурсы Российской Федерации[16] создана государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, которая включает информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления, находящиеся на территории Российской Федерации, в дипломатических представительствах и консульских учреждениях Российской Федерации.

Глобальная сфера информационной среды, как отмечает ряд авторов [2], не является физически определенным местом, а преодолевает границы, реализуясь в любом физическом или временном измерении. Такая среда создана слиянием совместных сетей компьютеров, информационных систем и телекоммуникационных инфраструктур, а формируемое таким образом цифровое пространство характеризуется анонимностью и доступностью информации, и обозначается в любых пространственных измерениях (на земле, в открытом море, международном воздушном пространстве или космическом пространстве), что допускает его характеристику как общемирового, общего пространства, или res communis omnium (общего блага всех). Это, в свою очередь, позволяет сделать вывод о том, что цифровое пространство полностью не подчинено суверенитету одного государства или группы государств и не защищено от апроприации.

Между тем достаточно показателен подход к регулированию информационной среды в стратегических документах США. Так, в соответствии со Стратегией операций в информационной среде (2023) Министерства обороны США (далее — Стратегия операций МО США)[17] понятие «информационная среда» (*Information Environment*) определено как совокупность социальных, культурных, лингвистических, психологических, технических и физических факторов, которые влияют на то, как люди и автоматизированные системы извлекают смысл из информации, действуют в соответствии с ней и подвергаются ее воздействию, включая отдельных лиц, организации и системы, которые собирают, обрабатывают, распространяют или используют информацию.

Дается определение понятия «информационная сила (мощь)» *(Informational Power)* как способности использовать информацию для достижения целей и получения информационного преимущества. Сущность информационной мощи заключается в способности проявлять свою волю посредством распространения, отрицания использования и сохранения информации для достижения целей. «Операции в информационной среде» (*Operations in the Information Environment*) рассматриваются в документе как военные действия, предполагающие комплексное использование нескольких информационных сил для воздействия на движущие силы поведения путем

информирования аудитории,

оказания влияния на соответствующих иностранных участников,

атаки и использования соответствующей информации участников, информационных сетей и информационных систем

и защиты дружественной информации, информационных сетей и информационных систем.

Стратегия операций МО США направлена на повышение способности министерства планировать, использовать ресурсы и информационную мощь для обеспечения комплексного сдерживания, проведения кампаний и создания устойчивых преимуществ, как описано в Стратегии национальной обороны (NDS). Эффективное применение информационной мощи должно пониматься более широко и целенаправленно включаться во весь спектр стратегий и операций Министерства обороны, мероприятий и инвестиций (OAIS) для поддержки продвижения национальных интересов на дипломатическом уровне, информационные, военные и экономические инструменты национальной мощи в поддержку конкретных целей оборонной политики. Такое изменение обеспечивает способность Министерства обороны позитивно влиять на поведение людей и автоматизированных систем, формируя оперативную среду и укрепляя силу и доверие к Соединенным Штатам. Программа SOIE Министерства обороны направлена на усиление и сбалансирование институциональной и оперативной синергии между операциями военной информационной поддержки, гражданскими вопросами (CA), связями с общественностью (PA), совместными операциями в области электромагнитного спектра (JEMSO), операциями в киберпространстве, космическими операциями, специальными техническими операциями (STO), действиями по дезинформации обороны (DDA), безопасность операций (OPSEC), новые и формирующиеся виды информационной деятельности и другие дисциплины, а также информационные аспекты физической силы.

Это соответствует подходу ***Стратегии международной политики Соединенных Штатов в области киберпространства и цифровых технологий*** (далее — Стратегия политики)[18], заключающемся в перераспределении ответственности за защиту киберпространства между правительством и организациями частного сектора, которые наиболее способны и располагают наилучшими возможностями для снижения рисков, а также перестройке стимулов в пользу долго-

[16] Указ Президента РФ от 22.12.2017 № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

[17] Strategy for Operations in the Information Environment, July, 2023, US Department of Defense. URL: https://media.defense.gov/2023/Nov/17/2003342901/-1/-1/1/2023-department-of-defense-strategy-for-operations-in-the-information-environment.pdf

[18] United States International Cyberspace & Digital Policy Strategy, US Department of State, 2024. URL: https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/

срочных инвестиций в кибербезопасность с помощью дипломатии, партнерских отношений и обмена информацией. В основе Стратегии политики лежат три принципа деятельности Госдепа США:

(i) позитивное видение киберпространства и цифровых технологий, ориентированное на использование преимуществ технологий и основанное на законе в целях безопасного использования цифровых технологий для поиска, получения и распространения информации и идей онлайн, участвуя в жизни свободных, открытых и информированных обществ, а также получения доступа к образовательным и экономическим возможностям для обеспечения инклюзивного экономического роста и надежного получения важнейших услуг и информации от своих правительств.

(ii) интеграция кибербезопасности, устойчивого развития и технологических инноваций, где кибербезопасность, защита данных и киберустойчивость являются предпосылками и факторами, способствующими экономическому росту и созданию здорового гражданского пространства, где граждане могут осуществлять свои права;

(iii) применение комплексного политического подхода, который использует соответствующие инструменты дипломатии и международного государственного управления во всей цифровой экосистеме, которая включает, помимо прочего, аппаратное обеспечение, программное обеспечение, протоколы, технические стандарты, поставщиков, операторов, пользователей и цепочки поставок, охватывающие телекоммуникационные сети, подводные кабели, облачные вычисления, центры обработки данных и инфраструктуру спутниковых сетей, операционные технологии, приложения, веб-платформы и потребительские технологии, а также Интернет вещей (IoT), искусственный интеллект (AI) и другие критически важные и появляющиеся технологии.

Национальная стратегия кибербезопасности США[19] поставила цель создать защищенную, устойчивую цифровую экосистему, в которой атаковать системы дороже, чем защищать их, где конфиденциальная или частная информация надежно защищена и охраняется, и где ни инциденты, ни ошибки не приводят к катастрофическим системным последствиям.

В Стратегии констатируются негативные последствия цифровизации и расширения использования информационного киберпространства. В частности, указывается, что мир вступает в новую фазу углубления цифровой зависимости. Благодаря новым технологиям и все более сложным и взаимозависимым системам кардинальные изменения в предстоящем десятилетии откроют новые возможности для процветания человечества, а также увеличат системные риски, связанные с ненадежностью систем.

Программное обеспечение и системы становятся все более сложными, обеспечивая ценность для компаний и потребителей, но также увеличивая коллективную незащищенность. Слишком часто новые функциональные возможности и технологии внедряются в и без того сложные и хрупкие системы в ущерб безопасности и отказоустойчивости. Широкое внедрение систем ИИ, которые могут действовать неожиданным образом даже для их собственных создателей, повышает сложность и риски, связанные со многими из наших наиболее важных технологических систем.

Цифровые технологии все чаще затрагивают самые чувствительные аспекты нашей жизни, обеспечивая удобство, но также создавая новые, зачастую непредвиденные риски. Пандемия COVID-19 заставила нас все глубже погружаться в цифровой мир. Поскольку наша жизнь тесно связана с потоковой передачей видео и аудио, носимыми устройствами и биометрическими технологиями, объем и конфиденциальность сбора персональных данных растут в геометрической прогрессии. Кража этих данных также растет быстрыми темпами и открывает новые возможности для злоумышленников следить за людьми, манипулировать ими и шантажировать.

Взаимодействие нового поколения стирает границы между цифровым и физическим мирами и подвергает некоторые из наших наиболее важных систем опасности сбоев. Заводы, энергосети, предприятия по очистке воды наряду с другими важными объектами инфраструктуры все чаще отказываются от старых аналоговых систем управления и быстро внедряют цифровые технологии оперативного управления (OT). Передовые беспроводные технологии, Интернет вещей и средства космического базирования, в том числе те, которые позволяют определять местоположение, навигацию и время для гражданских и военных целей, мониторинга окружающей среды и погоды, а также повседневных интернет-операций — от банковского дела до телемедицины — ускорят эту тенденцию, переведя многие из наших основных систем в оперативный режим и повысив эффективность кибератак, разрушительных и влияющих на нашу повседневную жизнь.

Вредоносная кибератакивность эволюционировала от создания помех к шпионажу и краже интеллектуальной собственности, от разрушительных атак на критически важную инфраструктуру до программ-вымогателей и кампаний влияния с использованием киберпространства, направленных на подрыв общественного доверия к основам нашей демократии. Когда-то доступные лишь небольшому числу стран, обладающих достаточными ресурсами, инструменты и сервисы для взлома, включая зарубежное коммерческое шпионское ПО, теперь широко доступны. Эти инструменты и сервисы расширяют возможности стран, которые ранее не имели возможности нанести ущерб интересам

[19] US National Cybersecurity Strategy, March 2023. URL: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

США в киберпространстве, и создают растущую угрозу со стороны организованных преступных синдикатов.

Правительства автократических государств с ревизионистскими намерениями агрессивно используют передовые кибернетические возможности для достижения целей, которые противоречат интересам США и общепринятым международным нормам. Их безрассудное пренебрежение верховенством закона и правами человека в киберпространстве угрожает национальной безопасности и экономическому процветанию США.

Новая Национальная стратегия кибербезопасности предусматривает новый подход к кибербезопасности, основанном на значительных достижениях, которые уже формируют стратегическую среду и цифровую экосистему США. Прежде всего это касается формирования современной и гибкой нормативно-правовой базы кибербезопасности, адаптированной к профилю риска каждого сектора, согласованной для сокращения дублирования, дополняющей сотрудничество государственного и частного секторов и учитывающей стоимость внедрения. *Новые и обновленные правила кибербезопасности должны быть выверены с учетом потребностей национальной и общественной безопасности, а также безопасности отдельных лиц, регулируемых организаций, их сотрудников, клиентов, операций и данных.* Ключевые сектора кибербезопасности — нефте- и газопроводы, авиация и железнодорожный транспорт, системы водоснабжения. Важно создать нормативные акты для обеспечения кибербезопасности критически важных объектов инфраструктуры. Кроме того, эти и другие критически важные сектора зависят от кибербезопасности и устойчивости своих сторонних поставщиков услуг. Облачные услуги позволяют применять более эффективные и экономичные методы обеспечения кибербезопасности в масштабах страны, но они также необходимы для обеспечения операционной устойчивости во многих секторах критической инфраструктуры.

Вместе с тем следует помнить и о том, что в стратегических документах США, таких как Национальная оборонная стратегия США (2022 г.), Федеральный закон США № 115-44 «О противодействии противникам Америки посредством санкций» (*Countering America's Adversaries Through Sanctions Act, CAATSA*) 2017 г., а также в Военной стратегии НАТО (2019 г.), Стратегической концепции НАТО от 29.06.2022 г. Российская Федерация рассматривается в качестве враждебного государства.

В КНР в 2017 г. разработан план более активного участия в мировых делах, дальнейшего экономического и социального развития, укрепления вооруженных сил и уделения более пристального внимания промышленным и технологическим инновациям, где поставлена цель добиться значительного обновления китайской нации к 2049 году. Определена приоритетность экономической стратегии для проведения более активной торговой политики, увеличения инвестиций, кредитования инфраструктурных проектов развивающихся стран, продвигая экономические программы, такие как инициатива «Пояс и путь», а также использования информации и применени асимметричных методов для противостояния своим противникам и доминирования над ними.

В европейских странах усилен контроль со стороны регулирующих органов, направленный на борьбу с незаконным контентом и рисками, связанными с услугами. Закон о цифровых услугах ЕС (*Digital Services Act, DSA*) налагает серьезные обязательства на поставщиков онлайн-посреднических услуг. В Соединенном Королевстве вступает в силу в марте 2025 г. Закон о безопасности в Интернете (*Online Safety Act, OSA*).

В последние годы на первый план вышли специальные законы по безопасности в Интернете, такие как Закон о цифровых услугах в ЕС, Законы о безопасности в Интернете в Великобритании, Австралии, Сингапуре. Защита детей занимает центральное место во многих из этих инициатив, а в Австралии принято законодательство, требующего от платформ социальных сетей препятствовать доступу пользователей моложе 16 лет к их услугам. В других юрисдикциях, например, в Южной Африке, применяется гибридный подход: регулирующий орган разрабатывает отраслевые кодексы поведения и управляет системой рассмотрения жалоб пользователей, а также обладает полномочиями издавать директивы общего применения.

Учитывая разрозненную динамику законотворчества на федеральном уровне и в штатах США, наряду с ограничением Первой поправки к Конституции США о защите свободы слова, ключевое внимание на федеральном уровне уделяется защите детей (проект федерального закона о защите конфиденциальности детей в Интернете еще проходит законодательный процесс). В ожидании принятия всеобъемлющего федерального закона в США частный сектор продолжает саморегулироваться, при этом крупные технологические компании определяют, как действовать в отношении модерации контента, а Верховный суд США вмешивается в случае необходимости.

Как и в случае с другими правовыми режимами, регулирующими трансграничную цифровую экономику, общим для глобальных правил онлайн безопасности является их экстерриториальный характер. Основное внимание в многочисленных нормативно-правовых базах по всему миру уделяется защите пользователей, которые находятся в определённой юрисдикции или выходят в Интернет из неё, независимо от местонахождения сервисов. Это требует от глобальных поставщиков онлайн-услуг ознакомления с множеством правил и их соблюдения. Это особенно сложно, учитывая, что нормативно-правовая база представляет собой разрозненную международную мозаику. В ответ на это и для обеспечения согласованности, правительства и регулирующие органы по всему миру сотрудничают по целому ряду вопросов, включая согласование нормативно-правовой базы и правоприменительной практики

в отношении онлайн-контента. В 2019 году в Заявлении министров юстиции США, Великобритании, Австралии, Канады о противодействии сексуальной эксплуатации и насилию в отношении детей, противодействии насильственному экстремизму и терроризму как в Интернете, так и за его пределами, иностранным боевикам-террористам и шифрованию[20], а затем в 2021 году на саммите G7 правительства Великобритании, Канады, Франции, Германии, Италии, Японии, США и ЕС приняли совместную декларацию[21] о принципах безопасности в Интернете для повышения онлайн-безопасности. С тех пор в феврале 2024 года правительства Австралии и Великобритании подписали совместный меморандум о взаимопонимании для укрепления двустороннего сотрудничества в борьбе с онлайн-угрозами. А в октябре 2024 года правительства США и Великобритании подписали соглашение об онлайн-безопасности, которое предусматривает более тесное сотрудничество, в частности, для обеспечения безопасности детей в Интернете. Хотя глобальное сотрудничество в отношении онлайн-сервисов не является чем-то новым (например, правоохранительные органы по всему миру всегда обменивались информацией о материалах, связанных с эксплуатацией детей), ожидается, что регулирующие органы будут активнее сотрудничать, чтобы решать проблемы быстро развивающейся цифровой экосистемы. Правовые рамки некоторых юрисдикций содержат только ответные требования, такие как уведомления об удалении отдельных фрагментов контента. Однако другие режимы безопасности в Интернете направлены на принятие упреждающих мер поставщиками онлайн-услуг по предотвращению и минимизации онлайн-ущерба (включая Великобританию, Австралию, Сингапур и, возможно, США). В результате наблюдается смещение ответственности за онлайн-ущерб на поставщиков услуг. Усилия по регулированию в этой сфере направлены на охват широкого круга технологических компаний. Законы Австралии, Великобритании, Сингапура, ЕС и других юрисдикций распространяются на широкий спектр онлайн-провайдеров, включая платформы социальных сетей, сервисы электронной коммерции, интернет-провайдеров, а также провайдеров услуг хостинга и хранения данных. В то время как в Великобритании широкое понятие «услуг, предоставляемых пользователям пользователями» (таких как приложения для обмена сообщениями, приложения для знакомств, игры с функциями общения и другие платформы социальных сетей, на которых пользователи взаимодействуют с контентом друг друга) не является отдельной категорией регулируемых субъектов во всех юрисдикциях, в некоторых юрисдикциях, например, в Австралии, это понятие относится к другим категориям регулируемых субъектов. Исторически сложилось так, что законы о безопасности в Интернете были сосредоточены на регулировании незаконного контента в Даркнете, регулируя такие области, как эксплуатация детей и контент, связанный с терроризмом. Однако такие страны, как США, Индонезия, Австралия и Великобритания стремились устранить по крайней мере некоторые аспекты вредоносного (но не обязательно незаконного) контента, включая кибербуллинг, домогательства или материалы с применением насилия. Некоторые страны также запрещают дезинформацию и мистификации с помощью своих режимов безопасности в Интернете. Учитывая потенциальное воздействие вреда, причиняемого онлайн, неудивительно, что несоблюдение требований влечет за собой целый арсенал правоприменительных полномочий для регулирующих органов, главное из которых — налагать штрафы, подобно Директиве ЕС о персональных данных (GDPR) в размере процента от мирового годового дохода за наиболее серьезные нарушения в соответствии с режимами Великобритании (10%) и ЕС (6%), при этом значительные финансовые штрафы также взимаются в других юрисдикциях — Австралия и Сингапур. Хотя в некоторых юрисдикциях также действуют приказы об удалении контента и блокировке доступа к онлайн-сервисам, не соответствующим требованиям, именно потенциальная уголовная ответственность высшего руководства в таких юрисдикциях, как Великобритания и Сингапур, превратила онлайн-безопасность в проблему, требующую решения на уровне совета директоров.

Последние исследования информационной среды[22] позволили сделать ряд выводов, в частности:

(a) наиболее важной характеристикой здоровой информационной среды является наличие достоверной информации;

(b) самой большой угрозой для информационной среды эксперты считают владельцев социальных сетей, за которыми следуют местные власти и иностранные правительства, политики и политические партии;

(c) генеративный ИИ может способствовать сохранению предубеждений, увеличению масштабов преследований и распространения дезинформации.

Информационная среда, таким образом, представляет собой сложно организованную технологическую структуру, которая не идентична информационной системе как совокупности содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. Информационная среда представляет собой адаптивную систему, сложность, структура и границы возможного которой возрастают с появлением новых социальных норм и технологий и которая подвергается негатив-

[20] URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822818/Joint_Meeting_of_FCM_and_Quintet_of_Attorneys_FINAL.pdf

[21] URL: https://www.gov.uk/government/publications/g7-digital-and-technology-ministerial-declaration

[22] Опрос экспертов. Глобальная информационная среда, International Panel on the Information Environment (IPIE), 2024. URL: https://cdn.prod.website-files.com/643ecb10be528d2c1da863cb/673c7f24757d3f3b9e930dee_SFP2024.1%20-%20FINAL-3_RU.pdf

ным влияниям, угрожающим ее целостности, психологическому и физическому здоровью ее участников, даже общественной безопасности и государственному строю. Это создаваемое цифровыми и информационно-коммуникационными технологиями цифровое, не аналоговое пространство, где сходятся человеческое познание, технологии и контент, где информация обрабатывается людьми, ИИ и нейронными сетями и которое включает технологии, используемые для обработки этой информации и доступа к ней, в том числе такие как мобильные телефоны, сеть Интернет и дополненная реальность, а также сопутствующий контент.

Литература

1. Дружилов С.А. Современная информационная среда и экология человека: психологические аспекты // Hygiene & Sanitation (Russian Journal). 2018. № 97. С. 597—602.
2. Моргунова Е.А., Шахназаров Б.А. Право интеллектуальной собственности в условиях развития новых технологий : монография. М. : Норма, ИНФРА-М, 2023. 186 с.
3. Карцхия А.А., Макаренко Г.И. Правовые аспекты современной кибербезопасности и противодействия киберпреступности // Вопросы кибербезопасности. 2023. № 1 (53). С. 28—44. DOI: 10.21681/2311-3456-2023-1-28-44 .
4. A. Wanless, J.N. Shapiro. A CERN Model for Studying the Information Environment, 2022 Carnegie Endowment for International Peace and Princeton University. URL: https://carnegie-production-assets.s3.amazonaws.com/static/files/Wanless_Shapiro_CERN_final.pdf
5. Michel J. Menou, Richard D. Taylor. A "Grand Challenge": Measuring Information Societies. Inf. Soc. 22(5):261–267.
6. Birger Hjørland. Theory and metatheory of information science: A new interpretation. Journal of Documentation, December 1998. URL: https://www.researchgate.net/publication/228717437
7. R. Mathar. Information Theory. URL: https://ti.rwth-aachen.de/teaching/InformationTheory/ws1819/data/InformationTheory.pdf
8. P. Röttger, B. Vedres. The Information Environment and Its Effects on Individuals and Groups. Oxford Internet Institute, University of Oxford, 2020, pp. 2–4. URL: https://royalsociety.org/-/media/policy/projects/online-information-environment/oie-the-information-environment
9. Floridi, Luciano (2010). Information: A Very Short Introduction. Oxford University Press, 2010.
10. Raber, Douglas and John M Budd (2003). Information as sign: semiotics and information science. Journal of Documentation.
11. Habermas, Jürgen (2015). The Theory of Communicative Action: Lifeworld and Systems, a Critique of Functionalist Reason. Vol. 2. John Wiley & Sons.

SECTION:
CONSTITUTIONAL LAW

THE LEGAL ASPECTS OF REGULATING THE INFORMATION ENVIRONMENT

Aleksandr Kartskhiia, *Dr.Sc. (Law), Professor at the Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russian Federation.*
E-mail: arhz50@mail.ru

Keywords: *cyberspace, national security, information technology law, digital law, personal data, cybersecurity, information protection.*

Abstract

Purpose of the study: a legal analysis of the information environment, its content and specific features of formation when using modern information, communication and digital technologies which are reflected in domestic and international law.

Methods used in the study: comparative legal analysis of current Russian and international laws in the field of digital information environment and the practice of using them as well as a formal logical study of the conceptual apparatus, content and structure of the subject under study.

Study findings: specific features of digital information environment and its content are worded, including from the standpoint of cybersecurity and national security in the information sphere. The author considers it natural that the information environment and digital technological space are formed in a new, non-analog physical dimension as a new area of legal regulation which entails forming special laws and special legal regulation in this field.

Research novelty: the concept, qualitative characteristics, and specific features of the content of digital information environment, its elements and extent of its impact on real relations are identified.

References

1. Druzhilov S.A. Sovremennaia informatsionnaia sreda i ekologiia cheloveka: psikhologicheskie aspekty. Hygiene & Sanitation (Russian Journal). 2018. No. 97. Pp. 597–602.
2. Morgunova E.A., Shakhnazarov B.A. Pravo intellektual'noi sobstvennosti v usloviiakh razvitiia novykh tekhnologii : monografiia. M. : Norma, INFRA-M, 2023. 186 pp.
3. Kartskhiia A.A., Makarenko G.I. Pravovye aspekty sovremennoi kiberbezopasnosti i protivodeistviia kiberprestupnosti. Voprosy kiberbezopasnosti. 2023. No. 1 (53). Pp. 28–44. DOI: 10.21681/2311-3456-2023-1-28-44 .
4. A. Wanless, J.N. Shapiro. A CERN Model for Studying the Information Environment, 2022 Carnegie Endowment for International Peace and Princeton University. URL: https://carnegie-production-assets.s3.amazonaws.com/static/files/Wanless_Shapiro_CERN_final.pdf
5. Michel J. Menou, Richard D. Taylor. A "Grand Challenge": Measuring Information Societies. Inf. Soc. 22(5):261–267.
6. Birger Hjørland. Theory and metatheory of information science: A new interpretation. Journal of Documentation, December 1998. URL: https://www.researchgate.net/publication/228717437
7. R. Mathar. Information Theory. URL: https://ti.rwth-aachen.de/teaching/InformationTheory/ws1819/data/InformationTheory.pdf
8. P. Röttger, B. Vedres. The Information Environment and Its Effects on Individuals and Groups. Oxford Internet Institute, University of Oxford, 2020, rr. 2–4. URL: https://royalsociety.org/-/media/policy/projects/online-information-environment/oie-the-information-environment
9. Floridi, Luciano (2010). Information: A Very Short Introduction. Oxford University Press, 2010.
10. Raber, Douglas and John M Budd (2003). Information as sign: semiotics and information science. Journal of Documentation.
11. Habermas, Jürgen (2015). The Theory of Communicative Action: Lifeworld and Systems, a Critique of Functionalist Reason. Vol. 2. John Wiley & Sons.