Научная статья
УДК: 341.492.1, 34.342.95
DOI: 10.17323/tis.2025.24882

Original article

ЭВОЛЮЦИЯ ДОКТРИНАЛЬНЫХ ПОДХОДОВ К РОЛИ МЕДИА В ВОПРОСАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РФ И США В XXI В.

EVOLUTION OF DOCTRINAL APPROACHES TO THE ROLE OF MEDIA IN INFORMATION SECURITY ISSUES IN THE RUSSIAN FEDERATION AND THE USA IN THE 21ST CENTURY

Андрей Вадимович КОЧКИН
Национальный исследовательский университет «Высшая школа экономики», Москва, Российская Федерация,
andrey_kochkin@mail.ru,
ORCID: 0000-0001-7505-2217

Информация об авторе
А.В. Кочкин — аспирант школы коммуникаций и медиа НИУ ВШЭ

Аннотация. Рассмотрена актуальная проблема эволюции роли медиа в доктринах информационной безопасности Российской Федерации и США на современном этапе. Цель — выявить основные трактовки медиа в действующих доктринах безопасности двух стран в контексте исторической трансформации их отношений. Задача исследования — анализ научной литературы и официальных документов России и США, посвященных проблеме обеспечения информационной безопасности, а также систематизация и обобщение официальных позиций двух стран по поводу трактовки роли медиа в системе обеспечения безопасности.

Методология исследования включает в себя общенаучные методы: синтез, анализ, систематизацию, описательный анализ, сопоставление, а также формально-логический метод. В исследовании были также применены такие специальные методы, как историографический анализ научного дискурса изучаемой темы; метод контент-анализа доктринальных документов России и США в сфере информационной безопасности, а также метод качественного анализа полученных данных.

По итогу проведенного исследования было выявлено, что для России характерна оборонительная трактовка медиа в рамках современного понимания информационной безопасности, что выражается в соответствующих официальных документах в области кибербезопасности и защиты данных. В США роль медиа с незначительного компонента национальной безопасности эволюционировала до наступательного оружия в информационных войнах, что также отражено в доктринальных документах данной страны.

Ключевые слова: медиа, национальная безопасность, информационная безопасность, доктрины безопасности, отношения России и США

Для цитирования: *Кочкин А.В.* Эволюция доктринальных подходов к роли медиа в вопросах информационной безопасности в РФ и США в XXI в. // Труды по интеллектуальной собственности (Works on Intellectual Property). 2025. Т. 52, № 1. С. 37–44; DOI: 10.17323/tis.2025.24882

Andrei V. KOCHKIN
National Research University “Higher School of Economics”, Moscow, Russian Federation,
andrey_kochkin@mail.ru,
ORCID: 0000-0001-7505-2217

Information about the author
A.V. Kochkin — postgraduate student at the School of Communication and Media of HSE University

Abstract. The author discusses an actual problem of the media evolution in the doctrines of information security of Russia and the United States at the present stage. The

research goal was to identify the main interpretations of the media in the current security doctrines of the two countries in the context of the historical transformation of their relations. The research objectives were to analyze the scientific literature and official documents of Russia and the United States devoted to the problem of ensuring information security, as well as to systematize and generalize the official positions of the two countries regarding the interpretation of the role of the media in the security system.

The research methodology includes a number of general scientific methods: synthesis, analysis, systematization, descriptive analysis, comparison, as well as the formal-logical method. The study also used such special methods as: historiographical analysis of the scientific discourse of the topic under study; the method of content analysis of doctrinal documents of Russia and the United States in the field of information security, as well as the method of qualitative analysis of the data obtained.

As a result, it was revealed that Russia is characterized by a defensive interpretation of the media within the framework of the modern understanding of information security, which is expressed in the relevant official documents in the field of cybersecurity and data protection. In the United States, the role of the media has evolved from an insignificant component of national security to an offensive weapon in information wars, which is also reflected in the doctrinal documents of this country.

Keywords: media, national security, information security, security doctrines, relations between Russia and the United States

For citation: *Kochkin A.V.* Evolution of Doctrinal Approaches to the Role of Media in Information Security Issues in the Russian Federation and the USA in the 21st Century // Trudi po Intellectualnoy Sobstvennosti (Works on Intellectual Property). 2025. Vol. 52 (1) P. 37–44; DOI: 10.17323/tis.2025.24882

ВВЕДЕНИЕ

Актуальность темы исследования предопределяется тем, что текущие отношения между Россией и Западом, возможно, находятся на самом сложном этапе со времен холодной войны. Более того, современный кризис нельзя свести лишь к политическим разногласиям по отдельным вопросам, поскольку он представляет собой системную проблему, связанную с высокой конкуренцией между державами на международной арене. При этом проблема информационной безопасности является наглядным примером концептуальных разногласий между Россией и США еще с 1990-х годов прошлого столетия [12, с. 17].

Современная ситуация в глобальном информационном пространстве требует четких и международно признанных определений таких ключевых понятий в сфере информационной безопасности, как «информационное пространство», «информационный суверенитет», «медиаугрозы» и тому подобные, что позволило бы разработать нормативно-правовую базу не только в сфере распространения ложной информации, но и в области защиты информационной безопасности населения конкретной страны.

В методическом отношении данная проблематика изучается очень активно, причем научный дискурс включает в себя работы как отечественных, так и зарубежных авторов.

Теоретико-методологические основы исследования составили постулаты и выводы, изложенные в фундаментальных работах таких авторов, как О.И. Калинин, М.В. Приходько [2], М.А. Сизьмин [9], Г.С. Мельник, С.Б. Никонов [10], В.В. Бухарин [11], И.А. Провоторов, М.А. Гайворонский [12], Н.П. Ромашкина [13] и др.

Концептуальные и историко-правовые основы изучения информационной безопасности Российской Федерации представлены в работах таких авторов, как Т.А. Полякова, Г.Г. Камалова [5], В.М. Редкоус [6], А.А. Смирнов [7], А.А. Стрельцов [8] и др.

Также в ходе анализа научной литературы по теме исследования были задействованы материалы Института государства и права Российской академии наук [1].

Методические аспекты исследования были проанализированы на основе работ таких зарубежных авторов, как М.К. Амитав [16], Бао Кхак Куок, Нгуен

Бао То [17], Г. Никипорец-Такигава, Т.В. Бучнев [18], М. Пачкова [19], С. Паудэл [20], Н. Пембецуглу [21], Ф. Семпа [22], Н.Дж. Шэллкросс [23] и др.

В исследовании были также использованы материалы администрации Белого дома [24, 25] и доктринальные документы Российской Федерации в отношении проблем информационной безопасности [3, 14, 15].

Методология исследования включает в себя ряд общенаучных методов: синтез, анализ, систематизация, описательный анализ, сопоставление, а также формально-логический метод. В исследовании были также применены такие специальные методы, как историографический анализ научного дискурса изучаемой темы, метод контент-анализа доктринальных документов России и США в сфере информационной безопасности, а также метод качественного анализа полученных данных.

ТРАКТОВКА РОЛИ МЕДИА В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ДОКТРИНАЛЬНЫХ ДОКУМЕНТАХ РОССИИ И США

В настоящее время эволюция трактовки медиа в контексте информационной безопасности вполне четко отражена в официальных документах России и США.

В нашей стране Доктрина информационной безопасности представляет собой совокупность официальных положений по обеспечению национальной безопасности Российской Федерации в информационной сфере. Правовой основой Доктрины являются Конституция Российской Федерации и соответствующие законы, общепризнанные нормы и принципы международного права, ратифицированные Россией международные договоры, а также указы Президента Российской Федерации и постановления Правительства Российской Федерации [3, 14, 15].

С точки зрения эволюции роли медиа необходимо рассмотреть первоначальный документ — Доктрину национальной безопасности России, утвержденную Указом Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [14], а затем и другие стратегические документы в области обеспечения национальной безопасности.

Доктрина 2016 г. определяет информационное пространство как совокупность интернета и других сетей связи, а также данных информационных технологий, объектов информационных технологий, систем и веб-ресурсов. К ним относятся организации, которые генерируют и обрабатывают данные, разрабатывают и используют соответствующие технологии, обеспечивают информационную безопасность, а также внедряют механизмы регулирования общественных отношений в этой сфере.

При этом в доктринальном списке угроз подчеркивается, что трансграничное распространение информации «все чаще применяется в геополитических целях и военных политических задачах, противоречащих международным законам, а также используется в террористической, экстремистской, криминальной и другой незаконной деятельности, вредящей международной безопасности и стратегической стабильности» [4, с. 54].

В Доктрине 2016 г. указано на то, что без должного учета влияния цифровых технологий на информационную безопасность значительно возрастает риск появления информационных угроз [14]. Одним из основных негативных факторов, оказывающих влияние на состояние информационной безопасности, является то, что несколько иностранных государств усиливают свои информационно-технологические возможности для воздействия на информационную инфраструктуру в военных целях [4, с. 55]. В то же время усиление параметров безопасности происходит среди организаций, занимающихся технической разведкой в отношении российских государственных органов, научных учреждений и оборонно-промышленных предприятий.

В настоящее время действует Стратегия национальной безопасности РФ, утвержденная Указом Президента РФ от 2 июля 2021 г. № 400 [15]. Применительно к исследуемой теме заслуживают интереса указание в числе национальных интересов России «развития безопасного информационного пространства, защиты российского общества от деструктивного информационно-психологического воздействия» (подп. 4 п. 25 Стратегии) и раздел, посвященный информационной безопасности (пп. 48–57 Стратегии) [15].

В рамках реализации Стратегии и других основополагающих документов в сфере национальной безопасности Российская Федерация принимает комплекс мер, направленных на обеспечение защиты информационного суверенитета. К числу такого рода мер относятся: совершенствование законодательной базы, развитие отечественных информационных технологий, укрепление системы кибербезопасности и противодействие внутренним и внешним информационным угрозам. Особое внимание уделяется формированию критической информационной инфраструктуры, способной функционировать в условиях повышенной уязвимости информационной инфраструктуры и обеспечивать устойчивость социально-экономического развития [15].

Направления деятельности, обозначенные в Стратегии 2021 г. в сфере информационной безопасности,

не ограничиваются техническими аспектами. В частности, из текста документа можно заключить, что ряд мер планируется в ближайшее время направить на развитие системы информационной культуры общества и повышение уровня медиаграмотности населения [15].

В Стратегии 2021 г. указано, что в условиях геополитических реалий Россия сталкивается с усилением информационного давления со стороны ряда государств и международных организаций [15]. Такого рода угрозы выражаются в попытках дискредитации внешней и внутренней политики России, распространении ложной информации о социально-экономическом положении страны и т.п. В этой связи защита информационного пространства приобретает стратегическое значение для обеспечения национальной безопасности и сохранения суверенитета Российской Федерации.

При этом роль медиа понимается в Стратегии 2021 г. как обоюдоострый ресурс в информационной войне, а не как полностью подчиненный государству информационный дискурс, над которым есть определенный контроль. В Стратегии 2021 г., однако, не содержится внятного определения термина «информационное пространство Российской Федерации», что существенно затрудняет дальнейшее законодательное регулирование информационных потоков в российских медиаканалах.

Более того, в стратегической перспективе отсутствие четкого определения понятия «информационное пространство» может привести к правовой неопределенности и расширенному толкованию нормативных актов. Такая ситуация, в свою очередь, вполне ожидаемо приведет к произвольному применению законов в отношении СМИ, блогеров и других субъектов информационных правоотношений. В итоге отсутствие четких определений в правовом поле информационной безопасности не только ограничит свободу слова и распространения информации, но также существенно снизит доверие к государственным институтам, ответственным за регулирование сферы СМИ.

Размытость понятия «информационное пространство» в современных доктринальных документах затрудняет также разработку эффективных механизмов защиты от дезинформации и манипулирования информацией, которые представляют собой серьезные угрозы национальной безопасности, что, например, подчеркивается в Стратегии 2021 г. [15].

В этой связи необходимо разработать более четкое и конкретное определение понятия «информационное пространство Российской Федерации», учитывающее как интересы национальной безопасности, так и конституционные свободу слова и права граждан на информацию. Данное определение должно быть закреплено на законодательном уровне и служить руководством для правотворческой и правоприменительной практики, обеспечивая предсказуемость и прозрачность регулирования медиасреды. При этом необходимо выявить ключевые особенности российского информационного пространства, чтобы понять его относительные границы.

Таким образом, в доктринальном дискурсе России медиа представляются в двух ипостасях: 1) как средство трансляции традиционных ценностей внутри страны; 2) как распространитель враждебной внешней информации, в том числе циркулирующей в российском медиапространстве.

Подход к медиа в контексте информационной безопасности в США существенно отличается от восприятия медиа в России. Так, в Национальном стратегическом плане кибербезопасности на 2024 г. указано, что «СМИ являются инструментом проведения наступательных информационных операций, направленных на продвижение демократических ценностей и прав человека во всем мире» [24]. В документе также говорится, что «средства массовой информации могут использоваться для оказания разведывательной поддержки таким операциям за рубежом» [24].

Восприятие медиа как инструмента внешней политики обусловлено, на взгляд автора этой статьи, историческим опытом США и их ролью в продвижении либеральных ценностей после Второй мировой войны. В свою очередь, холодная война укрепила «представление о медиа как о важном поле битвы за умы и сердца», где необходимо активно противостоять пропаганде противника и распространять собственные идеологические установки. Соответственно, американские государственные структуры, включая службы внешней и внутренней разведки, видят в СМИ потенциального союзника в достижении внешнеполитических целей [24].

В России исторически сложилось более скептическое отношение к независимым СМИ, особенно тем, которые получают финансирование из-за рубежа. Упоминание об «иностранных агентах» в законодательстве, регулирующем деятельность медиа, — яркий пример стремления государства очертить границы российского медиапространства и ограничить влияние в нем недружественных зарубежных медиаканалов. СМИ, получающие финансирование из-за рубежа, рассматриваются как потенциальный инструмент влияния со стороны недружественных государств, что превращает их в потенциальные источники дезинформации.

Разница в подходах проявляется и в восприятии проблемы свободы слова. В США это право человека

рассматривается как фундаментальное, гарантирующее возможность открытого выражения различных точек зрения, даже если они противоречат официальной позиции правительства [24].

В России, напротив, участие неподконтрольных государству СМИ в распространении информации должно стать основным вопросом обеспечения национальной безопасности и защиты традиционных ценностей с помощью умеренной и объективной неформализованной цензуры и ограничения доступа к определенной информации конкретных возрастных групп населения.

В результате анализа доктринальных документов можно утверждать, что медийное пространство в США характеризуется большей степенью терпимости к плюрализму и разнообразию мнений, даже при наличии определенных идеологических уклонов. В России же наблюдается тенденция к консолидации медиа по критерию контента, распространяемому в сфере в основном русскоязычного дискурса. В США, напротив, медиасфера была признана приоритетной для государственной поддержки усилий по обеспечению кибербезопасности, что демонстрирует важность медиа в наступательных операциях Пентагона [24].

В частности, Управление по научно-технической политике (OSTP) активно сотрудничает с другими межведомственными рабочими группами для разработки мер по обеспечению безопасности медиапространства, в том числе в области инвестиций для устранения угроз конфиденциальности, в разработке информационных систем и стандартов для обеспечения защиты данных и аналитики больших данных [21, с. 37].

Указанное межведомственное сотрудничество является частью более широкой стратегии администрации Белого дома по защите критически важной инфраструктуры и противодействию дезинформации [25], подрывающей доверие к демократическим институтам и создающей угрозу национальной безопасности США. Особое внимание уделяется разработке алгоритмов и систем, способных выявлять и нейтрализовывать скоординированные кампании по распространению дезинформации, а также предотвращать манипулирование общественным мнением с помощью ботов и фейковых аккаунтов [23, с. 9].

В рамках данных усилий в США также изучаются различные технологические решения, включая использование искусственного интеллекта для автоматизированного анализа данных, использование блокчейна для обеспечения прозрачности и достоверности информации, а также разрабатываются инструменты для проверки фактов и обнаружения фейкового контента.

Параллельно с развитием технологий ведется работа по совершенствованию нормативной базы, регулирующей деятельность интернет-платформ и социальных сетей. В США все большее внимание государства привлекают вопросы ответственности за контент, распространяемый медиа, и необходимости обеспечения прозрачности алгоритмов, определяющих рейтинг контента. Целью этих мер является создание более безопасной и защищенной информационной среды, в которой граждане США могут получать доступ только к достоверной информации и принимать обоснованные решения, базирующиеся на проверенных фактах [24].

Кроме того, Министерство внутренней безопасности США через Агентство по кибербезопасности и защите инфраструктуры сотрудничает с разработчиками открытого исходного кода для рассмотрения подходов к оценке рисков безопасности, следуя рекомендациям Комитета по кибербезопасности [24].

С точки зрения изменившейся роли средств массовой информации за последнее десятилетие можно сказать, что это решающий момент для дальнейшего развития концепции информационной безопасности. В частности, в период с 2014 по 2024 г. Соединенные Штаты разработали свою стратегию и доктрину для защиты киберпространства и создали Киберкомандование и множество других организаций для поддержки национальной медиасистемы. Некоторые эксперты утверждают, что Пентагон был вынужден найти новый смысл, сосредоточившись на том, как киберпространство влияет на глобальные конфликты и баланс сил [22, с. 80].

Все перечисленные идеи выражены в стратегиях киберзащиты 2011, 2015 и 2018 гг., в которых подчеркивается влияние медиа на киберповедение, эффективность сдерживания и риски эскалации конфликтов в рамках информационной войны.

Можно констатировать, что за последнее десятилетие Министерство обороны США добилось больших успехов в развитии своих возможностей в области «наступательных СМИ». Однако неопределенность относительно масштабов наступательных кибероперации Пентагона влияет на доверие к средствам массовой информации в Соединенных Штатах. Поэтому на сегодняшний день ключевой задачей для Министерства обороны США является четкое определение приемлемого поведения в информационном пространстве как для себя, так и для своих потенциальных геополитических конкурентов.

С точки зрения эволюции официального взгляда США на медиа необходимо подчеркнуть, что, в отличие от российского опыта, ключевыми событиями, повлиявшими на развитие концепции СМИ в доктри-

нальных документах по информационной безопасности, стали трагедия 11 сентября 2001 г. и геополитическая ситуация 2014 г. Эти события фактически заставили американское руководство переосмыслить важность информации как инструмента воздействия на потенциального противника. За последние два десятилетия в Соединенных Штатах произошел значительный сдвиг в доктринальном понимании роли медиа в контексте информационной безопасности. Медиаресурсы теперь рассматриваются как инструмент наступательных информационных операций (ИО) в поддержку других компонентов гибридной войны [24]. Иными словами, в настоящее время в вопросах информационной безопасности США придерживаются принципа «Лучшая защита — это нападение», который достаточно полно отражен в действующих доктринальных документах [24, 25]. США эффективно используют СМИ как инструмент информационной войны с 2014 г., а с 2022 г. американцы будут все больше поддерживать свои военные операции в Евразии с помощью медиа.

Напротив, в России основы современной доктрины информационной безопасности сосредоточены на защите от информационных угроз, что означает в большей степени ситуативное реагирование на информационные угрозы. В России активно разрабатываются базовые концепции и определяется точный перечень угроз в сфере информационной безопасности. К сожалению, такая реактивная стратегия может привести к стратегическому отставанию и вероятному поражению в будущих информационных войнах. Для усиления защиты информационного пространства от внешних угроз в виде вредоносного контента необходимо разрешить русскоязычным платформам создавать и размещать собственный контент, а также ввести соответствующий контроль над содержанием данной деятельности. Иными словами, для защиты информационного пространства России от вредоносного влияния недружественных медиа необходим проактивный подход с периодическим мониторингом информационного контента.

ВЫВОДЫ

По результатам исследования можно сформулировать следующие выводы.

1. Концепция международной информационной безопасности, отстаиваемая Россией, подразумевает, что государство как носитель государственного суверенитета играет ключевую роль в управлении информационными ресурсами и контроле над ними. Различия в восприятии роли СМИ, вопросов кибербезопасности и управления интернетом обострили отношения между Россией и Западом. После постоянной критики России со стороны западных СМИ правительство отреагировало ужесточением внутренней информационной политики, что привело к еще большей фрагментации информационного пространства России.

2. В то же время в США принят новый проактивный подход к роли медиа в информационной безопасности: данный ресурс фактически официально признан инструментом информационной поддержки военных операций США. После событий, связанных с международным терроризмом и кибератаками 11 сентября 2001 г., восприятие медиа как наступательного оружия в информационной войне особенно усилилось. Этот сдвиг отражен и в доктринальных документах, определяющих подход США к вопросам национальной безопасности. Пресса и другие средства массовой информации считаются частью «мягкой силы», способной оказывать существенное влияние на политический контекст и политическую повестку в других странах. Такая эволюция роли медиа поднимает вопросы об этических границах использования информационных ресурсов в целях государственной политики, поскольку существующая динамика неизбежно еще сильнее дестабилизирует международную ситуацию.

СПИСОК ИСТОЧНИКОВ

1. Динамика институтов информационной безопасности. Правовые проблемы. Институт государства и права РАН. М.: Канон, 2018. 264 с.
2. *Калинин О.И., Приходько М.В.* Контент-анализ как метод исследования информационной войны (на материале репрезентации китайско-американской торговой войны в медиадискурсе КНР и США) // Вестник Московского государственного лингвистического университета. Гуманитарные науки. 2023. № 12 (880). С. 39–47.
3. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г. // Собрание законодательства Российской Федерации. 2009. № 4. Ст. 445.
4. ОБСЕ. Ежегодный доклад за 2020 г. — URL: http://www.scrf.gov.ru/security/information/document114/ (дата обращения: 16.05.2024).
5. *Полякова Т.А., Камалова Г.Г.* Концептуальные основания развития института доступа к информации в российской федерации при применении цифровых технологий // Мониторинг правоприменения. 2020. № 4 (37). С. 22–28.
6. *Редкоус В.М.* Некоторые вопросы совершенствования правового регулирования в области обеспече-

ния информационной безопасности // Аграрное и земельное право. 2022. № 9 (213). С. 143–147.
7. *Смирнов А.А.* Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского Союза. М.: Юнити-Дана. 2017. 159 с.
8. *Стрельцов А.А.* Обеспечение информационной безопасности России. М.: Букинист, 2002. 296 с.
9. *Сизьмин М.А.* Информационная (информационно-психологическая) безопасность в структуре национальной безопасности (на примере США и России) // Baikal Research Journal. 2014. No 3. S. 20–25.
10. *Мельник Г.С., Никонов С.Б.* Медийный компонент в Доктрине информационной безопасности // Управленческое консультирование. 2018. № 1. С. 18–28.
11. *Бухарин В.В.* Сравнительный анализ нормативной базы по обеспечению информационной безопасности в США и РФ (конец XX — начало XXI в.) // iPolytech Journal. 2016. No 12. S. 4.
12. *Провоторов И.А., Гайворонский М.А.* Основные угрозы информационной безопасности при использовании социальных медиаресурсов в сети интернета // Экономика и социум. 2018. № 3 (46). С. 16–28.
13. *Ромашкина Н.П.* Вооружения без контроля: современные угрозы международной информационной безопасности // ИМЭМО РАН. 2018. № 2 (55). С. 23–49.
14. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». — URL: https://base.garant.ru/71556224/ (дата обращения: 12.02.2024).
15. Указ Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства Российской Федерации от 5 июля 2021 г. № 27 (часть II) ст. 5351.
16. *Amitav M.K.* Technology and Security in the 21st Century. SIPRI Research Report. 2023. Vol. 2. P. 6–18.
17. *Bao Khac Quoc, Nguyen Bao To.* US-Russia geopolitical risk and corporate cybersecurity risk: Evidence from 10-K reports // Computer Science. 2021. Vol. 4. P. 58–69.
18. *Nikiporets-Takigawa G., Buchnevb T.V.* Methodological Problems Concerning Concept's Formation of the National Cybersecurity in the Russian Federation // Humanities and Social Sciences Bulletin of the Financial University. 2022. Vol. 12 (1). P. 70–74.
19. Pačková Pavlíkova, M. Russian Active Measures in Cyberspace through the Lens of Security Sectors // Politické vedy. 2023. Vol. 25(4). P. 55–61.
20. *Paudel S.* A Study on Russian Cyberwarfare Capabilities and Approach towards Cybersecurity. — URL: https://www.researchgate.net/publication/361420683_A_Study_on_Russian_Cyberwarfare_Capabilities_and_Approach_towards_Cybersecurity (accessed: 16.05.2024).
21. *Pembecioglu N.* Pandect Law in media culture: Snowpiercer analysis // Interciencia. 2023. Vol. 4. P. 34–59.
22. *Sempa F.P.* US security strategies from the Cold War to the 21st Century. 2nd Edition. 2022. P. 78–112.
23. *Shallcross N.J.* Social Media and Information Operations in the 21st Century // Journal of Information Warfare. 2017. Vol. 16. № 1. P. 8–10.
24. United States government. Office of Security. — URL: https://www.commerce.gov/osy/programs/information-security (accessed: 12.02.2024).
25. White House. National Cybersecurity Strategy Implementation Plan. URL: https://www.whitehouse.gov/wp-content/uploads/2024/05/National-Cybersecurity-Strategy-Implementation-Plan-Version-2.pdf (accessed: 12.02.2024).

REFERENCES

1. Dinamika institutov informatsionnoy bezopasnosti. Pravovyye problemy. Institut gosudarstva i prava RAN. M.: Kanon. 2018. 264 s.
2. *Kalinin O.I., Prikhod'ko M.V.* Kontent-analiz kak metod izucheniya informatsionnoy voyny (na materiale reprezentatsii kitaysko-amerikanskoy torgovoy voyny v mediadiskurse Kitaya i SSHA) // Vestnik Moskovskogo gosudarstvennogo lingvisticheskogo universiteta. Gumanitarnyye nauki. 2023. No 12 (880). S. 39-47.
3. *Konstitutsiya Rossiyskoy Federatsii* (prinyata vsenarodnym golosovaniyem 12 dekabrya 1993 g. // Sobraniye zakonodatel'stva Rossiyskoy Federatsii. 2009. No 4. St. 445.
4. OBSE. Yezhegodnyy doklad 2020. — URL: http://www.scrf.gov.ru/security/information/document114/ (data obrashcheniya: 16.05.2024).
5. *Polyakova T.A., Kamalova G.G.* Kontseptual'nyye osnovaniya razvitiya instituta dostupa k informatsii v rossiyskoy federatsii pri primenenii tsifrovykh tekhnologiy // Monitoring pravoprimeneniya. 2020. No 4 (37). S. 22–28.
6. *Redkous V.M.* Nekotoryye voprosy sovershenstvovaniya pravovogo regulirovaniya v oblasti obespecheniya informatsionnoy bezopasnosti // Agrarnoye i zemel'noye pravo. 2022. No 9 (213). S. 143–147.
7. *Smirnov A.A.* Obespecheniye informatsionnoy bezopasnosti v usloviyakh virtualizatsii obshchestva. Opyt Yevropeyskogo Soyuza. M.: Yuniti-Dana. 2017. 159 s.

8. *Strel'tsov A.A.* Obespecheniye informatsionnoy bezopasnosti Rossii. M.: Bukinist. 2002. 296 s.
9. *Siz'min M.A.* Informatsionnaya (informatsionno-psikhologicheskaya) bezopasnost' v strukture natsional'noy bezopasnosti (na primere SSHA i Rossii) // Baykal'skiy nauchnyy zhurnal. 2014. N0 3. S. 20–25.
10. *Mel'nik G.S., Nikonov S.B.* Mediakomponenta v doktrine informatsionnoy bezopasnosti // Upravlencheskoye konsul'tirovaniye. 2018. No 1. S. 18–28.
11. *Bukharin V.V.* Sravnitel'nyy analiz normativno-pravovoy bazy obespecheniya informatsionnoy bezopasnosti v SSHA i Rossiyskoy Federatsii (konets XX — nachalo XXI v.) // iPolytech Journal. 2016. No 12. S. 4.
12. *Provotorov I.A., Gayvoronskiy M.A.* Osnovnyye ugrozy informatsionnoy bezopasnosti pri ispol'zovanii resursov sotsial'nykh setey v seti Internet // Ekonomika i obshchestvo. 2018. No 3 (46). S. 16–28.
13. *Romashkina N.P.* Oruzhiye bez kontrolya: sovremennyye ugrozy mezhdunarodnoy informatsionnoy bezopasnosti // IMEMO RAN. 2018. No 2 (55). S. 23–49.
14. Ukaz Prezidenta Rossiyskoy Federatsii ot 5 dekabrya 2016 No 646 "Ob utverzhdenii Doktriny informatsionnoy bezopasnosti Rossiyskoy Federatsii". — URL: https://base.garant.ru/71556224/ (data obrashcheniya: 12.02.2024).
15. Ukaz Prezidenta RF ot 2 iyulya 2021 g. No 400 "O Strategii natsional'noy bezopasnosti Rossiyskoy Federatsii" // Sobraniye zakonodatel'stva Rossiyskoy Federatsii ot 5 iyulya 2021 g. No 27 (ch. II). St. 5351.
16. *Amitav M.K.* Technology and Security in the 21st Century // SIPRI Research Report. 2023. Vol. 2. P. 6–18.
17. Bao Khac Quoc, Nguyen Bao To. US-Russia geopolitical risk and corporate cybersecurity risk: Evidence from 10-K reports // Computer Science. 2021. Vol. 4. P. 58–69.
18. *Nikiporets-Takigawa G., Buchnevb T.V.* Methodological Problems Concerning Concept's Formation of the National Cybersecurity in the Russian Federation // Humanities and Social Sciences Bulletin of the Financial University. 2022. Vol. 12 (1). P. 70–74.
19. *Pačková Pavlíkova M.* Russian Active Measures in Cyberspace through the Lens of Security Sectors // Politické vedy. 2023. Vol. 25(4). P. 55–61.
20. *Paudel S.* A Study on Russian Cyberwarfare Capabilities and Approach towards Cybersecurity. — URL: https://www.researchgate.net/publication/361420683_A_Study_on_Russian_Cyberwarfare_Capabilities_and_Approach_towards_Cybersecurity (accessed: 16.05.2024).
21. *Pembecioglu N.* Pandect Law in media culture: Snowpiercer analysis. Interciencia. 2023. Vol. 4. P. 34–59.
22. *Sempa F.P.* US security strategies from the Cold War to the 21st Century. 2nd Edition. 2022. P. 78–112.
23. *Shallcross N.J.* Social Media and Information Operations in the 21st Century // Journal of Information Warfare. 2017. Vol. 16. No 1. P. 8–10.
24. United States government. Office of Security. — URL: https://www.commerce.gov/osy/programs/information-security (accessed: 12.02.2024).
25. White House. National Cybersecurity Strategy Implementation Plan. — URL: https://www.whitehouse.gov/wp-content/uploads/2024/05/National-Cybersecurity-Strategy-Implementation-Plan-Version-2.pdf (accessed: 12.02.2024).