Вестник МГИМО-Университета. 2025. 18(5). С. 80-100
DOI 10.24833/2071-8160-2022-olf6

ИССЛЕДОВАТЕЛЬСКИЕ СТАТЬИ

Check for updates

Формирование международного режима в области информационной безопасности

С.В. Шитьков[1], Т.А. Полякова[2], А.А. Смирнов[2]

[1] Московский государственный институт международных отношений (университет) МИД России
[2] Институт государства и права Российской академии наук

В статье исследуются актуальные вопросы формирования международного режима в области обеспечения международной информационной безопасности в условиях геополитических трансформаций и турбулентности. В качестве теоретико-методологической базы исследования была использована теория международных режимов, разрабатываемая российскими и зарубежными исследователями.

Отталкиваясь от классического определения международного режима, авторы фиксируют внимание на нормах и принципах в области международной информационной безопасности. Нормы и принципы в области международной информационной безопасности как правила ответственного поведения в глобальном информационном пространстве были впервые предложены Россией и её партнёрами по ШОС в 2011 году в рамках дискуссии Генеральной Ассамблеи ООН. Однако, российские инициативы встретили сопротивление со стороны США, следствием чего стала фрагментация существующего нормативного режима в области международной информационной безопасности. В настоящее время соответствующие нормы и принципы, в основе которых лежат основополагающие принципы международного права, зафиксированные в Уставе ООН, представлены в резолюциях ГА ООН, а также закреплены в докладах Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности.

Зафиксированные в документах нормы не носят обязательного характера, однако вносят важный вклад в обеспечение международной стабильности за счёт структурирования ожиданий различных акторов в области информационной безопасности. Однако, отсутствие формального закрепления и институционализации данных норм в рамках международных договоров, снижает их легитимность.

Ключевые слова: международная информационная безопасность, информационные угрозы, международный режим, нормы ответственного поведения государств в ИКТ-среде

УДК 327:341.231.14:004.056"20"
Поступила в редакцию: 05.09.2022 г.
Принята к публикации: 11.12.2022 г.

Современная цифровая революция затрагивает все сферы жизни общества и государства. Как отмечает Н.А. Цветкова, международные отношения как система становится цифровой, при этом в ней формируются различные кластеры или подсистемы, в числе которых – система отношений по вопросам обеспечения информационной безопасности (Цветкова 2022). Можно согласиться с тем, что цифровые технологии для современных международных отношений играют ту же роль, что и ядерные технологии для второй половины XX века. Цифровое пространство является полем геополитических противоречий, в силу того доступ к передовым цифровым технологиям определяет возможности государства на международной арене и спектр доступных внешнеполитических возможностей, а также уровень экономического развития. При этом, как отмечают исследователи, лидерство в области цифровых технологий является залогом лидерства в мировой политике XXI века. Современные международные отношения перешли в эпоху, когда взаимодействие между странами, прокси-группами или пользователями в киберпространстве необходимо регулировать цифровыми правилами в духе Ялтинско-Потсдамских соглашений и проведения красных линий в интернете (Цветкова, 2022). Прежде всего, такие правила нужны для обеспечения стабильного развития информационной среды, что особенно востребовано в современных условиях роста числа и масштабов цифровых угроз, большая часть из которых носит траснграничный характер.

Наибольшую опасность сегодня носит военно-политическое измерение угроз информационной безопасности. Наметилась гонка цифровых вооружений, в которую вовлекается все большее число государств. Происходящие сегодня события в мире свидетельствуют о тенденции усиления информационного противоборства между ведущими державами. Государства все чаще используют информационно-коммуникационные технологии (далее – ИКТ) в качестве средств деструктивного воздействия на информационную инфраструктуру и общественное сознание. Особую опасность представляют атаки на объекты критической информационной инфраструктуры.

В настоящее время интенсивность информационного противостояния достигла пиковых значений после начала российской специальной военной операции на Украине. Так, глава киберкомандования США генерал Пол Накасоне в начале июня 2022 года прямо заявил о проведении серии наступательных кибероперациий в поддержку Украины[1]. Это информация в последующем была подтверждена белым домом[2]. Методы деструктивного информационного воздействия играют ключевую роль в современных гибридных войнах.

---

[1] Martin A. US military hackers conducting offensive operations in support of Ukraine, says head of Cyber Command Sky News. 1 June 2022. URL: https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139 (дата обращения: 02.06.2022).

[2] Фурсеев И. Белый дом подтвердил проведение «кибероперациий» против России // РБК. 2 июня 2022 г. URL: https://www.rbc.ru/politics/02/06/2022/6297d5699a7947622ed04206 (дата обращения: 02.06.2022).

Потенциал цифровых технологий все активнее применяется террористическими и экстремистскими организациями, преступниками и иными злоумышленниками для достижения своих противоправных целей. Особый размах приобрело мошенничество с использованием ИКТ, с которыми сталкивается большинство пользователей мобильной связи и сети «Интернет». Данные угрозы также носят трансграничный характер и затрагивают все государства.

Согласно оценкам учёных, так же, как и оценкам международных организаций, значимость угроз в цифровой среде сопоставима с проблемами цифровой стабильности. Цифровые вызовы актуализируют формирование международных инструментов, которые обеспечили бы предсказуемость в данной области, снизили бы издержки от взаимного недоверия ведущих игроков, а также сформировали бы общие ожидания от международного взаимодействия. Как отмечает, Министр иностранных дел Российской Федерации С.В. Лавров, Россия выступает последовательным сторонником консолидации действий государств для эффективного решения данной проблемы (Крустких 2021: 13). Именно Россия почти четверть века назад стала инициатором вынесения на уровень Организации Объединённых Наций темы противодействия угрозам в информационном пространстве и является последовательным приверженцем такой позиции и продвижения прогрессивных инициатив в этой сфере. Согласно Основам государственной политики в сфере международной информационной безопасности от 2021 года, Россия ставит своей задачей формирование международного режима в области обеспечения информационной безопасности. Проблемы формирования международного режима в области информационной безопасности имеют междисциплинарный характер и включают в себя «блок теоретико-методологических правовых вопросов применения норм, правил и принципов ответственного поведения государств, призванных способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной информационно-коммуникационной среды» (Полякова Шинкарецкая 2020: 138). В настоящей работе с позиций теории международных режимов будет изучены нормативные основания международного режима в области информационной безопасности, дана оценка актуальных тенденций развития международного режима.

Важность, значимость и востребованность выработки нормативных оснований регулирования информационной сферы и обеспечения её безопасного развития признается практически всеми государствами. Значимость выработки, закрепления и имплементации норм ответственного поведения зафиксирована в итоговых документах ГПЭ и РГОС ООН, при этом зафиксирована необходимость выработки универсальных норм для всех государств. Однако, в научной литературе и экспертных оценках представлены также рекомендации по выработке не инклюзивных, а эксклюзивных норм, в том числе для государств-союзников или норм для великих держав, а также норм для отдельных областей, как например, контроль экспорта цифровых технологий или защита данных.

Теория международных режимов как инструмент анализа сотрудничества

Для более глубокого анализа представляется целесообразным обратиться к основным положениям теории международных режимов, которая представляет собой аналитический инструмент, направленный на изучение сотрудничества в отдельных областях мировой политики, к числу которых можно отнести и международную информационную безопасность. На сегодняшний день теория режимов представляет собой одно из наиболее устойчивых теоретических направлений исследования международного сотрудничества, сохраняя своё влияние вот уже в течение трех десятилетий. Среди наиболее авторитетных авторов, занимающихся исследованиями международных режимов, могут быть названы Р. Аксельрод (Axelrod 1984: 224), (Axelrod, Keohane 1993), Кохейн (Axelrod, Keohane 1993), С. Краснер (Ruggie, Krasner 1983: 195-223), Ф. Краточвил (Kratochwil, Ruggie 1986: 753-775), Д. Миршаймер (Mearsheimer 1994: 5-49), Д. Най (Keohane, Nye 1989: 273), Д. Рагги (Ruggie 1983: 195-233), Э. Хаас (Haas 1992: 1-35), О. Янг (Levy, Young, Zuern 1995: 267-330). В российской науке проблемами международных режимов безопасности занимается проф. Петровский В.Е. (Петровский 1998). Систематизацией различных течений в рамках теории режимов занимался коллективы авторов под руководством А.Хасенклевера, который в своей работе выделил три направления в рамках данной теории: реалистское, либеральное и конструктивистское (Hasenclever, Mayer, Rittberger 2000: 3-33).

Согласно классическому определению, предложенному С. Краснером в 1983 году, «Международный режим — это набор явных или неявных принципов, норм, правил и процедур принятия решений, в отношении которых сходятся ожидания акторов в определенной области международных отношений». Режимы могут быть формальными и неформальными, сильно и слабо институционализированными. В основе любого режима лежат нормы и принципы, которые формируют поведение его участников.

Создание международного режима предполагает достижение согласия относительно его базовых элементов – принципов и норм, а затем правил и процедур принятия решений. Конкретизируя каждый из компонентов международных режимов, Краснер пишет: «Принципы отражают понимание причинности, фактов и обязательности (честности). Нормы являются стандартами поведения, выраженными в понятиях прав и обязанностей. Правила являются конкретными указаниями к действию. Процедуры принятия решений отражают преобладающую практику совершения и исполнения коллективного выбора»[3]. Причём, если принципы и нормы представляют собой собственно

[3] Ibidem.

характеристики режима, то правила и процедуры принятия решений могут меняться в рамках одного режима.

Р. Кохейн предпринял попытку конкретизировать связи между режимами и институтами, в очередной раз пересмотрев своё же собственное определение международного режима. «*Согласованные правила*», по его мнению, следует понимать «исключительно в формальных определениях (однозначно сформулированные правила, принимаемые более чем одним государством)», а международный режим, в таком случае, возникает после того, как «государства признают законность данных соглашений». В то же время перечень правил, по мнению Кохейна, не обязательно должен быть формально оформленным – достаточно, чтобы вовлечённые государства признавали за этими правилами право на существование[4].

О. Янг, исследуя эволюцию международного сотрудничества, выделил три стадии развития международных режимов: определение повестки дня, переговорная стадия и стадия имплементации достигнутых соглашений. Именно нормы и принципы, которые являются основой любого режима, определяются на стадии определения повестки дня. Как правило, данная стадия носит наиболее длительный характер.

Теоретики признают возможность и необходимости формирования режимов в сфере безопасности. В качестве примера устойчивых и эффективных международных режимов приводят режим контроля над ядерными вооружениями. Как представляется, для понимания специфики международного сотрудничества в сфере информационной безопасности может быть использован опыт из других сфер. При этом стратегической целью является гарантирование суверенитета государств в информационном пространстве (Бойко 2018: 26). Однако, если мы говорим о режимах и сотрудничестве в сфере безопасности, важно чёткое определение соответствующих норм и правил, которые формируют ценностные основания режима, а также их институциональное закрепление. В военно-политической проблематике цена ошибки очень высока, поэтому крайне важной представляется детальная спецификация и строгая формализация правил и процедур, лежащих в основе международного режима.

При этом режимы могут эволюционировать и развиваться. Как показывает Д. Най, обучение и опыт играли существенную роль в формировании режима контроля над ядерными вооружениями. Согласно подходу О. Янга, все режимы в ходе формирования проходят несколько стадий: определение по-

[4] «…agreements in purely formal terms (explicit rules agreed upon by more than one state) and to consider regimes as arising when states recognize these agreements as having continuing validity.... [A] set of rules need not be "effective" to qualify as a regime, but it must be recognized as continuing to exist» Цит. по Hasenclever, Mayer, Rittberger (1996) Указ. соч. С. 183

вестки дня, переговорная стадия, имплементация достигнутых соглашений (Зиновьева, 2017).

Подходы к определению международной информационной безопасности

В условиях ментального передела мира необходимо осмысление новой реальности и задач МИБ. Важно также дать точную дефиницию понятия «международная информационная безопасность». В Основах государственной политики Российской Федерации в области международной информационной безопасности[5] (далее – Основы государственной политики в области МИБ) под международной информационной безопасностью понимается «такое состояние глобального информационного пространства, при котором на основе общепризнанных принципов и норм международного права и на условиях равноправного партнёрства обеспечивается поддержание международного мира, безопасности и стабильности» (п. 6).

Как отмечается в докладе экспертов МГИМО, предложенный и продвигаемый Российской Федерацией термин МИБ подразумевает наличие не только технических, но и политико-идеологических угроз в данной области», что не коррелируется с западной концепцией кибербезопасности, акцентирующей внимание на технологическом измерении информационных угроз (Крутских, Зиновьева 2021: 6).

Вместе с тем представляется, что различие в подходах здесь имеет принципиальный характер. В России в основополагающих документах стратегического планирования в области национальной безопасности информационная безопасность рассматривается комплексно, как состояние защищенности от информационных угроз широкого спектра, как информационно-технических, так и информационно-психологических. Полагаем, что особенно четко данный подход зафиксирован в Стратегии национальной безопасности Российской Федерации 2021 года[6], где в содержание национальных интересов включена защита российского общества от деструктивного информационно-психологического воздействия (Смирнов 2021: 222-228).

---

[5] Указ Президента Российской Федерации от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» // СЗ РФ. 2021. № 16. Ст. 2746.

[6] Стратегия национальной безопасности Российской Федерации (утв. Указом Президента РФ от 2 июля 2021 г. № 400) // Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/Document/View/0001202107030001 (дата обращения: 08.07.2021).

Причина игнорирования США и иными западными державами блока информационно-психологических угроз связана вовсе не с недооценкой его значимости. Напротив, именно в Соединенных Штатах создана наиболее мощная и эффективная в мире система пропаганды и психологической войны, возможности которой они активно задействуют в продвижении своих национальных интересов в глобальном масштабе. Эта система во многом базируется на возможностях американской индустрии развлечений (Голливуд и пр.) и средств массовой информации, а в последнее время также – американских социальных сетей и цифровых сервисов. Однако развивая и многократно апробируя свою систему пропагандистского воздействия для достижения целей национальной политики, США не хотят для себя никаких ограничений в глобальном информационном пространстве. По этой причине они всячески уклоняются от подписания каких-либо юридически обязывающих документов в данной области. Однако, в условиях растущей уязвимости США в цифровой сфере, в экспертном сообществе США приходит понимание того, что технологическую и информационно-психологическую составляющие безопасности в цифровой среде разделять уже нецелесообразно (Seagal 2022).

В этой связи комплексный подход к дефиниции МИБ, сочетающий технические и психологические аспекты, который продвигается Россией и поддерживается многими странами, с высокой долей вероятности будет заложен в основу формирования международного режима в области информационной безопасности.

В трудах российских исследователей, равно как и в официальных документах, МИБ рассматривается в контексте триады информационных угроз, включающей угрозы использования ИКТ в военно-политических, террористических и криминальных целях (Зиновьева 2021: 37). В последнее время начинают обозначаться и другие угрозы МИБ, например применение ИКТ в экстремистских целях и вмешательства во внутренние дела государства, совершения компьютерных атак на критическую информационную инфраструктуру и др. (пп. г-е п. 8 Основ государственной политики в области МИБ), однако базовая триада угроз МИБ по-прежнему остается стрежневой. При этом во всех основных угрозах МИБ имплицитно присутствуют как технические, так и психологические составляющие, обоснованные нами выше.

Подход Российской Федерации формированию международного режима в области информационной безопасности

В Основах государственной политики в области МИБ в качестве цели государственной политики России в данной сфере выделено «содействие установлению международно-правового режима, при котором создаются условия для предотвращения (урегулирования) межгосударственных конфликтов в глобальном информационном пространстве, а также для формирования с учетом

национальных интересов Российской Федерации системы обеспечения международной информационной безопасности» (п. 9)[7].

Достижение данной цели осуществляется путем решения задач развития международного сотрудничества России на глобальном, региональном, многостороннем и двустороннем уровнях по вопросам формирования системы обеспечения МИБ, а также противодействия основным угрозам МИБ.

Кроме того, стратегические задачи российской государственной политики Российской Федерации в рассматриваемой области вытекают из положений пункта 5 Основ государственной политики в области МИБ и включают в себя:

продвижение российских подходов к развитию системы обеспечения МИБ на международной арене и российских инициатив в данной области;

содействие формированию международно-правовых механизмов предотвращения (урегулирования) конфликтов государств в глобальном информационном пространстве;

организацию межведомственного взаимодействия при реализации государственной политики в области МИБ.

В рамках реализации указанных стратегических задач в Основах государственной политики в области МИБ закреплены основные направления реализации государственной политики в данной сфере, и их ключевой составляющей является системное развитие правового обеспечения МИБ. Среди указанных направлений несомненными приоритетами являются содействие принятию странами-участницами ООН Конвенции об обеспечении МИБ и выработке новых принципов и норм международного права, регламентирующих поведение государств в глобальном информационном пространстве, а также заключение и реализация международно-правовых и иных договоренностей между Россией и иностранными государствами о сотрудничестве в сфере МИБ.

Необходимо отметить, что для реализации государственной политики Российской Федерации в области МИБ необходимым шагом организационно-правового характера стало создание в структуре МИД России Департамента международной информационной безопасности, который отличает многоуровневая специализация, предполагающая анализ проблем обеспечения МИБ в международно-правовом, военном-политическом и экономическом аспектах, а также в глобальных и региональных координатах внешней политики Российской Федерации (Крутских, Зиновьева 2021: 32).

Важную роль в рассматриваемой сфере также играют институты гражданского общества. В России в 2018 году создана Национальная Ассоциация международной информационной безопасности (НАМИБ), главная задача которой

[7] Указ Президента Российской Федерации от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» // СЗ РФ. 2021. № 16. Ст. 2746.

состоит в содействии реализации государственной политики в области МИБ[8]. Летом 2022 года НАМИБ получила аккредитацию при Рабочей группе открытого состава по безопасности и использованию информационно-коммуникационных технологий (РГОС), что значительно расширяет возможности ассоциации по продвижению российской позиции по МИБ на международной арене.

Эволюция международного сотрудничества в области международной информационной безопасности

В современных условиях мирового кризиса особенно очевидно, что уровень развития международно-правового регулирования сферы МИБ несмотря на её значимость, остаётся явно недостаточным, не системным. На современном этапе не сложилось единого универсального режима международной информационной безопасности, как формального, так и неформального.

На универсальном уровне до настоящего времени не выработан международный договор, регламентирующий данную сферу отношений. Российской Федерацией ещё в 2011 году в Екатеринбурге была представлена концепция Конвенции об обеспечении международной информационной безопасности. Через 10 лет в 2021 году был подготовлен её обновлённый вариант[9]. Однако она не получила поддержки, прежде всего из-за позиции США и стран Запада. Собственно, противоречия глобальных держав до настоящего времени являются главным препятствием для развития международного права в области МИБ.

Вместе с тем и несмотря на обострения, отсутствие универсального международного договора в области МИБ отнюдь не означает, что сегодня образовался полный вакуум международно-правового регулирования вопросов безопасности в информационном пространстве.

Во-первых, начиная с 1998 г. Генеральной Ассамблеей ООН был принят целый ряд резолюций под названием «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности», в которых выделены основные угрозы МИБ и намечены пути развития международного сотрудничества государств в данной области. К сожалению, указанные резолюции не носят юридически обязывающего характера.

Во-вторых, в 2000-е годы был принят ряд международных документов политического характера по вопросам развития информационного общества,

---

[8] Устав Национальной Ассоциации международной информационной безопасности (утв. 10 апреля 2018 г.) // Национальная Ассоциация международной информационной безопасности URL: https://namib.online/wp-content/uploads/2018/11/Ustav_NAMIB.pdf (дата обращения: 08.06.2022).

[9] Концепция Конвенции ООН об обеспечении международной информационной безопасности // Совет Безопасности Российской Федерации. URL: http://www.scrf.gov.ru/security/information/document112/ (дата обращения: 20.05.2022).

в которых было уделено значительное внимание вопросам безопасности использования ИКТ[10].

В-третьих, вопросы противодействия отдельным угрозам МИБ отчасти регламентированы в универсальных и региональных международных договорах в области СМИ и Интернета, борьбы с преступностью и терроризмом[11].

В-четвертых, в рамках ООН утверждены добровольные и необязательные нормы ответственного поведения государств в ИКТ-среде (они будут подробнее рассмотрены ниже).

В-пятых, на региональном и двустороннем уровне принят ряд обязательных международных договоров в области МИБ[12].

Кроме того, в последние годы наметились перспективы принятия универсального международного договора в области борьбы с преступлениями в сфере ИКТ – одной из составляющих триады основных угроз МИБ. В 2019 г. по инициативе нашей страны создан специальный комитет ООН в целях подготовки всеобъемлющей международной конвенции в данной области. В 2021 г. Российская Федерации внесла в данный комитет проект Конвенции ООН о противодействии использованию информационно-коммуникационных технологий в преступных целях[13]. Работу над данным проектом планируется завершить в 2023 году.

Однако перечисленные выше достижения на пути продвижения российских инициатив в области нормативного регулирования отдельных аспектов и направлений обеспечения МИБ ни в коей мере не отменяют необходимости принятия универсального международного договора в области МИБ, поскольку этот документ должен иметь юридически обязательный, императивный характер. Именно универсальный договор должен стать основной системы правового обеспечения МИБ и каркасом для развития практически всех базовых направлений противодействия угрозам МИБ. Главной задачей такого договора является закрепление мер, которые бы предотвратили использование ИКТ

---

[10] Окинавская хартия Глобального информационного общества от 22 июля 2000 г.; Женевская «Декларация принципов: построение информационного общества – глобальная задача в новом тысячелетии» от 12 декабря 2003 г.; Тунисская программа для информационного общества от 15 ноября 2005 г.

[11] Факультативный протокол к Конвенции о правах ребёнка, касающемся торговли детьми, детской проституции и детской порнографии, от 25 мая 2000 г.; Конвенция о киберпреступности от 23 ноября 2001 г. и протоколы к ней; Конвенция Совета Европы о защите детей от сексуальной эксплуатации и сексуальных злоупотреблений от 25 октября 2007 г.; Договоре о сотрудничестве государств – участников СНГ в борьбе с терроризмом от 4 июня 1999 г., Шанхайская Конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом от 15 июня 2001 г.; Конвенция ШОС по противодействию экстремизму от 9 июня 2017 г.

[12] Соглашение между правительствами государств – членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 г.; Соглашение о сотрудничестве государств – членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности от 30 ноября 2017 г.

[13] О внесении в Спецкомитет ООН российского проекта универсальной международной конвенции по противодействию использованию информационно-коммуникационных технологий в преступных целях // МИД России. 28.07.2021. URL: https://archive.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/4831832 (дата обращения: 27.09.2021).

в целях нарушения мира и безопасности и содействовали такой деятельности государств в ИКТ-среде, которая способствует экономическому и социальному развитию стран на основе соблюдения принципов и норм международного права (Крутских, Зиновьева 2021: 35).

Развитие международного регулирования международной информационной безопасности в региональных и двусторонних форматах

В связи со сложностью продвижения указанных идей международно-правового характера и в условиях происходящих глобальных изменений перспективы принятия универсального международного договора в области МИБ становятся все более трудно прогнозируемым, если не призрачными, по крайней мере в ближайшие годы. Это связано с агрессивной позицией западных держав, которые и ранее всячески блокировали продвижение российских инициатив, а в настоящее время заняли откровенную враждебную позицию в отношении России и её дипломатических попыток найти разрешение этого замкнутого круга.

Как отметил в своей статье Председатель Конституционного Суда Российской Федерации В.Д. Зорькин, Россия столкнулась с развязанной Западом системной войной против нашей страны, вследствие чего нам предстоит жить в условиях частичной международной изоляции. Однако, В.Д. Зорькин призывает не забывать, что помимо могучих врагов, у России есть множество друзей и союзников, которые весьма заинтересованы в поддержке нашей страны. Среди них страны ЕАЭС, БРИКС, ШОС и других региональных международных организаций (Зорькин 2022).

В преломлении к теме МИБ это означает необходимость в среднесрочной перспективе сосредоточиться на развитии правовых и иных договорённостей в рамках региональных международных организаций и в двустороннем формате. Кроме упомянутых Председателем Конституционного Суда РФ региональных объединений ЕАЭС, БРИКС и ШОС, необходимо также отметить такие значимые форматы, как СНГ, ОДКБ и Союзное государство России и Республики Беларусь. Как уже было отмечено, в рамках указанных региональных организаций за последние двадцать лет был принят ряд важных международно-правовых актов в области МИБ, включая международные договоры. В связи с этим дальнейшее наращивание усилий на данном направлении не теряет своего значения и может принести свои плоды в виде новых важных международных соглашений по отдельным аспектам обеспечения МИБ не только политического, но и правового характера.

В условиях развязанной против России информационной войны приоритетное значение имеет объединение усилий по обеспечению международной и национальной информационной безопасности с нашим ближайшим стратегическим союзником – Республикой Беларусь. Обеспечение информационной безопасности информационных ресурсов Союзного государства и входящих

в него государств отражено в Приоритетных направлениях и первоочередных задачах дальнейшего развития Союзного Государства на 2018–2022 годы, утверждённых постановлением Высшего Государственного Совета Союзного государства от 19 июня 2018 г. Представляется, что мощный импульс развитию системы обеспечения информационной безопасности Союзного государства способно придать принятие стратегического документа – концепции (а возможно стратегии) в области обеспечения информационной безопасности Союзного государства, требуется разработка и принятие такого документа в возможно короткие сроки.

На двустороннем уровне соглашения о сотрудничестве в области МИБ у России заключены также с Бразилией, Вьетнамом, Индией, Китаем, Кубой, Туркменистаном и другими странами (всего свыше 30 межправительственных соглашений). Представляется целесообразным дальнейшее развитие трека двустороннего сотрудничества, как наиболее гибкую составляющую формирования системы международной информационной безопасности.

Нормативные основания обеспечения международной информационной безопасности

Результаты многолетнего международного диалога по вопросам МИБ под эгидой ООН нашли отражение в целом ряде докладов Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (2010, 2013, 2015, 2021) (далее – доклады ГПЭ) и докладе Рабочей группы открытого состава (РГОС) по достижениями в сфере информатизации и телекоммуникаций в контексте международной безопасности A/75/816 от 18 марта 2021 г. (далее – Доклад РГОС 2021).

Анализ данных экспертных докладов позволяет выделить ряд основных политико-правовых механизмов обеспечения МИБ, вокруг которых строится диалог на глобальном уровне:

1. Нормы и принципы международного права.

Международное право остаётся базовой системой нормативного регулирования международных отношений на современном этапе, несмотря на отчётливые тенденции его эрозии и даже кризиса. В настоящее время государства в основном сходятся в позиции относительно применимости норм и принципов традиционного международного права для «поддержания мира и стабильности и для создания открытой, безопасной, стабильной, доступной и мирной информационно-коммуникационной среды» (п. 69 Доклада ГПЭ 2021). Отдельно обращается внимание на необходимость соблюдения государствами основополагающих принципов международного права, включая суверенное равенство государств, воздержания от угрозы силой или ее применения, разрешения споров мирными средствами и иных, для обеспечения МИБ. Вместе с тем в докладах ГПЭ и РГОС подчёркивается, что вопросы применимости конкретных норм

и принципов международного права, в частности международного гуманитарного права, к ИКТ-среде требуют дополнительного изучения.

2. Нормы, правила и принципы ответственного поведения государств.

Учитывая сложности в развитии системы международно-правового регулирования МИБ, международным сообществом были выработаны необязательные нормы ответственного поведения государств. Данные нормы представляют собой самостоятельный контур нормативного регулирования сферы МИБ, дополняющий существующее международное право. В докладах ГПЭ и РГОС необязательные нормы рассматриваются как правовой механизм, который способен снизить риски международному миру и безопасности и повысить предсказуемость поведения государств. В связи с новизной данных правил мы остановимся на их анализе подробнее ниже.

3. Меры укрепления доверия.

Помимо системы правовых и иных норм важную роль в предотвращении конфликтов играют определенные действия, направленные на повышение прозрачности, стабильности и определённости поведения государств в ИКТ-среде. Они получили название «мер укрепления доверия». К их числу относятся: принятие добровольных обязательств государствами, назначение компетентных координаторов и контактных пунктов на политическом и техническом уровнях, диалог и консультации, обмен информацией и положительным опытом. Отмечается, что организация и деятельности РГОС сами по себе являются важной мерой укрепления доверия.

4. Меры наращивания потенциала.

Данное направление обеспечения МИБ связано с повышением возможностей (потенциала) государств по противостоянию информационным угрозам и вызовам. Меры наращивания потенциала включают: разработку и реализацию национальных стратегий и программ в сфере ИКТ, создание и укрепление потенциала групп реагирования на компьютерные инциденты (CERT), укрепление безопасности объектов критической инфраструктуры, повышение правовых, политических и политических возможностей государства по выявлению и реагированию на инциденты в сфере ИКТ, укрепление кадрового потенциала и др. В данном контексте подчёркивается значимость обмена положительным опытом между государствами и оказания взаимной помощи: «деятельность по наращиванию потенциала представляет собой взаимонаправленный процесс, своего рода улицу с двусторонним движением, где участники учатся друг у друга, а все стороны извлекают пользу из общего улучшения положения дел с безопасностью в сфере ИКТ во всем мире» (п. 57 Доклада РГОС 2021).

Таким образом, можно сказать, что на международном уровне сложилось общее понимание нормативных оснований международного сотрудничества в области информационной безопасности. Режим находится на стадии обсуждения основных направлений имплементации уже выработанных норм.

Добровольные и необязательные нормы ответственного поведения государств в ИКТ-среде: характеристика и содержание

Представляется актуальным отметить, что процессы цифровой трансформации обуславливают необходимость «модернизации правовых подходов к урегулированию новых общественных отношений» (Полякова 2019: 4). А.В. Минбалеев обосновано указывает на то, что в современную цифровую эпоху методы правового регулирования должны быть достаточно гибкими и обеспечивать оперативную выработку системы способов и средств реагирования на новые угрозы и вызовы (Савенков, Полякова, Минбалеев 2021: 62). Исследования показывают, что эти выводы особенно значимы для правового регулирования сферы МИБ, где традиционные правовые источники регулирования в виде международных договоров пока недостаточно развиты. В этой ситуации важное значение имеет принятие и реализация иных международных актов в данной сфере, включая политико-декларативные документы и акты «мягкого права».

Одним из таких документов выступают *добровольные и необязательные нормы ответственного поведения государств в ИКТ-среде*. Данные нормы были закреплены в докладах ГПЭ A/70/174 от 22 июля 2015 г. (далее – Доклад ГПЭ 2015) и A/76/135 от 14 июля 2021 г. (далее – Доклад ГПЭ 2021). Генеральная Ассамблея ООН на 75-й сессии рекомендовала данные нормы для рассмотрения государствами.

Следует обратить внимание, что ранее в 2011 г. Россия, КНР, Таджикистан и Узбекистан представили Генеральной Ассамблее ООН «Правила поведения в области обеспечения международной информационной безопасности»[14]. В 2015 г. был направлен второй обновлённый вариант этого документа[15]. Полагаем, что указанный документ сыграл значимую роль в работе Группы правительственных экспертов ООН третьего и четвёртого созыва, и был учтён при подготовке их итоговых докладов.

В Докладе ГПЭ 2015 группа предложила государствам рассмотреть «рекомендации в отношении добровольных и необязательных норм, правил или принципов ответственного поведения государств, призванных способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ-среды» (п. 13). Изложим данные рекомендации по пунктам (см. примечание 1).

Нормативная природа добровольных и необязательных норм ответственного поведения государств в ИКТ-среде раскрыта в докладах ГПЭ 2015 и 2021.

---

[14] Письмо постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при Организации Объединённых Наций от 12 сентября 2011 года на имя Генерального секретаря. A/66/359. URL: https://digitallibrary.un.org/record/710973/files/A_66_359-RU.pdf (дата обращения: 02.06.2022).

[15] Письмо постоянных представителей Казахстана, Китая, Кыргызстана, Российской Федерации, Таджикистана и Узбекистана при Организации Объединённых Наций от 9 января 2015 года на имя Генерального секретаря. A/69/723. URL: https://digitallibrary.un.org/record/786846?ln=en (дата обращения: 02.06.2022).

Согласно указанным докладам, данные нормы «не предусматривают ограничения или запрета действий, согласующихся с нормами международного права», то есть, по сути, эти нормы не устанавливают новых правовых ограничений для государств.

При этом следует отметить, что в Докладе ГПЭ 2021 закреплено, что «нормы и существующее международное право существуют параллельно». Однако данное утверждение представляется дискуссионным, поскольку добровольные и необязательные нормы ответственного поведения государств в ИКТ-среде, направлены на детализацию основополагающих принципов и норм международного права относительно ИКТ-среды. Вместе с тем в докладах ГПЭ обозначается возможность разработки в перспективе дополнительных норм и, отдельно, отмечается возможность, что при необходимости возможна разработка в будущем «дополнительных твёрдых обязательств», т.е. юридически обязывающих международно-правовых норм.

Также в докладах ГПЭ отмечается, что «нормы ответственного поведения государств в ИКТ-среде отражают ожидания международного сообщества, определяют стандарты ответственного поведения и позволяют международному сообществу давать оценку действиям и намерениям государств» (п. 10 Доклада ГПЭ 2015). Таким образом, несмотря на отсутствие обязательной юридической силы, полагаем, что данные нормы могут рассматриваться в качестве определенных стандартов, позволяющих давать политико-правовую оценку действий государств в ИКТ-среде.

Заключение

Проведённое исследование показывает, что система обеспечения международной информационной безопасности находится в стадии формирования. Действующие международные договоры в сферах борьбы с преступностью, терроризмом и иными угрозами международной безопасности только частично затрагивают вопросы безопасного использования ИКТ. До настоящего времени отсутствует базовый универсальный международный договор в области МИБ, хотя имеется положительный опыт принятия подобных документах в форматах региональных организаций с участием России (ОДКБ, ШОС). В этой связи требуется дальнейшее продвижение российской инициативы по принятию Конвенции об обеспечении международной информационной безопасности.

Параллельно необходимо наращивать усилия по развитию международно-правового регулирования МИБ в форматах региональных международных организаций с участием России (СНГ, ОДКБ, ШОС, БРИКС, Союзное государство), а также на двустороннем уровне.

В настоящее время международный диалог строится вокруг развития следующих политико-правовых механизмом обеспечения МИБ: применения норм и принципов международного права; обеспечения выполнения необязательных

норм ответственного поведения государств; реализации укрепления доверия и наращивания потенциала.

В условиях отсутствия юридически обязательных международно-правовых актов в области МИБ существенная роль отводится иным механизмам нормативно регулирования, включая документы политического характера и акты «мягкого права». Одним из перспективных источников видятся добровольные и необязательные нормы ответственного поведения государств в ИКТ-среде. В настоящий момент данные нормы не получили полноценного юридического закрепления, однако в дальнейшем они могут стать основой для принятия международно-правовых актов. Тем не менее, даже в имеющемся виде они способны обеспечить снижение угрозы международному миру, безопасности и стабильности.

Примечание 1.

Добровольные и необязательные нормы ответственного поведения государств в ИКТ-среде

а) В соответствии с целями Устава ООН, в том числе касающимися поддержания международного мира и безопасности, государства должны сотрудничать в разработке и осуществлении мер по укреплению стабильности и безопасности в использовании ИКТ и предупреждению совершения действий в сфере ИКТ, признанных вредоносными или способных создать угрозу международному миру и безопасности;

б) В случае инцидентов в сфере ИКТ государства должны изучить всю соответствующую информацию, в том числе более общий контекст события, проблемы присвоения ответственности в ИКТ-среде, а также характер и масштабы последствий; Пункт с) государства не должны заведомо позволять использовать их территорию для совершения международно-противоправных деяний с использованием ИКТ;

в) Государства должны рассмотреть вопрос о наилучших путях сотрудничества в целях обмена информацией, оказания взаимопомощи, преследования лиц, виновных в террористическом и преступном использовании ИКТ, а также осуществлять другие совместные меры по противодействию таким угрозам. Государствам, возможно, потребуется рассмотреть вопрос о разработке новых мер в этой сфере;

г) В процессе обеспечения безопасного использования ИКТ государства должны соблюдать положения резолюций 20/8 и 26/13 Совета по правам человека о поощрении, защите и осуществлении прав человека в Интернете и резолюций 68/167 и 69/166 Генеральной Ассамблеи о праве на неприкосновенность личной жизни в эпоху цифровых технологий, чтобы обеспечить всестороннее уважение прав человека, включая право свободно выражать своё мнение;

д) Государство не должно осуществлять или заведомо поддерживать деятельность в сфере ИКТ, если такая деятельность противоречит его обязатель-

ствам по международному праву, наносит преднамеренный ущерб критически важной инфраструктуре или иным образом препятствует использованию и функционированию критически важной инфраструктуры для обслуживания населения;

е) Государства должны принимать надлежащие меры для защиты своей критически важной инфраструктуры от угроз в сфере ИКТ, принимая во внимание резолюцию 58/199 Генеральной Ассамблеи о создании глобальной культуры кибербезопасности и защите важнейших информационных инфраструктур и другие соответствующие резолюции;

ж) Государства должны удовлетворять соответствующие просьбы об оказании помощи, поступающие от других государств, критически важная инфраструктура которых становится объектом злонамеренных действий в сфере ИКТ. Государства должны также удовлетворять соответствующие просьбы о смягчении последствий злонамеренных действий в сфере ИКТ, направленных против критически важной инфраструктуры других государств, если такие действия проистекают с их территории, принимая во внимание должным образом концепцию суверенитета;

з) Государства должны принимать разумные меры для обеспечения целостности каналов поставки, чтобы конечные пользователи могли быть уверены в безопасности продуктов ИКТ. Государства должны стремиться предупреждать распространение злонамеренных программных и технических средств в сфере ИКТ и использование пагубных скрытых функций;

и) Государства должны способствовать ответственному представлению информации о факторах уязвимости в сфере ИКТ и делиться соответствующей информацией о существующих методах борьбы с такими факторами уязвимости, чтобы ограничить, а по возможности и устранить возможные угрозы для ИКТ и зависящей от ИКТ инфраструктуры;

к) Государства не должны осуществлять или заведомо поддерживать деятельность, призванную нанести ущерб информационным системам уполномоченных групп экстренной готовности к компьютерным инцидентам (также именуемым группами готовности к компьютерным инцидентам или группам готовности к инцидентам в сфере кибербезопасности) другого государства. Государство не должно использовать уполномоченные группы экстренной готовности к компьютерным инцидентам для осуществления злонамеренной международной деятельности.

Об авторах:

Сергей Владимирович Шитьков – проректор по правовым и административным вопросам МГИМО МИД России, Россия 119454, Москва, проспект Вернадского, 76. E-mail: inbox@inno.mgimo.ru

Татьяна Анатольевна Полякова – главный научный сотрудник, и.о. заведующего сектором информационного права и международной информационной безопасности Института государства и права РАН, доктор юридических наук, профессор, Заслуженный юрист Российской Федерации, Россия 119019, Москва, ул. Знаменка, д. 10. E-mail: polyakova_ta@mail.ru

Александр Александрович Смирнов – старший научный сотрудник сектора информационного права и международной информационной безопасности Института государства и права РАН, кандидат юридических наук, доцент. E-mail: smirnov_research@bk.ru

Конфликт интересов:
Авторы заявляют об отсутствии конфликта интересов.

Благодарности:
Статья подготовлена в рамках выполнения Государственного задания № 0136-2021-0042 «Правовое регулирование цифровой экономики, искусственного интеллекта, информационной безопасности».

UDC 327:341.231.14:004.056"20"
Received: September 05, 2022
Accepted: December 11, 2022

Emerging international regime of information security

Sergey V. Shitkov[1], Tatiana A. Polyakova[2], Aleksandr A. Smirnov[2]
DOI 10.24833/2071-8160-2022-olf6

[1] MGIMO University
[2] Institute of State and Law, Russian Academy of Sciences

Abstract: TThe article analyzes the formation of an emerging international regime for ensuring information security amid ongoing geopolitical transformations and global turbulence. The study draws on the theory of international regimes, developed in both Russian and Western academic traditions, as its theoretical and methodological foundation. Relying on the classical definition of an international regime, the authors focus on the evolution of norms and principles in the field of international information security. These norms—defining responsible state behavior in the global information space—were first proposed by Russia and its SCO partners in 2011 within the framework of discussions at the UN General Assembly. However, Russian initiatives encountered strong opposition from the United States, leading to the fragmentation of the emerging regulatory framework in this area.
At present, the relevant norms and principles, grounded in the fundamental principles of international law enshrined in the UN Charter, are reflected in UN General Assembly resolutions and the reports of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Al-

though these norms are non-binding, they play an important role in promoting international stability by structuring the expectations and behavior of states and other actors in the field of information security. Nevertheless, the absence of formal consolidation and institutionalization through legally binding international treaties undermines their legitimacy and limits their regulatory potential.

Key words: international information security, information threats, international law, international regimes, responsible state behavior, ICT environment

About the authors:

Sergey V. Shitkov – Vice-Rector for Legal and Administrative Issues of MGIMO University, Prospekt Vernadskogo, 76, 119454 Moscow, Russian Federation. E-mail: inbox@inno.mgimo.ru

Tatiana A. Polyakova – Doctor of Law, Professor, Honored Lawyer of the Russian Federation, Chief Researcher, Acting Head of the Information Law and International Information Security Sector of the Institute of State and Law, Russian Academy of Sciences (Moscow), 10 Znamenka str., 119019, Moscow, Russian Federation. E-mail: polyakova_ta@mail.ru

Aleksandr A. Smirnov – Candidate of Juridical Sciences, Associate professor, Senior researcher of the Information Law and International Information Security Sector of the Institute of State and Law, 10 Znamenka str., 119019, Moscow, Russian Federation.
E-mail: smirnov_research@bk.ru

Conflict of interests:
The authors declare the absence of conflict of interests

Acknowledgements:
The article was prepared as part of implementing the State task № 0136-2021-0042 «Legal regulation of the digital economy, artificial intelligence, information security".

References:

Axelrod R. The evolution of cooperation. N. Y.: Cambridge University Press, 1984.

Axelrod R., Keohane R. 1993. *Achieving Cooperation under Anarchy: Strategies and Institutions. Neorealism and neoliberalism: the contemporary debate.* New York.

Haas,P. 1992. Epistemic Communities and International Policy Coordination. Introduction. *International Organization.* №. 46 (1). P. 1-35.

Hasenclever A., Mayer P., Rittberger V. 1997. *Theories of International Regimes.* N. Y.: Cambridge University Press.

Hasenclever A., Mayer P., Rittberger V. 2000. Integrating theories of international regimes. *Review of International Studies.* №. 26. P. 3–33.

Keohane R. 1998. International institutions: can interdependence work? (The Frontiers of Knowledge). *Foreign Policy.* Vol. 110. P. 82-96.

Keohane R., Nye J. 1989. *Power and Interdependence: World Politics in Transition.* Boston: Little Brown.

Kratochwil F., Ruggie J. International Organization. 1986. A State of the Art and an Art of the State. *International Organization.* №. 40 (4). P. 753–775.

Levy M., Young O., Zuern M. 1995. The study of international regimes. *European Journal of International Relations.* № 3(1). P. 267-330.

Mearsheimer J. 1994. The False Promise of International Institutions. *International Security.* №. 15 (3). P. 5–49.

Ruggie J. 1983. *International regimes, transactions and change: embedded liberalism in the postwar economic order International Regimes.* Ithaca: Cornell University Press.

Young O. 1989. *International Cooperation: Building Regimes for Natural Resources and the Environment.* Ithaca.

Boiko S. 2018. Osnovy gosudarstvennoi politiki Rossiiskoi Federatsii v oblasti mezhdunarodnoi informatsionnoi bezopasnosti: regulirovanie i mekhanizmy realizatsii [Fundamentals of the State Policy of the Russian Federation in the field of international information security: regulation and implementation mechanisms]. *Mezhdunarodnaya zhizn'*. № 11. P. 24-35. (In Russian)

Krutskikh A.V,. Zinov'eva E.S. 2022. *Mezhdunarodnaya informatsionnaya bezopasnost': podkhody Rossii* [International information security: approaches of Russia]. Moscow, MGIMO University. (In Russian)

Polyakova T.A. 2019. Tsifrovizatsiya i sinergiya pravovogo obespecheniya informatsionnoi bezopasnosti [Digitalization and synergy of legal provision of information security]. *Informatsionnoe parvo.* №. 2. P. 4-7. (In Russian)

Polyakova T.A. 2020. *Modeli pravovogo regulirovaniya obespecheniya informatsionnoi bezopasnosti v usloviyakh bol'shikh vyzovov v global'nom informatsionnom obshchestve: monografiya* [Models of legal regulation of information security in the context of big challenges in the global information society: monograph]. Saratov: Amirit. (In Russian)

Polyakova T.A., Minbaleev A.V., Krotkova N.V. 2021. Razvitie nauki informatsionnogo prava i pravovogo obespecheniya informatsionnoi bezopasnosti: formirovanie nauchnoi shkoly informatsionnogo prava (proshloe i budushchee) [Development of the science of information law and legal provision of information security: formation of the scientific school of information law (past and future)]. *Gosudarstvo i parvo.* № .12. P. 97–108. (In Russian)

Polyakova T.A., Minbaleev A.V., Naumov V.B. 2018. Forsait-sessiya «Informatsionnaya bezopasnost' v XXI veke: vyzovy i pravovoe regulirovanie» [Foresight session "Information security in the 21st century: challenges and legal regulation]. *Trudy Instituta gosudarstva i prava Rossiiskoi akademii nauk.* Vol. 13. № .5. P.194-208. (In Russian)

Polyakova T.A., Shinkaretskaya G.G. 2020. Problemy formirovaniya sistemy mezhdunarodnoi informatsionnoi bezopasnosti v usloviyakh transformatsii prava i novykh vyzovov i ugroz [Problems of formation of the international information security system in the conditions of transformation of law and new challenges and threats]. *Pravo i gosudarstvo: teoriya i praktika.* №. 10 (290). P. 138-142. (In Russian)

Savenkova A.N., Polyakova T. A., Minbaleev A.V. 2021. *Tsifrovaya transformatsiya: vyzovy pravu i vektory nauchnykh issledovanii: monografiya* [Digital transformation: challenges to law and vectors of scientific research: monograph]. RG-Press. (In Russian)

Smirnov A.A. 2021. Chetvertyi prioritet: pravovoe zakreplenie zadach obespecheniya informatsionnoi bezopasnosti v novoi Strategii natsional'noi bezopasnosti Rossiiskoi Federatsii [Fourth priority: legal consolidation of information security tasks in the new National Security Strategy of the Russian Federation]. *Vestnik Voronezhskogo gosudarstvennogo universiteta. Seriya: Pravo.* 2021. №. 3 (46). P. 222-228. DOI: 10.17308/vsu.proc.law.2021.3/3552 (In Russian)

Vinogradova E.V., Polyakova T.A. 2021. O meste informatsionnogo suvereniteta v informatsionno-pravovom prostranstve sovremennoi Rossii [On the place of information sovereignty in the information and legal space of modern Russia]. *Pravovoe gosudarstvo: teoriya i praktika.* № 1(63). P. 32–49. DOI 10.33184/pravgos-2021.1.3 (In Russian)

Zinov'eva E.S. 2021. *Mezhdunarodnaya informacionnaya bezopasnost': problemy mnogostoronnego i dvustoronnego sotrudnichestva: monografiya* [International information security: problems of multilateral and bilateral cooperation]. Moscow, MGIMO-Universitet. P.280. (In Russian)

Список литературы на русском языке:

Бойко С. 2018. Основы государственной политики Российской Федерации в области международной информационной безопасности: регулирование и механизмы реализации. *Международная жизнь.* № 11. С. 24-35.

Виноградова Е.В., Полякова Т.А. 2021. О месте информационного суверенитета в информационно-правовом пространстве современной России. *Правовое государство: теория и практика.* № 1 (63). С. 32–49. DOI 10.33184/pravgos-2021.1.3

Зиновьева Е.С. 2021. *Международная информационная безопасность: проблемы многостороннего и двустороннего сотрудничества.* М.: МГИМО-Университет.

Крутских А.В., Зиновьева Е.С. 2022. *Международная информационная безопасность: подходы России.* МГИМО МИД России, 2021.

Полякова Т.А. 2019. Цифровизация и синергия правового обеспечения информационной безопасности. *Информационное право.* № 2. С. 4–7.

Полякова Т.А. 2020. *Модели правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе.* Саратов: Амирит.

Полякова Т.А., *Минбалеев А.В., Кроткова Н.В.* 2021. Развитие науки информационного права и правового обеспечения информационной безопасности: формирование научной школы информационного права (прошлое и будущее). *Государство и право.* № 12. С. 97–108.

Полякова Т.А., Минбалеев А.В., Наумов В.Б. 2018. Форсайт-сессия «Информационная безопасность в XXI веке: вызовы и правовое регулирование». *Труды Института государства и права Российской академии наук.* Т. 13. № 5. С. 194-208.

Полякова Т.А., Шинкарецкая Г.Г. 2020. Проблемы формирования системы международной информационной безопасности в условиях трансформации права и новых вызовов и угроз. *Право и государство: теория и практика.* № 10 (290). С. 138-142.

Савенков А.Н., Полякова Т.А., Минбалеев А.В. 2021. *Цифровая трансформация: вызовы праву и векторы научных исследований: монография.* РГ-Пресс, 2021. С. 62.

Смирнов А.А. 2021. Четвёртый приоритет: правовое закрепление задач обеспечения информационной безопасности в новой Стратегии национальной безопасности Российской Федерации. *Вестник Воронежского государственного университета.* Серия: Право. № 3 (46). С. 222-228. DOI https: doi.org/10.17308/vsu.proc.law.2021.3/3552