Article

ТЕОРЕТИЧЕСКИЕ И ПРАКТИЧЕСКИЕ АСПЕКТЫ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ТЕКУЩИХ УСЛОВИЯХ

Дмитрий Фатыхов*

DOI 10.24833/2073-8420-2024-2-71-140-147

Рецензия на книгу: *Зиновьева Е.С. 2021. Международная информационная безопасность: Проблемы двустороннего и многостороннего сотрудничества. Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации. 280 с. ISBN 978-5-9228-2454-5.*

Международная информационная безопасность (МИБ) – динамично развивающаяся область исследований. Современные информационно-коммуникационные технологии (ИКТ) стали неотъемлемой частью экономической и политической системы государств, а также повседневной жизни людей. Вместе с ИКТ постоянно эволюционируют информационные вызовы и угрозы безопасности. Проблемы и особенности функционирования информационной сферы, которые менее 10 лет назад не существовали или рассматривались преимущественно в теории, сегодня выходят на первый план. Кибербезопасность, защита компьютерных сетей от внешних воздействий, сбор, использование и защита информации (в том числе персональной), вопросы управления сетью Интернет, а также информационно-пропагандистское воздействие онлайн-сервисов (в особенности соцсетей), с одной стороны, представляют собой обособленные проблемы, затрагивающие различные технологические отрасли и сферы госрегулирования. Вместе с тем они же во многом взаимосвязаны, а потому требуют комплексного анализа как в теоретическом, так и в нормативном разрезе. Изданная в 2021 г. монография Е.С. Зиновьевой «Международная информационная безопасность: проблемы многостороннего и двустороннего сотрудничества» представляет собой как раз такую работу, что качественно выделяет ее на фоне других материалов на эту тему.

Актуальность сделанных в ней исследовательских выводов особенно явно проявилась в 2022 г. в связи с событиями вокруг

*** Фатыхов Дмитрий Русланович**, соискатель кафедры мировых политических процессов МГИМО МИД России
e-mail: d.fatykhov@gmail.com
ORCID ID: 0009-0006-8682-2153

специальной военной операции на Украине. В этой связи видится уместным проанализировать и дать оценку основным разделам монографии, в том числе в разрезе современных трендов в развитии международной информационной безопасности.

Рассматриваемая работа является содержательным и смысловым развитием монографии Е.С. Зиновьевой «Международная информационная безопасность» 2013 года. Новая монография детально рассматривает основные теоретические подходы к исследованию роли ИКТ в современной мировой политике и основные понятия, связанные с международной информационной безопасностью. Особый интерес представляют главы, посвященные детальному разбору всех основных форматов международного сотрудничества в сфере МИБ с акцентом на роль и участие в них России, а также на вопросы правового обеспечения информационной безопасности.

Детальная проработка этих вопросов делает монографию ценной в том числе в качестве отправной точки для углубленных исследований широкого спектра вопросов, связанных с ролью ИКТ в международных отношениях, проблем информационной безопасности, а также подходов в информационном сопровождении внешнеполитической деятельности стран и интеграционных блоков.

В ***первой главе*** работы рассматриваются ключевые тенденции, а также теоретические подходы к исследованию роли ИКТ в мировой политике, в особенности в вопросах безопасности. Автор справедливо отводит Интернету определяющую роль в формировании глобального информационного пространства, приводя актуальную статистику охвата населения Земли критической информационной инфраструктурой. Кратко пройдясь по истории создания Интернета, Е.С. Зиновьева выделяет ключевые тенденции его развития: рост числа пользователей (прежде всего за счет Азии и Ближнего Востока) при растущем доминировании мобильного доступа над стационарным; повальная популярность соцсетей; использование технологий Web 2.0 для формирования платформ политического дискурса и влияния на коллективное самосознание пользователей; унификация "традиционных" коммуникационных технологий (ТВ, телефония) на онлайн-платформах; рост облачных технологий хранения данных, а также технологий сбора и обработки "больших данных"; развитие "интернета вещей"; рост экономической значимости технологий block chain и криптовалют; развитие ИИ; технологическая биполярность с существенной концентрацией влияния в ИКТ-сфере у США и Китая.

Переходя к теоретико-методологическим основаниям анализа роли информационных технологий в международных отношениях, автор отмечает недостаточную научную проработку вопросов взаимовлияния мировой политики и технологической сферы. Е.Зиновьева критически относится к технологическому детерминизму, присущему ряду наиболее известных исследователей информационного общества, и скептически воспринимает продвигаемый ими тезис, что технологии сами по себе могут стать ключевым драйвером общественного развития. Вместо этого она исходит из предпосылки, что, несмотря на то, что контроль ключевых технологий действительно является фактором политического влияния, в конечном итоге технологии находятся на службе у людей, а пути технологического развития, как и прежде, определяются политическими интересами. Продолжая обзор исследований, посвященных мирополитическому измерению информатизации, она констатирует, что развитие ИКТ само по себе не устраняет анархичного и конфликтного характера мировой системы.

Государства, включая Россию, остро осознающие потенциал современных технологий, стремятся к технологическому и информационному суверенитету, а информационная составляющая стала в том числе важным критерием военной мощи. Последний тезис, необходимо отметить, особенно явно проявился на современном этапе специальной военной операции: доступ к онлайн-инфраструктуре, включая спутниковый Интернет, в сочетании с использованием новых технических средств, включая дроны [2], перевернул господствовавшие ранее представления об управлении войсками, а мобильные устройства и соцсети обеспечили беспрецедентные возможности как для информирования о ходе боевых действий, так и для дезинформации. Если "Буря в пустыне" была войной "в прямом эфире", то СВО, вероятно, войдет в историю как "война в режиме онлайн-трансляции".

Третья глава рассматривает понятие информационной безопасности и эволюцию подходов к ее изучению в мировой исследовательской литературе. Автор отмечает, что к началу 1990-х гг. секьюритизация информационной сферы, очевидная для

ключевых мировых игроков, стала предметом научного анализа сначала в США, а затем и в других странах, включая Россию, где постепенно сформировалось свое направление исследований, отличное от западного. Для последнего, как отмечает Е. Зиновьева, характерен в том числе акцент на информационно-психологический компонент ИКТ, возможность их использования для массированного воздействия на общественное мнение как в отдельных странах, так и в мировом масштабе. Информационная война, таким образом, может и не иметь явных проявлений (воздействие на критическую инфраструктуру и использование ИКТ в военных операциях), фактически не нарушая ход мирной жизни.

Продолжая тему общей характеристики угроз международной информационной безопасности, автор обращает внимание на их многогранность: информационные средства могут не только давать доступ к стратегической информации и воздействовать на общественное мнение, но и использоваться для физических атак на критическую инфраструктуру – в качестве примера приводится внедрение вируса Stuxnet в систему управления АЭС в Бушере в 2010 году (атака, приписываемая израильским спецслужбам, примечательна еще и тем, что полагалась не на Интернет-взлом, а на агентурную работу и физическое внедрение с использованием зараженного USB-накопителя [4]).

Использование ИКТ в военно-политических целях автор называет ключевой угрозой международной безопасности, рассматривая типологию форм информационной войны и теоретические подходы к рассмотрению данного феномена в контексте продолжающейся революции в военном деле. Ряд подходов и прогнозов развития военного дела, упомянутые в завершающей части главы, подтвердились в ходе Специальной военной операции на Украине. В частности, конфликт стал полигоном для боевого применения ранее не использовавшихся в таких масштабах самоуправляемых систем вооружений на основе ИИ и технологий дополненной реальности – ударных и разведывательных беспилотных летательных аппаратов, барражирующих боеприпасов, новых типов высокоточных вооружений.

В ***четвертой главе*** представлен углубленный анализ различных типов субъектов международных взаимодействий в сфере информационной безопасности.

Автор выделяет три группы субъектов угроз международной безопасности: государства, террористические организации и преступные группы, констатируя, впрочем, что в настоящий момент также растет роль бизнес-структур, сетевых сообществ и индивидов, а дешевизна и относительная простота в использовании отдельных видов информационного оружия позволяет использовать их малым государствам и негосударственным акторам.

Отдельно рассматривается использование ИКТ террористическими организациями для пропаганды, атак на информсистемы, планирования атак – в этом контексте рассмотрен кейс ИГИЛ – а также деятельность киберпреступников.

Говоря о субъектах международного сотрудничества в области информационной безопасности, автор обобщает ключевые подходы (секьюритизирующие дискурсы) к определению угроз в данной сфере: кибербезопасность (информационно-техническая составляющая) и информационную безопасность (техническая и информационно-психологическая составляющие), при этом подчеркивая роль государств как секьюритизирующих акторов, определяющих как состав и характер информационных угроз, так и пути противодействия им. Это обстоятельство препятствует налаживанию сотрудничества в сфере информационной безопасности: в частности, если Россия и Китай придерживаются широкой трактовки информационной безопасности (технический+психологический аспект), то США и страны Запада до недавнего времени предпочитали акцентировать исключительно кибербезопасность, вероятно, «развязывая» себе руки в части информационно-психологических операций, в том числе за рубежом. Тем не менее события вокруг якобы имевшего место внешнего вмешательства в президентскую кампанию 2016 г., в т.ч. путем воздействия на общественное мнение через соцсети, убедили Вашингтон в необходимости расширительной трактовки информационной безопасности, что нашло отражение в американской Стратегии национальной безопасности.

Рассматривая в пятой главе классификацию основных объектов информационной безопасности, автор заостряет внимание на обеспечении защиты критической инфраструктуры и противоречиях, возникающих при разработке соответствующего регулирования как на государственном, так и на наднациональном уровне. Значительная

часть критической инфраструктуры (автор упоминает систему доменных имен и адресов Интернета, а также глубоководные оптоволоконные кабельные линии) находится в частной собственности, однако задачи их защиты нерешаемы без согласованных усилий всех стран, в чьей зоне ответственности такая инфраструктура находится.

Определенные возражения может вызвать рассматриваемая автором дихотомия информационной и традиционной критической инфраструктуры, а также в увязке с ней – конвенционального и информационного оружия. События минувшего года показали не только значительную увязку традиционного и информационного оружия (упомянутые выше технологии БПЛА и сетевые технологии управления войсками), но и серьезный характер поражения критической информационной инфраструктуры обычными вооружениями. Диверсия на подводных ветках газопровода «Северный поток» в сентябре 2022 г., расположенных в одной акватории с российскими оптоволоконными кабелями, доставляющими трафик в Калининградскую область, наглядно продемонстрировала уязвимость сетевой инфраструктуры для скрытных физических атак, издержки защиты от которых были бы запредельно велики для любого субъекта международной информбезопасности. Можно согласиться с Е.Зиновьевой, что масштабное применение такой тактики маловероятно, но даже точечные удары по магистральным каналам связи способны вызвать серьезные перебои в работе критической сетевой инфраструктуры.

В отдельном параграфе рассматривается возросшая роль социальных сетей в контексте информационной безопасности и основные теоретические подходы к этому относительно новому феномену. Верно подчеркнуто, что технологии микротаргетирования, сбора персональных данных пользователей и постоянно совершенствующихся алгоритмов работы с ними создает качественно новые вызовы госбезопасности. В современных условиях утрачивается монополия государства на формулирование доминирующего политического дискурса, традиционно реализуемая посредством административного или экономического контроля над СМИ; государственная граница становится проницаема для воздействия внешних акторов на общественное мнение. В этом контексте особенно тревожен феномен «цифровой дипломатии» США, реализуемой как за счет государственного финансирования «альтернативных» электронных СМИ, так и через работу американских Интернет-гигантов, компаний-лидеров по сбору и обработке персональных данных (Google, Facebook, Twitter). Как заявил Главный исполнительный директор Twitter Параг Агравал, "свобода слова не в фокусе нашего внимания. Свобода слова в Интернете – это легко. Большинство людей могут высказываться свободно. Наша роль – определять, кто будет услышан"[1].

Европейский союз при этом ставится в один ряд с США в плане подходов к решению политических задач через соцсети – в качестве примера приводится работа группы стратегических коммуникаций «Восток» (East StratComTeam). Вместе с тем, необходимо признать, что ЕС, не имеющий собственных глобальных Интернет-компаний, работающих с пользовательскими данными, сегодня серьезно уступает Вашингтону по уровню влияния в этой сфере – с этим, как представляется, связана активная работа Евросоюза по созданию высокоэффективного регулирования работы Интернет-гигантов и обработки персональных данных своих граждан. Так, вступивший в силу с мая 2018 г. Общий регламент по защите данных (General Data Protection Regulation) примечателен тем, что его действие распространяется на интернет-компании, не учрежденные в европейской юрисдикции и зачастую не имеющие юридических лиц в ЕС, но при этом работающие с европейской аудиторией, а обсуждающийся проект Закона ЕС о цифровых услугах (Digital Services Act) отдельно регулирует деятельность «привратников» - крупных компаний, контролирующих важные цифровые экосистемы и де-факто способных устанавливать свои правила поведения в цифровой среде[2]. Наконец, из последних инициатив стоит отметить одобренный Европейским парламентом Закон об искусственном интеллекте (AI Act). Он предусматривает запрет на использование систем распознавания лиц и «удаленной биометрической идентификации» (в т.ч. систем распознавания эмоций)

[1] EmTech Stage: Twitter's CTO on misinformation // MIT Technology Review. Nov.18 2020
[2] The Digital Markets Act: ensuring fair and open digital markets // European Commission. Oct. 12 2022.

в режиме реального времени в общественных местах и устанавливает обязательство уведомлять пользователя об использовании систем генеративного ИИ. Также запрещено будет использование правоохранителями для профилактики правонарушений систем аналитики на основе алгоритмов[3].

В дополнение к роли соцсетей в контексте событий вокруг Украины необходимо отметить возросшую роль соцсетей в разведывательной работе. Разведка на основе открытых источников (Open Source Intelligence) – использование геолокации и метаданных добровольно размещаемого в соцсетях контента в военных целях – это высокоэффективный инструмент как для выбора военных целей, так и для объективного контроля их огневого поражения, и может осуществляться частными организациями по заказу военных ведомств [3].

Большая часть монографии ***(главы 6-7)*** посвящена разбору основных форматов международного сотрудничества по обеспечению международной безопасности, в том числе отдельно – в сфере управления Интернетом.

Открывая раздел о глобальных форматах сотрудничества в сфере международной безопасности, Е.С. Зиновьева отмечает, что соответствующие усилия ООН в целом идут в ногу с эволюцией вызовов и угроз в сфере ИКТ. Вместе с тем, по мнению автора, работа, запущенная с принятием в 1999 г. первой резолюции «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности» проходила под знаком попыток сохранить переговорный потенциал ООН в условиях трудноразрешимых международных противоречий в сфере МИБ. Не в последнюю очередь эти сложности были обусловлены позицией США, пользовавшихся преимуществами мирового лидера в развитии ИКТ на всем протяжении работы профильных групп в ООН, в то время как ряд стран, включая Россию, выступали за выработку общих правил поведения в глобальном информпространстве. На практике, как отмечает Е.С. Зиновьева, это выразилось в появлении на площадке ООН двух конкурирующих структур – Рабочей группы по МИБ расширенного состава, открытой для участия всех стран-членов, и продвигаемой Вашингтоном Группы правительственных экспертов в ограниченном составе 25 государств.

По итогу, несмотря на потенциал ООН как универсальной переговорной платформы по вопросам информационной безопасности, необходимо констатировать отсутствие обязывающих документов в сфере МИБ, принятых на площадке организации.

Любопытно включение в обзор Международного союза электросвязи (МСЭ), занятого преимущественно техническими вопросами трансграничной частотной координации и работы систем связи, однако принимающего решения и по концептуальным вопросам МИБ. Можно согласиться с выводом автора о крайней политизированности МСЭ и его ориентации на Запад – при этом в качестве яркого примера этому можно было бы выделить подход организации к Крыму: МСЭ с 2014 г. выступал с позиции де-факто непризнания российского суверенитета над полуостровом, не содействуя координации частотных присвоений с Украиной[4].

Всемирная встреча на высшем уровне по вопросам информационного общества рассматривается как попытка продвижения оонновских подходов к интернационализации МИБ и управления Интернетом, которая, впрочем, как и ООН в целом, столкнулась с трудностями в балансировании интересов многочисленных стейкхолдеров и принятии обязывающих итоговых документов.

После 2012 г. отмечается активизация работы МАГАТЭ по обеспечению информационной безопасности на атомных объектах; инициирована Программа компьютерной и информационной безопасности при профильном управлении организации. Важно проследить за дальнейшим развитием работы в этом направлении, особенно в свете событий на Украине. Сегодня МАГАТЭ взяло на себя функции главного переговорщика по обеспечению безопасности критической инфраструктуры, в особенности Запорожской АЭС – по мере снижения интенсивности боевых действий проблема физической безопасности объекта может уступить место защите от кибератак, направленных на дестабилизацию его работы.

В заключении отмечается относительное бездействие Группы семи в сфере международной информационной безопасности.

---

[3] MEPs ready to negotiate first-ever rules for safe and transparent AI. // European Parliament. Jun. 14 2023

[4] Госспецсвязи Украины попросит у МСЭ уточнить статус радиочастот, используемых в Крыму // НИИР, 7 апреля 2014

Представленный автором обзор региональных инициатив по регулированию МИБ носит комплексный характер, охватывая, пожалуй, все действующие на сегодняшний день региональные объединения. Состав участников этих инициатив и их характер в целом отражает описываемые автором в предыдущих разделах противоречия между глобальным Западом, стремящимся сохранить доминирование в сфере ИКТ, и группами стран во главе с Россией и Китаем, настаивающими на формировании общих правил поведения в сфере МИБ.

Так, первое международное соглашение в сфере информационной безопасности, подписанное и ратифицированное участниками, было разработано в рамках ШОС 2009 г. и было основано на ООНовских подходах к определению угроз в этой сфере – в целом ШОС ведет активную работу в этой сфере, исходя из приоритета международных взаимодействий в рамках ООН.

Аналогичным образом на формирование общих правил поведения ориентирована деятельность СНГ, направленная в том числе на гармонизацию соответствующего законодательства стран-членов – это в известном смысле сближает подходы Содружества и Евросоюза с его моделью наднационального регулирования через Директивы ЕС. ОДКБ, будучи организацией в сфере безопасности, также частично переносит свою деятельность в информационную сферу.

Комментируя инициативы в рамках ОБСЕ, Е.С. Зиновьева отмечает снижение активности Организации по теме МИБ после 2016 г. Здесь можно добавить, что это снижение в целом совпало с планомерной деградацией ОБСЕ из площадки для инклюзивного диалога по европейской безопасности в инструмент политического давления на Россию по украинскому вопросу. С де-факто прекращением участия РФ в работе ОБСЕ, в которой, по справедливому замечанию автора, и так недопредставлены сторонники инклюзивного подхода к МИБ из числа стран БРИКС, о какой-либо конструктивной роли Организации в этом вопросе говорить не приходится.

В разборе работы Евросоюза акцент сделан на том, что в сфере «жесткой» кибербезопасности ЕС после 2014 г. все больше следует в орбите подходов НАТО к противодействию т.н. «гибридным угрозам» со стороны России. В рамках этих подходов Евросоюз предпринимает шаги по изоляции европейского рынка данных, еще больше фрагментируя глобальное информационное пространство. НАТО же, будучи военным альянсом, изначально не настроена на формирование общих правил поведения в сфере МИБ, концентрируя свои усилия на активном сдерживании противников Альянса в киберпространстве.

АСЕАН и БРИКС, не претендуя на наднациональный характер и признавая приоритет суверенных интересов в сфере кибербезопасности, по мнению автора, являются важными переговорными площадками, на которых российская позиция о необходимости создания общих правил МИБ не только не маргинализируется, но и активно поддерживается большинством участников - в этом качестве они формируют значимый противовес западным подходам. Не случайно именно со странами БРИКС (Китай, Индия, ЮАР) у России заключены двусторонние соглашения, фиксирующие российские позиции по обеспечению справедливого режима международной безопасности в этой сфере, включая невмешательство в дела суверенных государств и взаимный отказ от кибератак как внешнеполитического инструмента.

Транснациональному уровню в вопросах глобальной кибербезопасности в работе Е.С. Зиновьевой уделено меньше внимания, чем международному, поскольку, как справедливо отмечает автор, в вопросах «жесткой» кибербезопасности бизнес выступает преимущественно проводником интересов государств. При этом IT-гиганты, как представляется, склонны рассматривать безопасность и защиту данных главным образом как способ защитить свои коммерческие интересы, и неохотно следуют правилам, в том числе международным, которые могут подорвать их позиции на соответствующих рынках – достаточно вспомнить рекордный штраф в размере более 4 млрд евро, который Европейский суд взыскал с Google за использование программных средств ОС Android против конкурентов[5], а также штраф в 4 млрд рублей за злоупотребление доминирующим положением аудиовизуального сервиса YouTube на российском рынке [1].

Седьмая глава посвящена критическому разбору существующей системы управления Интернетом и поиску путей налаживания равноправного международного

[5] Google: EU court confirms record €4 billion antitrust fine // Deutsche Welle. Sep. 14 2022

сотрудничества в этой сфере. Основным источником озабоченности в сложившейся системе является сохранение критической инфраструктуры адресного пространства сети Интернет под контролем НПО ICANN и ее дочерней организации PTI, не являющихся субъектами международного права и работающими по законам США.

Действенным путем преодоления данного кризиса легитимности Е. Зиновьева видит деполитизацию управления Интернетом и передачу соответствующих механизмов и инфраструктуры под международное управление структур ООН, главным образом – Международного союза электросвязи. Автор возлагает определенные надежды на запланированный на 2025 г. саммит ООН по вопросам развития информационного общества – к этому моменту накопившийся груз противоречий может вынудить США уступить лидирующие позиции в области управления Интернетом.

Такой осторожный оптимизм видится не в полной мере оправданным, принимая во внимание планомерную эскалацию напряженности между США и Китаем в последние годы, еще сильнее усугубившуюся на фоне украинского кризиса, в которой растущие озабоченности Вашингтона по поводу киберугроз и доминирования Пекина в IT-секторе играют важную роль [6]. В этих условиях США едва ли будут открыты к конструктивному решению вопроса интернационализации управления Интернетом.

В ***восьмой главе*** Е.Зиновьева обращает внимание на несовершенство существующей системы международного права в применении к информационной сфере. Неочевидность трактовок вопросов территориального суверенитета при агрессивных действиях государств и негосударственных акторов в информационной сфере не позволяет задействовать международно-правовые механизмы защиты государств. В адаптации к информационному пространству нуждаются нормы, регламентирующие применение силы и порядок реагирования на агрессию, а также нормы гуманитарного права.

Необходимость преодоления этих противоречий, по мнению автора, еще раз актуализирует важность создания действенных международных механизмов, которые регулировали бы в том числе специфическую и постоянно эволюционирующую сферу ИКТ. Международная информационная безопасность не должна характеризоваться односторонним диктатом отдельных стран, обязанность государств воздерживаться от атак на критические информационные инфраструктуры должна быть четко закреплена, а нормативная база должна быть достаточно развитой, чтобы давать четкую правовую оценку и должным образом реагировать на проявления агрессии в информационной сфере, исходя из незыблемости основополагающих принципов международного права: невмешательство во внутренние дела государств и неприменение силы и угрозы силой.

Работа завершается комплексным обзором основных внешнеполитических документов России в сфере МИБ и соответствующих направлений внешней политики Российской Федерации. Из представленного анализа видно, что Россия четко и последовательно придерживается своего подхода к выработке общих правил ответственного поведения в глобальном информационном пространстве, основанном на приоритетной роли международных механизмов ООН. Эффективное и устойчивое функционирование глобальной информационной системы при обеспечении безопасности государств возможно только в том случае, если конвенции в сфере МИБ будут иметь универсальный характер – это потребует ряда важных реформ, включая институционализацию управления Интернетом на основе равноправного участия всего мирового сообщества.

В развитие описанного подхода Е.С. Зиновьева формулирует политические рекомендации по дальнейшему развитию внешней политики России в информационной сфере.

Монографию Е.С. Зиновьевой «Международная информационная безопасность: проблемы многостороннего и двустороннего сотрудничества» можно рекомендовать к ознакомлению всем интересующимся вопросами современных тенденций в международном регулировании сферы ИКТ. Комплексный характер и грамотно структурированное изложение делает ее интересной как в самостоятельном качестве, так и в виде базы для углубленных исследований вопросов, затронутых в ее главах.

Работа хорошо высвечивает сохраняющиеся проблемы, связанные с попытками США сохранить доминирующее положение в вопросах МИБ и продолжить диктовать международную повестку в этой сфере, встраивая желаемую для них конфигурацию МИБ в т.н. «Международный порядок, основанный на правилах». Принимая во внимание озвученные автором сложности,

возникающие при сопряжении вопросов МИБ и международного права, такой подход размывает принцип верховенства международного права в регулировании межгосударственных взаимодействий [5. P. 228-240], а потому категорически неприемлем как для России, так и для других стран, претендующих на политическое и экономическое лидерство в многополярном миропорядке.

Литература:

1. Хабидулина Е. Российский суд оштрафовал Google на 4 млрд. рублей за неуплату штрафа ФАС // Forbes. 27 июня 2023.
2. Greenwood F. The Drone War In Ukraine Is Cheap, Deadly, and Made in China // Foreign Policy. February 16. 2023.
3. Hewson J. A Private Company Is Using Social Media to Track Down Russian Soldiers // Foreign Policy. March 2. 2023.
4. Kopfstein J. Stuxnet virus was planted by Israeli agents using USB sticks, according to new report // The Verge. April 13. 2012.
5. Lavrov S.V. On Law, Rights and Rules // Russia in Global Affairs. 19(3). 2021.
6. Luckenbaugh J. U.S. Ability to Withstand Chinese, Russian Cyberattacks Questioned // National Defense. July. 1. 2023.

THEORETICAL AND PRACTICAL ASPECTS OF INTERNATIONAL INFORMATION SECURITY UNDER CURRENT CONDITIONS

Book Review: *Zinovieva E.S., 2021. International information security: Problems of bilateral and multilateral cooperation. Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs of the Russian Federation, 280 p. ISBN 978-5-9228-2454-5*

Dmitriy R. Fatykhov,
post-graduate student,
MGIMO University,
Moscow, Russia

Ключевые слова:
международная безопасность, международная информационная безопасность, кибербезопасность, информационно-коммуникационные технологии, международные организации, международное сотрудничество

Keywords:
international security, international information security, cybersecurity, information and communications technology, international organizations, international cooperation

References:

1. Habidulina E., 2023. Rossijskij sud oshtrafoval Google na 4 mlrd rublej za neuplatu shtrafa FAS [Russian court fines Google 4 billion roubles for failing to pay FAS fine]. *Forbes*. June 27.
2. Greenwood F., 2023. The Drone War In Ukraine Is Cheap, Deadly, and Made in China. *Foreign Policy.* February 16.
3. Hewson J., 2023. A Private Company Is Using Social Media to Track Down Russian Soldiers. *Foreign Policy.* March 2.
4. Kopfstein J., 2012. Stuxnet virus was planted by Israeli agents using USB sticks, according to new report. *The Verge.* April 13.
5. Lavrov S.V., 2021. On Law, Rights and Rules. *Russia in Global Affairs.* № 19(3).
6. Luckenbaugh J., 2023. U.S. Ability to Withstand Chinese, Russian Cyberattacks Questioned. *National Defense.* July 1.