DOI: https://doi.org/10.24833/0869-0049-2024-4-146-161

Исследовательская статья
УДК: 341.3
Поступила в редакцию: 05.09.2024
Принята к публикации: 19.11.2024

Юлия Владимировна ПУЗЫРЕВА
Московский университет МВД России имени В.Я. Кикотя
Академика Волгина ул., д. 12, Москва, 117997, Российская Федерация
yuliya_dugina@mail.ru
ORCID: 0000-0003-4448-2200

МЕЖДУНАРОДНО-ПРАВОВАЯ КВАЛИФИКАЦИЯ МЕТОДОВ И СРЕДСТВ ВЕДЕНИЯ ВОЙНЫ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

ВВЕДЕНИЕ. *В современном мире ввиду нарастающих тенденций по милитаризации информационного пространства военные действия в данной сфере становятся реальностью и перспективой по ряду оперативных, тактических и иных преимуществ в сравнении с военными действиями в традиционных формах в пределах классических театров войны. Информационное военное противоборство будет осуществляться посредством использования нового вида оружия – информационного, которое не вписывается в устоявшуюся парадигму подходов к традиционному оружию, что, безусловно, порождает много вопросов и противоречивых экспертных мнений, однако остро нуждается в дальнейшей разработке и комплексном исследовании.*

МАТЕРИАЛЫ И МЕТОДЫ. *Учитывая многокомпонентность изучаемой темы, проведенное исследование базируется на результатах анализа научных трудов российских и зарубежных правоведов по международному гуманитарному праву (далее – МГП), экспертов в области военного дела, специалистов в сфере информационных технологий. Автор также исследует ключевые международные договоры по МГП, по тематике международной информационной безопасности (далее – МИБ), которые в своей совокупности формируют основы международно-правовой квалификации информационного оружия как средства ведения войны в условиях постепенной адаптации норм МГП к ситуациям враждебного использования информационного пространства. При проведении исследования были использованы аналитические и обзорные материалы Международного Комитета Красного Креста (далее – МККК) по проблематике кибероперации во время вооруженного конфликта. Методологическую основу составляют общенаучные и специальные методы исследования.*

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ. *Проанализированы две концепции, отражающие подходы к МИБ и угрозам в данной сфере через призму «кибер» тематики и информационного аспекта, в рамках каждой из которых формируется специфическая терминология, включая подходы к определению методов и средств ведения военных действий. Основой отечественной доктрины является информационная повестка безопасности, что определило разработку дефиниции «информационного оружия» и изучение его статуса как перспективного средства ведения войны в информационном пространстве. Представляется значимым выявление и обобщение доктринальных тенденций по квалификации информационного оружия как обычного оружия*

или оружия массового уничтожения, а также установление новых подходов по регулированию разработки и использования информационного оружия в вооруженных конфликтах.

ОБСУЖДЕНИЯ И ВЫВОДЫ. *В статье представлены авторские объективные оценки сложившихся доктринальных подходов как отечественных, так и зарубежных ученых по вопросу международно-правовой квалификации методов и средств ведения войны в информационном пространстве в целом и информационного оружия как средства ведения войны, в частности. Отдельно рассмотрены международные договоры по МГП и МИБ в части возможности применения их положений для регулирования ограничения поведения воюющих сторон в информационном противоборстве с учетом определенной адаптации норм МГП к условиям враждебного использования информационных технологий. Выявлены перспективы дальнейшего развития доктрины МГП по регулированию разработки и использования информационного оружия в вооруженных конфликтах.*

КЛЮЧЕВЫЕ СЛОВА: *информационное пространство, война в информационном пространстве; международное гуманитарное право; методы и средства ведения войны; информационное оружие; концепция «неявного оружия»; обычное оружие; новые виды оружия*

ДЛЯ ЦИТИРОВАНИЯ: Пузырева Ю.В. 2024. Международно-правовая квалификация методов и средств ведения войны в информационном пространстве. – *Московский журнал международного права.* № 4. С. 146–161. DOI: https://doi.org/10.24833/0869-0049-2024-4-146-161

Автор заявляет об отсутствии конфликта интересов.

THEATER OF WAR AND INTERNATIONAL LAW

DOI: https://doi.org/10.24833/0869-0049-2024-4-146-161

Research article
UDC: 341.3
Received: 5 September 2024
Approved: 19 November 2024

Yuliya V. PUZYREVA
Kikot Moscow University of the Ministry of Internal Affairs of Russia
12, Akademika Volgina St., Moscow, Russian Federation, 117997
yuliya_dugina@mail.ru
ORCID: 0000-0003-4448-2200

INTERNATIONAL LEGAL CHARACTERIZATION OF METHODS AND MEANS OF WARFARE IN THE INFORMATION SPACE

INTRODUCTION. *In the world, due to the growing trends in the militarization of the information space, military actions in this area are becoming a reality and a prospect for a number of operational, tactical and other advantages in comparison with military actions in traditional forms within the classical theaters of war. Information military confrontation will be carried out through the use of a new type of weapon – information, which does not fit into the established paradigm of approaches to traditional weapons, which, of*

course, gives rise to many questions and contradictory expert opinions, but is in dire need of further development and comprehensive research.

MATERIALS AND METHODS. *Given the complexity and multi-component nature of the topic under study, the study is based on the results of the analysis of scientific works by Russian and foreign legal scholars on international humanitarian law (IHL), experts in the field of military affairs, and specialists in the field of information technology. The author also examines key international treaties on IHL, on the topic of international information security (IIS), which together form the basis for the international legal qualification of information weapons as a means of waging war in the context of the gradual adaptation of IHL norms to situations of hostile use of information space. In conducting the study, analytical and review materials of the ICRC on the issue of cyber operations during an armed conflict were used. The methodological basis is made up of general scientific and special research methods.*

RESEARCH RESULTS. *The results of the conducted study established two formed concepts reflecting approaches to IIS and threats in this area through the prism of cybertopics and information aspect, within the framework of each of which specific terminology is formed, including approaches to defining methods and means of conducting military operations. It was determined that the domestic doctrine is built around the information agenda of security, which determined the development of the definition of "information weapons" and the study of its status as a promising means of waging war in the information space. It seems significant to identify and generalize doctrinal trends in the qualification of information weapons as weapons of mass destruction or conventional weapons, as well as to establish new approaches to regulating the development and use of information weapons in armed conflicts.*

DISCUSSION AND CONCLUSIONS. *The article presents the author's objective assessments of the existing doctrinal approaches of both domestic and foreign scientists on the issue of international legal qualification of methods and means of waging war in the information space in general and information weapons as a means of waging war in particular. Separately, international treaties on IHL and IIS are considered in terms of the possibility of applying their provisions to regulate the restriction of the behavior of warring parties in information warfare, taking into account a certain adaptation of IHL norms to the conditions of hostile use of information technologies. Prospects for further development of the IHL doctrine on regulating the development and use of information weapons in armed conflicts are identified.*

KEYWORDS: *information space, war in the information space; international humanitarian law; methods and means of warfare; information weapons; the concept of "invisible weapons"; conventional weapons; new types of weapons*

FOR CITATION: Puzyreva Yu.V. International legal characterization of methods and means of warfare in the information space. – *Moscow Journal of International Law.* 2024. No. 4. P. 146–161. DOI: https://doi.org/10.24833/0869-0049-2024-4-146-161

The author declares the absence of conflict of interest.

Введение

В современном мире действующие принципы и нормы международного права находятся в состоянии постоянной адаптации к изменяющимся условиям, в которых происходит развитие межгосударственных отношений, включая стремительные процессы «интернетизации» государств под воздействием научно-технического прогресса[1]. Происходящие тенденции побуждают государства обсуждать на различных международных площадках вопросы использования информационного пространства и информационно-коммуникационных технологий (далее – ИКТ) в контексте мирного функционирования, во благо развития цивилизации и построения глобального информационного общества [Капустин 2017:51]. Однако необходимо отметить и тревожные опасения, связанные

[1] Касенова М.Б. *Правовое регулирование трансграничного функционирования и использования Интернета:* автореф. дис. … д-ра юрид. наук. М., 2016. С. 3.

с использованием информационного пространства в противоправных целях как отдельными лицами, так и государствами.

Для формирования правовых универсальных основ противодействия таким угрозам под эгидой Организации Объединенных Наций (далее – ООН) на протяжении длительного времени формировались два направления переговорного процесса по вопросам укрепления международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, а также по вопросам проблематики МИБ и обеспечения ответственного поведения государств в информационном пространстве. Первый вектор многолетнего сотрудничества (инициированный Российской Федерацией в 1998 г.) завершился принятием в 2024 г. под эгидой *Специального межправительственного комитета ООН открытого состава по разработке всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях*[2] универсального международно-правового акта по борьбе с информационной преступностью, проект которого был представлен Генеральной Ассамблее ООН для обсуждения в ходе ее 78-й сессии в 2024 г.[3] В свою очередь проблематика МИБ на современном этапе успешно обсуждается на полях (также созданной по инициативе Российской Федерации) *Рабочей группы открытого состава ООН по вопросам безопасности в сфере использования ИКТ и самих ИКТ*[4], в рамках которой разрабатываются институционные механизмы сотрудничества государств в данной области, концепция будущей конвенции ООН об обеспечении МИБ[5] ввиду угроз использования новой информационной сферы построения отношений в военно-политических целях. Так, в концепции Конвенции ООН об обеспечении международной информационной безопасности[6] одной из существенных угроз МИБ обозначено использование государствами ИКТ в военно-политической и иных сферах в целях подрыва (ущемления) суверенитета, нарушения территориальной целостности, общественной и экономической стабильности суверенных

[2] Идея разработать конвенцию о борьбе с использованием информационных технологий в преступных целях получила одобрение в ходе 74-й сессии Генеральной Ассамблеи ООН. Инициатором соответствующей резолюции выступила Россия. В принятой тогда резолюции «Противодействие использованию информационно-коммуникационных технологий в преступных целях» было предложено учредить специальный межправительственный комитет для разработки международной конвенции. См. подробнее: ООН. Резолюция Генеральной Ассамблеи ООН 74/29 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Дос. ООН A/RES/74/29. – *Официальный сайт ООН.* URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/410/10/PDF/N1941010.pdf?OpenElement (дата обращения: 12.09.2024).

[3] Проект конвенции ООН против киберпреступности. Укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям. Специальный комитет по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях. Возобновленная заключительная сессия. Нью-Йорк, 29 июля – 9 августа 2024 г. – *Официальный сайт ООН.* URL: https://documents.un.org/doc/undoc/gen/v24/055/08/pdf/v2405508.pdf (дата обращения: 12.09.2024).

[4] В соответствии с резолюцией Генеральной Ассамблеи ООН №75/240 от 31 декабря 2020 г., а также с учетом итогов Рабочей группы ООН открытого состава (далее – РГОС) по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности в 2021 г. была создана новая РГОС по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025 гг. Запущенная по инициативе России РГОС является единственным открытым и всеохватным переговорным механизмом по проблематике МИБ под эгидой ООН, который позволит в долгосрочной перспективе вести системные и тематически специализированные переговоры по всему спектру вопросов обеспечения МИБ. См. подробнее: [Пузырева, Нефедов, Эриашвили 2024].

[5] В 2023 г. Россия представила обновленную версию концепции Конвенции ООН по международной информационной безопасности, которая призвана заложить прочную правовую основу мирного развития глобальной ИКТ-среды. См. подробнее: Об итогах шестой сессии Рабочей группы открытого состава ООН по вопросу международной информационной безопасности. – *Национальная ассоциация международной информационной безопасности (НАМИБ).* URL: https://namib.online/2023/12/ob-itogah-shestoj-sessii-rabochej-gruppy-otkrytogo-sostava-oon-po-mezhdunarodnoj-informacionnoj-bezopasnosti/ (дата обращения: 12.09.2024).

[6] Обновленная концепция Конвенции ООН об обеспечении международной информационной безопасности, предложенная Российской Федерацией (соавторы: Республика Беларусь, Боливарианская Республика Венесуэла, Корейская Народно-Демократическая Республика, Республика Никарагуа, Сирийская Арабская Республика). – *Национальная ассоциация международной информационной безопасности (НАМИБ).* URL: https://namib.online/wp-content/uploads/2023/07/Обновленная-Концепция-Конвенции-ООН-о-МИБ-русск.pdf (дата обращения: 12.09.2024).

государств, вмешательства в их внутренние дела, а также осуществления в глобальном информационном пространстве иных действий, препятствующих поддержанию международного мира и безопасности, проведение компьютерных атак на информационные ресурсы государств, в том числе на критическую информационную инфраструктуру.

Такие угрозы вполне обоснованны, поскольку не все государства стремятся к выработке унифицированных подходов по регулированию мирного использования ИКТ и информационного пространства в целом. Так, информационное пространство многими государствами[7] рассматривается как потенциальный *театр военных действий,* под которым необходимо понимать пространственные пределы, в которых воюющие государства могут вести военные действия в ходе вооруженного конфликта.

Современное информационное военное противоборство будет осуществляться посредством использования нового вида оружия – информационного, которое не вписывается в устоявшуюся парадигму подходов к традиционному или конвенционному оружию, что, безусловно, порождает много вопросов и противоречивых экспертных мнений, однако остро нуждается в разработке и исследовании.

В связи с этим возникает вопрос о применимости термина «средства и методы ведения войны» к столкновениям государств в информационном пространстве в рамках вооруженного конфликта. Кроме того, вызывает научный и практический интерес возможность толкования и применения принципа МГП об ограничении воюющих в выборе методов и средств ведения войны к таким информационным ресурсам и возникающим отношениям.

Прежде чем представить анализ указанных вопросов, необходимо подчеркнуть, что несмотря на повышенное внимание государств, международных правительственных и неправительственных организаций к киберпроблематике, уже более 30 лет ни на международно-правовом уровне, ни на уровне отечественной и зарубежной доктрины не удается выработать универсальные подходы к определению ключевых терминов в кибертехнологической области военных действий, как и в целом в сфере МИБ.

В общей сложности все имеющиеся концепции возможно разделить на две группы: с характеристикой «кибер» и с характеристикой «информационные». Представители «кибер» подхода акцентируют свое внимание на технических компонентах безопасности и существующих угрозах в данной сфере [Verhelst, Filling 2020:141-172; Sharp 1999; Rattray 2001][8]. Этот подход принято считать западным. Наиболее точно его суть раскрыта в Таллиннском руководстве по международному праву, применимому к кибероперациям (далее – Таллинское руководство), в котором ведется речь о киберпространстве, кибернападениях и кибероружии [Tallinn Manual … 2017].

Параллельная концепция, характеризующая международную безопасность через «информационную призму», подразумевает под собой комплексный учет не только технических, но и политико-идеологических, психологических аспектов[9]. Российская Федерация при поддержке своих партнеров на важных международных площадках отстаивает широкий подход ко всем дефинициям в сфере МИБ[10], закрепляя свои позиции в региональных договорах по МИБ, принятых под эгидой международных региональных организаций, участницей которых

[7] Согласно Стратегии национальной безопасности США 2022 г., киберпространство рассматривается как новая сфера вооруженной борьбы – область боевых действий наравне с воздухом, сушей, морем и космосом. В соответствии с положениями «Белой книги по вопросам национальной безопасности и обороны» Франции 2013 г., киберпространство также признается сферой вооруженного противоборства наряду с земной поверхностью, воздушной средой, мировым океаном и космосом. Согласно оборонной стратегии Китая 2019 г., киберпространство является ключевой областью национальной безопасности, а также экономического и социального развития. В связи с этим китайские военные разработали методы и средства защиты кибербезопасности страны и создали силы обороны киберпространства, соизмеримые с международным статусом Китая и совместимые со статусом кибердержавы. Начиная с 2002 г. НАТО, активным образом развивает свои возможности по применению ИКТ в военных целях и вырабатывает правовые условия использования таких технологий и информационного пространства в будущих вооруженных конфликтах. См. подробнее: [Конохов 2023:218-222].

[8] ISO/IEC 27032:2023/ Cybersecurity – Guidelines for Internet security. – *International Organization for Standardization-https.* URL://www.iso.org/standard/76070.html (accessed date: 19.10.2024).

[9] Международная информационная безопасность: подходы России. М.: МГИМО Университет, 2021. 32 с.

[10] Применение норм ответственного поведения государств в ИКТ--среде и международное сотрудничество (реферат по результатам исследования). М.: НАМИБ, 2022. 19 с.

является Российская Федерация[11], а также в двусторонних международных договорах Российской Федерации с зарубежными государствами в области обеспечения МИБ[12]. Именно в рамках данной концепции будет проведено исследование в статье, включая подход к используемой терминологии.

Средства или методы ведения войны в информационном пространстве?

По справедливому замечанию профессора И.И. Котлярова, в источниках и современной доктрине МГП не дается единого определения понятия «средства ведения войны» и «метода ведения войны», зачастую не проводится различие между методами и средствами уничтожения противника, что затрудняет квалификацию боевых действий воюющих сторон в случае противоправного применения ими сил и средств [Котляров 2011:31]. Вместе с тем анализ доктрины МГП позволяет выявить общие подходы ученых в части трактовки данных понятий. Так по мнению И.И. Котлярова, к средствам ведения войны необходимо относить оружие и боевую технику, применяемые вооруженными силами противоборствующих сторон для уничтожения живой силы, военных объектов и иных материальных средств противника, подавления его к сопротивлению [Котляров 2011:31]. Г.М. Мелков к средствам ведения войны также традиционно относит оружие, боевую технику и иные средства, применяемые для нанесения вреда и поражения противнику, которые многократно усиливают страдания людей, причиняют излишние повреждения и де лают смерть неизбежной [Мелков 1988:29-31]. Таким образом, *средством ведения войны* является определенный вид вооружения, компоненты его технического обеспечения и иная боевая техника.

Подходы к понятию «методы ведения войны» нашли отражение в трудах профессора М.И. Догеля, который отождествлял их со способами ведения войны и подразумевал «все те действия, все те средства, при помощи которых комбатанты одной из воюющих сторон стараются уничтожить силы сопротивления другой; такими средствами ослабить сопротивление врага являются физическая сила, насильственные действия, хитрость и обман» [Догель 1894:256].

Несмотря на разнообразие доктринальных подходов, И.И. Котляров отмечает объективную необходимость в понимании под *методами войны* определенных способов использования сил и средств ведения войны [Котляров 2009:46].

Что касается информационного оружия и в целом средств и методов ведения войны в информационном пространстве, то в данном вопросе необходимо отметить сложные и разноплановые взгляды среди отечественных и зарубежных ученых. Так, в настоящее время сформировано мнение, что нападения государств в информационном пространстве будет осуществляться при помощи информационного оружия, за которым необходимо признать статус нового вида оружия, а значит, и возможность квалификации его как средства ведения военных действий [Международное гуманитарное право… 2020:5]. При этом, как отмечают исследователи – сторонники киберконцепции, термин «кибероружие» является узким, поэтому его целесообразно заменить на категорию «киберсредства» [Гаркуша-Божко 2021:64-82]. Ряд ученых отстаивает более широкий и смешанный подход, определяя «информационные операции, проводимые с помощью информационного оружия», как новый метод ведения войны или как новый вид оружия [Шинкарецкая 2013:121]. Отдельные юристы-международники применяют общую трактовку, вводя в научный оборот категорию «методы и средства ведения войны в информационном пространстве» с предложением по дальнейшему включению указанной терминологии в международно-правовые документы [Конохов 2023:218]. Таким образом, в отдельных авторских концепциях отсутствует прямая характеристика информационного оружия как метода или средства ведения войны, хотя в МГП под данными

[11] Например, Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности 2009 г., Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности 2013 г., Соглашение о сотрудничестве государств – членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности 2017 г.

[12] В настоящее время заключено более тридцати таких соглашений от имени Правительства Российской Федерации с Правительствами иностранных государств. Двусторонние договоры размещены на сайте МИД России.

терминами понимаются разнопорядковые категории, а также прослеживается непреобладающая тенденция использования термина «кибероперации» с выходом на их квалификацию как методов ведения войны.

Как в отечественной [Талимончик 2016][13], так и в зарубежной доктрине [Franklin 2018; Pool 2013] наиболее распространенным и устоявшимся термином является «информационное оружие» («кибероружие»). Кроме того, данное понятие нашло отражение в некоторых международных договорах и концептуальных решениях государств. Так, в Соглашении между Правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 2009 г. содержится закрепленная дефиниция: «*информационное оружие*» – информационные технологии, средства и методы, применяемые в целях ведения информационной войны. Под эгидой СНГ в 2013 г. также было принято Соглашение о сотрудничестве в области обеспечения информационной безопасности, содержащее практически аналогичные положения по проблематике использования информационных технологий и достижений в военных целях.

Согласно Таллинскому руководству термин «оружие» применим к кибертехнологиям; их можно рассматривать таковыми в рамках концепции нового вида оружия и относить к нему следует «кибернетические средства ведения войны, которые по своей конструкции, использованию или предполагаемому использованию способны привести к травмам или гибели людей; или повреждению или уничтожению объектов, т. е. привести к последствиям, необходимым для квалификации кибероперации как нападения»[14] [Tallinn Manual … 2017:218].

В Основах военной политики Союзного государства в области международной информационной безопасности 2021 г. также закреплена дефиниция «информационное оружие» как ИКТ, предназначенных для воздействия на информационные объекты противника, при котором объект полностью или частично (временно) теряет способность к нормальному функционированию (выполнению боевой задачи) (п. 4)[15]. Более того, Российская Федерация и Республика Беларусь заложили в рамках Основ военной политики 2021 г. перспективные задачи по регулированию «международного режима нераспространения информационного оружия».

Признавая доктринальный и правовой подход к квалификации информационного оружия как средства ведения войны, необходимо определить практические сложности в его реализации. Как отмечает А.А. Стрельцов, информационные технологии или ИКТ не обладают признаками оружия в его традиционном понимании[16]. Он соглашается с перспективной регламентацией статуса информационного оружия как средства ведения военных действий только после полной адаптации МГП к ситуациям военного противоборства в информационном пространстве[17]. В качестве практического примера такой адаптации для разрешения вопроса по статусу информационного оружия как средства ведения войны предлагается *концепция «неявного оружия»*, согласно которой тот или иной механизм, устройство, средство может приобретать свойства оружия, когда используется для нанесения поражения живой силе и военной техники неприятеля[18]. Таким образом, автор допускает

[13] Стрельцов А.А. О проблемах адаптации международного права к информационным конфликтам. – *Информационно-аналитический портал Digital.Report.* URL: https://digital.report/problemyi-adaptatsii-mezhdunarodnogo-prava-k-informatsionnyim-konfliktam/ (дата обращения: 14.10.2024).

[14] Цит. по: Карасев П. США наращивают киберсилы. – *Российский совет по международным делам.* URL: https://russiancouncil.ru/analytics-and-comments/analytics/ssha-narashchivayut-kibersily/ (дата обращения: 14.10.2024).

[15] Основы военной политики Союзного государства в области международной информационной безопасности, утверждены министрами обороны Российской Федерации и Республики Беларусь в октябре 2021 г. – *Министерство обороны Российской Федерации.* URL: https://doc.mil.ru/documents/quick_search/more.htm?id=12422292@egNPA (дата обращения: 14.10.2024).

[16] Стрельцов А.А. О развитии международного права кибер-конфликтов. – *Информационно-аналитический портал Digital.Report*. URL: https://digital.report/pravo-cyber-konfliktov/ (дата обращения: 14.10.2024).

[17] Стрельцов А.А. О проблемах адаптации международного права к информационным конфликтам. – *Информационно-аналитический портал Digital.Report.* URL: https://digital.report/problemyi-adaptatsii-mezhdunarodnogo-prava-k-informatsionnyim-konfliktam/ (дата обращения: 14.10.2024).

[18] Данная концепция базируется на прецеденте, созданном резолюциями Совета Безопасности ООН по результатам обсуждения трагических событий, произошедших в США 11 сентября 2001 г., когда в качестве «неявного оружия» признавался летательный аппарат.

в перспективе квалификацию статуса информационного оружия как средства ведения военных действий с учетом формирования новых позиций государств в части расширения перечня запрещенных видов оружия и способов его использования при неправомерном силовом использовании информационных средств против территориальной целостности или политической независимости какого-либо государства [Стрельцов 2014:75-78].

Квалификация информационного оружия как обычного оружия или оружия массового уничтожения

Необходимо отметить, что появление в современном мире информационного оружия отражает тенденцию, в рамках которой государства десятилетиями и веками находятся в поиске наиболее передовых средств и технологий ведения вооруженной борьбы. Однако при этом такие военные новации всегда подлежали оценке не только с точки зрения эффективности военной стратегии, но и уровня угроз от их применения, наличия чрезмерных разрушительных, непоправимых, губительных или негуманных последствий от его использования. Достаточно вспомнить эволюцию ключевых международных договоров по ограничению воюющих в выборе средств ведения войны, принятие которых следовало за появлением и апробацией разрабатываемых государствами видов вооружений.

Международные договоры, посвященные средствам ведения войны, возможно условно разделить на соглашения, запрещающие использование отдельных видов оружия, характеризуемых как *оружие массового уничтожения*[19], и соглашения по ограничению применения *обычного вооружения,* которое может наносить чрезмерные повреждения или действие которых носит неизбирательный характер[20]. В данном контексте следует отметить дискуссионность точки зрения, что все остальные виды вооружения, не подпадающие под нормативное регулирование данных актов, считаются разрешенным к использованию на поле боя[21]. Так, еще в рамках Гаагских конференций мира государства-разработчики международных договоров о правилах ведения войны осознавали, что на нормативном уровне невозможно в полной мере разрешить все вопросы обеспечения защиты как вооруженных сил воюющих сторон, так и гражданского населения. Именно тогда была сформулирована знаменитая оговорка Мартенса, разработанная и предложенная Ф.Ф. Мартенсом в ходе переговоров в качестве спонтанного компромисса, которая и сегодня по-прежнему считается важным положением МГП, позволяющим восполнить пробелы правового регулирования ведения военных действий и отсылающим к признанным народами обычаям, принципу гуманности и требованиям общественного сознания[22].

Кроме того, в современном МГП выработаны нормы, учитывающие развитие научно-технического прогресса в части разработки современных методов и средств ведения войны, а также закрепляющие критерии для оценки правомерности их применения. В частности, речь идет о ст. 36 Дополнительного протокола I 1977 г. (далее – ДП I 1977 г.) «Новые виды оружия», согласно которой «при изучении, разработке, приобретении или принятии на вооружение новых

[19] В первую очередь речь идет о таких договорах, как: Конвенция о запрещении запасов бактериологического (биологического) и токсинного оружия и об их уничтожении 1972 г., Конвенция о запрещении военного или любого иного враждебного использования средств воздействия на природную среду 1977 г., Конвенция о запрещении разработки, производства, накопления и применения химического оружия и о его уничтожении 1993 г., Договор о нераспространении ядерного оружия 1968 г., Договор о запрещении ядерного оружия 2017 г.

[20] В частности, речь идет о Конвенции о запрещении или ограничении применения конкретных видов обычного оружия, которые могут считаться наносящими чрезмерные повреждения или имеющими неизбирательное действие 1980 г. и Протоколах к ней, регламентирующих статус наземных мин, мин-ловушек, зажигательных устройств, ослепляющего лазерного оружия и взрывоопасных пережитков войны.

[21] Так, профессор Л.Ф.Л. Оппенгейм, отмечал, что за исключением средств, применение которых специально запрещено договорами или обычаями, все другие средства лишения жизни или ранения комбатантов, которые существуют в настоящее время или могут быть изобретены в будущем, являются законными. См.: [Оппенгейм 1949:346].

[22] «Оговорка Мартенса» представляет собой следующее положение: «В случаях, не предусмотренных принятыми ими постановлениями, население и воюющие остаются под охраною и действием начал международного права, поскольку они вытекают из установившихся между образованными народами обычаев, из законов человечности и требований общественного сознания» [Ivanenko 2022:1708-1724].

видов оружия, средств или методов ведения войны Высокая Договаривающаяся Сторона должна определить, подпадает ли их применение, при некоторых или при всех обстоятельствах, под запрещения, содержащиеся в настоящем Протоколе или в каких-либо других нормах международного права, применяемых к Высокой Договаривающейся Стороне»[23].

Таким образом, любые создаваемые в современном мире новейшие военные технологии и виды вооружения, априори находятся в рамках международно-правового регулирования. Бесспорно, данный тезис имеет отношение и к разрабатываемому более чем ста двадцатью государствами информационному оружию[24].

Рассмотрим доктрину международного права и перспективы развития международно-правовых основ по квалификации информационного оружия как обычного оружия или оружия массового уничтожения.

Информационное оружие как оружие массового уничтожения

К настоящему времени в международном праве не выработано универсального понятия «оружия массового уничтожения» (далее – ОМУ), что связано с рядом военно-политических причин [Синякин 2012:13]. Однако на уровне доктрины международного права удалось сформировать критерии, с помощью которых оружие может быть идентифицировано в качестве ОМУ (целевой критерий, критерий разрушительности, неизбирательности, массовости, поражающие свойства новых видов и систем ОМУ и др.) [Синякин 2012:13; Котляров 2011: 41].

По мнению И.И. Котлярова, ОМУ включает виды оружия, способные при ограниченном привлечении сил и средств вызвать массовые потери и разрушения вплоть до необратимых изменений свойств окружающей среды [Котляров 2011:41]. Традиционно в качестве ОМУ принято рассматривать ядерное, химическое, биологическое оружие, а также средства воздействия на природную среду в военных или иных враждебных целях[25]. В отношении существующих и признанных видов ОМУ сформированы международно-правовые режимы нераспространения, запрета разработки, производства и накопления, применения[26].

Ученые допускают появление и других видов ОМУ, основанных на иных принципах действия, нежели традиционные виды, как, например, оружие, основанное на новых физических принципах, а также оружие на основе нанотехнологии[27]. Кроме того, к новым видам ОМУ, чей статус пока не нашел международно-правовой регламентации, относят лучевое и радиологическое оружие, обычные бомбы с урановыми сердечниками и др. [Сазонова 2018:62].

В продолжение дискуссии о новых видах ОМУ следует отметить научный подход, сформированный в западной доктрине международного права, о возможности классификации по крайней мере некоторых разновидностей информационного оружия[28] как ОМУ, в частности, тех его видов, которые направлены на крупномасштабное (физическое) уничтожение любой инфраструктуры, например, путем воздействия на критическую инфраструктуру государств [Hatch 2018; Kumar 2013; Kudláčková 2020; Lee

[23] Дополнительный протокол к Женевским конвенциям от 12 августа 1949 г., касающийся защиты жертв международных вооруженных конфликтов, от 8 июня 1977 г. (Протокол I). – *НПП Гарант*. URL: https://base.garant.ru/2540377/ (дата обращения: 12.10.2024).

[24] Генштаб сообщил, что более 120 стран разрабатывают информационное оружие. – *Сетевое издание РИА новости*. URL: https://ria.ru/20240207/oruzhie-1925887168.html (дата обращения: 12.10.2024 г.).

[25] В состав ОМУ также входит оборудование, средства доставки, боеприпасы и устройства, специально предназначенные для приведения в действие ОМУ или являющиеся их неотъемлемой частью.

[26] См.: Конвенция о запрещении запасов бактериологического (биологического) и токсинного оружия и об их уничтожении 1972 г.; Конвенция о запрещении военного или любого иного враждебного использования средств воздействия на природную среду 1977 г.; Конвенция о запрещении разработки, производства, накопления и применения химического оружия и о его уничтожении 1993 г.; Договор о нераспространении ядерного оружия 1968 г.; Договор о запрещении ядерного оружия 2017 г.

[27] Оружие на новых физических принципах. – Военная энциклопедия. С.Б. Иванов. М.: Военное издательство, 2002. Т. 6. С. 158.

[28] Вопросу классификаций, видов и типов информационного оружия посвящено значительное количество работ специалистов в области военного дела. См., напр.: [Макаренко 2016; Шеховцов, Кулешов 2012; Kumar 2013].

2024]. Имеются отдельные научные разработки, в которых проводится сравнительно-правовой анализ ядерного оружия и информационного оружия, результаты которого позволили автору признать их схожесть по ряду разрушающих критериев [Krepinevich 2012].

Среди серьезных опасностей, угроз и губительных последствий, связанных с применением информационного оружия, позволяющих ученым рассматривать его как ОМУ, определены следующие: непредсказуемость воздействия на системы и сети, которые не считаются целями; атака систем принимающей страны по принципу «эффекта бумеранга», включая гражданскую инфраструктуру, необходимую для выживания[29]; непрогнозируемые и незащищенные возможности обратного проектирования исходного кода со стороны злоумышленников, включая террористические организации, что приведет к неконтролируемым процессам разработки и распространения новых киберугроз, которые будет трудно устранить; сложности с установлением источника прямого кибернападения, что позволяет использовать информационное оружие «под прикрытием»; латентность процесса разработки и этапа внедрения информационного оружия [Kumar 2013].

Однако отдельные ученые возражают против категорирования информационного оружия как ОМУ на том основании, что оно не может напрямую ранить или убивать людей, разрушать объекты так же, как традиционные виды оружия, явно не соответствует юридическим и техническим определениям ОМУ, поэтому статус информационного оружия как ОМУ серьезно преувеличен [Carr 2013: 34-37].

Вызывает ряд вопросов мнение экспертов Центра по изучению оружия массового поражения Национального университета обороны США, отмечающих, что в будущем потенциал кибероружия и масштабной кибератаки будет сравним с угрозами от применения ОМУ. Однако на данный момент для Соединенных Штатов было бы неуместным и, возможно, невыгодным применять к кибероружию квалификацию как ОМУ, поскольку функционируют определенные международно-правовые режимы нераспространения и контроля за такими видами вооружений, а признание за кибероружием статуса ОМУ приведет к применению этих положений. В связи с этим эксперты отмечают, что пока США не пришли к однозначному выводу, хотят ли они инициировать разработку международного режима, ограничивающего военный потенциал киберпространства, или максимально использовать ресурсы своих кибервозможностей, в которых они являются признанным мировым лидером, нет никаких преимуществ в том, чтобы рассматривать кибероружие как ОМУ [The Future of Weapons … 2014:7]. В случае перспективного признания за информационным оружием статуса ОМУ ученые предлагают выработать концепцию ответного ядерного удара в отношении источника кибератак [The Future of Weapons… 2014:42].

Параллельно с разработкой в зарубежной доктрине вопроса квалификации информационного оружия как ОМУ вырабатывается концепция признания за информационным оружием новой категории – *оружия массового разрушения (поражения),* что следует считать новаторским [Arquilla 2021; Clarke, Knake 2011; Ядерное оружие 2013:57][30]. Общий концепт заключается в том, что в отличие от ОМУ такой тип оружия будет нацелен именно на одномоментные, стихийные и масштабные разрушения инфраструктуры государств.

Информационное оружие как обычное оружие

По справедливому замечанию И.И. Котлярова, в международном общем и гуманитарном праве не содержится определения «обычное оружие» [Котляров 2011:39]. В разных литературных источниках к нему относят традиционные

[29] В последнем (шестом) докладе о МГП и проблемах современных вооруженных конфликтов, подготовленном в 2024 г. МККК для Международной конференции Красного Креста и Красного Полумесяца, с озабоченностью отмечена губительная тенденция использования во время вооруженных конфликтов государственными и негосударственными субъектами кибероперациий для выведения из строя гражданской инфраструктуры и систем, особенно гражданских государственных служб, или для нарушения предоставления основных услуг. См. подробнее: Доклад МККК за 2024 г. о МГП и проблемах современных вооруженных конфликтов. – *Официальный сайт МККК*. URL: https://www.icrc.org/en/report/2024-icrc-report-ihl-challenges (дата обращения: 22.10.2024).

[30] Arquilla 2021; Clarke, Knake 2011; Ядерное оружие 2013:57.

виды оружия, боевое применение которых не приводит непосредственно к массовым потерям и разрушениям[31].

Действующие положения международных договоров не запрещают государствам владеть и использовать обычные вооружения. Именно поэтому, когда речь идет об обычных вооружениях, термины «контроль над вооружениями» и «ограничение вооружений» чаще используются, чем «разоружение»[32]. Однако применение некоторых видов обычного оружия могут вызывать озабоченность либо из-за способа их использования, либо из-за их конструкции, что идет вразрез с принципами МГП.

В отечественной доктрине международного права первым комплексным исследованием проблем запрещения или ограничения применения обычного оружия явилась монография профессора И.П. Блищенко «Обычное оружие и международное право», в которой автор не только выявил, что применение обычного оружия большой разрушительной силы в широких масштабах может привести к массовым жертвам среди населения и огромным разрушениям, сравнимым с применением средств массового уничтожения, но и разработал международно-правовые критерии запрещения или ограничения применения отдельных видов обычного оружия [Блищенко 1984].

Современное МГП запрещает или ограничивает применение определенных видов обычных вооружений, чтобы защитить гражданское население от неизбирательного действия и избавить комбатантов от излишних страданий. Одним из основных правовых актов в этой области является Конвенция о запрещении или ограничении применения конкретных видов обычного оружия, которые могут считаться наносящими чрезмерные повреждения или имеющими неизбирательное действие 1980 г. (известная как Конвенция о «негуманном» оружии, далее – КНО), дополненная протоколами, регламентирующими запрет или ограничения на применение наземных мин, мин-ловушек, зажигательных устройств, ослепляющего лазерного оружия и взрывоопасных пережитков войны[33].

Учитывая, что информационное оружие не обладает юридически-признанным статусом ОМУ, допустимо рассмотрение подходов к его квалификации как к обычному оружию, положение которого вполне урегулировано выработанными международными обычными и договорными нормами.

Как справедливо отмечено в одном из рабочих документов МККК по итогам шестой обзорной конференции по КНО 2021 г., новое оружие, средства и методы ведения военных действий, основанные на военном применении новых научных и технических разработок, вполне подпадают под широкую сферу применения КНО 1980 г.[34] Так, в частности, элементы информационного оружия, его технические компоненты, характеристики и особенности, а также использование таких средств в ходе военных действий должны соответствовать закрепленным (в частности, в преамбуле КНО) принципам защиты гражданского населения от военных действий, ненанесения чрезмерных повреждений (в том числе долговременного и серьезного ущерба природной среде), а также непричинения излишних страданий.

Кроме того, не теряют своей актуальности и значимости выработанные в МГП положения по оценке законности новых видов оружия, закрепленные в ст. 36 ДП I 1977 г. А в случаях, если то или иное государство не связано таковыми обязательствами, то, по мнению экспертов МККК, требование проводить правовую

[31] Данное оружие широко используется в условиях конфликтов и охватывают широкий спектр боевой техники, включая боевые танки, боевые бронированные машины, крупнокалиберные артиллерийские системы, боевые самолеты и беспилотные боевые летательные аппараты, боевые вертолеты, военные корабли, ракеты и ракетные пусковые установки, наземные мины, кассетные боеприпасы, стрелковое оружие, осветительное оружие и боеприпасы.

[32] Разоружение. Глобальные вопросы повестки дня. – *Официальный сайт ООН.* URL: https://www.un.org/ru/global-issues/disarmament (дата обращения: 22.10.2024).

[33] Конвенция о «негуманном» оружии – *Официальный сайт МИД России.* URL: https://www.mid.ru/ru/foreign_policy/international_safety/disarmament/obychnye_vooruzheniya/1413307/ (дата обращения: 27.10.2024).

[34] Мнения и рекомендации для шестой обзорной конференции по Конвенции о негуманном оружии Рабочий документ, представленный Международным Комитетом Красного Креста 8 ноября 2021 г. – *Официальный сайт МККК.* URL: https://www.icrc.org/sites/default/files/document_new/file_list/recommendations_ccw_revconf_rus.pdf (дата обращения: 27.10.2024).

экспертизу новых видов оружия также вытекает из обязательства соблюдать нормы МГП[35]. В любом случае государства заинтересованы в оценке законности новых видов оружия, чтобы убедиться, что их вооруженные силы могут вести военные действия в соответствии с принятыми международными обязательствами [Дауст 2002:845-847].

Для повышения эффективности оценки, с точки зрения МГП, гуманитарных последствий разработки новых технологий с целями военного использования и дальнейшего применения на практике в настоящее время МККК занимается пересмотром и обновлением Руководства по проверке соответствия нормам права новых видов оружия, средств и методов ведения войны (Меры по имплементации ст. 36 Дополнительного протокола I 1977 г.) 2006 г.

Несмотря на то что информационные технологии, информационное оружие и иные связанные с ним средства не подпадают под традиционную категорию «оружия», под эгидой SIPRI были проведены комплексные и новаторские исследования о применении в адаптационной форме положений ст. 36 ДП I 1977 г. к новым видам оружия, появление которых связано с развитием технологий, а именно: кибероружия, вооружения с искусственным интеллектом и робототехники [Boulanin 2013]. В исследованиях отмечено, что несмотря на то, что эти три области технологий находятся на разных стадиях развития (от зрелых до все еще формирующихся и экспериментальных), бесспорно, они окажут значительное влияние на будущее военных действий, поскольку способны коренным образом изменить способы применения силы и принятия важных решений на поле боя. Кроме того, несмотря на технические и эксплуатационные различия, военное применение этих областей технологий сопряжено с аналогичными трудностями в том, что касается оценки согласно ст. 36 ДП I 1977 г. Вместе с тем, как отмечают эксперты, провести такую оценку все же возможно.

Своеобразной поддержкой данного тезиса выступает правило 110 Таллиннского руководства 2.0, закрепляющего, что государствам следует проводить юридическую экспертизу «киберсредств ведения войны», и многие государства уже последовали этому примеру (Австралия, Бразилия, Германия, Канада, Швеция и др.)[36].

Таким образом, в теории и практике международного права сформировалось единое понимание, что несмотря на отсутствие точного определения «информационного оружия» (в зарубежных источниках «кибероружия»), все киберинструменты, способные «совершать атаки» в понимании МГП (т. е. реализовывать акты насилия в отношении противника, будь то в процессе нападении или обороны), следует рассматривать как оружие, подпадающее под действие правового предписания, в соответствии с которым МГП применяется ко «всем формам ведения войны и ко всем видам оружия, как прошлого, так и настоящего и будущего»[37], а также под действия ст. 36 ДП I 1977 г. Как отмечают эксперты, это важные формируемые концепции наглядно отражают, как под воздействием технологического прогресса расширяется значение отдельных положений МГП в части применения к вооруженным столкновениям в информационном пространстве[38]. Такая эволюция должна продолжаться с учётом развития и появления новых технологий, которые существенным образом меняют способы ведения боевых действий.

Как представляется, перспективы самостоятельного оформления международно-правового статуса информационного оружия на данный момент неоднозначны. Предложения ученых

[35] International humanitarian law and the challenges of contemporary armed conflicts. Recommitting to protection in armed conflict on the 70th anniversary of the Geneva Conventions. Report. 33rd International conference of the Red Cross and Red Crescent Geneva, Switzerland 9–12 December 2019. – *International Committee of the Red Cross.* URL: https://rcrc-conference.org/app/uploads/2019/10/33IC-IHL-Challenges-report_EN.pdf (accessed date: 27.10.2024).

[36] Legal review of cyber weapons, means and methods of warfare. – *Cyber Law Toolkit.* URL: https://cyberlaw.ccdcoe.org/wiki/Legal_review_of_cyber_weapons,_means_and_methods_of_warfare#National_positions (accessed date: 27.10.2024).

[37] Advisory Opinion of 8 July 1996. Legality of the Threat or Use of Nuclear Weapons. – *International Court of Justice.* URL: https://www.icj-cij.org/sites/default/files/case-related/93/093-19960708-ADV-01-00-EN.pdf (accessed date: 24.10.204).

[38] Klonowska K. Shifting the narrative: not weapons, but technologies of warfare. – *Humanitarian Law & Policy.* URL: https://blogs.icrc.org/law-and-policy/2022/01/20/weapons-technologies-warfare/ (accessed date: 27.10.2024); Международное гуманитарное право и кибероперации во время вооруженных конфликтов. Изложение позиции МККК. МККК, 2020. 32 с.

о разработке нового протокола к КНО 1980 г., который установит ограничения на применение информационного оружия, ИКТ-средств для ведения военных действий, а также урегулирует вопросы разработки и использования кибернаступательных потенциалов, не представляются объективно необходимыми и реально реализуемыми. По мнению российских представителей при ООН, к рассмотрению новых тем в рамках КНО следует подходить взвешенно, сбалансированно, учитывая гуманитарные озабоченности и законные оборонные интересы государств. Такой подход приобретает особую актуальность в свете активных попыток ряда стран и представителей гражданского общества апеллировать к гуманитарной составляющей в качестве абсолютного и единственно условия для введения ограничительно-запретительных режимов в отношении конкретных видов обычных вооружений[39]. Имеющееся международно-правовые основы для ведения военных действий (в части «права Гааги» и «права Женевы») являются достаточным для того, чтобы нивелировать гуманитарные риски в контексте использования новых видов вооружений.

В рамках развития вопроса по регулированию военного использования ИКТ и информационного пространства, включая методы и средства ведения войны, ряд ученых предлагает заключить соглашения о контроле над информационными вооружениями [Себекин 2021; Дылевский, Запивахин, Комов, Коротков, Петрунин 2014; Reinhold, Pleil, Reuter 2023; Ruhmann 2015], что на данном этапе также вызывает дискуссию ввиду ряда сложностей практического и политического характера.

Как представляется, ставить на повестку дня вопрос о необходимости разработки обязательных самостоятельных международных положений по изучаемой проблематике несколько несвоевременно, учитывая, что в сфере ИКТ и информационного пространства все еще идут исследования, и данная тема перспективно развивается. Вновь вернуться к данному вопросу возможно после достижения максимального универсального консенсуса экспертным сообществом, включающим ученых, юристов, инженеров, техников, военных специалистов, в отношении ключевых категорий и определений в сфере МИБ и имеющихся в ней военно-политических угроз. В связи с этим государствам следует апеллировать к действующим принципам и нормам МГП, закрепленным в ключевых договорах – Женевских конвенциях о защите жертв войны 1949 г. и Дополнительных протоколах к ним 1977 г., и определяющим базовые правила ведения военных действий в рамках любого театра войны и с учетом применения любого вида современного оружия.

Таким образом, в современном мире государствам, ученым, экспертам необходимо не только принимать во внимание тот факт, что новые достижения науки и техники неизбежно переходят в военный сектор, но и оперативно вырабатывать прогрессивные концепции, расширять толкование существующих норм и стремиться к адаптации положений международного права в части ограничения воюющих в выборе методов и средств ведения, защиты жертв войны и гражданских объектов, и в целом принципов и норм МГП к новейшим сферам отношений, включая информационное пространство и сферу ИКТ.

Проведенное исследование позволило обосновать авторскую гипотезу о возможности квалификации информационного оружия как средства ведения войны и признания за ним в перспективе статуса «обычного оружия». Регламентация вопросов разработки и использования данного вида оружия подпадает под действующие принципы и нормы МГП посредством определенной адаптации. Кроме того, учитывая, что информационная проблематика военных столкновений государств тесно связана со сферой МИБ, выработка договоренностей между государствами о предотвращении инцидентов в информационном пространстве или о ненападении в информационном пространстве будет являться дополнительным и эффективным средством сдерживания и минимизации рисков применения информационного оружия. Данные предложения активно обсуждаются Российской Федерацией на многих международных площадках, являются востребованными и актуальными, ввиду отсутствия на данный момент универсальных договоренностей государств по ответственному поведению в информационном пространстве.

[39] Выступление заместителя руководителя делегации Российской Федерации К.В. Воронцова в Первом комитете 76-й сессии Генеральной Ассамблеи ООН в ходе тематической дискуссии по разделу «Обычные вооружения». – *Постоянное представительство России пи ООН*. URL: https://russiaun.ru/ru/news/1comcw13102021 (дата обращения: 29.10.2024).

Список литературы

1. Блищенко И.П. 1984. *Обычное оружие и международное право.* Москва: Международные отношения. 216 с.
2. Гаркуша-Божко С.Ю. 2021. Международное гуманитарное право в киберпространстве: ratione materiae, ratione temporis и проблема квалификации кибератак. – *Цифровое право.* Т. 2. № 1. С. 64-82. DOI: 10.38044/2686-9136-2021-2-1-64-82.
3. Дауст И., Куплэнд Р., Исхой Р. 2002. Новые войны – новое оружие? Обязанность государств оценивать законность средств и методов ведения войны. – *Международный журнал Красного Креста.* № 845-847. С. 99-120.
4. Догель М. 1894. *Юридическое положение личности во время сухопутной войны.* Комбатанты. Казань: типолит. Имп. ун-та. 368 с.
5. Дылевский И.Н., Запивахин В.О., Комов С.А., Коротков С.В., Петрунин А.Н. 2014. Международный режим нераспространения информационного оружия: утопия или реальность? – *Военная мысль.* № 10. С. 3-12.
6. Капустин А.Я. 2017. К вопросу о международно-правовой концепции угроз международной информационной безопасности. – *Журнал зарубежного законодательства и сравнительного правоведения.* № 6. С. 44-51. DOI: 10.12737/article_5a1e71d7026536.36788152.
7. Конохов М.В. 2023. Средства и методы ведения воины в информационном пространстве: международно-правовые аспекты. – *Право и государство: теория и практика.* №11 (227). С. 218-222. DOI: 10.47643/1815-1337_2023_11_21.
8. Котляров И.И. 2009. Международное гуманитарное право об ограничении воюющих в выборе методов ведения войны. – *Московский журнал международного права.* № 2 (74). С. 44-62. DOI: 10.24833/0869-0049-2009-2-44-62.
9. Котляров И.И. 2011. Международное гуманитарное право о запрещенных средствах ведения войны. – *Московский журнал международного права.* № 1 (81). С. 31-48.
10. Макаренко С.И. 2016. Информационное оружие в технической сфере: терминология, классификация, примеры. – *Системы управления, связи и безопасности.* № 3. С. 292.
11. *Международное гуманитарное право и кибероперации во время вооруженных конфликтов.* 2020. Изложение позиции МККК. Перевод с английского с приложением оригинального текста. МККК. 32 с.
12. Мелков Г.М. 1988. *Международное право в период вооруженных конфликтов.* Москва: ВЮЗИ. 94 с.
13. Оппенгейм Л. 1949. *Международное право.* Т. II. п/т I. Москва.
14. Пузырева Ю.В., Нефедов Б.И., Эриашвили Н.Д. 2024. Роль Российской Федерации в формировании правовых основ современной системы международной информационной безопасности. – *Право и управление.* № 4. С. 38-45.
15. Сазонова К.Л. 2018. Современный международно-правовой статус оружия массового уничтожения (ОМУ) и вопросы международной ответственности государств за его применение. – *Национальная безопасность / Nota Bene.* № 6 (59). С. 52-65. DOI: 10.7256/2454-0668.2018.6.28480.
16. Себекин С. 2021. Возможен ли режим контроля за распространением кибервооружений? Подходы России и США. – *Пути к миру и безопасности.* С. 139-152.
17. Синякин И.И. 2012. *Терроризм с использованием оружия массового уничтожения: международно-правовые вопросы противодействия.* Монография. Москва: Норма. 191 с.
18. Стрельцов А.А. 2014. Основные направления развития международного права вооруженных конфликтов применительно к киберпространству. – *Право и государство: теория и практика.* № 3(111). С. 75-78.
19. Талимончик В.П. 2016. Международно-правовые средства борьбы с информационным оружием. – *Российский ежегодник международного права.* № S. С. 135-151.
20. Шеховцов Н.П., Кулешов Ю.Е. 2012. Информационное оружие: теория и практика применения в информационном противоборстве. – *Вестник Академии военных наук.* № 1 (38). С. 35-40.
21. Шинкарецкая Г.Г. 2013. Международное право и война в киберпространстве. – *Современное право.* № 8. С. 120-126.
22. *Ядерное оружие и международная безопасность в XXI веке.* 2013. Материалы международной конференции. Гл. ред. И.С. Иванов. Москва: Спецкнига. С. 57.
23. Arquilla J. 2021. *Bitskrieg: The New Challenge of Cyberwarfare.* London: Polity Press. 206 p.
24. Boulanin V., Verbruggen M. 2017. *Article 36 Reviews: Dealing with the Challenges posed by Emerging Technologies.* SIPRI. 51 p.
25. Carr J. 2013. The misunderstood acronym: Why cyber weapons aren't WMD. – *Bulletin of the Atomic Scientists.* № 69(5). P. 32-37. DOI: https://doi.org/10.1177/0096340213501373.
26. Clarke R., Knake R. 2011. *Cyber War: The Next Threat to National Security and What To Do About It.* Ecco, HarperCollins Publishers. 290 p.
27. Franklin A. 2018. An international cyber warfare treaty: Historical analogies and future prospects. – *Journal of Law & Cyber Warfare.* № 7(1). P. 149-164.
28. Hatch B.B. 2018. Defining a Class of Cyber Weapons as WMD: An Examination of the Merits. – *Journal of Strategic Security.* Vol. 11. No. 1. P. 43-61.
29. Ivanenko V. 2022. The origins, causes and enduring significance of the Martens Clause. – *International Review of the Red Cross.* № 104(920-921). P. 1708-1724. DOI:10.1017/S1816383122000273.
30. Krepinevich A. 2012. *Cyber warfare: a "nuclear option"?* Center for Strategic and Budgetary Assessments. 96 p.
31. Kudláčková I. 2020. Kybernetická zbraň: Přístupy k její definici. – *Revue pro právo a technologie.* Vol. 11. No. 21. P. 47-71.
32. Kumar D. 2013. Cyber Weapons – The New Weapons of Mass Destruction? – *Journal of the United Service Institution of India.* Vol. CXLII, No. 591.
33. Lee N. 2024. Cyber Warfare: Weapon of Mass Disruption. – *Counterterrorism and Cybersecurity.* Switzerland: Springer, Cham. P. 243-294.
34. Pool P. 2013. War of the cyber world: The law of cyber warfare. – *The International Lawyer.* № 47(2). P. 299-323.
35. Rattray G.J. 2001. *Strategic Warfare in Cyberspace.* London: MIT Press. 517 p.
36. Reinhold T., Pleil H., Reuter C. 2023. Challenges for Cyber Arms Control: A Qualitative Expert Interview Study. – *Z Außen Sicherheitspolit.* № 16. P. 289–310.

37. Ruhmann I. 2015. Neue Ansätze für die Rüstungskontrolle bei Cyber-Konflikten. Ed. by D. Cunningham, P. Hofstedt, K. Meer, I. Schmitt. – *INFORMATIK 2015 lecture notes in informatics (LNI)*. Bonn, Gesellschaft für Informatik. P. 571-585.
38. Sharp W.G. 1999. *Cyberspace and the Use of Force*. NY. 234 p.
39. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2017. 2nd ed. Cambridge: Cambridge University Press. 638 p.
40. *The Future of Weapons of Mass Destruction: Their Nature and Role in 2030*. 2014. Center for the Study of Weapons of Mass Destruction. National Defense University. Washington National Defense University Press. 75 p.
41. Verhelst A., Filling W.J. 2020. Global Governance Gaps in Cybersecurity: International and European Legal Perspectives. – *International Organisations Research Journal*. Vol. 15. № 2. P. 141-172.

References

1. Arquilla J. *Bitskrieg: The New Challenge of Cyberwarfare*. London: Polity Press. 2021. 206 p.
2. Blishchenko I.P. *Obychnoye oruzhiye i mezhdunarodnoye pravo [Conventional weapons and international law]*. Moscow: Mezhdunarodnyye otnosheniya. 1984. 216 p. (In Russ.)
3. Boulanin V., Verbruggen M. *Article 36 Reviews: Dealing with the Challenges posed by Emerging Technologies*. SIPRI. 2017. 51 p.
4. Carr J. The misunderstood acronym: Why cyber weapons aren't WMD. – *Bulletin of the Atomic Scientists*. 2013. № 69(5). P. 32-37. DOI: https://doi.org/10.1177/0096340213501373.
5. Clarke R., Knake R. *Cyber War: The Next Threat to National Security and What To Do About It*. Ecco, HarperCollins Publishers. 2011. 290 p.
6. Daust I., Kuplend R., Iskhoy R. Novyye voyny – novoye oruzhiye? Obyazannost' gosudarstv otsenivat' zakonnost' sredstv i metodov vedeniya voyny [New Wars – New Weapons? The Duty of States to Assess the Legitimacy of Means and Methods of Warfare]. – *Mezhdunarodnyy zhurnal Krasnogo Kresta [The International Journal of the Red Cross]*. 2002. No. 845-847. P. 99-120. (In Russ.)
7. Dogel' M. *Yuridicheskoye polozheniye lichnosti vo vremya sukhoputnoy voyny. Kombatanty. [Legal status of the individual during a land war. Combatants]*. Kazan': tipo-lit. Imp. un-ta. 1894. 368 p. (In Russ.)
8. Dylevskij I.N., Zapivahin V.O., Komov S.A., Korotkov S.V., Petrunin A.N. Mezhdunarodnyj rezhim nerasprostranenija informacionnogo oruzhija: utopija ili real'nost'? [The international regime for the non-proliferation of information weapons: utopia or reality?]. – *Voennaja mysl' [Military thought]*. 2014. № 10. S. 3-12. (In Russ.)
9. Franklin A. An international cyber warfare treaty: Historical analogies and future prospects. – *Journal of Law & Cyber Warfare*. 2018. № 7 (1). P. 149-164.
10. Garkusha-Bozhko S. Yu. Mezhdunarodnoye gumanitarnoye pravo v kiberprostranstve: ratione materiae, ratione temporis i problema kvalifikatsii kiberatak [International humanitarian law in cyberspace: ratione materiae, ratione temporis and the problem of qualifying cyberattacks]. – *Tsifrovoye pravo [Digital law]*. 2021.Vol. 2. No. 1. P. 64-82. DOI: 10.38044/2686-9136-2021-2-1-64-82. (In Russ.)
11. Hatch B.B. Defining a Class of Cyber Weapons as WMD: An Examination of the Merits. – *Journal of Strategic Security*. 2018. Vol. 11. No. 1. P. 43-61.
12. Ivanenko V. The origins, causes and enduring significance of the Martens Clause. – *International Review of the Red Cross*. 2022. № 104 (920-921). P. 1708-1724. DOI:10.1017/S1816383122000273.
13. *Jadernoe oruzhie i mezhdunarodnaja bezopasnost' v XXI veke [Nuclear weapons and international security in the 21st century]*. Materialy mezhdunarodnoj konferencii. Gl. red. I.S. Ivanov. Moskva: Specknіga. 2013. S. 57.
14. Kapustin A.Ya. K voprosu o mezhdunarodno-pravovoy kontseptsii ugroz mezhdunarodnoy informatsionnoy bezopasnosti [On the issue of the international legal concept of threats to international information security]. – *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya [Journal of Foreign Legislation and Comparative Law]*. 2017. No. 6. P. 44-51. DOI: 10.12737/article_5a1e71d7026536.36788152. (In Russ.)
15. Konokhov M.V. Sredstva i metody vedeniya voiny v informatsionnom prostranstve: mezhdunarodno-pravovyye aspekty [Means and methods of warfare in the information space: international legal aspects]. – *Law and state: theory and practice [Law and the State: theory and practice]*. 2023. No. 11 (227). P. 218-222. DOI: 10.47643/1815-1337_2023_11_21. (In Russ.).
16. Kotlyarov I.I. Mezhdunarodnoye gumanitarnoye pravo o zapreshchennykh sredstvakh vedeniya voyny [International humanitarian law on prohibited means of warfare]. – *Moskovskiy zhurnal mezhdunarodnogo prava [Moscow Journal of International Law]*. 2011. No. 1 (81). P. 31-48. (In Russ.).
17. Kotlyarov I.I. Mezhdunarodnoye gumanitarnoye pravo ob ogranichenii voyuyushchikh v vybore metodov vedeniya voyny [International humanitarian law on the limitation of belligerents in the choice of methods of waging war]. – *Moskovskiy zhurnal mezhdunarodnogo prava [Moscow Journal of International Law]*. 2009. No. 2 (74). P. 44-62. (In Russ.). DOI: 10.24833/0869-0049-2009-2-44-62.
18. Krepinevich A. Cyber warfare: a "nuclear option"? Center for Strategic and Budgetary Assessments. 2012. 96 p.
19. Kudláčková I. Kybernetická zbraň: Přístupy k její definici. – *Revue pro právo a technologie*. 2020. Vol. 11. No. 21. P. 47-71.
20. Kumar D. Cyber Weapons – The New Weapons of Mass Destruction? – *Journal of the United Service Institution of India*. 2013. Vol. CXLII, No. 591.
21. Lee N. Cyber Warfare: Weapon of Mass Disruption. – *Counterterrorism and Cybersecurity*. Switzerland: Springer, Cham. 2024. P. 243-294.
22. Makarenko S.I. Informacionnoe oruzhie v tehnicheskoj sfere: terminologija, klassifikacija, primery [Information weapons in the technical field: terminology, classification, examples]. – *Sistemy upravlenija, svjazi i bezopasnosti [Control, communication and security systems]*. 2016. № 3. S. 292.
23. Melkov G.M. *Mezhdunarodnoye pravo v period vooruzhennykh konfliktov [International law during armed conflicts]*. Moscow: VYUZI. 1988. 94 p. (In Russ.).
24. *Mezhdunarodnoye gumanitarnoye pravo i kiberoperatsii vo vremya vooruzhennykh konfliktov. Izlozheniye pozitsii MKKK. Perevod s angliyskogo s prilozheniyem original'nogo teksta. [International Humanitarian Law and Cyber Operations in Armed Conflict]*. ICRC Position Statement. Translation from English with appendix of the original text. ICRC. 2020. 32 p. (In Russ.).

25. Oppengejm L. *Mezhdunarodnoe pravo [International law]*. T. II. p/t I. Moscow. 1949. (In Russ.).
26. Pool P. War of the cyber world: The law of cyber warfare. – *The International Lawyer*. 2013. № 47(2). P. 299-323.
27. Puzyreva Ju.V., Nefedov B.I., Jeriashvili N.D. 2024. Rol' Rossijskoj Federacii v formirovanii pravovyh osnov sovremennoj sistemy mezhdunarodnoj informacionnoj bezopasnosti [The role of the Russian Federation in the formation of the legal foundations of the modern system of international information security]. – *Pravo i upravlenie [Law and management]*. № 4. S. 38-45. (In Russ.).
28. Rattray G.J. *Strategic Warfare in Cyberspace*. London: MIT Press. 2001. 517 p.
29. Reinhold T., Pleil H., Reuter C. Challenges for Cyber Arms Control: A Qualitative Expert Interview Study. – *Z Außen Sicherheitspolit*. 2023. № 16. P. 289–310.
30. Ruhmann I. Neue Ansätze für die Rüstungskontrolle bei Cyber-Konflikten. Ed. by D. Cunningham, P. Hofstedt, K. Meer, I. Schmitt. – *INFORMATIK 2015 lecture notes in informatics (LNI)*. Bonn, Gesellschaft für Informatik. 2015. P. 571-585.
31. Sazonova K.L. Sovremennyy mezhdunarodno-pravovoy status oruzhiya massovogo unichtozheniya (OMU) i voprosy mezhdunarodnoy otvetstvennosti gosudarstv za yego primeneniye [Current international legal status of weapons of mass destruction (WMD) and issues of international responsibility of states for their use]. – *Natsional'naya bezopasnost' / Nota Bene [National Security / Nota Bene]*. 2018. No. 6 (59). P. 52-65. DOI: 10.7256/2454-0668.2018.6.28480. (In Russ.).
32. Sebekin S. Vozmozhen li rezhim kontrolja za rasprostraneniem kibervooruzhenij? Podhody Rossii i SShA [Is it possible to control the proliferation of cyber weapons? Approaches of Russia and the USA]. – *Puti k miru i bezopasnosti [Ways to peace and security]*. 2021. S. 139-152. (In Russ.).
33. Sharp W.G. *Cyberspace and the Use of Force*. NY. 1999. 234 p.
34. Shehovcov N.P., Kuleshov Ju.E. Informacionnoe oruzhie: teorija i praktika primenenija v informacionnom protivoborstve [Information weapons: theory and practice of application in information warfare]. – *Vestnik Akademii voennyh nauk [Bulletin of the Academy of Military Sciences]*. 2012. № 1 (38). S. 35-40. (In Russ.).
35. Shinkaretskaya G.G. Mezhdunarodnoye pravo i voyna v kiberprostranstve [International law and war in cyberspace]. – *Sovremennoye pravo [Modern law]*. 2013. No. 8. P. 120-126. (In Russ.).
36. Sinyakin I.I. *Terrorizm s ispol'zovaniyem oruzhiya massovogo unichtozheniya: mezhdunarodno-pravovyye voprosy protivodeystviya [Terrorism with the use of weapons of mass destruction: international legal issues of counteraction]*. Monografiya. Moscow: Norma. 2012. 191 p. (In Russ.).
37. Strel'tsov A.A. Osnovnyye napravleniya razvitiya mezhdunarodnogo prava vooruzhennykh konfliktov primenitel'no k kiberprostranstvu [Main directions of development of international law of armed conflicts as applied to cyberspace]. – *Pravo i gosudarstvo: teoriya i praktika [Law and the State: theory and practice]*. 2014. No. 3 (111). P. 75-78. (In Russ.).
38. Talimonchik V.P. Mezhdunarodno-pravovye sredstva bor'by s informacionnym oruzhiem [International legal means of combating information weapons]. – Rossijskij ezhegodnik mezhdunarodnogo prava [Russian Yearbook of International Law]. 2016. № S. S. 135-151. (In Russ.).
39. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge: Cambridge University Press. 2017. 638 p.
40. *The Future of Weapons of Mass Destruction: Their Nature and Role in 2030*. Center for the Study of Weapons of Mass Destruction. National Defense University. Washington National Defense University Press. 2014. 75 p.
41. Verhelst A., Filling W.J. Global Governance Gaps in Cybersecurity: International and European Legal Perspectives. – *International Organisations Research Journal*. 2020. Vol. 15. № 2. P. 141-172.

Информация об авторе

Юлия Владимировна ПУЗЫРЕВА,
кандидат юридических наук, доцент, заместитель начальника кафедры прав человека и международного права, Московский университет МВД России имени В.Я. Кикотя

Академика Волгина ул., д. 12, Москва, 117997, Российская Федерация

yuliya_dugina@mail.ru
ORCID: 0000-0003-4448-2200

About the Author

Yuliya V. PUZYREVA,
Candidate of Juridical Sciences, Associate Professor, Deputy Head of the Department of Human Rights and International Law, Kikot Moscow University of the Ministry of Internal Affairs of Russia

12, Akademika Volgina St., Moscow, Russian Federation, 117997

yuliya_dugina@mail.ru
ORCID: 0000-0003-4448-2200