DOI: 10.17803/1994-1471.2022.139.6.168-176

Ю. А. Юдина*

Возможность применения средств обеспечения международной безопасности к информационному пространству

Аннотация. В статье для решения вопроса о приемлемости обращения государств к существующим механизмам обеспечения безопасного и планомерного развития международных отношений в ИКТ-среде определены основные подходы, фигурирующие в совместных коммюнике и соглашениях, изданных по итогам конференций и встреч на высоком уровне представителей Российской Федерации и ее партнеров и союзнического блока США, стран Европейского Союза и других государств. Путем толкования таких терминов, как «информационное оружие», «кибероружие», «кибершпионаж», выявлены сложности, сопутствующие процессу формирования безопасной ИКТ-среды. Результатом исследования стало выявление актуальных и оптимальных с точки зрения современного состояния права международной безопасности в отношении ИКТ-среды средств обеспечения безопасности, которые могут быть рекомендованы к использованию государствами с целью формирования безопасного режима взаимодействия в рамках отправления государствами своих функций на внешнеполитической арене в контексте глобального информационного пространства.
Ключевые слова: международная информационная безопасность; средства обеспечения международной безопасности; информационное оружие; кибероружие; ИКТ; кибершпионаж; информационное пространство; ИКТ-среда; информационная война; право международной безопасности; глобальная безопасность.
Для цитирования: *Юдина Ю. А.* Возможность применения средств обеспечения международной безопасности к информационному пространству // Актуальные проблемы российского права. — 2022. — Т. 17. — № 6. — С. 168–176. — DOI: 10.17803/1994-1471.2022.139.6.168-176.

Possibility of Applying the Means of Ensuring International Security to the Information Space

Yuliya A. Yudina, Expert of the Center for International Information Security and Science and Technology Policy, MGIMO MFA of Russia
pr. Vernadskogo, d. 76, Moscow, Russia, 119454
yudina.iuliia@gmail.com

Abstract. In order to resolve the issue of acceptability of the states' appeal to existing mechanisms for ensuring safe and systematic development of international relations in the ICT environment, the author determines the main approaches appearing in joint communiqués and agreements issued following the results of conferences and high-level meetings of representatives of the Russian Federation and its partners and the allied bloc of the USA, the countries of the European Union and other states. By interpreting such terms as "information weapons", "cyber weapons", "cyber espionage", the difficulties associated with the process of creating a secure ICT environment

* *Юдина Юлия Александровна*, эксперт Центра международной информационной безопасности и научно-технологической политики МГИМО МИД России
пр-т Вернадского, д. 76, г. Москва, Россия, 119454
yudina.iuliia@gmail.com

are identified. The result of the study is the identification of security tools that are relevant and optimal from the point of view of the current state of international security law in relation to the ICT environment and that can be recommended to be used by states in order to form a secure mode of interaction in the framework of the exercise by states of their functions in the foreign policy arena amid the global information space.
Keywords: international information security; means of ensuring international security; information weapon; cyber weapons; ICT; cyber espionage; information space; ICT environment; information war; international security law; global security.
Cite as: Yudina YuA. Vozmozhnost primeneniya sredstv obespecheniya mezhdunarodnoy bezopasnosti k informatsionnomu prostranstvu [Possibility of Applying the Means of Ensuring International Security to the Information Space]. *Aktual'nye problemy rossijskogo prava*. 2022:17(6):168-176. DOI: 10.17803/1994-1471.2022.139.6.168-176. (In Russ., abstract in Eng.).

Ситуация в мировом пространстве обострена конвергенцией реального и виртуального миров и влечет за собой неизбежное усиление противоборства между развитыми западными странами и развивающимся миром. Деятельность ряда западных стран сформировала атмосферу враждебности и конфронтации в глобальной информационной коммуникационной технологической среде (далее — ИКТ-среде). Вместе с тем привычное понимание войны между государствами все чаще и чаще отходит на второй план, становясь некоторым анахронизмом. Эти метаморфозы связаны в первую очередь с тем, что на смену кинетическому оружию пришло активное развитие и применение информационных коммуникационных технологий (далее — ИКТ) в целях, противоречащих Уставу ООН, или, как рассуждают исследователи, кинетическое оружие сменилось информационным или кибероружием[1]. С целью проникновения в критические структуры «врага», дестабилизации его внутренней политики и осуществления иных злонамеренных планов государства бросают многомиллионные силы и ресурсы для производства и апробации все более сложных ИКТ. Очевидно, что для нормализации отношений между государствами, а также их перевода в правовое русло в рамках обеспечения международной безопасности международному сообществу требуется согласование средств по обеспечению стабильного и безопасного сосуществования государств в информационном пространстве путем унификации понятийного аппарата и принятия на себя конкретных обязательств в данной сфере[2].

Обращает на себя внимание различие подходов ведущих государств к определению средств обеспечения МИБ. Так, Россия и ее союзники в процессе своего сотрудничества на платформах ШОС, СНГ, АСЕАН выдвигают концепцию демилитаризации информационного пространства[3]. В качестве аргумента выдвигается тезис о том, что превращение информационного пространства в военный полигон может расшатать или вовсе сломать сложившуюся систему глобальной безопасности.

Западные государства, напротив, предвосхищают использование ИКТ в военно-политических целях и активно продвигают его. Неудивительно, что США и их сателлиты относят противоборство в информационном пространстве к сфере регулирования международного гуманитарного права, а в качестве ключевых угроз рассматриваемому виду безопасности выделяют терроризм и преступность в кибернетическом пространстве.

Стремление западных государств развивать ИКТ и применять их в военно-политических

[1] *Lee B. Bagheri, Kao H.* A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems // Manufacturing Letters. 2015. Vol. 3. P. 18–23.

[2] *Батырь В. А.* Новые вызовы XXI века в сфере развития средств вооруженной борьбы // Евразийский юридический журнал. 2014. № 2 (69). С. 76–81.

[3] Конвенция об обеспечении международной информационной безопасности (концепция) от 22.09.2011 // СПС «КонсультантПлюс».

целях может иметь различное объяснение. Так, Лоран Гизель и Лукаш Олейник, специалисты Международного комитета Красного Креста, считают, что использование ИКТ в военно-политической сфере выгодно отличается от применения кинетического оружия даже в случае достаточно высокой стоимости услуг приглашенных хакеров, использования мощных компьютерных систем и т.д.[4] Это отличие заключается в весьма затруднительной атрибуции атакующего[5]. Для современной глобальной политической обстановки характерно использование методов политической атрибуции, ключевым аспектом которой является получение ответа на вопрос — кому выгодна данная атака, с какой страной у пострадавшего государства существенные разногласия или обостренная степень конкуренции, например на экономическом поприще. Тогда как техническая атрибуция, проводимая специалистами в сфере информационной безопасности, опускается, ее необходимость нивелируется, несмотря на то что это точный способ отследить источник атаки, определить его месторасположение и «маршрут» атаки.

Исследователи также приводят в пример случай на атомной электростанции в Натанзе (Иран). Осуществить атаку на данный объект физически при помощи кинетического оружия было бы гораздо эффективнее, нежели разрабатывать и применять вирус Stuxnet. Но та цель, которую преследовали заказчики атаки, — отбросить развитие ядерной промышленности Ирана на декаду лет — они смогли получить без особых негативных для себя последствий в геополитическом пространстве.

Вполне вероятно, что аналогичного обоснования могли придерживаться США, реализовав свои идеи по организации кибервойск и осуществлению кибератак на «вражеские» государства.

Исследователи считают, что для гармонизации отношений между государствами в ИКТ-среде чрезвычайно важно установить руководящие принципы, принять меморандумы о намерениях[6], а также возобновить совместные разработку и внедрение кодекса ответственного поведения государств[7], средств по предотвращению[8] и устранению конфликтов в сфере использования ИКТ, развитие международных мер укрепления доверия[9].

Очевидно, что для определения возможности применимости существующих средств обеспечения глобальной безопасности применительно к информационному пространству важно разобраться с некоторыми терминами и привести в должный вид понятийный аппарат. Так, следует определить, что собой представляют информационное оружие, кибероружие, как два этих понятия соотносятся друг с другом, и такими терминами, как информационная война и кибершпионаж.

---

4 ICRC Expert Meeting: The Potential Human Cost of Cyber Operations / eds L. Gisel and L. Olejnik. ICRC, Geneva, 2019. URL: www.icrc.or//ownloa/il/600/he-potential-human-cost-of-cyber-operations.pdf. 27.12.2020.

5 Сложность заключается в том, что на поиск организаторов атак тратится значительный временно́й ресурс с использованием массы агрегирующих информационных и иных источников. Особо подчеркнем, что атрибуция возможна всегда, так как всякий пользователь оставляет цифровой след в информационном пространстве.

6 *Крутских А. В.* К политико-правовым основаниям глобальной информационной безопасности // Международные процессы. 2007. Т. 5. № 1 (13). С. 28–37.

7 *Hague W.* Security and freedom in the cyber age — seeking the rules of the road : Speech to the Munich Security Conference, 4 February 2011 // URL: https://www.gov.uk/government/speeches/security-and-freedom-in-the-cyber-age-seeking-the-rules-of-the-road (дата обращения: 15.09.2021).

8 *Ромашкина Н. П.* Вооружения без контроля: современные угрозы международной информационной безопасности // Пути к миру и безопасности. 2018. № 2 (55). С. 64–83.

9 *Baseley-Walker B.* Transparency and confidence-building measures in cyberspace: towards norms of behavior // UNIDIR. Disarmament Forum, «Confronting cyberconflict». 2011. Iss. 4. P. 31–40. URL: http://www.unidir.org/files/publications/pdfs/confronting-cyberconflict-en-317.pdf. 15.09.2021.

Так, термин «информационное оружие» активно используется на площадках ШОС и СНГ. В качестве информационного оружия данные организации понимают ИКТ, которые государства используют с целью ведения противоборства друг с другом в информационном пространстве или информационной войны[10].

Не менее популярно определение термина «информационное оружие» в качестве средства, основанного на использовании информации и математической логики; целью которого числятся контроль или получение информации. Исследователи подчеркивают, что к такому оружию относятся «черви», «вирусы», удаленный контроль объекта секьюритизации, кража паролей и др.[11]

В публичных источниках представлено определение информационного оружия как совокупность средств, которая применяется для нарушения целостности информационных ресурсов на разных этапах их обработки: создания, распространения, хранения. Подчеркивается, что функционально информационное оружие действует путем копирования, искажения или уничтожения всей информации или ее части.

На фоне анализа представленных дефиниций возникает закономерный вопрос: является ли информационное оружие оружием как таковым? Чтобы понять специфику данного «инструмента», необходимо подробнее остановиться на рассмотрении другого термина, которым обозначают либо самостоятельный вид оружия, тождественный по названию с информационным оружием, либо составную часть информационного оружия. Так, обращает на себя внимание термин «кибероружие». СМИ, авторы научных исследований, а также многие политики, характеризуя атаки, совершенные при помощи ИКТ, или запугивая реальную или виртуальную аудиторию, обращаются к слову «кибероружие». Они отмечают, что кибероружие по средствам своего применения вполне сравнимо с оружием массового поражения, т.е. атаки в виртуальном пространстве могут иметь разрушительный эффект в реальном мире[12].

Представляются любопытными попытки дать определение кибероружию иностранными исследователями. Так, например, Стефано Мел, член Комиссии по кибербезопасности Итальянского Атлантического комитета, характеризует кибероружие следующим образом. Это программный или машинный код, набор компьютерных регламентов, которые используются в конфликте между национальными и ненациональными акторами[13] с целью вызвать прямо или косвенно физическое повреждение оборудования или нанести физический вред людям; осуществить саботаж или привести во временную или постоянную негодность информационные системы атакуемого государства[14].

Профессор Университета Хопкинса Томас Рид и профессор Королевского колледжа Лондона Питер МакБерни дают следующее определение кибероружия: код, целью создания и использования которого является причинение или угроза причинения физического, функционального или психического вреда структурам, системам или живым существам[15].

На фоне серии громких событий, связанных с заражением критически важной инфраструк-

[10] Соглашение между правительствами государств — членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 16.06.2009 // СПС «КонсультантПлюс», 2012.

[11] *Коротков А. В.*, *Зиновьева Е. С.* Безопасность критических информационных инфраструктур в международном гуманитарном праве // Вестник МГИМО-Университета. 2011. № 4. С. 154–162.

[12] *Харрис Ш.* Кибервойна: пятый театр военных действий. М. : Альпина нон-фикшн, 2016. С. 390.

[13] Здесь: государства, государственно-подобные образования и иные субъекты международного права. Прим. автора.

[14] *Mele S.* Cyber-Weapons: Legal and Strategic Aspects (Version 2.0) (June 7, 2013) // URL: https://ssrn.com/abstract=2518212 (дата обращения: 15.09.2021).

[15] *Rid T.*, *McBurney P.* Cyber-Weapons // The RUSI Journal. 2012. Vol. 157. Iss. 1. P. 6–13. DOI: 10.1080/03071847.2012.664354.

туры и других стратегических объектов вирусами, последние также стали причисляться к кибероружию[16], например вирусы типа Flame или зомби-сети, применяемые в качестве инструмента DDos-атак, т.е. таргетированных атак с целью рассылки спама или осуществления сбоя цифровых систем. Но может ли шпионская программа считаться оружием в строгом смысле слова? Фактически нарушая целостность информационной системы государства, но не уничтожая ее содержание и не искажая его, кибероружие может обозначаться указанным термином разве что в средствах массовой информации, но никак не в дискурсе научно-исследовательских работ или в контексте переговорной деятельности государств.

Впрочем, некоторые исследователи вовсе не согласны с таким подходом к определению кибероружия.

Так, например, В. В. Каберник указывает на то, что кибероружие совсем не обязательно обозначает программный код, воздействующий на компьютерную систему. Прямой целью атак могут служить не только программно-электронное оборудование, но и любые технические устройства, в основе которых лежит принцип обратной связи, например автомат, система сигнализации и оповещения. Автор подчеркивает, что важным условием возможности осуществления атак при помощи ИКТ на указанные объекты будет управляемость последних, предсказуемость их реакций[17].

На основании представленных дефиниций можно выявить некоторую тождественность понятий «информационное оружие» и «кибероружие», в связи с тем что оба термина используются для описания вредоносного программного кода. Однако, очевидно, если толковать оба термина не с позиции технологической составляющей, а ориентируясь на различия ключевых понятий в сфере международной информационной безопасности (далее — МИБ) — собственно международной информационной безопасности и кибербезопасности, можно обнаружить иную закономерность. Как известно, российские исследователи подчеркивают, что международная информационная безопасность, охватывающая все аспекты безопасности, начиная от технических и заканчивая психологическими, включает и кибербезопасность. В таком случае, если рассматривать информационное оружие в качестве средства воздействия на когнитивные функции человека, на его интеллектуальные возможности, с целью реализации противоправных планов, равно как и «инструмента» для воздействия на критическую инфраструктуру, можно обнаружить, что кибероружие представляет собой часть информационного оружия, т.е. соотносится с ним как частное с общим[18].

Важно отметить, что придание так называемому информационному оружию статуса оружия несет значительные риски для всего общества. Не секрет, что применение ИКТ в военно-политических целях носит специфический характер — граница между разведывательными и военными операциями становится эфемерна, размыта. Может ли государство держать информационный удар и ответить враждебному субъекту в случае обнаружения шпионских или диверсионных действий? А что делать, если этот субъект представляет собой неправительственную структуру, например частную компанию или отдельного хакера, работающего на себя и стремящегося к мировому господству? Цифровая

[16] В 2009 г. самолеты-истребители противовоздушной обороны военно-морских сил Франции были заражены вирусом, вследствие чего не могли подняться в воздух несколько дней; в 2010 г. Stuxnet поразил ядерные центрифуги иранской АЭС, поставив под угрозу срыва реализацию ядерной программы; атаки Carbanak в 2013 г. на финансовые организации по всему миру, в том числе СНГ, и т.д.

[17] *Каберник В. В.* Проблемы классификации кибероружия // Вестник МГИМО-Университета, 2013. № 2 (29). С. 72–78.

[18] Russia — US Bilateral on Cybersecurity. Critical Terminology foundations. EastWest Institute Worldwise Cybersecurity Initiative, Moscow state university information security institute. November 2013 // URL: http://wiki.informationsecurity.club/lib/exe/fetch.php?media=documents_all:russia-u_s_bilateral_on_terminology_rus.pdf.

защита, исходя из тех положений, что явствуют из кибердоктрин западных государств, обладает уникальным свойством — активностью, то есть возможностью атаковать в ответ с применением не только информационно-коммуникационных устройств, но и с использованием классического кинетического оружия; а кроме того, это качество защиты дает возможность государствам не дожидаться массированной атаки, нарушения своего цифрового суверенитета, а также осуществлять «превентивные» меры наступательного характера, то есть агрессивные военно-политические действия подменяют собой настоящие оборону и защиту.

Кроме того, остаются нерешенными вопросы, что́ представляет собой невраждебная кибератака: относится ли к такому типу использования ИКТ исключительно ошибочные действия хакеров, спецслужб или отдельных не заинтересованных в деструктивном и опасном воздействии на государство и его структуры лиц, или совершение такой атаки и есть кибершпионаж или диверсионные действия?

Важно понимать, что враждебные действия в информационном пространстве действительно отличаются от военного поведения в реальном мире. Несомненно, многие государства внедряют в свое законодательство концепции и доктрины, провозглашающие идентичные характеристики виртуальной и информационной войн, что явно прослеживается в целях, мотивах и интересах, преследуемых государствами, напоминают доктрины так называемой обычной войны: возмездие и сдерживание. Но всем политическим игрокам необходимо осознать, что использование ИКТ в военно-политических целях не есть новая война, новый ее вид — это смешанное ведение боевых действий, это классическая война с применением цифровых технологий, которой западные государства, например, промышляют с начала 2000-х гг.

Строго говоря, на сегодняшний день применение к обеспечению безопасности глобального информационного пространства существующего корпуса норм права международной безопасности маловероятно. Отследить, какой код будет спрограммирован на уничтожение больницы или атомной электростанции, на ликвидацию боевиков террористической организации или на военные отряды вражеского государства, представляется затруднительным действием. ИКТ в качестве оружия применяются исключительно исходя из целей и задач, которые перед собой ставит каждый конкретный пользователь. Нет конкретных параметров и алгоритмов расчета рисков, связанных с втягиванием в такие военно-политические действия с применением ИКТ неправительственных структур — транснациональные корпорации, сбой в системе которых может повлечь осуществление серии атак на критическую инфраструктуру как государства, под юрисдикцией которого находится компания, так и иного. Возможно ли применение санкций по отношению к таким компаниям, или ответственность за осуществление непреднамеренной кибератаки с негативными последствиями для чужой страны будет нести государство, к юрисдикции которой эта компания относится? Как известно, к комбатантам не могут относиться бизнес-структуры, гражданское общество, а потому для формирования приемлемого режима МИБ государствам важно решить, готовы ли они подвергать опасности все ключевые сферы жизнедеятельности своих граждан и свою безопасность, которая мгновенно теряет свою силу и значение при внедрении в концепции безопасности положения о возможности совершения наступательных или упреждающих операций с применением ИКТ, или использованием кинетического оружия в случае цифровой атаки на данное государство.

Бесспорно, что международным сообществом до сих пор не выработаны критерии применимости международного права к ИКТ-сфере, а также не разработаны методы адаптации действующих норм МГП или ПМБ применительно к новой высокотехнологичной сфере отношений. В силу того, что государствами не достигнут консенсус по поводу понимания ключевых направлений развития ИКТ-сферы и формирования единообразного правового режима этой области, все острее стоит вопрос об угрозе эскалации международных конфликтов с применением цифровых технологий, а также отодвигается процесс демилитаризации ИКТ-сферы.

Очевидно также и то, что международное сообщество не достигло консенсуса по вопросам определения информационной войны, что затрудняет определить реальные характеристики потенциальных действий силового характера, для осуществления которых могут быть использованы ИКТ. Отсутствие общности подходов к понятийному аппарату, кроме всего прочего, усугубляет и без того сложные процессы определения и фиксации агрессивных действий с использованием цифровых технологий, ввиду того что противоправные деяния военно-политического характера носят трансграничный характер, в рамках осуществления которых почти всегда нарушается цифровой суверенитет государства.

Привычным является определение «информационной войны», подразумевающее активное манипулятивное воздействие на население с помощью информационно-коммуникационных технологий. Обычно, говоря об этом явлении, авторы имеют в виду не саму информационную войну, но лишь только один из ее способов — информационный шпионаж. Примечательно, информационный шпионаж получил свое первоначальное распространение в период с 1990 по 2000-е гг. Тогда американский транснациональный телекоммуникационный конгломерат AT&T при помощи телефонного шифровальщика TSD-3600-E начал прослушивать телефонные разговоры. Новая волна информационного шпионажа поднялась в 2000 г. и никак не схлынет до сих пор. Он включает в себя произвольное массовое наблюдение, взлом данных, манипулирование общими криптографическими алгоритмами.

Отдельные исследователи рассматривают информационную войну, подразумевая информационное противоборство или совокупность отдельных элементов такого противоборства. Иногда исследователи и вовсе объединяют понятия информационной войны и информационного единоборства, не выделяя никаких отличительных черт. Такие характеристики подчеркивают, что даже при использовании ИКТ никакого нового вида или подвида вооруженных конфликтов международного характера не возникает.

Характерно также то, что ни правоведы, ни исследователи, ни дипломаты до сих пор не выстроили классификацию юридических фактов ИКТ-использования, отождествленных с использованием вооруженных сил, а следовательно, способных породить право на самооборону. Хотя отдельные государства настаивают на таком тождестве, применяя принцип коллективной обороны к цифровой сфере, а равно оценивая вмешательство (зачастую не доказанное и не подтвержденное фактами) в свои суверенные дела с использованием ИКТ-технологий в качестве акта агрессии, что позволяет им, согласно Таллиннскому мануалу, ответить на соответствующий «акт агрессии» как ударом с применением кинетического оружия, так и цифровых технологий, деструктивное воздействие которых может быть масштабнее и тяжелее любого существующего оружия.

Затруднение в определении средств обеспечения МИБ вызывает ограниченность одобряемых международным сообществом и не противоречащих международному праву способов, к которым может прибегнуть пострадавшая от атаки с использованием ИКТ сторона. Причем пробельность правовой регламентации отношений в рассматриваемой области ожидаемо ведет к невозможности судебного разрешения спорных ситуаций, а равно и тормозит развитие прецедентного права в данном направлении за отсутствие объективности, полноты доказательств, которые может предъявить пострадавшая от атак сторона, что неудивительно в условиях развития политической, но не технической атрибуции таких атак.

Как уже было отмечено, сложность технической атрибуции и упор, который делают некоторые государства на политическую атрибуцию (фактически на собственные догадки и доводы с позиции того, какому государству было бы «выгодно» атаковать данную сторону), тормозят процесс выработки норм, обязывающих государства не предоставлять свой национальный сегмент цифрового пространства, а равно и не допускать его использование для агрессивного поведения в отношении третьего государства.

При определении средств обеспечения МИБ был проведен учет существующих в международном праве средств обеспечения безопасности глобального пространства, был произведен анализ терминов «информационное оружие» и «кибероружие». Выдвигается положение о том, что информационное оружие не является оружием как таковым, но представляет собой

совокупность информационно-коммуникационных технологий (будь то код, программа, т.е. нематериальное, но идеальное устройство), воздействующих деструктивно на социально-экономическую, политическую сферу государства, а равно дестабилизирующих когнитивные функции населения пострадавшего государства. Вследствие чего установление контроля над «информационным оружием» невозможно, потому единственными оптимальными и приемлемыми средствами обеспечения МИБ являются мирные средства разрешения споров, меры по укреплению доверия, открытости и стратегической стабильности мира, деятельность международных организаций. Очевидно, что главным условием успешного использования указанных средств может стать абсолютное, безотлагательное соблюдение государствами таких основополагающих принципов, как невмешательство во внутренние дела государств и неприменение силы или угрозы силой с применением ИКТ. В перспективе международному сообществу может быть рекомендовано создание Международного суда по инцидентам в ИКТ-сфере.

БИБЛИОГРАФИЯ

1. *Батырь В. А.* Новые вызовы XXI века в сфере развития средств вооруженной борьбы // Евразийский юридический журнал. — 2014. — № 2 (69). — С. 76–81.
2. *Богданов А. Н.* «Американская однополярность» и системный баланс сил в начале XXI в. // Вестник Санкт-Петербургского университета. Политология. Международные отношения. — 2015. — № 2. — С. 96–97.
3. *Данельян А. А.* Международно-правовое регулирование киберпространства // Образование и право. — 2020. — № 1.
4. *Ильинская О. И.* К вопросу о способах обеспечения выполнения международных договоров // Актуальные проблемы российского права. — 2011. — № 3. — С. 238–243.
5. *Каберник В. В.* Проблемы классификации кибероружия // Вестник МГИМО-Университета. — 2013. — № 2 (29). — С. 72–78.
6. *Коротков А. В.*, *Зиновьева Е. С.* Безопасность критических информационных инфраструктур в международном гуманитарном праве // Вестник МГИМО-Университета. — 2011. — № 4. — С. 154–162.
7. *Крутских А. В.* К политико-правовым основаниям глобальной информационной безопасности // Международные процессы. — 2007. — Т. 5. — № 1 (13). — С. 28–37.
8. *Лукашук И. И.* Международное право. Общая часть. — 2-е изд. — М., 2004.
9. *Лукин А. Л.* Литтл Р. Баланс сил в международных отношениях: метафоры, мифы и модели (реферат) // Политическая наука. — 2011. — № 2. — С. 258–265.
10. *Ромашкина Н. П.* Вооружения без контроля: современные угрозы международной информационной безопасности // Пути к миру и безопасности. — 2018. — № 2 (55). — С. 64–83.
11. *Харрис Ш.* Кибервойна: пятый театр военных действий. — М. : Альпина нон-фикшн, 2016.
12. *Baseley-Walker B.* Transparency and confidence-building measures in cyberspace: towards norms of behavior // UNIDIR. Disarmament Forum, «Confronting cyberconflict». — 2011. — Iss. 4. — P. 31–40. — URL: http://www.unidir.org/files/publications/pdfs/confronting-cyberconflict-en-317.pdf.
13. *Hague W.* Security and freedom in the cyber age — seeking the rules of the road : Speech to the Munich Security Conference, 4 February 2011 // URL: https://www.gov.uk/government/speeches/security-and-freedom-in-the-cyber-age-seeking-the-rules-of-the-road.
14. ICRC Expert Meeting: The Potential Human Cost of Cyber Operations / eds L. Gisel and L. Olejnik. — ICRC, Geneva, 2019. — URL: www.icrc.or//ownloa/il/600/he-potential-human-cost-of-cyber-operations.pdf.
15. *Lee B. Bagheri, Kao H.* A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems // Manufacturing Letters. — 2015. — Vol. 3. — P. 18–23.
16. *Mele S.* Cyber-Weapons: Legal and Strategic Aspects (Version 2.0) (June 7, 2013) // URL: https://ssrn.com/abstract=2518212.

17. *Rid T.*, *McBurney P.* Cyber-Weapons // The RUSI Journal. — 2012. — Vol. 157. — Iss. 1. — P. 6–13. — DOI: 10.1080/03071847.2012.664354.
18. Russia — US Bilateral on Cybersecurity. Critical Terminology foundations. EastWest Institute Worldwise Cybersecurity Initiative, Moscow state university information security institute. November 2013 // URL: http://wiki.informationsecurity.club/lib/exe/fetch.php?media=documents_all:russia-u_s_bilateral_on_terminology_rus.pdf.

Материал поступил в редакцию 5 октября 2021 г.

REFERENCES (TRANSLITERATION)

1. Batyr V. A. Novye vyzovy XXI veka v sfere razvitiya sredstv vooruzhennoj borby // Evrazijskij yuridicheskij zhurnal. — 2014. — № 1 (69). — S. 76–81.
2. Bogdanov A. N. «Amerikanskaya odnopolyarnost» i sistemnyj balans sil v nachale XXI v. // Vestnik Sankt-Peterburgskogo universiteta. Politologiya. Mezhdunarodnye otnosheniya. — 2015. — № 2. — S. 96–97.
3. Danelyan A. A. Mezhdunarodno-pravovoe regulirovanie kiberprostranstva // Obrazovanie i pravo. — 2020. — № 1.
4. Ilinskaya O. I. K voprosu o sposobah obespecheniya vypolneniya mezhdunarodnyh dogovorov // Aktualnye problemy rossijskogo prava. — 2011. — № 3. — S. 238–243.
5. Kabernik V. V. Problemy klassifikacii kiberoruzhiya // Vestnik MGIMO-Universiteta. — 2013. — № 1 (29). — S. 72–78.
6. Korotkov A. V., Zinoveva E. S. Bezopasnost kriticheskih informacionnyh infrastruktur v mezhdunarodnom gumanitarnom prave // Vestnik MGIMO-Universiteta. — 2011. — № 4. — S. 154–162.
7. Krutskih A. V. K politiko-pravovym osnovaniyam globalnoj informacionnoj bezopasnosti // Mezhdunarodnye processy. — 2007. — T. 5. — № 1 (13). — S. 28–37.
8. Lukashuk I. I. Mezhdunarodnoe pravo. Obshchaya chast. — 2-e izd. — M., 2004.
9. Lukin A. L. Littl R. Balans sil v mezhdunarodnyh otnosheniyah: metafory, mify i modeli (referat) // Politicheskaya nauka. — 2011. — № 2. — S. 258–265.
10. Romashkina N. P. Vooruzheniya bez kontrolya: sovremennye ugrozy mezhdunarodnoj informacionnoj bezopasnosti // Puti k miru i bezopasnosti. — 2018. — № 1 (55). — S. 64–83.
11. Harris Sh. Kibervojna: pyatyj teatr voennyh dejstvij. — M. : Alpina non-fikshn, 2016.
12. Baseley-Walker B. Transparency and confidence-building measures in cyberspace: towards norms of behavior // UNIDIR. Disarmament Forum, «Confronting cyberconflict». — 2011. — Iss. 4. — P. 31–40. — URL: http://www.unidir.org/files/publications/pdfs/confronting-cyberconflict-en-317.pdf.
13. Hague W. Security and freedom in the cyber age — seeking the rules of the road: Speech to the Munich Security Conference, 4 February 2011 // URL: https://www.gov.uk/government/speeches/security-and-freedom-in-the-cyber-age-seeking-the-rules-of-the-road.
14. ICRC Expert Meeting: The Potential Human Cost of Cyber Operations / eds L. Gisel and L. Olejnik. — ICRC, Geneva, 2019. — URL: www.icrc.or//ownloa/il/600/he-potential-human-cost-of-cyber-operations.pdf.
15. Lee B. Bagheri, Kao H. A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems // Manufacturing Letters. — 2015. — Vol. 3. — P. 18–23.
16. Mele S. Cyber-Weapons: Legal and Strategic Aspects (Version 2.0) (June 7, 2013) // URL: https://ssrn.com/abstract=2518212.
17. Rid T., McBurney P. Cyber-Weapons // The RUSI Journal. — 2012. — Vol. 157. — Iss. 1. — P. 6–13. — DOI: 10.1080/03071847.2012.664354.
18. Russia — US Bilateral on Cybersecurity. Critical Terminology foundations. EastWest Institute Worldwise Cybersecurity Initiative, Moscow state university information security institute. November 2013 // URL: http://wiki.informationsecurity.club/lib/exe/fetch.php?media=documents_all:russia-u_s_bilateral_on_terminology_rus.pdf.