DOI: 10.48137/2074–2975_2022_5-6_66
УДК 327.(470+571).004

Информационно-коммуникационные технологии и информационная безопасность России

Владимир ШТОЛЬ
Александр ЗАДОХИН

Начало XXI столетия ознаменовалось стремительным развитием систем телекоммуникации и программного обеспечения. Появление глобального Интернета не только объединило пользователей компьютеров, но обеспечило свободный обмен разнообразной информацией в режиме реального времени и способствовало стиранию границ между государствами в информационном пространстве.

Помимо удобств и благ для пользователей современные информационно-коммуникационные технологии (ИКТ) несут вызовы и угрозы. Поэтому объективно стоит задача ослабить уязвимость их вредоносного использования и уж тем более не допустить перерастания угроз в цифровой сфере в серьёзный вооружённый конфликт.

Пандемия новой коронавирусной инфекции, заставившая перевести в онлайн целые кластеры нашей жизнедеятельности – от проведения деловых встреч до приобретения товаров, наглядно продемонстрировала мировую зависимость и уязвимость от ИКТ.

ШТОЛЬ Владимир Владимирович – доктор политических наук, профессор, профессор кафедры международных отношений Дипломатической академии МИД России. *E-mail:* v.shtol@gmail.com

ЗАДОХИН Александр Григорьевич – доктор политических наук, Почётный профессор Дипломатической академии МИД России. *E-mail:* aleksander_1945@mail.ru

Ключевые слова: информационно-коммуникационные технологии, национальная безопасность, терроризм, Россия, США.

Перечисляются угрозы в сфере международной информационной безопасности (МИБ): использование ИКТ и самих ИКТ в военно-политических, преступных и террористических целях.

Военно-политическое измерение угроз в сфере МИБ включает:

– использование ИКТ для подрыва суверенитета и нарушение территориальной целостности государств;

– подготовку и реализацию планов по проведению информационных операций и войн;

– вмешательство во внутренние дела государства;

– разжигание межэтнических, межрасовых и межконфессиональных конфликтов.

Преступность в информационном пространстве имеет глобальный характер и затрагивает все страны. Киберпреступники наносят значительный ущерб экономической деятельности государств, благополучию миллионов людей. Речь идёт о потерях, сопоставимых с эффектом от военных действий. Киберкриминал всё чаще используется в качестве маскировки для подрыва общественно-политической и социально-экономической обстановки внутри государств, несёт угрозу их суверенитету.

Широкое распространение таких противоправных практик, как фишинг, *DDoS-атаки*, различные вирусы-вымогатели, наносят колоссальный вред как технологически развитым, так и особенно развивающимся странам.

Большой опасностью для мира является использование ИКТ в качестве инструмента для пропаганды идеологии терроризма, привлечения к экстремистской и террористической деятельности новых сторонников, а также для организации коммуникации между ячейками этих организаций, планирования терактов, сбора финансовых средств и т. д.

Новые цифровые технологии

Новые цифровые технологии, создавая трансграничные коммуникации, бросают вызов национальному государству и исторически сложившемуся мировому порядку, основанному на принципах международного права, в том числе на принципе государственного суверенитета и территориальной целостности государств, а также культурной идентичности.

Более того, создание всё новых и новых цифровых технологий оказывает своё влияние на социальные отношения. Возникла новая виртуальная окружающая человека среда, которая не фиксируется его физическими рецепторами, но как чёрные дыры в космосе втягивает его в себя.

Пока футурологи размышляют о будущем развития цифровых технологий, бизнес-структуры осваивают новое рыночное пространство – производство мощных компьютеров, мобильных средств связи, машин с искусственным интеллектом, новейших роботов-андроидов, блокчейн-технологий и криптовалюты. Современный бизнес, прочно встав на цифровые рельсы, не способен себя защитить самостоятельно от действия киберпреступников.

Ущерб мировому бизнесу только от кибератак увеличивается из года в год.

В 2016 г. он составил 445 млрд долл., в 2017 г. – 1 трлн долл., в 2019 г. – более 2,5 трлн долл. [1], а в 2022 г., по прогнозу Всемирного экономического форума, сумма может вырасти до 8 трлн долл.

По данным Лаборатории Касперского, количество киберинцидентов в российских компаниях в первом квартале 2022 г. увеличилось в 4 раза. Такой рост связан в первую очередь с постоянным усложнением ландшафта угроз и расширением поверхности атак: злоумышленники используют разные тактики и техники, в том числе комбинированные.

Появились и активно действуют сообщества хакеров, куда могут входить как самоутверждающиеся хакеры-альтруисты, так и хакеры с определёнными, часто антигуманными целями, находящиеся на службе частных компаний и спецслужб. Исследователи квалифицируют кибератаку как информационно-коммуникационный акт, предпринимаемый с определёнными преступными целями, а именно для:

– проникновения в информационно-компьютерную систему государственных и негосударственных структур;

– проникновения в информационно-компьютерную систему частного лица;

– внедрения вируса в информационно-компьютерную систему государственных, негосударственных структур и частных лиц;

– создания информации с целью монетизации и шантажа;

– ведения кибервойн и т. д. [2].

Зафиксировано, что большинство современных кибератак исходит из стран Восточной Европы и осуществляется хакерами-одиночками просто ради самореализации [3]. В результате колоссальный ущерб наносится мировой экономике. Кроме того, на его ликвидацию и обеспечение информационной безопасности требуются значительные ресурсы. При этом обеспечить безопасность в цифровом пространстве самостоятельно неспособно ни одно государство.

В частности, российская экономика потеряла от преступной деятельности хакеров только в 2020 г. 3,5 трлн руб. [4], и такие потери ежегодно растут.

Научные разработки в сфере кибертехнологий продолжаются всё возрастающими темпами. Параллельно с использованием и развитием обычных вооружений разворачивается производство автономных средств на основе технологий искусственного интеллекта, что увеличивает соответствующие вызовы.

Хотя большинство государств осознаёт реальную опасность вызовов и угроз в цифровой среде и необходимость установления универсальных

---

[1] *Мельникова О. А.* Способно ли бизнес-сообщество внести свой вклад в активизацию переговорного процесса по вопросам международной информационной безопасности? // Международная жизнь. 2021. № 3.

[2] *Туктамышев Б. В.* Международно-правовое регулирование кибератак // URL: http://www.oboznik.ru/?p=54277

[3] *Степанова Ю., Тишина Ю.* Тёмная сторона даркнета // Коммерсантъ. 2021. 19 марта.

[4] Коммерсантъ. 2021. 30 июля.

международных регламентов использования информационно-коммуникационных технологий, но до сих пор отсутствуют всеобъемлющие международно-правовые договорённости в этой сфере.

Информационная безопасность

В настоящий момент просматривается тенденция разнонаправленной и хаотичной эволюции системы международных и национальных коммуникаций. В этом процессе, как отмечают исследователи, происходит значительное ограничение возможностей государства как регулятора, защитника своей инфраструктуры и своего информационного суверенитета. Это связано с появлением новых субъектов мировой политики, представленных различными общественными и политическими движениями, а также отдельными акторами.

При этом у целого ряда государств, и прежде всего постоянных членов Совета Безопасности ООН, обозначились разные подходы к вопросу о возможности регламентации использования ИКТ с учётом того, что в глобальном киберпространстве развернулась конкуренция национальных информационных стратегий, не учитывающая объективной необходимости укрепления глобальной безопасности.

США, как лидер коллективного Запада, пытаются навязать свои правила игры в вопросах организации информационного пространства, когда не принимаются во внимание, а порой и просто игнорируются интересы других государств и международное право.

Западные страны стремятся закрепить своё технологическое лидерство, узурпировать право самостоятельно и бездоказательно назначать ответственных в киберинцидентах, а также предпринимать односторонние силовые шаги в сфере ИКТ. Продвигаемые ими механизмы размывают ключевую роль ООН, становятся помехой для выстраивания системы международных отношений, отвечающей требованиям современной реальности, а при неблагоприятном стечении обстоятельств могут превратить мировое информпространство в новый театр военных действий.

При этом надо понимать, что глобальное по своей сути цифровое пространство не имеет границ. В силу этих причин ни одно государство не способно в одиночку защитить себя от подобных угроз.

Одними из важных проблем политики международной безопасности являются вопросы управления Интернетом.

Составной частью интернет-среды стало сообщество активных и пассивных, профессиональных и бытовых пользователей сетей Интернета со своим опытом и институтами, которые сформировали глобальное сетевое сообщество со специфической субкультурой и правилами, нередко идущих вразрез с общепринятыми традициями и ценностями.

Нельзя отрицать, что глобальные кибернетические сети обеспечили доступ широкого круга пользователей к разнообразной информации и новым ИКТ по всему миру. Именно появление сети Интернет наряду со

всеобщим распространением персональных компьютеров и телефонных приложений стало определяющим фактором в формировании и расширении трансграничного киберпространства при экспоненциально увеличивающемся числе его пользователей.

Из пространства коммуникации и обмена информации Интернет превращается в среду для тиражирования опасного и вредоносного контента, фишинговых программ, запрещённых и экстремистских материалов, сетевых вирусов. В настоящее время Интернет стал главной платформой как для распространения информации, так и политических манипуляций. Основным инструментом в этом являются уже не классические СМИ, а социальные сети и мессенджеры, которые при определённых условиях могут выступить источником дестабилизации любого общества и ресурсом давления на государственную власть [5].

Поэтому объективно возникла необходимость упорядочивания процессов в сетях Интернета, так как в определённой степени это стало вызовом национальным государствам и существующей модели организации мирового социума, не говоря уже о том, что Интернет стал использоваться в преступных целях, в частности, ИКТ способствовали началу своеобразной «нанотехнологической гонки вооружений».

При этом используются всё более совершенные инструменты информационного и психологического воздействия на пользователей Всемирной сети. Соответственно, актуален вопрос о разработке и создании механизма управления Интернетом. Очевидно, что речь может идти о международном формате под началом Организации Объединённых Наций.

Под эгидой ООН в Женеве (2003 г.) и Тунисе (2005 г.) прошли Всемирные встречи на высшем уровне по вопросам информационного общества. Для создания условий многостороннего политического диалога с участием всех заинтересованных сторон в рамках ООН в 2006 г. был создан Форум по управлению Интернетом *(Internet Govermance Forum – IGF)* .

Одним из вариантов могла бы стать передача прерогатив по управлению Интернетом Международному союзу электросвязи, который имеет необходимую экспертизу в этих вопросах. Но такой вариант противоречит подходам США, претендующим на свой контроль над Сетью.

Российская Федерация последовательно выступает за интернационализацию управления сетью Интернет, а также повышение роли государств в данном процессе. Нынешняя модель управления Интернетом, в которой нивелирована роль государств, являющихся гарантами прав и свобод своих граждан и играющих основную роль в вопросах его экономики, безопасности и стабильности критической информационной инфраструктуры, давно показала свою неэффективность и не обеспечивает гарантий безопасно-

[5] Замглавы МИД РФ Сыромолотов: Интернет стал большой платформой политических манипуляций. ТАСС. 5 февраля 2021 г. // URL: https://tass.ru/interviews/10631379?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com

сти пользователей Всемирной сети, а потому требует кардинального реформирования [5].

Возникшее интернет-пространство практически сразу превратилось в арену противоборства различных геополитических интересов и ценностей. Глобальные сети стали использоваться для вмешательства во внутренние дела государства, идеологического и психологического воздействия на общество и человека, размывания национальной культуры и распространения экстремистских идей.

В настоящее время в ряде стран осуществляется юридическая регламентация пользования Интернетом в границах национального пространства. В то же время сторонники либерального подхода и американские сетевые гиганты выступают за сохранение в Интернете существующего с момента его возникновения режима *free space*, объясняя это необходимостью якобы «соблюдения прав человека, свободы слова и самовыражения, свободы информации». Этой точки зрения придерживаются США, так как используют возможности социальных сетей *(Facebook, Twitter*, а также ресурсов типа *WikiLeaks)* для осуществления своей политики, вмешиваясь во внутренние дела суверенных государств и организуя различные «цветные революции» с целью свержения законных правительств под лозунгом «внедрения демократии».

При непосредственном участии Запада на Украине с начала 90-х годов, т. е. с провозглашением ею суверенитета, проводятся информационные провокационные акции, направленные на дискредитацию России и на формирование её негативного образа. В этой деятельности участвуют и западные СМИ, и интернет-каналы. Масштабы и интенсивность информационной войны вокруг украинского вопроса постоянно усиливаются с развитием информационно-телекоммуникационных технологий и использованием всё более изощрённых схем совершения киберпреступлений. С началом спецоперации России по демилитаризации и денацификации Украины резко увеличилось количество кибератак против информационных систем Российской Федерации.

Так, хакеры пытались атаковать сайты Роскосмоса, Роскомнадзора, Минобороны, Минкульта, Минэнерго, ФАС. Были временно недоступны сайты изданий ТАСС, «Коммерсантъ», РБК, «Известий», *RT* и других СМИ.

Была совершена кибератака на информационную инфраструктуру российского Министерства по чрезвычайным ситуациям. Подверглись хакерским атакам официальные сайты МЧС России и других федеральных и региональных структур страны.

Задача недопущения милитаризации информационного пространства становится особенно актуальной на фоне развития отдельными странами наступательных кибернетенциалов и распространения доктрин превентивных кибердударов. Предотвращение межгосударственной конфронтации в онлайн-среде становится одним из факторов стратегической стабильности.

США, бесцеремонно и агрессивно продвигающие американские ценности и идеи «демократии» во внешнее пространство, особо озабочены не просто «свободой передачи данных», но, как подчеркнул министр иностранных дел Российской Феде-

рации С. Лавров, стремятся навязать свои «правила игры». Уже звучали угрозы, что «если Москва… не примет изложенные на встрече президентов в Женеве 16 июня 2021 г. “правила игры”, то будет подвержена новому давлению» [6], в частности, с использованием военно-политического потенциала НАТО. Поэтому следует напомнить, как альянс относился и относится к безопасности Европы.

Во-первых, стратегический военный потенциал Америки в НАТО изначально был навязан европейцам сразу после окончания Второй мировой войны, чтобы в Европе было «меньше России».

Во-вторых, альянс во второй половине XX в. претендовал на роль защитника Западной Европы от советской угрозы, а начиная с 90-х годов – уже защитника от России не только западно- и восточноевропейских стран, но и всех постсоветских государств, считая их сферой своих национальных интересов. При этом США постоянно требовали от европейских союзников – членов НАТО увеличения своих военных бюджетов.

Нападение в цифровой среде рассматриваются НАТО в качестве неотъемлемой составляющей ведения войны в современных условиях.

В июне 2016 г. на саммите НАТО в Варшаве киберпространство было признано такой же сферой операций.

А в феврале 2017 г. были приняты обновлённый План кибероборонны и «дорожная карта» по освоению киберпространства как новой сферы операций.

На сегодняшний день большинство стран – членов альянса имеют собственные стратегии кибербезопасности и некоторые обладают киберкомандованиями с соответствующими подразделениями.

Важная роль в сфере укрепления киберпотенциала НАТО отводится странам, расположенным по периметру границ России, прежде всего Эстонии, Латвии, Литве, где уже не один год функционируют киберцентры, представляющие своего рода цифровые форпосты альянса для отработки стратегии информационно-гибридных войн.

Постбиполярную русофобскую политику Запада во главе с США вполне можно объяснить с помощью необихевиористской теории «фрустрации-агрессии» с возникновением у западных и особенно американских военно-политических элит «чувства неудовлетворённости»: они неудовлетворены тем, что, «встав с колен», Россия не приняла их «правила игры» и отвергла навязываемые ей «ценности».

Понимание информационной безопасности Российской Федерации сформулировано в Доктрине информационной безопасности Российской Федерации, которая «является основой для формирования государственной политики и развития общественных отношений в области обеспечения информационной безопасности, а также для выработки мер по совершенствованию системы обеспечения информационной безопасности» [7].

---

[6] *Лавров С.* О праве, правах и правилах // Коммерсантъ. 2021. 28 июля.

[7] Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ 5 декабря 2016 г. № 646) // URL: http://www.scrf.gov.ru/security/information/document5/

Особого внимания заслуживает утверждённая Указом Президента Российской Федерации от 2 июля 2021 г. № 400 обновлённая Стратегия национальной безопасности, которая впервые обозначила информационную безопасность как новый национальный приоритет.

Россия, наследуя миролюбивую внешнюю политику и опираясь на богатый тысячелетний духовно-культурный потенциал исторической России, выступает за мирное решение международных проблем и конфликтов.

Гуманитарные связи с различными странами мира являются основой для укрепления всестороннего сотрудничества.

С 60-х годов прошлого столетия в СССР действуют не только старые учебные заведения, но и создаются новые, где проходят обучение иностранные граждане. Кроме того, создаются культурные центры за рубежом, через которые реализуются разнообразные программы в области русского языка, искусства и литературы для доведения информации по вопросам образования, культуры и спорта, социально-экономической сфере, бизнеса до зарубежной общественности в целях формирования положительного образа нашей страны.

Более чем на 70 языках ведётся иновещание на десятки стран, осуществляются издания на различных языках мира.

Как представляется, у России большие возможности использовать опыт Советского Союза уже в цифровую эпоху для утверждения своей национальной идентичности и в киберпространстве. Это особенно актуально, поскольку коллективный Запад стремится сформировать негативный образ внешней политики России, фальсифицируя и переписывая итоги Второй мировой войны, стараясь Россию «превратить из страны-победителя в государство-агрессора» [8].

По сути дела, в киберпространстве разворачивается ещё один вид холодной войны против России [9].

Именно пытаясь потеснить Россию на всех мировых площадках, США, стремящиеся к доминированию и в глобальном киберпространстве, саботируют российские инициативы в ООН в области информационной безопасности [10]. И при этом Вашингтон одновременно предлагает «ограничивать развитие международной политико-правовой базы, регулирующей деятельность государств в информационном пространстве, рамками необязывающих политических документов» [11].

---

[8] *Мельникова О.* Информационное обеспечение внешнеполитической деятельности современных государств (политологический анализ). Автореферат дис. ... канд. полит. наук. М., 2020. С. 5.

[9] *Черненко Е. В.* Холодная война 2.0? Киберпространство как новая арена противостояния // Россия в глобальной политике. 2013. Т. 11. № 1.

[10] *Болгов Р. В.* Деятельность ООН в области информации и международные аспекты информационной безопасности России // Сравнительная политика. 2019. Т. 10. № 1.

[11] *Батуева Е. В.* Американская концепция угроз информационной безопасности и её международно-политическая составляющая. Автореферат дис. ... канд. полит. наук. М., 2014.

Вызовы глобальной информационной безопасности

На информационную кибербезопасность в будущем могут повлиять:

– тенденции развития информационных коммутационных технологий;

– рост числа пользователей компьютерными системами;

– размытие границ между цифровым и физическим миром;

– развитие скрытых сетей подобных «тёмному Интернету» и блокчейн-технологий;

– активное использование технологий искусственного интеллекта и сетевых роботов в военной сфере.

В перечень особых угроз глобальной информационной безопасности следует включить активную кибердеятельность военной организации НАТО.

Альянс считает возможным, что «при проведении всех своих операций и миссий Североатлантический союз в определённой степени будет опираться на гражданский госсектор или частный промышленный сектор, будь то в контексте инфраструктуры связи, логистики, оборудования (техники) или критически важных объектов инфраструктуры принимающей страны» [12], тем самым подвергая опасности жизнь гражданского населения, используя в том числе деятельность различных экстремистских организаций. Имея в своём составе хорошо подготовленных специалистов, эти структуры используют современные ИКТ для совершения различных актов агрессии и диверсий против объектов критической информационной инфраструктуры. Такая преступная деятельность развернулась в последние годы на Украине, с территории которой кибератаки против России осуществлялись одна за другой.

В отношении использования ИКТ западные эксперты занимают двойственную позицию.

Так, когда речь идёт об ответном кибердаре, они ссылаются на международное право, а когда о праве государства контролировать национальное киберпространство, то отрицают международно-правовой принцип национального суверенитета и, соответственно, право государства контролировать своё информационное пространство. В частности, немецкий профессор криминологии фон В. Хайнегг считает, что российские исследователи «надеются – будет наложен полный запрет на использование военной силы в киберпространстве», так как сама Россия отстаёт в развитии инновационных технологий [13].

Интересно, что так же отнеслись к предложению Российской империи созвать в 1899 г. в Гааге Первую Всемирную конференцию мира для обсуждения вопросов сохранения мира и сокращения вооружений. Западные государства, начавшие перевооружение своих армий и подготовку к большой войне, объяснили, что инициативы российского императора Николая II вызваны «отставанием России в области вооружений».

---

[12] *Брент Л.* Роль НАТО в кибернетическом пространстве // NATO. Review. 2019. 2 февраля.

[13] *Хайнегг В. фон.* Международное право и международная информационная безопасность: ответ Крутских и Стрельцову // URL: http://doc.knigi-x.ru

Тот факт, что информационные технологии позволяют совершать кибератаки, которые практически невозможно предотвратить, рассматривается рядом государств как необходимость совершения превентивных действий против потенциального и вероятного противника. Причём эксперты этих государств делают ссылку на ст. 51 Устава ООН, где фиксируется «неотъемлемое право государства прибегнуть к военной силе в порядке осуществления права на самооборону в случае вооружённого нападения, до тех пор, пока Совет Безопасности ООН не примет необходимых мер для поддержания международного мира и безопасности» [14]. Речь может идти не просто об отдельных кибератаках, а о спланированной кибероперации, когда могут применяться новые виды кибероружия и компьютерные программы, включая искусственный интеллект. Причём государство, решающее совершить этот превентивный шаг нападения, само определяет противника. В результате таких действий высока вероятность возникновения вооружённого киберконфликта. И это в то время, когда отсутствуют какие-либо международно-правовые договорённости о возможности международного контроля над использованием информационно-коммуникационных технологий в военных целях.

В заключение необходимо отметить, что:

– западные государства, обладающие мощным и развитым киберпотенциалом, рассчитывают на абсолютное доминирование в глобальном киберпространстве и приобретении стратегических преимуществ в информационной войне;

– происходит изменение логики глобального противостояния, когда интенсивное применение невоенных методов с использованием ИКТ приводит к достижению целей и без вооружённой борьбы;

– развивается тенденция к исчезновению промежуточных этапов между мирным состоянием международных отношений и переходом их в состояние войны, идёт размывание грани между обороной и нападением, ибо в цифровом информационном пространстве процесс развивается в режиме реального времени – «здесь и сейчас».

Безусловно, что потенциально наиболее тяжёлые последствия несут киберугрозы в области стратегических объектов. Именно поэтому вопрос международной информационной безопасности имеет глобальный характер не только с точки зрения уязвимости одного государства, но и масштаба возможных последствий для мира в целом.

В условиях кризиса постбиполярной системы стратегической стабильности и ликвидации международного контроля над вооружениями отсутствие в ближайшей перспективе возможности заключения договоров по регламентации использования кибертехнологий усугубляет проблемы международной информационной безопасности. Об этом свидетельствует украинский кризис.

---

[14] https://www.un.org/ru/about-us/un-charter/chapter-7.51

Вызывает беспокойство тот факт, что обострение международных отношений может произойти необязательно из-за действий одного государства. Информационную войну может спровоцировать самоутверждающийся хакер-националист, совершивший кибератаку со своего мобильного компьютера. Данный сценарий, по сути, может быть аналогом прецедента 18 июня 1914 г., когда националист Гавриил Принцип застрелил эрцгерцога Франца Фердинанда, что формально и послужило поводом к началу войны. Реальные военные действия, как известно, начались только через полтора месяца. Но в цифровую эпоху кибернетический «выстрел» может совершить автономный робот-андроид, то ли по «собственной воле», то ли в результате сбоя программы, и последующие катастрофические события будут разворачиваться в режиме реального времени без установленной III Гаагской конвенцией 1907 г. процедуры открытия военных действий или каким-то другим образом.

Именно поэтому главная цель России на международных переговорных площадках – закрепление на международном уровне подхода, основанного на предотвращении конфликтов с использованием ИКТ.

Закрепление чётких и одинаковых для всех «правил цифровой игры» позволило бы обеспечить большую предсказуемость поведения государств в информационном пространстве. Руководствуясь этими соображениями, Россия инициировала разработку под эгидой ООН универсальных правил, норм и принципов ответственного поведения государств в ИКТ-сфере.

Россия как один из инициаторов переговоров по вопросам международной информационной безопасности под эгидой ООН – первоначально в формате Группы правительственных экспертов, а с 2018 г. в рамках полноценного механизма Генеральной Ассамблеи – Рабочей группы ООН открытого состава – приветствует любые инициативы и предложения, направленные на обеспечение неконфликтного и безопасного информационного пространства.

Очевидно, что в дальнейшем потребуется разработка международной конвенции ООН в области цифровых технологий, которая должна определить концептуальные подходы к регулированию использования информационных технологий в военных целях, регламентировать их применение в отношении критически важных объектов инфраструктуры, включая гражданские объекты; а также сформулировать особые требования к разработке, созданию и распространению компьютерных программ обеспечения систем военного назначения или пригодных для подобного использования.

Библиография • References

Батуева Е. В. Американская концепция угроз информационной безопасности и её международно-политическая составляющая. Автореферат дис. ... канд. полит. наук. М., 2014. – 30 с.

[*Batueva E. V.* Amerikanskaya koncepciya ugroz informacionnoj bezopasnosti i eyo mezhdunarodno-politicheskaya sostavlyayushchaya. Avtoreferat dis. ... kand. polit. nauk. M., 2014. – 30 s.]

Болгов Р. В. Деятельность ООН в области информации и международные аспекты информационной безопасности России // Сравнительная политика. 2019. Т. 10. № 1. С. 59–69.

[*Bolgov R. V.* Deyatel'nost' OON v oblasti informacii i mezhdunarodnye aspekty informacionnoj bezopasnosti Rossii // Sravnitel'naya politika. 2019. T. 10. № 1. S. 59–69]

Брент Л. Роль НАТО в кибернетическом пространстве // NATO. Review. 2019. 2 февраля.

[*Brent L.* Rol' NATO v kiberneticheskom prostranstve // NATO. Review. 2019. 2 fevralya]

Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ 5 декабря 2016 г. № 646) // URL: http://www.scrf.gov.ru/security/information/document5/

[Doktrina informacionnoj bezopasnosti Rossijskoj Federacii (utv. Ukazom Prezidenta RF 5 dekabrya 2016 g. № 646) // URL: http://www.scrf.gov.ru/security/information/document5/]

Замглавы МИД РФ Сыромолотов: Интернет стал большой платформой политических манипуляций. ТАСС. 5 февраля 2021 г. // URL: https://tass.ru/interviews/10631379?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com

[Zamglavy MID RF Syromolotov: Internet stal bol'shoj platformoj politicheskih manipulyacij. TASS. 5 fevralya 2021 g. // URL: https://tass.ru/interviews/10631379?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com]

Коммерсантъ. 2021. 30 июля.

[Kommersant». 2021. 30 iyulya]

Лавров С. О праве, правах и правилах // Коммерсантъ. 2021. 28 июля.

[*Lavrov S.* O prave, pravah i pravilah // Kommersant». 2021. 28 iyulya]

Мельникова О. А. Способно ли бизнес-сообщество внести свой вклад в активизацию переговорного процесса по вопросам международной информационной безопасности? // Международная жизнь. 2021. № 3. С. 12–19.

[*Mel'nikova O. A.* Sposobno li biznes-soobshchestvo vnesti svoj vklad v aktivizaciyu peregovornogo processa po voprosam mezhdunarodnoj informacionnoj bezopasnosti? // Mezhdunarodnaya zhizn'. 2021. № 3. S. 12–19]

Мельникова О. Информационное обеспечение внешнеполитической деятельности современных государств (политологический анализ). Автореферат дис. ... канд. полит. наук. М., 2020. – 31 с.

[*Mel'nikova O.* Informacionnoe obespechenie vneshnepoliticheskoj deyatel'nosti sovremennyh gosudarstv (politologicheskij analiz). Avtoreferat dis. ... kand. polit. nauk. M., 2020. – 31 s.]

Степанова Ю., Тишина Ю. Тёмная сторона даркнета // Коммерсантъ. 2021. 19 марта.

[*Stepanova YU., Tishina YU.* Tyomnaya storona darkneta // Kommersant». 2021. 19 marta]

Туктамышев Б. В. Международно-правовое регулирование кибератак // URL: http://www.oboznik.ru/?p=54277

[Tuktamyshev B. V. Mezhdunarodno-pravovoe regulirovanie kiberatak // URL: http://www.oboznik.ru/?p=54277]

Хайнегг В. фон. Международное право и международная информационная безопасность: ответ Крутских и Стрельцову // URL: http://doc.knigi-x.ru

[*Hajnegg V. fon.* Mezhdunarodnoe pravo i mezhdunarodnaya informacionnaya bezopasnost': otvet Krutskih i Strel'covu // URL: http://doc.knigi-x.ru]

Черненко Е. В. Холодная война 2.0? Киберпространство как новая арена противостояния // Россия в глобальной политике. 2013. Т. 11. № 1. С. 162–170.

[*CHernenko E. V.* Holodnaya vojna 2.0? Kiberprostranstvo kak novaya arena protivostoyaniya // Rossiya v global'noj politike. 2013. T. 11. № 1. S. 162–170]

https://www.un.org/ru/about-us/un-charter/chapter-7.51

Статья поступила в редакцию 29 марта 2022 г.