МЕЖДУНАРОДНОЕ ПРАВО, ЕВРОПЕЙСКОЕ ПРАВО, ИНФОРМАЦИОННОЕ ПРАВО

К ВОПРОСУ О МЕЖДУНАРОДНО-ПРАВОВОЙ КОНЦЕПЦИИ УГРОЗ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КАПУСТИН Анатолий Яковлевич, первый заместитель директора Института законодательства и сравнительного правоведения при Правительстве Российской Федерации, доктор юридических наук, профессор
117218, Россия, г. Москва, ул. Большая Черемушkinsкая, 34
E-mail: Kapustin@izak.ru

Актуальность разработки международно-правовой концепции киберугроз определяется тем, что за последние десятилетия в результате научно-технологического прогресса складываются новые сферы межгосударственных отношений. Одним из технологических феноменов современности является Интернет. В статье рассматриваются проблемы становления международно-правовой концепции киберугроз. Одной из ключевых задач видится разработка международно-правовых вопросов определения угроз международной информационной безопасности или киберугроз. В связи с этим рассмотрены основные характеристики киберпространства и факторы, влияющие на степень его уязвимости от внешних воздействий. На основе анализа стратегических документов России и правовой доктрины разработано понимание киберугрозы и основных форм ее реализации: от простейших (кибервмешательство) до более сложных (кибератака).

На примерах возможных способов совершения кибератак предлагается международно-правовая квалификация деяний государств, совершенных против как информации, так и информационных систем. Рассматривается теоретическая обоснованность применимости категория «сила» к понятию кибератаки в контексте международно-правового запрета применения вооруженной силы.

Анализ международно-правовой доктрины, а также документов ООН, прежде всего резолюций Генеральной Ассамблеи ООН и Доклада Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности позволяет сделать вывод, что в настоящее время идет разработка международно-правовых мер противодействия угрозам международной безопасности в киберпространстве, складывается «мягкое» регулирование деятельности государств в сфере информационно-коммуникационных технологий, направленное на обеспечение добровольного соблюдения ими соответствующих обязательств в киберпространстве (нормы, правила и принципы ответственного поведения государств, меры по наращиванию потенциала, необходимость соблюдения международного права и его применимости к использованию информационно-коммуникационных технологий).

Ключевые слова: международное право, международно-правовое регулирование новых сфер межгосударственных отношений, кибербезопасность, киберугрозы, Интернет, киберпространство, кибервмешательство, кибератака (кибернападение), кибероперация, категория «сила», Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности.

THE QUESTION OF THE INTERNATIONAL LEGAL CONCEPT OF THREATS TO INTERNATIONAL INFORMATION SECURITY

A. Ya. KAPUSTIN, first deputy director of the Institute of Legislation and Comparative Law under the Government of the Russian Federation, doctor of legal sciences, professor
34, Bolshaya Cheremushkinskaya st., Moscow, Russia, 117218
E-mail: Kapustin@izak.ru

The importance of the development of the international legal concept of cyber threats is determined by the fact that new spheres of interstate relations are occurring as a result of scientific and technological progress over the past decades. One of the technological phenomena of present time is the Internet. The article deals with the problems of the formation of the international legal concept of cyber threats. One of these key tasks is the development of international legal issues to identify threats to international information security or cyber threats. For this purpose, the main characteristics of cyberspace and factors affecting the degree of its vulnerability from external influences are considered. The understanding of the cyber threat and its main forms of implementation has been developed on the basis of the analysis of Russia's strategic documents and legal doctrine: from the simplest (cyber-interference) to more complex (cyber-attack).

The international legal qualification of acts of states committed both against information and against information systems is proposed on the examples of possible ways to commit cyber-attacks. The theoretical validity of the applicability of the category "force" to the concept of cyber-attack in the context of the international legal prohibition of the use of armed force is considered. The

analysis of the international legal doctrine, as well as the UN documents, first of all the resolutions of the UN General Assembly and the Report of the Group of Governmental Experts on the achievements in the field of information and telecommunications in the context of international security, allows us to conclude that at present times the international legal measures are being developed to counter threats to the international security in cyberspace, the “soft regulation” of state activities in the field of ICT is forming, aimed at ensuring voluntary compliance with their respective obligations in cyberspace (rules, regulations and the principles of responsible conduct of states, capacity-building measures, the need to respect international law and its applicability to the use of ICT).

Keywords: international law, international legal regulation of new spheres of interstate relations, cyber security, cyber threats, the Internet, cyberspace, cyber interference, cyber-attack, cyber operations, “force” category, Report of the Group of Governmental Experts on the achievements in the field of information and telecommunications in the context of international security.

DOI: 10.12737/article_5a1e71d7026536.36788152

Современное международное право, сохраняя свое значение важнейшего нормативного регулятора межгосударственных отношений, призванного обеспечить стабильность международного порядка и прежде всего поддержание международного мира и безопасности, сталкивается с необходимостью включения в орбиту своего воздействия новых сфер отношений, формирующихся в том числе под воздействием научно-технологического прогресса. Одним из технологических феноменов современности, оказывающих глубокое влияние на жизнедеятельность человека и облик мира в целом, является Интернет, представляющий собой сложную единую информационно-техническую систему, включающую наряду с техническим и социальный компонент¹. Развитие интернет-технологий, расширяя социальные сферы его применения, по признанию специалистов, «диверсифицирует правовое регулирование значительного числа общественных отношений как на национальном, так и на международном уровне, а также вызывает необходимость правового регулирования новых общественных отношений»².

Разумеется, становление международно-правового регулирования новых сфер международных отношений — процесс не одномоментный, занимающий продолжительное время, требующий внимательного изучения государствами всех сторон и аспектов новых явлений. Такое отношение характерно и для реакции международного права на Интернет. До настоящего времени Интернет так и не стал предметом международно-правового регулирования или хотя бы международно-правового управления. Конвенция Совета Европы о преступности в сфере компьютерной информации 2001 г.³ затрагивает лишь один, пусть и

важный, вопрос, связанный со стремлением наладить международное сотрудничество в борьбе с использованием Интернета в преступных целях.

Между тем сегодня ни у кого не вызывает сомнений, что Интернет имеет международное значение как в связи с его трансграничным функционированием и использованием, так и в связи с тем, что международное сообщество признает важную роль Интернета, открывающего широкие возможности для развития цивилизации и построения глобального информационного общества⁴. В связи с этим для разработки концепции международно-правового регулирования Интернета необходим анализ его использования государствами в сфере межгосударственных отношений. Среди этих вопросов на первый план выступают проблемы обеспечения международного мира и безопасности в контексте использования информационно-коммуникационных технологий (ИКТ).

Государства еще в 1990-х гг. осознали негативный аспект неконтролируемого использования ИКТ в международных отношениях⁵. Однако продвиже-

ме государств — членов Совета Европы открыта для участия иных государств.

⁴ Генеральная Ассамблея ООН в 2016 г. отметила, что «распространение и использование информационных технологий и средств затрагивают интересы всего международного сообщества». См.: Резолюция Генеральной Ассамблеи ООН 71/28 «Достижения в сфере информации и телекоммуникаций в контексте международной безопасности». Дос. ООН A/Res/71/28. URL: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N16/399/53/PDF/N1639953.pdf?OpenElement>.

⁵ В 1998 г. Россия предложила США подписать на уровне президентов двух стран Коммюнике, посвященное вопросам регулирования обеспечения международной информационной безопасности, в котором указывалось, что реальное существование этих угроз определяет необходимость принятия превентивных мер. Эта инициатива не увенчалась успехом, хотя некоторые озабоченности были зафиксированы в Совместном заявлении сторон об общих вызовах безопасности на рубеже XXI в. В том же году по инициативе России Генеральная Ассамблея ООН приняла без голосования резолюцию «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» (53/70). Негативная позиция США по вопросу возможности международно-правового определения информационного оружия,

¹ См.: Информационное право: актуальные проблемы теории и практики: кол. монография / под общ. ред. И. Л. Бачило. М., 2009. С. 119—120.

² См.: Касенова М. Б. Правовое регулирование трансграничного функционирования и использования Интернета: автореф. дис. ... д-ра юрид. наук. М., 2016. С. 3.

³ В 2003 г. к этой Конвенции принят Дополнительный протокол относительно введения уголовной ответственности за правонарушения, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных систем. Россия в Конвенции не участвует. Конвенция кро-

ние вперед в деле создания международно-правового механизма противодействия угрозам международной информационной безопасности особо не ощущается, он так и не сформирован до настоящего времени⁶. В Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы⁷ также отмечено, что «международно-правовые механизмы, позволяющие отстаивать суверенное право государств на регулирование информационного пространства, в том числе в национальном сегменте сети “Интернет”, не установлены».

Новизна правовых проблем, с которыми сталкивается человечество в сфере использования ИКТ, обуславливает теоретическую и практическую значимость систематизации фактического материала для формирования категориального аппарата. Одной из таких ключевых задач видится разработка международно-правовых вопросов определения угроз международной информационной безопасности, или киберугроз.

В стратегических документах и законодательных актах России используется различная терминология для обозначения сети Интернет или информационного пространства. Так, в Федеральном законе от 27 июня 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» употребляются термины «информация», «информационная система», «информационно-телекоммуникационные сети» и др. В Концепции внешней политики Российской Федерации 2016 года⁸ встречаются термины «информационное пространство», «информационно-телекоммуникационная сеть “Интернет”». В Стратегию развития информационного общества в

информационной войны и установления международно-правового режима запрета враждебного использования ИКТ скорее всего была продиктована стремлением не ограничивать себя международно-правовыми обязательствами и сохранить свободу, надеясь на длительное технологическое преимущество в данной сфере. Аналогичным образом объяснялось отрицательное отношение США к идее создания международной организации по управлению Интернетом. См.: Касенова М. Б. Международно-правовое управление Интернетом. М., 2010. С. 68—72.

⁶ Хотя происходят некоторые подвижки в этом направлении, потому что в резолюции Генеральной Ассамблеи ООН 71/28, принятой 9 декабря 2016 г., сообщается о начале работы Группы правительственных экспертов, которая должна выработать общее понимание: исследование существующих и потенциальных угроз в сфере информационной безопасности и возможных совместных мер по их устранению и того, как международное право применяется к использованию ИКТ государствами, а также норм, правил и принципов ответственного поведения государств, мер укрепления доверия и наращивания потенциала и концепций. См.: Дос. ООН A/Res/71/28.

⁷ Утв. Указом Президента РФ от 9 мая 2017 г. № 203.

⁸ Утв. Указом Президента РФ от 30 ноября 2016 г. № 640.

Российской Федерации на 2017—2030 годы введены понятия «информационное пространство», «объекты критической информационной инфраструктуры»⁹.

В то же время в официальных документах наряду с понятием «Интернет» или «информационное пространство» используются выражения с приставкой «кибер», подчеркивающие связь объектов или действий с Интернетом. Например, в Концепции внешней политики Российской Федерации 2016 г. при характеристике вызовов и угроз, имеющих трансграничную природу, упоминается «киберпреступность». В свою очередь, гл. 28 УК РФ называется «Преступления в сфере компьютерной информации», в ней, например, дается определение состава преступления «неправомерный доступ к охраняемой законом компьютерной информации» (ст. 272) или «создание, использование и распространение вредоносных компьютерных программ» (ст. 273).

По мнению М. Б. Касеновой, такие различия в терминологическом употреблении, правовом значении и содержательных характеристиках обусловлены релевантностью их перевода с английского на национальные языки¹⁰. Вместе с тем в зарубежной и отечественной литературе для обозначения Интернета и производных от него выражений все шире прибегают к термину «киберпространство» и иным словам, содержащим приставку «кибер»¹¹. Понятия «угрозы государственной, экономической и общественной безопасности, исходящие из информационного пространства» (см. Концепцию внешней политики Российской Федерации 2016 г.) и «киберугрозы» близки, но не тождественны, тем не менее в дальнейшем для определения предмета исследования будет использоваться термин «киберугрозы».

Прежде чем приступить к анализу киберугрозы как ситуации, которая складывается в связи с использованием глобального киберпространства, имеет смысл

⁹ К таким объектам относятся информационные системы и информационно-телекоммуникационные сети государственных органов, а также информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления технологическими процессами, функционирующие в оборонной промышленности, в сфере здравоохранения, транспорта, связи, в кредитно-финансовой сфере, энергетике, топливной, атомной, ракетно-космической, горнодобывающей, металлургической и химической промышленности.

¹⁰ См.: Касенова М. Б. Правовое регулирование трансграничного функционирования и использования Интернета. С. 27.

¹¹ См., например: Киберпространство БРИКС: правовое измерение: монография. М., 2017; Хуторной С. Н. Киберпространство и становление сетевого общества: автореф. дис. ... канд. филос. наук. Воронеж, 2013; Kamal A. The Law of Cyberspace. An Invitation to the Table of Negotiations. Geneva, 2006; The International Dimensions of Cyberspace Law. Aldershot, 2000.

хотя бы коротко дать ему характеристику. Киберпространство было популярным определять как «становление цифрового мира», как «сложнейший феномен, созданный глобальной сетью компьютеров, которая использует телекоммуникационную инфраструктуру для передачи электронных посланий»¹². Оценивая степень подверженности Интернета или киберпространства внешним угрозам, можно выделить следующие его черты, позволяющие отличить его от иных сфер человеческой деятельности. Прежде всего следует отметить глобальный характер киберпространства: благодаря своим уникальным возможностям оно объединяет народы всех регионов и континентов Земли. Это весьма позитивный фактор, позволяющий утверждать, что «самой значительной определяющей характеристикой цифровых рубежей является бесполезность географических границ. Киберпространство — это трансграничные электронные коммуникации»¹³.

Тем не менее нельзя пройти мимо некоторых из его свойств, создающих благоприятную почву для злоупотреблений и потенциально опасных действий для других пользователей Интернета. Развитие ИКТ достигло такого уровня, что позволяет говорить о высокой степени зависимости современного мира от Интернета благодаря его тесной связи с важнейшими сферами жизнедеятельности современного общества (энергетикой, транспортом, телекоммуникациями, здравоохранением, государственными услугами и т. д.). Благодаря этому качеству складывается высокая степень уязвимости информационного общества от бесперебойного функционирования ИКТ. Автоматизация является усугубляющим данную ситуацию фактором. Все виды компьютеризованных устройств обновляются с автоматическими функциями подключения, что мы наблюдаем в случае Интернета вещей. К этому можно добавить анонимность и практически абсолютную неопределенность местонахождения лиц, вмешивающихся в деятельность компьютерной сети, что также способствует росту уязвимости киберпространства.

Таким образом, социально значимые характеристики киберпространства, делающие его удобной сферой для всевозможных злоупотреблений, позволяют сформулировать концепцию киберугроз и проанализировать возможные формы совершения действий в информационной сфере, которые могут приводить к причинению реального ущерба субъектам информационных отношений.

В Доктрине информационной безопасности Российской Федерации 2016 г.¹⁴ для характеристики при-

менения информационных технологий в неблагоприятных для национальных интересов страны целях используются весьма нейтральные выражения «информационное воздействие» или «информационно-техническое воздействие». Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» содержит два понятия: «компьютерная атака» и «компьютерный инцидент»¹⁵. В Докладе Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (далее — Доклад) встречаются более определенные понятия, например «злонамеренное использование ИКТ», «пагубные нападения», «вредоносные нападения»¹⁶. Если понятие «использования ИКТ» без эпитета «злонамеренное» еще может свидетельствовать о правомерном поведении субъектов в киберпространстве, то термин «нападение» без каких-либо дополнительных характеристик, указывающих на его противоправность, произвольно ассоциируется с недружелюбным действием, способным причинить ущерб¹⁷.

Для объективной оценки международно-правового регулирования противодействия киберугрозам необходимо иметь в виду, что оно находится еще на начальном этапе развития. Первые международные договоры о сотрудничестве государств в борьбе с киберугрозами разрабатываются и принимаются на региональном уровне. Так, Совет Европы принял ряд международно-правовых актов по сотрудничеству в сфере информации (Конвенция о защите физических лиц при автоматизированной обработке персональных данных 1981 г. и др.), в их числе упомянутая выше Конвенция о преступности в сфере компьютерной информации. Данный документ обязывает участников криминализировать преступные виды использо-

¹⁵ Вступает в силу с 1 января 2018 г.

¹⁶ Док. ООН А/70/174. В этом Докладе отмечаются тревожные тенденции в глобальной ИКТ-среде, создающие угрозу для всех государств, а злонамеренное использование ИКТ может нанести ущерб международному миру и безопасности. Ряд государств занимается наращиванием потенциала в сфере ИКТ для военных целей, опасность вредоносных нападений с использованием ИКТ на критически важную инфраструктуру является реальной и серьезной. Существует все более реальная опасность использования ИКТ для террористических целей. Многообразие злонамеренных негосударственных субъектов, быстротечность злонамеренных нападений в сфере ИКТ, а также трудности, связанные с определением источника инцидента в сфере ИКТ, увеличивают существующую угрозу.

¹⁷ В словаре русского языка С. И. Ожегова приводится следующее значение глагола «напасть»: выступить против кого-чего-н.; броситься на кого-что-н. с целью разгрома, уничтожения, нанесения ущерба. См.: Ожегов С. И. Словарь русского языка. М., 1982. С. 339.

¹² См.: Longworth E. The Possibilities for Legal Framework for Cyberspace — Including a New Zealand Perspective // The International Dimensions of Cyberspace Law. Aldershot, 2000. P. 13.

¹³ Ibid. P. 14.

¹⁴ Утв. Указом Президента РФ 5 декабря 2016 г. № 646.

вания компьютерных сетей и электронной информации, которые создают угрозу законным интересам государств и частных лиц в сфере использования и развития информационных технологий¹⁸. Конвенция о преступности в сфере компьютерной информации не единственный документ такого рода. В 2014 г. была принята Конвенция Африканского союза о кибербезопасности и защите персональных данных. В других регионах также приняты международно-правовые акты или еще идет обсуждение возможности заключения подобных документов¹⁹. Такого рода киберугрозы можно нейтрализовать с помощью мер, предусмотренных национальным уголовным правом, при необходимости путем международного сотрудничества в уголовно-правовой сфере. Субъектами, создающими такого рода угрозы, являются частные лица (физические или юридические), соответственно, хотя они регулируются международными договорами, они не затрагивают сферу международной безопасности.

Вместе с тем в Докладе отмечается два вида киберугроз: существующие и нарождающиеся. К ним относятся наращивание потенциала в сфере ИКТ для военных целей рядом государств, что делает более вероятным использование ИКТ в будущих конфликтах между государствами; опасность вредоносных нападений с использованием ИКТ на критически важную инфраструктуру, становящаяся серьезной и реальной; использование ИКТ для террористических целей, в том числе для совершения террористических нападений на объекты ИКТ или связанную с ИКТ инфраструктуру. Существующая угроза увеличивается благодаря многообразию злонамеренных негосударственных субъектов (включая преступные группировки и террористов), их различные мотивы, быстротечность злонамеренных нападений в сфере

ИКТ, а также трудности, связанные с определением источника инцидента в сфере ИКТ. Повышению уязвимости в условиях взаимозависимого мира может послужить разный уровень развития потенциала обеспечения безопасности в сфере ИКТ между государствами²⁰.

Г. Кершишник, посвятивший свое исследование проблеме киберугроз, использует ряд терминов, которые должны обозначить различную степень опасности для международной информационной безопасности случаев недружественного проникновения в киберпространство. В качестве наиболее общего понятия он использует выражение «кибервмешательство» (cyberintrusion), определяя в качестве «киберинцидентов»²¹ неприятные происшествия в киберпространстве, виновники которых так и не были обнаружены и преданы огласке. Наконец, следующей по степени опасности разновидностью кибервмешательства он называет кибернападение или кибератаку (cyberattack)²², а самой опасной — кибервойну (cyberwar)²³. Встречается также выражение «кибероперации»²⁴.

Проблема квалификации кибератаки или атаки на компьютерные сети как действия, подлежащего оценке в соответствии с международным правом, на сегодняшний день является особенно актуальной²⁵. Со-

²⁰ См.: Док. ООН А/70/174. С. 8/22-9/22.

²¹ Lotrionte and Tikk, Rapporteurs, Summary for Panel 3: Applicability of International Law to Cyberspace & Characterization of Cyber Incidents. CyberNormsWorkshop 2.0, Sept., 2012. URL: <http://citizenlab.org/cybernorns2012/>. Участники панели рассматривали в качестве киберинцидентов киберпреступления и кибершпионаж, что, разумеется, несколько сужает концептуальное пространство данной категории.

²² Встречается выражение «компьютерные сетевые атаки» (computer networkattacks). См: Dinniss H. H. Cyber Warfare and the Law of War. Cambridge, 2012. P. 4.

²³ См.: Kerschischnig G. Cyberthreats and International Law. The Hague, 2012. P. 86. Термин «кибервойна» начинает получать все большее распространение как в научной (см., например: Dinniss H. H. Op. cit.; Martin L. C. Cyber deterrence and Cyberwar. Santa Monica, 2009), так и в публицистической литературе (см.: Харрис Ш. Кибервойна@: Пятый театр военных действий М., 2016). Иногда используют термин «киберконфликт».

²⁴ См.: Еремян Л. Вызовы современных войн: актуальные вопросы международно-правового регулирования новых средств ведения войны. Ереван, 2017. С. 59; Blanck L. R. International Law and Cyber Threats from non-states Actors // Int'L L. Stud. Vol. 89. No. 406. 2013. P. 406-409.

²⁵ В Федеральном законе «О безопасности критической информационной инфраструктуры Российской Федерации» под компьютерным инцидентом понимается факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электропередачи, используемой для организации взаимодействия таких

¹⁸ В их числе противозаконный доступ, неправомерный перехват, воздействие на данные, воздействие на функционирование системы и др.

¹⁹ Так, страны БРИКС в Декларации, принятой в сентябре 2017 г. в Саме, заявили о стремлении развивать сотрудничество в соответствии с Дорожной картой практического сотрудничества БРИКС в обеспечении безопасности в сфере использования ИКТ и любыми другими согласованными механизмами и отметили инициативу Российской Федерации о межправительственном соглашении БРИКС по сотрудничеству в вопросах безопасности в сфере использования ИКТ. Можно отметить и такие документы, как Соглашение СНГ о сотрудничестве в борьбе с преступлениями в сфере компьютерной информации 2001 г., Соглашение ШОС о сотрудничестве в области обеспечения международной информационной безопасности 2009 г., Конвенция Лиги арабских государств о борьбе с преступлениями в области информационных технологий 2010 г. Кроме того, стало практиковаться принятие актов рекомендательного характера: Типовой закон Лиги арабских государств о борьбе с преступлениями в сфере информационных систем 2004 г. и т. д.

бытия последнего времени, особенно пропагандистские компании, развернувшиеся в результате гибридной войны западных государств против России, в том числе недоказанные, ничем не подтвержденные голословные обвинения нашей страны во вмешательстве во внутренние дела, в частности в выборы в США, ФРГ и других стран, наглядно свидетельствуют об острой необходимости анализа категорий киберопераций, кибератак и кибервмешательства с точки зрения международного права.

Рассматривая понятие кибератаки как способ применения имеющихся технологических возможностей государством или даже негосударственными субъектами против других государств или негосударственных образований, необходимо исходить из устоявшихся правовых или технических понятий и категорий. Не останавливаясь подробно на анализе понятий «кибервмешательства» и его возможных форм, а также дефиниций «киберопераций» и «кибернападения» («кибератаки») с точки зрения международного права, что бесспорно заслуживает отдельного и подробного рассмотрения с учетом как действующих норм международного права, так и особенностей киберпространства, в качестве иллюстративного примера рассмотрим возможность допущения юридического определения кибератак как разновидности применения силы государством в нарушение действующего международного права. Следует признать, что на сегодняшний день подобное допущение является не столь очевидным, как это может показаться на первый взгляд, хотя нельзя исключать возможности его использования при достижении достаточного уровня согласия государств.

В западной литературе дискутируется вопрос о возможности использования понятия силы²⁶ в контексте

объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки. В свою очередь, компьютерная атака — это целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации. Таким образом, согласно российскому законодательству компьютерный инцидент — это результат действия, обозначаемого компьютерной атакой. Как видно, данный подход различается с трактовкой видов вмешательства, предлагаемой Г. Кершишником.

²⁶ Г. И. Тункин указывал, что в западной литературе имеется достаточно много толкований понятия «сила». В более широком смысле понятие «сила» передается термином «мощь», которую Г. Моргентау определяет как власть над умами и действиями других людей. Все сторонники политики силы согласны с тем, что решающим фактором в отношениях между государствами являются вооруженные си-

киберугроз, которое, несмотря на свои покрытые глубокими седидами исторические корни, широко используется в мировой политике и международном праве, хотя его толкование подвергается значительным трансформациям и метаморфозам. Представляется, что по мере достижения прогресса в разработке международно-правового понимания использования ИКТ в контексте поддержания международной безопасности он вполне может выступить в качестве ключевой категории в решении задачи международно-правовой квалификации кибератаки²⁷. Однако нельзя забывать прошлый опыт, когда делались попытки расширительного толкования понятия силы, включавшего не только вооруженную силу государства, но и экономическую, информационную и другие составляющие внешнеполитического потенциала государства²⁸. Они были подвергнуты критике на том основании, что п. 4 ст. 2 Устава ООН запрещает применение исключительно вооруженной силы в международных отношениях, а все иные составляющие внешнеполитического потенциала не входят в сферу действия этой нормы. Кибератаки по определению нацелены на информацию и информационные системы²⁹. Однако они могут быть разделены на те, которые нацелены на информационные системы для того, чтобы повлиять на аппаратные средства и другие физические аспекты сети, и те, которые нацелены на информацию как таковую. Когда объектом нападения в конечном счете является физический объект, как это происходит, например, с манипулированием программным обеспечением управления скоростью вращения ядерных центрифуг или иных объектов критических информационных систем, эффекты кибератаки легче вписываются в привычные представления о применении силы.

Более сложная проблема возникает тогда, когда целью кибератаки является сама информация. В частности, когда последствием кибератаки не является разрушение собственно информации, а скорее причине-

лы. См.: Тункин Г. И. Право и сила в международной системе. М., 1983. С. 92.

²⁷ См.: Dinniss H. H. Op. cit. P. 65.

²⁸ В Специальном комитете ООН по выработке Декларации о принципах международного права, касающихся сотрудничества и дружественных отношений между государствами в соответствии с Уставом ООН 1970 г., этой позиции придерживались афро-азиатские страны, поддержанные восточноевропейскими государствами. См.: Ушаков Н. А. Правовое регулирование использования силы в международных отношениях. М., 1997. С. 12.

²⁹ Так, Г. Кершишник различает средства и методы реализации киберугроз. К первым он относит вирусы и черви, черные ходы (лазейки), зомби-сети. Ко вторым — ДОС-атаки, инфильтрацию, социальный инжиниринг; зондирование, незаконный сбор данных (мониторинг), картирование, методы анонимизации. См.: Kerschischnig G. Op. cit. P. 31—37.

ние ущерба функционированию информационного объекта в такой степени, что теряется возможность пользоваться информацией, содержащейся в данном объекте. Оценка последствий такого нападения, очевидно, будет зависеть от характера системы, которая подверглась кибератаке. Так, последствия порчи информации в системе управления воздушным движением, очевидно, будут более катастрофичны, чем те, которые могут произойти в каких-либо других информационных объектах, например в банках или небольших промышленных предприятиях. По мнению некоторых специалистов, первый пример будет совершенно точно рассматриваться как применение силы в общепринятом в международном праве смысле, а последний скорее всего будет восприниматься как причинение экономического ущерба. Отсюда делается вывод: принимая во внимание возможные негативные последствия, тот факт, что нападение на системы управления воздушным движением выльется в серьезный урон и возможные человеческие потери, явно позволяет отнести его к разновидности применения силы в нарушение п. 4 ст. 2 Устава ООН³⁰.

Представляется, что подобное умозаключение не в полной мере учитывает все возможные ситуации противоправных актов, имеющих трагические последствия, и их международно-правовую квалификацию. Так, при совершении террористических актов против воздушных судов, приводивших к человеческим жертвам, тем не менее не ставился вопрос об автоматическом применении п. 4 ст. 2 Устава ООН³¹. Как правило, подобные действия квалифицировались как уголовные преступления международного характера. Соответственно, проводить параллели и опираться лишь на доктринальное толкование Устава ООН при отсутствии ясно сформулированных положений международных договоров было бы по меньшей мере опрометчиво. Ссылка на аналогию в отношении характера причиненного ущерба, как было показано, не всегда может быть уместна. Это основание также необходимо проанализировать более внимательно.

Несомненно, что поведение государств в процессе использования ИКТ в отношениях с другими субъектами международного права должно основываться на признании и соблюдении основных принципов международного права³². На это же ориентиру-

ет и Доклад, ссылаясь на принципы суверенного равенства, разрешение международных споров мирными средствами таким образом, чтобы не подвергать угрозе международный мир и безопасность и справедливость; отказ в международных отношениях от угрозы силой или ее применения как против территориальной неприкосновенности или политической независимости любого государства, так и каким-либо другим образом, несовместимым с целями ООН; уважение прав человека и основных свобод; невмешательство во внутренние дела других государств³³. При этом следует обратить внимание, что если «кибервмешательство» при определенных обстоятельствах может рассматриваться как явное нарушение международного права, то этого нельзя утверждать в отношении запрета применения силы, поскольку до настоящего времени ограничение права использовать силу, подразумевает только вооруженную силу.

Упомянутый выше Доклад сформулировал нормы, правила и принципы ответственного поведения государств при осуществлении деятельности, связанной с ИКТ, призвал соблюдать меры укрепления доверия в целях создания мирной ИКТ-среды; оказывать содействие международному сообществу в сфере обеспечения безопасности ИКТ и в наращивании потенциала государствам, которые не обладают им; а также установил обязанность соблюдения государствами международного права, в частности, их обязанностей по Уставу ООН, ИКТ-среды. Кроме того, в Докладе подчеркивается обязанность государств выполнять их обязательства по международному праву, касающиеся уважения и защиты прав человека и основных свобод.

В Докладе упомянуто о неотъемлемом праве государств принимать меры, соответствующие междуна-

тореф. дис. ... канд. юрид. наук. М., 2008. С. 11. А. А. Стрельцов также отмечал, что «краеугольным камнем поддержания международного мира и безопасности является Устав ООН». См.: *Streltsov A. A. International Information Security: Description and Legal Aspects* // *Disarmament Forum*. No. 3. Geneva, UN, September 2007. P. 9. Юридический советник госдепартамента США Г. Кох, отвечая на вопрос о позиции США о возможности применения принципов международного права к киберпространству, однозначно подтвердил, что «установленные принципы международного права применяются в киберпространстве». См.: *Koh H. H. International Law in Cyberspace* // *Faculty Scholarship Series*. 4854. Paper. P. 3. URL: http://digitalcommons.law.yale.edu/fss_papers/4854. Однако эта убежденность не должна вводить в заблуждение: в практической политике администрация президента США Обамы в ООН занимала иную позицию, основанную на приоритете национальной юрисдикции США в отношении киберинцидентов. См.: *Kulikova A. Can a New UN Cyber Agreement Be a Win-Win Russia, US?* 2015. 28 Aug. // *Russia Direct*. 2015. 28 Aug.

³³ См.: Док. А/70/174, с. 16/22.

³⁰ См.: *Dinniss H. H. Op. cit.* P. 63.

³¹ Исключением было «дело Локерби», но в этой ситуации были специфические условия совершения теракта против воздушного судна, когда под подозрение в его совершении попало государство, а не изолированные террористические организации.

³² О. В. Мозолина отмечает, что «международно-правовое регулирование отношений в сфере Интернета основывается на общепризнанных принципах и нормах международного права». См.: *Мозолина О. В. Публично-правовые аспекты международного регулирования отношений в Интернете: ав-*

родному праву и признанные в Уставе ООН. Это очень важное признание; судя по всему, речь идет о признании правомерности использования права на самооборону, поскольку Устав ООН упоминает об этом праве как неотъемлемом праве государств в ст. 51. Подобным же косвенным образом указывается на применимость принципов международного гуманитарного права (гуманности, необходимости, пропорциональности и индивидуализации) в соответствующих случаях. Государства призываются не допускать использования своих представителей для совершения международно-противоправных деяний с использованием ИКТ, они должны выполнять свои международные обязательства в отношении таких деяний, приписываемых им в соответствии с международным правом. Таким образом, признается, что государства несут международную ответственность за совершенные противоправные деяния в киберпространстве, несмотря на отсутствие специальных норм международного права. В то же время в Докладе подчеркивается, что обвинения в организации и совершении противоправных деяний, выдвигаемые против государств, должны быть обоснованными.

Из этого можно сделать следующий вывод. В настоящее время идет разработка международно-правовых мер противодействия угрозам международной

безопасности в киберпространстве. Соответственно, складывается «мягкое регулирование» путем обращения международного сообщества к государствам добровольно соблюдать соответствующие обязательства. Это относится как к нормам, правилам и принципам ответственного поведения государств, которые определяются как «добровольные и необязательные», так и к мерам доверия, которые тоже называются «добровольные». Равным образом меры по наращиванию потенциала рекомендуются государствам, а утверждения о необходимости соблюдения международного права и его применимости к использованию ИКТ определяются как «мнения». Тем не менее нельзя недооценивать значение «мягкого регулирования» для утверждения международно-правового режима противодействия угрозам международному миру и безопасности в киберпространстве. Как показывает новейшая история становления международно-правовых механизмов регулирования новых сфер межгосударственных отношений, для него практически постоянно была характерна траектория от «мягких» форм регулирования к юридически обязательным договорным. Будем надеяться, что и в отношении преодоления киберугроз международному миру и безопасности эта логика международно-правового развития подтвердится.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

- Blanck L. R. International Law and Cyber Threats from non-states Actors // *Int'l L. Stud.* Vol. 89. No. 406. 2013.
- Dinniss H. H. *Cyber Warfare and the Law of War*. Cambridge, 2012.
- Kamal A. *The Law of Cyber-Space. An Invitation to the Table of Negotiations*. Geneve, 2006.
- Kerschischnig G. *Cyberthreats and International Law*. The Hague, 2012.
- Koh H. H. *International Law in Cyberspace* // Faculty Scholarship Series. 4854. Paper. URL: http://digitalcommons.law.yale.edu/fss_papers/4854.
- Kulikova A. Can a New UN Cyber Agreement Be a Win-Win Russia, US? Aug 28 2015 // *Russia Direct*. 2015. 28 Aug.
- Longworth E. The Possibilities for Legal Framework for Cyberspace — Including a New Zealand Perspective // *The International Dimensions of Cyberspace Law*. Aldershot, 2000.
- Martin L. C. *Cyber deterrence and Cyberwar*. SantaMonica, 2009.
- Streltsov A. A. International Information Security: Description and Legal Aspects // *Disarmament Forum*. No. 3. Geneva, UN, September 2007.
- The International Dimensions of Cyberspace Law*. Aldershot, 2000.
- Еремян Л. Вызовы современных войн: актуальные вопросы международно-правового регулирования новых средств ведения войны. Ереван, 2017.
- Информационное право: актуальные проблемы теории и практики: кол. монография / под общ. ред. И. Л. Бачило. М., 2009.
- Касенова М. Б. *Международно-правовое управление Интернетом*. М., 2010.
- Касенова М. Б. *Правовое регулирование трансграничного функционирования и использования Интернета: автореф. дис. ... д-ра юрид. наук*. М., 2016.
- Киберпространство БРИКС: правовое измерение: монография. М., 2017.
- Мозолина О. В. *Публично-правовые аспекты международного регулирования отношений в Интернете: автореф. дис. ... канд. юрид. наук*. М., 2008.
- Ожегов С. И. *Словарь русского языка*. М., 1982.
- Тункин Г. И. *Право и сила в международной системе*. М., 1983.
- Ушаков Н. А. *Правовое регулирование использования силы в международных отношениях*. М., 1997.
- Харрис Ш. *Кибервойн@: Пятый театр военных действий*. М., 2016.
- Хуторной С. Н. *Киберпространство и становление сетевого общества: автореф. дис. ... канд. филос. наук*. Воронеж, 2013.