Международные процессы, Том 21, № 3 (74), сс. 69–85
DOI 10.17994/IT.2023.21.3.74.2

# КОНЦЕПЦИЯ КИБЕРДЕЛИКТА И ОТВЕТСТВЕННОСТЬ В МЕЖДУНАРОДНОМ ПРАВЕ

МАКСИМ ИНОЗЕМЦЕВ
МГИМО МИД России, Москва, Россия

СЕМЁН СТЕПАНОВ
НИУ ВШЭ, Москва, Россия

**Резюме**

Цифровизация общественных отношений не только упрощает жизнь, но и создаёт благодатную почву для увеличения количества правонарушений в киберпространстве, в том числе с участием субъектов международного права. Потерпевшие страны зачастую прибегают к применению несоразмерных мер против государств-нарушителей, используя традиционный международно-правовой инструментарий. Кроме того, малоэффективным является отсутствие оптимальных средств реагирования на кибервмешательства малой интенсивности. Рассмотрев основные механизмы и сложности, с которыми сталкивается современное международное право при причинении вреда государствами с помощью цифровых технологий, авторы предлагают частноправовую концепцию киберделикта, использование которой, с одной стороны, позволяет устранить последствия нарушений ex post, а с другой – не приводит к эскалации существующего конфликта. При описании проблем межгосударственного взаимодействия подчёркивается вспомогательный характер использования частноправового инструментария. Задействовав как системный, так и компаративистский методы исследования, авторы раскрывают сущность и правовые последствия вариативной квалификации деяния как правонарушения (state responsibility) или действия, не запрещённого международным правом (state liability), а также обосновывают необходимость применения гибкой системы правового регулирования к праву причинения вреда в сети Интернет. При помощи критического метода выявляются недостатки современной доктрины международного права в рассматриваемом контексте. Посредством дедуктивного метода с опорой на отечественные и зарубежные доктринальные источники, нормативные акты, а также материалы судебной практики предлагается оптимальный режим ответственности за правонарушение в цифровой среде, который позволит создать надлежащие стимулы для совершенствования способов проведения кибервмешательств.

**Ключевые слова:**

киберделикт; кибервмешательство; кибератака; международное право; правонарушение; ответственность; цифровое право.

Первая четверть XXI века отмечена не только структурными изменениями общественных отношений, но и фундаментальными вызовами традиционным правовым конструкциям. В частности, их порождает специфика современной цифровой сферы, которая зачастую не позволяет автоматически применять существующие нормы и институты права [Иноземцев 2021]. Возникают новые способы заключе-

Дата поступления рукописи в редакцию: 06.12.2022
Дата принятия к публикации: 16.10.2023

*Для связи с авторами / Corresponding author:*
Email: inozemtsev@inno.mgimo.ru

ния и исполнения договоров (смарт-контракты[1]); в отдельных законодательных актах появляются объекты гражданских прав (цифровые права), вызывающие оживлённые дискуссии в академической и экспертной среде [Суханов 2021]; активно обсуждается возможность признания за искусственным интеллектом правосубъектности [Степанов 2021].

Зачастую внедрение цифровых технологий в государственный сектор и бизнес-процессы осуществляется с целью упростить социальное взаимодействие и свести к минимуму потенциальные риски, к примеру при помощи технологии распределённого реестра. Тем не менее у цифровизации существует и оборотная сторона: в лентах новостей содержится огромное количество информации о *DDoS*-атаках, утечках персональных данных и правонарушениях в сети Интернет. Ежедневно в мире происходит около 35 тыс. происшествий с проникновением в компьютерную систему безопасности[2]. Только за первый квартал 2022 г. количество кибератак на российские компании возросло с нескольких десятков в месяц до сотен тысяч в неделю[3].

Государства и крупные корпорации сталкиваются с беспрецедентными цифровыми атаками на важные объекты инфраструктуры, при этом противоправные действия хорошо организованы и имеют конкретную цель. Например, в 2014 г. на серверы американской кинокомпании *Sony Pictures Entertainment* была совершена масштабная хакерская атака, ответственность за которую взяла на себя северокорейская хакерская группировка «Хранители мира» (“Guardians of Peace”). Причиной атаки послужила готовящаяся премьера фильма «Интервью», в котором показана попытка покушения на лидера КНДР Ким Чен Ына. Результатом противоправного акта стала публикация конфиденциальной информации, персональных данных сотрудников и актёров. По оценкам экспертов, убытки компании составили около 200 млн долларов США[4]. В ответ Вашингтон пошёл на чрезвычайные меры: открыто объявил, что за действиями хакеров стоит Пхеньян, и ввёл против страны новые экономические санкции [Crootof 2018: 567].

Насколько принятие подобных мер соответствовало требованию пропорциональности ответа на атаку? Или же они, наоборот, вели к эскалации конфликта? Можно ли полагать, что противоправные действия осуществлялись под контролем или руководством северокорейского правительства? Если это так, то как надлежит квалифицировать деяние, послужившее причиной столь серьёзного вреда[5] – в качестве правонарушения (responsibility) или действия, не запрещённого международным правом (liability)? В зависимости от квалификации будут различаться правовые последствия. В международном праве утверждается обычная норма, согласно которой за вред, наступивший в результате действий, не запрещённых междуна-

[1] Смарт-контракт означает оформление договора в форме программного кода в блокчейне для обеспечения последующего автоматического и автономного самоисполнения заложенных в программу условий [Синицын, Дьяконова, Чурсина 2021: 43].

[2] *Donlon R.* Hacked! The Cost of a Cyber Breach, in 5 Different Industries // Property Casualty 360. 16.10.2015. URL: https://www.propertycasualty360.com/2015/10/16/hacked-the-cost-of-a-cyber-breach-in-5-different-industries/?slreturn=20220604043203 (accessed: 21.11.2022).

[3] *Новиков А.* Атака одной кнопкой: кто взламывает сайты российских компаний // Forbes. 31.03.2022. URL: https://www.forbes.ru/mneniya/460847-ataka-odnoj-knopkoj-kto-vzlamyvaet-sajty-rossijskih-kompanij (дата: 21.11.2022).

[4] Sony Pictures to Lose $200 Million Following Cyber Attack // Business Today. 23.12.2014. URL: https://www.businesstoday.in/latest/corporate/story/sony-pictures-cyber-attack-the-interview-release-cancelled-138613-2014-12-23 (accessed: 21.11.2022).

[5] В настоящей статье термины «ущерб», «вред», «убытки» понимаются как синонимы и означают такой материальный урон имуществу или другим интересам государства или его граждан, который можно определить в денежном исчислении.

родным правом, государство несёт материальную ответственность [Лукашук 2005: 413]. Подчёркивается, что она наступает не в связи с поведением, поскольку оно правомерно, а именно за причинённый вред (ответственность без вины), тогда как правовые последствия правонарушений государств, как правило, более существенные (реституция, компенсация и сатисфакция)[6].

Международное право постепенно вырабатывает понятия, с помощью которых описываются разнообразные правонарушения в сети Интернет: хактивизм, кибершпионаж, кибертерроризм, кибервойна и другие. Значимый вклад в развитие международного права применительно к сфере информационно-коммуникационных технологий внесла Группа правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности. В том числе удалось выработать перечень добровольных норм ответственного поведения государств в киберсфере, одобренный резолюцией ГА ООН 73/27 от 5 декабря 2018 года. В контексте международного уголовного права разрабатываются отдельные составы, посвящённые киберпреступлениям[7].

Между тем нередко государства не стремятся именовать то или иное посягательство кибератакой и говорить о кибервойне. В доктрине также отмечается недостаточная эффективность уголовно-правовых методов борьбы с киберпреступлениями, если только лица, обвиняемые в совершении преступления, физически не находятся в государстве, понёсшем ущерб [Maras 2016]. Все эти обстоятельства обусловливают необходимость поиска дополнительного инструментария для удовлетворения сторон конфликта. Подобной цели может послужить появившаяся в частном праве концепция киберделикта. Стоит оговориться, что мы не стремимся экстраполировать понятия из сферы гражданского права на международно-правовое поле, от чего предостерегал российский классик в этой области Ф. Ф. Мартенс. Последний подвергал критике подход своего немецкого коллеги А. Гефтера как раз по этой причине [Мартенс 1882: 432]. Обращение к частному праву является лишь вспомогательным, дополнительным средством. Оно может помочь в выявлении правовой природы, а также в определении принципов оптимального режима ответственности[8].

Предлагается рассмотреть основные проблемы, с которыми сталкивается международное право при причинении вреда государствами с помощью цифровых технологий, затем проанализировать концепцию киберделикта и дедуцировать оптимальный режим ответственности.

### Вызовы международному праву в цифровой среде

В ситуациях, когда нарушение в цифровой среде[9] сопряжено с ответственностью за международно-правовое деяние, потерпевшему государству надлежит доказать факт неисполнения обязательства по международному праву, а также квалифицировать поведение государства-делинквен-

[6] Более подробно о различиях ответственности за действия, не запрещённые международным правом, и ответственности за международное правонарушение см.: [Савельева 1996: 12–65].

[7] См., к примеру, Конвенцию о преступности в сфере компьютерной информации ETS № 185. Будапешт. 23.11.2001.

[8] Как справедливо отмечала Л.В. Савельева, «международное право в силу своей природы не может содержать института внедоговорной или деликтной ответственности. Все институты международного права, в том числе и институт ответственности государств, основаны на соглашении соответствующих субъектов. Поэтому формы закрепления прав и обязанностей субъектов во внутригосударственном и международном праве совершенно различны, ввиду чего механическое перенесение цивилистических конструкций в области международного права едва ли может принести положительные результаты» [Савельева 1996: 7–8].

[9] В настоящей работе термины «цифровая среда», «цифровое пространство», «сеть Интернет», «киберпространство» понимаются как синонимы.

та как противоправное [Shaw 2021: 677]. Эти же условия содержатся в ст. 2 Статей об ответственности государств за международно-противоправные деяния, принятых в 2001 г. (далее – «**Статьи**»)[10].

Одной из основных функций международно-правовой ответственности является сдерживание потенциального правонарушителя (превентивная функция) [Вылегжанин 2021: 14]. Она реализуется посредством выполнения ряда условий: (1) неотвратимость ответственности за причинение вреда и (2) вероятная тяжесть невыгодных для делинквента последствий.

Выполнить первое условие в теории международного права предлагается посредством вменения противоправного действия государству-нарушителю. В этом случае сразу же возникают трудности. *Во-первых*, кибероперации проводятся хакерскими группировками, поэтому доказать причастность конкретной страны непросто. *Во-вторых*, использование киберпрокси[11] делает этот процесс практически невозможным.

Остановимся на этой проблеме более подробно. В соответствии со ст. 8 Статей поведение хакерской группы может рассматриваться как деяние государства, если она действовала по его указаниям, под руководством или контролем[12]. Пока никакой специфики нет. В то же время проблема усугубляется, как только мы вводим категорию «киберпрокси». В литературе отмечается, что они выступают «посредниками, проводящими или непосредственно способствующими осуществлению наступательных кибероперациий благодаря осознанной поддержке (активной или пассивной) со стороны государства-бенефициара» [Maurer 2018: 11].

Выделяют по меньшей мере три типа взаимодействий между киберпрокси и государствами: *санкционирование* (осуществление пассивной государственной поддержки); *оркестровка* (киберпрокси действует в соответствии с указаниями государства, но не находится под его контролем); *делегирование* (прямой контроль со стороны государства) [Maurer 2018: 12]. Использование киберпрокси необходимо главным образом, чтобы усложнить процесс вменения противоправного действия государству-нарушителю и привлечения его к ответственности.

Приведём следующий пример: в 2015 г. хакеры вмешались в работу французского канала *TV5Monde*, в результате чего оборудование было выведено из строя, а убытки составили около 5 млн евро[13]. Изначально существовали все основания говорить о связи хакерской группировки с Исламским государством[14] как ввиду её наименования «Кибер Халифат», так и некоторых данных интернет-архитектуры. Тем не менее позднее выяснилось, что правонарушение совершили хакеры APT28, известные как "*Fancy Bear*" [Crootof 2018: 582].

С трудностями, характерными для идентификации государства-нарушителя, связано выявление мотивов кибервмешатель-

[10] Доклад Комиссии международного права. 53-я сессия (23 апреля – 1 июня и 2 июля – 10 августа 2001 г.) // ООН. URL: https://www.un.org/ru/documents/decl_conv/conventions/pdf/responsibility.pdf (дата обращения: 22.11.2022). Отметим, что Статьи об ответственности в большей мере представляют собой кодификацию применимых обычных международно-правовых норм, с учётом содержания и со значительными элементами прогрессивного развития.

[11] Несмотря на схожесть с привычной отечественному читателю категорией «прокси-сервер», их не следует отождествлять, поскольку последние представляют собой промежуточные серверы, которые используются на законных основаниях, тогда как цель киберпрокси исчерпывается наступательными кибердействиями.

[12] При этом аналогичные разъяснения содержатся и в правилах 15–17 Таллинского руководства 2.0 от 2017 года.

[13] *Corera G.* How France's TV5 Was almost Destroyed by 'Russian Hackers' // BBC. 10.10.2016. URL: https://www.bbc.com/news/technology-37590375 (accessed: 21.11.2022).

[14] Террористическая организация решением Верховного суда Российской Федерации от 29.12.2014 запрещена на территории Российской Федерации.

ства[15], хотя последние не являются элементом международно-противоправного деяния. Между тем следует признать, что тяжело устанавливаемый смысл этого явления предопределяет невозможность адекватного реагирования на него. Предположим, что какое-либо вредоносное действие в цифровой сфере приводит к уничтожению критического объекта инфраструктуры потерпевшей страны по не зависящим от воли государства-нарушителя обстоятельствам. Усложняет анализ и тот факт, что некоторые виды кибервмешательств в доктрине рассматриваются не только в качестве неизбежных в международном взаимодействии, но и как часть общепризнанных прав и обязательств государств [Lubin 2018: 203][16]. В реальном мире потерпевшее государство реагировало бы иначе на случай или непреодолимую силу, чем на преднамеренное деяние. Тем не менее в цифровой среде провести такое различие затруднительно.

Кроме того, можно поставить вопрос несколько иначе: целесообразно ли квалифицировать кибервмешательства вне рамок вооружённого конфликта в качестве «применения силы» или «вооружённого нападения» в соответствии с Уставом ООН? От этого зависит потенциал неотъемлемого права потерпевшего государства на самооборону. Как справедливо отмечает В.Н. Русинова, «с одной стороны, было бы неверным отрицать, что некоторые типы вредоносного использования компьютерных программ могут принимать военную форму и будет корректным давать им правовую оценку с позиции *jus ad bellum*. С другой же – [...] легко пересечь ту грань, когда результаты [...] будут прямо противоречить консенсусу государств о толковании объёма понятия «применение силы» как не охватывающего невоенные формы воздействия...» [Русинова 2022: 45]. При этом следует учитывать позицию Российской Федерации, согласно которой понятия «вооружённое нападение» и «применение силы» могут использоваться лишь в обстоятельствах вооружённого конфликта, а кибернападение вне этого контекста под них не подпадает [Русинова 2022: 46].

В связи с этим рассмотрим один из самых дискуссионных примеров квалификации кибервмешательства с точки зрения *jus ad bellum*. В 2010 г. США посредством использования программы *Stuxnet*, которая поражает ЭВМ под управлением операционной системы *Windows*, повредили около тысячи иранских центрифуг для обогащения урана[17]. Столь масштабные катастрофические последствия породили большое количество споров в доктрине по поводу возможности рассмотрения такой кибероперации в качестве вооружённого нападения [Hathaway et al. 2012: 836–837].

Равным образом существуют проблемы, связанные с применением контрмер. Например, ч. 1 ст. 52 Статей устанавливает, что до их принятия потерпевшая страна должна, *во-первых*, уведомить ответственное государство о решении принять контрмеры, *во-вторых*, указать поведение, которому ответственное государство должно следовать с тем, чтобы прекратить противоправное деяние, если оно продолжается. К тому же потерпевшее государство не может прибегнуть к контрмерам после прекращения противоправного поведения (ч. 3 ст. 52 Статей). Более того, принимая их, государство действует на свой страх и риск, поскольку без достаточного обоснования оно само становится ответственным за новое деяние [Лукашук 2005: 403]. Подобные требования выступают серьёзным препятствием к применению контрмер в ответ на кибервмешательства.

Сложность идентификации ответственного государства, а также стремительная скорость совершения этих нарушений приводят к тому, что противоправное деяние будет прекращено ещё до того, как оно обна-

[15] Кибервмешательство представляет собой собирательное понятие и используется для того, чтобы охватить действия государств разной интенсивности в цифровой среде.

[16] Типичным примером является кибершпионаж [Гаркуша-Божко 2021].

[17] *Fildes J.* Stuxnet Worm 'Targeted High-Value Iranian Assets' // BBC. 23.09.2010. URL: http://www.bbc.co.uk/news/technology-11388018 (accessed: 21.11.2022).

ружено. Это обстоятельство ставит довольно любопытный теоретический вопрос. Дело в том, что традиционно контрмеры отличаются от ответственности тем, что первые представляют собой право потерпевшего, тогда как последняя – обязанность нарушителя [Вылегжанин 2021: 24]. При этом, как мы отмечали, контрмеры главным образом необходимы для понуждения государства-делинквента к выполнению международно-правовых обязательств. В реальном мире, где многие противоправные деяния обладают публичным характером, легкораспознаваемы, а также происходят в течение определённого времени, контрмеры отчасти также выполняют специфичную для ответственности превентивную функцию [Crootof 2018: 587]. Тем не менее в цифровой среде границы обеих сфер более чёткие, что приводит к противоправности и неэффективности использования контрмер. В доктрине прямо отмечается, что они должны применяться не для предупреждения будущих кибервмешательств, а лишь в ответ на фактические нарушения в цифровой среде [Gill 2013: 231; Pirker 2013: 213].

При отсутствии чётких правил разграничения правомерного и противоправного поведения государств в киберпространстве удовлетворить условие, которое относится к вероятной тяжести неблагоприятных для делинквента последствий, представляется трудновыполнимой задачей. Репрезентативным является следующий пример. В июле 2015 г. две хакерские группировки "*Cozy Bear*" и "*Fancy Bear*" взломали сеть Национального комитета Демократической партии США. Хакеры получили доступ ко всей переписке по электронной почте и мессенджерам, которыми пользовались сотрудники комитета[18]. Год спустя администрация президента Б. Обамы публично вменила эти противоправные действия Российской Федерации[19]. По прошествии нескольких месяцев США ввели санкции против нескольких физических лиц и организаций, что стало несоразмерной реакцией на предполагаемое нарушение[20]. В американской доктрине, напротив, подобная реакция признаётся недостаточной и, следовательно, по мнению исследователей, способствует росту правонарушений в цифровой среде, не обеспечивая надлежащей превенции [Crootof 2018: 587].

Все вышеобозначенные причины предопределяют потребность разработать и предложить механизм, который, с одной стороны, выполнял бы функцию сдерживания, а с другой – удовлетворял бы стороны международного спора.

**Эволюция концепции киберделикта в частном праве**

В доктрине деликтного права существует несколько систем организации норм о причинении вреда: (1) монистическая, в основе которой лежит известный принцип генерального деликта[21] (Франция, Италия, Испания); (2) сингулярная, исходящая из существования отдельных случаев причинения вреда, не связанных общим признаком (Великобритания, США); (3) смешанная, в которой наряду с общими положениями наличествуют специальные деликтные составы (Германия, Швейцария) [van Dam 2013]. Впрочем, подобная классификация обладает рядом существенных недостатков. К примеру, как в Соединённом

[18] *Кузнецов А.* Российских хакеров обвинили во взломе сетей штаба Демократической партии [Электронный ресурс] // РБК. 14.06.2016. URL: https://www.rbc.ru/politics/14/06/2016/576031e59a79471dc26160b8 (дата обращения: 22.11.2022).

[19] *Sanger D.E., Savage Ch.* U.S. Says Russia Directed Hacks to Influence Elections // New York Times. 07.10.2016. URL: https://www.nytimes.com/2016/10/08/us/politics/us-formally-accuses-russia-of-stealing-dnc-emails.html (accessed: 21.11.2022).

[20] Office of the Press Secretary, White House. For Immediate Release. Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment // Obama White House. 29.12.2016. URL: https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity (accessed: 21.11.2022).

[21] Основополагающая идея этого положения в том, чтобы свести все многообразие случаев причинения вреда к единому началу (принципу).

Королевстве, так и в Соединённых Штатах учёные предпринимают весьма любопытные попытки дедуцировать фундаментальный принцип для всех деликтных моделей поведения [Murphy 2019].

Именно в рамках сингулярной системы и появился киберделикт (*Cybertort*), значительно отличающийся от классического варианта. Строго говоря, по причине отсутствия общего принципа возмещения вреда в обеих странах возникла необходимость в описании правонарушений, совершаемых в виртуальном пространстве.

В английской и американской литературе существует несколько точек зрения относительно содержания понятия «киберделикт». Один подход предлагает считать таковым всякие правонарушения, которые происходят в информационно-технологическом пространстве [Rustad 2009: 395]. Неудовлетворительность подобного понимания проистекает из его безграничности. Получается, что киберделиктом могут признаваться, например, и распространение ложных сведений в Интернете, и кража виртуального имущества в компьютерной игре.

Столь широкому подходу противостоит позиция, согласно которой основной характеристикой киберделикта, помимо его совершения в цифровой среде, надлежит считать наличие вредоносных последствий в реальном мире [Duranske 2008: 75]. Как следствие, в доктрине появился так называемый тест магического круга (*Magic Circle Test*), в соответствии с которым «деятельность, имеющая место в виртуальном мире, подчиняется праву реального мира в том случае, если пользователь [...] разумно осознаёт или должен разумно осознавать, что она влечёт последствия для реального мира» [Белых, Пучков 2020]. Ещё одним важным условием наступления ответственности за киберделикт является нарушение абсолютного права потерпевшего[22] [Finnis 2016: 195]. Несмотря на то что деление прав на абсолютные и относительные, бесспорно, встречается в англо-американской доктрине, оно не является первостепенным.

Анализируя вышеуказанные признаки, В.С. Белых и В.О. Пучков приходят к выводу, что под «киберделиктом в англо-американском праве предлагается понимать противоправное нарушение абсолютного гражданского права, совершённое в информационно-технологическом (виртуальном) пространстве и влекущее за собой причинение потерпевшему такого вреда, который отражается в реальном мире, в том числе в реальной экономике и бизнесе» [Белых, Пучков 2020].

Эти три критерия (совершение деяния в виртуальной среде, наличие последствий в реальном мире и нарушение абсолютного права) задают тональность всех дальнейших рассуждений. В то же время остаётся актуальным вопрос относительно противоправности поведения делинквента. В англо-американском деликтном праве аналогом противоправности в деликтах, связанных с небрежностью (*negligence*), с известной долей условности можно считать нарушение должной осмотрительности (*duty of care*)[23]. В этом случае возникает наиболее важная проблема: могут ли государство, суды или транснациональные корпорации устанавливать взаимные обязанности субъектов виртуального взаимодействия, нарушение которых приводит к ответственности за киберделикт?

В американской теории права высказывается довольно влиятельная точка зрения о неэффективности установления запретов в сети Интернет [Познер 2020: 104]. Тем не менее отсутствие правового воздействия побуждает к противоправному поведению. В связи с этим надлежит выявить оптимальную модель правового регулирования

[22] Под абсолютным правом необходимо понимать такое субъективное право, которому противостоит неопределённый круг обязанных субъектов.

[23] Общего учения об условиях деликтной ответственности в англо-американском праве не было выработано. Зачастую разные элементы деликта negligence используются как для определения вины (X (Minors) v. Bedforshire County Council. 1995. 2 AC 633), так и для установления противоправности (Smith v. Littlewoods Organisation Ltd. 1987. UKHL 18).

в случае причинения вреда в виртуальном пространстве.

Деликтное право, как известно, представляет собой лучший пример гибкой системы правового регулирования [Koziol 2017]. Её автор В. Вильбург полагал, что в частном праве существует множество оценок и целей, то есть целый спектр нормативных решений [Гаджиев 2018: 135]. По сути, имеется в виду гармоничное сосуществование таких принципов, как правовая определённость и гибкое регулирование. Получается, что, с точки зрения сторонников гибких систем, деликтное право представляет собой, с одной стороны, набор императивных (строгих) правил, с другой – набор общих (абстрактных) положений. Посредством закрепления небольшого набора императивных норм, а также ключевых для принятия решений факторов, которые обязан учесть судья при разрешении конкретного спора, законодатель может достичь более высокого уровня конкретизации и ограничить дискрецию суда [Гаджиев 2018: 136]. Судебное решение становится предсказуемым, удовлетворяя требование правовой определённости, что является несомненным достоинством подобного подхода. Вместе с тем суд способен учесть максимальное количество факторов для достижения справедливости в конкретном случае.

Говоря о поведении делинквента, обратим особое внимание на такое условие деликтной ответственности, как противоправность. Под ней следует понимать не просто нарушение нормы права или умаление субъективного права потерпевшего, а результат сопоставления разнообразных интересов: потерпевшего к обеспечению собственной безопасности, причинителя вреда к свободе действия, а также общественных интересов [Cartier 2007: 131]. Такое понимание, *во-первых*, иллюстрирует противоречие между свободой и безопасностью, *во-вторых*, подразумевает градацию благ, хотя на первый взгляд этот вывод не совсем очевиден. В случае определённых коллизий необходимо найти компромисс посредством расставления приоритетов [Коциоль 2016: 252]. К примеру, защита чести, достоинства и деловой репутации существует в конфликте с правом на свободное выражение мнения или правом на свободу средств массовой информации. Следовательно, проведение чёткой границы потребует всестороннего взвешивания всех коррелирующих интересов.

При таком фокусе рассмотрения проблемы получается, что от законодателя требуется, *во-первых*, установить случаи, когда поведение делинквента будет вовсе лишено противоправности (допустим, причинение вреда в состоянии необходимой обороны или с согласия потерпевшего). *Во-вторых*, необходимо определить абстрактные критерии, которые призваны помочь при обнаружении противоправности. При подобном подходе нагрузка на суды существенно возрастает, но это позволяет, как уже было отмечено, достичь справедливого решения в каждом конкретном случае.

Регулирование права причинения вреда в сети Интернет аналогичным образом должно следовать по пути максимальной гибкости. Это обстоятельство обусловлено несколькими важными политико-правовыми соображениями: 1) излишнее воздействие государства (речь об институциональном и систематическом принуждении)[24] сопряжено с высокими издержками[25];

[24] Мы исходим из гипотезы, согласно которой большинство правил поведения в Интернете формулируются в большей степени стихийно и, в большинстве случаев, на основе добровольной координации субъектов. Об институциональном принуждении см.: [де Сото Хесус 2008: 104].

[25] *Сухаревская А.* ВВС: Роскомнадзор может потратить на новую систему блокировок до 20 млрд рублей // Ведомости. 18.12.2022. URL: https://www.vedomosti.ru/technology/articles/2018/12/18/789620-roskomnadzor-blokirovok (дата обращения: 22.11.2022); Роскомнадзор выделил 57,7 млн рублей на разработку системы поиска запрещённого контента // Ведомости. 17.08.2022. URL: https://www.vedomosti.ru/technology/news/2022/08/17/936342-roskomnadzor-videlil-577-mln-rublei-na-razrabotku-sistemi-poiska-zapreschennogo-kontenta (дата обращения: 22.11.2022).

2) императивное регулирование приводит к потере социально значимой и ценной информации, которая может помочь государству держать потенциальные угрозы под контролем [Познер 2020: 104]; 3) чрезмерная реакция государства на возможные нарушения в Интернете может негативно отразиться на высокоинновационном характере деятельности некоторых субъектов Сети [де Сото Хесус 2008: 70–86].

Проанализировав общие положения деликтного права, связанные с причинением вреда в виртуальном пространстве, попробуем описать с учётом вышеизложенного оптимальную модель ответственности за киберделикт в международном праве.

**Ответственность за киберделикт в международном праве**

Важно отметить, что преимущество концепции киберделикта заключается в следующем. В отличие от иных категорий, разработанных для квалификации различных действий государств в виртуальном пространстве (кибероперация, кибервойна), она позволяет рассмотреть спектр моделей вредоносного поведения, следствием которых не всегда является причинение физического ущерба[26] (например, уничтожение информации о медицинских и фармацевтических исследованиях[27]; неправомерный доступ к спискам избирателей; вмешательство в работу фондового рынка).

Краеугольный камень доктрины деликтного права, как мы отмечали в предыдущем разделе, заключается в установлении стандартов, нарушение которых означает, что поведение нарушителя противоправно. Тем не менее при обсуждении ответственности государств (state liability) первостепенное значение приобретают именно вредоносные последствия, а не характеристика самого поведения. Строго говоря, первоначальное поведение необязательно должно быть противоправным, акцент смещается именно на результат (вред)[28]. Допустим, правовую квалификацию получает «серая зона» между кибервойной и правомерным поведением государства.

Обратим внимание на отдельные преимущества использования концепции киберделикта:

1) подобная квалификация позволяет потерпевшему государству требовать возмещение вреда, создавая тем самым новый вариант реагирования, который сводит к минимуму принятие несоразмерных поведению делинквента мер. С одной стороны, вероятность эскалации конфликта снижается, с другой – появляется сдерживающий нарушителя фактор *ex ante*, призванный сократить количество случаев причинения вреда;

2) во главу угла ставится компенсационная функция ответственности за киберделикт;

3) у государств появляется возможность манёвра в виртуальном пространстве, поскольку речь не идёт о *state responsibility*. Государство может правомерно действовать в «серой зоне», но будет обязано возместить вред в случае его причинения;

[26] В доктрине зачастую говорится о так называемых кибероперациях малой интенсивности, которые находятся вне поле зрения международного права. См.: [Walton 2017]. Думается, что такое наименование крайне неудачно и может ввести читателя в заблуждение. Как определять интенсивность, какие критерии для этого необходимы? На эти и многие другие вопросы не так просто получить однозначный ответ. По этой причине термин «киберделикт» представляется нам более подходящим.

[27] *Бацазова Ф., Веденеева Н.* Хакерские атаки сработали лишь с одним видом вакцин от COVID-19 // MK. 10.12.2020. URL: https://www.mk.ru/science/2020/12/10/khakerskie-ataki-srabotali-lish-s-odnim-vidom-vakcin-ot-sovid19.html (дата обращения: 22.11.2022).

[28] В национальном деликтном праве отдельных государств в равной степени наличествует подход к определению упречности поведения делинквента в зависимости от вредоносных результатов. К примеру, вождение автомобиля традиционно рассматривается в качестве правомерного поведения, однако причинённый при эксплуатации транспортного средства вред считается противоправным. Критику в адрес такого воззрения см.: [Jansen 2002].

4) этот режим ответственности создаёт надлежащие стимулы для совершенствования способов проведения кибервмешательств [Crootof 2018: 604–606].

Практическое применение такого подхода ставит ряд вопросов. *Во-первых*, каким должен быть характер вреда, чтобы государство-нарушитель было обязано его возместить? *Во-вторых*, существуют ли взаимные обязанности субъектов виртуального взаимодействия? *В-третьих*, как определить причинно-следственную связь между поведением и вредом? *В-четвёртых*, какой режим ответственности представляется оптимальным?

1. Национальное деликтное право разных государств направлено на защиту широкого спектра благ: личности, имущества, деловой репутации, экономических интересов. На международной арене аналогичным образом можно выявить палитру нуждающихся в охране интересов. К примеру, в соответствии с Указом Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» таковыми можно признать объекты критической инфраструктуры (п. 51); историческую память (п. 53); жизнь и здоровье граждан, причём в качестве наиболее уязвимой социальной группы в Указе поименована молодежь (п. 52); конституционные права и свободы человека и гражданина при обработке персональных данных, в том числе с использованием информационных технологий (подп. 8 п. 57), и так далее[29]. Для сравнения: в Стратегии по кибербезопасности Министерства обороны США[30] отмечается, что на Министерство обороны возлагается обязанность по защите интересов Соединённых Штатов от кибератак (независимо от квалификации) со значительными последствиями, включая гибель людей, катастрофический материальный ущерб, неблагоприятные последствия для внешней политики и экономики страны.

Установить закрытый перечень (*numerus clausus*) благ, подлежащих охране, означает обречь правовое регулирование на неудачу, поскольку скорость развития технологий обусловливает как появление новых вариаций вредоносного поведения, так и расширение перечня объектов, которым потенциально может быть причинён ущерб.

2. Можно предположить, что существуют три взаимные обязанности, которые несут государства: не причинять вред в виртуальном пространстве; проявлять должную осмотрительность; возместить вред, нанесённый в результате неосмотрительного поведения [Crootof 2018: 609].

Выделение подобных пунктов созвучно складывающимся в сфере ответственности за действия, не запрещённые международным правом, тенденциям. В 2006 г. Комиссией международного права (КМП) ООН были подготовлены «Проекты принципов, касающихся распределения убытков в случае трансграничного вреда, причинённого в результате опасных видов деятельности»[31]. Анализ этих документов позволяет сделать вывод, что указанную ответственность составляют первичные обязательства государств: 1) по предотвращению наступления вредоносных последствий (*duty to due diligence*, информирование, консультирование и прочее), по принятию надлежащих мер реагирования для уменьшения ущерба; 2) по обеспечению оперативной и адекватной компенсации в случае причинения вреда.

Обязанность проявлять должную осмотрительность относится к поведению, но не к результату. В этой связи, если ущерб наступил в случае непроявления государст-

[29] Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. 2021. № 27 (ч. II). Ст. 5351.

[30] The Department of Defense Cyber Strategy. April 2015. URL: https://www.hsdl.org/?view&did=764848 (accessed: 21.11.2022).

[31] Официальные отчёты Генеральной Ассамблеи. 61-я сессия (A/61/10). Дополнение № 10. Принципы содержатся в приложении к резолюции Генеральной Ассамблеи ООН A/RES/61/36 от 4 декабря 2006 года.

вом должной осмотрительности, это обстоятельство будет свидетельствовать о нарушении им своих обязательств. Данный факт приведёт к наступлению соответствующих последствий, предусмотренных общим международным правом (*state responsibility*). Речь идёт о прекращении деяния, если оно продолжается, предоставлении надлежащих заверений и гарантий неповторения, возможности применения к ответственному государству контрмер и санкций, полном возмещении вреда в виде реституции, компенсации и сатисфакции [Кожеуров 2016: 176].

Напротив, если ущерб наступил, несмотря на соблюдение обязанности по осмотрительности, государство должно предоставить оперативную, адекватную и эффективную компенсацию причинённого материального ущерба. Подобное обязательство относится к результату, а не к поведению. Иными словами, конкретные механизмы, модели, формы и способы такого возмещения определяются на усмотрение государства [Кожеуров 2016: 177]. Оно может принять на себя ответственность без вины (strict liability) или абсолютную ответственность, а также комбинировать различные режимы. Невыполнение обязательства по обеспечению компенсации влечёт ответственность государства (state responsibility).

Международный Суд ООН во многих случаях обращает внимание на существование у государств обязанности проявлять должную осмотрительность (*duty to due diligence*). Показательно, что в знаменитом решении по делу «Аргентины против Уругвая» (т.н. дело о целлюлозных заводах) отмечено, что обязанность проявлять должную осмотрительность состоит не только в принятии соответствующих правил и мер предосторожности, но и в определённом уровне осмотрительности при их соблюдении, а также в осуществлении контроля над государственными и частными лицами для защиты прав другой стороны[32].

Вместе с тем обязанность проявлять должную осмотрительность является наиболее дискуссионной. М. Шмитт утверждает, что в виртуальном пространстве она присутствует у государств [Schmitt 2015]. Напротив, Л. Чаркоп полагает, что обязанность проявлять должную осмотрительность, как это было установлено Международным Судом ООН в деле *Corfu Channel*, до сих пор находится в зачаточной форме [Chircop 2018: 667–668].

Тем не менее данное явление нашло своё воплощение в п. 6 Таллинского руководства 2.0 о международном праве, применимом к кибероперациям от 2017 года, разработанного по предложению Кибercентра НАТО[33]. В соответствии с указанным документом «государство должно руководствоваться принципом должной осмотрительности, не позволяя использовать свою территорию либо территориальную или кибернетическую инфраструктуру, находящуюся под его правительственным контролем, для кибероперации, которые затрагивают права других государств и оказывают на них неблагоприятное воздействие» [Schmitt 2017: 70]. Кроме того, в обязанности по осмотрительности также входят действия стран, направленные на прекращение кибероперации, проводимых с их территории, с использованием разумно доступных средств, когда они получают о них уведомление (п. 7 Таллинского руководства 2.0).

Вместе с тем предлагаемые Таллинскими руководствами подходы не обладают достаточным и универсальным свойством. Кроме того, они не носят обязывающего характера, а отражают предложения ряда исследователей, поддержанные группой

[32] Pulp Mills on the River Uruguay (Arg. v. Uru.), Judgment, 2010 I.C.J. Rep. 14 (Apr. 20). P. 69, 197.
[33] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence / Ed. by M. N. Schmitt. Cambridge: Cambridge University Press, 2017. 598 p. https://doi.org/10.1017/9781316822524

западных стран. В связи с этим целесообразной видится разработка дополнительных и нормативно применимых критериев для разрешения конфликтов в виртуальной среде. К примеру, при установлении содержания обязанности по должной осмотрительности следует учитывать, что чрезмерное ужесточение этого стандарта, вероятно, приведёт к созданию пагубных стимулов для государств вмешиваться в работу Сети. Иными словами, императивная обязанность предотвращать причинение вреда в виртуальном пространстве повлечёт усиление государством контроля за Интернетом. В то же время установление более мягкого стандарта создаст благоприятные условия как для свободного развития информационных технологий, так и для принятия государствами надлежащих мер предосторожности [Shackelford, Russel, Kuehn 2016].

Наконец, положения об ответственности можно структурировать иным образом: установить презумпцию того, что государства вправе заниматься не запрещённой международным правом деятельностью в виртуальном пространстве, даже если она наносит ущерб, при условии, что он во всяком случае будет компенсирован. Думается, что именно это решение удовлетворяет политико-правовым ожиданиям многих субъектов Сети [Crootof 2018: 612]. Повторно отметим: если для традиционных случаев закрепления объективной ответственности характерно стимулирование государств к созданию более надёжных источников повышенной опасности [Савельева 1996: 18], то в цифровой среде это обстоятельство может привести к повышению уровня государственного контроля над Интернетом с пагубными последствиями[34].

3. Следующий важный вопрос заключается в определении причинно-следственной связи. Разумеется, её установление отличается в случаях state liability от присвоения противоправного действия государству-нарушителю (*state responsibility*). Первое касается пагубных последствий тех действий, которые не запрещены международным правом [Sucharitkul 1996: 834–834]. Стоит отметить, что категория «причинность» может толковаться гораздо шире, чем понятие «присвоение» деятельности лиц или групп лиц, которые фактически действуют под руководством или контролем государства, в особенности если принимать во внимание обязанность по должной осмотрительности.

Р. Крутоф приводит пример, в соответствии с которым стандарт должной осмотрительности также облегчает проблему присвоения при совершении противоправного деяния [Crootof 2018: 613]. Предположим, государство А подвергается массированным кибервмешательствам, которые злонамеренно проводит государство В при использовании киберинфраструктуры государства С. Несмотря на то что А без труда может установить, что кибероперация была совершена С, первоначального нарушителя В обнаружить не так просто. Обязанность по должной осмотрительности позволяет потерпевшему государству информировать страну С об ущербе. Как итог, если последняя не предпримет разумных действий для прекращения кибероперации, она сама совершит противоправное деяние со всеми характерными последствиями.

На первый взгляд кажется, что подобное решение невообразимо расширяет пределы ответственности (responsibility) и приводит к эскалации конфликта. Иначе говоря, оно предоставляет возможность большему числу государств присвоить противоправные действия и прибегнуть к контрмерам. Тем не менее это сомнение может быть устранено следующим образом: нарушение осмотрительности должно приводить лишь к возмещению ущерба в контексте *state liability*.

4. При ответе на многие из вопросов, поставленных выше, красной нитью проходит

[34] В американской доктрине международного права в подтверждение этого тезиса зачастую приводят примеры из области частного права [Shackelford, Russel, Kuehn 2016].

обязанность должной осмотрительности. Выбор оптимального режима ответственности не станет исключением. Несомненно, государство должно нести ответственность за правомерные действия, связанные с высоким риском значительного ущерба, который может быть как непредвидимым, так и непредотвратимым, даже в случаях, если его поведение было осмотрительным. Речь идёт о так называемой объективной ответственности [Fitzmaurice 2008: 1022], юридическим основанием которой является компенсационная норма[35], в рассматриваемом случае – обязанность должной осмотрительности.

Как легко предположить, стандарт объективной ответственности значительно упрощает проблему. Если возможно установить, что в результате действий или бездействия государства был причинён ущерб, оно, бесспорно, обязано его возместить. Между тем предлагается несколько отойти от такого жёсткого подхода, *во-первых*, если поведение было связано с осуществлением общественно полезных задач [Walton 2017: 1497], *во-вторых*, когда потерпевшее государство не принимает никаких мер кибербезопасности [Gross 2015]. В последнем случае необходимо уменьшать объём объективной ответственности государства-нарушителя, поскольку отсутствие минимальных средств по кибербезопасности может рассматриваться как нарушение обязанности должной осмотрительности (своего рода *contributory negligence*).

Таким образом, киберделикт представляет собой наиболее эффективный механизм разрешения конфликтов в виртуальном пространстве, который, с одной стороны, позволяет получить возмещение потерпевшему государству, а с другой – не приводит к эскалации конфликта. При этом в орбиту исследования не входили два важных вопроса: возможность правотворческого трека для киберсреды и создание независимой международной организации для разрешения соответствующих споров. В отношении первой проблемы можно полностью согласиться с мнением В. Н. Русиновой, которая достаточно убедительно проиллюстрировала тщетность любых попыток государств прийти к консенсусу и, следовательно, маловероятность всеобъемлющих конвенций по вопросам цифровизации [Русинова 2022: 49]. Это же рассуждение обусловливает преждевременность любых решений второй проблемы.

* * *

Архитектура сети Интернет создаёт плодородные основания для всякого рода правонарушений. Как было показано, в международном праве на момент написания статьи отсутствует эффективный механизм урегулирования конфликтов в цифровой среде. Потерпевшие страны зачастую прибегают к несоразмерным мерам против государств-нарушителей, что способствует лишь эскалации конфликта. Усложняет обстоятельство и тот факт, что у государств не имеется никаких средств реагирования на кибероперации малой интенсивности. Решить эти и некоторые другие проблемы позволяет разработанная в частном праве концепция киберделикта. Опираясь на деликтное и международное право, мы пришли к выводу, что, с одной стороны, киберделикт позволяет устранить последствия нарушений *ex post*, а с другой – не приводит к эскалации конфликта. Кроме того, у государств появляется пространство для манёвров в виртуальной среде, поскольку оно может правомерно действовать в «серой зоне», но будет обязано возместить вред в случае его причинения. Думается, что признание режима ответственности за киберделикт позволит создать надлежащие стимулы для совершенствования способов проведения кибервмешательств.

[35] Более подробно о компенсационных нормах см.: [Савельева 1996: 31].

**Список литературы**

*Белых В.С., Пучков В.О.* Концепция киберделикта (Cybertort) в англо-американском праве // Юрист. 2020. № 10. С. 2–11.

*Гаджиев Г.А.* Принцип равного правонаделения и паритетной (эластичной) правовой защиты // Гражданское право: современные проблемы науки, законодательства, практики: Сб. статей к юбилею доктора юридических наук, профессора Евгения Алексеевича Суханова. М.: Статут, 2018. С. 132–150.

*Гаркуша-Божко С.Ю.* Проблема кибершпионажа в международном гуманитарном праве // Московский журнал международного права. 2021. № 1. С. 70–80. https://doi.org/10.24833/0869-0049-2021-1-70-80

*Иноземцев М.И.* Цифровое право: в поисках определённости // Цифровое право. 2021. Т. 2. №1. С. 8–28. https://doi.org/10.38044/2686-9136-2021-2-1-8-28

*Кодиоль Х.* Гибкая система — золотая середина в законодательстве и доктрине // Вестник гражданского права. 2016. Т. 16. № 6. С. 246–267.

*Кожеуров Я.С.* Дифференциация международной ответственности: тенденции и перспективы // Будущее международного права: Сб. статей / Под ред. К. А. Бекяшева. М.: Проспект, 2016. С. 166–178.

*Лукашук И.И.* Международное право. Особенная часть: Учебник для студентов юрид. фак. и вузов. М.: Волтерс Клувер, 2005. 517 с.

*Мартенс Ф.Ф.* Современное международное право цивилизованных народов. СПб.: Министерство Путей Сообщения, 1882. 419 с.

Международное право: В 2 ч. Ч. 2: Учебник для вузов / Отв. ред. А.Н. Вылегжанин. М.: Юрайт, 2021. 664 с.

*Познер Р.А.* Рубежи теории права / Пер. с англ. И.В. Кушнаревой; под ред. М.И. Одинцовой. М.: Изд. дом Высшей школы экономики, 2020. 482 с.

*Русинова В.Н.* Международно-правовая квалификация вредоносного использования информационно-коммуникационных технологий: в поисках консенсуса // Московский журнал международного права. 2022. № 1. С. 38–51. https://doi.org/10.24833/0869-0049-2022-1-38-51

*Савельева Л.В.* Проблема объективной ответственности в международном праве: Дис. ... канд. юрид. наук. М.: МГИМО МИД России, 1996. 180 с.

*Синицын С.А., Дьяконова М.О., Чурсина Т.И.* Смарт-контракты в цифровой экономике: договорное регулирование и разрешение споров // Цифровое право. 2021. Т. 2. № 4, С. 40–50. https://doi.org/10.38044/2686-9136-2021-2-4-40-50

*Степанов С.К.* Деконструкция правосубъектности или место искусственного интеллекта в праве // Цифровое право. 2021. Т. 2. № 2. С. 14–30. https://doi.org/10.38044/2686-9136-2021-2-2-14-30

*Суханов Е.А.* О гражданско-правовой природе цифрового имущества // Вестник гражданского права. 2021. Т. 21. № 6. С. 7–29.

*Уэрта де Сото Х.* Социализм, экономический расчёт и предпринимательская функция / Пер. с англ. В. Кошкина; под ред. А. Куряева. М.; Челябинск: ИРИСЭН; Социум, 2008. 488 с.

*Cartier M.* Begriff der Widerrechtlichkeit nach Art. 41 OR: Dissertation der Universität St. Gallen, Hochschule für Wirtschafts-, Rechts- und Sozialwissenschaften (HSG) zur Erlangung der Würde eines Doktors der Rechtswissenschaft. Nr. 3287. Eschen, 2007. S. 198.

*Chircop L.* A Due Diligence Standard of Attribution in Cyberspace // International and Comparative Law Quarterly. 2018. Vol. 67. No. 3. P. 643–668. https://doi.org/10.1017/S0020589318000015

*Crootof R.* International Cybertorts: Expanding State Accountability in Cyberspace // Cornell Law Review. 2018. Vol. 103. No. 3. P. 565–644.

*Dam C.* van. European Tort Law. 2nd ed. Oxford: Oxford University Press, 2013. 656 p.

*Duranske B.T.* Virtual Law: Navigating the Legal Landscape of Virtual Worlds. Chicago: ABA Publishing, 2008. 461 p.

*Finnis J.* Absolute Rights: Some Problems Illustrated // The American Journal of Jurisprudence. 2016. Vol. 61. No. 2. P. 195–215. https://doi.org/10.1093/ajj/auw015

*Gill T.D.* Non-Intervention in the Cyber Context // Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy / Ed. by K. Ziolkowski. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2013. P. 217–238.

*Hathaway O.* et al. The Law of Cyber-Attack // California Law Review. 2012. Vol. 100. No. 4. P. 817–885.

*Gross O.* Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents // Cornell International Law Journal. 2015. Vol. 48. No. 3. P. 481–511.

*Jansen N.* Das Problem der Rechtswidrigkeit bei § 823 Abs. 1 BGB // Archiv für die civilistische Praxis. 2002. Bd. 202. S. 517–554.

*Koziol H.* Das bewegliche System – die golden Mitte für Gesetzgebung und Dogmatik // Austrian Law Journal. 2017. Bd. 3. S. 160–182.

*Lubin A.* Cyber Law and Espionage Law as Communicating Vessels // Proceedings of the 10th International Conference on Cyber Conflict, CyCon X: Maximising Effects. 2018 / Ed. by T. Minárik, R. Jakschis, L. Lindström. Tallinn: NATO CCD COE Publications, 2018. P. 203–226.

*Fitzmaurice M.* International Responsibility and Liability // Oxford Handbook of International Environmental Law / ed. by D. Bodansky, J. Brunnee, E. Hey. Oxford: Oxford University Press, 2008. P. 1010–1035. https://doi.org/10.1093/oxfordhb/9780199552153.013.0044

*Maras M.-H.* Cybercriminology. Oxford: Oxford University Press, 2016. 448 p.

*Maurer T.* Cyber Mercenaries: The State, Hackers, and Power. Cambridge: Cambridge University Press, 2018. 266 p.

*Murphy J.* Heterogeneity of Tort Law // Oxford Journal of Legal Studies. 2019. Vol. 39. No. 3. P. 455–482. https://doi.org/10.1093/ojls/gqz008

*Nipperdey H.C.* Rechtswidrigkeit, Sozialadäquanz, Fahrlässigkeit, Schuld im Zivilrecht // Neue Juristische Wochenschrift. 1957. Bd. 10. S. 1777–1782.

*Pirker B.* Territorial Sovereignty and Integrity and the Challenges of Cyberspace // Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy / Ed. by K. Ziolkowski. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2013. P. 189–289.

*Rustad M.L.* The Role of Cybertorts in Internet Governance // The Comparative Law Yearbook of International Business. Vol. 31 / Ed. by D. Campbell. Alphen aan den Rijn: Kluwer Law International, 2009. P. 391–419.

*Schmitt M.* In Defense of Due Diligence in Cyberspace // Yale Law Journal Forum. 2015. No. 68. P. 68–81.

*Shackelford S., Russell S., Kuehn A.* Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors // Chicago Journal of International Law. 2016. Vol. 17. No. 1. P. 1–50. URL: https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1700&context=cjil

*Shaw M.* International Law. 9th ed. Cambridge: Cambridge University Press, 2021. 1308 p.

*Sucharitkul S.* State Responsibility and International Liability under International Law // The Loyola of Los Angeles International and Comparative Law Review. 1996. Vol. 18. P. 821–840.

*Walton B.A.* Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law // Yale Law Journal. 2017. Vol. 126. No. 5. P. 1460–1519.

# THE CONCEPT OF CYBERTORT AND LIABILITY IN INTERNATIONAL LAW

MAXIM INOZEMTSEV
MGIMO University, Moscow, 119454, Russia

SEMEN STEPANOV
HSE University, Moscow, 101000, Russia

**Abstract**

The digitalization of social relations not only simplifies life, but also creates the ground for an increase in the number of offences in cyberspace, including those involving subjects of international law. Victimized countries often resort to the use of disproportionate measures against offending States using traditional instruments of international law. In addition, the lack of optimal means of responding to low-intensity cyber-interference is ineffective. Having considered the main mechanisms and complexities faced by international law when states inflict harm through digital technologies, the authors propose a private law concept of cybertort, the use of which, on the one hand, makes it possible to eliminate the consequences

of ex post violations and, on the other hand, does not lead to an escalation of the existing conflict. In describing the problems of interstate interaction, the auxiliary nature of the use of private legal tools is emphasized. Using both systemic and comparativist methods of research, the authors reveal the essence and legal consequences of the variable qualification of an act as an offense (state responsibility) or an act not prohibited by international law (state liability), as well as substantiate the need to apply a flexible system of legal regulation to the law of causing harm on the Internet. Using the critical method, the shortcomings of the modern doctrine of international law in the considered context are revealed. Using the deductive method, with reference to Russian and foreign doctrinal sources, legal acts, as well as judicial practice, an optimal regime of liability for an offence in the digital environment is proposed, which creates appropriate incentives to improve the methods of cyber-interference.

**Keywords:**

cybertort; cyber interference; cyber-attack; international law; tort; liability; digital law.

## References

Belykh V.S., Puchkov V.O. (2020). Kontseptsiya kiberdelikta (Cybertort) v anglo-amerikanskom prave [The Cybertort Concept in the Anglo-American law]. *Yurist*. No. 10. P. 2–11.

Cartier M. (2007). *Begriff der Widerrechtlichkeit nach Art. 41 OR*. Dissertation der Universität St. Gallen, Hochschule für Wirtschafts-, Rechts- und Sozialwissenschaften (HSG) zur Erlangung der Würde eines Doktors der Rechtswissenschaft. Nr. 3287. Eschen. S. 198.

Chircop L. (2018). A Due Diligence Standard of Attribution in Cyberspace // International and Comparative Law Quarterly. Vol. 67. No. 3. P. 643–668. https://doi.org/10.1017/S0020589318000015

Crootof R. (2018). International Cybertorts: Expanding State Accountability in Cyberspace. *Cornell Law Review*. Vol. 103. No. 3. P. 565–644.

Dam C. van (2013). *European Tort Law*. 2nd ed. Oxford: Oxford University Press. 656 p.

Duranske B.T. (2008). *Virtual Law: Navigating the Legal Landscape of Virtual Worlds*. Chicago: ABA Publishing. 461 p.

Finnis J. (2016). Absolute Rights: Some Problems Illustrated. *The American Journal of Jurisprudence*. Vol. 61. No. 2. P. 195–215. https://doi.org/10.1093/ajj/auw015

Fitzmaurice M. (2008). International Responsibility and Liability. In D. Bodansky, J. Brunnee, E. Hey. (eds.). *Oxford Handbook of International Environmental Law*. Oxford: Oxford University Press. P. 1010–1035. https://doi.org/10.1093/oxfordhb/9780199552153.013.0044

Gadzhiev G.A. (2018). Printsip ravnogo pravonadeleniya i paritetnoy (elastichnoy) pravovoy zashchity [The Principle of Equal Entitlement and Parity (Elastic) Legal Protection]. *Civil Law: Modern Problems of Science, Legislation, Practice: Collection of Articles for the Anniversary of Doctor of Law, Professor Evgeny Alekseevich Sukhanov*. Moscow: Statut. P. 132–150.

Garkusha-Bozhko S.Y. (2021). Problema kibershpionazha v mezhdunarodnom gumanitarnom prave [The Problem of Cyber Espionage in International Humanitarian Law]. *Moscow Journal of International Law*. No. 1. P. 70–80. https://doi.org/10.24833/0869-0049-2021-1-70-80

Gill T.D. (2013). Non-Intervention in the Cyber Context. In: K. Ziolkowski. (ed.). *Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. P. 217–238.

Gross O. (2015). Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents. *Cornell International Law Journal*. Vol. 48. P. 481–511.

Hathaway O. et al. (2012). The Law of Cyber-Attack. *California Law Review*. Vol. 100. No. 4. P. 817–885.

Inozemtsev M.I. (2021). Tsifrovoe pravo: v poiskakh opredelennosti [Digital Law: the pursuit of certainty]. *Digital Law Journal*. Vol. 2. No. 1. P. 8–28. https://doi.org/10.38044/2686-9136-2021-2-1-8-28

Jansen N. (2002). Das Problem der Rechtswidrigkeit bei § 823 Abs. 1 BGB. *Archiv für die civilistische Praxis*. Bd. 202. S. 517–554.

Kozheurov Y.S. (2016). Differentsiatsiya mezhdunarodnoy otvetstvennosti: tendentsii i perspektivy [Differentiation of International responsibility: the trends and prospects]. In: K. A. Bekyasheva. (ed.). *The Future of International Law: Collection of Articles*. Moscow: Prospekt. P. 166–178.

Koziol H. (2016). Gibkaya sistema – zolotaya seredina v zakonodatel'stve i doktrine [Flexible System – Golden Mean in Legislation and Doctrine]. *Herald of Civil Law*. No. 6. P. 246–267.

Koziol H. (2017). Das bewegliche System – die golden Mitte für Gesetzgebung und Dogmatik. *Austrian Law Journal*. Bd. 3. S. 160–182.

Lubin A. (2018). Cyber Law and Espionage Law as Communicating Vessels. In: T. Minárik, R. Jakschis, L. Lindström (eds.). *Proceedings of the 10th International Conference on Cyber Conflict, CyCon X: Maximising Effects. 2018*. Tallinn: NATO CCD COE Publications. P. 203–226.

Lukashuk I.I. (2005). *Mezhdunarodnoe pravo. Osobennaya chast': Uchebnik dlya studentov yurid. fak. i vuzov* [International Law. Special Part: A textbook for law students]. 3rd ed., rev. and exp. Moscow: Walters Kluwer. 517 p.

Maras M.-H. (2017). *Cybercriminology*. Oxford: Oxford University Press. 448 p.

Martens F.F. (1882). *Sovremennoe mezhdunarodnoe pravo tsivilizovannykh narodov* [Modern International Law of Civilized Peoples]. Saint Petersburg: Ministerstvo Putey Soobshcheniya. 419 p.

Maurer T. (2018). *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge: Cambridge University Press. 266 p.

Murphy J. (2019). Heterogeneity of Tort Law. *Oxford Journal of Legal Studies*. Vol. 39. No. 3. P. 455–482. https://doi.org/10.1093/ojls/gqz008

Nipperdey H.C. (1957). Rechtswidrigkeit, Sozialadäquanz, Fahrlässigkeit, Schuld im Zivilrecht. *Neue Juristische Wochenschrift*. Bd. 10. S. 1777–1782.

Pirker B. (2013). Territorial Sovereignty and Integrity and the Challenges of Cyberspace. In: K. Ziolkowski. (ed.). *Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. P. 189–289.

Pozner R.A. (2020). *Rubezhi teorii prava* [Frontiers of the Theory of Law]. Moscow: Publishing House of the Higher School of Economics. 482 p.

Rusinova V.N. (2022). Mezhdunarodno-pravovaya kvalifikatsiya vredonosnogo ispol'zovaniya informatsionno-kommunikatsionnykh tekhnologiy: v poiskakh konsensusa [International Legal Qualification of the Harmful Use of Information and Communication Technologies: in search of consensus]. *Moscow Journal of International Law*. No. 1. P. 38–51. https://doi.org/10.24833/0869-0049-2022-1-38-51

Rustad M.L. (2009). The Role of Cybertorts in Internet Governance. In: D. Campbell. *The Comparative Law Yearbook of International Business*. Vol. 31. Alphen aan den Rijn: Kluwer Law International. P. 391–419.

Savel'eva L.V. (1996). *Problema ob"ektivnoи otvetstvennosti v mezhdunarodnom prave* [The problem of objective liability in international law]. PhD thesis. Moscow. 180 p.

Shackelford S., Russell S., Kuehn A. (2016). Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors. *Chicago Journal of International Law*. Vol. 17. No. 1. P. 1–50. URL: https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1700&context=cjil

Shaw M. (2021). *International Law*. 9th ed. Cambridge: Cambridge University Press. 1308 p.

Schmitt M. (2015). In Defense of Due Diligence in Cyberspace. *Yale Law Journal Forum*. No. 68. P. 68–81.

Sinitsyn S.A., Diakonova M.O., Chursina T.I. *Smart-kontrakty v cifrovoj ekonomike: dogovornoe regulirovanie i razreshenie sporov* [Smart-Contracts in the digital economy: Contractual regulation and dispute resolution]. *Tsifrovoe pravo*. Vol. 2. No. 4. P. 40–50. https://doi.org/10.38044/2686-9136-2021-2-4-40-50

Stepanov S.K. (2021). Dekonstruktsiya pravosub"ektnosti ili mesto iskusstvennogo intellekta v prave [Deconstruction of the Legal Personality of Artificial Intelligence]. *Digital Law Journal*. Vol. 2. No. 2. P. 14–30. https://doi.org/10.38044/2686-9136-2021-2-2-14-30

Sucharitkul S. (1996). State Responsibility and International Liability Under International Law. *The Loyola of Los Angeles International and Comparative Law Review*. Vol. 18. P. 821–840.

Suhanov E.A. (2021). O grazhdansko-pravovoy prirode tsifrovogo imushchestva [On the Civil Law Nature of Digital Property]. *Herald of Civil Law*. Vol. 21. No. 6. P. 7–29.

Uerta de Soto H. (2008). *Sotsializm, ekonomicheskiy raschet i predprinimatel'skaya funktsiya* [Socialism, Economic Calculation, and the Entrepreneurial Function]. Moscow; Chelyabinsk: IRISEN; Socium. 488 p.

Schmitt M.N. (ed.) (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Cambridge: Cambridge University Press. 598 p. https://doi.org/10.1017/9781316822524

Vylegzhanin A.N. (ed.). (2021). *Mezhdunarodnoe pravo. V 2 chastyakh. Ch. 2: Uchebnik dlya vuzov* [International Law. In 2 parts. Part 2: textbook for universities]. 4th ed. Moscow: Yurayt. 664 p.

Walton B.A. (2017). Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law. *Yale Law Journal*. Vol. 126. No. 5. P. 1460–1519.