Журнал международного права и международных отношений. 2022. № 3-4 (102-103). С. 3—11.
Journal of International Law and International Relations. 2022. N 3-4 (102-103). P. 3—11.
УДК 341 DOI: 10.33581/2072-0513-2022-3-4-3-11

ПРАВОВАЯ ОЦЕНКА ВВЕДЕНИЯ САНКЦИЙ ЗА ЗЛОНАМЕРЕННЫЕ ДЕЙСТВИЯ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Елена Довгань

Настоящая статья посвящена правовой оценке возможности применения санкций Советом Безопасности ООН и в одностороннем порядке государствами и региональными международными организациями в ответ на злонамеренные действия в информационном пространстве. Проанализированы основные случаи введения санкций в ответ на такую деятельность (атаки в отношении критической инфраструктуры; атаки, достигающие уровня вооруженного нападения; распространение враждебной либо злонамеренной информации; подрыв безопасности государства с использованием информационных технологий; совершение киберпреступлений) и дана их правовая оценка с точки зрения международного права.

Ключевые слова: доступ к правосудию; злонамеренные действия в информационном пространстве; информационная безопасность; киберпреступность; односторонние санкции; санкции.

«Legal Status of Sanctions Introduced in Response to Malicious Activity in Cyberarea» (Alena Douhan)

Current article focuses on the legal assessment and the possibility to use sanctions by the UN Security Council as well as states and regional organisations unilaterally in response to the malicious activity in cyberarea. The article identifies the main situations when sanctions were introduced with reference to malicious cyberactivity such as: attacks over critical infrastructure; attacks which can be qualified as an armed attack; dissemination of hostile propaganda or malicious information; cybercrimes; undermining state security through cybermeans, and presents legal qualification on the use of sanctions from the international law point view.

Keywords: access to justice; cybercrimes; cybersecurity; malicious activity in cyberarea; sanctions; unilateral sanctions.

Современные информационные технологии (далее — ИТ) существенным образом изменили мир. Все чаще деятельность с использованием ИТ, даже если она осуществляется физическими и юридическими лицами, признается в качестве угрозы международному миру и безопасности, безопасности государств и личности (резолюции Совета Безопасности ООН (далее — СБ ООН) 2419 (2018) [52], 2490 (2019) [53], 2462 (2019) [54].

В результате ряд государств и международных организаций, включая США, Европейский союз (далее — ЕС), Великобританию, Австралию, разработали национальное законодательство, позволяющее введение санкций без полномочий, полученных от СБ ООН, в отношении государств, физических и юридических лиц, в том числе граждан — резидентов третьих стран, за злонамеренную деятельность с использованием ИТ. При этом правовая оценка предпринимаемых мер обычно не осуществляется. Данная проблема также практически не исследована в международном праве, несмотря на появление единичных работ в 2021—2022 гг. [1; 9]. В связи с вышеизложенным актуальность темы исследования не подлежит сомнению.

В настоящее время применение, а также виды, формы, цели и методы осуществления санкций существенно расширяются. Отдельные авторы понимают киберсанкции как *«санкции, уполномочивающие внесение в списки иностранных граждан, юридических лиц и правительственные учреждения третьих стран за различные виды злонамеренной деятельности в информационном пространстве, включая кибератаки»* [11], что, на наш взгляд, некорректно не только в свете ссылки на наличие права введения таких санкций, которое в международном праве отсутствует, но и в связи с тем, что традиционно виды санкций определяются исходя из вида принимаемых мер (экономические, финансовые) либо объекта, к которому они применяются (целевые, секторальные). Как будет отражено ниже, предпринимаемые государствами и междуна-

Автор:
Довгань Елена Фёдоровна — доктор юридических наук, профессор кафедры международного права факультета международных отношений Белорусского государственного университета, *e-mail: alena.f.douhan@gmail.com*
Белорусский государственный университет. Адрес: 4, пр. Независимости, Минск, 220030, БЕЛАРУСЬ

Author:
Douhan Alena — Doctor of Law, Professor of the Department of International Law of the Faculty of International Relations, Belarusian State University, *e-mail: alena.f.douhan@gmail.com*
Belarusian State University. Address: 4, Nezavisimosti ave., Minsk, 220030, BELARUS

родными организациями меры со ссылкой на злонамеренную деятельность с использованием ИТ осуществляются различными методами, включая финансовые, целевые и пр. В связи с этим в настоящей статье термин «киберсанкции» не используется.

СБ ООН рассматривал вопрос о создаваемых деятельностью в сфере ИТ угрозах в ряде случаев. Так, Совет признал, что деятельность отдельных физических и юридических лиц в информационном пространстве может создавать угрозу международному миру и безопасности; определил риски использования ИТ в террористической деятельности; закрепил обязанность государств обеспечить безопасность своих граждан в первую очередь от террористической активности во всех формах, в том числе путем контроля информационных потоков, оборота криптовалют, предотвращения легализации преступных доходов и финансирования терроризма (резолюция 2462 (2019) [54, para. 19]), данных о пассажирах на авиасообщениях (резолюция 2482 (2019) [51, para. 15(c)]), расследования террористических преступлений; обратил внимание, что распространение информации может носить злонамеренный характер, возбуждать ненависть, вспышки экстремизма, радикализацию населения и создавать угрозу поддержанию международного мира и безопасности (резолюция 2490 (2019) [13; 53, para. 2]); создал Панель экспертов для оценки использования ИТ Северной Кореей (далее — КНДР) в качестве механизма обхода санкций (резолюция 1874 (2009) [48]). Единственный случай принятия санкций СБ ООН в отношении ряда и лиц и организаций, в том числе ответственных за подготовку атак с использованием ИТ, касается ситуации в Йемене: заморожены счета и активы, введены запрет на поездки (резолюция 2140 (2014) [55, para. 11—19]) и эмбарго на поставку вооружений лицам, в отношении которых введены санкции, или организациям под их контролем (резолюция 2216 (2015) [56, para. 14—19]). Соответствующие лица квалифицируются как вовлеченные в террористическую деятельность.

В отличие от СБ ООН, практика государств и региональных организаций по введению санкций со ссылкой на злонамеренную деятельность в информационном пространстве в последние пять лет активно расширяется.

Так, законодательство США предусмотрело введение санкций за действия с использованием ИТ путем атак на критическую инфраструктуру, вмешательства в избирательный процесс, нарушения функционирования компьютерных систем или операций, неправомерного использования финансовых средств и персональных данных и пр. (исполнительный приказ 13694 от 1 апреля 2015 г. (в ред. исполнительного приказа 13757 от 28 декабря 2016 г.) [7; 58]), существенных деструктивных вирусных атак, предотвращения доступа к системам (Акт о снижении влияния России в Европе и Евразии [60, para. 224]), подрыва доверия к выборам в США, скрытой пропаганды и дезинформации, распространяемой с использованием ИТ (исполнительный приказ 13848 от 12 сентября 2018 г. [30]), предотвращения доступа, ухудшения качества, прерывания функционирования информационных технологий и систем, несанкционированного доступа, уничтожения, распространения данных, осуществления информационного влияния (Акт о противодействии противникам Америки посредством санкций [23, para. 224], исполнительный приказ 14024 от 15 апреля 2021 г. [8]). На основании указанных документов США введены санкции в отношении 303 физических и юридических лиц более чем из 10 государств [6], в том числе со ссылкой на незаконное вмешательство в выборы в отношении 2 государственных органов Российской Федерации, 46 граждан и 13 компаний Российской Федерации и Украины [67]; за совершение хищений имущества с использованием ИТ в отношении 5 граждан Нигерии [63]. Возможно также внесение в санкционные списки лиц, сотрудничающих с уже находящимися под санкциями лицами и организациями, например КНДР (так называемые вторичные санкции [40]). Санкции США вводятся путем замораживания счетов, запрета на въезд и размещения информации о лице в качестве преступника, террориста либо угрозы национальной безопасности США.

ЕС впервые принял законодательство, предусматривающее введение санкций за деятельность в информационном пространстве в 2019 г., оговорив возможность запретов на выдачи виз, разрешений на въезд и заморозку счетов включенных в списки лиц (регламент ЕС 2019/796 от 17 мая 2019 г. [22, p. 1]) в связи с тем, что их деятельность создает угрозу ЕС либо осуществлению внешней политики ЕС (пп. 5—6). В результате были введены санкции в отношении 8 лиц и 4 организаций из России, Китая и КНДР (имплементирующие регламенты Совета 2020/1125 от 30 июля 2020 г. [19, p. 4—9], 2020/1536 от 22 октября 2020 г. [20, p. 1—4]). Регламент ЕС 2022/350 от 1 марта 2022 г. также запретил вещание российских СМИ *Sputnik* и *RT* в ЕС, квалифицировав их как распространяющие дезинформацию, пропаганду, манипуляцию общественным мнением, подтасовку фактов (пп. 3, 5—7), представляющие «гибридную угрозу», угрозу безопасности и публичному порядку ЕС (пп. 3, 8) [18; 21].

Регламент о киберсанкциях Великобритании [61] во многом дублировал регламент ЕС и ввел санкции в отношении тех же лиц, которые уже находились под санкциями ЕС [9, p. 933]. В декабре 2021 г. Австралия внесла изменения в Акт об автономных санкциях, закрепив возможность их введения в ответ на «злонамеренную деятельность в киберпространстве» [5, para. 4].

Применение санкций и иных видов принудительных мер в ответ на злонамеренные действия с использованием ИТ вызывает ряд серьезных вопросов с точки зрения международного права. Определенные рамки устанавливаются СБ ООН в рамках борьбы с международным терроризмом. Так, СБ ООН прямо закрепляет обязанность государств принять широкий перечень необходимых мер для предотвращения использования ИТ в целях *«распространения враждебной пропаганды, разжигания насилия, отмывания денег и финансирования терроризма, оправдания террористической деятельности и идеологии, вовлечения в террористическую деятельность, планирования и совершения террористических актов»* (резолюции 2419 (2018) [52, preamble], 2462 (2019) [54, preamble, para. 19, 20]). Фактически СБ ООН оставляет разработку совокупности законодательных, административных и иных мер в указанных случаях на усмотрение каждого конкретного государства, указывая, однако, на их обязанность обеспечить соответствие предпринимаемых мер их обязательствам, вытекающим из международного права, международного гуманитарного права, права прав человека и права беженцев (резолюции 2501 (2019) [49, preamble], 2535 (2020) [50, para. 7], 2482 (2019) [51, preamble, para. 15(c)], 2462 (2019) [54, para. 6, 24]).

Вместе с тем введение государствами односторонних санкций в отношении государственных органов, должностных, физических и юридических лиц в рамках противодействия злонамеренной деятельности с использованием ИТ значительно выходит за рамки борьбы с терроризмом и вызывает ряд вопросов с точки зрения их правовой квалификации.

Так, возможность применения односторонних санкций государствами для реализации санкций СБ ООН, концепция подразумеваемой, молчаливой или общей санкции [7, p. 401; 28, p. 373; 33, p. 538; 34, p. 17—19; 36, p. 125; 39, p. 63—64] либо возможность применения принудительных мер за нарушение санкционного режима СБ ООН без предоставления им дополнительных полномочий неоднократно осуждались в международно-правовой доктрине [29, p. 13—15; 35, p. 282; 57, p. 654]. Уже с 1998 г. Генеральная Ассамблея ООН призывала государства *«прекратить использование односторонних принудительных мер, которые не санкционированы соответствующими органами ООН»* (резолюция 52/181 [66, para. 2]). Именно поэтому применение дополнительных мер государствами для обеспечения реализации санкций СБ ООН, применяемых в отношении КНДР, либо контртеррористических целевых санкций против лидеров оппозиционных хуситских групп в Йемене при отсутствии санкции СБ ООН неправомерно.

Устав ООН не закрепляет возможность применения односторонних принудительных мер без санкции СБ ООН. Вследствие этого, как и любые иные односторонние санкции, санкции в ответ на злонамеренную деятельность в информационном пространстве могут применяться лишь в тех случаях, если они не нарушают международных обязательств государств, включая обязательства в области прав человека, либо если их противоправность может быть исключена в порядке контрмер в соответствии с правом международной ответственности [см.: 25].

Следует учитывать, что право государства действовать в порядке контрмер не является неограниченным. В соответствии со статьей 49(1) Проекта статей об ответственности государств за международные противоправные деяния 2001 г. (далее — ПСОГ) *«государство-жертва может принимать контрмеры против государства, ответственного за совершение международного противоправного деяния с тем, чтобы побудить его выполнять его международные обязательства»* [26, p. 43—59; 62]. Согласно статье 48 ПСОГ контрмеры могут применяться иными, чем непосредственно затронутое государство, странами в случае нарушения обязательств *erga omnes*, например совершения актов агрессии, геноцида, военных преступлений. Таким образом, государства могут применять односторонние санкции в порядке контрмер к государству в ответ на нарушение им международных обязательств, непосредственно затрагивающих права применяющего меры государства, либо в случае совершения нарушения обязательств *erga omnes* при соблюдении ограничений статей 49—51 ПСОГ, а именно необходимость, пропорциональность допущенному нарушению, запрет нарушать императивные нормы международного права, применять силу, репрессалии по международному гуманитарному праву, нарушать основополагающие права человека [26, para. 6; 27, s. 66; 65, p. 136—137]. В доктрине справедливо подчеркивается, что санкции не могут носить характер наказания [32, p. 62], а должны применяться в соответствии с международно-правовыми стандартами.

Таким образом, в качестве контрмер могут быть квалифицированы только односторонние санкции, применяемые к государству за нарушение его международных обязательств для того, чтобы обеспечить их выполнение с должным учетом атрибутивности злонамеренной деятельности государства в информационной сфере (ПСОГ, стст. 4—11) [26, p. 40—52].

С учетом вышеизложенного возможность квалифицировать применение односторонних санкций в ответ на злонамеренную деятельность с использованием ИТ весьма сомнительна. Так, применение санкций к государственным органам и должностным лицам государства не соответствует принципу

суверенного равенства государств как императивной норме международного права, положениям об иммунитетах государств и их собственности, особенно, когда в результате введения санкций налагается арест на имущество всех компаний, находящихся под контролем соответствующего государственного органа.

Представляется невозможным согласиться с позицией некоторымх авторов, в соответствии с которой иммунитеты государственной собственности распространяются лишь на механизмы судебного разбирательства согласно обычным нормам международного права, закрепленным в Конвенции о юрисдикционных иммунитетах государств и их собственности, и неприменимы в отношении принятия административных решений [11, p. 935]. Иммунитет государств и их собственности носит абсолютный характер, является производным от наличия государственного суверенитета и принципа суверенного равенства государств и служит для целей обеспечения функционирования государства. Поскольку административное решение предоставляет еще меньше гарантий по сравнению с судебным процессом, отказ в предоставлении иммунитета на основании такого решения является нарушением международного права. Более того, ни в одном из случаев введения санкций против государственных органов или должностных лиц третьих стран не приводились факты нарушения международных обязательств соответствующим государством.

Показательной также является формулировка документов о введении санкций в рассматриваемых ситуациях. Так, статья 1(6) регламента ЕС 2019/796 закрепляет возможность вводить санкции, *«где это необходимо для достижения совместной внешней политики и политики безопасности»* [22, p. 4], что не соответствует требованиям статьи 49 ПСОГ [26, p. 129—131]. Провозглашение же возможности введения санкций *«в ответ на кибератаки, которые оказывают существенное воздействие на третьи страны и международные организации»*, если это представляется необходимым для достижения целей союза, не соответствует целям контрмер, субъекту, который уполномочен предпринимать действия в порядке контрмер (непосредственно затронутое государство либо любое государство в случае нарушения обязательств *erga omnes*), основанию применения контрмер (причинение значительного ущерба, а не нарушение международного обязательства, как предусмотрено ПСОГ) [26, p. 129—131].

В доктрине отмечается, что соответствующий регламент ЕС должен *«обеспечить ЕС финансовыми рычагами для того, чтобы наказывать за кибератаки напрямую, более жестко и эффективно»* [1, p. 317], введение санкций мешает развитию добрососедских отношений между государствами. Однако вводящие санкции государства предпочитают использовать данный подход, поскольку привлечение к уголовной ответственности с соблюдением бремени доказательства и требований должного процесса в отношении кибератак на практике весьма сложно [1, p. 320].

Как отмечалось выше, США вводят односторонние санкции за действия в информационном пространстве, которые в отдельных случаях даже не могут быть квалифицированы в качестве преступных, а доказательства их атрибутивности конкретному государству отсутствуют. Примечательно также, что в подавляющем большинстве случаев санкции представляются в качестве мер, направленных против государств (например, Акт о снижении влияния России в Европе и Евразии, Акт о противодействии противникам Америки посредством санкций) [37, p. 5], несмотря на то, что они применяются к конкретным физическим и юридическим лицам. На практике это создает дополнительные репутационные риски для государств и влечет овер-комплаенс (применение ограничений государствами и частными субъектами, даже если они прямо не предусматриваются санкционными режимами).

В этой связи весьма актуальной остается проблема атрибутивности деяния государству, что согласно решению Международного суда ООН по делу о военной и квазивоенной деятельности против Никарагуа 1986 г. [12, p. 62—65] и решению Международного уголовного трибунала по делу Тадича [42] требует всеобъемлющего контроля. Тот же подход отражен в таллинском руководстве 2.0, где указано, что для атрибутивности деяний в информационном пространстве физическое либо юридическое лицо должно действовать под прямым руководством либо контролем государства [59, p. 94—96], что не позволяет рассматривать действия физических и юридических лиц, в отношении которых введены односторонние санкции, в качестве деяний государства. Как следствие, полагаем, что исключения согласно праву международной ответственности в данной ситуации неприменимы. Контрмеры не могут применяться и к физическим и юридическим лицам, обвиняемым в совершении киберпреступлений (таллинское руководство 2.0, правила 20—21) [59, p. 111—122].

Показательным в этой связи является введение США санкций в отношении шести граждан Нигерии за *«хищение более чем 6 млн дол. США путем мошенничества с использованием информационных технологий»* [62]. Изданный американским Управлением по контролю за иностранными активами (*OFAC)* пресс-релиз содержит информацию об инкриминируемых деяниях и их схемах, фотографии и личные данные лиц, их совершивших, что и служит основанием для введения в отношении них санкций [64].

Полагаем, однако, что сама возможность введения санкций в рамках борьбы с киберпреступностью является весьма спорной. СБ ООН требует от государств предпринимать действия по ее предотвращению и пресечению посредством традиционных механизмов международно-правового сотрудничества (заключение договоров, оказание правовой помощи, обмен опытом, реализация рекомендаций Межправительственной комиссии по финансовому мониторингу), равно как и путем привлечения ответственных в их совершении лиц к уголовной ответственности [24; 44].

При наличии финансового ущерба американским гражданам США обязаны были возбудить уголовное преследование в отношении подозреваемых лиц, провести расследование в соответствии с требованиями уголовного процесса, запросить о помощи полицию в целях сбора доказательств и привлечения виновных лиц к ответственности.

Полагаем также, что введение односторонних санкций со ссылкой на совершение преступлений против государства, граждан государства либо его юридических лиц с использованием ИТ путем принятия решений органами исполнительной, а не судебной власти существенным образом затрагивает право на должный процесс и доступ к правосудию. По данным, получаемым из конфиденциальных источников, решения принимаются на основании закрытых секретных данных и не разглашаются. В результате лицо теряет возможность защиты своих прав в суде, а при введении против него санкций его имущественные права, свобода передвижения, право на защиту личной жизни, репутацию, экономические, трудовые и социальные права нарушаются без возможности обеспечения их эффективной защиты посредством обращения к судебным механизмам [25, p. 98—112].

Введение односторонних санкций в отношении подозреваемых лиц на основании решения исполнительного органа власти (*OFAC*) вместо возбуждения уголовного дела недопустимо, поскольку имеет крайне низкие стандарты доказывания, лишает лиц права на доступ к справедливому судебному разбирательству, нарушает презумпцию невиновности.

Необходимо отдельно остановиться на обеспечении презумпции невиновности согласно статье 14(2) Международного пакта о гражданских и политических правах 1966 г. [31] (далее — МПГПП) при введении односторонних санкций со ссылкой на злонамеренную деятельность в информационном пространстве. Комитет по правам человека (далее — КПЧ) в пункте 30 замечания общего порядка № 32 закрепляет, что *«вина не может презюмироваться, пока вина обвиняемого не доказана, с тем, чтобы дать ему возможность воспользоваться выгодами разумного сомнения»*, и требует от государств воздерживаться от публичных заявлений о вине обвиняемого до вступления в законную силу решения суда [3]. Ни одно из указанных требований в случае введения санкций за совершение киберпреступлений не соблюдается.

Более того, даже возможность обжалования внесения в санкционные списки США весьма ограничена, длительна (до 5 лет), ресурсо- и финансово затратна. Договор о функционировании ЕС предусматривает возможность обжалования введения санкций в Суд ЕС (ст. 275 [13]), однако последний обычно фокусируется на оценке обеспечения минимальных процессуальных гарантий, избегая затрагивать вопрос о праве собственности как подлежащий ограничению при определенных условиях [9, p. 938], равно как и вопросы презумпции невиновности и репутационных рисков. До настоящего момента заявлений о пересмотре санкций, введенных со ссылкой на злонамеренность действий в информационном пространстве, не отмечалось.

Таким образом, введение односторонних санкций государствами со ссылкой на совершение лицами преступлений с использованием ИТ без возбуждения уголовного дела нарушает право на справедливое судебное разбирательство, презумпцию невиновности и пр.

Не менее сложным является вопрос о возможности введения запрета на вещание СМИ, в том числе в Интернет-пространстве. Полагаем, что в данном случае любые ограничения также могут вводиться только с соблюдением международно-правовых стандартов. Совет ООН по правам человека подчеркивает важность свободного, справедливого, сбалансированного доступа к информации (резолюция 33/3 от 29 сентября 2016 г. [41, para. 6*j*]) для обеспечения права на развитие. Возможные ограничения предусмотрены в ряде международных договоров, включая пункт 3 статьи 19, статью 20 МПГПП [31]. В частности, запрещаются:

— пропаганда войны;

— выступления в пользу национальной, расовой или религиозной ненависти, представляющие собой подстрекательство к дискриминации, вражде или насилию (ст. 20 МПГПП [31]);

— приказы не оставлять никого в живых (ст. 40 Дополнительного протокола I [43]);

— прямое и публичное побуждение к совершению актов геноцида (ст. 3 Конвенции о предупреждении преступления геноцида и наказании за него 1948 г. [17]);

— распространение детской порнографии (ст. 9 Конвенции о киберпреступности [16]);

— распространение расистских и ксенофобских материалов посредством онлайн-средств, угрозы и оскорбления (стст. 3—5 Протокола к Конвенции о киберпреступности 2003 г. [2]);

— отрицание, чрезвычайная минимизация, одобрение или оправдание геноцида или преступлений против человечества (ст. 6 Протокола к Конвенции о киберпреступности 2003 г. [2]);

— призывы к свержению правительства, вовлечение в террористическую деятельность (пп. 24—29 доклада Специального докладчика по свободе выражения мнений [46]).

Согласно статье 19(3) МПГПП возможно также введение ограничений *«для уважения прав и репутации других лиц, охраны государственной безопасности, общественного порядка, здоровья или нравственности населения»*. Аналогичный подход отражен в Уставе Международного телекоммуникационного союза (ст. 34) [15]. При этом любые ограничения могут вводиться исключительно на основании закона согласно замечанию общего порядка № 34 [4] при должном уважении свободы выражения мнений в качестве приоритета (пп. 24—30, 46 доклада Генеральной Ассамблеи ООН 66/290 [47]).

Специальный докладчик ООН по свободе выражения мнений неоднократно настаивал на том, что бремя доказывания обоснованности введения ограничений, включая соответствие международным договорам, обоснованность, необходимость и пропорциональность, лежит на государстве (пп. 32—35 резолюции Совета ООН по правам человека 29/32 [45]; пп. 41, 45 доклада 67/357 [46]). При этом ограничения должны толковаться максимально узко, для того чтобы избежать злоупотребления со стороны государства (п. 45 доклада 67/357 [46]).

Документы ЕС, уполномочивающие введение ограничений на вещание российских информационных источников *RT* и *Sputnik* в ЕС, содержат отсылку на нарушение безопасности и публичного порядка и приверженность свободе выражения мнения (п. 8 регламента 2022/350) и вводятся в законодательном порядке, что в целом соответствует требованиям статьи 19 МПГПП. Вместе с тем регламент не отображает ни одного из критериев, выработанных КПЧ в замечаниях общего порядка. Обоснование принятия регламента не было озвучено и каким-либо иным способом обосновано. Попытка канала *RT France* оспорить введение запрета на вещание и потребовать его снятия в качестве обеспечительных мер не была удовлетворена Судом общей компетенции ЕС в *«связи с недоказанностью наличия гуманитарного и социального вреда»*, обязанность доказывания которого лежит на канале *RT France* [38]. Фактически в данном случае Суд переложил бремя доказывания необходимости введения ограничений на свободу вещания с ЕС на медиакомпанию, что противоречит приведенным выше резолюциям органов ООН, а также требованию пункта 35 замечаний общего порядка № 34 [4].

В доктрине также поднимаются вопросы о соответствии санкций, вводимых со ссылкой на злонамеренные действия в киберсфере, с точки зрения двусторонних договоров, норм международного торгового и инвестиционного права [9], что требует отдельного подробного исследования.

На основании вышеизложенного представляется возможным сделать следующие выводы.

Совершенствование ИТ значительным образом повлияло на развитие общественных отношений и любых форм взаимодействия между государствами. К сожалению, создание правовых норм, особенно в области международного права, существенно отстает, и зачастую государства действуют, либо игнорируя существующие правовые нормы, либо толкуя их излишне широко. Значительные проблемы возникают в свете все более активного принятия национальных правовых актов и применения односторонних санкций со ссылкой на злонамеренную деятельность в информационном пространстве.

Устав ООН не препятствует СБ ООН принимать принудительные меры с использованием либо без использования вооруженных сил в случае угрозы миру, нарушения мира или актов агрессии, в том числе, если такие действия совершаются с использованием ИТ. В настоящее время, однако, Совет рассматривает данную проблему в разрезе противодействия терроризму и применяет целевые санкции к вовлеченным лицам за террористическую деятельность независимо от использования ими ИТ в любых формах.

Имплементация решений СБ ООН должна осуществляться в соответствии с нормами международного права. Расширенное толкование санкций СБ ООН, одностороннее принятие принудительных мер государствами, в том числе для обеспечения выполнения таких санкций, нарушает положения Устава ООН и недопустимо. Применение односторонних санкций государствами для имплементации санкций СБ ООН возможно только в случае принятия последним дополнительной резолюции, непосредственно уполномочивающей на совершение таких действий.

При введении санкций в отношении государственных органов и должностных лиц в полном объеме должен соблюдаться принцип суверенного равенства, юрисдикционных иммунитетов государств и их собственности. Не допускается отступление от международно-правовых норм и стандартов в области прав человека со ссылкой на административный, а не судебный либо законодательный порядок принятия решений.

Уголовная ответственность за противоправную деятельность, осуществляемую с использованием ИТ, не должна подменяться применением государствами односторонних санкций. Применение целевых санкций в таких случаях нарушает экономические права, право на собственность, свободу передвижения, презумпцию невиновности, гарантии должного процесса и право на защиту репутации. Недоступность возможности обжалования, помимо репутационных рисков, влечет невозможность защиты нарушенных прав и доступа к правосудию.

Любые односторонние меры в отношении деятельности СМИ, социальных сетей и платформ могут иметь место только в том случае, если они не нарушают международных обязательств государств, в том числе в отношении свободы прессы, доступа к информации и выражения мнения. Любые ограничения могут вводиться исключительно в строгом соответствии со статьями 19—20 МПГПП, иными нормами международного права, вступившими в силу для государства для запрета пропаганды войны, геноцида, выступлений в пользу национальной, расовой или религиозной ненависти, представляющих собой подстрекательство к дискриминации, вражде или насилию, предотвращения распространения детской порнографии, уважения прав и репутации других лиц, охраны государственной безопасности, общественного порядка, здоровья или нравственности населения и пр. при соблюдении критериев добросовестности, обоснованности, необходимости и пропорциональности. Бремя доказывания обоснованности соответствующих ограничений лежит на государстве.

Список использованных источников

1. Abusedra, A. Use of Cyber Means to Enforce Unilateral Coercive Measures in International Law / A. Abusedra, M. A. Bakar, I. Md. Toriqul // Unilateral Sanctions in International Law / ed. by S. P. Subedi. — Oxford: Hart, 2021. — P. 301—326. (http://dx.doi.org/10.5040/9781509948413.ch-012)
2. Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems: Strasbourg, 28 Jan. 2003 [Electronic resource] // Council of Europe. — Mode of access: <https://rm.coe.int/16800816of>. — Date of access: 20.04.2022.
3. Article 14: Right to equality before courts and tribunals and to a fair trial: general comment N 32: UN Doc. CCPR/C/GC/32 [Electronic resource] // UN Treaty Body Database. — Mode of access: <https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fGC%2f32&Lang=en>. — Date of access: 24.04.2022.
4. Article 19: Freedom of opinion and expression: general comment N 34: UN Doc. CCPR/C/GC/34 [Electronic resource] // Office of the High Commissioner United Nations for Human Rights. — Mode of access: <http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>. — Date of access: 24.04.2022.
5. Autonomous Sanctions Amendment (Magnitsky-style and Other Thematic Sanctions) Act 2021 [Electronic resource] // legislation.gov.uk. — Mode of access: <https://www.legislation.gov.au/Details/C2021A00128>. — Date of access: 24.04.2022.
6. Bartlett, J. Sanctions by the Numbers: Spotlight on Cyber Sanctions / J. Bartlett, M. Ophel [Electronic resource] // Center for a New American Security. — 04.05.2021. — Mode of access: <https://www.cnas.org/publications/reports/sanctions-by-the-numbers-cyber>. — Date of access: 24.04.2022.
7. Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities: Executive Order 13694 of 1 Apr. 2015 [Electronic resource] // Discover U.S. Government Information. — Mode of access: <https://www.govinfo.gov/content/pkg/CFR-2016-title3-vol1/pdf/CFR-2016-title3-vol1-e013694.pdf>. — Date of access: 24.04.2022.
8. Blocking Property with Respect to Specified Harmful Foreign Activities of the Government of the Russian Federation: Executive Order 14024 of 15 Apr. 2021 [Electronic resource] // Federal Register. — Mode of access: <https://www.federalregister.gov/documents/2021/04/19/2021-08098/blocking-property-with-respect-to-specified-harmful-foreign-activities-of-the-government-of-the>. — Date of access: 24.04.2022.
9. Bogdanova, I. Unilateral Cyber Sanctions: Between Questioned Legality and Normative Value / I. Bogdanova, M. M. Callo-Müller // Vanderbild Journal of Transnational Law. — 2021. — Vol. 54, N 4. — P. 911—954. (https://doi.org/10.48350/161762)
10. Byers, M. Terrorism, the Use of Force and International Law after 11 September 2001 / M. Byers // International & Comparative Law Quarterly. — 2002. — Vol. 51, N 2. — P. 401—414. (https://doi.org/10.1093/iclq/51.2.401)
11. Callo-Müller, M. V. Unilateral Cyber Sanctions and Global Cybersecurity Law-Making / M. V. Callo-Müller, I. Bogdanova [Electronic resource] // OpinioJuris. — 24.01.2022. — Mode of access: <http://opiniojuris.org/2022/01/24/unilateral-cyber-sanctions-and-global-cybersecurity-law-making/>. — Date of access: 24.04.2022.
12. Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States Of America): judgment of 27 June 1986 [Electronic resource] // International Court of Justice. — Mode of access: <https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf>. — Date of access: 16.12.2021.
13. Chainoglou, K. Psychological warfare / K. Chainoglou [Electronic resource] // Oxford Public International Law. — August 2016. — Mode of access: <https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e385>. — Date of access: 13.02.2022.
14. Consolidated Version of the Treaty on the Functioning of the European Union // Official Journal of the European Union. — 2012. — Vol. 55, C 326. — P. 47—390.
15. Constitution of the International Telecommunication Union: entered into force 1 July 1994 [Electronic resource] // International Telecommunication Union. — Mode of access: <https://www.itu.int/en/council/Documents/basic-texts/Constitution-E.pdf>. — Date of access: 24.04.2022.
16. Convention on Cybercrime: Budapest, 23 Nov. 2001 [Electronic resource] // Council of Europe. — Mode of access: <https://rm.coe.int/1680081561>. — Date of access: 20.04.2022.
17. Convention on the Prevention and Punishment of the Crime of Genocide [Electronic resource] // United Nations. — Mode of access: <https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.1_Convention%20on%20the%20Prevention%20and%20Punishment%20of%20the%20Crime%20of%20Genocide.pdf>. — Date of access: 24.04.2022.
18. Council Decision (CFSP) 2022/351 of 1 March 2022 amending Decision 2014/512/CFSP concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine // Official Journal of the European Union. — 2022. — Vol. 65, L 65. — P. 5—7.
19. Council Implementing Regulation (EU) 2020/1125 of 30 July 2020 implementing Regulation 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States // Ibid. — 2020. — Vol. 63, L246. — P. 4—9.
20. Council Implementing Regulation (EU) 2020/1536 of 22 October 2020 of implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States // Ibid. — Vol. 63, L351I. — P. 1—4.
21. Council Regulation (EU) 2022/350 of 1 March 2022, amending Regulation (EU) N 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine // Ibid. — 2022. — Vol. 65, L 65. — P. 1—4.
22. Council Regulation 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States // Ibid. — 2020. — Vol. 62, L 129I. — P. 4—9.

23. Countering America's Adversaries Through Sanctions Act, 2 August 2017 [Electronic resource] // congress.gov. — Mode of access: <https://www.congress.gov/115/plaws/publ44/PLAW-115publ44.htm>. — Date of access: 24.04.2022.
24. Countering the Use of the Internet for Terrorist Purposes: decision N 7/06: Doc. MC.DEC/7/06, 5 Dec. 2006 [Electronic resource] // Organization for Security and Co-operation in Europe. — Mode of access: <https://www.osce.org/files/f/documents/d/3/23078.pdf>. — Date of access: 24.04.2022.
25. Douhan, A. F. Regional Mechanisms of Collective Security: The New Face of Chapter VIII of the UN Charter? / A. F. Douhan. — Paris: L. Harmattan, 2013. — 244 p.
26. Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries // Yearbook of the International Law Commission. — 2001. — Vol. II, Part Two [Electronic resource] // Office of Legal Affair of the United Nations. — Mode of access: <https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf>. — Date of access: 24.04.2022.
27. Geyrhalter, D. Friedenssicherung durch Regionalorganisationen ohne Beschluß des Sicherheitsrates / D. Geyrhalter. — Cologne: LIT, 2001. — 239 s.
28. Gowlland-Debbas, V. The Limits of Unilateral Enforcement of Community Objectives in the Framework of UN Peace Maintenance / V. Gowlland-Debbas // European Journal of International Law. — 2000. — Vol. 11, N 2. — P. 361—383. (https://doi.org/10.1093/ejil/11.2.361)
29. Hofmann, R. International Law and the Use of Military Force against Iraq / R. Hofmann // German Yearbook of International Law. — 2002. — Vol. 45. — P. 9—34.
30. Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election: Executive Order 13848 of 12 Sept. 2018 [Electronic resource] // Federal Register. — Mode of access: <https://www.federalregister.gov/documents/2018/09/14/2018-20203/imposing-certain-sanctions-in-the-event-of-foreign-interference-in-a-united-states-election>. — Date of access: 24.04.2022.
31. International Covenant on Civil and Political Rights [Electronic resource] // Refworld. — Mode of access: <https://www.refworld.org/docid/3ae6b3aa0.html>. — Date of access: 28.04.2022.
32. Kern, A. Economic sanctions: Law and Public Policy / A. Kern. — New York: Palgrave Macmillan, 2009. — 359 p.
33. Körbs, H. Die Friedensdicherungduech die Vereinten Nationen und Regionalorganizationen / H. Körbs. — Bochum: Brockmeyer, 1997. — 595 p.
34. Malanczuk, P. Humanitarian Intervention and the Legitimacy of the Use of Force / P. Malanczuk. — Amsterdam: Spinhuis, 1993. — 69 p.
35. McWhinney, E. International Law-based Responses to the September 11 International Terrorist Attacks / E. McWhinney // Chinese Journal of International Law. — 2002. — Vol. 1, N 1. — P. 280—286. (https://doi.org/10.1093/oxfordjournals.cjilaw.a000421)
36. Müllerson, R. Jus ad Bellum and International Terrorism / R. Müllerson // International Law and the War on Terror / ed. F. L. Borch and P. S. Wilson. — Naval War College, 2003. — P. 75—127.
37. North Korea Sanctions Program: updated on 2 Nov. 2016 [Electronic resource] // U.S. Department of the Treasury. — Mode of access: <https://home.treasury.gov/system/files/126/nkorea.pdf>. — Date of access: 24.04.2022.
38. Opération militaire en Ukraine: le président du Tribunal rejette la demande de RT France visant à suspendre les sanctions adoptées par le Conseil Tribunal de l'Union européenne: communique de presse N 54/22, Luxembourg, le 30 mars 2022 [Electronic resource] // Court of Justice of the European Union. — Mode of access: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-03/cp220054fr.pdf>. — Date of access: 24.04.2022.
39. Orakhelashvili, A. The Impact of Peremptory Norms / A. Orakhelashvili // European Journal of International Law. — 2005. — Vol. 16, N 1. — P. 59—88. (https://doi.org/10.1093/ejil/chi103)
40. PRK Cyber Threat Advisory 'Guidance on the North Korean Cyber Threat', 15 Apr. 2020 [Electronic resource] // U.S. Department of the Treasury. — Mode of access: <https://home.treasury.gov/system/files/126/dprk_cyber_threat_advisory_20200415.pdf>. — Date of access: 24.04.2022.
41. Promotion of a democratic and equitable international order: UN Doc. A/HRC/RES/33/3 [Electronic resource] // Official Documents System of the United Nations. — Mode of access: <https://undocs.org/en/A/HRC/RES/33/3>. — Date of access: 24.04.2022.
42. Prosecutor v. Tadic: appeal judgment of 27 Febr. 2001 [Electronic resource] // International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia since 1991. — Mode of access: <https://www.icty.org/x/cases/tadic/acjug/en/vuj-aj010227e.pdf>. — Date of access: 16.12.2021.
43. Protocol Additional to the Geneva Conventions of 12 Aug. 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) [Electronic resource] // International Humanitarian Law Databases. — Mode of access: <https://ihl-databases.icrc.org/en/ihl-treaties/api-1977>. — Date of access: 24.04.2022.
44. Regional Workshop on Countering the Use of the Internet for Terrorist Purposes for Judges, Prosecutors and Investigators from South Eastern Europe, 16—17 Nov. 2016, Skopje: Doc. CIO.GAL/224/16, 8 Feb. 2017 [Electronic resource] // Organization for Security and Co-operation in Europe. — Mode of access: <https://www.osce.org/files/f/documents/7/e/299091.pdf>. — Date of access: 24.04.2022.
45. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye: UN Doc. A/HRC/29/32 [Electronic resource] // Official Documents System of the United Nations. — Mode of access: <https://undocs.org/en/A/HRC/29/32>. — Date of access: 24.04.2022.
46. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression: UN Doc. A/67/357 [Electronic resource] // Official Documents System of the United Nations. — Mode of access: <https://undocs.org/en/A/67/357>. — Date of access: 24.04.2022.
47. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression: UN Doc. A/66/290 [Electronic resource] // Official Documents System of the United Nations. — Mode of access: <https://undocs.org/en/A/66/290>. — Date of access: 24.04.2022.
48. Resolution 1874 (2009) adopted by the Security Council at its 7426th meeting, on 14 April 2015: UN Doc. S/RES/2216(2015) [Electronic resource] // Official Documents System of the United Nations. — Mode of access: <https://undocs.org/en/S/RES/2216(2015)>. — Date of access: 24.04.2022.
49. Resolution 2501 (2019) adopted by the Security Council at its 8686th meeting, on 16 December 2019: UN Doc.S/RES/2501(2019) [Electronic resource] // Official Documents System of the United Nations. — Mode of access: <https://undocs.org/en/S/RES/2501(2019)>. — Date of access: 24.04.2022.
50. Resolution 2535 (2020) adopted by the Security Council at its 8748th meeting, on 14 July 2020: UN Doc. S/RES/2535(2020) [Electronic resource] // Official Documents System of the United Nations. — Mode of access: <https://undocs.org/en/S/RES/2535(2020)>. — Date of access: 24.04.2022.
51. Resolution 2482 (2019) adopted by the Security Council at its 8582nd meeting, on 19 July 2019: UN Doc. S/RES/2482(2019) [Electronic resource] // Official Documents System of the United Nations. — Mode of access: <https://undocs.org/en/S/RES/2482(2019)>. — Date of access: 24.04.2022.

52. Resolution 2419 (2018) adopted by the Security Council at its 8277th meeting, on 6 June 2018, UN Doc. S/RES/2419 (2018) [Electronic resource] // Official Documents System of the United Nations. — Mode of access: <https://undocs.org/en/S/RES/2419(2018)>. — Date of access: 24.04.2022.
53. Resolution 2490 (2019) adopted by the Security Council at its 8624th meeting, on 20 September 2019: UN Doc. S/RES/2490(2019) [Electronic resource] // Official Documents System of the United Nations. — Mode of access: <https://undocs.org/en/S/RES/2490(2019)>. — Date of access: 24.04.2022.
54. Resolution 2462 (2019) adopted by the Security Council at its 8496th meeting, on 28 March 2019: UN Doc. S/RES/2462 (2019) [Electronic resource] // Official Documents System of the United Nations. — Mode of access: <https://undocs.org/en/S/RES/2462(2019)>. — Date of access: 24.04.2022.
55. Resolution 2140 (2014) Adopted by the Security Council at its 7119th meeting, on 26 February 2014: UN Doc. S/RES/2140(2014) [Electronic resource] // Official Documents System of the United Nations. — Mode of access: <https://undocs.org/en/S/RES/2140(2014)>. — Date of access: 24.04.2022.
56. Resolution 2216 (2015) adopted by the Security Council at its 7426th meeting, on 14 April 2015: UN Doc. S/RES/2216(2015) [Electronic resource] // Official Documents System of the United Nations. — Mode of access: <https://undocs.org/en/S/RES/2216(2015)>. — Date of access: 24.04.2022.
57. Schaller, Ch. Massenvernichtungswaffen und Präventivkrieg Möglichkeiten der Rechtvertiefungeiner Militörishcen Intervention im Irak aus Völkerrechtlicher Sicht / Ch. Schaller // Zeitschrift für Ausländisches Öffentliches Recht und Völkerrecht. — 2002. — Vol. 62, N 3. — P. 641—668.
58. Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities: Executive Order 13757 of 28 Dec. 2016 [Electronic resource] // U.S. Department of the Treasury. — Mode of access: <https://home.treasury.gov/system/files/126/cyber2_eo.pdf>. — Date of access: 24.04.2022.
59. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / ed. M. N. Schmitt. — Cambridge: Cambridge University Press, 2017. — 598 p.
60. The Countering Russian Influence in Europe and Eurasia Act of 2017, as amended (CRIEEA; P.L. 115-44, Title II, § 224; 22 U.S.C. 9524(d)) [Electronic resource] // Office of the Law Revision Counsel. United States Code. — Mode of access: <https://uscode.house.gov/view.xhtml?path=/prelim@title22/chapter102&edition=prelim>. — Date of access: 24.04.2022.
61. The Cyber (Sanctions) (EU Exit) Regulations 2020/597 of 17 May 2020 [Electronic resource] // legislation.gov.uk. — Mode of access: <https://www.legislation.gov.uk/uksi/2020/597/made>. — Date of access: 24.04.2022.
62. The Protection of Human Rights and the Principle of Non-Intervention in Internal Affairs of States: session in Santiago de Compostela — 1989 [Electronic resource] // Institut de Droit International. — Mode of access: <https://www.idi-iil.org/app/uploads/2017/06/1989_comp_03_en.pdf>. — Date of access: 24.04.2022.
63. Treasury Sanctions Nigerian Cyber Actors for Targeting U.S. Businesses and Individuals: Press Release, 16 June 2020 [Electronic resource] // U.S. Department of the Treasury. — Mode of access: <https://home.treasury.gov/news/press-releases/sm1034>. — Date of access: 24.04.2022.
64. Treasury Sanctions Russian Cyber Actors for Virtual Currency Theft: Press Release, 16 Sept. 2020 [Electronic resource] // U.S. Department of the Treasury. — Mode of access: <https://home.treasury.gov/news/press-releases/sm1123>. — Date of access: 24.04.2022.
65. Tzanakopoulos, A. State Responsibility for Targeted Sanctions / A. Tzanakopoulos // American Journal of International Law. — 2019. — Vol. 113. — P. 135—139. (https://doi.org/10.1017/aju.2019.22)
66. Unilateral economic measures as a means of political and economic coercion against developing countries: UN Doc. A/RES/52/181 [Electronic resource] // Official Documents System of the United Nations. — Mode of access: <https://undocs.org/en/A/RES/52/181>. — Date of access: 24.04.2022.
67. US sanctions on Russia: updated on 18 Jan. 2022 [Electronic resource] // Federation of American Scientists. — Mode of access: <https://sgp.fas.org/crs/row/R45415.pdf>. — Date of access: 24.04.2022.

Статья поступила в редакцию 6 мая 2022 г.