Журнал международного права и международных отношений. 2022. № 1-2 (100-101). С. 9—18.
Journal of International Law and International Relations. 2022. N 1-2 (100-101). P. 9—18.
УДК 327 DOI: 10.33581/2072-0513-2022-1-2-9-18

ТЕОРИЯ И ПРАКТИКА ВВЕДЕНИЯ САНКЦИЙ ЗА ЗЛОНАМЕРЕННУЮ ДЕЯТЕЛЬНОСТЬ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Елена Довгань

В статье подробно рассматривается практика введения санкций Советом Безопасности ООН и государствами либо региональными организациями в одностороннем порядке со ссылкой на злонамеренность действий в информационном пространстве. Раскрывается понятие санкций в международном праве, выявляются конкретные случаи, когда действия государств либо частных лиц рассматривались в качестве основания введения односторонних санкций, дается обзор соответствующего законодательства США, Европейского союза, Великобритании, Австралии, определяются современные тенденции и применимые сферы международно-правового регулирования. Сделанные в заключении выводы отражают современные проблемы использования санкций, как международных, так и односторонних, в контексте деятельности в киберпространстве.

Ключевые слова: злонамеренные действия в информационном пространстве; информационная безопасность; киберпреступность; киберсанкции; односторонние санкции; санкции.

«Malicious Activity in Cyberarea as a Ground for Introduction of Sanctions: Theory and Practice» (Alena Douhan)

Current article provides an overview of the practice of application of sanctions both of the UN Security Council and by states and regional organisations unilaterally with reference to malicious activity in cyberspace. Article idefines the notion of 'sanctions' in international law, refers to specific cases of malicious activity, practice of the use of sanctions by the UN Security Council and by states and regional organisations unilaterally, follows recent developments of legislation of the United States of America, European Union, United Kingdom and Australia; identifies contemporary tendencies and applicable areas of international law. The author identifies on the conclusion contemporary problems of the use of international and cybersanctions in cyberarea.

Keywords: cybercrimes; cybersanctions; cybersecurity; malicious activity in cyberarea; sanctions; unilateral sanctions.

Современные информационные технологии (далее — ИТ) кардинальным образом изменили мир. В настоящее время практически каждая сфера отношений затрагивается развитием ИТ как на международном, так и на национальном уровнях. Совет Безопасности ООН (далее — СБ ООН) в своих резолюциях 2419 (2018) [62], 2490 (2019) [63], 2462 (2019) [64] и в ряде иных прямо признает, что деятельность физических лиц и организаций в информационной сфере может создавать угрозу международному миру и безопасности.

Как следствие, последние годы все более актуальным стало обсуждение возможности введения санкций в ответ на некие злонамеренные действия государств, физических и юридических лиц. Так, в 2020 г. восемь физических лиц и четыре организации из России, Китая и Северной Кореи были включены в санкционные списки Европейского союза как «обеспечивающие поддержку, вовлеченные или способствовавшие кибератакам публично известным как *"WannaCry", "NotPetya"* и *"Operation Cloud Hopper"»* [21, p. 4].

Принятие санкций в таких ситуациях может являться весьма спорным с точки зрения международного права. При этом, в отличие от общих аспектов обеспечения информационной безопасности [17; 45], использования ИТ в качестве средств и методов ведения войны [70, p. 85; 73, p. 287—288; 87], их влияния на свободу личной и семейной жизни и свободу выражения мнения [57; 58], формирующегося права быть забытым [44, p. 75; 90], оценку нарушений прав человека при отключении государствами доступа к сети Интернет на своей территории [76], работы, посвященные оценке влияния ИТ на применение санкций [3; 12], носят единичный характер и весьма фрагментарны. В связи с этим актуальность обзора

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 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

практики применения санкций со ссылкой на злонамеренность использования ИТ не подлежит сомнению.

Проблема применения санкций в современном международном права сама по себе является весьма сложной. До настоящего времени отсутствует единое понимание термина «санкции» в международном праве. Используется множество иных терминов, например «ограничительные меры», «меры безопасности», «контрсанкции», вторичные санкции и др. В комментариях к Проекту статей об ответственности государств за международные противоправные деяния 2001 г. признавалось, что понятие санкций является одним из наиболее спорных в современном международном праве [31, p. 31, 128]. Они настолько часто упоминаются в международном и национальном контексте и включают столь широкое число видов, форм и методов, используемых различными субъектами, что на слух часто принимаются как должное без их правовой либо гуманитарной оценки.

Полагаем, что термин «санкции» не может быть сам по себе определен в качестве правомерной либо неправомерной деятельности. Так, Устав ООН непосредственно уполномочивает СБ ООН принимать решение о применении невоенных либо военных мер в ситуациях угрозы миру, нарушения мира либо акта агрессии (ст.ст. 41, 42) и требует от государств исполнения принятых Советом решений (ст. 25) [1]. Вместе с тем статус односторонних санкций не настолько однозначен в международном праве. В связи с этим и особенно с учетом вовлечения ИТ в использование односторонних санкций необходима оценка каждого конкретного вида деяний для определения их правомерности либо неправомерности.

Считаем, однако, необоснованным использование предлагаемого М. В. Калло-Мюллер и И. Богдановой понятия «киберсанкции» как *«санкции, уполномочивающие внесение в списки иностранных граждан, юридических лиц и правительственных учреждений третьих стран за различные виды злонамеренной деятельности в информационном пространстве, включая кибератаки»* [13]. Традиционно характеристика санкций определяется исходя из используемого инструментария (экономические, финансовые, военные) либо объекта (секторальные, целевые). Полагаем также необоснованной ссылку на наличие права введения таких санкций, которое в международном праве отсутствует. Как следствие, в настоящей статье рассматривается практика применения санкций в ответ на некое злонамеренное действие в информационном пространстве.

В связи с отсутствием единого определения в настоящей статье под термином «санкции» понимаются меры давления, принимаемые любыми акторами, без абсолютной оценки их правомерности либо неправомерности. Они включают как санкции СБ ООН, принимаемые им в ситуациях угрозы миру, нарушения мира или акта агрессии, согласно главе VII Устава ООН, так и односторонние меры давления без предварительного решения вопроса о их правомерности либо неправомерности [1].

Неправомерное использование ИТ как основание введения односторонних санкций активно обсуждается в правовой доктрине и на практике. Генеральной Ассамблеей ООН в резолюции 68/167 признается, что *«к деятельности с использованием информационных технологий должны применяться те же нормы, что и оффлайн»* [78, para. 3]. В ряде иных резолюций СБ ООН и Генеральной Ассамблеи [34, para. 7—8; 62, преамбула, para. 5; 64, преамбула, para. 19, 21; см. также: 79, p. 3—11, 32—34] отмечается, что злонамеренное использование информации и коммуникативных технологий, в том числе частными лицами, может представлять собой угрозу международному миру и безопасности. Аналогичный подход отражен в отчете 70/174 Группы экспертов по развитию в сфере информации, телекоммуникаций в контексте информационной безопасности [43, para. 3].

По состоянию на апрель 2022 г., СБ ООН ни разу не принимал решений по введению санкций в ответ на злонамеренное распространение информации либо применение ИТ, делая упор на 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) [64, para. 19]), данных по пассажирам на авиасообщениях (резолюция 2482 (2019) [61, para. 15 (c)]), расследования террористических преступлений. Организация по безопасности и сотрудничеству в Европе при оценке международных обязательств государств в части противодействия использованию сети Интернет для террористических целей также делает упор на проведении расследования и привлечении лиц к ответственности с полным соблюдением процессуальных гарантий и принципов должного процесса [25; 55].

СБ ООН также указывает на необходимость предотвращения использования сети Интернет для вовлечения в террористическую деятельность и радикализацию общества [18, p. 77; 54], рассматривает возможность квалификации отдельных видов террористической деятельности в качестве военных преступлений, преступлений против человечности, геноцида (резолюция 2490 (2019) [63, para. 2]).

Традиционно признается, что при определенных условиях использование ИТ может быть квалифицировано *в качестве вооруженного нападения* [7, para. 253—256] либо *представлять собой метод ведения военно-*

го противостояния в рамках вооруженного конфликта немеждународного характера [6, para. 436—437]. Для квалификации в качестве вооруженного нападения использование ИТ должно соответствовать следующим характеристикам: осуществление государством против государства; создание угрозы существованию государства [29, p. 175—176; 40, p. 114—115; 87]; причинение смерти либо телесных повреждений значительному количеству людей, серьезное повреждение гражданского и военного имущества, включая объекты критической инфраструктуры [70, p. 106—107; 73, p. 287—288] и возможную утрату контроля над территорией/частью территории государства (п. 255 Комментария Комитета Красного Креста (МККК) к ст. 2 Женевской конвенции I) [см. также: 27, p. 26]; наличие причинно-следственной связи между применением ИТ и негативными последствиями; быстрота наступления последствий (секунды либо минуты между применением ИТ и наступлением последствий) [46, p. 63—73].

Еще одним видом злонамеренной деятельности в сети Интернет являются *атаки на критическую инфраструктуру*, к которой в доктрине относят атаки в отношении плотин, атомных электростанций, систем контроля вооружений, банковских счетов и операций, газо- и нефтепроводов, линий электропередачи, систем налогообложения, правительственных серверов и ИТ-систем [27, p. 12—17], иных видов критической инфраструктуры; перехват контроля над системами противовоздушной обороны [32, p. 18], системами контроля за дамбами, аэронавигацией либо поездами, которые могут привести к авариям [6, para. 437], и пр. Возможные ответы государства на атаки на объекты критической инфраструктуры зависят от того, кто осуществляет такую атаку, непосредственного объекта инфраструктуры и последствий атаки.

В том случае если такая атака осуществляется государством либо может быть ему атрибутирована, а последствия действий достигают уровня вооруженного нападения, государства имеют право действовать в порядке коллективной самообороны согласно статье 51 Устава ООН [1]. Атаки с использованием ИТ в отношении объектов критической инфраструктуры, которые могут быть квалифицированы в качестве сооружений, содержащих опасные силы в понимании статьи 56(1) Дополнительного протокола I к Женевским конвенциям 1977 г., касающегося защиты жертв международных вооруженных конфликтов (дамбы, атомные станции и пр.), должны быть расследованы как серьезные нарушения международного гуманитарного права согласно статье 85 Протокола, а лица, их совершившие, — привлечены к ответственности в соответствии со стандартами справедливого судебного разбирательства.

Недавним примером атак с использованием ИТ являются многократные атаки повстанцев-хуситов в Йемене морских и нефтедобывающих целей в Саудовской Аравии с использованием дронов и беспилотных морских судов, повлекшие значительное число человеческих жертв (по предварительным оценкам, за годы атак с обеих сторон погибли около 10 000 человек гражданского населения [88]), а также причинившие серьезный ущерб экономике и коммерческому мореплаванию (Отчет комиссии экспертов от 25 января 2021 г.) [38, para. 62—70]. Наибольшее внимание уделялось атаке, осуществленной с использованием 10 дронов в отношении нефтедобывающих установок в Саудовской Аравии 14 сентября 2019 г. [33], которая привела к снижению нефтедобычи в Саудовской Аравии практически на 60 % и повышению цены на нефть в мире на 15 % [42; 82]. Проведенное под эгидой ООН расследование позволило лишь установить, что дроны, по всей видимости, были идентичны производимым в Иране, но не определить, с территории какого государства и кем они были направлены (Отчет Генерального секретаря ООН *S*/2020/531 [47, para. 11—14; 67]). Атаки в отношении нефтедобывающих и нефтеперерабатывающих установок и нефтехранилищ в Саудовской Аравии продолжаются до настоящего времени.

Ситуация в Йемене неоднократно признавалась СБ ООН в качестве угрожающей международному миру и безопасности. В отношении ряда лиц и организаций, в том числе ответственных за организацию атак с использованием ИТ, приняты целевые санкции: заморожены счета и активы, введены запрет на поездки (резолюция 2140 (2014) [65, para. 11—19]) и эмбарго на поставку вооружений лицам, в отношении которых введены санкции, или организациям под их контролем (резолюция 2216 (2015) [66, para. 14—19]).

В ситуации, когда атаки на критическую инфраструктуру не достигают уровня вооруженного нападения либо квалификации в качестве угрозы международному миру и безопасности, государства могут предпринимать меры в соответствии с международным и национальным правом в отношении совершающих их лиц. На практике, как будет рассмотрено ниже, ряд государств вводят односторонние санкции со ссылкой на атаки на критическую инфраструктуру.

СБ ООН неоднократно указывал, что распространение информации также может носить злонамеренный характер, возбуждать ненависть, вспышки экстремизма, радикализацию населения и создавать угрозу поддержанию международного мира и безопасности (резолюция 2490 (2019) [14, para. 3; 63, para. 2]), содействовать распространению враждебной пропаганды в нарушение требований статей 19, 20 Международного пакта о граждан-

ских и политических правах 1966 г. (далее — МПГПП) [28]. Общий комментарий № 36 Комитета ООН по правам человека указывает, что распространение враждебной пропаганды, разжигание военных действий представляют собой прямое нарушение права на жизнь [5]. В решении Международного уголовного трибунала по Руанде (*Case* N *ICTR*-99-52-*A*) основатели телевизионной и радиокомпаний, а также главный редактор журнала *Kangura* были признаны виновными в «разжигании геноцида посредством опубликованных и распространяемых через радио и телевидение материалов» [74, para. 52], результатом чего явилось «полное либо частичное уничтожение этнической группы Тутси» [36, para. 157—201, 316—320], т. е. в совершении международных преступлений.

Именно поэтому в настоящий момент актуальными являются правовая оценка и решение о возможных ответных мерах в ситуациях использования социальных сетей и средств массовой информации для осуществления пропаганды, распространения не всегда верифицированной информации, призывов к насилию. Так, разрешение на размещение в *Facebook* материалов, призывающих к насилию в отношении российских граждан, президентов и должностных лиц [85] со ссылкой на необходимость сбросить стресс, вызываемый развитием ситуации в Украине [81], позднее суженное до заявлений с территории Украины [53], является прямым нарушением статей 19, 20 МПГПП, привело к всплеску русофобии в ряде стран и, как следствие, было осуждено на уровне Верховного комиссара ООН по правам человека и Генерального секретаря ООН [50; 52]. Вместе с тем вопрос о мерах реагирования в данной ситуации на уровне ООН не рассматривался.

В настоящее время *Meta* ссылается на введение ограничений со ссылкой на распространение фейковых новостей со стороны Российской Федерации и Республики Беларусь путем использования ложных аккаунтов в социальных сетях и деятельности группы хакеров *UNC*1151/*Ghostwriter* [41]. Действующая политика компании свидетельствует о направленности на предотвращение распространения политики Российской Федерации в отношении ситуации в Украине [49].

Актуальным также является вопрос о предотвращении доступа к средствам массовой информации, социальным сетям и платформам со ссылкой на размещение на них злонамеренной, неверифицированной либо фейковой информации, блокировке аккаунтов физических либо юридических лиц.

Рассмотрим практику государств в ответ на злонамеренные либо противоправные действия в сфере информационных технологий. Как отмечалось выше, практика СБ ООН в части введения санкций в ответ на злонамеренные действия в сфере ИТ достаточно ограничена, в отличие от практики государств, которая постоянно расширяется. Так, в частности, исполнительный приказ 13694 от 1 апреля 2015 г. (в ред. от 28 декабря 2016 г. [75]), в качестве оснований введения санкций США [11; 69, p. 113—115] рассматривал атаки на критическую инфраструктуру, вмешательство в избирательный процесс, нарушение функционирования компьютерных систем или операций, неправомерное использование финансовых средств и персональных данных и пр. Впоследствии данный перечень был дополнен следующими положениями: «существенные деструктивные вирусные атаки, предотвращение доступа к системам» (п. 224 Акта о противодействии противникам Америки посредством санкций (2017) [24]), меры, направленные на «подрыв доверия к выборам в США, скрытая пропаганда и дезинформация», распространяемая с использованием ИТ (исполнительный приказ 13848 от 12 сентября 2018 г. [48]), «предотвращение доступа, ухудшение качества, прерывание функционирования информационных технологий и систем, несанкционированный доступ, уничтожение, распространение данных, осуществление информационного влияния» (п. 224 Акта о противодействии противникам Америки посредством санкций (2017) [24]; исполнительный приказ 14024 от 15 апреля 2021 г. [10]).

По данным Управления США по контролю за иностранными активами, за вмешательство в выборы в США введены санкции против двух государственных органов Российской Федерации, 46 граждан и 13 компаний Российской Федерации и Украины [83, p. 14]. Указанные действия квалифицируются как составляющие угрозу национальной безопасности и заявляются в качестве основания введения односторонних санкций путем замораживания счетов и имущества [26].

В ответ на деяния, которые могут быть квалифицированы в качестве киберпреступлений (в частности, за кражу около 6 млн дол. США. у жертв, проживающих/находящихся на территории США, путем мошенничества с использованием ИТ), в санкционные списки были включены шесть граждан Нигерии [80]. Весьма известным является открытие уголовного дела в отношении основателя *Wikileaks* Дж. Ассанжа в связи с получением доступа к информации, представляющей государственные секреты США, путем использования ИТ и ее распространением [51].

Некоторые из санкций США в ответ на злонамеренную деятельность государств в информационной сфере вводятся со ссылкой на имплементацию резолюций СБ ООН 1718 (2006) и 2397 (2017). Например, в отношении КНДР в рамках борьбы с распространением оружия массового уничтожения делается упор на пре-

дотвращение попыток страны обойти санкции СБ ООН и США с помощью использования ИТ [15; 30]. Так, в руководстве по противодействию киберугрозам КНДР от 15 апреля 2020 г. США ссылается на ее деятельность по вмешательству в функционирование либо уничтожению критической инфраструктуры США, включающую киберпреступления, шпионаж, кражи, вымогательство либо отмывание денег с использованием ИТ, криптоджекинг. Указанные преступления подлежат уголовному преследованию, в том числе с назначением наказания в виде тюремного заключения на срок до 20 лет, штрафа в размере до 1 млн дол. США, ареста счетов всех, кто вовлекается в деятельность по обходу санкций США [30]. Фактически в данном случае речь идет о применении вторичных санкций к гражданам США и третьих стран, не вовлеченным в совершение преступлений, однако взаимодействующим с компаниями из КНДР. США также, используя программу *Rewards for Justice*, изначально созданную для борьбы с терроризмом, предлагает награду в размере 5 млн дол. за информацию, которая ведет к «разрушению финансовых механизмов лиц, вовлеченных в деятельность, поддерживающую КНДР, включая отмывание денег, обход санкций, совершение киберпреступлений» [68].

Группа экспертов, учрежденная СБ ООН на основе резолюции 1874 (2009) в целях разработки рекомендаций для СБ ООН, государств и Комитета по санкциям в части имплементации санкций СБ ООН по КНДР [59, para. 26; 60, para. 1]), неоднократно отмечала использование КНДР ИТ, включая операции с крипто-валютами для обхода экономических санкций (отчет Группы экспертов *S*/2019/691, пп. 57—71), и рекомендовала СБ ООН ввести дополнительные санкции для обеспечения контроля государств в сфере обращения криптовалют (отчет *S*/2020/151, рекомендации, прил. 73, пп. 26—28; отчет *S*/2019/691, выводы, пп. 8—11 [39; 56]). Финальный отчет 2021 г., помимо атак в финансовом секторе, также указывал на атаки *Lazarus Group* на оборонные объекты в Израиле, группы *Beagleboyz* на финансовые счета и активы банков ряда стран, а также рассылку неких злонамеренных ссылок членам экспертной группы (*S*/2021/211 [37, para. 126—129]) и рекомендовал, помимо внесения в санкционные списки дополнительных лиц, ряд мер по предотвращению обхода санкций СБ ООН при обеспечении применения гуманитарных изъятий и минимизации ущерба гражданскому населению (прил. 100 к отчету). Однако до настоящего времени дополнительные санкции СБ ООН не были приняты.

По данным Центра новой Американской безопасности, за период 2011 — май 2021 г. США были введены санкции со ссылкой на незаконную деятельность в сфере ИТ в отношении 303 физических и юридических лиц более чем из 10 государств. Стремительный скачок в отношении вводимых так называемых киберсанкций фиксируется с 2018 г. [9].

Санкции в ответ на злонамеренные действия с использованием ИТ с мая 2019 г. начали применяться также в практике ЕС и Великобритании путем введения запретов на выдачу виз, разрешений на въезд и заморозки счетов включенных в списки лиц (регламент ЕС 2019/796 [23, p. 1]). При этом угроза внешним интересам ЕС понимается весьма широко, включая те, которые «осуществляются против органов, институтов, агентств и должностных лиц ЕС, делегаций ЕС, в отношении третьих стран и международных организаций, совместной внешней политики и политики безопасности, миссий и специальных представителей ЕС» (пп. 5—6 регламента).

На основании указанного регламента в 2020 г. ЕС ввел санкции в отношении восьми лиц и четырех организаций из России, Китая и КНДР за «обеспечение поддержки или вовлеченность либо способствование атакам с использованием ИТ либо попыткам таких атак, подрывающих целостность Организации по запрещению химического оружия, а также атак, известных как *“WannaCry”, “NotPetya”, “Operation Cloud Hopper”*» (имплементирующий регламент Совета 2020/1125 [21, p. 4]) либо «вовлеченность в атаки с использованием ИТ со значительным эффектом, которые продолжают представлять внешнюю угрозу Союзу, государствам-членам, в частности атаки против Федерального парламента Германии, которая имела место в апреле—мае 2015 г.» (имплементирующий регламент 2020/1536 [20, p. 1]).

Великобритания в связи с выходом из ЕС приняла регламент о киберсанкциях в развитие Закона об отмывании денег [77], во многом дублировавшего регламент ЕС, на основании которого были введены в силу санкции в отношении тех же лиц, которые уже находились под санкциями ЕС [12, p. 933]. Примечательно, что согласно Разъяснительному меморандуму к данному регламенту оценка гуманитарного воздействия, равно как оценка соответствия принимаемого регламента международному праву, не проводилась [35].

Изменения, внесенные в декабре 2021 г. Австралией в Акт об автономных санкциях 2011 г., закрепили возможность введения односторонних санкций Австралией в ответ на «злонамеренную деятельность в киберпространстве» [34, para. 4]. До настоящего времени односторонние санкции в целях противодействия деятельности в сфере ИТ Австралией не вводились.

Необходимо отметить, что перечень злонамеренной активности в отдельных случаях толкуется исключительно широко. В качестве злонамеренного действия в киберпространстве, влекущего уголовную ответственность, ОАЭ и Бахрейном рассматривалось также выражение

симпатии в любой форме к Катару, включая ожидание прекращения спора между Катаром и четырьмя государствами, которые ввели санкции против него, либо осуждение введенных против него санкций, в качестве киберпреступления. Так, в частности, законодательство ОАЭ предусматривало в ответ на такие действия штраф в размере до 500 000 риалов и тюремное заключение от 3 до 15 лет; законодательство Бахрейна — до 5 лет тюремного заключения (Отчет о страновом визите в Катар (2021)) [2, p. 151; 86, para. 47—48]. Указанные нормы были устранены после заключения Декларации Аль-Ула в январе 2021 г.

В настоящее время государства и частные компании также активно вводят меры по запрету либо ограничению распространения различного рода информации не только своими гражданами, но и информационными порталами и гражданами третьих стран под различными предлогами: как распространение пропаганды, поощрение терроризма, распространение нежелательной или фейковой информации и пр. При этом практика государств в этой сфере неединообразна и часто противоречива.

Например, разрешения целого ряда СМИ, в частности *Sputnik, RT* и подчиненных им компаний, были отозваны *Youtube*, а также в ЕС, США, Австралии, Канаде [4; 89] и Великобритании [71] за политику, отражающую позицию Российской Федерации в конфликте в Украине в 2022 г. Регламент ЕС 22/350 запретил вещание указанных СМИ, квалифицировав их как распространяющие дезинформацию, пропаганду, манипуляцию общественным мнением, подтасовку фактов (пп. 3, 5—7), представляющие «гибридную угрозу» и угрозу безопасности и публичному порядку ЕС (пп. 3, 8) [19; 22], обосновывая это тем, что указанные СМИ контролируются Российской Федерацией. Регламент и решение, однако, не обосновывают соблюдения требований статей 19, 20 МПГПП.

Принятое в ответ решение Российской Федерации об ограничении вещания и доступа в сети Интернет *BBC*, Голоса Америки, *Deutsche Welle, Meduza* и др. было, напротив, осуждено государствами ЕС как ограничивающее свободу выражения мнения [72], несмотря на доступные отчеты о методах формирования общественного мнения мирового сообщества в отношении конфликта в Украине с использованием неверифицированной или постановочной информации [16]. Аналогичные возражения были представлены Государственным департаментом США после закрытия Российской Федерацией доступа к *Instagram* и *Facebook* в связи с возбуждением уголовного дела в отношении компании *Meta* по статьям 205.1 и 280 Уголовного кодекса Российской Федерации по обвинению в разжигании экстремизма и призывам к террористической деятельности [84].

На основании вышеизложенного представляется возможным сделать следующие выводы.

Развитие ИТ изменило широкий спектр вопросов функционирования государств, жизни людей, обеспечения безопасности, в том числе основания, методы применения и субъектов санкций. Злонамеренность деятельности в информационном пространстве зачастую трактуется государствами и региональными организациями как основание для введения широкого круга финансовых, экономических, целевых санкций, санкций с использованием ИТ, особенно с учетом того, что деятельность физических и юридических лиц в информационной среде неоднократно признавалась СБ ООН в качестве угрозы международному миру и безопасности.

При этом злонамеренность понимается исключительно широко и включает, в том числе деяния физических и юридических лиц, которые могут быть квалифицированы в качестве преступных, а также те, которые традиционно не криминализируются. В настоящее время перечень государств и международных организаций, закрепивших такую возможность, включает США, ЕС, Великобританию, Австралию.

Использование в доктрине термина «кибersанкции» как применение различного вида односторонних принудительных мер в ответ на злонамеренную деятельность в информационной сфере, в том числе с использованием ИТ, поскольку характеристика санкций базируется либо на их объекте (целевые, секторальные), либо на методологии (экономические, финансовые), на наш взгляд, некорректно.

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, СБ ООН рассматривает данную проблему в разрезе противодействия терроризму и делает упор, в первую очередь, на развитие национального законодательства, направленного на предотвращение создания угрозы информационной безопасности государств и лиц на их территории, использования сети Интернет для планирования, организации, осуществления и финансирования террористических актов и легализации преступных доходов, привлечение виновных лиц к ответственности.

Имплементация решений СБ ООН включает широкий перечень мер, подлежащих применению государствами, в том числе сбор информации, блокировку террористических и экстремистских сайтов, отслеживание схем совершения трансграничных преступлений с использованием сети Интернет, вовлечения лиц в террористическую деятельность, отмывание

преступных доходов и финансирование терроризма, борьбу с киберпреступностью. Вместе с тем любые меры, направленные на имплементацию решений СБ ООН, могут приниматься исключительно в соответствии с международным правом.

Несмотря на расширяющуюся практику государств в части введения санкций со ссылкой на злонамеренную деятельность с использованием ИТ, их правовая либо гуманитарная оценка обычно не проводится. Любые меры могут приниматься государствами исключительно при наличии достаточной доказательной базы, правовой оценки с учетом положений международного права, международного гуманитарного права, права прав человека, включая свободу выражения мнений и допустимость введения ограничений в соответствии с положениями статей 19 и 20 МПГПП, обеспечения права на справедливое судебное разбирательство, доступ к правосудию и ряда иных прав.

Список использованных источников

1. Устав Организации Объединенных Наций [Электронный ресурс] // Организация Объединенных Наций. — Режим доступа: <https://www.un.org/ru/about-us/un-charter/full-text>. — Дата доступа: 13.02.2022.
2. Abusedra, A. The Impact of Unilateral sanctions on regional Integration Treaties with Special reference to the Gulf Cooperation council / A. Abusedra // Unilateral Sanctions in International Law / ed. by S. P. Subedi. — Oxford: Hart, 2021. — P. 137—160. (http://dx.doi.org/10.5040/9781509948413.ch-005)
3. Abusedra, A. Use of Cyber Means to Enforce Unilateral Coercive Measures in International Law / A. Abusedra, M. A. Bakar, I. Md. Toriqul // Ibid. — P. 233—254. (http://dx.doi.org/10.5040/9781509948413.ch-012)
4. Alter, R. RT America Shuts Down Amid Russian State-Media Bans / R. Alter [Electronic resource] // Vulture. — 06.03.2022. — Mode of access: <https://www.vulture.com/2022/03/youtube-tiktok-meta-block-russia-owned-rt.html>. — Date of access: 24.04.2022.
5. Article 6: right to life: general comment N 36: UN Doc. CCPR/C/GC/36 [Electronic resource] // Official Documents System of the United Nations. — Mode of access: <https://undocs.org/en/ CCPR/C/GC/36>. — Date of access: 24.04.2022.
6. Article 3: Conflicts not of an international character: Commentary of 2016. Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (12 Aug. 1949) [Electronic resource] // International Committee of the Red Cross. — Mode of access: <https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=BE2D518CF5DE54EAC1257F7D0036B518>. — Date of access: 24.04.2022.
7. Article 2: Application of the Convention: Commentary of 2016. Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (12 Aug. 1949) [Electronic resource] // International Committee of the Red Cross. — Mode of access: <https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=BE2D518CF5DE54EAC1257F7D0036B518>. — Date of access: 24.04.2022.
8. 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.
9. 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.
10. 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.
11. Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities: Executive Order 13694 of 1 Apr. 2015 [Electronic resource]. — 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.
12. 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)
13. 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.
14. 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.
15. Chepkova, T. North Korea Committing Cybercrimes to Avoid US Sanctions / T. Chepkova, A. James [Electronic resource] //be[in]crypto. — 03.06.2019. — Mode of access: <https://beincrypto.com/north-korea-cybercrimes-us-sanctions/>. — Date of access: 24.04.2022.
16. Cohen, D. Ukraine's Propaganda War: International PR Firms, DC Lobbyists and CIA Cutouts / D. Cohen [Electronic resource] // Indybay. — 29.03.2022. — Mode of access: <https://www.indybay.org/newsitems/2022/03/29/18848846.php>. — Date of access: 24.04.2022.
17. Confronting an "Axis of Cyber"? China, Iran, North Korea and Russia in Cyber Space / ed. by F. Rugge. — Milano: Ledizioni Ledi Publishing, 2018. — 181 p.
18. Conway, M. Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research / M. Conway // Studies in Conflict &Terrorism. — 2017. — Vol. 40, N 1. — P. 77—98. (https://doi.org/10.1080/1057610X.2016.1157408)
19. 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.
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. — 2020. — Vol. 63, L351I. — P. 1—4.
21. 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.
22. 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.

23. 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.
24. 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
25. 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.
26. Cyber-related Sanctions Programm: updated on 3 July 2017 / OFAC [Electronic resource] // U.S. Department of the Treasury. — Mode of access: <https://home.treasury.gov/system/files/126/cyber.pdf>. — Date of access: 24.04.2022.
27. Cyber Warfare: a Review of Theories, Law, Policies, Actual Incidents — and the Dilemma of Anonymity / P. C. Reich [et al.] // European Journal of Law and Technology. — 2010. — Vol. 1, N 2. — P. 1—58.
28. De Branbandere, E. Propaganda / E. de Branbandere. — Max Planck Encyclopedias of International Law. — 2019. [Electronic resource] // Oxford Public International Law. — August 2019. — Mode of access: <https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e978?prd=MPIL>. — Date of access: 16.04.2022.
29. Dinstein, Y. War, Aggression and Self-Defence. 3rd ed. / Y. Dinstein. — Cambridge: Cambridge University Press, 2001. — 336 p.
30. DPRK 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.
31. 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.
32. Draft Report on Aggression and the Use of Force (May 2016) [Electronic resource] // International Law Association. — Mode of access: <https://ila.vettoreweb.com/Storage/Download.aspx?DbStorageId=1055&StorageFileGuid=c911005c-6d63-408e-bc2d-e99bfc2167e4>. — Date of access: 24.04.2022.
33. Drone attacks on Saudi oil sites disrupt supplies [Electronic resource] // France 24. — 15.09.2019. — Mode of access: <https://www.france24.com/en/20190915-drone-attacks-saudi-aramco-sites-disrupt-oil-supplies-us-blames-iran>. — Date of access: 24.04.2022.
34. Effects of terrorism on the enjoyment of human rights: UN Doc. A/RES/72/246 [Electronic resource] // Official Documents System of the United Nations. — Mode of access: <https://undocs.org/en/A/RES/72/246>. — Date of access: 24.04.2022.
35. Explanatory Memorandum to the Cyber (Sanctions) (Eu Exit) Regulations 2020/597 [Electronic resource] // legislation.gov.uk. — Mode of access: <https://www.legislation.gov.uk/uksi/2020/597/pdfs/uksiem_20200597_en.pdf>. — Date of access: 24.04.2022.
36. Ferdinand Nahimana, Jean-Bosco Barayagwiza, Hassan Ngeze v. The Prosecutor: judgement, 28 Nov. 2007, case N ICTR-99-52-A / International Criminal Tribunal for Rwanda [Electronic resource] // Refworld. — Mode of access: <http://www.worldcourts.com/ictr/eng/decisions/2007.11.28_Nahimana_v_Prosecutor.pdf>. — Date of access: 24.04.2022.
37. Final report of the Panel of Experts established pursuant to resolution 1874 (2009): UN Doc. S/2021/211* [Electronic resource] // Official Documents System of the United Nations. — Mode of access: <https://undocs.org/en/S/2021/211>. — Date of access: 24.04.2022.
38. Final report of the Panel of Experts on Yemen: UN Doc. S/2021/79* [Electronic resource] // Official Documents System of the United Nations. — Mode of access: <https://undocs.org/en/S/2021/79>. — Date of access: 24.04.2022.
39. Final report of the Panel of Experts submitted pursuant to resolution 1879 (2019): UN Doc. S/2020/151 [Electronic resource] // Official Documents System of the United Nations. — Mode of access: <https://undocs.org/en/S/2020/151>. — Date of access: 24.04.2022.
40. Frowein, J. A. Legal Consequences for International Law Enforcement in the Case of Security Council Inaction / J. A. Frowein // The Future of International Law Enforcement: New Scenarios — New Law / ed. J. Delbrück. — Berlin: Dunker and Humblot, 1993. — P. 111—125.
41. Galtan, S. Meta: Ukrainian officials, military targeted by Ghostwriter hackers / S. Galtan [Electronic resource] // BleepingComputer. — 28.02.2022. — Mode of access: <https://www.bleepingcomputer.com/news/security/meta-ukrainian-officials-military-targeted-by-ghostwriter-hackers/>. — Date of access: 24.04.2022.
42. Gardner, F. Saudi oil facility attacks: Race on to restore supplies / F. Gardner [Electronic resource] // BBC. — 20.09.2019. — Mode of access: <https://www.bbc.com/news/world-middle-east-49775849>. — Date of access: 24.04.2022.
43. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: UN Doc. A/70/174 [Electronic resource] // Official Documents System of the United Nations. — Mode of access: <https://undocs.org/en/A/70/174>. — Date of access: 24.04.2022.
44. Hagen, J. Protecting the Digitized Society: The Challenge of Balancing Surveillance and Privacy / J. Hagen, O. Lysne // The Cyber Defense Review. — 2016. — Vol. 1, N 1. — P. 75—90.
45. Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense / ed. by E. G. Carayannis, D. F. J. Campbell, M. P.Efthymiopoulos. — New York: Springer International Publishing, 2018. — 354 p.
46. Harrison, H. Cyber Warfare and the Laws of War / H. Harrison. — Cambridge: Cambridge University Press, 2014. — 321 p. (https://doi.org/10.1017/CBO9780511894527)
47. Implementation of Security Council resolution 2231 (2015): Ninth report of the Secretary-General: UN Doc. S/2020/531 [Electronic resource]. — Mode of access: <https://undocs.org/en/S/2020/531>. — Date of access: 24.04.2022.
48. 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.
49. Klepper, D. Meta: Russian invasion driving more disinformation online / D. Klepper [Electronic resource] // ABC News. — 08.04.2022. — Mode of access: <https://abcnews.go.com/Business/wireStory/meta-russian-invasion-driving-disinformation-online-83930631>. — Date of access: 24.04.2022.
50. Mahadi, H. UN High Commissioner for Human Rights Bachelet speaks out against Russophobia / H. Mahadi [Electronic resource] // Oops Top: Explory Technology. — 20.03.2022. — Mode of access: <https://oopstop.com/un-high-commissioner-for-human-rights-bachelet-speaks-out-against-russophobia/>. — Date of access: 24.04.2022.
51. Melzer, N. The Trial of Julian Assange. A study of persecution / N. Melzer. — London: Verso, 2022. — 368 p.
52. Nigal, A. UN Condemns Facebook Owner Meta For Allowing 'hate Speech' Against Russians / A. Nigal [Electronic resource] // RepublicWorld.com. — 12.03.2022. — Mode of access: <https://www.republicworld.com/world-news/russia-ukraine-crisis/un-condemns-facebook-owner-meta-for-allowing-hate-speech-against-russians-articleshow.html>. — Date of access: 24.04.2022.

53. Paul, K. How Meta fumbled propaganda moderation during Russia's invasion of Ukraine / K. Paul, M. Vengattil [Electronic resource] // Euronews. — 11.04.2022. — Mode of access: <https://www.euronews.com/next/2022/04/11/ukraine-crisis-meta-insight>. — Date of access: 24.04.2022.
54. Radicalisation in the digital era: the use of the internet in 15 cases of terrorism and extremism / I. von Behr [et al.]. — RAND, 2013 [Electronic resource] // RAND. — Mode of access: <https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf>. — Date of access: 24.04.2022.
55. 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.
56. Report of the Panel of Experts established pursuant to resolution 1874 (2009): UN Doc. S/2019/691* [Electronic resource] // Official Documents System of the United Nations. — Mode of access: <https://undocs.org/en/S/219/691>. — Date of access: 24.04.2022.
57. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression: UN Doc. A/HRC/35/22 [Electronic resource] // Official Documents System of the United Nations. — Mode of access: <https://undocs.org/en/A/HRC/35/22>. — Date of access: 24.04.2022.
58. Report of the Special Rapporteur to the General Assembly on the temporary challenges to freedom of expression: UN Doc. A/71/373 [Electronic resource] // Official Documents System of the United Nations. — Mode of access: <https://undocs.org/en/A/71/373>. — Date of access: 24.04.2022.
59. Resolution 1874 (2009) adopted by the Security Council at its 6141st meeting, on 12 June 2009 UNSC Res 1874 of 12 June 2009: UN Doc. S/RES/1874(2009) [Electronic resource] // Official Documents System of the United Nations. — Mode of access: <https://undocs.org/en/S/RES/1874(2009)>. — Date of access: 24.04.2022.
60. Resolution 2515 (2020) adopted by the Security Council on 30 March 2020: UN Doc. S/RES/2515(2020) [Electronic resource] // Official Documents System of the United Nations. — Mode of access: <https://undocs.org/en/S/RES/2515(2020)>. — Date of access: 24.04.2022.
61. Resolution 2482 (2019) adopted by the Security Council at its 8582nd meeting, on 19 July 2019, 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.
62. Resolution 2419 (2018) adopted by the Security Council at its 8277th meeting, on 6 June 2018, 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.
63. Resolution 2490 (2019) adopted by the Security Council at its 8624th meeting, on 20 September 2019, 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.
64. 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.
65. 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.
66. Resolution 2216 (2015) adopted by the Security Council at its 7426th meeting, on 14 April 2015, 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.
67. Resolution 2231 (2015) adopted by the Security Council at its 7488th meeting, on 20 July 2015: UN Doc. S/RES/2231 (2015) [Electronic resource] // Official Documents System of the United Nations. — Mode of access: <https://undocs.org/en/S/RES/2231(2015)>. — Date of access: 24.04.2022.
68. Rewards for Justice. North Korea [Electronic resource] // U.S. Department of the Treasury. — Mode of access: <https://rewardsforjustice.net/?north-korea=north-korea>. — Date of access: 24.04.2022.
69. Romano, S. M. Psychological War Reloaded: Cyber-Sanctions, Venezuela and Geopolitics / S. M. Romano // Revista Internacional de Pensamiento Politico. — 2017. — Vol. 12. — P. 105—124. (https://doi.org/10.46661/revintpensampolit.3227)
70. Roscini, M. World Wide Warfare — Jus ad bellum and the Use of Cyber Force / M. Roscini // Max Planck Yearbook of United Nations Law. Vol. 14 / ed. by A. von Bogdandy, R. Wolfrum. — Brill, 2010. — P. 85—130.
71. RT: Russian-backed TV news channel disappears from UK screens [Electronic resource] // BBC. — 03.03.2022. — Mode of access: <https://www.bbc.com/news/entertainment-arts-60584092>. — Date of access: 24.04.2022.
72. Russia blocks access to BBC and Voice of America websites [Electronic resource] // Reuters. — 04.03.2022. — Mode of access: <https://www.reuters.com/business/media-telecom/russia-restricts-access-bbc-russian-service-radio-liberty-ria-2022-03-04/>. — Date of access: 24.04.2022.
73. Schmitt, M. 'Attack' as a Term of Art in International Law: The Cyber Operations Context / M. Schmitt // Proceedings of the 4th International Conference on Cyber Conflict / ed. by Ch. Czosseck., R. Ottis and K. Ziolkowski. — NATO CCD COE. — 2012. — P. 283—293.
74. Skordas, A. Mass Media, Influence on International Relations / A. Skordas [Electronic resource] // Oxford Public International Law. — April 2014. — Mode of access: <https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e385>. — Date of access: 13.02.2022.
75. 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.
76. Targeted, Cut Off, and Left in the Dark: The #KeepItOn report on internet shutdowns in 2019 (2020) [Electronic resource] // accessnow. — Mode of access: <https://www.accessnow.org/keepiton-2019-report>. — Date of access: 24.04.2022.
77. 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.
78. The right to privacy in the digital age: UN Doc. A/RES/68/167 [Electronic resource] // Official Documents System of the United Nations. — Mode of access: <https://undocs.org/en/A/RES/68/167>. — Date of access: 24.04.2022.
79. The use of Internet for Terrorist purposes, 2012 [Electronic resource] // United Nations Office on Drugs and Crime. — Mode of access: <https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf>. — Date of access: 24.04.2022.

80. 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.
81. Trevelyan, M. Facebook owner defends policy on calls for violence that angered Russia / M. Trevelyan [Electronic resource] // Reuters. — 14.03.2002. — Mode of access: <https://www.reuters.com/world/kremlin-says-meta-would-have-cease-work-russia-if-reuters-report-is-true-2022-03-11/>. — Date of access: 24.04.2022.
82. Two Major Saudi Oil Installations Hit by Drone Strike, and U.S. Blames Iran [Electronic resource] // The New York Times. — 14.09.2019. — Mode of access: <https://www.nytimes.com/2019/09/14/world/middleeast/saudi-arabia-refineries-drone-attack.html>. — Date of access: 24.04.2022.
83. 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.
84. US State Department condemns Russia's decision to recognize Meta as extremist organization [Electronic resource] // TASS: Russian News Agency. — 21.03.2022. — Mode of access: <https://tass.com/world/1425401?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com>. — Date of access: 24.04.2022.
85. Vengattil, M. Facebook allows war posts urging violence against Russian invaders / M. Vengattil, E. Culliford [Electronic resource] // Reuters. — 11.03.2022. — Mode of access: <https://www.reuters.com/world/europe/exclusive-facebook-instagram-temporarily-allow-calls-violence-against-russians-2022-03-10/>. — Date of access: 24.04.2022.
86. Visit to Qatar: Report of the Special Rapporteur on the negative impact of unilateral coercive measures on the enjoyment of human rights, Alena Douhan*: UN Doc. A/HRC/48/59/Add.1 [Electronic resource] // Official Documents System of the United Nations. — Mode of access: <https://undocs.org/en/A/HRC/48/59/Add.1>. — Date of access: 24.04.2022.
87. Woltag, J.-C. Cyber Warfare / J.-C. Woltag [Electronic resource] // Oxford Public International Law. — August 2015. — Mode of access: <https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e280?prd=EPIL>. — Date of access: 16.04.2022.
88. Yaakoubi, A. E. Saudi Aramco petroleum storage site hit by Houthi attack, fire erupts / A. E. Yaakoubi, M. E. Dalah [Electronic resource] // Reuters. — 26.03.2022. — Mode of access: <https://www.reuters.com/world/middle-east/saudi-air-defences-destroy-houthi-drones-state-tv-2022-03-25/>. — Date of access: 24.04.2022.
89. YouTube blocks Russian state-funded media, including RT and Sputnik, around the world [Electronic resource] // France24. — 12.03.2022. — Mode of access: <https://www.france24.com/en/europe/20220312-youtube-blocks-russian-state-funded-media-including-rt-and-sputnik-around-the-world>. — Date of access: 24.04.2022.
90. Ziemele, I. Privacy, Right to, International Protection / I. Ziemele [Electronic resource] // Oxford Public International Law. — November 2015. — Mode of access: <https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e863>. — Date of access: 13.02.2022.

Статья поступила в редакцию 27 апреля 2022 г.