10.46272/2587-8476-2023-14-1-52-71

Киберсанкции как инструмент конкуренции в глобальном киберпространстве

Балахонова Светлана Игоревна, МГИМО МИД России, Москва, Россия

Контактный адрес: s.balakhonova@inno.mgimo.ru

АННОТАЦИЯ

В данной работе рассматривается проблематика киберсанкций как нового инструмента формирования мирового порядка и глобальной конкуренции великих держав, которая постепенно переходит в киберпространство на фоне растущей роли информационно-коммуникационных технологий (ИКТ), повторяя при этом контуры геополитического соперничества, что создает потенциал для быстрого перехода конфликта из киберпространства в реальное. С этой целью были исследованы риски, которые несут в себе кибератаки; изучена природа противоречий между нормами международного права и киберсанкциями; проведен анализ правовых основ ключевых государств-инициаторов и рассмотрена практика введения киберсанкций. Изучение перечисленных аспектов позволило прийти к выводу о том, что киберсанкции являются традиционными мерами сдерживания, ограничения и наказания за злонамеренные действия в киберпространстве. Данный анализ выявил, что, применяя киберсанкции, США преследуют свои национальные интересы, главным образом экономические, в то время как ЕС скорее использует этот инструмент для проецирования своей нормативной силы. Наряду с этим в процессе трансформации мирового порядка киберсфера, открывая возможности для асимметричных войн, используется государствами для компенсации геополитического неравенства в условиях отсутствия правил, регулирующих поведение, а ущерб от кибератаки может быть значительным как с политической, так и с экономической точки зрения. Однако консенсус великих держав относительно выработки единых норм, регулирующих поведение в киберпространстве, в кратко- и среднесрочной перспективе не представляется возможным, поскольку ключевые государства-инициаторы (США и ЕС) все чаще прибегают к односторонним мерам, в то время как основные государства-цели (Россия и Китай) апеллируют к нормам международного права. По мере размывания основ неолиберального мирового порядка антагонизм государств будет усиливаться, а поскольку на сегодняшний день киберсанкции не обязывают инициатора предоставлять доказательства, давать точную оценку ущерба и не влекут за собой обратного эффекта как такового, повышая лишь имиджевые издержки для оппонентов, популярность такого вида санкций будет расти.

КЛЮЧЕВЫЕ СЛОВА

киберсанкции, киберпространство, кибербезопасность, кибератака, мировой порядок, великие державы

Введение

Сегодня кибербезопасность является неотъемлемой частью концепции национальной безопасности государства, а разработка и внедрение новых технологий сопряжены со значительными для нее рисками. При этом, несмотря на растущую важность данного вида безопасности, глобальные правила, регулирующие ответственное поведение в киберпространстве, не выработаны.Такое положение дел сохраняется, несмотря на усилия, предпринятые ООН и региональными организациями, по установлению правил ответственного поведения в киберпространстве. Не стали глобальными обязательными нормами и инициативы частного сектора, например, со стороны *Microsoft*.

Этот правовой вакуум создал условия для практики введения односторонних мер – санкций, которые стали одним из самых распространенных инструментов внешней политики, выступая альтернативой и дополнением применению силы, а также способом подкрепления переговорных позиций. Данное средство стало восприниматься как важнейший инструмент в рамках усилий по отражению агрессии, восстановлению демократии, осуждению нарушений прав человека и нанесению удара по режимам, укрывающим террористов и международных военных преступников. Три фактора объясняют широкое применение санкций после окончания холодной войны[1]: вновь обретенная государствами возможность вмешиваться в дела, которые были недоступны для них; выход безопасности за рамки военных угроз (теперь секьюритизация охватывает социально-экономические, экологические и гуманитарные измерения); неготовность государств нести более значимые издержки, которые влечет за собой военное вмешательство.

Таким образом, санкции представляют собой экономические, торговые, финансовые и иные ограничительные меры, которые используются государством-инициатором или международными организациями против государства-мишени для достижения определенных политических целей, в частности для изменения политического курса государства – объекта санкций[2]. Несмотря на то что санкции по своему воздействию представляют экономические инструменты, поскольку направлены в первую очередь на ограничение торговых связей инициатора санкций и страны-объекта, доступа к финансовым рынкам, активам и технологиям[3], они зачастую имеют в своей основе политическую природу[4] и нацелены на сохранение (или усиление) политического доминирования государств-инициаторов.

Тема исследования киберсанкций обретает актуальность, поскольку, помимо дипломатических заявлений, осуждающих злонамеренные действия в киберпространстве, государства начали принимать правила, позволяющие вводить односторонние экономические санкции против иностранных граждан, юридических лиц и государственных органов, причастных к вредоносной кибердеятельности. Эти санкции получили название «киберсанкции». Феномен киберсанкций

1 Weiss 1999.
2 Тимофеев 2018.
3 Hufbauer et al. 2007.
4 Baldwin, Pape 1998.

оживил дебаты о законности односторонних экономических санкций, а также о том, какие виды злонамеренной киберактивности вызывают особую озабоченность у государств.

Актуальность темы также обусловлена трансформацией мирового порядка, в рамках которой конкуренция великих держав переходит в сферу технологий и киберпространства, где взаимодействие реального и виртуального миров значительно увеличивает плотность обстоятельств, которые необходимо учитывать, и, следовательно, усложняет взаимодействие международных акторов. Несмотря на то что кибероперации часто выбираются как политически менее затратный вариант (без использования традиционных типов вооружения)[1] и, следовательно, не привлекают такого же внимания, как классические войны, предотвращение конфликтов в киберпространстве не чисто теоретическая задача, поскольку возможен быстрый переход конфликта из киберпространства в реальное. Более того, потребность в киберсанкциях может резко усилиться на фоне растущей цифровизации всех аспектов жизни, что создает возможности для новых кибератак.

Киберсанкции как новое явление в области глобальной конкуренции великих держав в условиях трансформации мирового порядка

Формирование мирового порядка – декларируемый мегатренд XXI в., процесс сложный, многоуровневый, важнейшая составляющая которого – структурное оформление взаимодействия между наиболее влиятельными мировыми державами[2]. Порядок можно определить как относительно предсказуемый набор действий, взаимодействий и результатов в рамках конкретной социальной системы. Порядок в области мировой политики определяется правилами (нормами и институтами) и моделями поведения (действиями, реакциями, результатами), которые отражают то, как акторы понимают и применяют эти правила.

В период после холодной войны неолиберальный экономический порядок все более интернационализировался. После финансового кризиса 2008 г. этот в высшей степени глобализированный экономический порядок подвергался все большим рискам, что обусловило формирование нового геоэкономического порядка. Вследствие этого геополитическая расстановка сил также изменилась, что привело к разным моделям поведения ключевых государств[3], включая, в первую очередь, Россию, Китай и США.

Растущее в последнее десятилетие экономическое и стратегическое соперничество данных держав в геоэкономическом порядке происходит в условиях глубокой экономической интеграции и растущих цифровых связей, что меняет представления о стратегических возможностях и рисках, связанных с взаимозависимостью. Характер и инструментарий глобальной конкуренции меняются по мере развития технологий и усиления глобальной торговой, финансовой, техно-

1 Patryk Pawlak, Eneken Tikk, and Mika Kerttunen, “Cyber Conflict Uncoded. The EU and Conflict Prevention in Cyberspace,” EUISS, April 17, 2020, accessed Novermber 3, 2022, https://www.iss.europa.eu/content/cyber-conflict-uncoded.
2 Шаклеина 2022, 36.
3 Roberts et al. 2019.

логической и информационной зависимости. Системное противоборство сегодня охватывает не только традиционные сферы доступа к факторам производства, но также ведется в космической области, киберпространстве и информационно-психологической сфере[1]. Причем в двух нетрадиционных конкурентных пространствах – космосе и киберсфере – все три великие державы (США, Китай и Россия) имеют растущие стратегические интересы[2].

«Начиная со Второй промышленной революции каждая волна промышленной революции делала доступной для человеческой деятельности новую область: Вторая добавила воздушную область к наземной и морской, Третья открыла космическую область, Четвертая создала киберсферу»[3]. Экономическое и технологическое соперничество только усиливается по мере того, как данные становятся центральным полем конкуренции из-за их потенциально крупных экономических выгод и рисков для безопасности, особенно с учетом их роли в развитии искусственного интеллекта. В частности, для США речь идет о стратегической независимости от неамериканских (особенно из страны-противника или оппонента) поставщиков критических технологий в целях минимизации рисков кибершпионажа[4].

Указанные выше условия служат предпосылкой для конкуренции великих держав в киберпространстве. Особого внимания в данном случае заслуживают киберсанкции, которые выступают одним из основных инструментов взаимодействия ключевых игроков в этой сфере, поскольку именно здесь наиболее ярко проявляется их политическая борьба. Киберсанкции представляют собой традиционные меры (например, запрет на поездки или замораживание активов), которые используются для сдерживания, ограничения и наказания за злоумышленные действия, происходящие в киберпространстве. Киберсанкции обрели обязательный характер норм и оформились как конкретный механизм в ответ на злонамеренные кибероперации[5]. Таким образом, государства прибегают к старому методу – санкциям, – чтобы противостоять относительно новой угрозе кибервторжений.

Необходимо отметить, что враждебное использование ИКТ редко происходит за пределами ранее существовавшего или более широкого военно-политического спора, вследствие чего злонамеренное использование ИКТ государством может привести к эскалации ранее существовавших враждебных отношений. Наряду с этим, использование кибервозможностей в конфликтной ситуации часто включает в себя нанесение ущерба гражданской инфраструктуре и, следовательно, имеет широкомасштабные последствия для жизнедеятельности общества. Ввиду этого конкуренция в киберпространстве повторяет контуры

1 Jeffrey Engstrom, "Systems Confrontation and System Destruction Warfare," RAND Corporation, 2018, accessed November 3, 2022, https://www.rand.org/pubs/research_reports/RR1708.html.
2 Thomas F. Lynch III, "The New Era of Great Power Competition and the Biden Administration," National Defense University Press, 2021, accessed November 3, 2022, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-103/JFQ-103_18-33_Lynch.pdf?ver=4uPAV7gCvJLcH57SlVrZuw%3D%3D.
3 Alexander L. Vuving, "Hindsight, Insight, Foresight: Thinking About Security in the Indo-Pacific," Daniel K. Inouye Asia-Pacific Center for Security Studies, September 2020, accessed November 3, 2022, https://dkiapcss.edu/wp-content/uploads/2020/09/Hindsight-Insight-Foresight-Thinking-about-Security-in-the-Indo-Pacific.pdf.
4 Лексютина 2020.
5 Erica Moret, Francesco Giumelli, Martin Van Horenbeeck, "Galactic Collision: Cyber Sanctions and Real-World Consequences," Geneva Grauate Institute, June 25, 2021, accessed November 3, 2022, https://repository.graduateinstitute.ch/record/299228.

геополитического соперничества великих держав, а главными инициаторами киберсанкций выступают США, ЕС и Великобритания, которые первыми ввели законы, разрешающие применение киберсанкций. В начале декабря 2021 г. к ним присоединилась Австралия, приняв закон, разрешающий применение санкций в ответ на злонамеренную киберактивность. Основными же странами-целями являются Россия, КНДР, Иран и Китай.

В эту новую эру межгосударственной конкуренции киберсфера, открывающая возможности для ведения асимметричных войн, используется государствами для «выравнивания сил на геополитическом поле»[1] и зачастую выходит за рамки международного права или приемлемых норм поведения в киберпространстве. Именно отсутствие совместных правил и норм в киберпространстве способствовало резкому повороту к конфронтации[2].

Противоречия между юридическим обоснованием введения киберсанкций и международным правом как отражение антагонизма великих держав

С теоретической точки зрения кибератаки могут подпадать под действие статьи 2.4 Устава ООН[3], если они выводят из строя банковскую систему страны, энергетическую сеть или наносят значительный ущерб каким-либо иным образом. В таком случае кибератака может быть сравнима с ситуацией, когда эта инфраструктура подвергается атаке посредством обычных военных действий. Тогда можно было бы апеллировать к понятию «агрессия», определение которой было дано ООН в 1974 г.: «Агрессией является применение вооруженной силы государством против суверенитета, территориальной неприкосновенности или политической независимости другого государства, или каким-либо другим образом, несовместимым с Уставом Организации Объединенных Наций»[4]. Так, ряд экспертов полагает, что с точки зрения международного права некоторые кибератаки в определенных условиях приобретают черты актов агрессии, например, нарушение суверенитета и политической независимости государства[5].

Тем не менее киберсанкции могут быть несовместимы с международным правом по нескольким аспектам. Например, данные санкции могут нарушать обычное международное право государственного иммунитета. Оно включает в себя иммунитет от юрисдикции (иммунитет от вынесения судебного решения) и иммунитет от принудительного исполнения[6]. Наряду с этим основным предварительным условием для введения контрмер является предшествующее нарушение обязательства по международному праву – международно-противоправное деяние, в то время как односторонние санкции приводятся в действие на основании внутреннего законодательства государства без предварительного разрешения

1 Erica Moret, Francesco Giumelli, Martin Van Horenbeeck, "Galactic Collision: Cyber Sanctions and Real-World Consequences."
2 Thomas F. Lynch III and Phillip C. Saunders, "Contemporary Great Power Geostrategic Dynamics: Relations and Strategies," National Defense University Press, November 4, 2020, accessed November 3, 2022, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2404308/3a-contemporary-great-power-geostrategic-dynamics-relations-and-strategies/.
3 Устав ООН. [Электронный ресурс]. URL: https://www.un.org/ru/about-us/un-charter/full-text (дата обращения: 30.08.2022).
4 Резолюция 3314 «Определение агрессии» (XXIX) Генеральной Ассамблеи от 14 декабря 1974 года // ООН. [Электронный ресурс]. URL: https://www.un.org/ru/documents/decl_conv/conventions/aggression.shtml (дата обращения: 28.08.2022).
5 Лобач, Смирнова 2020, 63.
6 Bogdanova, Vásquez Callo-Müller 2021.

какой-либо региональной или международной организации. Применение устоявшегося принципа международного права об уважении суверенитета в киберпространстве сталкивается не только с проблемой неопределенности пределов его применения и объема защищаемой инфраструктуры, но и с расхождением официальных позиций разных государств в отношении правового характера этого принципа как основополагающего.

До настоящего времени ни одно государство официально не называло другое государство ответственным за международную кибероперацию. Подобная «осторожная атрибуция» характеризуется двумя основными чертами: 1) публичное разоблачение организатора кибератаки не связано с нарушением конкретной нормы международного права; 2) подобные действия не сопровождаются предоставлением доказательств, отвечающих хотя бы одному из критериев, которые могут быть применимы в соответствии с международным правом[1]. Применение санкций в принципе помогает избежать необходимости предоставлять доказательства и ассоциировать вину за преступление с конкретным государством, что обеспечивает свободу от давления стандартов доказывания, применимых в международном праве. Ситуация усугубляется и тем, что приписывание кибератак конкретному субъекту невозможно, учитывая анонимный характер Интернета.

В некоторых случаях киберсанкции могут нарушать не только международное право, но и обязательства, взятые государством в соответствии с инструментами международного экономического права. Они не могут быть оправданы как контрмеры и скорее всего не будут соответствовать и критериям ВТО, чтобы их было возможно обосновать в рамках исключения для национальной безопасности[2]. Зачастую киберсанкции могут использоваться как инструменты недобросовестной конкуренции и торгового протекционизма. Ввиду данных фактов киберсанкции могут быть обжалованы в инвестиционных судах за несоответствие международным инвестиционным стандартам.

С другой стороны, киберсанкции могут быть эффективным инструментом с нормативным потенциалом для регулирования поведения в киберпространстве, поскольку они задают определенные рамки поведения в нем.

В целом, появление односторонних киберсанкций отражает гораздо более глубокую проблему международного права: очевидную неспособность государств согласовывать международные правила, регулирующие в киберпространстве как на уровне ООН, так и на уровне многосторонних и двусторонних торговых соглашений[3]. На сегодняшний день все еще не установлены международные критерии поведения в киберпространстве. Следовательно, будет сложно установить, какую норму международного права нарушило государство, осуществившее кибератаку.

Важным аспектом является разница в подходах к киберсанкциям. Если страны коллективного Запада прибегают к использованию односторонних мер, формируя правовые основы для их введения, то Россия и Китай апеллируют к междуна-

1 Rusinova et al. 2020.
2 Bogdanova, Vásquez Callo-Müller 2021.
3 Ibid.

родному праву и выработке правил игры в киберпространстве на многосторонней площадке ООН. При этом в попытке снизить остроту нарастающих политических конфликтов США, Россия и Китай заключали двусторонние соглашения о киберпространстве. Так, на фоне растущих в 2015 г. обвинений в адрес Китая в связи с его операциями экономического кибершпионажа в США президент Б. Обама и председатель КНР Си Цзиньпин достигли «общего понимания»[1] по пресечению такой деятельности, в соответствии с которым оба лидера обязались, чтобы их правительства не поддерживали киберкражи корпоративной информации. Тем не менее через год после подписания соглашения в ходе развернувшейся торговой войны США обвинили Китай в нарушении согласованных правил, что вновь иллюстрирует недоверие сторон к двусторонним соглашениям в области кибербезопасности, а также процесс секьюритизации, который выступает в качестве специфического мотива технологического противостояния США и Китая[2].

Подходы США и ЕС и многосторонние подходы к формированию правовых основ, регламентирующих введение киберсанкций

США

Правовая основа, регулирующая введение односторонних мер в ответ на злонамеренные действия в киберпространстве, появилась в США 1 апреля 2015 г., когда президент Б. Обама издал указ №13694 о блокировке собственности определенных лиц, занимающихся серьезной злонамеренной кибердеятельностью. Согласно определению *OFAC*, злонамеренные кибердействия – умышленные действия, совершенные путем несанкционированного доступа к компьютерной системе, в том числе путем удаленного доступа; обход одной или нескольких мер защиты; или компрометация безопасности оборудования или программного обеспечения в цепочке поставок.

В соответствии с системой киберсанкций США, существуют три основные категории злонамеренных действий с использованием киберпространства[3]: (i) злонамеренные атаки, которые вызывают значительные сбои компьютеров и компьютерных сетей, поддерживающих критически важные сектора инфраструктуры; (ii) киберкражи и незаконное присвоение коммерческой тайны; (iii) незаконное присвоение информации с целью вмешательства или подрыва избирательных процессов или институтов. Недавно были приняты и другие исполнительные указы, преследующие цели обнаружения и пресечения злонамеренных действий с использованием киберпространства. Однако правила, установленные этими положениями, относятся к импорту и экспорту информационных и коммуникационных технологий и услуг в США и из США, и, таким образом, они не являются киберсанкциями, если опираться на вышеупомянутое определение.

1 Patryk Pawlak, Eneken Tikk, and Mika Kerttunen, "Cyber Conflict Uncoded. The EU and Conflict Prevention in Cyberspace," EUISS, April 17, 2020, accessed Novermber 3, 2022, https://www.iss.europa.eu/content/cyber-conflict-uncoded..
2 Данилин 2020a.
3 "Executive Order 13757", U.S. Department of the treasury, December 28, 2016, accessed November 3, 2022, https://home.treasury.gov/system/files/126/cyber2_eo.pdf.

Издав данный указ, США дали понять, что могут применить жесткие экономические санкции в ответ на кибератаки. Подобные санкции применяются в отношении физических или юридических лиц, которые сознательно получают или используют коммерческую тайну для коммерческого или конкурентного преимущества или личной финансовой выгоды, которая была незаконно присвоена с помощью киберсредств, если они знают об этом. Санкции также применяются, если физические или юридические лица совершают попытки, помогают или оказывают материальную поддержку такой деятельности.

Санкции США могут быть введены президентом США в соответствии с *CAATSA*, а определение лиц, на которых распространяются санкции в соответствии с исполнительными указами, входит в компетенцию министра финансов[1]. Установленный в США режим киберсанкций разрешает применять санкции в отношении физических и юридических лиц, считающихся ответственными за злоумышленные действия с использованием киберсредств, которые «наносят ущерб или значительно компрометируют» предоставление критически важных услуг, «значительно нарушают» доступность компьютера или сети компьютеров или «приводят к незаконному присвоению» значительного объема средств, ресурсов или интеллектуальной собственности. Киберсанкции могут быть следующими[2]: (i) блокировка имущества и прав собственности; (ii) запрет на поездки; (iii) полный запрет на передачу финансовых средств целевым объектам и на получение финансовых средств от них.

Европейский союз

С 2013 г. ЕС разрабатывает политику и регуляторные меры для реагирования на «злонамеренные» кибероперации, направленные против ЕС из третьих стран. Первая стратегия кибербезопасности была принята в 2013 г. и последний раз была подтверждена в декабре 2020 г. [3]

В Договоре о Европейском Союзе «ограничительные меры» упоминаются как один из ряда инструментов, которые можно использовать для достижения целей ОВПБ. Конвенция Совета Европы о киберпреступности является наиболее важным юридически обязывающим документом, который содержит положения о наказании за незаконный доступ к данным и их перехват, вмешательство в системы и неправомерное использование устройств, а также положения о взаимной помощи при расследовании и уголовном судопроизводстве. Тем не менее, применение Конвенции к текущим кибератакам ограничено. Одна из ключевых причин этого заключается в том, что ни Россия, ни Китай не подписали ее.

В июне 2017 г. Совет ЕС в решении ОВПБ согласился разработать «рамку дипломатического реагирования», известную как набор инструментов киберди-

1 Vera Rusinova, Ekaterina Martynova, Polina Kurakina, "Fighting Cyber-Attacks With Sanctions: New Threats, Old Responses," SSRN, December 8, 2020, accessed November 3, 2022, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3742751.
2 Executive Order 13757, U.S. Department of the treasury, December 28, 2016, accessed November 3, 2022, https://home.treasury.gov/system/files/126/cyber2_eo.pdf.
3 Bendiek A., Schulze M. "Attribution: A Major Challenge for EU Cyber Sanctions," Stiftung Qissenschaft und Politik, December 16, 2021, accessed November 3, 2022, https://www.swp-berlin.org/10.18449/2021RP11/.

пломатии[1], чтобы позволить Союзу выработать общий, скоординированный дипломатический ответ на серьезные киберинциденты. Однако меры были дублирующими и не имели дополнительного эффекта. Новая система киберсанкций была введена в 2019 г. Основные документы ЕС, определяющие введение киберсанкций – Решение Совета 2019/797 и Регламент Совета 2019/796. Киберсанкции ЕС включают такие меры, как запрет на поездки[2], замораживание средств[3], замораживание экономических ресурсов[4], запрет на участие в деятельности, направленной на обход введенных ограничительных мер[5], а также запрет лицам и организациям ЕС предоставлять средства или экономические ресурсы подсанкционным организациям и людям[6]. Киберсанкции ЕС также могут быть введены, если кибердеятельность нацелена на третьи государства или международные организации и такие атаки имеют значительный эффект.

Система киберсанкций ЕС определяет кибератаки как: 1) доступ к информационным системам; 2) вмешательство в информационную систему; 3) перехват данных, если такие действия не санкционированы должным образом владельцем или другим правообладателем системы, данных или их части, или не разрешены в соответствии с законодательством Союза или соответствующего государства-члена. В отличие от США, рамки определения киберсанкций ЕС представляются более точными в формулировании критериев для применения киберсанкций.

Для определения того, имеет ли кибератака значительный эффект, во внимание принимаются следующие факторы:[7] (a) объем, масштаб, воздействие или тяжесть вызванных нарушений, в том числе в отношении экономической и общественной деятельности, основных услуг, важнейших государственных функций, общественного порядка или общественной безопасности; (b) количество затронутых физических или юридических лиц, организаций; (c) количество заинтересованных государств-членов; (d) сумма причиненного экономического ущерба, например, в результате крупномасштабного хищения средств, экономических ресурсов или интеллектуальной собственности; (e) экономическая выгода, полученная преступником для себя или для других; (f) количество и характер украденных данных или масштаб утечек данных; (g) характер доступа к конфиденциальным коммерческим данным.

Дипломатический ответ должен быть последовательным с юридической, технической и политической точек зрения. Однако отсутствие общего подхода

1 Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), June 7, 2017, accessed November 3, 2022, URL: https://ccdcoe.org/uploads/2018/11/EU-170607-CyberDiplomacyToolbox-1.pdf.

2 Council Decision (CFSP) 2021/796 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, European Sources Online, May 18, 2021, accessed November 3, 2022, URL: https://www.europeansources.info/record/council-decision-cfsp-2021-796-amending-decision-cfsp-2019-797-concerning-restrictive-measures-against-cyber-attacks-threatening-the-union-or-its-member-states/.

3 Council Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, EUR-lex, May 17, 2019, accessed November 3, 2022, URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0796.

4 Ibid.

5 Council Decision (CFSP) 2021/796 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacksthreatening the Union or its Member States, European Sources Online, May 18, 2021, accessed November 3, 2022, URL: https://www.europeansources.info/record/council-decision-cfsp-2021-796-amending-decision-cfsp-2019-797-concerning-restrictive-measures-against-cyber-attacks-threatening-the-union-or-its-member-states/.

6 Council Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, EUR-lex.

7 Ibid.

к кибератакам между государствами-членами ЕС, возможное несоответствие киберсанкций основным правам человека и отсутствие доказательств, на основании которых осуществлялась атрибуция кибератак, снижают эффективность санкционного режима ЕС. Вследствие этого демонстрация и реализация пропорционального, последовательного и, прежде всего, юридически обоснованного ответа ЕС на кибератаки является достаточно сложной задачей. Лица, включенные в перечень, оспаривают ограничительные меры ЕС (финансовые санкции и ограничения на поездки) в суде. В соответствии со статьей 263 IV Договора о функционировании Европейского Союза[1] цели таких карательных мер пользуются полной правовой защитой Европейского суда.

Прежде чем ввести киберсанкции, ЕС необходимо точно определить атрибуцию кибератак. Однако на уровне ЕС процесс присвоения, т.е. технического, правового и политического возложения индивидуальной ответственности за кибератаки, является непоследовательным и отчасти противоречивым. Присвоение является суверенным актом государств-членов, обладающих различными техническими и разведывательными возможностями. Роль ЕС заключается только в координации, сборе доказательств и обмене разведданными между государствами-членами и институтами ЕС. Учитывая растущее количество и интенсивность атак в киберпространстве, атрибуция приобретает ключевое значение. Более того, способность ЕС к атрибуции в значительной степени зависит от обмена разведывательными данными с США и Великобританией. И если разведывательный альянс «Пять глаз», в состав которого входят США, Великобритания, Канада, Австралия и Новая Зеландия, координирует свою атрибуцию и публичное возложение ответственности на государство, совершившее кибератаку, оказывая сильное влияние на средства массовой информации[2], то процессы подобной координации в рамках ЕС затруднены. Соответственно, они идут медленнее, и введение санкций после совершенной кибератаки происходит спустя месяцы и даже годы.

Таким образом, правовая основа, разработанная для киберсанкций ЕС, не всегда отражает технические реалии кибероперациий. Критерии, которым должен соответствовать киберинцидент, чтобы оправдать юридические санкции, должны быть сформулированы более точно. Необходимо провести более четкое различие между успешными кибератаками и попытками. Поэтому технические и юридические формулировки должны быть определены точнее. Киберинциденты должны быть более четко дифференцированы в соответствии с их интенсивностью и техническими характеристиками, чтобы адаптировать дипломатический ответ ЕС и обеспечить его соразмерность. Государствам-членам ЕС рекомендуется гармонизировать критерии, необходимые для установления ответственности за кибератаку. Кроме того, доказательства атрибуции должны быть более прозрачными, не ставя под угрозу доступ к оперативной информации. В целом политика атрибуции ЕС демонстрирует, что вертикальную, гори-

1 Договор о функционировании Европейского Союза. // Право Европейского Союза. [Электронный ресурс]. URL: https://eulaw.ru/treaties/tfeu/ (дата обращения: 30.08.2022).

2 Annegret Bendiek, Matthias Schulze. “Attribution: A Major Challenge for EU Cyber Sanctions,” Stiftung Qissenschaft und Politik, December 16, 2021, accessed November 3, 2022, https://www.swp-berlin.org/10.18449/2021RP11/.

зонтальную и институциональную согласованность во внешних действиях ЕС и между государствами-членами необходимо совершенствовать. На это, в частности, нацелена новая Стратегия кибербезопасности ЕС от 2020 г.[1], согласно которой частные компании, государственные учреждения и национальные органы власти должны систематически осуществлять всесторонний обмен информацией о киберинцидентах.

ООН и многосторонние усилия

Со стороны ООН также был предпринят определенный шаг в попытке регулировать деятельность в киберпространстве, когда группа правительственных экспертов ООН в своем отчете за 2015 г.[2] отметила важность мирного разрешения споров. Однако большинство мер, предлагаемых на уровне ООН, сосредоточены прежде всего на поощрении государственного сдерживания в использовании киберинструментов для злонамеренных операций, поддержке сотрудничества между государствами и снижении риска недопонимания и просчетов в киберпространстве.

Несмотря на то что нормы и меры укрепления доверия, предложенные ООН, впоследствии были одобрены ОБСЕ, Большой семеркой, Группой двадцати и ЕС, основной проблемой существующих подходов является их необязательный характер, а значит, отсутствие механизмов обеспечения соблюдения, вследствие чего в ближайшее время консенсус в ООН по данному вопросу вряд ли возможен[3]. Предотвращение киберконфликтов с помощью добровольных мер не дает гарантий, что контрагент не будет предпринимать злоумышленные действия в киберпространстве. Проблема также заключается в отсутствии точного определения понятия «кибератаки» и ее критериев, которые в ряде случаев остаются неоднозначными. Точно так же отсутствуют и признанные на международном уровне различия таких понятий, как «киберпреступность» и «кибервойна»[4], что затрудняет согласованные международные действия по данному направлению. Таким образом, Совет Безопасности ООН еще не определил кибероперации как угрозу международному миру и безопасности, хотя эта идея неофициально обсуждалась в течение многих лет.

Более заметное участие региональных организаций[5] также могло бы способствовать выработке механизмов для предотвращения эскалации и возникновения киберконфликтов. Однако все региональные организации действуют в рамках соответствующих исторических, географических и культурных контекстов, что влияет на их мандаты, возможности и свободу действий. ОБСЕ, например,

1 "New EU Cybersecurity Strategy and New Rules to Make Physical and Digital Critical Entities More Resilient," European Commission, December 16, 2020, accessed November 3, 2022, URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391.
2 "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note by the Secretary-General," United Nations, July 22, 2015, accessed November 3, 2022, URL: https://digitallibrary.un.org/record/799853#record-files-collapse-header.
3 Erica Moret, Patryk Pawlak, "The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?" European Union Institute for Security Studies, July 12, 2017, accessed November 3, 2022, https://www.iss.europa.eu/content/eu-cyber-diplomacy-toolbox-towards-cyber-sanctions-regime.
4 Карасев 2022.
5 Benatar, Marco and Kristof Gombeer. "Cyber Sanctions: Exploring a Blind Spot in the Current Legal Debate." European Society of International Law, May 28, 2011, accessed November 3, 2022, https://www.researchgate.net/publication/228148961_Cyber_Sanctions_Exploring_a_Blind_Spot_in_the_Current_Legal_Debate.

первой приняла комплекс мер по укреплению доверия[1], которые определили тон обсуждения мер по укреплению доверия в глобальном масштабе. Однако ранее существовавшие конфликты политического или военного характера осложняют реализацию этих мер: ОБСЕ борется с ограниченным доверием между своими членами, в частности, после кибератак на Украину, Грузию и Черногорию. АСЕАН, в свою очередь, сталкивается со сложными отношениями между Китаем и другими странами региона. Организация американских государств (ОАГ) испытывает трудности от разногласий между США и другими ее членами, такими как Куба и Венесуэла. В этих обстоятельствах роль региональных организаций как беспристрастных посредников поставлена под сомнение.

Практика введения киберсанкций и ее особенности

США, будучи активным актором, вводящим санкции, неоднократно применяли киберсанкции. Так, чтобы противостоять растущим киберугрозам из-за рубежа, Министерство финансов ввело ряд санкций, связанных с кибербезопасностью, в соответствии как с CYBER2[2] , так и с программами для конкретных стран, преимущественно против России (141), Ирана (112) и Северной Кореи (18)[3].

Например, в марте 2016 г. США ввели санкции против Северной Кореи, в частности против лиц, которые «участвовали в деятельности по подрыву кибербезопасности путем использования компьютерных сетей или систем против целей за пределами Северной Кореи от имени правительства Северной Кореи»[4]. В соответствии с этими решениями северокорейский программист П.Д. Хек, а также организация, на которую он работал, совместное предприятие *Chosun Expo*, были добавлены в список подсанкционных лиц. В сентябре 2019 г. эти санкции были распространены на три кибергруппы, спонсируемые северокорейским государством, – *Lazarus Group, Bluenoroff* и *Andariel*[5].

В 2017 г. от атаки *Wanna Cry* пострадало порядка 230 тысяч компьютеров примерно в 150 странах, в том числе государствах-членах ЕС. В июне 2017 г. Северную Корею обвинили США[6], а в октябре 2017 г – Великобритания[7]. Со стороны ООН, хотя и последовало осуждение атаки от начальника отдела киберпреступности Управления ООН по наркотикам и преступности, никаких действий в соответствии с международным правом предпринято не было.

В том же году посредством использования вредоносной программы, аналогичной *Petya*, шифровки жесткого диска и замены загрузчика *Microsoft* на платежный запрос была совершена атака *Not Petya.* В середине октября 2020 г. США

1 Patryk Pawlak, Eneken Tikk, and Mika Kerttunen, “Cyber Conflict Uncoded. The EU and Conflict Prevention in Cyberspace,” EUISS, April 17, 2020, accessed Novermber 3, 2022, https://www.iss.europa.eu/content/cyber-conflict-uncoded.“
2 “Executive Order 13694, U.S. Department of the Treasury, April 1, 2015, accessed November 3, 2022, URL: https://home.treasury.gov/system/files/126/cyber_eo.pdf.
3 Bartlett Jason and Ophel Megan, “Sanctions by the Numbers: Spotlight on Cyber Sanctions,” Center for a New American Security, May 2, 2021, accessed November 3, 2022, https://www.cnas.org/publications/reports/sanctions-by-the-numbers-cyber.
4 “Executive Order 13722“, U.S. Department of State, March 14, 2016, accessed November 3, 2022, URL: https://www.govinfo.gov/content/pkg/CFR-2017-title3-vol1/pdf/CFR-2017-title3-vol1-eo13722.pdf.
5 “Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups,” U.S. Department of the Treasury, September 13, 2019, accessed November 3, 2022, URL: https://home.treasury.gov/news/press-releases/sm774.
6 “The United States Applauds the EU’s Action on Cyber Sanctions,” U.S. department of State, July 30, 2020, accessed November 3, 2022, URL: https://2017-2021.state.gov/the-united-states-applauds-the-eus-action-on-cyber-sanctions/index.html.
7 Jack Goldsmith, “The Strange WannaCry Attribution,” Lawfare, December 21, 2017, accessed November 3, 2022, https://www.lawfareblog.com/strange-wannacry-attribution.

предъявили обвинение шести гражданам России[1]. ЕС ввел экономические санкции 30 июля 2020 г., применяя Регламент 2020/1125[2], – точечные санкции в отношении отдельных лиц.

В 2018 г. США ввели санкции против российских физических и юридических лиц за «злонамеренную российскую киберактивность, включая их попытки вмешательства в выборы в США, разрушительные кибератаки и вторжения в критически важные объекты инфраструктуры»[3].

1 июня 2020 г. граждане Нигерии были включены в список киберсанкций США[4]. Эти лица были привлечены к санкциям за организацию и осуществление двух видов кибермошенничества. По данным Министерства финансов США, лица, находящиеся под санкциями, украли «более шести миллионов долларов у жертв по всей территории страны».

В сентябре 2020 г. российские граждане, работающие в Агентстве интернет-исследований, были добавлены в список подсанкционных лиц[5]. Кроме того, в октябре 2020 г. российское государственное научно-исследовательское учреждение, которое предположительно связано с деструктивным вредоносным ПО *Triton*, было включено в список лиц, находящихся под санкциями. Данные санкции были введены в рамках положений раздела 224 Закона о противодействии противникам Америки посредством санкций, который допускает введение односторонних санкций против любого лица на территории Российской Федерации, которое заведомо ведет серьезнуюдеятельность, подрывающую кибербезопасность[6].

В апреле 2021 г. было объявлено о новых санкциях США против Российской Федерации[7]. Некоторые из недавно введенных ограничений нацелены на российские технологические компании, «поддерживающие усилия российских разведывательных служб по осуществлению злонамеренных действий в киберпространстве против США».

Среди основных кейсов кибератак на ЕС можно выделить *Bundestag Hack* 2015 г. и атаку на Организацию по запрещению химического оружия (ОЗХО) в Гааге в 2018 г.

Так, в апреле 2015 г. член парламентской группы Левой партии в Бундестаге открыл ссылку в электронном письме, предположительно отправленном ООН, в котором якобы содержалась информация об украинском конфликте. Однако ссылка вела на вредоносный сайт с Троянским вирусом. 22 октября 2020 г. Совет ЕС принял санкции в отношении 85-го Главного центра специального назначе-

1 United States District Court for the Western District of Pennsylvania, United States of America, October 15, 2020, accessed November 3, 2022, URL: https://www.justice.gov/opa/press-release/file/1328521/download.
2 "Council Implementing Regulation (EU) 2020/1125 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States", EUR-lex, July 30, 2020, accessed November 3, 2022, URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32020R1125.
3 "Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks," U.S. Department of the Treasury, March 15, 2018, accessed November 3, 2022, URL: https://home.treasury.gov/news/press-releases/sm0312.
4 "Treasury Sanctions Nigerian Cyber Actors for Targeting U.S. Businesses and Individuals," U.S. Department of the Treasury, June 16, 2020, accessed November 3, 2022, URL: https://home.treasury.gov/news/press-releases/sm1034.
5 "Treasury Sanctions Russia-Linked Election Interference Actor," U.S. Department of the Treasury, September 10, 2020, accessed November 3, 2022, URL: https://home.treasury.gov/news/press- releases/sm1118.
6 "Countering America's Adversaries Through Sanctions Act-Related Sanctions," U.S. Department of the Treasury, August 2, 2017, accessed November 3, 2022, URL: https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/countering-americas-adversaries-through-sanctions-act-related-sanctions.
7 "Treasury Sanctions Russia with Sweeping New Sanctions Authority," U.S. Department of the Treasury, April 15, 2021, accessed November 3, 2022, URL: https://home.treasury.gov/news/press-releases/jy0127.

ния ГУ ГШ МО РФ, применив положения Регламента 2020/1536[1]. В соответствии со статьей 3 Регламента 2019/796, были введены точечные экономические санкции, а также ограничение на въезд в соответствии со статьей 4 Решения 2019/797[2].

В 2018 г. была осуществлена кибератака на ОЗХО в Гааге, в которой были обвинены четыре агента российской разведки, вследствие чего в 2020 г. ЕС ввел санкции в соответствии с Регламентом об осуществлении 2020/1125[3] и дополнением к нему 2020/1744[4].

При рассмотрении данных примеров можно прийти к выводу, что государства, вводившие киберсанкции, не представили никаких доказательств, что кибератака была совершена той или иной страной, а также самого факта ее свершения или попытки. Вследствие этого затруднена и оценка ущерба, а значит, и соотнесение степени ответственности и наказания. Введение киберсанкций было обосновано лишь публичными обвинениями со стороны США, ЕС и Великобритании в адрес России и КНДР. Эпизоды демонстрируют политическое разделение и использование коллективным Западом киберсанкций как дополнительного рычага политического и экономического давления на оппонентов. Тенденции последних 20 лет подтверждают данный тезис направлением эволюции проблем кибербезопасности: от рассуждений о хакерских атаках и интернет-террористических актах в 1990-х гг.[5] до обвинений РФ в кибератаках против государств Запада[6].

1 Council Implementing Regulation (EU) 2020/1536 of implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, EUR-lex, October 22, 2020, accessed November 3, 2022, URL: https://eur-lex.europa.eu/legal-content/%20EN/TXT/?uri=CELEX:32020R1536.

2 Ibid.

3 Council Implementing Regulation (EU) 2020/1125 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, EUR-lex, July 30, 2020, accessed November 3, 2022, URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32020R1125.

4 Council Implementing Regulation (EU) 2020/1744 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, EUR-lex, November 23, 2020, accessed November 3, 2022, URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32020R1744.

5 Furnell, Warren 1999.

6 Hansen, Nissenbaum 2009.

Место киберсанкций в условиях усилившегося санкционного противостояния

Сравнительный анализ правовых актов, проведенный на основе «Базы правовых актов»[1], собранной исследователями Центра экспертизы санкционной политики ИМИ МГИМО и содержащей 284 правовых акта, включая 151 для США (с 1917 по 2022 г.) и 84 акта для ЕС (с 1992 г. по 2022 г.), регулирующих введение санкций в США и ЕС, а также исследование практики введения киберсанкций позволили прийти к выводу, что США выступают «законодателем моды» в сфере киберсанкций, а ЕС – скорее последователем. Именно США и ЕС дают наиболее точные определения кибератакам. При этом ЕС формулирует достаточно точные критерии для оценки степени эффекта кибератаки, которые позволяют оценить ущерб в количественных показателях, чего нет у США. США делают акцент на ущербе, нанесенном важной инфраструктуре, на недобросовестном использовании коммерческой тайны и подрыве работы избирательных институтов. Таким образом, США фокусируются скорее на последствиях кибератаки, а ЕС больше обращает внимание именно на ее «качество»: непосредственно сам факт вмешательства, количество украденных данных.

Можно предположить, что последствия киберсанкций США будут скорее наносить стране-цели экономический ущерб, а последствия киберсанкций ЕС – политический и имиджевый. США среди целей киберсанкций фокусируются на противодействии национальной угрозе безопасности, внешней политике и экономике США. Причем меры США нацелены «не только на ограничение потенциала развития страны-оппонента, но также на воспроизводство на рынках высоких технологий доминирования американских компаний в отдельных ключевых сферах, что позволяет им оставаться структурообразующим игроком глобальных стоимостных цепочек (ГСЦ), рынков и отраслей»[2]. А ЕС говорит скорее о поддержании глобальной безопасности и стабильности, создании открытого глобального киберпространства, отмечая при этом и экономическую конкурентоспособность ЕС, и поддержание демократии. Так, ЕС использует киберсанкции как инструмент для своей *normative power*, а США заявляют только о национальных интересах.

Инструментарий в рамках правовых оснований США, ЕС, Великобритании и Канады ограничен тремя мерами: заморозка активов; запрет на передачу финансовых и экономических средств целевым объектам и на получение финансовых экономических средств от них; запрет на поездки. Декларируемая цель Великобритании достаточно размыта, говорится только о «предотвращении соответствующей киберактивности». Законодательная база Австралии еще находится в разработке, поэтому отсутствует четкое определение кибератаки и не декларируются цели. В случае с ЕС, закон о киберсанкциях «имеет обратную силу», поскольку сама правовая база была принята в мае 2019 г., а обвинение было предъявлено по делу апреля 2015 г., таким образом, киберсанкции были введены лишь спустя пять лет после предполагаемой российской атаки.

1 Арапова, Кудинов 2022.
2 Данилин 2020b.

Таким образом, основные инициаторы киберсанкций – США и ЕС, а Великобритания и Австралия скорее следуют в фарватере их политики, основываясь на их опыте при разработке своей правовой основы в области киберсанкций. Несовершенство правовых баз у основных инициаторов киберсанкций позволяет им широко применять инструментарий данного вида санкций, поскольку обвинение и оценка ущерба производятся каждой страной самостоятельно, а процедура предоставления доказательств и оценка их качества и источников, их предоставляющих, никак не регламентированы.

При рассмотрении более общих трендов в сфере киберсанкций можно отметить, что коллективный Запад выступает наиболее активным инициатором киберсанкций, причем наибольшее количество введенных санкций приходится на США. Именно санкции США имеют наибольший эффект по сравнению с санкциями, введенными другими странами, что обусловлено лидерством США в мировой финансовой системе и размером рынка страны. Недавние киберсанкции ЕС были встречены в США с большим одобрением, что свидетельствует об общем понимании ценности данного инструмента[1]. При этом важно отметить, что вторичные санкции США вызывают разногласия с ЕС, в частности, с Германией, однако подобные протесты ЕС не влияют на избранный США политический курс. Доля санкций ООН выглядит достаточно умеренной. Россия, Китай и КНДР, напротив, являются крупными санкционными объектами.

Ситуация на Украине и вокруг нее и вмешательство в выборы в США выступают основными мотивами для введения киберсанкций в отношении России. Если рассматривать причины введения киберсанкций в более общем понимании, то необходимо выделить такие области, как кибербезопасность, нераспространение ОМУ и права человека.

Учитывая эти выводы, представляется целесообразным более широко говорить о международном экономическом порядке, который движется в сторону «геоэкономического порядка»[2]. Данный сдвиг знаменует собой значительный отход от неолиберального порядка после окончания холодной войны. Как продемонстрировала торговая и технологическая война между США и Китаем, подобный геоэкономический порядок подразумевает значительную правовую неопределенность для экономических операторов, поскольку границы между защитой и протекционизмом все больше стираются, а перспективы эффективного разрешения споров в судебном порядке уменьшаются. Рассмотренный режим киберсанкций этому способствует. Какой баланс будет достигнут между экономическими проблемами и соображениями безопасности в этом новом порядке, зависит не только от внутренних тенденций в России, США и Китае, но и от реакции третьих акторов, включая международные организации, такие как ВТО, третьи государства и частных акторов, таких как корпорации и «мозговые центры».

Таким образом, развитие режима киберсанкций находится под влиянием тех же факторов, которые влияют и на формирование нового мирового порядка,

1 Ivan Timofeev, “Sanctions Against Russia: A Look into 2021,” RIAC, March 11, 2021, accessed November 3, 2022, https://russian-council.ru/en/activity/publications/sanctions-against-russia-a-look-into-2021/.
2 Roberts et al. 2019.

что вновь отражает политическое разделение мира. Следовательно, использование киберсанкций выступает модифицированным и адаптированным к новым условиям инструментом стран Запада в их попытке сохранить устройство мира на основе неолиберального мирового порядка с учетом переноса конкуренции в технологическую сферу.

Всего за последнее десятилетие можно выделить не менее девяти санкционных эпизодов, связанных с киберпроблемами и вмешательством в выборы. На фоне растущей цифровизации всех аспектов жизни потребность в киберсанкциях может существенно возрасти. Данный тренд может быть усилен также за счет участия корпораций в разработке документов, регламентирующих поведение в киберпространстве. Так, на сегодняшний день уже имеются следующие инициативы: соглашение о технологиях кибербезопасности, предложенное *Microsoft*[1], Хартия доверия *Siemens*[2] и Рамочная программа кибербезопасности Национального института стандартов и технологий[3].

Если говорить о перспективах регулирования киберпространства на уровне международного права, то согласие великих держав не представляется возможным[4] по крайней мере в средне- и долгосрочной перспективах, вследствие чего фокус дискуссии сместится в сторону односторонних мер и их потенциала. Уже сегодня киберсанкции США, ЕС и Великобритании могут сигнализировать о красных линиях в киберпространстве[5]. Тренд также может усилиться за счет роста тенденции использования односторонних киберсанкций в США и ЕС – двух юрисдикциях, которые устанавливают стандарты для других государств в формулировании санкционной политики. Сужение угла обсуждения киберсанкций как односторонней меры приведет к тому, что киберсанкции будут все чаще и чаще нарушать международное право или обязательства, которые государства взяли на себя в рамках международного экономического права.

В условиях нового витка санкционного давления в 2022 г. и разрыва экономических связей между крупными международными игроками увеличивается потенциал применения киберсанкций, поскольку снижение технологической зависимости позволяет основным государствам-инициаторам вводить данные санкции без материального ущерба как такового, в отличие от санкций в энергетическом секторе, и при этом повышать имиджевые издержки для своих оппонентов.

Заключение

На фоне растущей конкуренции великих держав (России, Китая и США) в процессе формирования мирового порядка в XXI в. и перехода соперничества в технологическую плоскость кибербезопасность приобретает все более важное зна-

1 Bartlett Jason and Ophel Megan, "Sanctions by the Numbers: Spotlight on Cyber Sanctions," Center for a New American Security, May 2, 2021, accessed November 3, 2022, https://www.cnas.org/publications/reports/sanctions-by-the-numbers-cyber.
2 Bogdanova, Vásquez Callo-Müller 2021.
3 "Cybersecurity Framework," NIST, May 2017, accessed November 3, 2022, URL: https://www.nist.gov/industry-impacts/cybersecurity-framework.
4 *Стрельцов, Анатолий.* Основные проблемы применения международного права к ИКТ-среде // Digital Report. [Электронный ресурс]. URL: https://digital.report/osnovnyie-problemyi-primeneniya-mezhdunarodnogo-prava-k-ikt-srede/ (дата обращения: 28.08.2022).
5 Bogdanova, Vásquez Callo-Müller 2021.

чение. Однако на глобальном уровне все еще отсутствуют какие-либо правила, которые могли бы установить рамки поведения в киберпространстве. Данный фактор способствует распространению практики применения отдельными государствами односторонних мер – киберсанкций. Этот феномен вызвал не только дискуссии о законности применения подобных мер в принципе, но и опасения относительно возможного перехода конфликта из киберпространства в реальное, поскольку конкуренция в киберпространстве зачастую повторяет контуры геополитического соперничества великих держав.

В эпоху цифровизации киберсфера используется государствами для компенсации геополитического неравенства, поскольку позволяет вести асимметричные войны. Вследствие кибератаки может быть нарушен суверенитет государства и нанесен значительный ущерб, особенно в экономической сфере. Более того, киберсанкции вступают в противоречие как с нормами обычного международного права (нарушение государственного иммунитета ввиду распространения национальной юрисдикции одного государства на другое), так и с нормами международных организаций, прежде всего ВТО (использование санкций в качестве инструмента недобросовестной конкуренции).

Анализ правовых основ ключевых стран, инициирующих киберсанкции, а также практики применения подобных мер позволяет прийти к выводу о том, что государства-инициаторы руководствуются прежде всего политическими и экономическими соображениями, поскольку на практике отсутствовали какие-либо доказательства факта свершения или попытки кибератаки, а следовательно, размер ущерба было невозможно оценить, тем не менее санкции были введены.

Можно прогнозировать, что страны коллективного Запада продолжат практику применения киберсанкций, поскольку они не несут обратного эффекта как такового (как в случае с санкциями против российского энергетического комплекса), но повышают имиджевые издержки для оппонента. Наряду с этим в ближайшей перспективе не представляется возможным и консенсус великих держав относительно норм, регулирующих правила поведения в киберпространстве, поскольку по мере перехода мира от неолиберального порядка к «геоэкономическому» страны Запада будут пытаться сохранить устройство мира на выгодных для себя условия, прибегая к односторонним мерам, а Россия и Китай (основные страны-цели) продолжат апеллировать к международному праву.

СПИСОК ЛИТЕРАТУРЫ / REFERENCES

Арапова, Е.Я., Кудинов, А.С. Особенности санкционного регулирования в США, ЕС и Великобритании: сравнительный анализ // Полис. Политические исследования. – 2022. – №6. – С.151–165. https://doi.org/10.17976/jpps/2022/0/11.

Arapova, Ekaterina Ya., Kudinov, Alexei S. “Peculiarities of Sanctions Regulation in the USA, EU and Great Britain: Comparative Analysis.” *Polis. Political Studies*, no. 6 (2022): 151–165 [In Russian].

Данилин, И.В. Американо-китайская технологическая война: риски и возможности для КНР и глобального технологического сектора // Сравнительная политика – 2020a – №4 – С. 160–176. https://doi.org/10.24411/2221-3279-2020-10056.

Danilin, Ivan V. “The U.S.-China Technology War: Risks and Opportunities for P.R.C. and Global Tech Sector.” *Comparative Politics Russia,* no. 4 (2020): 160–176 [In Russian].

Данилин, И.В. Концептуализация стратегии США в технологической войне против КНР: экономика, политика, технонационализм // Международная аналитика – 2020b – Том 11 (4) – С. 21–38. https://doi.org/10.46272/2587-8476-2020-11-4-21-38.

Danilin, Ivan V. “Conceptualizing American Strategy in the Technology War against China: Economy, Geopolitics, Techno-Nationalism.” *The Journal of International Analytics* 11, no. 4 (2020): 21–38 [In Russian].

Карасев, П.А. Эволюция национальных подходов к ведению кибервойны // Международная аналитика – 2022 – Том 13 (2) – С. 79–94. https://doi.org/10.46272/2587-8476-2022-13-2-79-94.

Karasev, Pavel A. "Evolution of National Approaches to Cyber Warfare." *Journal of International Analytics* 13, no. 2 (2022): 79–94 [In Russian].

Лексютина, Я.В. Американо-китайские отношения в 2018–2019 гг.: торговая война и процесс декаплинга // Мировая экономика и международные отношения – 2020 – Т. 64 (6) – С. 85–93. https://doi.org/10.20542/0131-2227-2020-64-6-85-93.

Leksyutina, Yana V. "U.S.-China Relations in 2018–2019: Trade War and the Process of Decoupling." *World Economy and International Relations* 64, no. 6 (2020): 85–93 [In Russian].

Лобач, Д.В., Смирнова, Е.А. Компьютерные сетевые атаки как акт агрессии в условиях развития современных международных отношений: pro et contra // Российский журнал правовых исследований – 2020 – Т. 7 – №4 – С. 59–65. https://doi.org/10.17816/ RJLS46326.

Lobach, Dmitriy V., and Evgeniya A. Smirnova. "Computer Network Attacks as an Act of Aggression in the Context of the Development of Modern International Relations: Pros and Cons." *Russian Journal of Legal Studies* 7, no. 4 (March 14, 2021): 59–65 [In Russian].

Тимофеев, И.Н. Экономические санкции как политическое понятие // Вестник МГИМО-Университета – 2018 – №2 – С. 26–42. https://doi.org/10.24833/2071-8160-2018-2-59-26-42.

Timofeev Ivan N. "Economic Sanctions as a Concept of Power Politics." *MGIMO Review of International Relations*, no. 2 (2018): 26–42 [In Russian].

Шаклеина, Т.А. Россия и США в современных международных отношениях – М: Аспект Пресс, 2022 – 448 с.

Shakleina, Tatiana A. *Russia and the USA in Modern International Relations.* Moscow: Aspect Press, 2022 [In Russian].

Baldwin, David A., and Robert A. Pape. "Evaluating Economic Sanctions." *International Security* 23, no. 2 (1998): 189–198.

Bogdanova, I., and M. Vásquez Callo-Müller. "Unilateral Cyber Sanctions: Between Questioned Legality and Normative Value." V*anderbilt Journal of Transnational Law* 54, no. 4 (2021): 911–954.

Furnell, Stephen M., and M.J. Warren. "Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium?" *Computers & Security* 18, no. 1 (January 1999): 28–34. https://doi:10.1016/S0167-4048(99)80006-6.

Hansen, Lene, and Helen Nissenbaum. "Digital Disaster, Cyber Security, and the Copenhagen School." I*nternational Studies Quarterly* 53 (2009): 1155–1175.

Hufbauer, Clyde G., Jeffrey Schott, Kimberly A. Elliott, and Barbara Oegg. *Economic Sanctions Reconsidered.* Washington, DC: Peterson Institute for International Economics, 2007.

Roberts, Anthea, Moraes Henrique Ch., and Victor Ferguson "Toward a Geoeconomic Order." *Journal of International Economic Law* 22, no. 4 (May 2019): 655–676.
https://dx.doi.org/10.2139/ssrn.3389163.

Weiss, Thomas. "Sanctions as a Foreign Policy Tool: Weighing Humanitarian Impulses." *Journal of Peace Research* 36, no. 5 (1999): 499–509.

Сведения об авторе

Светлана Игоревна Балахонова,
эксперт Центра экспертизы санкционной политики
Института международных исследований МГИМО МИД России,
Россия, Москва, пр. Вернадского, 76, 119454.
e-mail: s.balakhonova@inno.mgimo.ru

Дополнительная информация

Поступила в редакцию: 19 января 2023.
Переработана: 1 февраля 2023.
Принята к публикации: 3 февраля 2023.

Конфликт интересов

Автор заявляет об отсутствии потенциального конфликта интересов.

Цитирование

Балахонова, С.И. Киберсанкции как инструмент конкуренции в глобальном киберпространстве // Международная аналитика – 2023 – Т. 14 (1) – С. 52–71.
https://doi/org/10.46272/2587-8476-2023-14-1-52-71

Cyber Sanctions as a Tool of Competition in Global Cyberspace

ABSTRACT

This paper delves into the issue of cyber sanctions as a novel tool in the context of the transforming global order and the fierce competition amongst great powers, which is gradually extending into cyberspace due to the growing role of information and communication technologies. The contours of geopolitical rivalry are reflected in cyberspace, creating the potential for a quick transition from cyberspace to reality. The article investigates the risks posed by cyber-attacks, studies the nature of the contradictions between the norms of international law and cyber sanctions, carries out an analysis of the legal frameworks of the main initiating countries, and reviews the practice of imposing cyber sanctions. Following these efforts, the conclusion was reached that cyber sanctions are traditional measures used to deter, limit, and punish malicious actions in cyberspace. An analysis of the legal bases of the main initiating countries revealed that the United States pursues its national interests, while the EU rather uses the tool to project its normative power. The cybersphere, amid this process of transforming the world order, creates opportunities for asymmetric wars and is used by states to compensate for geopolitical inequalities in the absence of rules governing behavior. The damage from a cyber-attack can be significant both politically and economically. However, the consensus of the great powers on the development of common norms governing behavior in cyberspace is not possible in the short and medium term. This is due to the fact that the key initiating countries (the U.S. and the EU) are increasingly resorting to unilateral measures, while the main target states (Russia and China) appeal to the norms of international law. As the foundations of the neoliberal world order are being eroded, the antagonism of states will increase. Cyber sanctions do not oblige the initiator to provide evidence, give an accurate assessment of the damage, and do not entail the opposite effect per se, increasing only the image costs for opponents. Therefore, cyber sanctions are expected to become more widespread in the future.

KEYWORDS

cyber sanctions, cyberspace, cyber security, cyber attack, world order, great powers

Author

Svetlana I. Balakhonova,
Expert of the Sanctions Policy Expertise Center of the Institute for International Studies, MGIMO, 76 Vernadsky Avenue, Moscow, 119454.
e-mail: s.balakhonova@inno.mgimo.ru

Additional information

Received: January 19, 2023. Revised: February 1, 2023. Accepted: February 3, 2023.

Disclosure statement

No potential conflict of interest was reported by the author.

For citation

Balakhonova, Svetlana I. "Cyber Sanctions as a Tool of Competition in Global Cyberspace." *Journal of International Analytics* 14, no. 1 (2023): 52–71.
https: //doi/org/10.46272/2587-8476-2023-14-1-52-71