Энергетическая безопасность

ЭНЕРГЕТИЧЕСКАЯ БЕЗОПАСНОСТЬ В ЭПОХУ ДИГИТАЛИЗАЦИИ

Николай Андреевич МОЛЧАНОВ,
доктор военных наук, профессор кафедры интеграционного и европейского права Университета имени О.Е. Кутафина (МГЮА), заслуженный деятель науки Российской Федерации
namolchanov@msal.ru
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9, каб. 543

Елена Константиновна МАТЕВОСОВА,
кандидат юридических наук, доцент кафедры теории государства и права Университета имени О.Е. Кутафина (МГЮА)
ekmatevosova@msal.ru*, 125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9, каб. 455*

Аннотация. *В статье рассматриваются современные проблемы обеспечения национальной и международной энергетической безопасности, связанные с усилением угроз в киберпространстве. Кибератака на объекты критической инфраструктуры стран (объекты энергетики) является одним из инструментов политического давления, причиняя значительный неизбирательный ущерб, подрывающий государственность. Особое внимание в статье уделяется рискам воздействия кибертехнологий на электроэнергетическую систему государства.*

Авторы формулируют вывод о необходимости активизации процесса международного правотворчества в установлении правовых границ использования информационно-коммуникационных технологий.

Анализ международных юридических документов, российских и зарубежных правовых актов позволяет выявить общие для всех стран вызовы энергетической безопасности и особенности национальных подходов в реализации энергетической политики, основным направлением которой сегодня является обеспечение кибербезопасности в энергетическом секторе экономики.

Ключевые слова: *энергетическая безопасность, энергетическая система, электроэнергетика, кибербезопасность, кибератака, критическая инфраструктура, национальная безопасность, международное право.*

DOI: 10.17803/2311-5998.2020.67.3.086-095

N. A. MOLCHANOV,
doctor of Military Sciences, Professor of the Integration and European Law Department of the Kutafin Moscow State Law University (MSAL), Honored Science Worker of Russian Federation
namolchanov@msal.ru
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

E. K. MATEVOSOVA,
PhD in Law, Associate Professor of the Department of Theory of the State and Law of the Kutafin Moscow State Law University (MSAL)
ekmatevosova@msal.ru
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

ENERGY SECURITY IN THE AGE OF DIGITALIZATION

Abstract. *The article discusses modern problems of ensuring national and international energy security, related to the increasing threats in cyberspace. A cyberattack on the critical infrastructure of countries (electric power industry) is one of the tools of political pressure, causing significant indiscriminate damage that undermines statehood. Particular attention is paid to the risks of the impact of cyber technologies on the state's electric power system.*
The authors formulate a conclusion about the need to intensify the process of international law-making in fixing the legal boundaries of the use of information and communication technologies.
An analysis of international legal documents, russian and foreign legal acts allows us to identify common for all countries challenges to energy security and the features of national approaches in the implementation energy policy, the main direction of which today is to ensure cybersecurity in the energy sector of the country's economy.
Keywords: *energy security, energy system, electricity sector, cybersecurity, cyberattack, critical infrastructure, national security, international law.*

Современные разработки в области искусственного интеллекта являются двигателем прогресса в обществе, запуская процессы дигитализации[1], охватывающие абсолютно все сферы общественной жизни. Вопрос о том, какой путь предстоит преодолеть поездному составу научно-технического-прогресса при ускоренном движении по графику дигитализации, остается открытым, поскольку цифровые технологии изменяют мир, не только созидательно преобразовывая его, но и безжалостно разрушая.

Сегодня в глобальном киберпространстве совершается все больше враждебных действий и актов агрессии (в военно-политических, террористических и иных преступных целях), направленных на дискредитацию информационного

[1] Дигитализация — усиливающееся взаимодействие и сближение между цифровым и физическим миром.

суверенитета государств. По мнению академика А. А. Кокошина, «“киберпространство” — это зона повышенной степени стратегической неопределенности. Ведение кибервойн, особенно проведение “боевых кибернетических операций”, все более существенно влияет на рост стратегической неопределенности в мировой политике в целом»[2].

Генеральный секретарь ООН Антонио Гутерриш в своих выступлениях довольно часто обращается к проблеме кибербезопасности, в частности к вопросу о применимости к ней норм международного гуманитарного права, призывая страны признать, что сегодня государства, хотя и замаскированно, но ведут между собой кибервойны, которые должны иметь определенные международно-правовые рамки[3]. Такая позиция главного выразителя интересов народов мира вызывает немалые споры в части не только рассуждений о международном праве, но и самой необходимости введения правового режима кибервойны, которая, согласно подходам ряда государств, в том числе и России, должна быть вне правового поля, исходя из презюмируемого запрета на подобное развитие мировых событий. Вместе с тем следует отметить, что особого внимания заслуживают высказывания Антонио Гутерриша о личной убежденности в том, что «в отличие от великих сражений прошлого, которые начались артиллерийским или воздушным обстрелом, следующая война начнется с массированной кибератаки с целью уничтожить военный потенциал... и парализовать базовую инфраструктуру, такую как электрические сети»[4]. В настоящее время в официальных заявлениях и призывах политических деятелей национального и международного представительства все чаще звучат предостережения о возрастании риска деструктивного кибервоздействия на объекты критической инфраструктуры государств, а именно на объекты энергетики. Следствием столь повышенного внимания (оправданного с точки зрения катастрофичности возможных последствий, но во многом искусственно создаваемого с учетом имеющихся у государств и иных субъектов средств для реального осуществления подобных атак) к данной проблеме является технологическая гонка, которая не решает проблем национальной и международной энергетической безопасности, а, наоборот, порождает все новые угрозы.

Вопрос о роли науки и техники в контексте международной безопасности и разоружения был впервые включен в повестку дня Первого комитета Генеральной Ассамблеи ООН в 1988 г. В докладе от 17 июля 2018 г. «Последние достижения в области науки и техники и их потенциальное воздействие на усилия в области международной безопасности и разоружения»[5] Генеральным секретарем ООН отмечается, что «киберпространство по своей природе способствует совершению нападений, так как объекты критически важной инфраструктуры — от финансо-

---

[2] *Кокошин А. А.* Некоторые макроструктурные изменения в системе мировой политики. Тенденции на 2020—2030-е годы // Полис. Политические исследования. 2014. № 4. С. 41.

[3] См. выступление А. Гутерриша на церемонии открытия Мюнхенской конференции по безопасности: URL: https://www.un.org/sg/en/content/sg/speeches/2018-02-16/address-opening-ceremony-munich-security-conference (дата обращения: 25.08.2019).

[4] U.N. chief urges global rules for cyber warfare // Reuters. 19.02.2018.

[5] В докладе рассматриваются только те научно-технические достижения, практическая реализация которых представляется возможной в ближайшие пять лет, т. е. до 2023 г.

вого сектора до энергосетей и ядерных объектов — уязвимы в силу зависимости их функционирования от компьютерных сетей»[6].

А вопрос информационной безопасности включен в повестку дня ООН с 1998 г. благодаря инициативе России, представившей проект резолюции по этому вопросу в Первом комитете Генеральной Ассамблеи ООН[7]. С 2004 г. была создана Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, изучающая угрозы миру, отдельным регионам и странам, связанные с использованием информационно-коммуникационных технологий[8], в отчетах и рекомендациях которой на протяжении многих лет обозначается наличие угроз деструктивного воздействия злоумышленников на критическую инфраструктуру и объекты информатизации государства, в том числе и в особенности системы электроснабжения.

В 2016 г. в Международном энергетическом агентстве была создана межведомственная рабочая группа по цифровизации и энергетике, в своем первом подробном докладе[9] подтверждающая интенсификацию кибернарушений, влияющих на энергетический сектор (с использованием вредоносного программного обеспечения, фишинга, сетевых роботов и других инструментов). Эксперты утверждают, что полностью предотвратить кибератаки невозможно, но вырабатывают рекомендации к минимизации их последствий. «Цифровая энергетическая безопасность» должна обеспечиваться на основе трех концептуальных положений[10]:

— устойчивость (т. е. способность адаптироваться к новым вызовам, оперативно восстанавливаться после кибердаров и сохранять функциональность критически важных объектов инфраструктуры);
— «кибергигиена» (т. е. основной набор мер предосторожности и мониторинга работы оборудования организации, культура его настройки и использования);
— «безопасность по замыслу» (т. е. инкорпорация целей и стандартов безопасности в основную стадию процесса проектирования внедряемых технологий, при которой меры безопасности предшествуют их созданию, а не наоборот).

Непосредственным объектом кибератаки, совершаемой с целью подрыва энергетической безопасности другого государства, является не вся энергетическая система, а те уязвимости, которые у нее имеются, обнаруживаемые противником при помощи использования специальных методов, предполагающих

---

[6] П. 75 Доклада Генерального секретаря от 17.07.2018 (A/73/177). 73-я сессия Генеральной Ассамблеи ООН // Система официальной документации ООН. URL: https://undocs.org (дата обращения: 25.08.2019).

[7] Генеральной Ассамблеей ООН 4 января 1999 г. была принята Резолюция A/RES/53/70 «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности».

[8] В 2019 г. на основании Резолюции Генеральной Ассамблеи ООН A/RES/73/27 дополнительно создана Рабочая группа открытого состава с целью продолжения выработки норм, правил и принципов ответственного поведения государств, а также путей их реализации.

[9] См.: Digitalization & Energy / International Energy Agency, 2017. 188 p. // URL: https://www.iea.org (дата обращения: 25.08.2019).

[10] Digitalization & Energy. P. 128.

топологический анализ данных («компьютерное зрение» фокусируется на слабо защищенных элементах энергетической инфраструктуры).

Доктринальные взгляды на обеспечение энергетической безопасности в эпоху дигитализации отражаются в актах национального законодательства ведущих стран мира, претерпевающих существенные изменения с учетом развития информационных технологий, потребностей в энергоресурсах, сотрудничества или конфронтации с другими странами, состояния национальной безопасности в целом и ряда других объективных факторов.

Национальная безопасность и социально-экономическое развитие России во многом зависят от возможностей топливно-энергетического комплекса, включающего в себя нефтяную, газовую, угольную и торфяную отрасли, электроэнергетику и теплоснабжение.

Новые трансграничные угрозы энергетической безопасности России в условиях возрастания политизированности международных отношений потребовали корректировки такого документа стратегического планирования, как Доктрина энергетической безопасности Российской Федерации, новая редакция которой была утверждена 13 мая 2019 г.[11]

В Доктрине различаются такие, взаимосвязанные, но не тождественные, понятия, такие как угроза, вызов и риск в области энергетической безопасности. Если вызов энергетической безопасности есть совокупность условий и факторов, не только способных привести к возникновению угрозы, но и создающих новые стимулы для развития мировой энергетики, то угроза энергетической безопасности и риск в данной области связаны с наступлением исключительно отрицательных последствий.

Так, вызовом энергетической безопасности является развитие и распространение прорывных технологий в сфере энергетики, в том числе цифровых и интеллектуальных технологий, что, как очевидно, стимулирует к развитию энергетического сектора в новых направлениях.

Международное сообщество, как и раньше, продолжает видеть в прогрессе при разработке и внедрении новейших информационных технологий и средств коммуникации широчайшие позитивные возможности для развития цивилизации (на общее благо всех государств, созидательный потенциал человечества и дополнительные сдвиги к лучшему)[12].

Одной из угроз энергетической безопасности является «противоправное использование информационно-телекоммуникационных технологий, в том числе осуществление компьютерных атак на объекты информационной инфраструктуры и сети связи, используемые для организации их взаимодействия, способное привести к нарушениям функционирования инфраструктуры и объектов топлив-

---

[11] Указ Президента РФ от 13.05.2019 № 216 «Об утверждении Доктрины энергетической безопасности Российской Федерации» // СЗ РФ. 2019. № 20. Ст. 2421.

[12] Резолюция A/RES/53/70 Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» принята 4 января 1999 г. на 79-м пленарном заседании 53-й сессии Генеральной Ассамблеи ООН // Система официальной документации ООН. URL: https://documents.un.org/prod/ods.nsf (дата обращения: 25.08.2019).

но-энергетического комплекса», которое не может не нанести ущерб энергетике государства.

Риски в области энергетической безопасности связаны как с внутренними, так и с внешними вызовами и угрозами энергетической безопасности. Риском трансграничного характера является «несоответствие технологического уровня российских организаций топливно-энергетического комплекса современным мировым требованиям и чрезмерная зависимость их деятельности от импорта некоторых видов оборудования, технологий, материалов и услуг, программного обеспечения, усугубляющаяся монопольным положением их поставщиков».

Таким образом, риск занимает некое переходное положение — любой вызов энергетической безопасности может перерасти в угрозу, а сама потенциальная возможность такой модуляции и есть, собственно, риск.

Доктрина энергетической безопасности Российской Федерации конкретизирует и развивает положения документов стратегического планирования и правовых актов в сфере обеспечения национальной безопасности[13]. Согласно Доктрине информационной безопасности Российской Федерации национальным интересом в информационной сфере является обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры России (в мирное время, в период непосредственной угрозы агрессии и в военное время). Принятый в 2017 г. именно в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[14] содержит ряд положений, значимых для обеспечения безопасности критической информационной инфраструктуры в сфере энергетики. Однако, как представляется, усиление киберфактора в энергетической политике современного государства (и с учетом лидирующих позиций России на мировых энергетических рынках) требует от российского законодателя принятие отдельного комплексного правового акта, системно регулирующего вопросы обеспечения информационной безопасности в энергетическом секторе экономики страны.

Рассматривая зарубежный опыт, следует упомянуть, что в целях обеспечения кибербезопасности по конкретным секторам экономики Европейская комиссия с 2013 г. создавала всеобъемлющую законодательную базу, с учетом следующих особенностей энергетического сектора[15]:

— требования реального времени (при управлении современными энергетическими системами при определенных условиях стандартные меры безопасности, к примеру, аутентификация команды или проверка цифровой подписи,

[13] Стратегия национальной безопасности Российской Федерации, Стратегия экономической безопасности Российской Федерации на период до 2030 года, Стратегия научно-технологического развития Российской Федерации, Доктрина информационной безопасности Российской Федерации, Энергетическая стратегия России на период до 2030 года и т. д.

[14] Российская газета. № 167. 31.07.2017.

[15] Commission staff working document / Commission Recommendation on cybersecurity in the energy sector, SWD(2019) 1240 final, Brussels, 03.04.2019 // URL: https://ec.europa.eu/energy/sites/ener/files/swd2019_1240_final.pdf (дата обращения: 25.08.2019).

уже не могут применяться из-за свойственной им временно́й задержки, препятствующей производительности системы);

— «каскадные» эффекты (электрические сети и газопроводы тесно взаимосвязаны по всей Европе и за пределами Европейского Союза, вследствие чего перебои в работе системы в одной стране способны привести к отключению электроэнергии или нехватке поставок в других регионах и странах);

— комбинирование устаревших систем с новыми технологиями (многие элементы энергетической системы были спроектированы и построены задолго до создания самих кибертехнологий, однако сегодня используемое устаревшее и инновационное оборудование должно функционировать совместно без сбоев, сохраняя устойчивость к любым киберугрозам).

Согласно рекомендациям и разъяснениям Европейской комиссии, каждый «подсектор» (электроэнергетики, нефтегазовый и ядерный) имеет определенную специфику[16].

Представляется, что указанные особенности в равной степени относимы и к другим странам (в том числе и России), не входящим в Европейский Союз, поскольку «требования реального времени» напрямую связаны с соответствующими международными техническими стандартами, «каскадные» эффекты возможны во многих странах, имеющих взаимосвязанный комплекс технологических подсистем единой энергетической системы, а «комбинирование устаревших систем с новыми технологиями» является актуальной задачей для всех государств, участвующих в научно-техническом прогрессе.

Поиск эффективных мер по управлению рисками в области энергетической безопасности не ограничивается только лишь разработкой более передовых цифровых технологий. К примеру, в июне 2019 г. Сенатом США принят Закон о безопасности энергетической инфраструктуры[17], направленный на устранение тех программных уязвимостей, которые могут позволить хакерам получить доступ к энергосистеме. Данным законопроектом предлагается разработка национальной киберстратегии для защиты (путем «изоляции») энергосистемы от атак, для реализации которой требуется замена автоматизированных систем на низкотехнологичные (так называемые аналоговые ручные, контролируемые операторами). Основным средством защиты энергосистемы как национальной критической инфраструктуры будут «ретротехнологии», используемые еще до создания цифровых, а кроме того, на страже объектов энергетического сектора будут новые технологии, разрабатываемые современными лабораториями, но при этом имеющие архаичные принципы действия. Такое политическое решение, которое с большой вероятностью преодолеет все формальные законотворческие процедуры, свидетельствует о том, что в киберпространстве, на решающем поле

[16] См.: Cyber Security in the Energy Sector. EECSP Report, february 2017 // URL: https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf (дата обращения: 25.08.2019) ; Commission recommendation of 3.4.2019 on cybersecurity in the energy sector // URL: https://ec.europa.eu (дата обращения: 25.08.2019).

[17] Законопроект S. 174 «Securing Energy Infrastructure Act» [Report No. 116—71]. 116th Congress (2019—2020) // Официальный сайт федеральной законодательной информации США. URL: https://www.congress.gov/bill (дата обращения: 25.08.2019).

битвы XXI в., противоборствующие стороны используют уже не новые образцы оружия, а тактические хитрости.

Особую остроту дискуссии об укреплении мер доверия и активизации сотрудничества государств в области обеспечения энергетической безопасности в бесконфликтном международном пространстве придают публикации в различных национальных средствах массовой информации, имеющих наибольший удельный вес в мировой политике. Так, 15 июня 2019 г. в The New York Times была опубликована статья об усилении кибератак США на российскую электросеть[18], в которой сообщается, что с 2012 г. США установили разведывательные зонды в системах управления российской электрической сетью, а на данный момент упор сделан на размещение внутри российской системы потенциально опасного программного кода, который может быть использован для наблюдения или нападения. При этом авторы статьи задаются вопросом о том, может ли энергосистема или любая другая критически важная инфраструктура, обеспечивающая жилые дома, фабрики и больницы, являться законной целью для так называемых онлайн-атак. Публикация вызвала привычное твиттер-негодование американского президента[19], заявившего о ложных источниках издания, однако ряд политических деятелей, не опровергая содержания статьи, отказались как-либо ее комментировать, ссылаясь на недопустимость обсуждения вопросов, касающихся разведывательной деятельности.

Публикации средств массовой информации, безусловно, не являются достаточными и достоверными источниками, на основе которых возможны оценка и прогнозирование состояния национальной и международной энергетической безопасности, однако очевидным представляется, что отдельные внешнеполитические посылы (адресованные конкретным странам или международным объединениям), по тем или иным причинам не оформленные в официальное заявление государства, могут иметь и публицистическое выражение, эффект которого не уступает прямой речи политиков.

Следует признать, что под влиянием цифровизации практика современных международных отношений в контексте рассматриваемой проблематики во многом выстраивается на основе «дипломатии канонерок». Любое заявление о возможности кибервмешательства в энергетическую систему другого государства (в наступательных или даже оборонительных целях) является «демонстрацией» своего превосходства в цифровых достижениях, имеющих не только гражданское, но и военное применение. В отличие от военно-морских сил, у берегов противника цифровую мощь демонстрировать не приходится, достаточно политических заверений в ее наличии, а подтвердить или опровергнуть действительность намерений и реальность исходящей от «киберканонерки» угрозы невозможно.

Массовые и повторяющиеся отключения электричества были зафиксированы в Венесуэле с марта 2019 г., подобный блэкаут происходил в июне текущего года на территории Уругвая, в большей части Аргентины, отдельных районах Парагвая и Чили, а также южной части Бразилии. До настоящего времени причины сбоя в работе объектов электроэнергетики этих стран не установлены. Руководство

[18] U. S. Escalates Online Attacks on Russia's Power Grid // NYT. 15.06.2019.

[19] *Trump D. J.* (@realDonaldTrump). 15.06.2019.18:15 p.m. Tweet. 17.06.2019.19:13 p.m. Tweet.

Венесуэлы, погруженной во тьму, не сомневается в злонамеренных кибератаках США на их национальную электрическую сеть и с целью объективного расследования данного инцидента считает необходимым обращение с соответствующими жалобами в международные организации. Не признавая своей причастности к этим событиям, США заявляют о том, что основными причинами возникновения такого аварийного электроэнергетического режима являются в целом неэффективная энергетическая политика Венесуэлы, износ генерирующего оборудования и неквалифицированное техническое обслуживание объектов электроэнергетики. Ряд экспертов, представляющих себя в независимом статусе, в качестве причин отключения электроэнергии в других пяти странах Южной Америки также указывают на системные ошибки в проектировании и функционировании энергосистемы[20]. Данные события вызвали серьезные проблемы в работе учреждений здравоохранения, промышленности, транспорта и других организаций, имеющих важное социально-экономическое значение. Отсутствие международно-правовой основы для расследования дел, связанных с кибервмешательством в национальную энергетическую систему, технические препятствия в установлении источника угрозы (субъектов, виновных в намеренных киберманипуляциях), а также противоречивость фактического материала о хронологии и последствиях этих событий существенно затруднит ход возможного расследования, результаты которого при любом заключении вызовут возрастание международной напряженности.

Как отмечается российскими и зарубежными учеными, в последние годы кибератаки становятся все более распространенным явлением, представляют серьезную угрозу международной и национальной безопасности. С использованием кибертехнологий увеличиваются риски «отключения ядерных центрифуг, противовоздушной обороны и электрических сетей»[21].

В настоящее время экспертным сообществом особое внимание уделяется проблеме обеспечения ядерной безопасности, в частности объектов ядерного топливного цикла, на которые могут быть совершены кибератаки[22]. Многие исследовательские работы[23] посвящены рассмотрению национальных подходов к обеспечению безопасности этих объектов, их сходству и различиям, а также анализу киберинцидентов, в действительности угрожавших безопасности ядерно опас-

---

[20] Massive blackout hits tens of millions in South America // Associated Press News. 17.06.2019. URL: https://www.apnews.com/a29b1da1a91542faa91d68cf8e97a34d (дата обращения: 25.08.2019).

[21] *Hathaway Oona A. and Crootof R.* The Law of Cyber-Attack // Yale Law School Legal Scholarship Repository. Faculty Scholarship Series. 2012. Paper 3852. Pp. 817—885. URL: https://digitalcommons.law.yale.edu/fss_papers/3852 (дата обращения: 25.08.2019).

[22] По мнению специалистов, ядерные объекты устроены так, что их функционирование может быть нарушено с помощью киберсредств самыми разными способами, в частности выведением из строя систем безопасности, нарушением технологических процессов и работы спутниковых систем и систем связи, а также нарушением целостности данных.

[23] См.: Cyber Security at Nuclear Facilities: National Approaches An ISS Research Project in Cooperation with the Nuclear Threat Initiative (NTI) // URL: https://media.nti.org/pdfs/Cyber_Security_in_Nuclear_FINAL_UZNMggd.pdf (дата обращения: 25.08.2019).

ных объектов конкретных стран. Данная проблема заслуживает самостоятельного предметного научного исследования с опорой на фактологические данные.

Увеличение числа международных форумов, экспертных площадок и организаций, участвующих в решении обозначенных проблем, не гарантирует значительного результата, поскольку важен не сам по себе процесс обсуждения (крайне затянутого ввиду отсутствия политической воли или непрофессионального подхода), а те решительные шаги, которые предпринимаются странами.

Проблемы обеспечения кибербезопасности в энергетическом секторе требуют международного обсуждения в целях укрепления доверия между странами и выработки конкретных международно-правовых норм, запрещающих ведение кибервойны или, допуская военные кибердействия, ограничивающих их согласованными условиями и рамками. Споры о применимости существующего международного права к киберпространству и противоборству в его пределах должны смениться международным правотворчеством, в противном случае сохранение неопределенности в регулировании ряда ключевых вопросов приведет к губительным последствиям для всего мира.

БИБЛИОГРАФИЯ

1. *Кокошин А. А.* Некоторые макроструктурные изменения в системе мировой политики. Тенденции на 2020—2030-е годы // Полис. Политические исследования. — 2014. — № 4. — С. 38—62.
2. Digitalization & Energy / International Energy Agency. — 2017. — 188 p.
3. *Hathaway O. A. and Crootof R.* The Law of Cyber-Attack // Yale Law School Legal Scholarship Repository. Faculty Scholarship Series. — 2012. — Paper 3852. — Pp. 817—885.