УДК 338.12.017

Значение некоторых вызовов национальной безопасности для развития экономики Китайской Народной Республики

Капустин Андрей Андреевич
Студент,
кафедра международных отношений и внешней политики России,
Московский государственный институт международных отношений (университет)
Министерства иностранных дел Российской Федерации,
119454, Российская Федерация, Москва, просп. Вернадского, 76;
e-mail: mr.andreykapustin@yandex.ru

Рыбалова Анастасия Андреевна
Студент,
кафедра востоковедения,
Московский государственный институт международных отношений (университет)
Министерства иностранных дел Российской Федерации,
119454, Российская Федерация, Москва, просп. Вернадского, 76;
e-mail: ar-editors@yandex.ru

Аннотация

Китайская Народная Республика занимает все более важное место в современной системе международных отношений. В частности, это первая в мире экономика по ВВП (ППС), вклад Пекина в мировой экономический рост в 2016 году составил около 35%. Кроме того, страна занимает стратегически важное положение в АТР – наиболее динамично растущем регионе мира, располагая самым крупным населением и постоянно возрастающими технологическими возможностями. Не будет преувеличением заявить, что внешней и внутренней политикой КНР, равно так же, как и любой другой страны, движет объективное стремление обеспечения национальной безопасности. Вместе с тем, важно понимать, что в современном мире государства сталкиваются со все возрастающим количеством вызовов: это не только и не столько прямые военные угрозы, сколько риски террористических атак, глобальное распространение ОМУ, экономические кризисы. Усугубляются традиционные риски, включая обеспечение энергобезопасности. С переходом к «экономике знаний» и значительным повышением роли информации все ярче проявляются опасности кибертерроризма. Настоящая статья ставит своей целью рассмотреть некоторые аспекты тех рисков на международной арене, с которыми сталкивается КНР сегодня.

Для цитирования в научных исследованиях

Капустин А.А., Рыбалова А.А. Значение некоторых вызовов национальной безопасности для развития экономики Китайской Народной Республики // Экономика: вчера, сегодня, завтра. 2017. Том 7. № 4А. С. 258-271.

Ключевые слова

Национальная экономика, Россия, Китай, энергетическая безопасность, ТЭК, ВИЭ, энергобаланс, информационная безопасность, кибербезопасность, кибертерроризм, критическая инфраструктура.

Введение

Китайская Народная Республика – наиболее крупный потребитель энергии в мире. В частности, в 2015 году КНР потребила 3101 млн т. н.э. энергии [BP Statistical Review, 2016, 24, www], в то время как идущие на втором месте Соединенные Штаты – только 2,196 млн т. н.э., Индия – 882 млн т. н.э., Россия – 718 млн т. н.э., а Япония – 435 млн т. н.э. В соответствии с прогнозом компании BP, уже к 2035 году энергопотребление Китая будет составлять около трети от общего энергопотребления в мире (рис. 1).

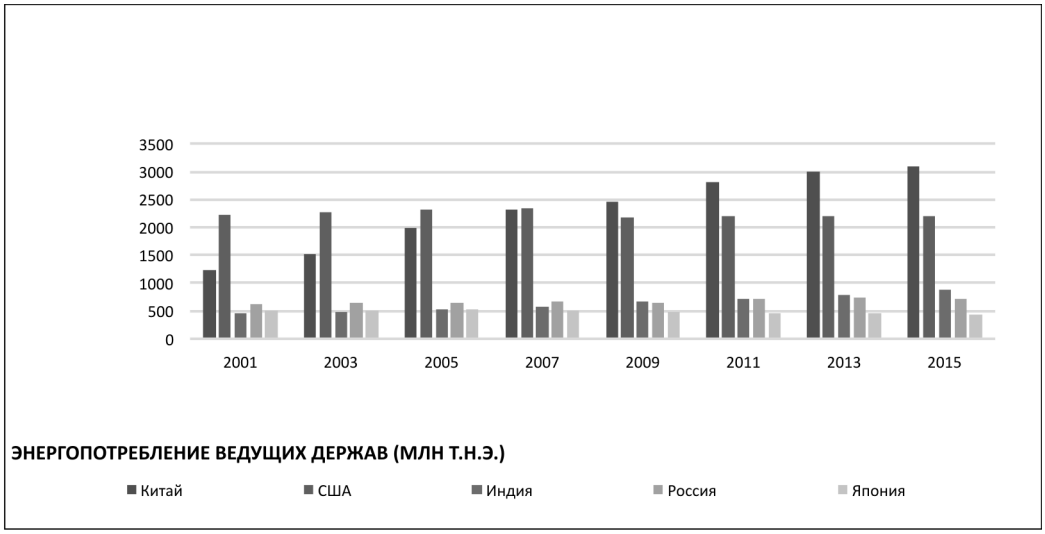

Рисунок 1. Энергопотребление ведущих стран мира

Обеспечение энергетической безопасности

Интересна структурная характеристика ТЭК КНР, которая в значительной мере объясняется исторической спецификой этой страны: так, технологические и финансовые возможности Китай приобрел лишь к началу XXI века, в то время как на протяжении политики «открытости» основная ставка делалась на ускоренное развитие промышленности, в связи

с чем требовалось резко увеличить производство энергии. В результате, сегодня ключевая роль принадлежит углю – самому экологически «грязному» ресурсу, но зато весьма недорогому. В настоящее время на Китайскую Народную Республику приходится до 46% общемирового производства и около 40% мирового потребления угля. Китайское правительство осознает вероятные проблемы, в связи с чем вероятно сокращение добычи в наиболее близких к крупным городам карьерах, на что в январе 2016 года принято решение сократить добычу на 20%, выделив 4,5 млрд. долларов на закрытие производств. При этом потребление угля вырастет на 31%, достигнув пика в конце 20-х годов, после чего пойдет на медленный спад [Energy outlook…, 2015, 185, www].

Всего в структуре энергопотребления Китая около 66% приходится на уголь, преимущественно в промышленности, сконцентрированной в центре страны и на восточном побережье, что приводит к возникновению серьезных экологических рисков. В частности, один из наиболее высоких уровней загрязнения отмечается в Пекине, где в мае 2017 года уровень содержания микрочастиц в воздухе превышал допускаемый ВОЗ в 20 и более раз. Вероятно, что китайская зависимость от поставок нефти может увеличиться с 59% в 2014 году до 76% к 2035 году, что может превзойти даже показатели Соединенных Штатов Америки в 2005 году. (рис. 2)).

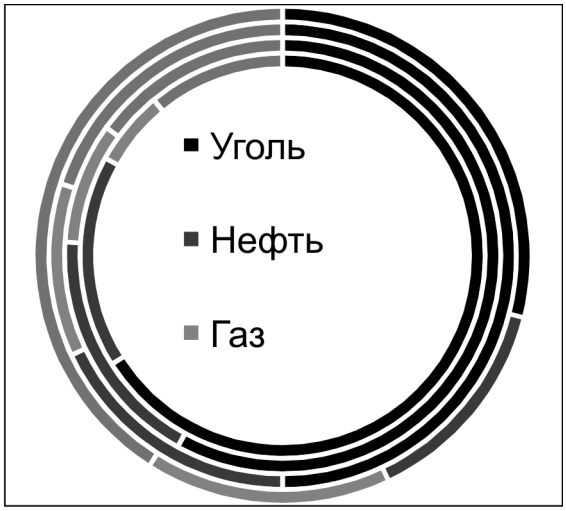

Рисунок 2. Структура энергопотребления Китая

Таким образом, в сфере энергобезопасности перед Китаем очевидны две важные проблемы: во-первых, это необходимость отхода от преобладающего потребления угля хотя бы в долгосрочной перспективе, что, кстати, отмечается и в соответствующих энергетических стратегиях Пекина, а во-вторых, повышение диверсифицированности поставок углеводородов, поскольку нарастающая нестабильность на Ближнем Востоке ставит вопрос использования экспортных возможностей других стран. Ожидается, что к 2030 году потребление нефти в общем энергобалансе составит около 18%, к 2050 году вероятно определенное снижение данного показателя в связи с развитием рынка электромобилей. Определенной про-

блемой остаются преимущественные поставки с Ближнего Востока (Саудовская Аравия, Оман) и Африки – в целом около 6 млн баррелей в день.

Интересно, что разрешение обеих проблем создает благоприятный фон для дальнейшего развития взаимоотношений в энергетике с Россией. В частности, наиболее оптимальным средством замены мощностей по выработке энергии с использованием угля является развитие потребление природного газа, который может быть использован как на производствах, так и в жилом секторе для отопления, в ряде габаритных транспортных средств. В этом плане единственной реальной альтернативой, которая была бы конкурентоспособна по цене, выглядит наращивание поставок из России (вероятно, что импорт из России в 2030-х годах в Китай составит до 65 млн. т. нефти).

Что касается природного газа, то в 2015 году потребление этого энергоресурса составило 6%, однако к 2035 году вероятно значительное увеличение его использования до 12%, а к 2050 году – до 16% [BP Energy Outlook 2035, 50, 72, www]. Повышению привлекательности природного газа способствует снижение стоимости нефти, поскольку зачастую цена на газ в контрактах (например, в соглашении на поставку газа по восточному маршруту «Сила Сибири») привязывается именно к стоимости барреля нефти. Тем не менее в динамике сохраняется ряд переменных; оказывает свое влияние также и конкуренция с другими вариантами: технологиями «чистого угля», снижением энергоемкости как таковой.

Быстро растет применение альтернативной энергетики. Особенно развивается ветряное и солнечное направления. В частности, КНР готова инвестировать значительные средства в ВИЭ: так, по итогам 2015 года Пекин обошел США – многолетнего лидера в данном направлении (102,5 млрд долларов против 44,1 млрд долларов). Значительная часть вложений пришлась именно на СЭС и ВЭС. Согласно экспертным прогнозам, к 2030 году до 7,5% мощностей генерации электроэнергии в стране придется на ВИЭ (сегодня этот показатель составляет около 1,5%). В целом, за следующие 20 лет доля возобновляемых источников энергии АЭС и крупных ГЭС совокупно возрастет с 11% до 20%.

Китай достиг значительных успехов в строительстве традиционных ГЭС: так, мощность самой крупной ГЭС «Три ущелья» (三峡), составляет более 22,5 млн кВт [Анисько, 2010, 10]. Данная гидроэлектростанция – крупнейшая в мире. Вторая по величине – «Силоду» (溪洛渡), которая уже существенно уступает в масштабах (13, 86 ГВт) [溪洛渡水电站首台机组正式并网发电, 2013, www], но тем не менее находится на третьем месте в мире. В соответствии с опубликованным в 2016 году Тринадцатым планом развития энергетики, китайское правительство собирается увеличить установленную мощность АЭС к 2020 году до 58 ГВт, что составит двукратное увеличение по сравнению с 26 ГВт в 2015 году.

Согласно прогнозам китайских специалистов, рост потребления электроэнергии должен составить до 3,5%, причем основным трендом будет его постепенное замедление. В частности, согласно информации BP, с начала XXI века энергопотребление Китая увеличивалось в среднем на 8% в год, однако до 2025 года ожидается рост не более чем на 3%, а с 2025 по

2035 год – лишь на 1,5%, что объясняется не столько даже снижением темпов роста экономики, сколько ее снижающейся энергоемкостью [BP Energy Outlook, 2017, 34, www].

Самообеспечение энергоресурсами в ближайшей перспективе может составить до 85%, а оставшиеся 15% будут импортированы. Особенно значительна доля импорта нефти – до 60% от общего энергопотребления в 2015 году, природный газ (около 30%), а также уран. Пекин продолжит придерживаться политики диверсификации поставок: так, основными экспортерами по-прежнему останутся страны Персидского залива, а также Африки. Значение нашей страны также увеличится: по итогам 2015 года Россия уже выходила на первое место по поставкам нефти в КНР, что подтверждается результатами 2017 года. В ряде отраслевых специализированных направлений импорта (в частности, по урану с Казахстаном) Китай будет концентрироваться на наращивании кооперации с отдельными державами [Россия уступила…, 2017, www].

КНР находится в существенно иной позиции, чем его соседи в Азии. Так, в отличие от Южной Кореи и Японии Пекин располагает богатейшими запасами углеводородов, запасы сланцевой нефти уступают лишь таковым в России и США, что говорит о том, что ситуация с развитием ТЭК значительно более комплексна. Сегодня перед Китаем стоит задача не просто обеспечить поставки углеводородов с учетом географической диверсификации (для КНР ситуация с поставками ближневосточной нефти представляет дополнительную трудность, поскольку узкий Малаккский пролив уязвим в случае гипотетических недружественных действий со стороны третьих держав, например, США или Индии), но также и с целью изменения структуры потребления энергии, перехода от угля к более экологически чистым ресурсам таким, как природный газ или ВИЭ.

Таким образом, перед страной стоит значительная по своей комплексности задача, а обеспечение энергобезопасности соединяет в себе гармонизированное развитие как внутреннего производства энергии, так и внешнего сотрудничества с возрастающим числом государств.

Обеспечение информационной безопасности

В эпоху киберугроз и информационных войн перед Китаем стоят новые вызовы обеспечения своей безопасности. КНР не только регулярно сталкивается с обвинениями в свой адрес в кибершпионаже (страна занимает первое место в мире по количеству кибератак, произведенных с ее территории) [Страны, из которых…, 2013, www], но и сама нередко становится жертвой хакеров. Можно выделить следующие виды информационных воздействий: экономика как цель информационного угроз, кибератаки на критическую инфраструктуру, кибертерроризм и «культурная экспансия» как информационное средство массового влияния.

Китайский интернет-рынок на сегодняшний день является вторым по величине после США, его объем составляет 2,7 трлн. долларов. Количество Интернет-пользователей (пер-

вое место в мире) превышает 710 млн человек (для сравнения США (3-е место) – 277 млн, Россия (6-е место) – 87,5 млн) [Пользователи интернета…, www], каждый из которых проводит в Интернете в среднем 26,5 часов в неделю. По прогнозам, объем онлайн-продаж в КНР по итогам 2016 года достигнет 707 млрд. долларов, по итогам 2017 года – 838 млрд., а в 2018 году составит 959 млрд. долларов [Открытость и взаимодействие…, 2016, 4, www]. Такой огромный рынок привлекает не только бизнес-сообщество, но и потенциальных противников Китая. Только в 2015 году число кибератак в КНР за год подскочило на 51,7%, ущерб от них вырос на 10% [Запад «проглотил»…, 2016, www].

Благодаря обнародованным Э. Сноуденом документам, китайским властям стало известно, что Агентство национальной безопасности США имело доступ к внутренним сетям крупной китайской IT-компании *Huawei* и ряда университетов Китая. К тому же АНБ могло экспортировать в КНР оборудование американских фирм со встроенными шпионскими программами [Коростиков, 2015, www]. В 2008 году компания *Alibaba* начала движение «де-IOE», которое заключалось в отказе от продукции, выпущенной такими американскими IT-гигантами, как EMC, IBM, Oracle, и замене на китайские аналоги *Huawei* и *Inspur*.

Еще одна проблема, с которой КНР сталкивается в киберпространстве, – это неспособность предложить собственные инновационные разработки, из-за чего страна вынуждена идти по модели «догоняющего развития», копируя и дорабатывая иностранные технологии. В связи с этим, несмотря на приоритетное развитие информационного сектора последние 10 лет, Китай значительно уступает развитым странам по обеспечению кибербезопасности страны. Так, Китай занимает лишь 59 место из 139 по Индексу сетевой готовности 2016 года [Networked Readiness Index, www] и 14 место в рейтинге Кибербезопасности 2014 года [The Global Cybersecurity Index, www].

Следующие аспекты кибербезопасности, требующие особенного рассмотрения, это противодействие кибертерроризму и обеспечение безопасности критической инфраструктуры. Кибертерроризм – это совершение террористических действий при помощи компьютеров и компьютерных сетей, а также использование киберпространства в целях террористических групп, в том числе и для совершения непосредственно терактов. Кибертерроризм носит трансграничный характер, поэтому Пекин отводит важную роль Совету Безопасности ООН и координации с членами международного сообщества. В частности, путем создания механизмов взаимодействия правоохранительных органов ряда государств с целью пресечения сетевых преступлений, обмена эффективными технологиями по борьбе с терроризмом в киберпространстве и усовершенствования международной законодательной базы.

Для защиты национального суверенитета и государственной безопасности в киберпространстве 7 ноября 2016 года ПК ВСНП принял закон о кибербезопасности, согласно которому, иностранный контент теперь будут проверять особенно тщательно. Зарубежные компании будут обязаны предоставлять ключи шифрования по требованию представителей власти, а счета нерезидентов Китая и зарубежных компаний будут замораживаться, в

случае, если правоохранительные органы КНР заподозрят их в деятельности наносящей ущерб информационной инфраструктуре страны. Провайдеры будут обязаны хранить пароли и переписку пользователей и передавать их властям. Параллельно будет ужесточаться контроль, в ходе которого на соответствие действующим национальным стандартам и сертификационным требованиям будут проверены поставщики ПО для стратегически важных объектов в сфере телекоммуникации, энергетики, финансов, водоснабжения, управления инфраструктурой и т. д.

По мнению некоторых экспертов, невозможно создать эффективную оборону в информационном пространстве «без создания потенциала для кибератак» [Ибрагимова, 2013, 179]. Так, чтобы не допустить нападения на свою критическую инфраструктуру, государству может понадобиться вывести из строя компьютерные сети противника за пределами собственной территории. Народно-освободительная армия Китая разработала детальную доктрину о нападении на сетевую инфраструктуру. Пекин, осознавая свое отставание по всем другим видам оружия, делает ставку на кибератаки и проникновение в информационную инфраструктуру, что может помочь задержать ответ потенциального противника [Черненко, Габуев, 2011].

Таблица 1. Контингент специальных подразделений по кибероперациям основных стран мира

Страна	Финансирование ($ млн в год)	Численность (человек)
США	7000	9000
Китай	1500	20000
Великобритания	450	2000
Южная Корея	400	700
Россия	300	1000
Германия	250	1000
Франция	220	800
Северная Корея	200	4000
Израиль	150	1000

В НОАК существуют специальные подразделения, которые занимаются проведением кибероперациий. По оценкам некоторых экспертов, их контингент превышает 30 тыс. человек, на поддержание из бюджета выделяется от 1,5 млрд долларов в год (в США Киберкомандование насчитывает 9 тыс. человек, финансирование составляет 7 млрд долларов, в России численность кибервойск превышает 1 тыс. человек, на их поддержание ежегодно может отводиться около 300 млн долларов) [Прогноз развития энергетики…, 5, www]. В рамках военных структур обязанности по оборонительным и наступательным действиям в информационном пространстве несут Третье и Четвертое управление Генерального Штаба (ГШ) НОАК. Под началом Третьего управления действуют несколько НИИ и более десяти оперативных бюро. В задачи данного управления, кроме проведения радио – и радиотехнической разведки, входит разведка в киберпространстве и обеспечение кибербезопасности НОАК. Четвертое управление ГШ занимается организацией и проведением наступательных операций в электронной среде.

Еще одна угроза, существующая в информационном пространстве и представляющаяся важной в современных реалиях, это «культурная экспансия» в Интернете. Информационная война второго поколения нацелена на манипулирование общественным сознанием, подрыв авторитета государственных органов, формирование политической напряженности, инициирование массовых беспорядков. КНР стремится прежде всего не допустить «культурной экспансии» под лозунгом распространения так называемых «западных демократических ценностей». Нарушение свободы слова, цензура в Интернете, централизованный контроль за информацией (прежде всего при помощи партийной структуры) являются неизменным поводом для обвинений со стороны стран Запада. Пекин в свою очередь пытается реализовывать в Интернете систему «управляемая открытость» [Корсаков, 2012].

Особое внимание в КНР уделяется широкому освещению событий, которые могут отрицательно сказаться на имидже страны (техногенные катастрофы, землетрясение в провинции Сычуань в 2008 году, массовые волнения в Тибете и Синьцзяне в марте 2008 и июле 2009 годов соответственно). В ходе событий 2008 года в Тибете в западной прессе было опубликовано множество негативных сообщений о ситуации в автономном районе, которые не соответствовали действительности. Для опровержения дезинформации был создан специальный сайт *Anti-CNN.com*, в результате чего китайским пользователям удалось добиться извинений от ряда зарубежных СМИ [Ибрагимова, 2013, 179].

Однако на практике существует разница между провозглашенным курсом политики «открытости» в Интернете и реальными действиями правительства. Интернет способствует развитию неформальной коммуникации и сплачиванию отдельных протестных сообществ в более крупные неформальные группы, что вызывает опасения у существующей политической системы. Например, в июле 2009 года во время волнений в Синьцзян (Уйгурского автономного округа) более месяца был отключен Интернет, международная телефония и доступ к зарубежным источникам информации. Фактически провинция находилась в информационной изоляции [Евдокимов, 2011].

Для цензуры в Интернете Китай использует «Золотой щит» или в западных СМИ «Великий китайский файервол», который представляет собой систему фильтрации контента в Интернете. Отсев нежелательной информации происходит при помощи серверов на канале между провайдерами и международными сетями. Вследствие работы «Золотого щита» на территории Китая затруднена работа *Google*, *Facebook*, а *Apple* вынуждена терять тысячи пользователей каждый месяц. Кроме того, резидентам КНР сложно получить доступ к VPN. По расчетам западных СМИ, на данную систему работают около 30 000 человек, называемые «50-центовой армией» (умаодан), большинство из которых студенты. За удаление единицы материала или создание комментария, выгодно освещающего позицию правительства, они получают по 0,5 юаня [Herold, Marolt, 2011, 58].

Вышеперечисленные методы обеспечения безопасности в киберпростарантве оказывают непосредственное влияние на экономику Китая. Наиболее чувствительны к новым *hi-*

tech угрозам гиганты китайского ИКТ-комплекса (*Alibaba*, *Lenovo*, *Huawei*, *Xiaomi*, *ZTE*), а также крупные иностранные IT-компании. В случае кибератак или установления контроля над инфраструктурой этих компаний, полагают в Пекине, есть опасность установления через их ресурсы контроля над китайским сегментом Интернета и финансовыми потоками, проходящими через *Chinanet*. Зарубежные компании будут вынуждены вложить серьезные инвестиции для того, чтобы адаптироваться к требованиям новых законов, касающихся кибербезопасности, что может как сократить их инновационный бюджет, так и поставить под угрозу конфиденциальность их корпоративной информации.

К 2049 году должно быть закончено строительство информационного общества. По данным ЮНКТАД, экспорт ИКТ-индустрии из Китая в 2013 году составил 769 млрд. долл. США или 43% мирового объема. В 2014 году объем электронной коммерции превысил 2,2 трлн. долларов (21% ВВП) с ростом – 31,4% и занятостью более 20 млн человек (из них 18 млн. – частичная занятость) [12]. Прогноз на 2017 год составляет 3,3 трлн. Долларов, на конец 2016 года доля КНР в международной электронной коммерции достигла 39,2%.

Заключение

Сегодня в условиях стабильно снижающихся темпов роста ВВП последние несколько лет на уровне правительства на Интернет-сектор возлагаются большие надежды по спасению экономики. Таким образом, информационная безопасность для Китая представляется не менее важной, чем ядерная, а обеспечение суверенитета в информационном пространстве становится одним из национальных приоритетов.

В целом, очевидно, что важные вопросы безопасности, как энергетической, так и кибербезопасности, тесно переплетены с перспективами продолжения экономического роста Китайской Народной Республики, поэтому им уделяется самое пристальное внимание.

Библиография

1. Алексеев Г.Ф. и др. Перспективы энергетического сотрудничества Россия–АТР: (в экспертных оценках). М.: Academia, 2010. 340 с.
2. Анисько А.В. Китай: проблемы и перспективы развития топливно-энергетического комплекса // Молодые востоковеды стран СНГ. М.: ИВ РАН, 2010. С. 7-24.
3. Аристова Л.Б., Лузянин С.Г., Семенова Н.К., Томберг И.Р., Пан Давэй, Сунь Юнсян, Ян Юйли, Чжан Цзяньжун, Ли Лифань. Потенциал и перспектива сотрудничества КНР и РФ в области традиционной и нетрадиционной энергии. М.: Центр стратегической конъюнктуры, 2014. 254 с.
4. Боровский Ю.В. Современные проблемы мировой энергетики. М.: Навона, 2011. 232 с.

5. Евдокимов Е. Политика Китая в глобальном информационном пространстве // Международные процессы. 2011. Т. 9. № 1(25). URL: http://www.intertrends.ru/twenty-fifth/009.htm
6. Запад «проглотил» новый китайский закон о кибербезопасности // Международное радио Китая. 2016. 18 ноября. URL: http://russian.cri.cn/3060/2016/11/18/1s592270.htm
7. Ибрагимова Г. Стратегия КНР в области управления интернетом и обеспечения информационной безопасности // Индекс Безопасности. 2013. № 1(104). Т. 19. С. 169-184.
8. Коломыченко М. В интернет ввели кибервойска // Коммерсантъ. 2017. 1 января. С. 1. URL: https://www.kommersant.ru/doc/3187320
9. Коростиков М. Китай перепрограммирует киберпространство // Коммерсантъ. 2015. 19 октября. URL: http://www.kommersant.ru/doc/2835875
10. Корсаков Г. Информационное оружие супердержавы // Пути к миру и безопасности. 2012. Вып. 1(42). С. 34-59.
11. Открытость и взаимодействие. Дыхание Китая // Международное радио Китая). 2016. № 5(15). С. 4.
12. Пользователи интернета в мире. URL: http://www.bizhit.ru/index/polzovateli_interneta_v_mire/0-404/
13. Прогноз развития энергетики мира и России до 2040 года // Сайт Аналитического центра при Правительстве РФ. URL: http://ac.gov.ru/files/publication/a/2194.pdf
14. Россия уступила первое место по поставкам нефти в Китай // InvestBrothers. 2017. 28 марта. URL: https://investbrothers.ru/2017/03/28/rf_ustupila_pervoe_mesto/
15. Страны, из которых чаще всего совершаются хакерские атаки // Rate1. 2013. 17 августа. URL: http://www.rate1.com.ua/ehkonomika/tekhnologii/2708/
16. Черненко Е., Габуев А. Оружие к бою // Коммерсантъ. 2011. № 26(4567). 15 февраля. URL: https://www.kommersant.ru/doc/1585823
17. Шульцева В. Цифровая экономика Китая. Ч. 1: Первая миля. 2015. Вып. 4. URL: http://www.lastmile.su/journal/article/4702
18. BP Energy Outlook 2017 edition. URL: https: //www.bp.com/content/dam/bp/pdf/energy-economics/energy-outlook-2017/bp-energy-outlook-2017.pdf
19. BP Energy Outlook 2035. URL: https: //www.bp.com/content/dam/bp/pdf/energy-economics/energy-outlook-2015/bp-energy-outlook-2035-booklet.pdf
20. BP Statistical Review 2016. URL: https: //www.bp.com/content/dam/bp/pdf/energy-economics/statistical-review-2016/bp-statistical-review-of-world-energy-2016-full-report.pdf
21. Burkney T., Simon N. China's Global Renewable Energy Expansion How the World's Second-Largest National Economy is Positioned to Lead the World in Clear-Power Investment // Total Production of Energy and Its composition. 2017. URL: http://ieefa.org/wp-content/uploads/2017/01/Chinas-Global-Renewable-Energy-Expansion_January-2017.pdf
22. Energy outlook for Asia and the Pacific 2015. URL: https://www.adb.org/sites/default/files/publication/30429/energy-outlook.pdf

23. Herold D.K., Marolt P. (ed.) Online Society in China: creating, celebrating and instrumentalising the online carnival. London; N.Y.: Routledge, 2011. 210 p.
24. Networked Readiness Index // World Economic Forum. URL: http: //reports.weforum.org/global-information-technology-report-2016/networked-readiness-index/
25. The Global Cybersecurity Index (GCI) // ABI RESEARCH/ ITU Telecom. URL: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/WP-GCI-101.pdf
26. 溪洛渡水电站首台机组正式并网发电 // 北极星电力网新闻中心. 2013. 15 июля. URL: http://news.bjx.com.cn/html/20130715/445839.shtml

The importance of some national security challenges for the development of the economy of the People's Republic of China

Andrei A. Kapustin
Student,
Department of international relations and foreign policy of Russia,
Moscow State Institute of International Relations
of the Ministry of Foreign Affairs of the Russian Federation,
119454, 76 Vernadskogo av., Moscow, Russian Federation;
e-mail: mr.andreykapustin@yandex.ru

Anastasiya A. Rybalova
Student,
Department of oriental studies,
Moscow State Institute of International Relations
of the Ministry of Foreign Affairs of the Russian Federation,
119454, 76 Vernadskogo av., Moscow, Russian Federation;
e-mail: ar-editors@yandex.ru

Abstract

This article is devoted to the issue of a number of important challenges of the Chinese national security and the ways to mitigate this kind of risks. China is the largest modern economy, the world's top trade nation and still one of the fastest developing emerging countries. Beijing has been the most significant energy consumer since 2008. However, according to the analysis of the Chinese energy consumption structure, the primary resource is coal, that is why the country is now facing huge ecological problems. The second uncertainty is the necessity to diversify hydrocarbon imports in order to make the country less dependent on certain energy

exporters. Finally, China is striving to develop new energy technologies (or methods of production). Another important security issue is cyber security. China faces 3 major challenges in its attempts to maintain security in this sphere, which are information security in economics; cyber terrorism and protection of critical infrastructure; cultural expansion in the Internet. The article describes some instruments with the help of which Beijing preserves security in cyberspace and states the importance of cybersecurity for the Chinese economy.

For citation

Kapustin A.A., Rybalova A.A. (2017) Znachenie nekotorykh vyzovov natsional'noi bezopasnosti dlya razvitiya ekonomiki Kitaiskoi Narodnoi Respubliki [The importance of some national security challenges for the development of the economy of the People's Republic of China]. *Ekonomika: vchera, segodnya, zavtra* [Economics: yesterday, today and tomorrow], 7 (4A), pp. 258-271.

Keywords

National economy, Russia, China, energy security, renewables, energy balance, hydrocarbons, natural gas, information security, cyber security, cyber terrorism, critical infrastructure.

References

1. Alekseev G.F. et al. (2010) *Perspektivy energeticheskogo sotrudnichestva Rossiya–ATR: (v ekspertnykh otsenkakh)* [Perspectives of Russia-Asia-Pacific energy cooperation: (in expert assessments)]. Moscow: Academia Publ.
2. Anis'ko A.V. (2010) Kitai: problemy i perspektivy razvitiya toplivno-energeticheskogo kompleksa [China: problems and prospects for the development of the fuel and energy complex]. *Molodye vostokovedy stran SNG* [Young Orientalists of the CIS countries]. Moscow: IV RAN, pp. 7-24.
3. Aristova L.B., Luzyanin S.G., Semenova N.K., Tomberg I.R., Pan Davei, Sun' Yunsyan, Yan Yuili, Chzhan Tszyan'zhun, Li Lifan' (2014) *Potentsial i perspektiva sotrudnichestva KNR i RF v oblasti traditsionnoi i netraditsionnoi energii* [Potential and prospects for cooperation between China and Russia in the field of traditional and non-traditional energy]. Moscow: Center for Strategic Studies.
4. Borovskii Yu.V. (2011) *Sovremennye problemy mirovoi energetiki* [Modern problems of world energy]. Moscow: Navona Publ.
5. *BP Energy Outlook 2017 edition*. Available at: https: //www.bp.com/content/dam/bp/pdf/energy-economics/energy-outlook-2017/bp-energy-outlook-2017.pdf [Accessed 11/02/17].
6. *BP Energy Outlook 2035*. Available at: https: //www.bp.com/content/dam/bp/pdf/energy-economics/energy-outlook-2015/bp-energy-outlook-2035-booklet.pdf [Accessed 10/02/17].

7. *BP Statistical Review 2016*. Available at: https: //www.bp.com/content/dam/bp/pdf/energy-economics/statistical-review-2016/bp-statistical-review-of-world-energy-2016-full-report.pdf [Accessed 10/02/17].
8. Burkney T., Simon N. (2017) *China's global renewable energy expansion how the world's second-largest national economy is positioned to lead the world in clear-power investment. Total production of energy and its composition*. Available at: http://ieefa.org/wp-content/uploads/2017/01/Chinas-Global-Renewable-Energy-Expansion_January-2017.pdf [Accessed 16/02/17].
9. Chernenko E., Gabuev A. (2011) Oruzhie k boyu [Weapons to battle]. *Kommersant*" [Businessman], 26(4567), 15th February. Available at: https://www.kommersant.ru/doc/1585823 [Accessed 15/02/17].
10. *Energy outlook for Asia and the Pacific 2015*. Available at: https://www.adb.org/sites/default/files/publication/30429/energy-outlook.pdf [Accessed 15/02/17].
11. Evdokimov E. (2011) Politika Kitaya v global'nom informatsionnom prostranstve [China's policy in the global information space]. *Mezhdunarodnye protsessy* [International processes], 9-1(25). Available at: http://www.intertrends.ru/twenty-fifth/009.htm [Accessed 14/02/17].
12. Herold D.K., Marolt P. (ed.) (20110 *Online society in China: creating, celebrating and instrumentalising the online carnival*. London; N.Y.: Routledge Publ.
13. Ibragimova G. (2013) Strategiya KNR v oblasti upravleniya internetom i obespecheniya informatsionnoi bezopasnosti [China's strategy in the field of Internet governance and ensuring information security]. *Indeks Bezopasnosti* [Security Index], 1(104)-19, pp. 169-184.
14. Kolomychenko M. (2017) V internet vveli kibervoiska [Cyber-warfare entered the Internet]. *Kommersant*" [Businessman], 1st January, pp. 1. Available at: https://www.kommersant.ru/doc/3187320 [Accessed 14/02/17].
15. Korostikov M. (2015) Kitai pereprogrammiruet kiberprostranstvo [China reprograms cyberspace]. *Kommersant*" [Businessman], 19th October. Available at: http://www.kommersant.ru/doc/2835875 [Accessed 18/02/17].
16. Korsakov G. (2012) Informatsionnoe oruzhie superderzhavy [Information weapon of the superpower]. *Puti k miru i bezopasnosti* [Ways to peace and security], 1(42), pp. 34-59.
17. *Networked Readiness Index. World Economic Forum*. Available at: http: //reports.weforum.org/global-information-technology-report-2016/networked-readiness-index/ [Accessed 19/02/17].
18. Otkrytost' i vzaimodeistvie. Dykhanie Kitaya [Openness and interaction. The Breath of China] (2016). *Mezhdunarodnoe radio Kitaya* [International Radio of China], 5(15), pp. 4.
19. *Pol'zovateli interneta v mire* [Internet users in the world]. Available at: http://www.bizhit.ru/index/polzovateli_interneta_v_mire/0-404/ [Accessed 14/02/17].
20. Prognoz razvitiya energetiki mira i Rossii do 2040 goda [Forecast of the development of energy in the world and in Russia until 2040]. *Sait Analiticheskogo tsentra pri Pravitel'stve RF*

[Site of the Analytical Center under the Government of the Russian Federation]. Available at: http://ac.gov.ru/files/publication/a/2194.pdf [Accessed 19/02/17].

21. Rossiya ustupila pervoe mesto po postavkam nefti v Kitai [Russia gave the first place in oil supplies to China] (2017). *InvestBrothers*, 28th March. Available at: https://investbrothers.ru/2017/03/28/rf_ustupila_pervoe_mesto/ [Accessed 19/02/17].
22. Shul'tseva V. (2015) *Tsifrovaya ekonomika Kitaya. Ch. 1: Pervaya milya. 2015. Vyp. 4* [Digital Economy of China. Part 1: The first mile. 2015. Vol. 4]. Available at: http://www.lastmile.su/journal/article/4702 [Accessed 19/02/17].
23. Strany, iz kotorykh chashche vsego sovershayutsya khakerskie ataki [Countries from which hacker attacks are most often committed] (2013). *Rate1*, 17th August. Available at: http://www.rate1.com.ua/ehkonomika/tekhnologii/2708/ [Accessed 14/02/17].
24. The Global Cybersecurity Index (GCI). *ABI RESEARCH/ ITU Telecom*. Available at: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/WP-GCI-101.pdf [Accessed 14/02/17].
25. Zapad "proglotil" novyi kitaiskii zakon o kiberbezopasnosti [The West "swallowed" the new Chinese law on cybersecurity] (2016). *Mezhdunarodnoe radio Kitaya* [International Radio of China], 18th November. Available at: http://russian.cri.cn/3060/2016/11/18/1s592270.htm [Accessed 14/02/17].
26. 溪洛渡水电站首台机组正式并网发电 (2013). 北极星电力网新闻中心. 15th July. Available at: http://news.bjx.com.cn/html/20130715/445839.shtml [Accessed 14/02/17].