ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.94
DOI: 10.21822/2073-6185-2023-50-2-142-152 Обзорная статья / Review Paper

Формирование системы требований по обеспечению информационной безопасности на объектах критической информационной инфраструктуры в кооперации Российской Федерации и Китайской Народной Республики на примере газопровода «Сила Сибири»

А.Р. Семишкур, И.И. Лившиц
Национальный исследовательский университет ИТМО,
191002, г. Санкт-Петербург, ул. Ломоносова, 9, Россия

Резюме. Цель. Целью исследования является аналитический обзор законодательства для формирования системы требований по обеспечению и контролю информационной безопасности на объектах критической информационной инфраструктуры в кооперации Российской Федерации и Китайской Народной Республики. **Метод.** Проведен обзор с использованием различных методов сравнительного анализа для нахождения сходств и различий в подходах стран-партнеров в вопросе критической информационной инфраструктуры. **Результат.** Сформированы предложения по совершенствованию российского законодательства в сфере управления информационной безопасностью на объектах критической информационной инфраструктуры. **Вывод.** Направление данного исследования является весьма актуальным и требует дальнейшего развития организационно-технических мероприятий по реализации требований нормативно правовых документов по защите информации на объектах информатизации специального назначения.

Ключевые слова: критическая информационная инфраструктура, кооперация, контроль безопасности, информационная безопасность, требования

Для цитирования: А.Р. Семишкур, И.И. Лившиц. Формирование системы требований по обеспечению информационной безопасности на объектах критической информационной инфраструктуры в кооперации Российской Федерации и Китайской Народной Республики на примере газопровода «Сила Сибири». Вестник Дагестанского государственного технического университета. Технические науки. 2023; 50(2):142-152. DOI:10.21822/2073-6185-2023-50-2-142-152

Formation of a system of requirements for ensuring information security at critical information infrastructure facilities in cooperation between the Russian Federation and the People's Republic of China on the example of the Power of Siberia gas pipeline

A.R. Semishkur, I.I. Livshits
National Research University ITMO",
9 Lomonosov St., St. Petersburg 191002, Russia

Abstract. Objective. The purpose of the study is an analytical review of the legislation for the formation of a system of requirements for ensuring and controlling information security at critical information infrastructure facilities in cooperation between the Russian Federation and the People's Republic of China. **Method.** Reviewed using various benchmarking methods - historical, socio-cultural, legal to find similarities and differences in the approaches of partner countries on the issue of Critical Information Infrastructure. **Result.** Proposals have been made to improve Russian legislation regarding the management of information security at critical information infrastructure facilities. **Conclusion.** The direction of this study is very relevant and requires further development of organizational and technical measures to implement the requirements of legal documents on the protection of information at special-purpose informatization objects.

Key words: critical information infrastructure, cooperation, security control, information security, requirements

For citation: A.R. Semishkur, I.I. Livshits. Formation of a system of requirements for ensuring information security at critical information infrastructure facilities in cooperation between the Russian Federation and the People's Republic of China on the example of the Power of Siberia gas pipeline. Herald of Daghestan State Technical University. Technical Science. 2023; 50(2):142-152. DOI:10.21822/2073-6185-2023-50-2-142-152

Введение. На сегодняшний день российский магистральный газопровод для поставок газа в страны в страны Азиатско-Тихоокеанского региона «Сила Сибири» для большинства граждан является неоднозначным проектом. Объект, задуманный ещё в 1997 году [1], веденный в эксплуатацию только в 2019 году [2] постоянно сталкивался с различными преградами в момент реализации и, в последствии, во время работы газопровода. Примерами проблем, связанных с «Силой Сибири», могут послужить: подписание 30-летнего договора на поставку газа до завершения строительства проекта [3], не предоставление денежного аванса со стороны Китая на строительство[4]. Стоит также упомянуть, что по экономическим прогнозам полная окупаемость проекта наступит только к 2048 году [5], а действительная стоимость газа для китайской стороны изменчива и менее маржинальна, чем поставки в Европу [6]; к тому же не выполнен план на постройку трубопровода для Японии [7]. Однако, успешное завершение строительства и ввод в эксплуатацию «Силы Сибири» представляется ярким прецедентом и примером успешной кооперации на объекте критической информационной инфраструктуры на международной арене. Заинтересованность Китая и России в функционировании объекта неоспорима. Китай стремится сократить свою зависимость от угольной энергетики [8], диверсифицировать поставки природного газа [9] и устранить опору исключительно на внутренние ресурсы.

Россия, после событий 2014 и 2022 годов, окруженная санкциями, стремится найти надежных партнеров в Азиатско-Тихоокеанском регионе, но прежде всего стремится к расширению экономических связей с Китайской Народной Республикой, что указывается в энергетической стратегии страны до 2035 года[10].

Международное сотрудничество, в части объектов критической информационной инфраструктуры, становится толчком для формирования методик и мер реагирования на угрозы и инциденты информационной безопасности. Успешность проектов создает прецедент и стремление к воплощению новых планов, именно поэтому рассмотрение проекта «Сила Сибири», поиск ключевых методик контроля безопасности взаимодействия и своевременная реакция на данную потребность является актуальным, принимая во внимание напряженную международную ситуацию и диверсии на «Северных потоках»[11].

Постановка задачи. Целью исследования является аналитический обзор законодательства для формирования системы требований по обеспечению информационной безопасности на объектах критической информационной инфраструктуры в кооперации Российской Федерации и Китайской Народной Республики.

Международные события, а именно присоединение Крыма и Специальная военная операция, постепенно ослабляют традиционное восприятие Российской Федерации, как энергетической сверхдержавы в глазах мирового сообщества. Из-за политических разногласий вводятся санкции [12], разрываются крупные сделки, а также применяются искусственные механизмы сдерживания экономического благосостояния (отказ от импорта энергоресурсов, введения «заморозок» активов, усложнения схем оплаты в иностранной валюте [13]). Указанные меры сдерживания применяются государствами европейского и североамериканского сообщества и заставляют вспомнить о другом направлении развития и сотрудничества России как евразийского государства.

Поиск верного пути – объект многовековых споров, связанных с глубинными историческими предпосылками, географическим расположением и ментальностью населения[14]. «Особый путь», не похожий на остальные, видится единственно верным, особенно, когда западные соседи в очередной раз стремятся оборвать любые связи с нашей страной, а азиатские приспосабливаются к ситуации. Именно из-за этого экспорт российских энергоносителей в такой напряженный, в политическом плане, 2022 год, вырос на 38% по сравнению с 2021[15]. Азиатский поворот России необходим и перспективен. В «Энергетической стратегии Российской Федерации на период до 2035 года»[10] значительная часть внимания уделяется развитию экономических связей со странами Азиатско-Тихоокеанского региона, в особенности Китайской Народной Республики. Главная роль отводится экспорту энергоресурсов и основным продуктам экспорта топливо-энергетических комплекса – природному и сжиженному газу.

Данное сотрудничество важно не только для России. Генеральный секретарь КНР, Си Цзиньпин, сделал вывод о результатах сотрудничества в 2022 году: «в этом году китайско-российское экономическое и торговое сотрудничество неуклонно развивалось, были достигнуты новые успехи в энергетике, инвестициях, взаимообмене и других областях, что способствует общему развитию двух стран», а также выразил стремление к тесному практическому сотрудничеству и углублению всеобъемлющей стратегической координации в различных областях[16].

Однако стоит говорить не только об экономической выгоде, но и постепенном идеологическом сближении двух государств, совершившемся за последние годы. Позиция компартии КНР с начала СВО всегда оставалась нейтральной, а В.В. Путин в видеоконференции с генеральным секретарем Си заметил, что Москва и Пекин одинаково смотрят «на причины, ход и логику происходящей трансформации глобального геополитического ландшафта»[17]. Не мудрено, в XXI веке концепция биполярного мира – давно позабытое прошлое времен Холодной Войны, а стремление не повторять данный сюжет, активное развитие экономик и приход к многополярности – вот одна из основных целей всех потенциальных сверхдержав (США, КНР, ЕС, РФ, Индия). Очевидно, в своем несогласии с Соединенными Штатами и Евросоюзом, Россия и Китай нашли друг в друге союзника не только экономического, но и идеологического.

Методы исследования. Присущее обоим государствам постоянное стремление к укреплению экономического и политического суверенитета, идентичные идеи об уникальности пути развития удивительным образом проникают в сферу информационных технологий. Одним из очевидных примеров может послужить процесс балканизации интернета. Проект «Золотой щит» был запущен в Китае в 2003 году. В настоящее время файрвол блокирует более 600 000 веб-доменов [18], в том числе 135 из 1000 самых популярных веб-сайтов мира, тем самым становясь самой строгой и продвинутой системой интернет-цензуры в мире.

Законотворчество России определяет сходные направления деглобализации и суверенности интернета, но отстает в своей радикальности от китайского. Огораживание интернета началось в 2014, когда был дополнен закон «Закон об обработке персональных данных в информационно-телекоммуникационных сетях», ограничивающий хранение персональных данных российских пользователей территорией РФ и вступил в силу «Закон о блогерах», российский федеральный закон № 97-ФЗ от 5 мая 2014 г., впоследствии отмененный в 2017 году, но позволивший федеральной власти опробовать инструменты управления общественным мнением в сети. Окончательно независимость российского интернета утвердилась законом о «Суверенном интернете» от 2019-го года. Количество сайтов, заблокированных к доступу на территории страны около 606 345[19].

Действия правительства Китая и России по регулированию интернета схожи и в малых чертах большого целого:

1. Специально созданные государством организации для мониторинга интернета. В Китае такую роль выполняет – Бюро общественной информации и надзора за сетевой безопасностью, а в России – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). В обоих случаях, применяются другие силовые ведомства для расследования преступлений;
2. Создаются, или же существуют аналоги социальных сетей (в КНР – Sina Weibo, в РФ – VK, вместо Facebook), сайтов (в КНР – BiliBili, в РФ – RuTube, вместо YouTube) и поисковых систем (в КНР – Weibo, в РФ – Яндекс, вместо Google), которые пользуются популярностью или продвигаются исключительно внутри страны на замену иностранным аналогам. Тем самым, посредством «мягкой силы», граждане заключены в сообщества без возможности взаимодействовать с пользователями всего мира. Владельцам «аналогов» приходится выполнять требования властей из-за риска быть заблокированными;
3. Происходит блокировка популярных социальных сетей (Instagram, Twitter), иностранных новостных изданий (BBC News) и госорганов недружественных стран (ЦРУ США);
4. Превалирующее большинство интернет-СМИ имеют государственную поддержку. За материалы, противоречащие официальному мнению государства, следует блокировка [20] или статус иностранного агента[21];
5. Государство создает организации оплачиваемых (иногда прогосударственными пользователи становятся добровольно), активных в интернете патриотов для астротурфинга[22]. В КНР такими являются умаоданы (прям. пер. с кит. 50-центовая партия; неофициальное название китайских проправительственных блогеров и участников интернет-форумов, берут свое название от цены за один пост или комментарий, размещённый в интернете) и цзыганьу (прям. пер. с кит. самостоятельная пятёрка; неофициальное название китайских блогеров, поддерживающих в своих ресурсах и блогах правительство КНР, продвигают свои идеи бесплатно*)*, в России они представлены работниками Агентства интернет-исследований;
6. Реакция других стран на вышеперечисленные действия оборачивается блокировками СМИ, пользователей выступающих с пропагандой и или поддержкой действий Китая и России [23].

Все эти процессы идеологически сближают такие разные, с первого взгляда, страны. В контексте того, что госуправление проникло в интернет и саму информационную безопасность, стоит поговорить о явной приверженности КНР и РФ государственной системе управления безопасностью критической информационной инфраструктуры в таком же стиле.

Термин кибернационализм (*eng.* cyber-nationalism; см. новый национализм, цифровой национализм) окончательно не устоялся в научной среде, часто используется в контексте описания социальных взаимодействий между пользователями интернета, их поведения по отношению к пользователям из «стран-противников» и изъявлению мнения поддерживающего вектор государственной пропаганды и повестки. Как мы могли в этом убедиться выше, КНР и РФ действительно активны в этом направлении. Однако, также верно использование данного словосочетания для описания модели внутренней политики государства по отношению к защите критической информационной инфраструктуры.

Данный термин, как и остальные в русском переводе с приставкой кибер-, берет своё начало в американской научно-технической среде [24] и используется, в большинстве случаев, для описания не одобряемых американским научным сообществом действий. Его неоднократно использовали по отношению к осуждаемым либеральной повесткой государствам, но в особенности для Китая [25] и России [26].

Модель цифрового национализма характеризуется тотальным протекторатом сверху; подчинением индивидуальных предпринимателей и юридических лиц данного сектора государству; обязательной прозрачностью иностранных IT-компаний на внутреннем рынке;

верховенством государства по вопросам информационной безопасности, информационных систем, персональных данных, законодательно закрепленном в государственных документах стран [27]. Для понимания актуальности модели кибернационализма в законах Китая и России, необходимо выполнить их сравнение.

Проводя сравнительный анализ законов о критической информационной инфраструктуре в Российской Федерации – Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.17 N 187-ФЗ» [28] и Китайской Народной Республики – Государственный приказ № 745 от 17.08.21 [29] невозможно не заметить приверженности исполнения данной модели на практике. Тем самым, сравнение двух законодательных актов важно для понимания общности подходов и демонстрации, того, что система требований двух государств идеальна для диффузии и выведения общей методики по обеспечению безопасности объектов КИИ.

Список субъектов, определяемых, как часть КИИ в России (ст. 2. п. 8) гораздо шире, чем в Китае (гл. 1. ст. 2). Это объясняется большим количеством полезных ископаемых и ресурсов. РФ официально декларирует свой интерес к индивидуальным предпринимателям и юридическим лицам, когда КНР иносказательно приписывает все к лаконичной формулировке «объектам ИС, которые могут серьезно угрожать национальной безопасности, национальной экономике и средствам к существованию людей, а также общественным интересам в случае их повреждения, потери своих функций или утечки данных», тем самым немного иносказательно, но аналогично выражая свой контроль над данной сферой. Органы исполнительной власти, выполняющие надзор, защиту и реагирующие на компьютерные инциденты, связанные с КИИ в обоих случаях узконаправленны, а также очень специализированы. Они полностью отвечают запросам РФ (ст.6) и КНР (гл.1 ст.3) и были законодательно учреждены специально для регулирования данной сферы.

Определение объекта, как часть КИИ, в России проводится предприятиями самостоятельно, необходимо провести самостоятельную категоризацию и направить отчёт с полученным уровнем в «Государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак» (ст.7). В Китае нет категорирования по уровню значимости объекта. Государственная организация «Отдел по охране труда» самостоятельно рассматривает различные области инфраструктуры, создает для них перечень факторов и анализирует субъекты, а после уведомляет организации о присвоении статуса КИИ (гл.2). Данный подход видится нам более комплексным и вовлеченным в процесс безопасности.

Обязательства, права и обязанности субъектов КИИ для России изложены в ст.9. Постановления Китая (гл.3 ст.12-21) больше направлены на самоуправление внутри КИИ и малый контакт с контролирующими ведомствами, исключительно в крайних случаях возникновениях чрезвычайных происшествий и проблем с категоризацией. Данные меры азиатского партнера видятся намного более продуктивными, чем российские бюрократические обязанности о необходимости излагать все аспекты происходящего на объекте в вышестоящие органы. Разумная децентрализация и самоуправление – это эффективное средство к ослаблению бюрократии и большей производительности. Также в нормативно-правовых актах Китая симпатизирует пункт относительно наличия должного качества ПО.

Полное перечисление ответственности за несоблюдение законодательства относительно защиты объектов критической информационной инфраструктуры для России, по правовой традиции помещена в ТК ст.81[30]; ГК 1064, 1069 [31]; КоАП ст. 13.12.1-7[32]; УК. гл. 28., гл. 29. ст.274-276,283-84 [33]. Все наказания за несоблюдение закона в Китае (гл.5) описаны в самом документе, в отличие от РФ. Это обусловлено исключительно российской правовой традицией. Примечательно то, что в обеих странах (в России это введено только с Указом №250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»[34]) ответственными за инциденты оказываются специальные отделы и глава КИИ. Суммы штрафов за те же правонарушения в Китае значительно выше, а

срок исполнения уголовных преступлений серьезнее. Говоря о расследовании преступлений в КНР за неподчинение вышестоящим органам также наказуемо. Интересным аспектом закона показалось примечание о «беспристрастности» и отсутствии «фаворитизма» касательно выбора ПО или людей на работу что можно списать на китайскую специфику. Требования к системам безопасности и защиты на объектах КИИ России указаны в ст. 10 и Указе №250, а для Китая в гл.4. Складывается ощущение, что закон КНР намного более всеобъемлющь и выражает большую поддержку в защите КИИ. Законы по охране деятельности разными ведомствами присутствуют в обоих случаях, но правительство Китая намного сильнее выражает свою заинтересованность в безопасности своих объектов благодаря возмещению финансов (потраченных на проверку соответствиям) и призыву к кооперации между смежными сферами. Из-за наличия коммунистического «пятилетнего планирования» и плановой экономики в целом, освещается призыв к выполнению поставленных экономических и государственных задач. Призыв к покупке определенного ПО – отсутствует, ограничения на выбор производителя нет, поэтому владельцы объектов КИИ КНР вольны осуществлять закупку ПО самостоятельно, в то время как сейчас на повестке горячих обсуждений правительство РФ призывает в срочном порядке переходить на «доверенные программно-аппаратные комплексы», что вызывает очень много трудностей в накаленной экономической обстановке и отсутствии отечественных альтернатив [35]. Для экономики Китая выбраны приоритетные сферы, а именно энергетика и телекоммуникация, которые получают поддержку в исследованиях и улучшении ИБ, когда в России защита всей критической информационной инфраструктуры остается важной задачей.

Обсуждение результатов. Мы сравнили законы о КИИ Российской Федерации и Китайской Народной Республики. Складывается впечатление, что КНР выражает больше заботы и интереса о своих объектах критической информационной инфраструктуре (КИИ). Это можно списать на то, что их закон был выпущен только 17 августа 2021 года, однако в мае 2023 года появится дополнительный национальный стандарт «Технологии информационной безопасности и требования к защите критической информационной инфраструктуры» [36]. РФ представили свой документ 26 июля 2017 года, за это время появилось множество дополняющих нормативных документов, затрагивающие такие темы, как: правила категорирования, о регулировании ГосСОПКА, затрагивающие роль ФСБ и регуляционные аспекты ФСТЭК [37] и самый новейший Указ №250.

Можно заметить, что законы двух стран схожи, отвечают всем запросам правительства и подходят для специфики обоих стран. Тем самым, кооперация и близость по вопросу информационной безопасности в критической информационной инфраструктуре между Российской Федерацией и Китайской Народной Республикой представляется возможной. Однако, опираясь на более свежий закон Китая считаем необходимым выдвинуть несколько требований для улучшения законодательства России на основе выполненного сравнения.

1. **Свести к минимуму или полностью избавится от бюрократического, бумажного аспекта в области КИИ.** В обеих странах государственные организации – это та инстанция, перед которой необходимо отчитываться о состоянии объектов КИИ, но если внутреннее самоуправление в КНР намного свободнее и контакт с государством сведен исключительно к чрезвычайным происшествиям, проверкам (возмещаемым государством в финансовом плане) и изначальным процессом категоризации со стороны «Отдела по охране труда», то в РФ дела обстоят по-другому. Постоянные отчёты, требования, проверки и самостоятельная категоризация только усложняют жизнь объектов. Модернизация и упрощение этого важного для государства процесса может облегчить жизнь как самих владельцев КИИ, так и федеральных органов. Цифровизация данного процесса, большее участие государства для доказательства своей заинтересованности может кардинально изменить обстановку в данной сфере, сократить время реакции на инциденты и повысить уровень информационной безопасности

как одного объекта КИИ так и их совокупности в целом.

2. **Качество программного обеспечения.** Неоднократно упоминаемый в законодательных актах Китая пункт о выборе ПО надлежащего качества вызывает интерес, особенно потому что Россия сейчас оказалась в вынужденной ситуации необходимости перехода с средств защиты информации от «недружественных» стран на их аналоги или продукты отечественного производства. Уровень развития технологий в КНР не соизмерим с российским, они самостоятельно производят СЗИ и ПО, совершенно не нуждаясь в иностранных продуктах, а государство активно помогает с рекомендациями по выбору необходимых компонентов. В России же значительно ограничен круг отечественных разработчиков СЗИ и ПО надлежащего качества, отвечающие всем запросам объектов КИИ. Такая резкая необходимость перехода до 1 января 2025 года[34] только пугает, именно поэтому государству необходимо взять это направление под свой контроль, оказывать помощь объектам КИИ и развивать сферу информационных технологий для того чтобы отвечать запросам внутренней инфраструктуры.
3. **Использование искусственного интеллекта.** Данный пункт вытекает из двух предыдущих и связан с введением искусственного интеллекта, как инструмента контроля ИБ на объектах КИИ. Стоит отметить, что китайские эксперты в области информационной безопасности уже говорят о необходимости скорейшего освоения данного процесса и введения его на объекты КИИ на законодательном уровне [38]. Проекты по претворению данной идеи в жизнь уже отмечаются во многих странах. Именно поэтому в нашем процессе импортозамещения стоит приглядеться и к этой технологии, которая в будущем поможет укреплению безопасности на важных государственных объектах инфраструктуры.

Во-первых, это поможет перевести рядовых работников на борьбу с реальными атаками высокого уровня и повысить эффективности защиты.

Во-вторых, принять диверсифицированные алгоритмы и модели анализа угроз для формирования связи существующей системы защиты, например, путем строительства интеллектуального центра управления сетевой безопасностью, расширения возможностей оборудования безопасности с низким уровнем интеллекта и повысить уровень интеллекта системы защиты в целом.

В-третьих, активно тренировать технологии искусственного интеллекта для тестирования существующей системы защиты, чтобы разумно дополнять стратегию безопасности.

Вывод. Китайская Народная Республика, определенная как ключевой партнер Российской Федерации в настоящее время, демонстрируется государством близким по духу не только в экономическом, идеологическом, но и законодательном плане. Кажущаяся, с обывательской точки зрения, далекая ментальность и вынужденность данного союза предстает с радикально другой стороны.

Аналитический обзор, выполненный на стыке международных отношений и информационной безопасности, раскрывает более глубокие первопричины сходства и целей кооперации. Идеологическая близость находит свои отголоски и в государственном отношении к информационной безопасности объектов критической информационной инфраструктуры. Рассмотренные ключевые законы двух государств демонстрируют, что контроль безопасности также осуществляется по модели кибернационализма, однако для улучшения методики контроля безопасности считаем необходимым: цифровизировать процессы взаимодействия КИИ с государством; государству помочь КИИ с импортозамещением СЗИ и ПО, а также присмотреться к введению искусственного интеллекта для управления информационной безопасностью на объектах критической информационной инфраструктуры.

Библиографический список:

1. Визиты президентов России в КНР. Досье. 01.09.15 // Информационное агентство ТАСС: [Электронный ресурс]. Режим доступа: https://tass.ru/info/2226232 (дата обращения: 20.01.23).

2. Shabbir F. Putin, Xi Expected to Hold Teleconference for Launching Power of Siberia Dec 2 – Kremlin. 25.11.19 // Urdupoint: [Electronic source]. URL: www.urdupoint.com/en/business/putin-xi-expected-to-hold-teleconference-for-770525.html (accessed: 17.04.2021).
3. Alexey Miller: Russia and China signed the biggest contract in the entire history of Gazprom. 21.05.14 // Gazprom: [Electronic source]. URL: www.gazprom.com/press/news/2014/may/article191451/ (accessed: 31.01.2023).
4. Серов М. Китайцы не дали «Газпрому» денег на строительство «Силы Сибири». 24.09.14 // Ведомости: [сайт]. URL: www.vedomosti.ru/politics/articles/2014/09/24/gazoobraznye-dengi#ixzz3FSiSTTEW (дата обращения: 31.01.2023).
5. Фаляхов Р. Газ по телемосту: Путин и Си Цзиньпин запустили «Силу Сибири» 02.12.19 // Газета.ru: [сайт]. URL: www.gazeta.ru/business/2019/12/01/12841694.shtml (дата обращения: 31.01.2023).
6. Эксперт Понкратов рассказал, насколько выгоден для РФ китайский рынок газа. 24.03.22 // Regnum: [сайт]. URL: https://regnum.ru/news/economy/3543678.html (дата обращения: 31.01.2023).
7. Gas Will Be Delivered to Japan through Vladivostok.16.06.08 // Vladivostok Times: [Electronic source]. URL: https://web.archive.org/web/20090805160316/http://vladivostoktimes.com/show/?id=26289&p=2 (accessed: 31.01.2023).
8. A glut of new coal-fired power stations endangers China's green ambitions. 21.05.20 // The Economist: [Electronic source]. URL: www.economist.com/china/2020/05/21/a-glut-of-new-coal-fired-power-stations-endangers-chinas-green-ambitions (accessed: 31.01.2023).
9. Диверсификация источников энергии – залог дальнейшего развития энергетического сектора Китая. 17.01.23 // TVBrics: [сайт]. URL: https://tvbrics.com/news/diversifikatsiya-istochnikov-energii-zalog-dalneyshego-razvitiya-energeticheskogo-sektora-kitaya/ (дата обращения: 31.01.2023).
10. Энергетическая стратегия Российской Федерации на период до 2035 года // Официальный сайт Министерства энергетики Российской Федерации (Минэнерго России): [Электронный ресурс]. Режим доступа: https://minenergo.gov.ru/node/1026 (дата обращения: 20.01.23).
11. Шаипова М. Загадка о трубе: кто взорвал «Северный поток». 18.11.22 // Известия: [сайт]. URL: https://iz.ru/1427697/mariia-shaipova/zagadka-o-trube-kto-vzorval-severnyi-potok (дата обращения: 31.01.2023).
12. All sanctions // Datawrapper: [Electronic source]. URL: https://www.datawrapper.de/_/MGzSP/ (accessed: 01.02.2023).
13. Россия перевела расчеты за газ в рубли. Что это меняет для Европы // РБК: [Электронный ресурс]. Режим доступа: https://www.rbc.ru/business/31/03/2022/6245b6c39a7947e7182a7ff2 (дата обращения: 01.02.2023).
14. На трех стульях. Какой исторический путь выбирают россияне? // Проект «Россия будущего: 2017 → 2035»: [Электронный ресурс]. Режим доступа: http://2035.media/2017/10/24/russian-path/ (дата обращения: 01.02.2023).
15. Доходы России от экспорта энергоносителей в 2022 году выросли на 38%. 22.08.22 // Neftegaz.ru: [Электронный ресурс]. Режим доступа: https://neftegaz.ru/news/finance/747770-dokhody-rossii-ot-eksporta-energonositeley-v-etom-godu-vyrosli-na-38/ (дата обращения: 01.02.2023).
16. Главы государств Китая и России обменялись поздравлениями с Новым годом 《中俄两国元首互致新年贺电》. 31.12.22 // CCTV: [Электронный ресурс]. Режим доступа: https://news.cctv.com/2022/12/31/ARTIRKkLYDfjrf439iyWWxfy221231.shtml?spm=C94212.P4YnMod9m2uD.ENPMkWvfnaiV.138 (дата обращения: 05.01.2023).
17. США сделали предупреждение Китаю после беседы Си Цзиньпина с Путиным. 31.12.22 // РБК: [Электронный ресурс]. Режим доступа: https://www.rbc.ru/rbcfreenews/63af4d209a79472e12f0ed8c (дата обращения: 01.02.2023).
18. Список сайтов, заблокированных в Китае. 《中國封鎖之網站列表》.// ChinaVPN: [Электронный ресурс]. Режим доступа: https://www.chinavpn.tips/cn/websites-services-banned-in-china/ (дата обращения: 01.02.2023).
19. Мониторинг реестров // Роскомсвобода: [Электронный ресурс]. Режим доступа: https://reestr.rublacklist.net/ru/?status=1&gov=all&date_start=&date_end= (дата обращения: 01.02.2023).
20. Цензура (контроль) в интернете Опыт Китая // Tadviser : [Электронный ресурс]. Режим доступа: URL: http://fic.vscc.ac.ru/index.php?/forum/597 (дата обращения: 01.02.2023).
21. СМИ, заблокированные и закрытые в России после начала «военной спецоперации» на Украине // Такие Дела: [Эл.рес.]. Режим доступа: https://takiedela.ru/list/zablokirovannye-smi/ (дата обращения: 02.02.2023).
22. Бессчетнова А.А. Астротурфинг как социальная проблема современности // Форум интернет-конференций ВолНЦ РАН: [Эл. рес.]. Режим доступа: http://fic.vscc.ac.ru/index.php?/forum/597 / (дата обращения: 02.02.2023).
23. Meta заявила, что закрыла сети фальшивых аккаунтов, занимавшихся «тайными операциями распространения влияния» из Китая и России // Октагон: [Электронный ресурс]. Режим доступа:

https://octagon.media/novosti/meta_zayavila_chto_zakryla_seti_falshivyx_akkauntov_zanimavshixsya_tajnymi_operaciyami_rasprostraneniya_vliyaniya_iz_kitaya_i_rossii.html (дата обращения: 02.02.2023).
24. Марков А.С. Кибербезопасность и информационная безопасность как бифуркация номенклатуры научных специальностей // Вопросы кибербезопасности. 2022. N 1(47), С. 2-9.
25. Wu X. Chinese Cyber Nationalism: Evolution, Characteristics, and Implications. Lanham, MD: Lexington Books. p. 158.
26. Limonier K. Russia in Cyberspace: Issues and Representations // Cairn Info: [Electronic source]. URL: https://www.cairn-int.info/article-E_HER_152_0140--russia-in-cyberspace-issues.htm (accessed: 01.02.2023).
27. Alekseenko A. New Russian Model BIT and the Practice of Investment Arbitration. // Manchester Journal of International Economic Law 16(1) PP. 79-93.
28. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ
29. Положение о защите критической информационной инфраструктуры Государственный приказ № 745 от 17.08.21 《关键信息基础设施安全保护条例》// Государственный совет КНР: [Электронный ресурс]. Режим доступа: http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm (дата обращения: 19.01.22).
30. «Трудовой кодекс Российской Федерации» от 30.12.2001 N 197-ФЗ (ред. от 22.11.2021) (с изм. и доп., вступ. в силу с 30.11.2021).
31. «Гражданский кодекс Российской Федерации» [Электронный ресурс]. Режим доступа: https://base.garant.ru/10164072/ (дата обращения: 20.01.22).
32. «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 N 195-ФЗ (ред. от 30.12.2021) (с изм. и доп., вступ. в силу с 10.01.2022).
33. «Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ (ред. от 30.12.2021).
34. Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» // Официальный интернет-портал правовой информации: [Электронный ресурс]. Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202205010023 (дата обращения: 01.02.2023).
35. Доработанный текст проекта Постановления Правительства Российской Федерации «О порядке перехода субъектов критической информационной инфраструктуры на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры» (подготовлен Минпромторгом России 11.08.2022) // Гарант.ру: [Электронный ресурс]. Режим доступа: https://www.garant.ru/products/ipo/prime/doc/56833508/ (дата обращения: 01.02.2023).
36. Национальный стандарт «Технологии информационной безопасности и требования к защите критической информационной инфраструктуры» будет внедрен в мае следующего года 《信息安全技术 ▪键信息基础设施安全保护要求》国家标准将于明年5月实施// Государственный совет КНР: [Электронный ресурс]. Режим доступа: http://www.gov.cn/xinwen/2022-11/07/content_5725199.htm (дата обращения: 01.02.2023).
37. Нормативные документы о безопасности КИИ // КИИ 187-ФЗ: [Электронный ресурс]. Режим доступа: https://187.ussc.ru/blog/detail/normativnye-dokumenty-o-bezopasnosti-kii/ (дата обращения: 01.02.2023).
38. Точка зрения академика | Фэн Дэнго: три ключевые возможности для защиты безопасности критической информационной инфраструктуры《院士观点|冯登国：▪键信息基础设施安全保护三大▪键能力》// NetEase: [Электронный ресурс]. Режим доступа: https://baijiahao.baidu.com/s?id=1714661850130545665&wfr=spider&for=pc (дата обращения: 01.02.2023).

References:

1. Visits of Russian presidents to China. Dossier. 09/01/15 // TASS News Agency: [Electronic source]. URL: https://tass.ru/info/2226232 (accessed: 20.01.23). (In Russ)
2. Shabbir F. Putin, Xi Expected to Hold Teleconference for Launching Power of Siberia Dec 2 – Kremlin. 25.11.19 // Urdupoint: [Electronic source]. URL: www.urdupoint.com/en/business/putin-xi-expected-to-hold-teleconference-for-770525.html (accessed: 17.04.2021).
3. Alexey Miller: Russia and China signed the biggest contract in the entire history of Gazprom. 21.05.14 // Gazprom: [El.sou.]. URL: www.gazprom.com/press/news/2014/may/article191451/ (accessed: 31.01.2023).
4. Serov M. The Chinese did not give Gazprom money for the construction of the Power of Siberia. 24.09.14 Vedomosti: [Electronic source]. URL: www.vedomosti.ru/politics/articles/2014/09/24/gazoobraznye-dengi#ixzz3FSiSTTEW (accessed: 31.01.2023). (In Russ)
5. Falyakhov R. Gas via teleconference: Putin and Xi Jinping launched the “Power of Siberia”. 02.12.19 // Gazeta.ru: [Electronic source]. URL: www.gazeta.ru/business/2019/12/01/12841694.shtml (accessed: 31.01.2023). (In Russ)
6. Expert Ponkratov told how beneficial the Chinese gas market is for the Russian Federation. 24.03.22 // Regnum: [Electronic source]. URL: https://regnum.ru/news/economy/3543678.html (accessed: 31.01.2023). (In Russ)

7. Gas Will Be Delivered to Japan through Vladivostok.16.06.08 // Vladivostok Times: [Electronic source]. URL: https://web.archive.org/web/20090805160316/http://vladivostoktimes.com/show/?id=26289&p=2 (accessed: 31.01.2023). (In Russ)
8. A glut of new coal-fired power stations endangers China's green ambitions. 21.05.20 // The Economist: [Electronic source]. URL: www.economist.com/china/2020/05/21/a-glut-of-new-coal-fired-power-stations-endangers-chinas-green-ambitions (accessed: 31.01.2023).
9. Diversification of energy sources is the key to further development of the energy sector in China. 17.01.23 // TVBrics: [Electronic source] URL: https://tvbrics.com/news/diversifikatsiya-istochnikov-energii-zalog-dalneyshego-razvitiya-energeticheskogo-sektora-kitaya/ (accessed: 31.01.2023). (In Russ)
10. Energy strategy of the Russian Federation for the period up to 2035 // Official website of the Ministry of Energy of the Russian Federation (Ministry of Energy of Russia): [Electronic source]. URL: https://minenergo.gov.ru/node/1026 (accessed: 20.01.23). (In Russ)
11. Shaipova M. Riddle about the pipe: who blew up the Nord Stream. 18.11.22 // Izvestia: [Electronic source]. URL: https://iz.ru/1427697/mariia-shaipova/zagadka-o-trube-kto-vzorval-severnyi-potok (accessed: 31.01.2023). (In Russ)
12. All sanctions // Datawrapper: [Electronic source]. URL: https://www.datawrapper.de/_/MGzSP/ (accessed: 01.02.2023).
13. Russia has translated payments for gas into rubles. What does this mean for Europe? // RBK: [Electronic source]. URL: https://www.rbc.ru/business/31/03/2022/6245b6c39a7947e7182a7ff2 (accessed: 01.02.2023). (In Russ)
14. On three chairs. What historical path do the Russians choose? // Project "Russia of the Future: 2017 → 2035": [Электронный ресурс]. Режим доступа: http://2035.media/2017/10/24/russian-path/ (accessed: 01.02.2023). (In Russ)
15. Russia's energy export revenues grew by 38% in 2022.. 22.08.22 // Neftegaz.ru: [Electronic source]. URL: https://neftegaz.ru/news/finance/747770-dokhody-rossii-ot-eksporta-energonositeley-v-etom-godu-vyrosli-na-38/ (accessed: 01.02.2023). (In Russ)
16. The heads of state of China and Russia exchanged congratulations on the New Year《中俄两国元首互致新年贺电》. 31.12.22 // CCTV: [Electronic source]. URL: https://news.cctv.com/2022/12/31/ARTIRKkLYDfjrf439iyWWxfy221231.shtml?spm=C94212.P4YnMod9m2uD.ENPMkWvfnaiV.138 (accessed: 05.01.2023).
17. The United States issued a warning to China after Xi Jinping's conversation with Putin. 31.12.22// RBK: [Electronic source]. URL: https://www.rbc.ru/rbcfreenews/63af4d209a79472e12f0ed8c (accessed: 01.02.2023).
18. List of sites blocked in China. 《中國封鎖之網站列表》.// ChinaVPN: [Electronic source]. URL: https://www.chinavpn.tips/cn/websites-services-banned-in-china/ (accessed: 01.02.2023).
19. Monitoring registries // Roscomsvoboda: [Electronic source]. URL: https://reestr.rublacklist.net/ru/?status=1&gov=all&date_start=&date_end= (accessed: 01.02.2023).
20. Censorship (control) on the Internet Experience of China // Tadviser: [Electronic source]. URL: https://www.tadviser.ru/index.php (accessed: 01.02.2023).
21. Media blocked and closed in Russia after the start of the "military special operation" in Ukraine // Takie Dela: [Electronic source]. URL: https://takiedela.ru/list/zablokirovannye-smi/ (accessed: 02.02.2023). (In Russ)
22. Beschetnova A.A. Astroturfing as a social problem of our time. Forum of Internet Conferences VolRC RAS: [El. source]. URL: http://fic.vscc.ac.ru/index.php?/forum/597 (accessed: 02.02.2023). (In Russ)
23. Meta Says It Shut Down Networks of Fake Accounts Engaged in "Clandestine Spread of Influence Operations" from China and Russia // Octagon: [Electronic source]. URL: https://octagon.media/novosti/meta_zayavila_chto_zakryla_seti_falshivyx_akkauntov_zanimavshixsya_tajnymi_operaciyami_rasprostraneniya_vliyaniya_iz_kitaya_i_rossii.html (accessed: 02.02.2023). (In Russ)
24. Markov A.S. Cybersecurity and information security as a bifurcation of the nomenclature of scientific specialties. *Issues of cybersecurity.* 2022; 1(47): 2-9. (In Russ)
25. Wu X. Chinese Cyber Nationalism: Evolution, Characteristics, and Implications. Lanham, MD: Lexington Books. p. 158.
26. Limonier K. Russia in Cyberspace: Issues and Representations // Cairn Info: [Electronic source]. URL: https://www.cairn-int.info/article-E_HER_152_0140--russia-in-cyberspace-issues.htm (accessed: 01.02.2023).
27. Alekseenko A. New Russian Model BIT and the Practice of Investment Arbitration. Manchester Journal of International Economic Law 16(1):79-93.
28. Federal Law "On the Security of Critical Information Infrastructure of the Russian Federation" dated July 26, 2017 N 187-FZ
29. Regulation on the protection of critical information infrastructure State Order No. 745 dated 17.08.21 《关键信息基础设施安全保护条例》// State Council of the People's Republic of China: [Electronic source]. URL: http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm (accessed: 19.01.22).

30. "Labor Code of the Russian Federation" dated December 30, 2001 N 197-FZ (as amended on November 22, 2021) (as amended and supplemented, effective from November 30, 2021). (In Russ)
31. "Civil Code of the Russian Federation" .Base Garant: [Electronic source]. URL: https://base.garant.ru/10164072/ (accessed: 20.01.22). (In Russ)
32. "Code of the Russian Federation on Administrative Offenses" dated December 30, 2001 N 195-FZ (as amended on December 30, 2021) (as amended and supplemented, effective from January 10, 2022).
33. "Criminal Code of the Russian Federation" dated 06/13/1996 N 63-FZ (as amended on 12/30/2021).
34. Decree of the President of the Russian Federation of May 1, 2022 No. 250 "On additional measures to ensure the information security of the Russian Federation". Official Internet portal of legal information: [Electronic source]. URL: http://publication.pravo.gov.ru/Document/View/0001202205010023 (accessed: 01.02.2023). (In Russ)
35. The finalized text of the draft Decree of the Government of the Russian Federation "On the procedure for the transition of subjects of critical information infrastructure to the predominant use of trusted software and hardware systems at their significant objects of critical information infrastructure" (prepared by the Ministry of Industry and Trade of Russia on August 11, 2022) // Garant.ru: [Electronic source]. URL: https://www.garant.ru/products/ipo/prime/doc/56833508/ (accessed: 01.02.2023). (In Russ)
36. The national standard "Information security technologies and requirements for the protection of critical information infrastructure" will be implemented in May next year《信息安全技术 ▪键信息基础设施安全保护要求》国家标准将于明年5月实施// State Council of the People's Republic of China: [Electronic source]. URL: http://www.gov.cn/xinwen/2022-11/07/content_5725199.htm (accessed: 01.02.2023).
37. Regulatory documents on the safety of CII // CII 187-FZ: [Electronic source]. URL: https://187.ussc.ru/blog/detail/normativnye-dokumenty-o-bezopasnosti-kii/ (accessed: 01.02.2023).
38. Academician's point of view | Feng Denguo: Three Key Opportunities to Protect Critical Information Infrastructure Security《院士观点|冯登国：▪键信息基础设施安全保护三大▪键能力》// NetEase: [Electronic source]. URL: https://baijiahao.baidu.com/s?id=1714661850130545665&wfr=spider&for=pc (accessed: 01.02.2023).

Сведения об авторах:

Семишкур Алена Романовна, магистрантка, факультет безопасности информационных технологий; all7al@bk.ru

Лившиц Илья Иосифович, доктор технических наук, профессор; livshitz.il@yandex.ru

Information about the authors:

Alena R. Semishkur, Master's student, Faculty of Secure Information Technologies, all7al@bk.ru

Ilya I. Livshitz, Dr.Sci. (Eng.), Prof., Faculty of Secure Information Technologies, livshitz.il@yandex.ru

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/ Received 06.05.2023.

Одобрена после рецензирования/ Reviced 01.06.2023.

Принята в печать/ Accepted for publication 01.06.2023.