УДК 338.2; 338.49
DOI: http://dx.doi.org/10.15211/vestnikieran1202196102

Александр КОТОВ

РАЗВИТИЕ КРИТИЧЕСКИХ ИНФРАСТРУКТУР В ГЕРМАНИИ: ВЫХОД ИЗ ТЕНИ

Аннотация. *Эпидемия коронавируса по-новому выявила значимость критически важной инфраструктуры (КВИ) для развития экономики. В Германии официальная Стратегия, посвящённая управлению этими объектами, действует с 2009 г., но именно 2020 г. стал поворотным. В статье анализируется отражение концепции КВИ в различных отраслевых стратегиях ФРГ. Показано, что коронавирус стал катализатором формирования нового регулирования в информационно-коммуникационной отрасли. Отмечено, что обеспечение защиты критически значимых инвестиций открывает возможности для дальнейшего развития цифровой инфраструктуры. Автор делает вывод, что развитие КВИ и достижение технологического суверенитета в ключевых областях будет одним из приоритетов экономической политики ФРГ. В перспективе продолжится разработка новых инициатив Германией и стимулирование дальнейшего сотрудничества европейских государств друг с другом в этой сфере для обеспечения инвестиционного контроля в политико-хозяйственном пространстве ЕС.*

Ключевые слова*: Германия, критическая инфраструктура, отрасли, Европейский союз, кибербезопасность, стратегические инвестиции, иностранные инвестиции, технологический суверенитет.*

Критически важная инфраструктура в отраслевых стратегиях ФРГ

Обеспечение жизнестойкости систем, реализующих основные государственные функции, всё чаще ставится в центр внимания из-за эпидемии коронавируса[1]. Тема устойчивости КВИ на первый план выдвигает вопросы способности противостоять этой и другим опасностям и гибко на них реагировать[2]. Отметим, что одни из первых политических действий по защите критической инфраструктуры были предприняты в Германии в конце 1990-х гг. С созданием межведомственной рабочей группы в 1997 г. по инициативе Федерального министерства внутренних дел (BMI) была образована не только первоначальная организационная единица для защиты КВИ, но и акроним «KRITIS», который используется до сих пор[3]. В 2009 г. была принята федеральная «Национальная стратегия защиты критических инфраструктур», в которой кратко изложены цели и политико-стратегический подход федерального правительст-

© *Котов Александр Владимирович* – кандидат экономических наук, старший научный сотрудник Центра германских исследований Отдела страновых исследований ИЕ РАН. ***Адрес***: 125009, Россия, Москва, ул. Моховая, д. 11, стр. 3. ***E-mail***: alexandr-kotov@yandex.ru.

Статья поступила в редакцию: 25.01.2021.

[1] Williamson R.D. Morris J.C. Lessons from the COVID-19 Pandemic for Federalism and Infrastructure: A Call to Action // Public Works Management and Policy. 2021. №1. P. 6-12. DOI: 10.1177/1087724X20969165; Jovanović A., Klimek, P., Renn, O. et al Assessing resilience of healthcare infrastructure exposed to COVID-19: emerging risks, resilience indicators, interdependencies and international standards // Environment Systems and Decisions. 2020. №2. P. 252-286. DOI: 10.1007/s10669-020-09779-8

[2] Fekete A., Rhuner J. Sustainable Digital Transformation of Disaster Risk-Integrating New Types of Digital Social Vulnerability and Interdependencies with Critical Infrastructure // Sustainability. 2020. №12(22). P. 1-18. DOI: 10.3390/su12229324; Hauschild E. Herausforderung Sicherheit. Griephan Global Security. 2007. №1. P. 21-25.

[3] Was ist KRITIS? URL: https://ag.kritis.info/kritis/ (дата обращения 29.11.2020).

ва[1]. В Германии к КВИ относятся организации или объекты, имеющие важное значение для государства, отказ или нарушение работы которых может привести к долгосрочным перебоям в поставках, значительным сбоям в общественной безопасности или другим серьёзным нарушениям (энергетика, информационно-телекоммуникационные технологии (ИКТ), здравоохранение и др.)[2].

Стратегические документы из других областей политики затрагивают отдельные аспекты защиты КВИ. В «пилотном проекте пространственного планирования» потенциал территориально-ориентированных действий для предотвращения рисков был исследован с межотраслевой позиции обеспечения безопасности различных объектов[3]. Учёт межотраслевого подхода становится необходимым там, где вследствие пространственной близости различных инфраструктур сосредоточение внимания на отдельных отраслевых правилах безопасности недостаточно или может помешать выработке целостного решения.

Одной из стратегий реагирования на опасности, тесно связанные с защитой критических инфраструктур, является Стратегия кибербезопасности[4]. В ней основное внимание уделяется угрозам, исходящим от киберпространства. В контексте «Стратегии Германии по адаптации к изменению климата»[5] большую роль играет целый ряд различных явлений из спектра природных опасностей и мер соответствующей политики. «Стратегия безопасности для грузовых перевозок и логистики»[6] является примером отраслевого стратегического документа, который относится непосредственно к защите КВИ и напрямую к стратегии *KRITIS*. Она определяет значимость защиты критически важных инфраструктур для грузовых перевозок и логистики.

Активизация интереса к критически важной инфраструктуре: внешние и внутренние факторы

Эпидемия коронавируса обнаружила различные акценты в дискуссии в ФРГ по проблемам развития КВИ и, прежде всего, в сфере информационной безопасности. Толчком стал совместный доклад трёх федеральных ведомств, отвечающих за IT-безопасность в Германии, в котором было предупреждение об атаках на объекты критически важной инфраструктуры[7]. На восьми страницах Федеральная разведывательная служба (BND), Федеральное управление по защите конституции (*BfV*) и Федеральное управление по информационной безопасности (*BSI*) описывали, как будут действовать предполагаемые хакеры. Хотя в документе впрямую не упоминалось о происхождении хакерской группы, в докладе была ссылка на сообщения из США, которые «закрепили» группу за Россией.

Надо отметить, что многие публикации немецкой прессы, посвящённые на протяжении 2020 г. защите критически важных инфраструктур и взломам системно значимых компьютер-

[1] Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.html (дата обращения 29.11.2020).
[2] Kritische Infrastrukturen Definition und Übersicht. URL: https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/einfuehrung_node.html. (дата обращения 29.11.2020).
[3] Vorsorgendes Risikomanagement in der Regionalplanung. Modellvorhaben der Raumordnung (MORO). Bundesministerium für Verkehr und digitale Infrastruktur, Berlin, 2015. URL: http://www.agl-online.de/fileadmin/62agl/medien/Downloads/agl_PRC_MORO-Risiko_Endbericht_20150727web.pdf (дата обращения 29.11.2020).
[4] Cyber-Sicherheitsstrategie für Deutschland. Bundesministerium des Innern. Berlin, 2016. URL: https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf (дата обращения 29.11.2020).
[5] Deutsche Anpassungsstrategie an den Klimawandel. Bundesregierung, 2008. URL: https://www.bmu.de/fileadmin/bmu-import/files/pdfs/allgemein/application/pdf/das_gesamt_bf.pdf (дата обращения 29.11.2020).
[6] Sicherheitsstrategie für die Güter-verkehrs- und Logistikwirtschaft. Schutz kritischer Infrastrukturen und verkehrsträgerübergreifende Gefahrenabwehr. Bundesministerium für Verkehr und digitale Infrastruktur. Berlin, 2014. URL: https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/sicherheitsstrategie.pdf?__blob=publicationFile (дата обращения 29.11.2020).
[7] Kritische Infrastruktur: Behörden warnen vor Hackerangriffen. URL: https://www.br.de/nachrichten/deutschland-welt/kritische-infrastruktur-behoerden-warnen-vor-hackerangriffen (дата обращения 29.11.2020).

ных сетей, заканчивались практически в обязательном порядке упоминанием, что за этим якобы есть российский след. Так было с кибератакой на компьютерную систему отделения неотложной помощи университетской клиники Дюссельдорфа в сентябре 2020 г., когда врачи в течение 13 дней не могли должным образом получить доступ к рентгеновским снимкам и компьютерным томограммам. Прокуратура не определила происхождение кибератаки и продолжает расследовать нападения, но изначально предполагалось, что она идёт из России[1]. Специалисты энергосетей в начале ноября 2020 г. также ожидали атак именно из России на свои объекты, мотивируя тем, что на тот момент политическая ситуация в отношениях между Германией и Россией сильно обострилась[2].

На наш взгляд, в ФРГ, безусловно, есть естественное желание защитить потенциально важные системы перед внешней угрозой, откуда бы она ни исходила. Но не менее важна нацеленность этих публикаций на внутреннего потребителя, когда в условиях коронокризиса появилась возможность резко увеличить финансирование определённых систем. Обеспечение национальной безопасности открывает возможности для дальнейшего развития инфраструктуры, которая, цифровизируясь, открывается всё больше на внешний мир. Следует отметить, что в 2020 г. понятие критически важных инфраструктур пыталось «разбухать». Так, по словам президента Ассоциации сберегательных касс (*DSGV*) эти 378 банковских учреждений по всей Германии являются частью «критической инфраструктуры» во время эпидемии, т.к. две трети всех компаний в Германии их клиенты[3].

Федеральная ассоциация немецких компаний по переработке и утилизации стали (*BDSV*) выступила с обращением к Федеральному министерству внутренних дел оперативно предпринять общенациональное расширение сектора и отраслевую классификацию критически важных инфраструктур за счёт отрасли сортировки, переработки и утилизации отходов. В *BDSV* лоббировали позицию, что члены объединения являются важным межотраслевым звеном: они замыкают циклы, которые необходимо срочно поддерживать даже во время кризиса[4].

Министерство экономики и энергетики ФРГ очередной выпуск, посвящённый программе поддержки инновационного предпринимательства (*ZIM*), посвятило опыту поддержки проектов разработки решений безопасности для КВИ. Это может быть особенно важно для разнообразных потребностей малых и средних предприятий, не имеющим собственного IT-отдела, чтобы получать конкретные рекомендации для действий, подходящих на их уровень компетенций[5].

Сближение позиций в правительственной коалиции по вопросам развития ИКТ

Что касается собственно развития инфотелекоммуникационных технологий и профильной инфраструктуры, то нынешняя правительственная коалиция ФРГ согласилась с тем, что следует провести обзор политики безопасности производителей КВИ, например, в отношении развития сетей *5G*. Ранее ХДС/ХСС и СДПГ дискутировали о том, как внутри страны принимать решения об исключениях, поскольку *Huawei* создавал компоненты сетей *5G* дешевле,

[1] Hacker greifen Kliniken an. URL: https://www.faz.net/aktuell/wirtschaft/digitec/mehr-hacker-angriffe-auf-kliniken-und-kritische-infrastruktur-17062421.html (дата обращения 29.11.2020).
[2] Die Netzwerke im Blick behalten. URL: https://www.it-zoom.de/it-director/e/die-netzwerke-im-blick-behalten-26931/ (дата обращения 29.11.2020).
[3] Die Banken als kritische Infrastruktur. URL: https://www.neues-deutschland.de/artikel/1134596.coronakrise-die-banken-als-kritische-infrastruktur.html (дата обращения 29.11.2020).
[4] Corona: Stahlrecycling als kritische Infrastruktur. URL: https://www.stahleisen.de/2020/04/01/corona-stahlrecycling-als-kritische-infrastruktur/ (дата обращения 29.11.2020).
[5] IT-Sicherheit auch für die Kleinen. BMWi, ZIM-Erfolgsbeispiel. №56. URL: https://www.zim.de/ZIM/Redaktion/DE/Publikationen/Erfolgsbeispiele/Kooperationsnetzwerke/056-it-sicherheit-auch-fuer-die-kleinen.pdf?__blob=publicationFile&v=5 (дата обращения 29.11.2020).

но, возможно, менее надёжно, чем его конкуренты. Изначально в правительственной линии не было единства о том, как вести себя с китайской компанией. Канцлерин Ангела Меркель и министр экономики и энергетики Петер Альтмайер представляли позицию ХДС о том, что Германия, которая зависит от свободной торговли, не должна с самого начала исключать каких-либо производителей из разработки немецкой мобильной сети *5G* будущего. Министр иностранных дел Хайко Маас (СДПГ), в свою очередь, предостерегал от подобных шагов по отношению к Китаю. Аналогичную позицию занимала Федеральная разведывательная служба (*BND*). Её руководитель Бруно Каль называл сеть *5G* «самой значимой КВИ будущего» и указал, что китайские компании должны были бы иметь тесные контакты с официальным Пекином.

В период эпидемии следует констатировать сближение этих позиций навстречу друг другу. По словам депутата бундестага Торстена Фрая (ХДС), в настоящее время между ведомством федерального канцлера и соответствующими министрами существует консенсус в отношении того, что в закон следует включить возможность запрета на установку критически важных компонентов в случае возникновения противоречивых вопросов политики безопасности. Нильс Шмид (СДПГ), официальный представитель парламентской фракции по внешней политике, также заявил: «Коалиция в принципе согласна с тем, что критически важные инфраструктуры будут не только подлежать чисто техническому контролю безопасности в будущем, но и что надёжность политики безопасности производителей будет проверяться перед установкой компонентов». Важно отметить, что новая позиция правительственной коалиции, которая с высокой вероятностью станет соответствующей частью нового закона об IT-безопасности, – это не «против *Huawei*» в контексте её инициатив расширения *5G*, а более долгосрочный закон, объединяющий техническое и политическое регулирование для всех потенциально критических инфраструктур[1].

Усиление инвестиционного контроля во внешнеторговом регламенте ФРГ

Эпидемия и защита критически важных инфраструктур стимулировали ужесточение инвестиционного контроля во внешнеторговом праве Германии. После того как контроль над межотраслевыми инвестициями несколько раз ужесточался с момента поглощения *Kuka AG* китайским инвестором, федеральное правительство снова значительно расширило сферу его действия. В начале октября 2020 г. вступил в силу Регламент ЕС 2019/452 от 19 марта 2019 г.[2] Согласно нему в обновлённом Постановлении о внешней торговле (*Außenwirtschaftsverordnungen, AWV*) различаются две процедуры контроля инвестиций: отраслевой контроль инвестиций (§60 *AWV*) вступает в силу, когда иностранный инвестор приобретает не менее 10% прав голоса в компании по производству вооружений. Такое приобретение считается «неэффективным» до тех пор, пока Федеральное министерство экономики и энергетики (*BMWi*) не даст своего одобрения. С другой стороны, межотраслевой контроль инвестиций (§55 *AWV*) вступает в силу независимо от сектора и, в частности, если иностранный инвестор из государства, не являющегося членом ЕС, превышает пороговое значение в 10% или 25% прав голоса в немецкой целевой компании. Если *BMWi* считает, что транзакция влияет на общественный

[1] Ein letzter Berliner Streitpunkt zu Huawei. URL: https://www.stuttgarter-zeitung.de/inhalt.kritische-infrastruktur-5g-netz-ein-letzter-berliner-streitpunkt-zu-huawei.be2120dc-0319-4abf-8181-bec94046b949.html (дата обращения 29.11.2020); IT-Sicherheitsgesetz 2.0: Dritter Referentenentwurf. URL: https://www.vde.com/topics-de/digital-security/aktuelles/cybersecurity-recht/it-sicherheitsgesetz-2-0-dritter-referentenentwurf (дата обращения 29.11.2020).

[2] Verordnung (EU) 2019/452 des Europäischen Parlaments und des Rates vom 19. März 2019. URL: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:32019R0452 (дата обращения 29.11.2020); Белов В.Б. Контроль за стратегическими прямыми инвестициями в ЕС // Европейский Союз: факты и комментарии. 2020. №100. С. 59-64. DOI: 10.1521/eufacts220205964

порядок или безопасность ФРГ, могут быть приняты ограничительные меры (вплоть до запрета на транзакцию). Какое именно из пороговых значений используется, зависит от того, включён ли сектор целевой компании в каталог отраслей КВИ. Само федеральное правительство ожидает увеличения примерно на 20 подобных процедур в год[1].

Кроме того, процессуальные сроки могут быть продлены и приостановлены – период исследования также может быть начат заново. Помимо этого запрещается передавать покупателю информацию и технологии, связанные с компанией, до или во время текущего процесса проверки. Новые группы случаев связаны с пандемией COVID-19 и в первую очередь относятся к компаниям из сектора здравоохранения (например, производители средств защиты, производители основных лекарственных средств и вакцин). Органы управления впервые получат возможность тестировать критерии проверки, связанные с инвесторами. Например, *BMWi* сможет принять во внимание, находится ли потенциальный покупатель под контролем третьей страны или он уже участвовал в деятельности, которая оказала влияние на общественный порядок или безопасность. Ожидается, что в ближайшие месяцы будут внесены дополнительные корректировки, и что каталог будет дополнен другими ключевыми направлениями (например, искусственным интеллектом, робототехникой и полупроводниками)[2].

Также в рамках новых правил инвестиционного контроля предусмотрен обмен информацией между странами – членами ЕС и Европейской комиссией в дополнение к требованию национального одобрения при 25%-ном участии через соответствующие транзакции в Европе. Целью является скоординированный контроль прямых иностранных инвестиций на всей территории ЕС. У других стран – членов сообщества и Комиссии ЕС имеется 35 дней, чтобы прокомментировать планируемое инвестиционное решение. Таким образом, страны ЕС, формально не препятствуя иностранным инвестициям как таковым, одновре́менно вполне естественно создают условия для предотвращения угроз безопасности или стимулирования инвестиций из третьих стран в критически важные инфраструктуры и технологии (оборона, энергетика, цифровая инфраструктура, водоснабжение разработка вакцин, лекарств, медицинских изделий и средств индивидуальной защиты и др.).

* * *

Дальнейшая разработка политики Германии по защите КВИ будет продолжена. Европейский союз также предполагает оказывать значительное влияние на защиту аналогичных инфраструктур в государствах-членах, особенно в связи с заключённым всеобъемлющим инвестиционным соглашением с Китаем[3]. Основой будут предложения по дальнейшим законодательным актам по защите КВИ, сетевой и информационной безопасности. Эти инициативы активно поддерживаются и в значительной степени формируются германской стороной в рамках новой промышленной стратегии[4]. Ожидается, что Германия также будет способствовать сотрудничеству государств-членов друг с другом и с ЕС, будь то в ходе дальнейшего раз-

[1] Auswirkungen der EU-Screening-Verordnung und verschärften Investitionskontrolle. URL: https://www.investmentplattformchina.de/die-neue-eu-screening-verordnung-und-verschaerfte-investitionskontrollen/ (дата обращения 29.11.2020).
[2] Die Verschärfung der Investitionskontrolle im Außenwirtschaftsrecht. URL: https://www.menoldbezler.de/de/aktuelles/die-verschaerfung-der-investitionskontrolle-im-aussenwirtschaftsrecht (дата обращения 29.11.2020).
[3] «Wird unsere Position verbessern»: Europäische Wirtschaft lobt Investitionsabkommen trotz Defiziten. URL: https://www.handelsblatt.com/politik/international/china-und-eu-wird-unsere-position-verbessern-europaeische-wirtschaft-lobt-investitionsabkommen-trotz-defiziten/26843494.html?ticket=ST-10376244-d6qwrOVOL93025EnbJlc-ap3 (дата обращения 29.11.2020).
[4] Белов В.Б. Германия – сложный поиск новой промышленной стратегии // Современная Европа. 2019. №4(90). С. 27-37. DOI: 10.15211/soveurope420192736

вития «Европейской программы защиты критически важных инфраструктур»[1] или в связи с темами управления стихийными бедствиями или в рамках программ НАТО. В этом случае целесообразно говорить о переплетении вопросов технологической, военной безопасности, гражданской защиты, практическая реализация которых отражает интересы по защите КВИ в Германии в обозримом будущем.

Список литературы

Белов В.Б. Германия – сложный поиск новой промышленной стратегии // Современная Европа. 2019. №4(90). С. 27-37. DOI: 10.15211/soveurope420192736

Белов В.Б. Контроль за стратегическими прямыми инвестициями в ЕС // Европейский Союз: факты и комментарии. 2020. №100. С. 59-64. DOI: 10.1521/eufacts220205964

Современная Германия: экономика и политика / под общ. ред. В.Б. Белова. М.: ИЕ РАН; «Весь мир», 2015.

References

Belov, V.B. (2019). Germanija – slozhnyj poisk novoj promyshlennoj strategii [Germany – a challenging search for a new industrial strategy]. Sovremennaja Evropa [Contemporary Europe]. 4 (90). P. 27-37. (In Russian). DOI: 10.15211/soveurope420192736

Belov, V.B. (2020). Kontrol’ za strategicheskimi prjamymi investicijami v ES [Control over strategic direct investment in the EU]. Evropejskij Sojuz: fakty i kommentarii [European Union: facts and comments]. 100. P. 59-64. (In Russian). DOI: 10.1521/eufacts220205964

Belov, V. B. (ed.) (2015). Sovremennaya Germaniya: ekonomika i politika [Modern Germany: Economics and Politics]. Moscow: Institut Evropy RAN; «Ves’ mir». (In Russian).

Fekete, A., Rhuner, J. (2020). Sustainable Digital Transformation of Disaster Risk-Integrating New Types of Digital Social Vulnerability and Interdependencies with Critical Infrastructure. Sustainability. 2020. 12(22). P. 1-18. DOI: 10.3390/su12229324

Hauschild, E. (2007). Herausforderung Sicherheit [Security challenge]. Griephan Global Security. 1. P. 21-25. (In German).

Jovanović, A., Klimek, P., Renn, O. et al (2020). Assessing resilience of healthcare infrastructure exposed to COVID-19: emerging risks, resilience indicators, interdependencies and international standards. Environment Systems and Decisions. 40(2). P. 252-286. DOI**:** 10.1007/s10669-020-09779-8

Williamson, R.D. Morris, J.C. (2021). Lessons from the COVID-19 Pandemic for Federalism and Infrastructure: A Call to Action. Public Works Management and Policy. 26(1). P. 6-12. DOI: 10.1177/1087724X20969165

Development of Critical Infrastructures in Germany: Out of the Shadow

Author. Alexander Kotov, Candidate of Science (Economics), Senior Researcher, Center for German Studies, Department for Countries Studies, Institute of Europe, Russian Academy of Sciences. **Address**: 11-3, Mokhovaya str., Moscow, Russia, 125009. **E-mail**: alexandr-kotov@yandex.ru.

Abstract. The coronavirus epidemic has redefined the importance of critical infrastructure for economic development. In Germany, formally, the Strategy for the Protection of Critical Infrastruc-

[1] EU grants €38 million for protection of critical infrastructure against cyber threats URL: https://ec.europa.eu/digital-single-market/en/news/eu-grants-eu38-million-protection-critical-infrastructure-against-cyber-threats (дата обращения 29.11.2020).

ture has been in effect since 2009, but it was 2020 that became a turning point. The article analyzes the reflection of the concept of critical infrastructure in various sectoral strategies of Germany. The paper demonstrates that the Coronavirus has become a catalyst for the folding of new regulation in the information and communication industry. It is emphasized that ensuring the protection of critical investments opens up opportunities for the further development of digital infrastructure. The author concludes that the development of critical infrastructures and the achievement of technological sovereignty in key areas will be one of the priorities of the Germany`s economic policy. Most likely, an active proposal of new initiatives by Germany and stimulation of further cooperation of European states with each other in this area is expected to ensure investment control in the political and economic space of the EU.

Key words: Germany, critical infrastructure, industries, European Union, cybersecurity, strategic investment, foreign investment, technological sovereignty.

DOI: http://dx.doi.org/10.15211/vestnikieran1202196102