УДК-327.7
DOI: 10.17072/2218-1067-2018-3-5-18

КИБЕРБЕЗОПАСНОСТЬ: ПРОБЛЕМЫ ФОРМИРОВАНИЯ ЕДИНОЙ ПОЛИТИКИ В ЕВРОПЕЙСКОМ СОЮЗЕ

В. И. Пантин, Н. В. Кардава[1]

Цель статьи – анализ наиболее сложных и актуальных проблем обеспечения кибербезопасности в странах ЕС и формирования единой политики в этой сфере. Рассмотрены общие политические и экономические факторы актуализации проблем кибербезопасности на национальном, наднациональном и глобальном уровнях. На примере Германии показано, что политика в сфере обеспечения кибербезопасности в ряде развитых стран ЕС более эффективна, чем политика на наднациональном общеевропейском уровне. Сделан вывод, что отличительной чертой немецкого подхода к обеспечению кибербезопасности является его комплексный и фундаментальный характер; этот подход включает целую систему нормативных актов, планов и институтов. Выявлены основные подходы, тенденции и противоречия, связанные с выработкой на наднациональном уровне ЕС единой стратегии в области кибербезопасности. Проанализированы основные документы и действия Европейской комиссии и других органов ЕС в этой области, включая киберстратегию ЕС (2013 г.), директиву ЕС по кибербезопасности (2016 г.), общий регламент ЕС о защите данных (2018 г.). Вместе с тем показано, что значительная активность руководящих органов ЕС в сфере обеспечения кибербезопасности сталкивается с неспособностью ряда стран выполнить все директивы, распоряжения, регламенты и другие нормативные акты. Определены наиболее серьезные препятствия на пути осуществления общей политики в области обеспечения кибербезопасности в ЕС: различный уровень экономического, технологического и социального развития входящих в него стран, несовпадение интересов различных политических акторов, разные подходы отдельных государств ЕС к регулированию киберпространства, сложности координации политики в сфере кибербезопасности. Сделан вывод, что эти препятствия связаны прежде всего с недостаточной сформированностью едино-

[1] Пантин Владимир Игоревич – заведующий отделом сравнительных политических исследований Национального исследовательского института мировой экономики и международных отношений им. Е.М. Примакова РАН, доктор философских наук. E-mail: v.pantin@mail.ru (ORCID: 0000–0002–4218–4579. Researcher ID: K–5736–2017).

Кардава Николай Вахтангович – младший научный сотрудник отдела сравнительных политических исследований Национального исследовательского института мировой экономики и международных отношений им. Е.М. Примакова РАН. E-mail: kardava98@mail.ru.

го политического пространства в ЕС. В то же время вероятно, что проблемы кибербезопасности будут способствовать более ускоренному и эффективному формированию такого пространства на наднациональном уровне. Кроме того, по мнению авторов, некоторые шаги ЕС по обеспечению кибербезопасности при соответствующей их адаптации и корректировке могут быть полезными для России.

Ключевые слова: Европейский союз; Германия; регулирование киберпространства; общая политика; кибербезопасность; киберугрозы; наднациональное политическое пространство.

Актуализация проблем кибербезопасности: политические и экономические аспекты

В настоящее время в связи с бурным развитием информационных технологий и их использованием многочисленными акторами для достижения своих политических, экономических и других целей проблемы обеспечения кибербезопасности выходят на первый план. Это связано с тем, что в глобальном киберпространстве, которое стало важнейшим полем информационной, политической, экономической и культурной конкуренции, сталкиваются интересы различных политических акторов, включая государства и союзы государств, корпорации, финансовые группы, политические партии и движения, неправительственные организации, другие группы интересов. Кроме того, в киберпространстве активно действуют различные криминальные группы (хакеры) и международные террористы, осуществляется экономический и военный шпионаж, делаются попытки вывести из строя целые предприятия и объекты инфраструктуры [2, 125–127; 10, 2]. По своим последствиям экономический, политический и военный ущерб от кибератак может превышать потери от экономических санкций и даже от военных конфликтов. Так, по данным Интерпола в Европе в 2012 г. совокупный ущерб, причиненный киберпреступностью, достиг ошеломляющих размеров в 750 млрд евро[1]. По данным специалистов Совета Европы в начале 2000-х гг. ущерб в европейских странах от вирусных атак ежегодно составлял около 12 млрд долл., а от нарушения прав интеллектуальной собственности – порядка 250 млрд долл. [7].

Кибербезопасность – достаточно широкое понятие, которое подразумевает различные средства и подходы к обеспечению безопасности в киберпространстве. Согласно определению Международного союза электросвязи, кибербезопасность представляет собой набор средств, стратегии и принципы

[1] Киберпреступления обходятся в миллиарды евро. 21.04.2016. [Kiberprestupleniya obhodyatsya v milliardy evro. [The cost of cybercrimes is milliards euro]. Available at: URL: https://europulse.ru/news/kiberprestupleniya-obhodyatsya-v-milliardyi-evro (accessed: 14.06.2018).

обеспечения безопасности, гарантии безопасности, подходы к управлению рисками, действия и практический опыт, страхование и технологии, которые могут быть использованы для защиты киберсреды, ресурсов организации и пользователя. Кибербезопасность включает меры защиты и действия, позволяющие осуществить защиту киберпространства как в гражданской, так и в военной области от таких угроз, которые связаны с его взаимозависимыми сетями и информационной инфраструктурой или могут нанести им урон [2, 133].

Помимо кибератак, связанных с деятельностью хакеров, киберпреступников, вымогателей, международных террористов, все более актуальной становится также проблема защиты личных данных пользователей социальных сетей от скрытого сбора информации. Эта информация, учитывающая индивидуальные предпочтения, вкусы и наклонности индивидуальных пользователей сети, широко используется при распространении контактной рекламы, интернет-продаж, а также, что немаловажно, в политических целях, например, в ходе избирательных кампаний. Одним из характерных примеров массового использования данных пользователей социальных сетей в политических целях является предвыборная кампания Д. Трампа в 2016 г.: использование этих данных сыграло немалую роль в его победе на президентских выборах в США. При этом разделить собственно киберпреступность, деятельность спецслужб и использование данных пользователей компьютерных сетей в политических целях становится все труднее. Так, Агентство национальной безопасности (АНБ) в США активно использует базы личных данных для слежки за многими миллионами людей, шантажа политических деятелей и организации в других странах различного рода внутренних переворотов и «цветных революций». В частности, АНБ установило «жучки» в кабинетах представительства ЕС в Вашингтоне, штаб-квартире ООН в Нью-Йорке и Совета ЕС в Брюсселе. Прослушке с использованием компьютерных устройств также подвергались 38 посольств и миссий различных стран в Нью-Йорке и Вашингтоне. К числу самых громких дипломатических скандалов относятся выявленные прослушки телефонных переговоров президента Бразилии Дилмы Русефф и канцлера Германии Ангелы Меркель, а также перехват защищенной спутниковой связи с Москвой президента РФ Д.А. Медведева из Лондона во время саммита G20 в апреле 2009 г. [2, 127].

Учитывая сказанное, можно констатировать, что проблемы обеспечения кибербезопасности остро стоят как перед рядовыми гражданами, так и перед всеми, даже самыми мощными государствами и союзами государств, политическими и государственными деятелями, корпорациями и финансовыми структурами. В то же время в современном мире согласованные действия разных стран по обеспечению кибербезопасности на наднациональном и тем более на глобальном уровне сталкиваются с многочисленными препятствиями, включая различие интересов государств и других политических акторов, разный уровень технического, экономического, социального развития, использование кибер-

пространства государствами и транснациональными корпорациями в целях экономического и иного шпионажа и др. В этой связи весьма значимым представляется вопрос о том, как развитие наднациональных политических пространств влияет на решение проблем кибербезопасности, равно как и вопрос об обратном влиянии проблем обеспечения кибербезопасности на формирование и развитие наднациональных политических пространств. Поскольку Европейский союз представляет собой весьма важный и характерный пример развития такого наднационального политического пространства, в данной статье рассмотрены основные проблемы, тенденции и противоречия, связанные с формированием единой политики ЕС в области обеспечения кибербезопасности. Некоторые из шагов ЕС по защите европейского киберпространства могут также представлять значительный интерес для России и других стран – членов Евразийского экономического союза.

Национальные и общеевропейская стратегии по кибербезопасности

Принципиально важной научно-теоретической и практически-политической проблемой является вопрос о соотношении национальных и общеевропейской стратегий в области обеспечения кибербезопасности. Острота этой проблемы во многом определяется тем, что страны ЕС сильно различаются по уровню социально-экономического и технологического развития; в связи с этим в целом ряде стран ЕС национальная стратегия по кибербезопасности либо разработана в недостаточной степени, либо существует главным образом на бумаге или на электронном носителе. При этом, несмотря на требования Европейской комиссии ко всем государствам ЕС как можно быстрее разработать национальные стратегии обеспечения кибербезопасности, многие страны разработали подобную стратегию во многом формально, без создания соответствующих инструментов ее реализации. Помимо прочего, это связано с тем, что выработка и использование таких инструментов требует затраты немалых финансовых средств, которую в существующих условиях долгового кризиса не могут себе позволить наиболее бедные страны Евросоюза, такие как Болгария, Румыния, Греция, Португалия и ряд других государств. Кроме того, налицо существенные различия между странами ЕС в использовании Интернета и в уровне развития цифровой экономики.

Одним из возможных способов сравнения разных стран по уровню обеспечения кибербезопасности может служить так называемый глобальный рейтинг кибербезопасности, который учитывает показатели данной страны в следующих пяти сферах: 1) правовые нормы в области кибербезопасности и их выполнение; 2) технические меры и наличие соответствующих инструментов для их реализации; 3) организационные меры в сфере кибербезопасности; 4) развитие потенциала кибербезопасности и 5) участие в международном сотрудничестве по ее обеспечению [1, 30]. Согласно глобальному рейтингу кибербе-

зопасности 2015 г., наиболее продвинутыми в области разработки и применения национальных стратегий кибербезопасности среди стран – членов ЕС являются Норвегия, Эстония, ФРГ, Австрия, Венгрия, Нидерланды [1, 14]. Отдельно стоит Великобритания с ее относительно благополучной ситуацией в области кибербезопасности; вместе с тем, по итогам Brexit Великобритания находится в процессе выхода из ЕС, хотя формально пока что остается его членом. В то же время в десятку наиболее передовых стран мира в области обеспечения кибербезопасности среди европейских стран по глобальному рейтингу 2015 г. входили лишь Норвегия (6-е место), Эстония (9-место) и ФРГ (10-е место). Наименее благополучными в плане кибербезопасности среди стран, входящих в ЕС, являются Румыния, Болгария, Бельгия, Португалия, Греция [1, 15]. Несмотря на то, что обеспечение кибербезопасности среди стран ЕС в целом коррелирует с уровнем их экономического развития, встречаются также и исключения: некоторые экономически развитые и богатые страны, например, Бельгия, Люксембург, Лихтенштейн, Ирландия, Исландия, в области киберзащиты находятся в одном ряду с такими странами, как Румыния, Болгария, Албания, Македония.

Особый интерес для России представляет опыт и практики обеспечения кибербезопасности в таких крупных и передовых в этой области странах, как ФРГ. При этом следует иметь в виду, что экономика Германии находится в эпицентре различного рода кибератак и промышленного шпионажа и заметно страдает от них, поэтому вопрос кибербезопасности для нее является одним из ключевых. Так, ущерб немецкого бизнеса от различного рода электронных преступлений (кража данных, шпионаж и саботаж) составлял по некоторым оценкам 51 млрд евро в 2015 г. и 55 млрд евро в 2016 г. Соответственно в Германии разработана и постоянно совершенствуется система киберзащиты, призванная противостоять кибератакам и другим угрозам информационной инфраструктуры.

Следует отметить, что отличительной чертой немецкого подхода к обеспечению кибербезопасности является его комплексный и фундаментальный характер, он включает целую систему нормативных актов, планов и институтов, призванных реализовывать эти планы. Еще в 2005 г. в ФРГ был разработан и принят «Национальный план защиты информационной инфраструктуры», а в 2007 г. – «План реализации защиты критических элементов инфраструктуры». Эти документы, разработанные при участии правительства, бизнеса и других структур, определяют общую стратегию реагирования на кризисы в сфере информационных технологий и содержат рекомендации бизнес-сообществу по действиям в случае крупных кибератак. Согласно этим документам, операторы разрабатывают и должны применять соответствующие процедуры раннего оповещения, причем в документах четко определены структуры и лица, которые информируются, в первую очередь, после обнаружения и фиксации той или иной кризисной ситуации. Кроме того, в «Плане реализации защиты критиче-

ских элементов инфраструктуры» содержатся указания по созданию рабочих групп по различным аспектам кибербезопасности, включая кризисное управление, проведение антикризисных учений, обеспечение постоянной доступности критически важных сервисов.

Созданное в 1991 г. Федеральное управление по информационной безопасности Германии (BSI), которое представляет собой составную часть МВД, является главным органом, ответственным за национальную кибербезопасность ФРГ. Этот орган формирует политику и план действий в области информационной безопасности с целью предотвращения, определения и реагирования на инциденты и кризисы в этой сфере. BSI, в частности, выпускает предупреждения и оповещения о вирусах и других вредоносных программах в ИТ-продуктах и услугах, дает рекомендации по противодействию вредоносным программам и действиям, а также организует информационный обмен с более чем 50 000 негосударственных организаций, включая малый и средний бизнес.

В 2011 г. в ФРГ была принята новая Федеральная стратегия кибербезопасности, которая призвана обеспечить многосторонний межведомственный подход к обеспечению безопасности в киберпространстве на национальном уровне [3]. Стратегия ориентирована прежде всего на защиту критически важных информационных структур и на выявление дополнительных возможностей в сфере обеспечения бескризисного функционирования информационной инфраструктуры Германии. Среди наиболее важных направлений Федеральной стратегии можно выделить следующие:

- безопасность информационных технологий в Германии осуществляется на основании совместной деятельности гражданского общества и государства, при этом комплекс инструментов защиты от киберугроз постоянно расширяется;

- с помощью Национального центра кибербезопасности (Nationales Cyber-Abwehrzentrum, NCAZ) происходит оптимизация оперативного сотрудничества между всеми органами государственной власти и обеспечивается защита от кибератак критически значимых объектов национальной ИТ-инфраструктуры и экономики;

- координация превентивных мер и междисциплинарных подходов в области кибербезопасности в государственном и частном секторах возложена на Национальный совет кибербезопасности, который выступает дополнительным связующим звеном ИТ-управления на федеральном уровне с участием различных министерств и других федеральных органов;

- эффективный контроль за преступностью в киберпространстве включает в себя целый комплекс институтов с участием предпринимателей и компетентных правоохранительных органов для разработки соответствующих рекомендаций [3, 28–29].

Наконец, в апреле 2017 г. вооруженные силы ФРГ создали киберкомандование (Cyber and Information Space Command, CIS), задачей которого является

отражение хакерских и шпионских атак. Согласно разработанному Бундесвером плану, к 2021 г. численность CIS будет составлять 14,5 тыс. сотрудников, из которых 1,5 тыс. человек будут гражданскими лицами. Таким образом, в ФРГ налажено достаточно тесное взаимодействие гражданских и военных структур в области киберзащиты и отражения хакерских и шпионских атак в киберпространстве.

Следует еще раз подчеркнуть, что система мер и институтов в ФРГ постоянно развивается в соответствии с усилением старых или возникновением новых киберугроз. Так, в 2017 г. правительство ФРГ рассматривало вопрос о возможном внесении изменений в Конституцию страны с целью нанесения ответных ударов по хакерам, атакующим частные компьютерные сети. При этом под мерами противодействия хакерам понимается, в частности, отключение серверов, используемых при осуществлении кибератак. Помимо прочего, это указывает на решимость ФРГ любыми средствами защитить свою информационную инфраструктуру от многочисленных киберугроз, не останавливаясь даже перед изменением основного закона страны – Конституции.

Основные меры по выработке единой политики ЕС в сфере кибербезопасности

Различные шаги и попытки выработать единую политику в сфере кибербезопасности в Европе и, в частности, в ЕС предпринимаются с давних пор, на протяжении почти двух десятилетий. Еще в 2001 г. в Будапеште была принята Конвенция Совета Европы о киберпреступности, призванная регулировать правовые отношения в глобальной компьютерной сети для предотвращения преступлений в этой сфере и контроля над преступностью, связанной с применением компьютеров. В 2003 г. был принят дополнительный протокол к Конвенции о киберпреступности. Несмотря на то, что в Конвенции значительное место уделено вопросам координации действий разных стран на межгосударственном уровне против несанкционированного вмешательства в работу компьютерных систем, она не стала эффективным инструментом обеспечения кибербезопасности в Европе. В значительной мере это связано с тем, что в Конвенции не были прописаны конкретные механизмы, инструменты и способы реализации правовых норм на наднациональном уровне и контроля за их исполнением.

В связи с этим в 2004 г. в рамках ЕС было создано Европейское агентство по сетевой и информационной безопасности (European Network and Information Security Agency, ENISA), призванное координировать и направлять деятельность различных стран по противодействию киберугрозам. Однако на первых порах деятельность этого агентства была весьма ограниченной: так, в 2010 и в 2012 гг. агентство проводило киберучения с целью определить готовность государственных и частных организаций ЕС к отражению кибератак. В учениях 2012 г. принимали участие более 300 специалистов по компьютерной безопас-

ности различных банков, интернет-провайдеров и государственных учреждений из 25 стран ЕС [2, 154]. В 2013 г. был образован и начал свою работу Европейский центр по борьбе с киберпреступностью (European Cybercrime Centre, ECC), призванный оказывать информационную, оперативную и экспертную поддержку расследованиям по киберпреступлениям на региональном и международном уровнях. Перед центром были поставлены задачи определить тенденции в сфере киберпреступности, способствовать обмену информацией о ней между странами ЕС, анализировать принятые на национальном уровне превентивные меры и оперативные действия, проводить спецподготовку полицейских, судебных и прокурорских кадров в сфере борьбы с киберпреступностью [5].

В 2013 г. была представлена киберстратегия ЕС под названием «Открытое, безопасное и надежное киберпространство»[1]. Целью стратегии ЕС является повышение устойчивости и наращивание потенциала в области кибербезопасности государств – членов ЕС, включая усиление борьбы с киберпреступностью, формирование эффективной инфраструктуры обеспечения информационной безопасности, разработку принципов координации международной политики в области кибербезопасности. Следует отметить, что реализация последнего пункта, а именно координации и согласования политики государств, входящих в ЕС, на общеевропейском и международном уровне является самым сложным для выполнения.

Среди других значимых мер, направленных на формирование единой политики ЕС по противодействию киберугрозам, следует отметить «Директиву ЕС по кибербезопасности», принятую и опубликованную в 2016 г. [9]. Согласно этой директиве, государства-члены ЕС совместно с Европейской Комиссией и Европейским агентством по сетевой и информационной безопасности (ENISA) должны создать группу взаимодействия. Основными функциями этой группы являются рассылка данных и обмен информацией между ее участниками, а также борьба с угрозами и инцидентами в области кибербезопасности. Кроме того, в директиве содержится требование создать сеть национальных групп с целью организации быстрого и эффективного операционного взаимодействия при помощи обмена информации и поддержки стран – членов ЕС для разрешения трансграничных инцидентов в киберпространстве. Эта директива, разработанная Европейской комиссией и одобренная с некоторыми поправками Европейским парламентом, вступила в силу в августе 2016 г. С этого момента начался процесс перенесения основных положений директивы в национальное законодательство стран – членов ЕС и определения операторов, которые будут на практике обеспечивать кибербезопасность в Европе. Важно обратить внимание

[1] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels, 2013. Available at: URL: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (accessed: 14.06.2018).

на то, что принятие и особенно реализация директивы на практике сразу же, еще на стадии обсуждения в Европейском парламенте столкнулись со значительными проблемами и противоречиями. Большинство этих проблем и противоречий связаны с тем, каким именно образом государства, являющиеся членами ЕС, будут организовывать сотрудничество для осуществления согласованного ответа на кибератаки и другие инциденты в киберпространстве. Уже здесь, на этой первоначальной стадии формирования инструментов обеспечения кибербезопасности в рамках ЕС, отчетливо проявилась несформированность единого политического пространства, которое позволили бы проводить единую и согласованную политику в области внутренней и внешней безопасности, в данном случае кибербезопасности.

Недостатки и трудности реализации «Директивы ЕС по кибербезопасности» проявились, в частности, в том, что уже вскоре после принятия директивы Европейская комиссия предприняла более решительные шаги, не дожидаясь согласования интересов стран ЕС и организации между ними сотрудничества в киберпространстве. В сентябре 2017 г. председатель Еврокомиссии Жан-Клод Юнкер предложил преобразовать агентство по сетевой и информационной безопасности (ENISA) в Европейское агентство киберзащиты, одновременно увеличив его финансирование и расширив его штаты. По замыслу Европейской комиссии это агентство должно защищать страны ЕС и европейские компании от информационных угроз, причем его действия должны включать «активную оборону», подразумевающую ответные кибератаки в случае покушения на сетевую безопасность ЕС. Предложение было сделано во время пленарной сессии Европарламента в Страсбурге. В ходе выступления глава Еврокомиссии заявил о недостаточной защищенности государств-членов ЕС от киберугроз. По словам Юнкера, кибератаки могут представлять для демократии и стабильности большую угрозу, чем ружья и танки, поскольку в сети не существует понятия государственных границ. В этом же выступлении Юнкер констатировал что, только за 2016 г. в странах ЕС было зафиксировано более 4 тыс. кибератак, причем примерно 80% европейских компаний сталкивались с различного рода киберугрозами[1].

Еще одной мерой, призванной усилить кибербезопасность в ЕС, является предложенное Европейской комиссией в 2017 г. введение сертификатов для выпускаемой в странах ЕС цифровой продукции и цифровых услуг. С точки зрения Еврокомиссии, сертификация может играть решающую роль в усилении безопасности и развитии единого европейского рынка цифровых продуктов и услуг, поскольку сертификаты будут действительными на всей территории ЕС. Разработчики сертификации исходили из того, что эти документы смогут га-

[1] Еврокомиссия предложила создать агентство по киберзащите. 13.09.2017. [Evrokomissiya predlozhila sozdat' agentstvo po kiberzashchite. [The European Commission proposed the establishment of Cybersecurity Agency]. Available at: URL: https://www.securitylab.ru/news/488472.php (accessed: 14.06.2018).

рантировать соответствие продуктов и услуг требованиям кибербезопасности. В то же время следует заметить, что само по себе введение сертификации не обеспечивает кибербезопасность и не страхует от многочисленных кибератак как извне, так и изнутри ЕС. О том, что проблема кибербезопасности по-прежнему, несмотря на все предпринятые меры, остается весьма актуальной для стран ЕС, свидетельствуют, в частности, результаты заседания Совета Европы на Мальте в 2017 г. [8].

Важным шагом на пути защиты данных пользователей компьютерных сетей стал общий регламент ЕС о защите данных (General Data Protection Regulation, GDPR), разработанный и одобренный Европейским парламентом еще в 2016 г. и вступивший в силу в конце мая 2018 г. Этот регламент, призванный регулировать распространение и использование личных данных граждан стран ЕС, устанавливает нормы, в соответствии с которыми пользователи из стран ЕС имеют право знать, как именно используются их персональные данные, которые они предоставляют о себе в компьютерных сетях[1]. Существенно, что новые правила являются экстерриториальными и распространяются на операторов, обрабатывающих персональные данные европейцев не только в странах ЕС, но и за его пределами. В случае использования данных с нарушением принятого в ЕС регламента предусмотрен штраф вплоть до 20 млн евро.

Следует отметить, что принятие этого регламента в ЕС уже вызвало значительно недовольство со стороны США, так как американские корпорации широко используют личные данные европейцев для проведения рекламных и других кампаний, а американские спецслужбы столь же широко пользуются данными европейцев для своих целей. После принятия регламента это будет делать несколько труднее, и тем не менее можно не сомневаться, что американские спецслужбы и корпорации найдут новые технические средства сбора личных данных пользователей сетей в странах ЕС. Поэтому говорить о высокой эффективности принимаемых в ЕС мер по защите личных данных и в целом по обеспечению кибербезопасности пока что, по меньшей мере, преждевременно. В то же время следует констатировать, что некоторые из перечисленных шагов ЕС в сфере кибербезопасности при соответствующей адаптации и корректировке могут быть полезными как для России, так и для других стран Евразийского экономического союза (ЕАЭС), в том числе для координации действий стран – членов ЕАЭС по противодействию киберугрозам. К числу таких шагов, как представляется, относятся, например, создание централизованного агентства киберзащиты, способного отвечать на кибератаки, сертификация выпускаемой в России и других странах ЕАЭС цифровых продуктов и услуг, меры по защите

[1] В Евросоюзе вступил в силу новый закон о защите персональных данных // Интерфакс. 25.05.2018. [V Evrosojuze vstupil v silu novyj zakon o zashhite personal'nyh dannyh // Interfaks. 25.05.2018. [General Data Protection Regulation came into effect in the EU // Interfax. 25.05.2018]. Available at: URL: http://www.interfax.ru/world/614304 (accessed: 14.06.2018).

персональных данных пользователей компьютерных сетей, предусматривающие значительные штрафы за незаконное использование этих данных.

Некоторые выводы

Подводя итоги, можно сделать вывод, что несмотря на значительные усилия Европейской Комиссии и других органов ЕС, ситуация в области проведения единой политики в сфере киберзащиты остается сложной и противоречивой. Налицо заметное расхождение между отлаженной системой мер по обеспечению кибербезопасности на уровне отдельных стран (Норвегии, Германии, Австрии и др.) и недостаточной сформированностью соответствующей системы на наднациональном уровне ЕС. Руководящие органы ЕС лишь в последние годы всерьез озаботились выработкой и реализацией единой политики стран ЕС в области киберзащиты. Пока что сделанные шаги, направленные на проведение такой политики, явно недостаточны, особенно в плане их эффективной реализации всеми странами ЕС.

Основная проблема эффективного обеспечения кибербезопасности состоит в том, что оно требует создания в ЕС единого европейского политического пространства. Однако на этом пути существует множество подводных камней и препятствий, которые, в первую очередь, связаны с разными подходами отдельных государств к регулированию киберпространства, а также со сложностями в осуществлении ими сотрудничества и координации действий по обеспечению кибербезопасности. В этом плане уместно сравнение с отсутствием единой европейской политики в отношении инокультурной миграции, а также с проблемой формирования общеевропейского пространства безопасности. Несмотря на провозглашаемое проведение единой политики ЕС в области миграции и ее регулирования, разные страны ЕС проводят совершенно разную миграционную политику. Так, страны Вышнеградской группы (Польша, Венгрия, Чехия, Словакия) отказываются принимать иммигрантов из стран Ближнего Востока и Африки, выстраивая барьеры на пути миграции из других стран ЕС. В то же время Германия, Франция, Бельгия, Италия, Швеция принимают массы иммигрантов, что заметно сказывается на их внутренней социальной и политической ситуации, на обеспечении внутренней безопасности этих государств и других стран ЕС [4; 6].

В известном смысле сходная ситуация существует для ЕС и в сфере кибербезопасности. Значительная активность в этой сфере руководящих органов ЕС сталкивается с неспособностью ряда стран выполнить все директивы, распоряжения, регламенты и другие нормативные акты. Кроме того, следует учитывать, что параллельно с реакцией ЕС на прежние киберугрозы непрерывно появляются все новые угрозы кибербезопасности, на которые государства и наднациональные структуры ЕС не всегда успевают вовремя отреагировать. Во многом это происходит из-за сложных процедур согласования на национальном

и наднациональном уровнях, требующих значительного времени, а также из-за несформированности в ЕС единого политического пространства. Тем не менее, несмотря на все эти проблемы, вызовы и трудности, система обеспечения кибербезопасности в странах ЕС довольно быстро развивается и совершенствуется, чему способствует столь же быстрое накопление опыта регулирования и координации действий стран – членов ЕС в сфере кибербезопасности. Более того, можно предположить, что именно необходимость адекватного ответа на все новые вызовы и угрозы кибербезопасности в итоге станет одним из действенных стимулов для формирования единого политического пространства ЕС.

Библиографический список

1. Глобальный индекс кибербезопасности и профили по киберблагополучию: отчет. Женева, ABI Research, 2015. 516 с. Global'nyj indeks kiberbezopasnosti i profili po kiberblagopoluchiyu. Otchet. [Global Cybersecurity Index and Cyberwellness Profiles. Report]. Geneva, ABI Research, 2015. 516 p.].
2. *Господарик Ю.П., Пашковская М.В.* Международная экономическая безопасность. М., 2016. 416 с. [Gospodarik Ju.P., Pashkovskaya M.V. Mezhdunarodnaya ekonomicheskaya bezopasnost'. [International Economic Security]. Moscow, Synergy University Publ., 2016. 416 p.].
3. *Елин В.М.* Сравнительный анализ правового обеспечения информационной безопасности в России и за рубежом: монография. М., 2016. 168 с. [Elin V.M. Sravnitel'nyj analiz pravovogo obespecheniya informacionnoj bezopasnosti v Rossii i za rubezhom. Monografiya. [Comparative Analysis of the Legal Support for Information Security in Russia and in Foreign Countries. Monograph]. Moscow, 2016. 168 p.]
4. ЕС перед вызовами миграционного кризиса. Позиции европейских стран: аналитический доклад / под ред. Н.К. Арбатовой, А.М. Кокеева. М., ИМЭМО РАН, 2016. 52 с. [ES pered vyzovami migracionnogo krizisa. Pozicii evropejskikh stran. [The EU faced with the migration crisis. Positions of European countries. Analytical Report. Ed. by N.K. Arbatova, A.M. Kokeev]. Moscow, IMEMO Publ., 2016. 52 p.].
5. *Нижегородцев Д.* Европейский центр борьбы с киберпреступностью подвел итоги первого года работы // Деловая газета «Взгляд». 2014. 11 февр. [Nizhegorodcev D. Evropejskij centr bor'by s kiberprestupnost'yu podvel itogi pervogo goda raboty // Delovaya gazeta «Vzglyad». 11.02.2014. [European cybercrime centre sums up its first year work // Online newspaper “Vzglyad”. 11.02.2014]. Available at: https://vz.ru/news/2014/2/11/671970.html (accessed 14.06.2018).
6. *Потемкина О.Ю.* Вышнеградская группа и «гибкая солидарность» // Современная Европа. 2016. № 6. С. 43–52. [Potemkina O.Yu. Vishegradskaya gruppa i «gibkaya solidarnost'» // Sovremennaya Evropa. [Visegrad group and “flexible solidarity” // Contemporary Europe. 2016. No. 6. P. 43–52].

7. *Сейник В.* Борьба с киберпреступностью – одна из составляющих международной безопасности / Центр исследования компьютерной преступности. 19.04.2008. [Sejnik V. Bor'ba s kiberprestupnost'yu – odna iz sostavlyayushchikh mezhdunarodnoj bezopasnosti / Centr issledovaniya komp'yuternoj prestupnosti. [Struggle Against Cybercrime as Part of International Security / Computer Crime Research Center. 19.04.2018]. Available at: http://www.crime-research.ru/articles/Seynik/ (accessed 14.06.2018).
8. *Соловьев А.И., Куприяновский В.П., Соловьев С.А.* Единый цифровой рынок Европейского Союза: текущее состояние и направления развития // International Journal of Open Information Technologies. 2017. Vol. 5. No. 10. P. 47–54. [Solov'ev A.I., Kupriyanovskij V.P., Solov'ev S.A. Edinyj cifrovoj rynok Evropejskogo Soyuza: tekushchee sostoyanie i napravleniya razvitiya. [Single Digital Market in the European Union: Current State and Development Trends // International Journal of Open Information Technologies. 2017. Vol. 5. No. 10. P. 47–54].
9. *Haeni R.* 2016. Cybersecurity: New EU Directive Published. 20.07.2016. Available at: https://news.pwc.ch/28616/cybersecurity-new-eu-directive-published/ (accessed 14.06.2018).
10. *Schreier F., Weekes B., Winkler T.H.* Cybersecurity: The Road Ahead. Geneva Centre for the Democratic Control of Armed Forces (DCAF). DCAF Horizon 2015 Working Paper No. 4. Available at: https://dcaf.ch/sites/default/files/publications/documents/Cyber2.pdf (accessed 14.06.2018).

CHALLENGES FOR BUILDING THE EU COMMON CYBERSECURITY POLICY

V. I. Pantin
Doctor of Philosophical Sciences, Head of the Department for Comparative Political Studies, Primakov National Research Institute of World Economy and International Relations, RAS

N. V. Kardava
Junior Research Fellow, Department for Comparative Political Studies, Primakov National Research Institute of World Economy and International Relations, RAS

The article analyzes the most complex and topical problems of ensuring cybersecurity in the EU countries and of forming a common policy in this field. The authors consider the general political and economic factors that make the cybersecurity problems challenging at the national, supranational and global levels. The German case shows that in several developed EU member countries, national cybersecurity policy proves to be more efficient than a supranational one. The authors conclude that the German approach to ensuring cybersecurity is characterized by its complex and fundamental nature. It comprises a whole system of normative acts, plans and institutions. The article outlines the key approaches, trends and contradictions related to developing a common EU cybersecurity strategy. The authors analyze the main documents and actions of the European Commission and other EU bodies in this field, including the Cybersecurity Strategy of the European Union (2013), the EU Directive on the Security of Networks and Information Systems (2016), and the General Data Protection Regulation (2018). At the same time, the authors show that the EU governing bodies' activity in the field of cybersecurity is faced with the inability of several member countries to comply with all the directives, orders, regulations and other normative acts. The authors define the major impediments to the implementation of the common EU cybersecurity policy: different levels of economic, technological and social development of its member countries; the mismatch between the interests of different political actors; different approaches of individual EU states to regulating cyberspace; the complexity of cybersecurity policy coordination between the EU member countries. The authors conclude that the obstacles primarily flow from the underdevelopment of the EU common political space. At the same time, cybersecurity problems are likely to contribute to a more accelerated and effective formation of such a space at the supranational level. Furthermore, the authors consider that some of the steps taken by the EU to ensure cybersecurity, properly adapted and adjusted, could be useful for the Russian Federation.

Keywords: European Union; Germany; regulation of the cyberspace; common policy; cybersecurity; cyber threats; supranational political space.