Т.А. Романова, А.Н. Малова*

ПРОБЛЕМА ПРИМЕНЕНИЯ КАТЕГОРИИ «СТРЕССОУСТОЙЧИВОСТЬ» В ПОЛИТИКЕ КИБЕРБЕЗОПАСНОСТИ ЕВРОСОЮЗА**

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Санкт-Петербургский государственный университет»
199034, Санкт-Петербург, Университетская набережная, 7/9

Особая природа киберсреды — взаимозависимость между материальными и социальными объектами, сложность организации — заставляет ведущих субъектов мировой политики искать новые стратегии ведения своей деятельности в этой области. В Европейском союзе обсуждение проблем кибербезопасности ведется с опорой на категорию «стрессоустойчивость», которая в этом контексте рассматривается как способность системы адаптироваться к новым вызовам, гибко реагировать на угрозы, успешно восстанавливаться после ударов. В данной статье с помощью дискурс-анализа изучены причины появления и логика развития дискурса стрессоустойчивости в политике ЕС в области кибербезопасности, выявлены особенности интерпретации данной категории в официальных документах, продемонстрированы проблемы, сопряженные с ее применением на практике.

Авторы прослеживают постепенную эволюцию подходов ЕС к определению объекта кибербезопасности — от традиционных интерпретаций киберпространства к экосистемным терминам и концепциям. Последние, как отмечено в статье, в наибольшей степени соответствуют пониманию кибербезопасности в категориях стрессоустойчивости. В рамках такого подхода интернет предстает не как статичный объект, который нужно контролировать и защищать, а как сложная гетерогенная система, где состояние безопасности неразрывно связано с состояниями опасности.

В официальных документах ЕС пока не сложилось единой и четкой дефиниции стрессоустойчивости. Тем не менее, как подчеркивают авторы, и в этой области можно проследить постепенную

* *Романова Татьяна Алексеевна* — кандидат политических наук, доцент Санкт-Петербургского государственного университета (e-mail: t.romanova@spbu.ru, romanova@mail.sir.edu); *Малова Алёна Николаевна* — аспирантка Санкт-Петербургского государственного университета (e-mail: alenamalova5@gmail.com).

** Статья подготовлена за счет гранта Российского научного фонда, проект № 17-18-01110.

трансформацию официального дискурса от чисто технических определений ко все большему учету социально-политических факторов. Впрочем, официальный дискурс ЕС в этом отношении остается крайне противоречивым. В частности, это касается определения соотношения таких понятий, как «киберстрессоустойчивость» и «кибербезопасность». Авторы отмечают тенденцию к нарастающей секьюритизации киберсферы в дискурсе ЕС о кибербезопасности, что чревато выхолащиванием понятия «стрессоустойчивость», превращением его в простой эвфемизм. Однако в конечном счете, приходят к выводу авторы статьи, чрезмерная секьюритизация киберсферы невыгодна самому ЕС, и постепенно его политика в области кибербезопасности будет все более последовательно выстраиваться на принципах стрессоустойчивости.

Ключевые слова: Европейский союз, стрессоустойчивость, кибербезопасность, киберугрозы, киберстрессоустойчивость, киберэкосистема, секьюритизация, критическая информационная инфраструктура, Европейское агентство по сетевой и информационной безопасности, ENISA.

В последние годы необходимость обеспечения кибербезопасности стала общепризнанной. В Евросоюзе (ЕС) обсуждение этой проблемы сегодня ведется с опорой на категорию «стрессоустойчивость» (resilience) [о переводе см.: Гудалов, Тулупов, 2018; Романова, 2017]. Классические словари определяют это слово как свойство (качество, умение, способность) быстро возвращаться в прежнее состояние после столкновения с проблемами, восстанавливаться после трудностей[1]. Однако в социальных науках наделение смыслом этой категории часто зависит от контекста и цели участников.

Современные авторы, пишущие о стрессоустойчивости, обычно опираются на выводы исследователей, работавших в отличных от социальных наук сферах, прежде всего в экологии. Так, базовым для трудов в области стрессоустойчивости стало исследование канадского эколога К.С. Холлинга, который использовал рассматриваемую категорию при изучении свойств экологических систем [Holling, 1973]. В частности, К.С. Холлинг отделял стрессоустойчивость от методов управления, основан-

[1] 'Resilience — the quality of being able to return quickly to a previous good condition after problems' // Cambridge Business English dictionary. Available at: https://dictionary.cambridge.org/ (accessed: 28.03.2019); 'Resilience — the ability of a substance or object to spring back into shape; elasticity' // Oxford dictionary. Available at: https://en.oxforddictionaries.com/ (accessed: 28.03.2019).

ных на поиске стабильности, «отскакивании назад» к состоянию баланса, и характеризовал ее как устойчивость отношений элементов внутри системы, способность последней поглощать различные изменения, продолжая свое существование [Holling, 1973]. От данной категории также отталкиваются С. Доверс и Дж. Хэндмер, специалисты по экологической политике, говоря о проблеме устойчивого развития. Исследователи противопоставляют стрессоустойчивое управление управлению рисками и выделяют несколько его типов: а) поддержание статус-кво; б) периферийные перемены и адаптация, т.е. стрессоустойчивость через изменение взгляда на угрозы; в) открытость и качественная перестройка системы [Dovers, Handmer, 1992].

В целом категория «стрессоустойчивость» часто применяется как теоретическая основа для изучения политики развития [Aradau, 2017], экологической политики [Rothe, 2017], управления катастрофами [Milliano, Jurriens, 2016]. Значительную часть корпуса литературы об этой категории составляют исследования, рассматривающие ее как особую практику безопасности. В этой связи представляют интерес работы Д. Чендлера, Дж. Кофи, Ф. Бурбо и К. Арадау.

Ф. Бурбо, специалист в области международной безопасности, исследует соотношение концепций «стрессоустойчивости» и «секьюритизации», указывая, что стрессоустойчивость может играть одну из двух ролей. С одной стороны, она выступает в качестве альтернативы секьюритизации в ситуациях, когда доминантный дискурс безопасности не отвечает требованиям системы. С другой стороны, обращение к идее стрессоустойчивости может служить первым шагом к секьюритизации, например, когда она сама направлена на поддержание статус-кво либо маргинальные изменения, не ведущие к системной трансформации [Bourbeau, 2013, 2015, 2017].

К. Арадау, специалист в области критических исследований в международных отношениях, выделяет несколько эпистемных режимов безопасности в зависимости от того, какое знание можно получить о рисках. Эксперт подчеркивает, что, в отличие от безопасности как предотвращения угрозы благодаря углублению знания о ней или статистическому прогнозированию ее наступления, стрессоустойчивость пригодна для сложных систем, характеристиками которых являются неопределенность и ранее неизвестные шоки, не поддающиеся изучению [Aradau, 2017]. Таким образом, коренное отличие классических режимов

безопасности от стрессоустойчивости состоит в стремлении предусмотреть заранее все риски и защититься от них.

Д. Чендлер и Дж. Кофи в свою очередь утверждают, что безопасность логически предшествует стрессоустойчивости, и, следуя рассуждениям С. Доверса и Дж. Хэндмера, выделяют несколько видов последней. По их мнению, до ее достижения безопасность обеспечивается путем предотвращения угроз и рисков, после этого система принимает их неотвратимость и учится с ними работать, существовать в их присутствии. Авторы рассматривают: а) стрессоустойчивость как «отскакивание назад» к равновесию; б) аутопоэзную стрессоустойчивость как продвижение вперед, трансформацию и адаптацию к кризисам; в) стрессоустойчивость как эволюцию системы, предполагающую интерпретацию проблем и рисков как возможностей для дальнейшего развития [Chandler, Coaffee, 2017].

Наконец, интерес для анализа проблем и перспектив применения категории «стрессоустойчивость» в области кибербезопасности представляет обращение к исследованиям, сосредоточенным на конкретных эмпирических кейсах. Например, Дж. Кофи и П. Фасси изучают практику слияния безопасности и стрессоустойчивости при борьбе с терроризмом [Coaffee, Fussey, 2017]. Б. Эванс и Дж. Рид рассматривают сужение практик стрессоустойчивости за счет большей инкорпорации в них вопросов безопасности на примере использования систем массового слежения в Великобритании [Evans, Reid, 2013].

Исследования кибербезопасности ЕС обширны и включают, например, работы о киберсиле Евросоюза и проецировании ее на международную арену [Dunn Cavelty, 2013, 2018], о европейской кибердипломатии [Renard, 2018], проникновении принципов кибербезопасности в различные направления политики Брюсселя [Farrand, 2018], об управлении в области киберпреступности и национальных стратегиях кибербезопасности отдельных стран — членов ЕС [Christou, 2016, 2018; Brassett, Vaughan-Williams, 2015; Herrington, Aldrich, 2013]. Отечественные исследователи отмечают комплексность сферы кибербезопасности Евросоюза и стремятся классифицировать основные подходы Брюсселя к рискам в киберсреде [Зворыкина, Земледельцев, 2014; Кацы, Шматкова, 2018]. В фокус внимания ученых также попадают проблема выработки единой политики кибербезопасности ЕС и национальные стратегии стран-членов [Пантин, Кардаева, 2018]. Однако российские авторы чаще останавливаются на правовых аспектах рассматриваемой темы [Кацы, Шматкова, 2018; Шафеев, 2018],

тогда как политологические исследования встречаются реже [Пантин, Кардаева, 2018].

Ряд экспертов [Christou, 2016, 2017; Dunn Cavelty, 2013, 2018; Kaufmann, 2015] особое внимание уделяют категории «стрессоустойчивость» для более разностороннего анализа политики ЕС в области кибербезопасности. Последняя в данном контексте — это способность к самозащите через внутреннюю готовность к угрозам, а также через умение восстановиться после удара. М. Данн Кавелти (Цюрихский центр исследований безопасности; исследования в области международной безопасности и кибербезопасности) и Дж. Кристу (Уорикский университет; исследования в области европейской безопасности) видят именно принципы стрессоустойчивости залогом успешности ЕС в сфере кибербезопасности [Christou, 2017; Dunn Cavelty, 2018]. Дж. Кристу также обращает внимание на нормативное и ценностное основания политики в области кибербезопасности ЕС и, опираясь на идеи С. Доверса и Дж. Хэндмера, вырабатывает специфические критерии для достижения наиболее продвинутой практики «безопасности как стрессоустойчивости». Он отмечает, что для этой идеи характерны приоритет плюрализма над эффективностью, гибкость и адаптивность, а также согласованность и связанность между всеми акторами, уровнями и политиками [Christou, 2016, 2017, 2018].

Цель настоящей статьи — выявить логику возникновения категории «стрессоустойчивость» в дискурсе ЕС о кибербезопасности и потенциальные последствия ее появления. Опираясь на существующие типологии стрессоустойчивости, мы постараемся определить особенности интерпретации стрессоустойчивости в области кибербезопасности в официальных документах ЕС, а также продемонстрировать проблемы, связанные с применением данного концепта на практике. В связи с этим, следуя задачам статьи, мы проанализируем составляющие европейской системы кибербезопасности и основные принципы, на которых она основана; определим место категории «стрессоустойчивость» в документах о кибербезопасности; а также представим различные интерпретации данной категории в текстах и ее соотношение с другими концепциями.

Стрессоустойчивость — это альтернативный и при этом далеко не однородный способ организации безопасности. Эта неоднородность в кибербезопасности ЕС, а также соотношение стрессоустойчивости с другими практиками ее обеспечения и исследуются в данной статье. С учетом сказанного ее новизна

заключается в анализе принципов, составляющих основу системы кибербезопасности ЕС, в их рассмотрении через категорию «стрессоустойчивость».

Актуальность исследования обусловлена необходимостью переосмыслить подходы к обеспечению безопасности в связи с развитием новых технологий. Особая природа киберсреды — взаимозависимость между материальными и социальными объектами, сложность организации — позволяет говорить о необходимости поиска новых эффективных стратегий организации и управления. Таким образом, изучение стратегий кибербезопасности, выбранных Евросоюзом, видится актуальным как с точки зрения теоретического осмысления новых тенденций, так и с позиции анализа практического опыта использования теоретических новаций.

Методологической основной статьи стал дискурс-анализ. Исследованы политические и технические тексты ЕС, а именно Европейского агентства по сетевой и информационной безопасности (ENISA), Еврокомиссии, Верховного представителя ЕС по иностранным делам и политике безопасности, Европарламента и Европейского совета. Ранее аналогичный метод для исследования кибербезопасности использовала М. Кауфманн (Институт исследований мира, Норвегия), чтобы продемонстрировать, как выбор той или иной лексики для обозначения явлений в кибербезопасности в документах ENISA может быть признаком проникновения категории «стрессоустойчивость» в эту сферу и триггером для изменения политики [Kaufmann, 2015]. В данной статье авторы обращаются к более широкому корпусу документов и анализируют разные интерпретации стрессоустойчивости, которые присутствуют в документах о кибербезопасности, а также выявляют ее специфические направления (безопасность общего рынка и критической инфраструктуры, внешняя политика), где проникновение исследуемой категории было более успешным.

В следующем разделе мы охарактеризуем эволюцию регулирования и основные принципы организации кибербезопасности в ЕС и рассмотрим главные составляющие данной сферы, что позволит увидеть предпосылки для проникновения в нее категории «стрессоустойчивость». Далее мы проследим, как эта категория использовалась в документах до и после формулирования официальной стратегии кибербезопасности, что позволит сопоставить разные подходы к безопасности и разные интерпретации стрессоустойчивости в текстах. В заключение мы

проанализируем различные понимания стрессоустойчивости, а также место категории в политике ЕС в киберсфере.

* * *

Европейские механизмы защиты и регулирования угроз, связанных с киберпространством, начали складываться в 1970-е годы [Christou, 2017]. Строго говоря, до выхода Стратегии кибербезопасности ЕС (далее — Стратегия) в 2013 г. это была не система кибербезопасности, а ряд норм и правил, которые регулировали складывающееся информационное общество, а именно сферы, так или иначе теперь представляющие собой элементы кибербезопасности.

Первая опора кибербезопасности в ЕС ориентирована на слаженную и эффективную работу внутреннего рынка. Меры этой опоры связаны с обеспечением безопасности информационных сетей и критической информационной инфраструктуры, защитой данных[2], обменом информацией об инцидентах и общей стандартизацией и гармонизацией процедур управлениями рисками. Основными направлениями деятельности в этой связи являются усиление ENISA[3] и развитие взаимодействия агентства с другими ответственными органами на уровне ЕС и стран-членов, создание единого рынка кибербезопасности и имплементация директивы по сетевой и информационной безопасности[4]. Второй элемент, борьба с киберпреступностью, предполагает более тесное взаимодействие соответствующих органов стран-членов,

---

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) // Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504 (accessed: 23.03.2019).

[3] ENISA (создано в 2004 г.) имеет следующие функции: улучшение информационной и сетевой безопасности в ЕС, развитие культуры информационной безопасности, содействие в разработке стандартов для единого рынка.

[4] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union // Official Journal of the European Union. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN (accessed: 09.02.2019). Директива предписывает операторам и провайдерам критически важных сервисов сообщать о серьезных инцидентах национальным органам системы кибербезопасности; странам-членам — принять национальные стратегии кибербезопасности. Кроме того, согласно положениям директивы создана сеть групп реагирования на инциденты компьютерной безопасности (CSIRTs).

Европейского центра борьбы с киберпреступностью[5], а также с третьими странами. Основные направления работы в данном случае — это гармонизация законодательства и совместные расследования[6]. Кибероборона исторически наименее развита из всех трех сфер деятельности в киберсфере. Здесь ЕС требует расширения взаимодействия в области безопасности и обороны для лучшего обнаружения, реагирования и восстановления после возможных кибератак, включая гибридные угрозы[7].

Три рассмотренных направления показывают, что кибербезопасность эволюционно включала не только логику собственно безопасности, но также (и в гораздо большей степени) правовую логику и логику экономической эффективности. Но только с появлением Стратегии все эти элементы стали складываться в систему.

Стратегия кибербезопасности и более поздние документы расширили поле активности ЕС: они уже предполагают распространение принципов кибербезопасности объединения на международных партнеров, организации, а также гражданское общество и частный бизнес. Роль Брюсселя в глобальном управлении киберпространством видится в том, чтобы способствовать распространению универсальных ценностей, бороться с негативными проявлениями всеобщей взаимозависимости, а также создавать условия для развития стрессоустойчивой информационной инфраструктуры и доступа к интернету в третьих странах[8].

---

[5] Европейский центр по борьбе с киберпреступностью (European Cybercrime Centre, EC3) был создан в 2013 г. в структуре Европола. EC3 занимается расследованиями серьезных киберпреступлений и служит платформой для обмена информацией между странами-членами.

[6] Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. European Commission. Brussels, 13.09.2017. JOIN (2017) 450 final // Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2017:0450:FIN (accessed: 20.07.2018).

[7] Ibidem.

[8] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity strategy of the EU: An open, safe and secure cyberspace. European Commission and High Representative of the European Union for Foreign Affairs and Security Policy. Brussels, 07.02.2013. JOIN (2013) 1 final // European External Action Service (EEAS). Available at: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (accessed: 28.11.2018); Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. European Commission. Brussels, 13.09.2017. JOIN (2017) 450 final // Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2017:0450:FIN (accessed: 20.07.2018); Shared Vision, Common

Здесь читается желание, с одной стороны, оказывать влияние на политические преобразования, но не прямо, а используя в качестве основы технические вопросы защиты и развития критической инфраструктуры [Романова, 2017], а с другой — защититься от возможных вызовов Глобальной сети через создание удобных для ЕС «правил игры».

Ключевой составляющей европейского дискурса о кибербезопасности является вопрос о ценностях. Подчеркивается, что «киберпространство должно существовать согласно тем же законам и нормам, которые применяются в обычной жизни»[9]. Кроме того, вся система кибербезопасности ЕС базируется на многоакторной модели управления и соответственно на общей ответственности за коллективную и индивидуальную кибербезопасность[10], что в целом согласуется с управлением, основанным именно на принципе стрессоустойчивости. Возможно, по этим причинам проникновение категории в сферу кибербезопасности ЕС было предсказуемым и неизбежным. По мнению Дж. Кристу, только подход к безопасности как стрессоустойчивости позволит ЕС оставаться верным своим идеалам, особенно в мире «после Сноудена», когда такие ценности, как права человека, неприкосновенность частной жизни, свобода и демократия, не раз стано-

---

Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy. European Union. Brussels, June 2016 // EEAS. Available at: https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf (accessed: 26.11.2018).

[9] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity strategy of the EU: An open, safe and secure cyberspace. European Commission and High Representative of the European Union for Foreign Affairs and Security Policy. Brussels, 07.02.2013. JOIN (2013) 1 final // Official Journal of the European Union. Available at: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (accessed: 28.11.2018).

[10] Ibidem. См. также: Communication from the Commission from the European Parliament and the Council. Internet Governance: Next Steps. Commission of the European Communities. Brussels, 18.06.2009. COM (2009) 277 final // Official Journal of the European Union. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0277:FIN:EN:PDF (accessed: 26.11.2018); European principles and guidelines for Internet resilience and stability. European Forum for Member States. Version of March 2011 // Ministerul Afacerilor Interne. Centrul national de coordonare a protectiei infrastructurilor critice. Available at: http://ccpic.mai.gov.ro/docs/guidelines_internet_fin.pdf (accessed: 20.07.2018); Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Agenda for Europe. European Commission. Brussels, 19.05.2010. COM (2010) 245 final // Official Journal of the European Union. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF (accessed: 28.02.2019).

вились жертвами агрессивной интерпретации кибербезопасности со стороны приверженцев киберсуверенитета [Christou, 2017].

Поскольку сфера кибербезопасности понимается в ЕС очень широко, одной из проблем европейского дискурса о стрессоустойчивости киберпространства является отсутствие последовательности в определении сферы, которая должна стать стрессоустойчивой: это может быть интернет или киберпространство, а также «киберсреда», «киберэкосистема» и «экосистема кибербезопасности».

Наиболее распространен термин «киберпространство», хотя это и самое консервативное понятие, относящееся ко времени становления интернета и формирования утопических представлений о пространстве, независимом от реальности и свободном от существующих в ней властных отношений [Manjikian, 2010]. Этот термин часто используется взаимозаменяемо с понятием «интернет». Например, в Стратегии киберпространство/интернет описывается, с одной стороны, прагматично как продолжение реального мира, но с другой — с нотой утопичности как эмансипирующая технология, способная освободить людей политически и социально, как, например, во время «Арабского пробуждения»[11].

Более точны постепенно проникающие из технических отчетов в политические документы экосистемные термины, позволяющие говорить о сфере комплексно и в целом более соответствующие стрессоустойчивости как способу системного мышления. Впервые эта терминология была введена в 2011 г. в отчете для ENISA, где виден переход от понимания интернета как пространства к осознанию его как экосистемы[12]. По мнению М. Кауфманн, подобное переосмысление Глобальной сети глубоко перформативно, т.е. не является случайным выбором новой метафоры вместо общепринятой, но представляет собой осознанное действие, призванное создать основу для нового подхода к регулированию этой сферы, в котором агентство в част-

[11] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity strategy of the EU: An open, safe and secure cyberspace. European Commission and High Representative of the European Union for Foreign Affairs and Security Policy. Brussels, 07.02.2013. JOIN (2013) 1 final // EEAS. Available at: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (accessed: 28.11.2018).

[12] Inter-X: Resilience of the Internet Interconnection Ecosystem. Summary Report. April 2011 // European Union Agency for Network and Information Security (ENISA). Available at: https://www.enisa.europa.eu/publications/interx-report (accessed: 20.07.2018).

ности и ЕС в целом готовят для себя важное место [Kaufmann, 2015]. ENISA представляет интернет не как площадку, которую нужно контролировать, защищать от угроз и опасностей, а как гетерогенную сложную систему, успешно развивающуюся от одного кризиса к другому, где состояние безопасности связано с состояниями опасности[13].

Ссылаясь на М. Фуко и других постструктуралистов, М. Кауфманн отмечает, что ENISA, переосмысляя интернет и связанную с ним инфраструктуру как экосистему, совершает политический шаг, так как стремится диктовать то, какими методами данное пространство или экосистема должно управляться, т.е. рассчитывает трансформировать существующие властные отношения [Kaufmann, 2015].

Данный концептуальный поворот в восприятии проблем кибербезопасности ENISA косвенно свидетельствует о значении, которое агентство начинает придавать категории «стрессоустойчивость» как методу управления. На примере более поздних документов мы видим, как новые термины (интернет-экосистема, или киберэкосистема) постепенно проникают в тексты ЕС[14], демонстрируя растущую популярность категории в сфере европейской кибербезопасности. Далее мы проследим эволюцию появления категории в текстах ЕС и проанализируем значения, которые ей придаются.

* * *

На данный момент ENISA в своем *кратком глоссарии* в наиболее общем виде предлагает следующее релевантное для своей деятельности базовое определение стрессоустойчивости: способность организации абсорбировать последствия прерывания деятельности и продолжать предоставлять минимально допустимый уровень сервиса[15].

---

[13] Ibidem.

[14] Proposal for a Regulation of the European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ('Cybersecurity Act'). Council of the European Union. Brussels, 29.05.2018. 9350/18 // Council of the European Union. Available at: http://data.consilium.europa.eu/doc/document/ST-9350-2018-INIT/en/pdf (accessed: 26.11.2018).

[15] Glossary. P–Z // ENISA. Available at: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/bcm-resilience/glossary/p-z (assessed: 20.07.2018).

При этом в *специальных исследованиях*[16], подготовленных для ENISA, нет единого взгляда на стрессоустойчивость, но, напротив, выделяются потенциально разные характеристики этого понятия для различных операторов информационных сетей, что согласуется с интерпретацией стрессоустойчивости как контекстного явления [Dunn Cavelty et al., 2015]. Документы, подготовленные другими институтами и органами ЕС, непосредственно посвященные кибербезопасности, четкого определения стрессоустойчивости не дают, но позволяют проследить некоторые изменения в понимании этой категории с течением времени.

Категория появляется в документах начала 2000-х годов, где она применяется по отношению к защите сетей и информационной инфраструктуры как части политики регулирования электронной коммуникации, защиты данных и предотвращения киберпреступности[17]. Причем стрессоустойчивость появляется как дополнение или замена классического подхода к безопасности информационных сетей как неактуального в цифровом мире. В сообщении «*Безопасность сетей и информационная безопасность...*» (2001) категория «стрессоустойчивость» отсутствует, но дается определение безопасности как «способности сетей или информационной системы уверенно *сопротивляться* случайным повреждениям или злонамеренным действиям...» (курсив наш. — *Авт.*)[18]. Это же определение переходит в более поздний

---

[16] Gaps in standardization related to resilience of communication networks. ENISA. 18.12.2009 // ENISA. Available at: https://www.enisa.europa.eu/publications/archive/gapsstd (accessed: 26.11.2018); Inter-X: Resilience of the Internet Interconnection Ecosystem. Summary Report. ENISA. April 2011 // ENISA. Available at: https://www.enisa.europa.eu/publications/interx-report (accessed: 20.07.2018); Enabling and managing end-to-end resilience. ENISA. 24.01.2011. Available at: https://www.enisa.europa.eu/publications/end-to-end-resilience (accessed: 20.07.2018).

[17] См., например: Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions. Creating a Safer Information Society by Improving the Security of Infrastructures and Combating Computer-Related Crime. Commission of the European Communities. Brussels, 26.01.2001. COM (2000) 890 final // Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52000DC0890&from=IT (accessed: 26.11.2018).

[18] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. Network and Information Security: Proposal for a European Policy Approach. Commission of the European Communities. Brussels, 06.06.2001. COM (2001) 298 final // Commission of the European Communities. Available at: http://ec.europa.eu/transparency/regdoc/rep/1/2001/EN/1-2001-298-EN-F1-1.Pdf (accessed: 26.11.2018).

текст Регламента о создании ENISA[19]. Если взглянуть на эти формулировки через призму классификации стрессоустойчивости Д. Чендлера и Дж. Кофи [Chandler, Coaffee, 2017], то можно заключить, что «способность сопротивляться угрозам» соответствует не традиционной безопасности как таковой, а именно стрессоустойчивости как «отскакиванию назад» к равновесию. Это тот вид технической или инженерной стрессоустойчивости, от которой призывал отказаться К.С. Холлинг [Holling, 1973], чтобы сконцентрироваться на способности системы развиваться в условиях кризиса.

Безопасность в документах 2001 г. также характеризуется Еврокомиссией как «товар, продаваемый и покупаемый на рынке, как часть соглашения между сторонами», а регулирование сферы информационной безопасности объясняется, как и в современных документах по стрессоустойчивости, необходимостью борьбы с несовершенствами рынка[20].

Уже через несколько лет Комиссия начала все больше отходить от технической равновесной интерпретации стрессоустойчивости, понимая важность социально-политической составляющей для успешного применения этой концепции в киберсфере. В Стратегии безопасного информационного общества 2006 г.[21] подчеркивается необходимость распространения культуры безопасности через динамичный единый подход, вовлекающий всех заинтересованных лиц и основанный на диалоге, партнерстве и расширении общих возможностей, а также разнообразии, открытости и операционной совместимости. Комиссия обращает внимание, что важно не концентрироваться на негативных

---

[19] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency // Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32004R0460 (accessed: 19.02.2019).

[20] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. Network and Information Security: Proposal for a European Policy Approach. Commission of the European Communities. Brussels, 06.06.2001. COM (2001) 298 final // Commission of the European Communities. Available at: http://ec.europa.eu/transparency/regdoc/rep/1/2001/EN/1-2001-298-EN-F1-1.Pdf (accessed: 26.11.2018).

[21] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A strategy for a Secure Information Society — 'Dialogue, Partnership and Empowerment'. Commission of the European Communities. Brussels, 31.05.2006. COM (2006) 251 final // Commission of the European Communities. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0251&from=RO (accessed: 26.11.2018).

аспектах работы с угрозами и видеть в безопасности возможность, достоинство и конкурентное преимущество, а не затратное обязательство[22]. Последнее утверждение иллюстрирует желание Комиссии перенести внимание с жесткого противодействия внешним вызовам киберсреды на необходимость внутренних преобразований в самом ЕС, т.е. изменить отношение к этим угрозам на принципах стрессоустойчивости.

В 2011 г. по результатам работы Европейского форума для стран-членов государства заняли более консервативную позицию и определили стрессоустойчивость как способность организации абсорбировать шоки и продолжать функционировать перед лицом опасностей[23], что согласуется с базовым определением ENISA, но идет вразрез с эволюционировавшим видением Еврокомиссии и более развернутыми исследованиями агентства. Как будет показано далее, подобные противоречия проникли и в более поздние документы ЕС по кибербезопасности.

* * *

В 2013 г. Еврокомиссия и Верховный представитель ЕС по иностранным делам и политике безопасности (далее — Верховный представитель) презентовали совместное комплексное видение кибербезопасности, обозначив пять векторов развития сферы:

– достижение киберстрессоустойчивости;

– снижение уровня киберпреступности;

– развитие киберсоставляющей политики безопасности и обороны;

– развитие индустриально-технологических ресурсов кибербезопасности;

– развитие последовательной международной политики ЕС в области кибербезопасности.

Стратегия демонстрирует некоторые терминологические подвижки, а также раскрывает неравномерность проникновения стрессоустойчивости в сферу кибербезопасности.

В документе вводится понятие «киберстрессоустойчивость» (cyber resilience), которое подразумевает меры, направленные на решение задач цифровизации ЕС как вектора развития единого

[22] Ibidem.

[23] European principles and guidelines for Internet resilience and stability. European Forum for Member States. Version of March 2011 // Ministerul Afacerilor Interne. Centrul national de coordonare a protectiei infrastructurilor critice. Available at: http://ccpic.mai.gov.ro/docs/guidelines_internet_fin.pdf (accessed: 20.07.2018).

рынка[24]. Эти меры предполагают достижение стрессоустойчивости информационных сетей, обеспечение информационной безопасности и конфиденциальности данных как на европейском уровне, так и на уровне стран-членов [Кацы, Шматкова, 2018]. Впоследствии эти идеи развиваются в специализированном Сообщении, где особое внимание уделяется созданию конкурентоспособных товаров и услуг, инвестициям и обеспечению корректной работы рынка, в частности, через выработку общих стандартов[25]. Стандартизация и сертификация составляют часть стратегии по созданию «правил игры» в киберсфере и пространства для частных игроков, и на данный момент общая добровольная сертификация товаров и услуг является основой реформы сферы кибербезопасности — Акта о кибербезопасности (по состоянию на март 2019 г. инициатива проходит одобрение в Европейском парламенте и Совете ЕС)[26].

Противовесом киберстрессоустойчивости в Стратегии выступает понятие «кибербезопасность», определенное как «меры

[24] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Single Market Strategy for Europe. European Commission. Brussels, 06.05.2015. COM (2015) 192 final // Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2015%3A192%3AFIN (accessed: 20.08.2018); Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Agenda for Europe. European Commission. Brussels, 19.05.2010. COM (2010) 245 final // Official Journal of the European Union. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF (accessed: 28.02.2019).

[25] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry. European Commission. Brussels, 05.07.2016. COM (2016) 410 final // European Commission. Available at: https://ec.europa.eu/digital-single-market/en/news/communication-strenghtening-europes-cyber-resilience-system-and-fostering-competitive-and (accessed: 28.02.2019).

[26] Proposal for a Regulation of the European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ('Cybersecurity Act'). Council of the European Union. Brussels, 29.05.2018. 9350/18 // Council of the European Union. Available at: http://data.consilium.europa.eu/doc/document/ST-9350-2018-INIT/en/pdf (accessed: 26.11.2018); Press release (2018) EU to create a common cybersecurity certification framework and beef up its agency — Council agrees its position, 08.06.2018 // Council of the European Union. Available at: http://www.consilium.europa.eu/en/press/press-releases/2018/06/08/eu-to-create-a-common-cybersecurity-certification-framework-and-beef-up-its-agency-council-agrees-its-position/ (accessed: 26.07.2018).

по защите киберпространства...»[27]. Подобная дефиниция резко отделяет данный термин от стрессоустойчивости и от логики системного управления. Во-первых, в английской версии используется словосочетание «cyber domain»[28], что имеет явную коннотацию с определенной ограниченной территорией, находящейся под чьей-то юрисдикцией. Во-вторых, речь идет прежде всего о защитных действиях, а не управлении. Согласно логике Стратегии и ее определениям кибербезопасность включает киберстрессоустойчивость, но наделяется противоположным стрессоустойчивости значением.

При этом, несмотря на явные различия в наполнении понятий, в отдельных местах они используются взаимозаменяемо. Отмечается, например, что для достижения кибербезопасности важны общая ответственность, культура (культура безопасности данных[29], или культура кибергигиены[30]), осведомленность конечных пользователей и расширение набора механизмов их участия в общем процессе (empowerment), а также реинтерпретация угроз как возможности для улучшения и развития[31]. Если вспомнить типологию Д. Чендлера и Дж. Кофи [Chandler, Coaffee, 2017],

---

[27] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity strategy of the EU: An open, safe and secure cyberspace. European Commission and High Representative of the European Union for Foreign Affairs and Security Policy. Brussels, 07.02.2013. JOIN (2013) 1 final // EEAS. Available at: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (accessed: 28.11.2018).

[28] Domain — 'an area of territory owned or controlled by a particular ruler or government' // Oxford dictionary. Available at: https://en.oxforddictionaries.com/definition/domain (accessed: 28.11.2018).

[29] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry. European Commission. Brussels, 05.07.2016. COM (2016) 410 final // European Commission. Available at: https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-410-EN-F1-1.PDF (accessed: 26.11.2018).

[30] Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. European Commission. Brussels, 13.09.2017. JOIN (2017) 450 final // Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2017:0450:FIN (accessed: 20.07.2018).

[31] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity strategy of the EU: An open, safe and secure cyberspace. European Commission and High Representative of the European Union for Foreign Affairs and Security Policy. Brussels, 07.02.2013. JOIN (2013) 1 final // EEAS. Available at: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (accessed: 28.11.2018).

можно сделать вывод, что все перечисленные целевые качества отличают дискурс о стрессоустойчивости, причем аутопоэзной, т.е. трансформационной, направленной на поиск инновационных путей развития в присутствии угроз [Chandler, Coafee, 2017], но не кибербезопасность, интерпретируемую в Стратегии в терминах защиты территории от угроз.

Европейская комиссия и Верховный представитель не демонстрируют последовательности в использовании и других терминов, создавая в Стратегии некий концептуальный хаос. Здесь мы видим примеры и классической безопасности, и стрессоустойчивости, и риск-менеджмента — категорий из разных эпистемных режимов безопасности в классификации К. Арадау [Aradau, 2017]. Что касается стрессоустойчивости, то в тексте Стратегии эта категория применяется для характеристики двух направлений из пяти (киберстрессоустойчивость и внешнеполитическая активность ЕС), тогда как остальные составляющие кибербезопасности рассматриваются по большей части в других терминах либо речь идет о самостоятельном регулировании странами-членами[32].

Более поздние документы ЕС показывают, что с течением времени были сделаны попытки применить категорию стрессоустойчивости системно, в том числе в вопросах киберпреступности, безопасности и обороны. Наиболее комплексной попыткой стало Сообщение Комиссии 2017 г., где подчеркивается необходимость перехода от реактивного к проактивному подходу к защите европейских обществ, ценностей, прав и свобод. Важно, что в данном Сообщении также отводится большая роль в обеспечении безопасности и стрессоустойчивости обществу и отдельным гражданам, тогда как, например, в Стратегии речь шла по большей части о государствах и бизнесе. Кроме того, достижение общего состояния кибербезопасности рисуется как вызов для всего общества. Эта идея прослеживается и в рабочем документе Еврокомиссии по оценке эффективности мер, предложенных в Стратегии[33].

Одним из ресурсов стрессоустойчивости потенциально видится сам ЕС как наднациональный актор, обладающий нужным

[32] Ibidem.

[33] Commission Staff Working Document Assessment of the EU 2013 Cybersecurity Strategy. European Commission. Brussels, 13.09.2017. SWD (2017) 295 final // European Commission. Available at: https://ec.europa.eu/transparency/regdoc/rep/other/SWD-2017-295-F1-EN-0-0.PDF (accessed: 23.03.2019).

набором компетенций и механизмов для борьбы с киберугрозами, причем, как указывается в Сообщении Комиссии 2017 г., вовлеченность Брюсселя увеличивается во всех компонентах политики кибербезопасности[34].

С одной стороны, согласно собственной оценке Еврокомиссией результатов реализации Стратегии (2013), представленной в 2017 г.[35], ограниченность компетенций ЕС в сфере безопасности и обороны препятствует применению всеохватывающих стрессоустойчивых подходов в кибербезопасности, а участие стран-членов в инициативах по кибероборонe носит скорее технический и выборочный характер.

С другой стороны, развитые рыночная и правовая составляющие кибербезопасности ЕС, а также традиционно сильный ценностный компонент его политики могут служить подспорьем для успешной стратегии кибербезопасности и обороны. Как отмечают многие исследователи, обилие координационных, консультационных и экспертных платформ, различных формальных и неформальных практик, низовой ответственности, многоакторность, а также приверженность ценностям свободы и правам человека в международном киберрегулировании — т.е. стрессоустойчивость — могут способствовать становлению ЕС как «мягкой» киберсилы на международной арене без радикальной трансформации современной модели сотрудничества в сфере безопасности и обороны [Dunn Cavelty, 2018; Christou, 2016].

Тон и аргументация упомянутого Сообщения демонстрируют, что изменение дискурса ЕС о кибербезопасности в сторону большей экосистемности мотивировано увеличением количества и сложности инцидентов в киберсфере, ростом убытков от киберпреступлений и, что особенно важно, политической мотивацией атак. При этом Комиссия отмечает, что теперь злонамеренные действия в киберпространстве угрожают не только экономикам стран-членов и перспективе строительства единого цифрового

---

[34] Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. European Commission. Brussels, 13.09.2017. JOIN (2017) 450 final // Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2017:0450:FIN (accessed: 20.07.2018).

[35] Commission Staff Working Document Assessment of the EU 2013 Cybersecurity Strategy. European Commission. Brussels, 13.09.2017. SWD (2017) 295 final // European Commission. Available at: https://ec.europa.eu/transparency/regdoc/rep/other/SWD-2017-295-F1-EN-0-0.PDF (accessed: 23.03.2019).

рынка, но и функционированию демократий, свободам и ценностям[36].

Уже после хакерских атак на правительственные учреждения Эстонии и другие эстонские сайты в 2007 г. кибератаки стали рассматриваться как отдельная серьезная угроза безопасности ЕС [Dunn Cavelty, 2018]. В заявлениях чиновников[37] и в стратегических документах делается акцент на политических угрозах, исходящих от конкретных государственных акторов или акторов, поддерживаемых отдельными странами, которые стремятся к реализации своих геополитических интересов[38]. Так, в Резолюции 2019 г. Европейский парламент обвиняет Россию в осуществлении слежки, кибер- и гибридных атак, а также во вмешательстве в выборы и референдумы в целях дестабилизации европейских обществ[39]. Подобная риторика сигнализирует о восприятии кибератак как *политических* угроз для стран-членов и самого ЕС, что может свидетельствовать о тенденции к секьюритизации данной проблематики.

---

[36] Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. European Commission. Brussels, 13.09.2017. JOIN (2017) 450 final // Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2017:0450:FIN (accessed: 20.07.2018).

[37] См., например: Speech by Vice-President Ansip on cybersecurity at the RSA Conference 2018. San Francisco, 18.04.2018 // European Commission. Available at: http://europa.eu/rapid/press-release_SPEECH-18-3430_en.htm (accessed: 26.07.2018); President Jean-Claude Juncker's State of the Union Address. Brussels. 13.09.2018 // European Commission. Available at: http://europa.eu/rapid/press-release_SPEECH-17-3165_en.htm (accessed: 26.07.2018).

[38] Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. European Commission. Brussels, 13.09.2017. JOIN (2017) 450 final // Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2017:0450:FIN (accessed: 20.07.2018); Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Tackling Online Disinformation: A European Approach. European Commission. Brussels, 26.04.2018. COM (2018) 236 final // Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0236&from=EN (accessed: 28.11.2018); Council conclusions on malicious cyber activities — approval. Council of the European Union. Brussels, 16.04.2018 (OR. en) 7925/18 // Council of the European Union. Available at: http://data.consilium.europa.eu/doc/document/ST-7925-2018-INIT/en/pdf (accessed: 29.03.2019).

[39] European Parliament resolution of 12 March 2019 on the state of EU-Russia political relations. European Parliament. (2018/2158(INI)) // European Parliament. Available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2019-0157+0+DOC+PDF+V0//EN (accessed: 14.03.2019).

По мнению Ф. Бурбо, подобная артикуляция угроз может означать, что стрессоустойчивость используется акторами секьюритизации как эвфемизм [Bourbeau, 2017] и носит декларативный характер. Эксперт объясняет, что в подобной ситуации правительство стремится сконструировать наиболее убедительную для общества угрозу и представить любые изменения или неопределенности как опасность, которой нужно сопротивляться [Dovers, Handmer, 1992; Bourbeau, 2015, 2017]. По сути, это означает отход от стрессоустойчивого управления. Вместе с тем секьюритизация киберсферы невыгодна ЕС и вряд ли будет последовательно реализована, так как основными стимулами для развития политики Европейского союза в области кибербезопасности остаются развитие цифрового рынка через технические вопросы регулирования и вовлечение гражданского общества. Что касается артикуляции рисков, то это можно рассматривать как попытку сознательного использования институтами ЕС внешнего стимула для проведения внутренних изменений в процессе реализации стратегии стрессоустойчивого управления [Chandler, Coaffee, 2017]. Последние отчеты Европола показывают, что секьюритизация кибератак используется ЕС достаточно избирательно. Согласно данным Агентства источники большинства кибератак, совершенных против объектов в ЕС, находились на территории стран-членов, а не за пределами Союза. Таким образом, киберугрозы лишь в редких случаях носят внешний характер[40].

Активизация международной деятельности ЕС в сфере кибербезопасности, которая была артикулирована в Стратегии, может быть, во-первых, одним из способов влиять на партнеров, например, через продвижение технических реформ, направленных на защиту инфраструктуры и информации, что имеет для ЕС не только чисто прикладную, но и ценностную составляющую. Во-вторых, она может рассматриваться как возможность оказать влияние на глобальное управление интернетом, связать вопросы внутренней безопасности с внешней.

---

[40] 2018 Europol Internet Organised Crime Threat Assessment (IOCTA) // Europol. Available at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018 (accessed: 23.03.2019); 2017 Europol Internet Organised Crime Threat Assessment (IOCTA) // Europol. Available at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017 (accessed: 23.03.2019).

* * *

Анализ документов ЕС показывает проникновение категории «стрессоустойчивость» в европейский дискурс о кибербезопасности. Стрессоустойчивость позволяет Евросоюзу пересмотреть традиционное понимание безопасности и в целом переосмыслить взаимосвязь между состояниями опасности и безопасности. В современной ситуации глобальной взаимозависимости угрозы носят системный характер, и правительства часто не способны обеспечить качественное регулирование той или иной сферы своей деятельности без привлечения других акторов, что особенно проявляется в области кибербезопасности. Уникальная природа киберсреды, невозможность предусмотреть, выявить и подготовиться ко всем угрозам требуют иных подходов в безопасности, отличных от простого выявления и защиты от угроз. Стрессоустойчивость представляется в этой связи удачным решением благодаря принципиальной установке на принятие состояния опасности как неотъемлемого элемента современности. Тем не менее документы ЕС демонстрируют, что стрессоустойчивость представляет собой довольно абстрактную категорию, консенсус о наполнении ее смыслом пока не достигнут. Отсутствие последовательного определения ее сути и параметров ее достижения ярко проявляется даже в новейших документах ЕС.

Тем не менее можно констатировать, что политика Брюсселя в области кибербезопасности в процессе своего развития и институционального оформления постепенно все больше перенимает логику стрессоустойчивости. Принципы, характеризующие подходы ЕС в данной области (многоакторность, общая ответственность, приверженность свободе и правам человека, вера в интернет для всех) — позволяют при желании перестроить все управление этой сферой на принципах стрессоустойчивости. Ре-интерпретация отдельных составляющих киберсреды как экосистемы в документах ENISA видится в этой связи органичным, естественным и логичным процессом. При этом подчеркивание экосистемных свойств сферы кибербезопасности не только позволяет говорить о переосмыслении безопасности в терминах стрессоустойчивости, но также сигнализирует о стремлении ЕС стать локомотивом изменений в этой сфере.

Проблемным моментом дискурса ЕС о стрессоустойчивости в области кибербезопасности в настоящий момент является его противоречивость. С одной стороны, было сформулировано

отдельное понятие «киберстрессоустойчивость», однако его применение ограничивается по большей части политикой в области защиты информационной инфраструктуры, исключая киберпреступления и кибероборону. Такое разделение может говорить о фрагментированности дискурса кибербезопасности, о сосуществовании одновременно различных практик безопасности, что может затруднить формирование экосистемы кибербезопасности на принципах принятия рисков, а не защиты от них. С другой стороны, можно предположить, что именно стремление к достижению киберстрессоустойчивости единого рынка может стать стимулом для перенесения подобного подхода и на другие сферы.

СПИСОК ЛИТЕРАТУРЫ

1. Гудалов Н., Тулупов Д. Семиотика стрессоустойчивости в международных отношениях: многообразие академических и политических смыслов // Полития. 2018. № 1 (88). С. 135–147. DOI: 10.30570/2078-5089-2018-88-1-135-147.

2. Зворыкина Ю.В., Земледельцев С.В. О подходах к обеспечению кибербезопасности в ЕС // Противодействие терроризму. Проблемы XXI века — Counter-terrorism. 2014. № 1. С. 38–42.

3. Кацы Д.В., Шматкова Л.П. Кибербезопасность и развитие цифровой экономики в Европейском союзе // Евразийский юридический журнал. 2018. № 3 (118). С. 343–345.

4. Пантин В.И., Кардаева Н.В. Кибербезопасность: проблемы формирования единой политики в Европейском союзе // Вестник Пермского университета. Политология. 2018. № 3. С. 5–18. DOI: 10.17072/2218-1067-2018-3-5-18.

5. Романова Т.А. Категория «стрессоустойчивость» в Европейском союзе // Современная Европа. 2017. № 4 (76). С. 17–28.

6. Шафеев К.А. Правовое регулирование ответственности за киберпреступления в праве Европейского союза // Право в сфере Интернета. М.: Статут, 2018. С. 7–26.

7. Aradau C. The promise of security. Resilience, surprise, and epistemic politics // The Routledge handbook of international resilience / Ed. by D. Chandler, J. Coaffee. London: Routledge, 2017. P. 79–91.

8. Barrinha A., Renard T. Cyber-diplomacy: The making of an international society in the digital age // Global Affairs. 2017. Vol. 3. No. 4–5. P. 353–364.

9. Bendiek A., Bossong R., Schulze M. The EU's revised cybersecurity strategy: Half-hearted progress on far-reaching challenges // Stiftung Wissenschaft und Politik. Deutsches Institut für Internationale Politik und Sicherheit. 2017. No. 47. Available at: http://nbn-resolving.de/urn:nbn:de:0168-ssoar-55103-4 (accessed: 28.11.2018).

10. Bourbeau P. Resiliencism: Premises and promises in securitisation research // Resilience. International Policies, Practices and Discourse. 2013. Vol. 1. No. 1. P. 3–17. DOI: 10.1080/21693293.2013.765738.

11. Bourbeau P. Resilience and international politics: Premises, debates, agenda // International Studies Review. 2015. Vol. 17. No. 3. P. 374–395. DOI: https://doi.org/10.1111/misr.12226.

12. Bourbeau P. Resilience, security, and world politics // The Routledge handbook of international resilience / Ed. by D. Chandler, J. Coaffee. London: Routledge, 2017. P. 26–37.

13. Brassett J., Vaughan-Williams N. Security and the performative politics of resilience: Critical infrastructure protection and humanitarian emergency preparedness // Security Dialogue. 2015. Vol. 46. No. 1. P. 32–50. DOI: 10.1177/0967010614555943.

14. Buzan B., Wæver O., Wilde J. Security: A new framework for analysis. London; Boulder, CO: Lynne Rienner Publishers, 1998.

15. Carrapico H., Barrinha A. European Union cyber security as an emerging research and policy field // European Politics and Society. 2018. Vol. 9. No. 3. P. 299–303. DOI: 10.1080/23745118.2018.1430712.

16. Chandler D., Coaffee J. Introduction. Contested paradigms of international resilience // The Routledge handbook of international resilience / Ed. by D. Chandler, J. Coaffee. London: Routledge, 2017. P. 3–9.

17. Christou G. The challenges of cybercrime governance in the European Union // European Politics and Society. 2018. Vol. 19. No. 3. P. 355–375.

18. Christou G. Cybersecurity in the European Union: Resilience and adaptability in governance policy. Houndmills, Basingstoke: Palgrave Macmillan, 2016.

19. Christou G. The EU's approach to cybersecurity // EU-Japan security cooperation: Challenges and opportunities. University of Essex. Online paper series, 2017. Available at: https://pdfs.semanticscholar.org/24d4/4e449c490610bd3f341b28765dc8da1e2db6.pdf (accessed: 28.11.2018).

20. Coaffee J., Fussey P. The politics of security-driven resilience // The Routledge handbook of international resilience / Ed. by D. Chandler, J. Coaffee. London: Routledge, 2017. P. 293–306.

21. Dovers S.R., Handmer J.W. Uncertainty, sustainability, and change // Global Environmental Change. 1992. Vol. 2. No. 4. P. 262–276. DOI: 10.1016/0959-3780(92)90044-8.

22. Dunn Cavelty M. Europe's cyber-power // European Politics and Society. 2018. Vol. 19. No. 3. P. 304–320. DOI: 10.1080/23745118.2018.1430718.

23. Dunn Cavelty M. The normalization of cyber-international relations // Strategic trends 2015: Key developments in global affairs / Ed. by O. Thränert, M. Zapfe. Zurich: Center for Security Studies (CSS), 2015. P. 81–98.

24. Dunn Cavelty M. A resilient Europe for an open, safe and secure cyberspace // Occasional Papers. Swedish Institute of International Affairs. 2013. Vol. 23. P. 3–13.

25. Dunn Cavelty M., Kaufmann M., Kristensen K.S. Resilience and (in)security: Practices, subjects, temporalities // Security Dialogue. 2015. Vol. 46. No. 1. P. 3–14. DOI: 10.1177/0967010614559637.

26. Evans B., Reid J. Dangerously exposed: The life and death of the resilient subject // Resilience. 2013. Vol. 1. No. 2. P. 83–98. DOI: 10.1080/21693293.2013.770703.

27. Farrand B. Combatting physical threats posed via digital means: The European Commission's developing approach to the sale of counterfeit goods on the Internet // European Politics and Society. 2018. Vol. 19. No. 3. P. 338–354. DOI: 10.1080/23745118.2018.1430721.

28. Herrington L., Aldrich R. The future of cyber-resilience in an age of global complexity // Politics. 2013. Vol. 33. No. 4. P. 299–310. DOI: 10.1111/1467-9256.12035.

29. Holling C.S. Resilience and stability of ecological systems // Annual Review of Ecology and Systematics. 1973. Vol. 4. No. 1. P. 1–23. DOI: 10.1146/annurev.es.04.110173.000245.

30. Kaufmann M. Resilience governance and ecosystemic space: A critical perspective on the EU approach to Internet security // Environment and Planning D: Society and Space. 2015. Vol. 33. No. 3. P. 512–527. DOI: 10.1177/0263775815594309.

31. Manjikian M. From global village to virtual battlespace: The colonizing of the Internet and the extension of Realpolitik // International Studies Quarterly. 2010. No. 54. P. 381–401. DOI: 10.1111/j.1468-2478.2010.00592.

32. Milliano C., Jurriens J. Realities of resilience in practice: Lessons learnt through a pilot EU Aid Volunteer Initiative // Resilience. 2016. Vol. 4. No. 3. P. 79–94. DOI 10.1080/21693293.2015.1094171.

33. Renard T. EU cyber partnerships: Assessing the EU strategic partnerships with third countries in the cyber domain // European Politics and Society. 2018. Vol. 19. No. 3. P. 321–337. DOI: 10.1080/23745118.2018.1430720.

34. Rothe D. Climate change and security: From paradigmatic resilience to resilience multiple // The Routledge handbook of international resilience / Ed. by D. Chandler, J. Coaffee. London: Routledge, 2017. P. 171–184.

35. Zebrowski C., Sage D. Resilience and critical infrastructure: Origins, theories, and critiques // The Palgrave handbook of security, risk and intelligence. London: Palgrave MacMillan, 2016. P. 117–135.

T.A. Romanova, A.N. Malova

THE EUROPEAN UNION CYBERSECURITY POLICY: OPERATIONALIZATION OF THE RESILIENCE CONCEPT

Saint Petersburg State University
7/9 Universitetskaya embankment, Saint-Petersburg, 199034

The unique nature of cyberspace, characterized by interdependence between material and social objects as well as the complexity of its structures, urges leading actors of world politics to seek new strategies of organizing their activities within this area. In the European Union, cybersecurity issues are debated on the basis of the resilience category. In this context the latter is understood as a system's ability to adjust to new challenges, flexibly respond to threats, and successfully recover after blows. Using a discourse analysis approach the authors examine the genesis of the resilience discourse and the logic of its development in the EU cybersecurity policy, reveal nuances of how this category is interpreted in official documents as well as point out difficulties regarding practical application of this category.

The authors trace a gradual evolution of the EU approach towards cybersecurity from the well-established definitions of cyberspace to the ecosystem

terms and concepts, which are particularly relevant to the resilience-based concept of cybersecurity. Within this approach, the Internet is considered not as a static object but as a complex heterogeneous system where a state of security is inextricably linked to a state of insecurity.

There is no single and coherent definition of resilience in the EU official documents yet. Nevertheless, it is stressed that one can see a gradual transformation of the official discourse from purely technical definitions to inclusion of a wider range of socio-political factors. However, the EU official discourse on this issue remains highly controversial. This refers, for instance, to the lack of a unified understanding of the 'cyberresilience' and 'cybersecurity' concepts. The authors highlight a tendency towards increasing securitization of the cybersphere in the EU cybersecurity discourse, which might lead to the narrowing of the concept of 'cyberresilience' and its transformation into a common euphemism. At the same time the authors conclude that the EU itself is not interested in oversecuritization of the cybersphere, and thus the EU cybersecurity policy will eventually evolve towards resilience-based approaches.

Keywords: the European Union, resilience, cybersecurity, cyberthreats, cyberresilience, cyberecosystem, securitization, Critical Information Infrastructure, European Union Agency for Network and Information Security, ENISA.

About the authors: *Tatiana A. Romanova* — PhD (Political Science), Associate Professor at the Saint-Petersburg State University (e-mail: t.romanova@spbu.ru, romanova@mail.sir.edu); *Alyona N. Malova* — PhD Candidate at the Saint-Petersburg State University (e-mail: alenamalova5@gmail.com).

Acknowledgements: The reported study was funded by the Russian Science Foundation according to the research project 17-18-01110.

REFERENCES

1. Gudalov N., Tulupov D. 2018. Semiotika stressoustoichivosti v mezhdunarodnyh otnosheniyah: mnogoobrazie akademicheskih i politicheskih smyslov [Semiotics of resilience in international relations: The diversity of academic and political meanings]. *Politiya*, vol. 1, no. 88, pp. 135–147. DOI: 10.30570/2078-5089-2018-88-1-135-147. (In Russ.)

2. Zvorykina Y.V., Zemledeltsev S.V. 2014. O podkhodakh k obespecheniyu kiberbezopasnosti v ES [EU cyber security approaches]. *Protivodeystvie terrorizmu. Problemy XXI veka — Counter-terrorism*, no. 1, pp. 38–42. (In Russ.)

3. Katsy D.V., Shmatkova L.P. 2018. Kiberbezopasnost i razvitie tsifrovoi ekonomiki v Evropeiskom soyuze [Cybersecurity and development of the digital economy in the European Union]. *Evraziiskii yuridicheskii zhurnal*, no. 3, vol. 118, pp. 343–345. (In Russ.)

4. Pantin V.I., Kardaeva N.V. 2018. Kiberbezopasnost: problemy formirovaniya edinoi politiki v Evropeiskom soyuze [Cybersecurity: Challenges for building the

EU common cybersecurity policy]. *Vestnik Permskogo universiteta. Politologiya*, no. 3, pp. 5–18. DOI: 10.17072/2218-1067-2018-3-5-18. (In Russ.)

5. Romanova T.A. 2017. Kategoriya 'stressoustoichivost' v Evropeiskom soyuze [Resilience category in the European Union]. *Sovremennaya Evropa*, vol. 4, no. 76, pp. 17–28. (In Russ.)

6. Shafeev K.A. 2018. Pravovoe regulirovanie otvetstvennosti za kiberprestupleniya v prave Evropeiskogo soyuza [Responsibility for cybercrime in the EU law]. In Rozhkova M.A. (ed.). *Pravo v sfere interneta* [Internet law]. Moscow, Statut Publ., pp. 7–26. (In Russ.)

7. Aradau C. 2017. The promise of security. Resilience, surprise and epistemic politics. In Chandler D., Coaffee J. (eds.). *The Routledge handbook of international resilience*. London, Routledge, pp. 79–91.

8. Barrinha A., Renard T. 2017. Cyber-diplomacy: The making of an international society in the digital age. *Global Affairs*, vol. 3, no. 4–5, pp. 353–364.

9. Bendiek A., Bossong R., Schulze M. 2017. The EU's revised cybersecurity strategy: Half-hearted progress on far-reaching challenges. *Stiftung Wissenschaft und Politik -SWP- Deutsches Institut für Internationale Politik und Sicherheit*, vol. 47. Available at: http://nbn-resolving.de/urn:nbn:de:0168-ssoar-55103-4 (accessed: 28.11.2018).

10. Bourbeau P. 2013. Resiliencism: Premises and promises in securitisation research. *Resilience. International Policies, Practices and Discourse*, vol. 1, no. 1, pp. 3–17. DOI: 10.1080/21693293.2013.765738.

11. Bourbeau P. 2015. Resilience and international politics: Premises, debates, agenda. *International Studies Review*, vol. 17, no. 3, pp. 374–395. DOI: 10.1111/misr.12226.

12. Bourbeau P. 2017. Resilience, security, and world politics. In Chandler D., Coaffee J. (eds.). *The Routledge handbook of international resilience*. London, Routledge, pp. 26–37.

13. Brassett J., Vaughan-Williams N. 2015. Security and the performative politics of resilience: Critical infrastructure protection and humanitarian emergency preparedness. *Security dialogue*, vol. 46, no. 1, pp. 32–50. DOI: 10.1177/0967010614555943.

14. Buzan B., Wæver O., Wilde J. 1998. *Security: A new framework for analysis*. London, Boulder, Lynne Rienner Publishers.

15. Carrapico H., Barrinha A. 2018. European Union cyber security as an emerging research and policy field. *European Politics and Society*, vol. 19, no. 3, pp. 299–303. DOI: 10.1080/23745118.2018.1430712.

16. Chandler D., Coaffee J. 2017. Introduction. Contested paradigms of international resilience. In Chandler D., Coaffee J. (eds.). *The Routledge handbook of international resilience*. London, Routledge, pp. 3–9.

17. Christou G. 2018. The challenges of cybercrime governance in the European Union. *European Politics and Society*, vol. 19, no. 3, pp. 355–375. DOI: 10.1080/23745118.2018.1430722.

18. Christou G. 2016. *Cybersecurity in the European Union: Resilience and adaptability in governance policy*. Houndmills, Basingstoke, Palgrave Macmillan.

19. Christou G. 2017. The EU's approach to cybersecurity. *EU-Japan security cooperation: Challenges and opportunities*. University of Essex. Online paper series. Available at: https://pdfs.semanticscholar.org/24d4/4e449c490610bd3f341b28765dc8da1e2db6.pdf (accessed: 28.11.2018).

20. Coaffee J., Fussey P. 2017. The politics of security-driven resilience. In Chandler D., Coaffee J. (eds.). *The Routledge handbook of international resilience*. London, Routledge, pp. 293–306.

21. Dovers S.R., Handmer J.W. 1992. Uncertainty, sustainability and change. *Global Environmental Change*, vol. 2, no. 4, pp. 262–276. DOI: 10.1016/0959-3780(92)90044-8.

22. Dunn Cavelty M. 2018. Europe's cyber-power. *European Politics and Society*, vol. 19, no. 3, pp. 304–320. DOI: https://doi.org/10.1080/23745118.2018.1430718.

23. Dunn Cavelty M. 2015. The normalization of cyber-international relations. In Thränert O., Zapfe M. (eds.). *Strategic trends. Key developments in global affairs*. Center for Security Studies, ETH Zurich, pp. 81–98.

24. Dunn Cavelty M. 2013. A resilient Europe for an open, safe and secure cyberspace. *Occasional Papers, Swedish Institute of International Affairs*, vol. 23, pp. 3–13.

25. Dunn Cavelty M., Kaufmann M., Kristensen K.S. 2015. Resilience and (in)security: Practices, subjects, temporalities. *Security Dialogue*, vol. 46, no. 1, pp. 3–14. DOI: https://doi.org/10.1177/0967010614559637.

26. Evans B., Reid J. 2013. Dangerously exposed: The life and death of the resilient subject. *Resilience*, vol. 1, no. 2, pp. 83–98. DOI: 10.1080/21693293.2013.770703.

27. Farrand B. 2018. Combatting physical threats posed via digital means: The European Commission's developing approach to the sale of counterfeit goods on the Internet. *European Politics and Society*, vol. 19, no. 3, pp. 338–354. DOI: 10.1080/23745118.2018.1430721.

28. Herrington L., Aldrich R. 2013. The future of cyber-resilience in an age of global complexity. *Politics*, vol. 33, no. 4, pp. 299–310. DOI: 10.1111/1467-9256.12035.

29. Holling C.S. 1973. Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics*, vol. 4, no. 1, pp. 1–23. DOI: 10.1146/annurev.es.04.110173.000245.

30. Kaufmann M. 2015. Resilience governance and ecosystemic space: A critical perspective on the EU approach to Internet security. *Environment and Planning D: Society and Space*, vol. 33, no. 3, pp. 512–527. DOI: 10.1177/0263775815594309.

31. Manjikian M. 2010. From global village to virtual battlespace: The colonizing of the Internet and the extension of Realpolitik. *International Studies Quarterly*, no. 54, pp. 381–401. DOI: 10.1111/j.1468-2478.2010.00592.

32. Milliano C., Jurriens J. 2016. Realities of resilience in practice: Lessons learnt through a pilot EU Aid Volunteer Initiative. *Resilience*, vol. 4, no. 3, pp. 79–94. DOI 10.1080/21693293.2015.1094171.

33. Renard T. 2018. EU cyber partnerships: Assessing the EU strategic partnerships with third countries in the cyber domain. *European Politics and Society*, vol. 19, no. 3, pp. 321–337. DOI: 10.1080/23745118.2018.1430720.

34. Rothe D. 2017. Climate change and security: From paradigmatic resilience to resilience multiple. In Chandler D., Coaffee J. (eds.). *The Routledge handbook of international resilience*. London, Routledge, pp. 171–184.

35. Zebrowski C., Sage D. 2016. Resilience and critical infrastructure: Origins, theories and critiques. In Dover R., Huw D., Goodman MS. (eds.). *The Palgrave handbook of security, risk and intelligence*. London, Palgrave MacMillan, pp. 117–135.