ОРИГИНАЛЬНАЯ СТАТЬЯ

DOI: 10.26794/2226-7867-2022-12-1-70-74
УДК 32(045)

Методологические проблемы формирования концепции национальной кибербезопасности Российской Федерации

Г.Ю. Никипорец-Такигава[a], Е.В. Бучнев[b]
Российский государственный социальный университет, Москва, Россия
[a] https://orcid.org/0000-0002-5611-8396; [b] https://orcid.org/0000-0002-5511-9784

АННОТАЦИЯ

Развитие информационных технологий и повсеместная цифровизация многих видов жизнедеятельности создают проблему информационной защищенности индивида в цифровом пространстве, а также указывают на необходимость разработки системы контроля за данным пространством. В предлагаемой статье рассматриваются основные проблемы концепции российской политики национальной кибербезопасности. Авторы отмечают, что на политику безопасности и защиты информационных ресурсов и данных влияют две разнонаправленные тенденции: отсутствие четкого определения интернет-пространства и его границ в законодательной базе и интерес государственного сектора к независимости и защищенности этого пространства от возможных угроз и атак. Формирование концепции национального интереса в поле кибербезопасности ведет к решению сразу нескольких задач как на внутреннем поле цифрового присутствия, так и на международной арене. Авторы приводят ряд основополагающих терминов, которые будут интересны и необходимы для дальнейших исследований в данном направлении, и обращают внимание на недостаточную терминологическую разработанность данной темы.
Ключевые слова: кибербезопасность; цифровое пространство; киберпреступность; интернет-пространство; цифровизация; киберугроза

Для цитирования: **Никипорец-Такигава Г.Ю., Бучнев Е.В. Методологические проблемы формирования концепции национальной кибербезопасности Российской Федерации. *Гуманитарные науки. Вестник Финансового университета*. 2022;12(1):70-74. DOI: 10.26794/2226-7867-2022-12-1-70-74**

ORIGINAL PAPER

Methodological Problems Concerning Concept's Formation of the National Cybersecurity in the Russian Federation

G. Yu. Nikiporets-Takigawa[a], E.V. Buchnev[b]
Russian State Social University (RSSU), Moscow, Russia
[a] https://orcid.org/0000-0002-5611-8396; [b] https://orcid.org/0000-0002-5511-9784

ABSTRACT

The development of information technologies and the widespread digitalisation of many life factors needs an individual's information security in the digital space. Also, it indicates the need to develop a system of control over this space. This article discusses the main problems concerning the Russian national cybersecurity policy concept. The authors note that two multidirectional trends influence the implementation of the security policy and the protection of information resources and data. First, it is the lack of a clear definition of the Internet space and its boundaries in the legislative framework. Second, the significant interest of the public sector in the independence and security of this space from possible threats and attacks. The formation of the concept of national interest in the field of cybersecurity leads to the solution of several tasks at once, both in the internal domain of digital presence and in the international arena. The authors provide several fundamental terms that will be interesting and necessary for further research in this direction. We have drawn attention to the insufficient terminological elaboration of this topic.
Keywords: cybersecurity; digital space; cybercrime; internet space; digitalisation; cyber threat

For citation: **Nikiporets-Takigawa G. Yu., Buchnev E.V. Methodological problems concerning concept's formation of the national cybersecurity in the Russian Federation. *Gumanitarnye Nauki. Vestnik Finasovogo Universiteta = Humanities and Social Sciences. Bulletin of the Financial University*. 2022;12(1):70-74. (In Russ.). DOI: 10.26794/2226-7867-2022-12-1-70-74**

ВВЕДЕНИЕ

На данном этапе развития цивилизации интернет-пространство формирует новый процесс социализации. Если в рамках географических границ и политических административных единиц мы говорим о развитии и возможном сворачивании процесса глобализации, в цифровом пространстве глобализация — процесс, состоявшийся и практически завершившийся. Возникает новая форма государственности — e-government и e-governance. Интернет-пространство создает законы и нормы поведения и участия. Это пространство, как и любое другое, подвержено угрозам различного характера, но, в отличие от нецифровых пространств, угрозам неосязаемым и в силу этого не поддающимся контролю. Развитие информационных технологий обусловило возникновение новых видов и причин конфликтов и кризисов. Интернет-пространство, в частности как политический институт, развивается стремительнее других нецифровых пространств. Оно не просто отвечает на запросы, но и создает прецеденты[1], казавшиеся невозможными несколько лет назад[2]. Подобные обстоятельства указывают не только на особую важность процессов, происходящих в интернет-пространстве, но и на необходимость их защиты.

Система кибербезопасности должна включать те меры и действия, которые способствуют защите процессов, операций и информации внутри интернет-пространства. Однако существуют трудности в идентификации, понимании характера, источника и направления кибератак, и это обстоятельство актуализирует необходимость формирования национальной концепции кибербезопасности.

Стратегия национальной кибербезопасности должна работать как на персонализированную защиту индивидуума, так и на защиту государства и социума. Если по отношению к социуму в целом данная политика должна выступать в качестве одной из функций государства, то в случае киберзащиты индивидуумов участие государства требует сложной детализации.

МЕТОДЫ

В рамках исследования использовался классический метод анализа документации и нормативно-правовой базы Российской Федерации. Критический анализ позволил выявить проблемное поле, очертить круг необходимых дополнительных исследований, способствующих дальнейшему формированию концепции государственного присутствия в интернет-пространстве, а также определить степень взаимодействия в нем государства и гражданина. Для выборки был проведен контент-анализ концепции стратегии кибербезопасности Российской Федерации (проект)[3] и Руководящих указаний по кибербезопасности[4], позволивший прояснить заинтересованность в кибербезопасности как залоге независимости государственной политики и власти в целом.

РЕЗУЛЬТАТЫ

Развитие отечественных информационных технологий в России, как и в других странах, происходило преимущественно в области военно-промышленного комплекса и выступало не только гарантом безопасности и подконтрольности советского вооружения, но и подтверждало высокий уровень знаний советских специалистов и их возможность самостоятельно разрабатывать и исследовать информационное пространство как таковое. Впоследствии, в связи с распадом СССР и экономическим и социальным кризисами, информационные технологии в сознании граждан все чаще стали ассоциироваться с определенным уровнем благосостояния и избранностью. Первое десятилетие существования независимого российского государства ставило перед населением вопросы выживания во время социального и экономического кризиса, а также диктовало необходимость знакомства с информационными технологиями, которые постепенно стали проникать в быт рядовых граждан. Цифровизация проникла практически во все сферы жизнедеятельности: денежные средства начали массового вытесняться из обращения благодаря банковским картам, а в дальнейшем и технологиям бесконтактной оплаты; электросамокаты и электровелосипеды с внутренним программным обеспечением позволили большому количеству граждан передвигаться

[1] URL: https://anri.org.ru/2019/06/09/v-zashhitu-ivana-golunova/

[2] URL: https://style.rbc.ru/life/5f1ffd909a7947b6725c35ac

[3] Концепция стратегии кибербезопасности Российской Федерации. URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf

[4] Международный стандарт ИСО/МЭК 27032:2012. URL: https://www.iso.org/standard/44375.html

на недоступные ранее расстояния в крупных городах [1]. Цифровизация услуг образования делает процесс получения знаний и умений не только более быстрым, но и формирует безбарьерное образовательное пространство [2, 3]; медицинские и муниципальные услуги, которые начали развиваться в столице, позволяют перевести огромный объем работы в цифровое поле [4].

Таким образом, в развитых странах сформировалось общество потребления, получившее возможность использовать технологические средства и информационное пространство, но не выработавшее достаточного опыта по защите этого пространства и своего нахождения в нем. На данный момент в государстве существуют не только региональные[5], но и федеральные интернет-ресурсы[6], которые аккумулируют в себе сразу несколько функций и институтов [5]: медицина, образование, транспорт, Пенсионный фонд, трудовая деятельность. При этом оценить степень защищенности информации и доверия к такой защите у населения достаточно сложно, так как известные исследовательские центры не располагают подобной статистикой. Хотя подобная информация могла бы быть полезна для целого ряда исследований в контексте киберзащиты и кибербезопасности [6].

Отдельно следует отметить попытки государства сформировать нормативную базу для выстраивания политики кибербезопасности. Речь идет о стратегии кибербезопасности Российской Федерации [7]. Не вызывает сомнения тот факт, что развитие цифровых технологий в России происходило намного быстрее, чем во многих странах Европы, Африки и Азии. Однако разграничение интернет- и информационного пространства происходит в нашей стране достаточно медленно, о чем свидетельствует наличие двух отдельных терминов: «интернет-пространство» и «цифровое пространство».

Процесс формирования национальной стратегии, начавшийся в 2013–2014 гг., не привел к созданию официального документа, закрепляющего обязанности государства в отношении обеспечения кибербезопасности. Однако в 2014 г. был разработан и предложен к обсуждению проект концепции стратегии кибербезопасности Российской Федерации. Основной задачей указанной концепции, как следовало из введения, было обоснование актуальности формирования национальной политики интернет-безопасности. В данном проекте была предпринята попытка закрепить основные принципы национальной стратегии и ее место в государственно-правовой системе Российской Федерации. Концепция рассматривала цифровизацию как неотъемлемую составляющую развития современного демократического государства, ориентированного на эффективность и социальную ответственность, а внедрение цифровых процессов в систему государственного и экономического управления — как логичный критерий совершенствования самой системы.

Данный документ должен был аккумулировать в себе предыдущие предложения и разработки[7], направленные на формирование множества аспектов российской информационной безопасности[8,9]. Тем не менее особого внимания заслуживает попытка представить интернет-пространство как систему отношений государства и гражданина, заинтересованных в безопасности личности и информации.

В рамках проведенного анализа документа был выделен пункт V указанной стратегии, где сформулированы основные принципы, выступающие базисом для стратегии государственной кибербезопасности. Проект предлагал 6 принципов, каждый из которых затрагивал: участников системы взаимоотношений в интернет-пространстве, первостепенную защиту личности (либо организации) и приравненной к ней информации, необходимость сотрудничества всех участников системы взаимоотношений для обеспечения максимальной защищенности, границы ответственности сторон в случае возникновения потенциальных киберугроз, важность оценки приоритетности риска кибербезопасности и возможных негативных последствий.

Проектная концепция позволила выявить государственные интересы, границу

[5] Сайт мэра Москвы. URL: https://www.mos.ru

[6] ГОСУСЛУГИ. URL: https://www.gosuslugi.ru

[7] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

[8] Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 05.12.2016 № 646).

[9] Стратегия развития информационного общества в Российской Федерации (утв. Указом Президента РФ от 07.02.2008 № Пр-212).

необходимой защиты и своего (государственного) присутствия в информационном пространстве. Сами взаимоотношения государства и гражданина рассматривались как партнерские, взаимовыгодные и взаимно необходимые.

Для обеспечения кибербезопасности государство предложило не просто идентифицировать возникающие угрозы, но и координировать действия всех участников, присутствующих в информационном поле. Данная система позволила бы обеспечить максимально эффективное использование государственных усилий по поддержанию защиты ресурсов и выбор рациональных методов защиты.

Следует отметить, что в данном документе интернет-пространство понимается как независимое поле интересов, где государство должно помочь обеспечить максимальную защиту своих граждан. Следовательно, такая защита от всех возможных киберугроз и кибератак — помощь гражданам от государства, что не предполагает полного контроля и вмешательства с его стороны в интернет-пространство. Более того, имеются в виду именно совместные усилия граждан и государства по обеспечению личной кибербезопасности, что подразумевает также и большую степень усилий самого гражданина по обеспечению своей защищенности. Таким образом, именно данное сотрудничество государства и гражданина будет формировать благоприятную среду для функционирования механизмов защиты и создаст защищенность всего интернет-пространства. Из этого следует, что кибербезопасность — это не система законов и требований, а система кооперации внутри интернет-пространства. Этот аспект особенно важен в настоящее время (когда все чаще звучат призывы о независимости и автономности российского интернета, а следовательно, и интернет-пространства), так как он позволяет понять, что существуют концепции, которые не ставят своей целью подчинение интернет-пространства государству, но пытаются сформировать новый вид сотрудничества с гражданином.

ПЕРСПЕКТИВЫ

Формирование национальной политики кибербезопасности — процесс длительный и комплексный. Существование независимого, но безопасного для государства и граждан интернет-пространства — залог успешного функционирования не только экономических и политических институтов государства (обеспечение которого является одной из первостепенных функций государства как такового), но и общества в целом. Исследование проблемных зон нормативно-правовой базы политики государственной кибербезопасности должно стать основой для прояснения и разделения государственной и личной ответственности по созданию безопасного интернет-пространства, для разграничения защиты этого пространства и использования его государством в определенных целях.

Национальная кибербезопасность подразумевает не только нормативно-правовое регулирование данного поля взаимоотношений, но и развитие грамотности использования интернет-ресурсов, цифровой культуры; формирование четкого представления о личных цифровых данных гражданина, требующих такой же защиты, как физические и материальные ресурсы.

СПИСОК ИСТОЧНИКОВ

1. Степанов В.И. Создание инфраструктуры велосипедного транспорта в г. Москве. *Большая Евразия: Развитие, безопасность, сотрудничество.* 2020;3(1):938–940.
2. Понизовкина И.Ф. Цифровизация высшего образования: перспективы и риски. *Право и практика*. 2020;(1):194–202.
3. Лукьянец А.Н., Ельмендеева М.А. Педагогические технологии в эпоху цифровизации высшего образования. *Азимут научных исследований: педагогика и психология*. 2020;9(4):171–173.
4. Шандора Н. Цифровизация системы здравоохранения: опыт и перспективы. *Наука и инновации*. 2020;(2):38–43. URL: https://doi.org/10.29235/1818–9857–2020–2–38–43
5. Hayes R.A. One click, many meanings: interpreting paralinguistic digital affordances in social media. *Journal of Broadcasting & Electronic Media*. 2016;(60):171–187.
6. Урнов М.Ю. Россия: виртуальные и реальные политические перспективы. *Общественные науки и современность*. 2014;(5):52–62.
7. Литвинов Д.А. Оценка политики России в области кибербезопасности и возможные варианты ее совершенствования. *Вестник науки и образования*. 2019;19–2(73):76–82.

REFERENCES

1. Stepanov V. I. Creation of cycling infrastructure in Moscow. *The Greater Eurasia: Development, security, cooperation = Bol'shaya Evraziya: Razvitie, bezopasnost', sotrudnichestvo*. 2020;3(1):938–940. (In Russ.).
2. Ponizovkina I. F. Digitalisation of higher education: prospects and risks. *Law and practice = Pravo i praktika*. 2020;(1):194–202. (In Russ.).
3. Lukyanets A. N., Elmendeeva M. A. Pedagogical technologies in the era of digitalisation of higher education. *The azimuth of scientific research: pedagogy and psychology = Azimut nauchnykh issledovanii: pedagogika i psikhologiya*. 2020;9(4):171–173. (In Russ.).
4. Shandora N. Digitalization of the healthcare system: experience and prospects. *Science and innovation = Nauka i innovatsii*. 2020;(2):38–43. URL: https://doi.org/10.29235/1818–9857–2020–2–38–43. (In Russ.).
5. Hayes R. A. One click, many meanings: interpreting paralinguistic digital affordances in social media. *Journal of Broadcasting & Electronic Media*. 2016;(60):171–187.
6. Urnov M. Yu. Russia: virtual and real political perspectives. *Social sciences and modernity = Obshchestvennye nauki i sovremennost'*. 2014;(5):52–62. (In Russ.).
7. Litvinov D. A. Assessment of Russia's cybersecurity policy and possible options for its improvement. *Bulletin of science and education = Vestnik nauki i obrazovaniya*. 2019;19–2(73):76–82. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Галина Юрьевна Никипорец-Такигава — доктор политических наук, кандидат филологических наук, декан гуманитарного факультета, Российский государственный социальный университет, Москва, Россия
nikiporetsgiu@rgsu.net
Евгений Владимирович Бучнев — аспирант, ассистент гуманитарного факультета, Российский государственный социальный университет, Москва, Россия
buchnevev@rgsu.net

ABOUT THE AUTHORS

Galina Yu. Nikiporets-Takigawa — Dr. Sci. (Political Sciences), Cand. Sci. (Philological Sciences), Dean of the Faculty of Humanities, RSSU, Moscow, Russia
nikiporetsgiu@rgsu.net
Evgeny V. Buchnev — Assistant and Postgraduate student at the Faculty of Humanities RSSU, Moscow, Russia
buchnevev@rgsu.net

Статья поступила 10.12.2021; принята к публикации 20.12.2021.
Авторы прочитали и одобрили окончательный вариант рукописи.
The article was received on 10.12.2021; accepted for publication on 20.12.2021.
The authors read and approved the final version of the manuscript.