DOI 10.20310/2587-9340-2021-5-17-161-170
УДК 34.09
Шифр научной специальности 12.00.01

НЕКОТОРЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОЙ СФЕРЕ

А.В. Парамонов, В.В. Харин
ФГБОУ ВО «Тамбовский государственный университет им. Г.Р. Державина»
392000, Российская Федерация, г. Тамбов, ул. Интернациональная, 33
ORCID: https://orcid.org/0000-0002-3288-3341, e-mail: paramonowtmb@mail.ru
ORCID: https://orcid.org/0000-0002-2841-709X, e-mail: vadimka.va@mail.ru

Аннотация. Информационная среда в настоящее время выступает обязательной составной частью жизнедеятельности общества и государства. Виртуальное пространство и новые технологии не только облегчают и улучшают жизнь современного человека, но и содержат реальные и серьезные угрозы национальной безопасности. Виртуальная (несуществующая) среда оказывает большое воздействие на реальную (практическую) жизнь личности, общества и государства. Опасность заключается в том, что государство в лице своих органов и должностных лиц не успевает вовремя создавать и корректировать законодательную базу противодействия. Было выявлено, что единые меры, а также единство политики в сфере обеспечения информационной безопасности в мире на уровне Деклараций и Конвенций ООН так и не были приняты, в связи с чем противодействие виртуальным угрозам, а также обеспечение безопасности информационной среды возлагается на региональные и государственные системы обеспечения национальной безопасности. При анализе основополагающих документов обеспечения национальной безопасности РФ в виртуальной сфере было выявлено, что законодатель основной акцент делает на угрозы информационного воздействия со стороны иностранных государств, не охватывая и не раскрывая весь объем и современное состояние возможных негативных явлений и угроз в данной сфере.

Ключевые слова: цифровая среда; информационная безопасность; национальная безопасность; противодействие новым угрозам

Современное общество невозможно представить без информационной среды. Цифровая реальность настолько интегрировалась в общественные отношения, что в настоящее время можно наблюдать постепенное вытеснение «классических» взаимоотношений и обществен-

ных процессов в виртуальное пространство. С одной стороны, данные веянья соответствуют «духу времени»: жизнь и взаимоотношения усложняются, важной характеристикой человека становится его мобильность и возможность «быть на связи». Новые технологии и изобретения направлены на облегчение жизнедеятельности человека: помощь с целью сокращения каждодневных хлопот, разнообразие развлекательных продуктов для отдыха, новые возможности для профессиональной деятельности и т. д.

С другой стороны, такое бурное развитие информационной среды и внедрение новых технологий несет в себе существенную опасность как для общества, так и для государства. Высокий уровень интегрированности и зависимости современного человека позволяет манипулировать им, а современные технологии (которые направлены на замену человека во многих сферах) также несут определенную угрозу для повседневной жизнедеятельности общества [1, с. 17]. В связи с этим бурное развитие новых технологий следует рассматривать как актуальную угрозу национальной безопасности государства.

Стоит отметить быстрое развитие информационных технологий и, как следствие, бурное развитие новых угроз. Это выступает одной из первых характеристики новых технологий как угрозы национальной безопасности. Опасность заключается в том, что государство в лице своих органов и должностных лиц не успевает вовремя создавать и корректировать законодательную базу противодействия, что представляет опасность для всей системы национальной безопасности в целом [2, с. 165]. В начале 2000-х гг. информационные технологии только начинали входить в обиход общества и серьезных проблем и угроз не представляли (несли скорее положительные эмоции и полезный функционал). В то время вопросы безопасности в цифровой сфере не были столь актуальны и представляли интерес исключительно для узкоспециализированных специалистов. За 20 лет цифровая среда очень сильно эволюционировала, став важной составной частью общества и государства, а проблемы виртуальной среды приобрели характер глобальных, в связи с чем большое количество как научных деятелей, так и практикующих специалистов в IT-сфере стремятся решить насущные проблемы в области обеспечения безопасности информационных систем [3, с. 113].

В современных условиях информация (данные), а также среда, в которой она реализуются, представляет особый интерес для человечества. В связи с этим вопросы обеспечения безопасности как техниче-

ского, так и гуманитарного характера приобретают статус актуальных: не только государства, но и широкие массы (аудитории) рядовых граждан заинтересованы в обеспечении безопасности [4, с. 70].

Согласно данным, которые были оглашены в рамках Всемирного экономического форума, в настоящее время человечество переживает четвертую (информационную) революцию: информация становится главным ресурсом, а информационные технологи и новшества коренным образом изменяют модели экономической деятельности, социальные взаимодействия субъектов, вносят изменения в политическую сферу[1]. Согласно данным «TheBostonConsultingGroup», в современном мире компьютерная сеть Интернет выступает одной из наиболее перспективных и эффективных площадок для коммуникации, деятельности, взаимодействий и т. д., вытесняя при этом эффективность и нужду в реальных связях[2].

В связи с вышеуказанным стоит отметить, что, казалось бы, виртуальная (несуществующая) среда оказывает большое воздействие на реальную (практическую) жизнь личности, общества и государства. В связи с этим можно сделать вывод о том, что проблематика и угрозы виртуального пространства несут весомую угрозу для практической (реальной) жизнедеятельности и функционирования общества и государства.

Важность и роль цифровой среды в современном обществе осознают многие субъекты международной арены. Осознание всего потенциала управления, владения и возможностей внесения изменений в виртуальные процессы выступает современным и весьма интересным геополитическим инструментом, завладеть и реализовать который стремятся многие государства. Можно сказать, что между современными державами идет ожесточенная борьба за роль в новой информационной революции, ведь в современных условиях обывательское выражение «кто владеет информацией, тот владеет миром» приобретает характер целей и задач для современных государств. Практические реализации данных противостояний стали приобретать все более острый характер: наличие «информационных войн», создание ведущими государствами киберподразделений в составе вооруженных сил и т. д. [5, с. 92].

[1] The World Economic Forum. URL: https://www.weforum.org/ (дата обращения: 17.01.2021).

[2] Россия онлайн? Догнать нельзя отстать: доклад / The Boston Consulting Group (BCG). 2017. 25 марта. С. 18.

Новой и серьезной угрозой информационной среды выступают кибератаки. Опасность заключается в том, что реализуются данные атаки небольшим количеством людей – специалистов IT-сферы, однако негативные последствии успешно реализованных кибератак приводят к серьезным финансовым потерям, нарушениям функционирования инфраструктур, реальным жертвам и т. д. Ярким примером выступает распространение в 2017 г. компьютерных вирусов “WannaCry” и “Petya”, которые пронизывали работу огромного количества коммерческих и государственных организаций в более чем 150 странах, что принесло серьезный ущерб экономической сфере. Также стоит отметить целенаправленные возможности использования кибератак государствами для достижения своих геополитических целей в цифровой среде [6, с. 98].

Проблема противодействия информационным угрозам и поддержания безопасности в информационной сфере в международных масштабах обсуждается на международной арене с начала XX века. Здесь можно отметить и отдельные двусторонние соглашения, и многосторонние инициативы. Так, в рамках инициативы Российской Федерации в 2003 г. была создана «Группа правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности» (ГПЭ). Также стандарты и нормы регламентации безопасности информационной среды острого реализуются в рамках Шанхайской организации сотрудничества (ШОС) и Организации договора о коллективной безопасности (ОДКБ) [7, с. 84].

Однако стоит отметить, что единые меры, а также единство политики в сфере обеспечения информационной безопасности в мире на уровне Деклараций и Конвенций ООН так и не были приняты. Основной причиной данного серьезного пробела международного права выступает противоречие в видении системы обеспечении безопасности информационной сферы ряда государств: европейские державы во главе с США, с одной стороны, Россия, Китай и их партнеры в сфере обеспечения информационной безопасности – с другой. В данном случае можно проследить и геополитические причины, так как каждая сторона пытается реализовать системы безопасности во главе со своим государством с целью воздействия на международное информационное пространство и контроля за его деятельностью [8].

В связи с данным положением стоит отметить, что противодействие виртуальным угрозам, а также обеспечение безопасности информационной среды возлагается на региональные и государственные сис-

темы обеспечения национальной безопасности, где государства самостоятельно выстраивают свою политику и системы обеспечения, в том числе и на законодательном уровне [9, с. 191].

В России законодатель осознает значение и угрозу манипулирования информационной сферы в рамках обеспечения национальной безопасности. При анализе Стратегии национальной безопасности РФ, в разделе II «Россия в современном мире» можно встретить упоминания о нарастающих угрозах в виртуальном пространстве: «все большее влияние на характер международной обстановки оказывает усиливающееся противоборство в глобальном информационном пространстве, обусловленное стремлением некоторых стран использовать информационные и коммуникационные технологии для достижения своих геополитических целей, в том числе путем манипулирования общественным сознанием и фальсификации истории» (21); «появляются новые формы противоправной деятельности, в частности с использованием информационных, коммуникационных и высоких технологий. Обостряются угрозы, связанные с неконтролируемой и незаконной миграцией, торговлей людьми, наркоторговлей и другими проявлениями транснациональной организованной преступности» (22)[3]. Однако говорить о полноценном осознании роли и важности цифровой среды в жизнедеятельности современного обществ со стороны законодателя не приходится, так как в ключевых позициях – «национальные интересы и стратегические национальные приоритеты» – такая категория как защита и обеспечение безопасности функционирования информационной среды отсутствует.

Более детально основные угрозы и основы обеспечения безопасности в информационном пространстве представлены в Доктрине информационной безопасности РФ, которая по своему функционально-практическому характеру является логическим продолжением Стратегии национальной безопасности, но со смещением в информационную сферу. Данный документ содержит национальные интересы в информационной сфере, стратегические цели и основные направления обеспечения информационной безопасности, организационные основы обеспечения безопасности в данной сфере[4]. Однако при детальном анализе, на наш взгляд, положения Доктрины информационной безо-

[3] О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 31.12.2015 № 683 // СЗ РФ. 2016. № 1. Ст. 212.

[4] Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 5.12.2016 № 646 // СЗ РФ. 2016. № 50. Ст. 7074.

пасности РФ основной акцент делают на угрозы информационного воздействия со стороны иностранных государств, не охватывая и раскрывая весь объем и современное состояние возможных негативных явлений и угроз в данной сфере [10, с. 162].

При пересмотре и переоценивании дестабилизирующих факторов, которые могут оказать разрушительное воздействие на российское общество и государство, а значит имеют статус угрозы национальной безопасности РФ, следует отметить то обстоятельство, что современные конфликты, а также вмешательства в суверенные дела государств сопровождаются именно в виртуальном пространстве.

Данная тенденция была задана еще в начале XX века: стоит возомнить ожесточенное противостояние США и Ирана в рамках ядерной политики (которое, между прочим, продолжается и сейчас), в рамках которого военные специалисты IT-сферы в начале 2010 г. пытались реализовать вредоносные программы для воздействия на ядерную инфраструктуру Ирана [8].

Начальные этапы и координирование действий оппозиционных движений в рамках «цветных революций» с целью свержения легитимных властей также зарождается и развивается в виртуальном пространстве: основным инструментом выступают в основном социальные сети и другие виртуальные платформы социальных коммуникаций. Так осуществляется пропаганда «нестабильности» и «очернения» легитимных властей, вследствие чего нарастает реальное неудовлетворение и склонность к революционным действиям. Данные возможности информационной сферы были апробированы и показали свою эффективность в рамках «цветных революций» в Африканских государствах, а также наблюдались в ходе государственных переворотов и попыток таких переворотов в странах Европы и СНГ.

Более того, некоторые специалисты говорят о наличии и активной деятельности международных субъектов, целью которых является «расшатывание» внутригосударственных обстановок, развитие конфликта между обществом и государством, поддержка оппозиционных движений посредством виртуальной среды. В связи с этим можно говорить о появлении и развитии цифровых революционных транснациональных корпораций, которые представляют собой угрозу не только для отдельных государств, но и для всей системы международной (коллективной) безопасности в целом[5].

[5] Цифровая контрреволюция как угроза национальной безопасности России. URL: https://russtrat.ru/analytics/18-yanvarya-2021-0010-2709 (дата обращения: 20.01.2021).

Также специалисты говорят о наличии и возможности применения «кибероружия», которым, по разным данным, могут обладать более 30 государств. В связи с возрастающей ролью информационной среды в жизни современного общества и государства данное оружие постепенно вливается в триаду оружий массового поражения: атомное, химическое и биологическое. В данный момент возможности применения и реализации «кибероружия» рассматриваются относительно несерьезно, но с все большей интеграцией общества и государства в виртуальную сферу (а такие процессы сейчас активно происходят) угрозы и деструктивное воздействие применения такого оружия будут только возрастать [8].

В связи с вышеперечисленным следует проанализировать угрозы виртуального пространства более подробно. Соответствующие угрозы целесообразно выделять в качестве отдельного дестабилизирующего фактора. При этом каждый из других перечисленных факторов в настоящий период усугубляется использованием информационной среды и информационных технологий в деструктивных целях, милитаризацией мирных информационных технологий, а также легкостью, внезапностью и быстродействием как информационно-технологического, так и информационно-психологического оружия.

Список литературы

1. *Шабаева О.А.* Право в условиях цифровой реальности: постановка проблемы // Сибирский юридический вестник. 2019. № 1. С. 16-20.
2. *Самородов В.Ю.* Цифровизация в современной культуре правотворчества: тренд на обновление и позитивная тенденция правовой жизни // Актуальные проблемы государства и права. 2020. № 14. С. 165-179. DOI 10.20310/2587-9340-2020-4-14-165-179.
3. *Матевосова Е.К.* Тенденции и приоритеты развития российского законодательства в эпоху глобализации // Вестник Университета имени О.Е. Кутафина. 2018. № 4. С. 111-117.
4. *Есаулов В.Т.* Противодействие информационным угрозам как важное направление политики национальной безопасности Российской Федерации // Власть. 2009. С. 69-72.
5. *Полякова Т.А., Савенкова Д.Д.* Актуальные проблемы юридической ответственности в сфере обеспечения информационной безопасности (понятие, основания возникновения, виды) // Вестник Южно-Уральского государственного университета. Серия: Право. 2018. № 3. С. 88-94.
6. *Плотникова Т.В., Харин В.В.* Киберпреступность как угроза международной безопасности // Актуальные проблемы государства и права. 2018. № 8. С. 96-107. DOI 10.20310/2587-9340-2018-2-8-96-107.
7. *Сивоволов Д.Л.* Новые угрозы национальному суверенитету России в сфере информационной безопасности // Социум и власть. 2015. № 6. С. 82-88.

8. *Павлова Н.Н.* Угрозы в информационных технологиях. URL: https://sciencefo-rum.ru/2018/article/2018005038 (дата обращения: 09.01.2021).
9. *Карпов Р.А.* Национальная безопасность РФ в условиях информационной войны // Власть. 2017. № 7. С. 191-192.
10. *Молчанов Н.А., Матевосова Е.К.* Доктрина информационной безопасности Российской Федерации (новелла законодательства) // Актуальные проблемы российского права. 2017. № 2. С. 159-165.

Поступила в редакцию 31.01.2021 г.
Поступила после рецензирования 27.02.2021 г.
Принята к публикации 30.03.2021 г.

Информация об авторах
Парамонов Андрей Валерьевич – кандидат педагогических наук, зав. кафедрой специальной подготовки и обеспечения национальной безопасности. Тамбовский государственный университет им. Г.Р. Державина, г. Тамбов, Российская Федерация. E-mail: paramonowtmb@mail.ru
Харин Вадим Витальевич – контролер Управления безопасности. Тамбовский государственный университет им. Г.Р. Державина, г. Тамбов, Российская Федерация.
ORCID: https://orcid.org/0000-0002-2841-709X, e-mail: vadimka.va@mail.ru

Для цитирования
Парамонов А.В., Харин В.В. Некоторые аспекты обеспечения национальной безопасности в информационной сфере // Актуальные проблемы государства и права. 2021. Т. 5. № 17. С. 161-170. DOI 10.20310/2587-9340-2021-5-17-161-170

DOI 10.20310/2587-9340-2021-5-17-161-170

SOME ASPECTS OF ENSURING NATIONAL SECURITY IN THE INFORMATION SPHERE

Andrey V. Paramonov, Vadim V. Kharin
Derzhavin Tambov State University
33 Internatsionalnaya St., Tambov 392000, Russian Federation
ORCID: https://orcid.org/0000-0002-3288-3341, e-mail: paramonowtmb@mail.ru
ORCID: https://orcid.org/0000-0002-2841-709X, e-mail: vadimka.va@mail.ru

Abstract. The information environment is currently an indispensable part of life of society and state. Virtual space and new technologies not only make life easier and better for modern people, but also pose real and serious threats to national security. The virtual (non-existent) environment has a great impact on the real (practical) life of the individual, society and state. The danger lies in the fact that the state, represented by its bodies and officials, does not have time to create and correct the legislative framework for counteraction in

time. We reveal that unified measures, as well as the unity of the policy in the field of information security in the world at the level of the UN Declarations and Conventions, have not been adopted, therefore, countering virtual threats, as well as ensuring the security of the information environment, is imposed on regional and state systems ensuring national security. When analyze the fundamental documents for ensuring the national security of the Russian Federation in the virtual sphere, it is revealed that the legislator places the main emphasis on threats of informational influence from foreign states, without covering and not disclosing the entire volume and current state of possible negative phenomena and threats in this area.

Keywords: digital environment; information security; national security; countering new threats

References

1. Shabayeva O.A. Pravo v usloviyakh tsifrovoy real'nosti: postanovka problemy [Law in the context of digital reality: problem statement]. *Sibirskiy yuridicheskiy vestnik – Siberian Law Herald*, 2019, no. 1, pp. 16-20. (In Russian).
2. Samorodov V.Y. Tsifrovizatsiya v sovremennoy kul'ture pravotvorchestva: trend na obnovleniye i pozitivnaya tendentsiya pravovoy zhizni [Digitalization in the modern culture of law-making: a trend for renewal and a positive trend in legal life]. *Aktual'nye problemy gosudarstva i prava – Current Issues of the State and Law*, 2020, vol. 4, no. 14, pp. 165-179. DOI 10.20310/2587-9340-2020-4-14-165-179 (In Russian).
3. Matevosova E.K. Tendentsii i prioritety razvitiya rossiyskogo zakonodatel'stva v epokhu globalizatsii [Trends and priorities of development of the Russian legislation in the era of globalization]. *Vestnik Universiteta imeni O.E. Kutafina – Courier of the Kutafin Moscow State Law University*, 2018, no. 4, pp. 111-117. (In Russian).
4. Esaulov V.T. Protivodeystviye informatsionnym ugrozam kak vazhnoye napravleniye politiki natsional'noy bezopasnosti Rossiyskoy Federatsii [Countering information threats as an important direction of the national security policy of the Russian Federation]. *Vlast'* [Authority], 2009, pp. 69-72. (In Russian).
5. Polyakova T.A., Savenkova D.D. Aktual'nyye problemy yuridicheskoy otvetstvennosti v sfere obespecheniya informatsionnoy bezopasnosti (ponyatiye, osnovaniya vozniknoveniya, vidy) [Topical problems of legal responsibility in the sphere of providing information security (concept, basis of emergence, types)]. *Vestnik Yuzhno-Ural'skogo gosudarstvennogo universiteta. Seriya: Pravo – Bulletin of the South Ural State University Series "Law"*, 2018, no. 3, pp. 88-94. (In Russian).
6. Plotnikova T.V., Kharin V.V. Kiberprestupnost' kak ugroza mezhdunarodnoy bezopasnosti [Cybercrime as a threat to international security]. *Aktual'nye problemy gosudarstva i prava – Current Issues of the State and Law*, 2018, vol. 2, no. 8, pp. 96-107. DOI 10.20310/2587-9340-2018-2-8-96-107. (In Russian).
7. Sivovolov D.L. Novyye ugrozy natsional'nomu suverenitetu Rossii v sfere informatsionnoy bezopasnosti [New threats to the national sovereignty of Russia in the sphere of information security]. *Sotsium i vlast' – Society and Power*, 2015, no. 6, pp. 82-88. (In Russian).
8. Pavlova N.N. *Ugrozy v informatsionnykh tekhnologiyakh* [Threats in Information Technology]. (In Russian). Available at: https://scienceforum.ru/2018/article/2018005038 (accessed 09.01.2021).

9. Karpov R.A. Natsional'naya bezopasnost' RF v usloviyakh informatsionnoy voyny [The national security of the Russian Federation in terms of the information war]. *Vlast'* [Authority], 2017, no. 7, pp. 191-192. (In Russian).
10. Molchanov N.A., Matevosova E.K. Doktrina informatsionnoy bezopasnosti Rossiyskoy Federatsii (novella zakonodatel'stva) [The doctrine of information security of the Russian federation (new law)]. *Aktual'nyye problemy rossiyskogo prava – Actual Problems of Russian Law*, 2017, no. 2, pp. 159-165. (In Russian).

Received 31 January 2021
Reviewed 27 February 2021
Accepted for press 30 March 2021

Information about the authors

Andrey V. Paramonov – Candidate of Pedagogical Sciences, Head of Special Training and National Security Department. Derzhavin Tambov State University, Tambov, Russian Federation.
ORCID: https://orcid.org/0000-0002-3288-3341, e-mail: paramonowtmb@mail.ru
Vadim V. Kharin – Security Management Controller. Derzhavin Tambov State University, Tambov, Russian Federation.
ORCID: https://orcid.org/0000-0002-2841-709X, e-mail: vadimka.va@mail.ru

For citation

Paramonov A.V., Kharin V.V. Nekotoryye aspekty obespecheniya natsional'noy bezopasnosti v informatsionnoy sfere [Some aspects of ensuring national security in the information sphere]. *Aktual'nye problemy gosudarstva i prava – Current Issues of the State and Law*, 2021, vol. 5, no. 17, pp. 161-170. DOI 10.20310/2587-9340-2021-5-17-161-170 (In Russian, Abstr. in Engl.)