ФИЛОСОФИЯ НАУКИ И ТЕХНИКИ

УДК 343.1
DOI: 10.18384/2310-7227-2021-4-125-133

СОЦИАЛЬНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНТЕРНЕТ-СРЕДЫ: ПРОБЛЕМЫ, РЕАЛИИ, ПЕРСПЕКТИВЫ

Гурьянова А. В.[1], Тимофеев А. В.[2]
[1]Самарский государственный экономический университет
443090, г. Самара, ул. Советской Армии, д. 141, Российская Федерация
[2]Самарский государственный технический университет
443100, г. Самара, ул. Молодогвардейская, д. 244, Российская Федерация

Аннотация
Цель. Проанализировать механизм социально-правового регулирования интернет-среды с учётом детерминирующих его информационных и технологических инноваций, психологических аспектов воздействия на пользователей, экономических и правовых факторов, включая предпринимаемые в этом отношении новейшие законодательные инициативы.
Процедура и методы исследования. В исследовании рассматривается киберпреступность как феномен социально-правового порядка, демонстрирующий прогрессирующую динамику распространения по всему современному миру. В исследовании используются диалектический, сравнительный и прогностический методы, а также методы типологии, анализа и синтеза. В исследовании приводятся актуальные статистические данные в затрагиваемой проблемной области. Особое внимание уделяется специфике правового регулирования киберпреступности в зарубежных странах, а также опыту противодействия киберпреступлениям в современной России.
Результаты. В исследовании показано, что в современных условиях актуальная правовая база и применяемая в её рамках практика регулирования интернет-среды пока остаются слаборазвитыми. Эволюция компьютерных технологий значительно опережает сформированную в этой области систему правоотношений. Это затрудняет оперативную разработку законов, регулирующих отношения и деятельность в киберпространстве, увеличивает шансы киберпреступников на безнаказанность. Именно поэтому киберпреступность считается сегодня одной из наиболее существенных угроз для государственных систем национальной безопасности и глобальной модели устойчивого развития. В исследовании показано, что современные меры противодействия киберпреступности основаны по большей части на правовом опыте западных стран, и этого явно недостаточно для эффективного противостояния данной угрозе.
Теоретическая и/или практическая значимость. С помощью результатов сравнения различных нормативных документов, приведённых в работе, можно установить, какие дополнительные инструменты правового регулирования требуется ввести в законодательную сферу, затрагивающую систему взаимоотношений в интернет-среде.

Ключевые слова: интернет-среда, киберпреступность, кибербезопасность, право, правовое регулирование

SOCIO-LEGAL REGULATION OF THE INTERNET ENVIRONMENT: PROBLEMS, REALITIES, PROSPECTS

***A. Guryanova*[1], *A. Timofeev*[2]**
[1]*Samara State University of Economics*
ul. Sovetskoy Armii 141, Samara 443090, Russian Federation
[2]*Samara State Technical University*
ul. Mologvardeyskaya 244, Samara 443100, Russian Federation

Abstract.
Aim. To analyze the mechanism of the socio-legal regulation of the Internet environment, taking into account the information and technological innovations determining it, the psychological aspects of the impact on the users, the economic and legal factors, including the latest legislative initiatives taken in this field.
Methodology. The study examines cybercrime as a phenomenon of the social and legal character, demonstrating the progressive dynamics of its spread all over the modern world. Dialectical, comparative, and predictive methods, as well as methods of typology, analysis, and synthesis are used in the study. The study provides actual statistical data in the affected problem area. Special attention is paid to the specifics of the legal regulation of cybercrime in foreign countries and to the experience of countering cybercrime in modern Russia.
Results. The study shows that in modern conditions, the current legal base and the practice of regulating the Internet environment still remain underdeveloped. The evolution of computer technologies is significantly ahead of the system of legal relations formed in this area. This makes difficult to develop operatively the laws regulating relations and activities in cyberspace, and increases the chances for cybercriminals to avoid punishment. That's why cybercrime today is considered as one of the main threats to the state system of national security and the global model of sustainable development.
Research implications. Using the results of a comparison of various regulatory documents given in the work, it is possible to establish which additional instruments of legal regulation are required to be introduced into the legislative sphere affecting the system of relationships in the Internet environment.

Keywords: the Internet environment, cybercrime, cyber security, law, legal regulation

Введение

В современных условиях совершенно очевидно, что основополагающим фактором, влияющим на жизнь социума в XXI в., является динамичное внедрение и развитие информационных, телекоммуникационных и цифровых технологий. Новый цифровой период в истории человечества уже вошёл в активную стадию своего развития и приобрёл поистине глобальный характер [1, с. 63]. Система социальных взаимодействий в цифровую эпоху выстраивается на основе активного использования интернет-технологий, что делает разнообразные виды современных коммуникаций всё более доступными, стимулирует развитие инновационных сфер человеческой деятельности и поведения. По данным Глобального цифрового обзора "Digital 2020", в начале 2020 г. ресурсами сети воспользовались 4,5 млрд человек, что приблизительно составляет около 60% современного человечества[1].

Но широкое распространение сетевых технологий привело не только к прогрессивному развитию общества, но и к распространению абсолютно новых видов социальных угроз, в том числе в сфере преступной деятельности. Это, например, киберпреступность, которая стремительно развивалась в течение первых двух десятилетий XXI в. Сегодня она считается одной из наиболее существенных проблем

[1] Kemp S. Digital 2020: Global Digital Overview [Электронный ресурс]. URL: https://datareportal.com/reports/digital-2020-global-digital-overview (дата обращения: 31.10.2021).

многих современных государств, препятствующей эффективному функционированию входящих в их состав социальных институтов, эффективному осуществлению ими внутренней и внешней политики. Очевидно, что киберпреступные действия представляют серьёзную угрозу самой парадигме информационной безопасности.

Сегодня киберпреступность является проблемой не только частных пользователей интернета: она уже приобрела широкий социальный и международный резонанс. Специалисты Сбербанка подсчитали, что в 2020 г. потери российской экономики от киберпреступлений составили более 3,5 трлн рублей. А к концу 2021 г. эта цифра может увеличиться вдвое, что составит в общей сложности 7 трлн рублей. По данным Сбербанка, в настоящее время число мировых киберпреступников составляет около 1,5 млн человек, а к концу 2021 г. это число может увеличиться ещё на 30%[1]. Только в России за последние 7 лет количество киберпреступлений увеличилось в 20 раз, а за последние 5 лет – в 25 раз[2].

Такая тенденция ярко выраженной негативной направленности существенно усилилась с начала 2020 г. в связи с пандемией коронавируса, когда был осуществлён вынужденный перевод большей части процессов и операций в онлайн-формат [5, p. 567]. В период пандемии количество киберпреступлений увеличилось на 92% по сравнению с аналогичным периодом предыдущего года. В 2020 г. эксперты зафиксировали рост киберпреступности на 85%[3], причём только 25% киберпреступлений из общего числа были успешно раскрыты[4].

Опыт правового регулирования интернет-среды в зарубежных странах

Уже два десятилетия назад (23 ноября 2001 г.) членами Совета Европы была принята «Конвенция о киберпреступности»[5]. Этот знаменитый правовой документ стал одним из первых серьёзных шагов мирового сообщества, предпринятых в направлении правового урегулирования интернет-среды. Она также представляла собой первый официальный документ, регламентирующий необходимость юридического преследования киберпреступников. В Конвенции были упомянуты пять основных видов «преступлений против конфиденциальности, целостности и доступности компьютерных данных и систем»[6]. В их числе указывались: «незаконный доступ; незаконный перехват; вмешательство в данные; вмешательство в систему; неправильное использование устройств»[7].

По прошествии двух десятилетий безусловным лидером в сфере правового регулирования интернет-среды может считаться современная Германия. 1 января 2018 г. здесь были приняты изменения в исходный «Закон о совершенствовании правоприменения в социальных сетях (Закон о сетевом правоприменении)» 2017 г.[8] В соответствии с данными изменениями все ведущие сетевые платформы, такие как “Twitter” и “Facebook”, должны быстро удалять из своей области любой незаконный контент. Причём уровень такой «незаконности» устанавливается в чётком соответствии с 22 главами Уголовного кодекса Германии[9]. В случае, если данное тре-

1 Сбербанк подсчитал потери российской экономики в 2021 году от киберпреступности // ТАСС : [сайт]. https://tass.ru/ekonomika/8761953 (дата обращения: 31.10.2021).

2 Путин словами «Мы не успеваем» объяснил рост числа преступлений в ИТ // РБК : [сайт]. URL: https://www.rbc.ru/politics/03/03/2021/603f6ae59a7947b29b0e9b18 (дата обращения: 31.10.2021).

3 Путин: Ущерб от киберпреступности в 2021 году может достичь $ 6 трлн // Комсомольская правда : [сайт]. URL: https://www.kp.ru/online/news/4089829 (дата обращения: 31.10.2021).

4 Путин словами «Мы не успеваем» объяснил рост числа преступлений в ИТ // РБК : [сайт]. URL: https://www.rbc.ru/politics/03/03/2021/603f6ae59a7947b29b0e9b18 (дата обращения: 31.10.2021).

5 Convention on Cybercrime [Электронный ресурс]. URL: https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (дата обращения: 31.10.2021).

6 Там же.

7 Там же.

8 Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act) [Электронный ресурс]. URL: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2 (дата обращения: 31.10.2021).

9 German Criminal Code // CNBC : [сайт]. URL: https://www.cnbc.com/2018/03/08/germany-looks-to-revise-

бование будет нарушено или не выполнено оперативно, штраф за нарушение может составить колоссальную сумму, доходящую до 50 млн евро[1].

В современной Великобритании действует несколько законов, ограничивающих права частных пользователей интернета в интересах государства в целом. Одним из них является «Закон о защите данных» от 2018 г.[2] Этот Закон регулирует обработку персональных данных, касающихся физических лиц, парламента и Короны. В нём также содержится положение о соблюдении законодательства по защите данных. В целом, в Великобритании действует не менее шести законов (один из них – совместный с Францией) по регулированию деятельности в интернете.

В 2016 г. члены Европейского Союза совместными усилиями создали «Кодекс поведения по противодействию незаконным высказываниям ненависти в интернете»[3]. Данный Кодекс был согласован с четырьмя ключевыми платформами-участницами, в число которых входили “Facebook”, “Microsoft”, “Twitter” и “YouTube”. В дополнение к Кодексу в 2019 г. была принята «Директива об авторском праве на едином цифровом рынке»[4]. Цель директивы – заставить “Google”, “Facebook” и другие платформы выплачивать компенсации издателям и художникам. В Италии существуют аналогичные правовые акты, касающиеся защиты авторских прав и предусматривающие досудебную блокировку подозрительных сайтов.

США также традиционно сильны в области обеспечения собственной кибербезопасности. Интернет здесь регулируется как минимум восемью профильными законами. Уже в июле 2007 г. президент Дж. У. Буш принял «Закон о защите Америки»[5], позволивший спецслужбам прослушивать любые иностранные телефонные звонки и разговоры. Данный Закон действовал в течение 180 дней, а затем Конгресс отказался его продлевать. Но его основные положения были включены в последующий «Закон о поправках к FISA»[6] 2008 г. Данный закон используется в качестве правовой основы для программ массового слежения, широко практикуемых современной Америкой.

Один из самых известных современных законов в сфере правового урегулирования интернет-среды был принят в Китае в 2017 г. Это «Закон о кибербезопасности»[7]. Его целью являются защита национального «суверенитета в киберпространстве», а также регулирование деятельности сетевых провайдеров, производимых ими продуктов и услуг, помогающих собирать, хранить и обрабатывать данные пользователей. Этот закон выступает гарантом информационной безопасности в стратегически важных отраслях экономики страны. Штраф для нарушителей может составить до 1 млн юаней в зависимости от степени тяжести совершенного киберпреступления.

В современной Индии также существует ряд законов, регламентирующих сферу интернет-активности. Один из них носит название «Закон об информацион-

social-media-law-as-europe-watches.html (дата обращения: 31.10.2021).

1 Ellyatt H. Germany Looks to Revise Social Media Law as Europe Watches // CNBC : [сайт]. URL: https://www.cnbc.com/2018/03/08/germany-looks-to-revise-social-media-law-as-europe-watches.html (дата обращения: 31.10.2021).

2 Data Protection Act 2018 // Legislation.gov.uk. URL: https://www.legislation.gov.uk/ukpga/2018/12/section/1/enacted (дата обращения: 31.10.2021).

3 Code of Conduct on Countering Illegal Hate Speech Online: First Results on Implementation // European Commission : [сайт]. URL: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=29738&no=1 (дата обращения: 31.10.2021).

4 The Directive on Copyright in the Digital Single Market [Электронный ресурс]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0790&from=EN (дата обращения: 31.10.2021).

5 Protect America Act of 2007 (PAA) [Электронный ресурс]. URL: https://www.justice.gov/archive/ll/docs/text-of-paa.pdf (дата обращения: 31.10.2021).

6 FISA Amendments Act // Congress.gov. URL: https://www.congress.gov/bill/110th-congress/house-bill/6304 (дата обращения: 31.10.2021).

7 Segal A. China’s New Cybersecurity Law // Council on Foreign Relations : [сайт]. URL: https://www.cfr.org/blog/chinas-new-cybersecurity-law (дата обращения: 31.10.2021).

ных технологиях»[1]. Данный закон предусматривает уголовную ответственность за отправку сообщений оскорбительного характера. В законе также есть глава, дающая властям страны право перехватывать, отслеживать и расшифровывать информацию с помощью любого компьютерного ресурса.

В современной Турции действует весьма строгий закон «О регулировании публикаций в интернете и борьбе с преступлениями, совершаемыми с помощью таких публикаций» или, как его ещё кратко называют, «Закон об интернете»[2]. Данный закон предоставляет властям страны право на блокировку подозрительных сайтов в досудебном порядке. Под «подозрительными» подразумеваются сайты, содержащие информацию незаконного характера и в особенности оскорбляющие государственные принципы.

Как видим, в большинстве стран современного мира, как западных, так и восточных, приняты и действуют законы, регулирующие деятельность и поведение пользователей в интернет-среде. Данные законы различаются по степени строгости в отношении правонарушителей, но само их количество и значительный разброс представленной территориальной дислокации свидетельствует о настоятельной потребности их внедрения, дальнейшего совершенствования и актуализации.

Меры противодействия киберпреступности в современной России

Весьма показательно, что Уголовный кодекс Российской Федерации до сих пор не содержит такого понятия, как «киберпреступность», а гл. 28 данного кодекса, посвящённая «преступлениям в сфере компьютерной информации», является одной из самых незначительных по объёму в этом важнейшем правовом документе. В гл. 28 содержится всего 4 статьи, предусматривающие наступление ответственности за преступления, совершённые с помощью и посредством инновационных технологий и компьютерной техники.

Так, ст. 272 «Незаконный доступ к компьютерной информации» предусматривает ответственность в случаях уничтожения, блокирования, изменения или копирования компьютерной информации[3]. В ст. 273 – «Создание, использование и распространение вредоносных компьютерных вирусов» – за все вышеперечисленные деяния предусматривается уголовная ответственность[4]. Ст. 274 «Нарушение Правил эксплуатации компьютеров, компьютерных систем или их Сетей» предполагает наличие крупного ущерба (более 1 млн руб.)[5]. Если же ущерб составляет хотя бы на 1 руб. меньше, преступление не квалифицируется в качестве уголовно наказуемого, и вследствие этого уголовная ответственность не наступает.

В 2017 г. в Уголовный кодекс России было внесено ещё одно важное дополнение, нашедшее отражение в ст. 274.1. В данной статье предусматривается ответственность за незаконное воздействие на критически важную информационную инфраструктуру Российской Федерации[6].

Очевидно, что четырёх вышеназванных статей (даже с внесённым в них дополнением) недостаточно для эффективного противодействия киберпреступности, обеспечения информационной безопасности страны и реализации модели её устойчивого развития. Не случайно поэтому Президент России В. В. Путин, выступая 20 ноября 2020 г. на саммите Азиатско-Тихоокеанского экономического со-

[1] Information Technology Act 2000 [Электронный ресурс]. URL: https://www.meity.gov.in/content/information-technology-act-2000-0 (дата обращения: 31.10.2021).

[2] On Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publication ("The Internet Law") [Электронный ресурс]. URL: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)011-e (дата обращения: 31.10.2021).

[3] Уголовный кодекс Российской Федерации // СПС Косультант Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_10699 (дата обращения: 31.10.2021).

[4] Там же.

[5] Там же.

[6] Там же.

трудничества (АТЭС), охарактеризовал ситуацию с ростом киберпреступности следующими словами: «Мы не успеваем»[1].

В своём выступлении президент акцентировал внимание на том, что стремительное развитие технологий закономерно приводит к росту числа киберпреступных операций. Российский лидер также отметил, что за развитием электронной коммерции и предоставлением различных онлайн-услуг стоит «наше будущее». Но в связи с быстрым обновлением и изменением технологий поле для незаконной мошеннической деятельности тоже увеличивается[2]. В такой ситуации крайне важно своевременно информировать граждан о превентивных мерах и способах защиты от киберпреступников. Следует также наладить эффективное взаимодействие правоохранительных органов с интернет-провайдерами, представителями банковского сообщества и операторами мобильной связи. Кроме того, необходимо целенаправленно развивать международное сотрудничество в области защиты персональных данных и противодействия киберпреступности.

Проблемы теории и практики регулирования интернет-среды

Очевидно, что в современных реалиях киберпреступность предстаёт как одна из наиболее существенных угроз государственной безопасности и устойчивому развитию стран мирового сообщества [2, с. 95]. Исследования в этой области «высвечивают» сложнейшую систему криминогенных факторов, которая уже создана и функционирует в глобальной сети. Со временем преступные связи становятся всё более разветвлёнными, охватывают всё большее количество участников – как киберпреступников, так и киберпотерпевших. Именно поэтому следует уделять особое внимание осмыслению влияния технологических достижений на социальные процессы [7], человеческому фактору в сфере киберпреступности [3], проблемам кибербезопасности в контексте защиты частной жизни и свободы человека [4].

Предметом исследовательского интереса выступают также происходящие в сущности современной преступности киберизменения [6] и формат новой законодательной базы, соответствующей этой предметной области. Однако проводимых теоретических изысканий явно недостаточно для разработки нормативной правовой документации, в полной мере соответствующей динамике и уровню развития современной киберпреступности. Актуальная правовая база и применяемая в её рамках практика регулирования интернет-среды остаются пока ещё слаборазвитыми и во многих аспектах непроработанными. Эволюция компьютерных технологий значительно опережает правовую систему, сформированную в данной предметной области. Это, в свою очередь, затрудняет оперативную разработку законов, регулирующих взаимоотношения и деятельность в киберпространстве, увеличивает шансы киберпреступников на безнаказанность и успешность совершаемых ими хакерских атак.

Следует также отметить, что жертвы киберпреступной деятельности часто сами не обращаются в полицию и не сообщают о совершённых в их отношении правонарушениях по причине элементарного неверия в реальный результат данной процедуры. Предпосылкой гражданского бездействия может считаться также недостаточная компьютерная образованность и правовая неосведомлённость многих пользователей, лично претерпевших от разного рода киберпреступных деяний. Если же посмотреть на данную ситуацию с другой стороны, работникам правоохранительных органов чрезвычайно сложно идентифицировать личность кибермошенника, поскольку большинство из них – это высококвалифицированные программисты, которые не оставляют за собой практически никаких «следов».

[1] Путин словами «Мы не успеваем» объяснил рост числа преступлений в ИТ // РБК : [сайт]. URL: https://www.rbc.ru/politics/03/03/2021/603f6ae59a7947b29b0e9b18 (дата обращения: 31.10.2021).

[2] Сбербанк подсчитал потери российской экономики в 2021 году от киберпреступности // ТАСС : [сайт]. https://tass.ru/ekonomika/8761953 (дата обращения: 31.10.2021).

Жертвы киберпреступников зачастую даже не подозревают о совершённом в отношении них преступлении: для того, чтобы этот факт подтвердить, требуется немало усилий и временных затрат. Все возможные «виртуальные следы» к этому времени, как правило, уже исчезают. Сталкиваясь с киберпреступлениями, сотрудники правоохранительных органов вынуждены прибегать к помощи высококвалифицированных специалистов в области программирования, но их число среди полицейских пока ещё недостаточно. Общей судебной и следственной практики по делам данной категории не существует. Отсутствует также объединённая программа предотвращения и решения проблем киберпреступности.

Заключение

В современном мире сфера киберпреступности отличается колоссальной вариативностью и динамикой распространения – количество киберпреступников и киберпреступлений возрастает в геометрической прогрессии. Сама по себе глобальная интернет-среда, естественно, не в состоянии противостоять шквалу разного рода предпринимаемых в её пределах незаконных деяний. Причём последние затрагивают не только частные интересы конкретных пользователей и даже целых государств – они уже приобрели ярко выраженный глобальный характер.

Сегодня в рамках интернет-среды киберпреступниками апробируются всё новые виды совершения преступных деяний. Для каждого из них необходимо найти эффективный метод противодействия, что, как уже отмечалось выше, вызывает немалые трудности. Как следствие, всё большее количество пользователей интернета страдает от хакерских атак и деструктивных действий киберпреступников. Однако общий уровень компьютерной грамотности при этом практически не повышается, особенно среди старшего поколения пользователей.

Процент же онлайн-коммуникаций и активности различных интернет-сообществ, напротив, существенно возрастает. Особенно тревожной тенденцией является то, что в их составе активируется всё большее количество экстремистских и террористических группировок. Их существование во многом обеспечивается анонимностью участия и ростом случаев манипулирования человеческим сознанием и поведением посредством интернет-среды и применяемых в её рамках технологических ресурсов и инструментов.

Как было показано выше, определённые меры по противодействию киберпреступности принимаются во всём цивилизованном мире, особенно в технически развитых странах, вступивших на путь цифровизации. В основном эти меры основаны на юридическом опыте стран Западной Европы. С их помощью постепенно повышается уровень компьютерной грамотности, возрастает осведомлённость пользователей интернет-среды о видах и способах совершения киберпреступлений, внедряются эффективные в этой сфере инструменты правового регулирования. Разумеется, деятельность в данном направлении следует продолжать и активировать. Особое внимание при этом должно уделяться дальнейшему развитию правовых актов о киберпреступлениях. Это необходимое условие эффективного правового регулирования интернет-среды, обеспечения кибербезопасности и выхода на приоритетный путь устойчивого развития в современном глобализированном мире.

Статья поступила в редакцию 01.10.2021.

ЛИТЕРАТУРА

1. Гурьянов Н. Ю., Гурьянова А. В. Цифровая глобализация в контексте развития цифровой экономики и цифровых технологий // Вестник Московского государственного областного университета. Серия: Философские науки. 2020. № 3. С. 63–69.
2. Тимофеев А. В., Комолов А. А. Киберпреступность как социальная угроза и объект правового регулирования // Вестник Московского государственного областного университета. Серия: Философские науки. 2021. № 1. С. 95–101.

3. Cybercrime in Context. The Human Factor in Victimization, Offending, and Policing [Электронный ресурс] / ed. M. W. Kranenbarg, R. Leukfeldt. URL: https://link.springer.com/book/10.1007/978-3-030-60527-8 (дата обращения: 31.10.2021).
4. Cybersecurity, Privacy and Freedom Protection in the Connected World: Proceedings of the 13th International Conference on Global Security, Safety and Sustainability [Электронный ресурс] / ed. H. Jahankhani, A. Jamal, Sh. Lawson. URL: https://link.springer.com/book/10.1007/978-3-030-68534-8 (дата обращения: 31.10.2021).
5. Guryanova A. V., Petinova M. A., Guryanov N. Yu. Socio-economic Problems and Perspectives of Globalization in the Context of Coronavirus Pandemic // Economic Systems in the New Era: Stable Systems in an Unstable World: Proceedings of the Institute of Scientific Communications Conference (ISC) 2020: Lecture Notes in Networks and Systems. Vol. 160 / ed. S. I. Ashmarina, J. Horák, J. Vrbka, P. Šuleř. Springer: Cham, 2021. P. 567–573.
6. Rethinking Cybercrime [Электронный ресурс] / eds. T. Owen, J. Marshall. URL: https://link.springer.com/book/10.1007/978-3-030-55841-3 (дата обращения: 31.10.2021).
7. Technological Prerequisites and Humanitarian Consequences of Ubiquitous Computing and Networking / A. Guryanova, E. Khafiyatullina, M. Petinova, V. Frolov, A. Makhovikov // Digital Economy: Complexity and Variety vs. Rationality: Proceedings of the Institute of Scientific Communications Conference (ISC) 2019: Lecture Notes in Networks and Systems. Vol. 87 / ed. E. Popkova, B. Sergi. Springer: Cham, 2020. P. 1040–1047.

REFERENCES

1. Gur'yanov N. Yu., Gur'yanova A. V. [Digital Globalization in the Context of Digital Economy and Digital Technologies Development]. In: *Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta. Seriya: Filosofskie nauki* [Bulletin of Moscow Region State University. Series: Philosophy], 2020, no. 3, pp. 63–69.
2. Timofeev A. V., Komolov A. A. [Cybercrime as a Social Threat and an Object of Legal Regulation]. In: *Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta. Seriya: Filosofskie nauki* [Bulletin of Moscow Region State University. Series: Philosophy], 2021, no. 1, pp. 95–101.
3. Kranenbarg M. W., Leukfeldt R., eds. Cybercrime in Context. The Human Factor in Victimization, Offending, and Policing. Available at: https://link.springer.com/book/10.1007/978-3-030-60527-8 (accessed: 31.10.2021).
4. Jahankhani H., Jamal A., Lawson Sh., eds. Cybersecurity, Privacy and Freedom Protection in the Connected World: Proceedings of the 13th International Conference on Global Security, Safety and Sustainability. Available at: https://link.springer.com/book/10.1007/978-3-030-68534-8 (accessed: 31.10.2021).
5. Guryanova A. V., Petinova M. A., Guryanov N. Yu. Socio-economic Problems and Perspectives of Globalization in the Context of Coronavirus Pandemic. In: Ashmarina S. I., Horák J., Vrbka J., Šuleř P., eds. *Economic Systems in the New Era: Stable Systems in an Unstable World: Proceedings of the Institute of Scientific Communications Conference (ISC) 2020: Lecture Notes in Networks and Systems. Vol. 160.* Springer, Cham, 2021, pp. 567–573.
6. Owen T., Marshall J. Rethinking Cybercrime. Available at: https://link.springer.com/book/10.1007/978-3-030-55841-3 (accessed: 31.10.2021).
7. Guryanova A., Khafiyatullina E., Petinova M., Frolov V., Makhovikov A. Technological Prerequisites and Humanitarian Consequences of Ubiquitous Computing and Networking. In: Popkova E., Sergi B., eds. *Digital Economy: Complexity and Variety vs. Rationality: Proceedings of the Institute of Scientific Communications Conference (ISC) 2019: Lecture Notes in Networks and Systems. Vol. 87.* Springer, Cham, 2020, pp. 1040–1047.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Гурьянова Анна Викторовна – доктор философских наук, профессор, заведующий кафедрой теории права и философии Самарского государственного экономического университета;
e-mail: annaguryanov@yandex.ru

Тимофеев Александр Вадимович – кандидат педагогических наук, доцент кафедры информационных технологий Самарского государственного технического университета;
e-mail: timofeev_av@list.ru

INFORMATION ABOUT THE AUTHORS

Anna V. Guryanova – Dr. Sci. (Philosophy), Prof., Head of the Department, Department of the Theory of Law and Philosophy, Samara State University of Economics;
e-mail: annaguryanov@yandex.ru

Alexander V. Timofeev – Cand. Sci. (Pedagogy), Assoc. Prof., Department of Information Technologies, Samara State Technical University;
e-mail: timofeev_av@list.ru

ПРАВИЛЬНАЯ ССЫЛКА НА СТАТЬЮ

Гурьянова А. В., Тимофеев А. В. Социально-правовое регулирование интернет-среды: проблемы, реалии, перспективы // Вестник Московского государственного областного университета. Серия: Философские науки. 2021. № 4. С. 125–133.
DOI: 10.18384/2310-7227-2021-4-125-133

FOR CITATION

Guryanova A. V., Timofeev A. V. Socio-Legal Regulation of the Internet Environment: Problems, Realities, Prospects. In: *Bulletin of Moscow Region State University. Series: Philosophy*, 2021, no. 4, pp. 125–133.
DOI: 10.18384/2310-7227-2021-4-125-133