Оригинальная статья / Original article

https://doi.org/10.21869/2223-1552-2021-11-6-243-259

Цифровая сетевая платформа: классификация опасностей социотехнической конвергенции

В. В. Зотов[1] ✉, И. А. Асеева[2], В. Г. Буданов [3]

[1] Московский физико-технический институт (национальный исследовательский университет)
Институтский пер. 9, Московская область, г. Долгопрудный 141701, Российская Федерация

[2] Институт научной информации по общественным наукам РАН
Нахимовский проспект 51/21, г. Москва 117418, Российская Федерация

[3] Институт философии РАН
ул. Гончарная 12, стр.1, г. Москва 109240, Российская Федерация

✉ e-mail: zotov.vv@mipt.ru

Резюме

Актуальность *исследования обусловлена тем, что создание цифровых сетевых платформ сопровождается неоднозначным процессом социотехнической конвергенции, в ходе которого возникают как положительные, так и неблагоприятные последствия, как преднамеренные, так и непреднамеренные.*

Цель *данной статьи – выявить и структурировать наиболее серьёзные неблагоприятные опасности социотехнической конвергенции цифровых сетевых платформ.*

Задачи: *уточнить понятия опасности и рисков социотехнической конвергенции; определить внутренние и внешние предметные сферы их проявления.*

Методология *исследования базируется на концепции платформенных исследований, дополненных авторами идеями социотехнической конвергенции. Для классификации рисков использовался метод таксономии, источником информации для которой стал аналитический обзор академической литературы и публицистики по проблемам цифровизации.*

Результатом *исследования стала классификация опасностей социотехнической конвергенции. В зависимости от положения источника опасности были разделены на внешние и внутренние. Внешние опасности классифицировались в зависимости 1) от положения источника опасностей, 2) от состава цифровой сетевой платформы, которая обладает определённой структурой, и 3) от уровня субъектности опасностей, то есть уровня влияния пользователя на процессы функционирования, возможность контролировать наступления тех или иных результатов. Внешние опасности были также классифицированы по двум основаниям – уровню субъектности и объекту её проявления. Итогом таксономического деления стала классификация по таким предметным областям, как цифровые данные, цифровой надзор, цифровая мораль, цифровая идентификация, цифровая конфиденциальность, цифровая коммуникация, цифровая доступность, цифровая компетентность, цифровые кластеры.*

Вывод. *Авторы приходят к выводу, что таксономия может стать основой для дальнейших исследований по выявлению и управлению побочными эффектами цифровизации.*

Ключевые слова: *цифровые сетевые платформы; цифровые данные; цифровой надзор; цифровая мораль; цифровая идентификация; цифровая конфиденциальность; цифровая коммуникация; цифровая доступность; цифровые кластеры; цифровая компетентность.*

Конфликт интересов: *В представленной публикации отсутствует заимствованный материал без ссылок на автора и (или) источник заимствования, нет результатов научных работ, выполненных авторами публикации лично и (или) в соавторстве, без соответствующих ссылок. Авторы декларируют отсутствие конфликта интересов, связанных с публикацией данной статьи.*

Финансирование: *Исследование выполнено при финансовой поддержке РФФИ и ЭИСИ в рамках научного проекта № 21-011-31719 «Социотехническая конвергенция в условиях цифровизации сетевых пространств».*

Для цитирования*:* Зотов В. В., Асеева И. А., Буданов В. Г. Цифровая сетевая платформа: классификация опасностей социотехнической конвергенции // Известия Юго-Западного государственного университета. Серия: Экономика. Социология. Менеджмент. 2021. Т. 11, № 6. С. 243–259. https://doi.org/10.21869/2223-1552-2021-11-6-243-259.

Поступила в редакцию 18.10.2021 Принята к публикации 16.11.2021 Опубликована 29.12.2021

Digital Network Platform: Classification of Sociotechnical Convergence Hazards

Vitaly V. Zotov[1] ✉, Irina A. Aseeva[2], Vladimir G. Budanov[3]

[1] Moscow Institute of Physics and Technology (National Research University)
9 Institutsky Per., Moscow Region, Dolgoprudny 141701, Russian Federation

[2] Institute of Scientific Information on Social Sciences of the Russian Academy of Sciences
51/21 Nakhimovsky Prospekt, Moscow 117418, Russian Federation

[3] Institute of Philosophy of the Russian Academy of Sciences
12 Goncharnaya str., p. 1, Moscow 109240, Russian Federation

✉ e-mail: zotov.vv@mipt.ru

Abstract

The relevance *of the study is due to the fact that the creation of digital network platforms is accompanied by an ambiguous process of socio-technical convergence, during which both positive and negative consequences arise, both intentional and unintended.*

The purpose *of this publication is to identify and structure the most serious adverse dangers of socio-technical convergence of digital network platforms.*

Objectives: *to give definitions of the concept of danger and risks of socio-technical convergence; determine the internal and external subject areas of their manifestation.*

Metodology. *The research methodology is based on the concept of platform research, supplemented by the authors with the ideas of sociotechnical convergence. To classify risks, the taxonomy method was used, the source of information for which was an analytical review of academic literature and journalism on digitalization problems.*

The result *of the study was the classification of the dangers of sociotechnical convergence. Depending on the position of the source, the hazards were divided into external and internal. External hazards were classified depending 1) on the position of the source of hazards, 2) on the composition of the digital network platform, which has a certain structure, and 3) on the level of subjectivity of hazards, that is, the level of user influence on the functioning processes, the ability to control the occurrence of certain results. External dangers were also classified on two grounds: the level of subjectivity and the object of its manifestation. The taxonomic division resulted in the classification according to such subject areas as digital data, digital surveillance, digital morality, digital identity, digital privacy, digital communication, digital accessibility, digital competence, digital clusters.*

Conslusion. *The authors conslusion that taxonomy can form the basis for further research to identify and manage the side effects of digitalization.*

Keywords*: digital networking platforms; digital data; digital surveillance; digital morality; digital identity; digital privacy; digital communication; digital accessibility; digital clusters; digital competence.*

Conflict of interest*: In the presented publication there is no borrowed material without references to the author and (or) source of borrowing, there are no results of scientific works performed by the authors of the publication, personally and (or) in co-authorship, without relevant links. The authors declares no conflict of interest related to the publication of this article.*

Funding: *The reported study was funded by RFBR and EISR according to the research project №21-011-31719 "Sociotechnical convergence in the conditions of digitalization of network spaces".*

For citation: Zotov V. V., Aseeva I. A., Budanov V. G. Digital Network Platform: Classification of Sociotechnical Convergence Hazards. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Ekonomika. Sotsiologiya. Menedzhment = Proceedings of the Southwest State University. Series: Economics, Sociology and Management*. 2021; 11(6): 243–259. (In Russ.) https://doi.org/10.21869/2223-1552-2021-11-6-243-259.

Received 18.10.2021 Accepted 16.11.2021 Published 29.12.2021

***

Введение

В цифровом обществе новые информационно-телекоммуникационные и цифровые технологии объединены для повышения эффективности функционирования экономики, социальной сферы и публичного управления. Развитие таких цифровых технологий, как «Интернет вещей» (IoT), искусственный интеллект и большие данные (big data), обусловливает содержание трансформации современного общества. Благодаря им новым трендом информатизации, пришедшем на смену компьютеризации, интернетизации и сетевизации, следует признать цифровизацию – создание цифровых сетевых платформ, которые могут обладать аналитическими и прогностическими функциями [1]. Большие возможности цифрового представления информации приводят к тому, что идёт создание цифровых сетевых платформ как системы сетевого информационного взаимодействия пользователей. Сегодня именно благодаря цифровым сетевым платформам человек, не выходя из дома, приобретает билеты, совершает покупки, управляет финансами, получает услуги. Основная декларируемая цель цифровизации общества – сделать жизнь человека максимально комфортной и безопасной, повысить её качество. С этой целью цифровые сетевые платформы собирают различные данные, получаемые из всевозможных источников: от датчика до суперкомпьютера, от индивида за персональным компьютером до рассредоточенных в пространстве групп людей, пользующихся гаджетами.

Отметим, что социальные сети («ВКонтакте», «Одноклассники» и «Фейсбук»), государственные порталы («Госуслуги»), коммерческие интернет-порталы и веб-службы («Яндекс», «Сбер») уже превращаются в цифровые сетевые платформы, которые используют технологии, собирающие, агрегирующие и анализирующие без ведома своих пользователях большие объёмы персональных данных для создания их цифровых профилей. Цифровые сетевые платформы – это совокупность технико-технологических решений, обеспечивающих ведение реестра пользователей, задание алгоритмов их взаимодействия и хранение информации об осуществлённых ими онлайн-транзакциях (цифровых следах). В их основе лежит взаимодействие между акторами и актантами, которое реализуется благодаря не только прямому вводу информации человеком в стационарное или мобильное устройство, но и информации, получаемой со смарт-устройств и датчиков.

Материалы и методы

В процессе работы над исследованием мы опирались на концепцию «новой экологической парадигмы» – направление, которое начало развиваться с конца XX в. в связи с глобальными средовыми изменениями и их социокультурной интерпретацией (Р. Данлоп, У. Каттон, Л. Милбрес, О. Яницкий). Также методология исследования базируется на концепции платформенных исследований, дополненных авторами идеями социотехнической конвергенции. Для классификации рисков использовался метод таксономии, источником информации для которой стал аналитический обзор академической литературы и публицистики по проблемам цифровизации.

Результаты и их обсуждение

В данном исследовании выявлены и структурированы наиболее серьёзные неблагоприятные опасности социотехнической конвергенции цифровых сетевых платформ, а также уточнены понятия опасности и рисков социотехнической конвергенции, определены внутренние и внешние предметные сферы их проявления. Опишем результаты детально.

Определение научной проблемы и цели исследования

Проектирование цифровых сетевых платформ должно осуществляться таким образом, чтобы не противоречили друг другу эффективность технологий и гуманитарные аспекты жизни человека. Это достигается за счёт «конвергенции» (от английского converge – «сводить в одну точку», «сводить воедино»), т. е. под цифровой конвергенцией мы понимаем объединение возможностей человека и цифровых технологий в одной системе для более эффективного решения определённого класса задач. Соответственно, концепт социотехнической конвергенции по своей сути подразумевает синергетическую коэволюцию человека, наделенного цифровыми компетенциями, способного взаимодействовать с другими акторами на сетевой платформе, и, собственно, технико-технологической и программно-алгоритмической составляющих цифровых сетевых платформ. Но такая социотехническая конвергенция содержит в себе определённые вызовы для человека, требующие осмысления и научного исследования.

Признание того, что социотехническая конвергенция может иметь как положительные, так и неблагоприятные последствия, как преднамеренные, так и непреднамеренные, углубляет наше поле теоретизирование в этой области [2, p. 273]. Дело в том, что сегодня назревает необходимость регулирования «темной стороны» последствий внедрения цифровых сетевых платформ. Термин nightside («тёмная сторона») относится к «совокупности негативных явлений, которые связаны с использованием ИТ и могут нанести ущерб благополучию людей, организации и общества» [3, p. 61].

В условиях цифровизации общества порождаемые современными технологиями опасности и угрозы становятся в такой степени очевидными, что их последствия могут далеко превосходить описанное Джорджем Оруэллом в его антиутопии «1984». Поэтому риски и побочные эффекты, связанные с все более широким использованием цифровых сетевых платформ, требуют более тщательного анализа. Целью исследования является выявление и структурирование опасностей, угроз и рисков социотехнической конвергенции в условиях цифровизации социально-сетевого пространства.

Структура цифровой сетевой платформы

Цифровая сетевая платформа как совокупность цифровых технологий используется для создания специализированной системы сетевого взаимодействия представителей заинтересованных сторон в рамках определённой предметной сфере. Отсюда её ключевыми элементами являются непосредственно цифровая инфраструктура как совокупность цифровых технологий хранения и обработки данных, цифровые пользователи как заинтересованные стороны и цифровой интерфейс как множество устройств, обеспечивающих вход и взаимодействие пользователей.

Цифровая инфраструктура обеспечивает хранение больших данных и аналитическую обработку информации с помощью комплекса информационно-телекоммуникационных и цифровых технологий.

Влияние цифровизации на жизнь людей возможно только тогда, когда они станут цифровыми пользователями. Цифровой пользователь – это человек, осуществивший процедуру регистрации и последующей авторизации на цифровой

сетевой платформе в целях доступа к её информационным ресурсам и функционалу. Крайне важно понимать, что само сообщество пользователей является важной частью цифровой платформы, поскольку без совокупности представителей заинтересованных сторон цифровая платформа не имеет ценности. При этом, чем больше и разнообразнее сообщество, тем большую ценность платформа может представлять для её участников.

Ввод и вывод данных обеспечиваются благодаря цифровому интерфейсу как совокупности средств и правил, обеспечивающих взаимодействие пользователя и цифровой платформы посредством сети Интернет. Передача информации от пользователя в цифровую платформу довольно часто является аспектом, определяющим комфортабельность жизнедеятельности пользователя. Доступ в сеть Интернет эволюционировал от модемного, доступного для одного устройства или локальной сети, к беспроводным сетям по технологии Wi-Fi. Сейчас у пользователя возможность «выхода в Интернет» появляется благодаря функционалу смартфонов, планшетов и других современных технологичных устройств. В последние годы наблюдается значительный рост использования «Интернета вещей» (IoT), что меняет традиционный образ жизни на более высокотехнологичный [4]. Сегодня на потребительский рынок выводится все больше технических новинок: дистанционно контролируемая бытовая техника, носимые устройства (браслеты, часы, очки, брелоки), элементы «умного дома», включая измерительные приборы для сферы ЖКХ, мультимедийные системы, системы управления климатом и безопасностью, а также устройства для автомобилей [5]. Люди на цифровых платформах начали общаться не только друг с другом, но и с техническими устройствами, принадлежащими как им самим, так и другим людям. Технология «Интернета вещей» подсоединяет к сети устройства, которым разрешается собирать, анализировать, обрабатывать и передавать данные другим гаджетам сети. Сами гаджеты все чаще общаются между собой, информируя человека о результатах такого контакта постфактум.

На функционирование цифровых сетевых платформ оказывают воздействия внешние и внутренние опасности.

Опасности, угрозы и риски

Прежде всего, обозначим наше понимание терминов «опасность», «угроза» и «риск». Понятие «опасность» часто связывают с совокупностью определённых факторов и условий, которые обладают объективно существующей возможностью оказания негативного воздействия на человека, среду его обитания. В рамках данного исследования мы рассматриваем опасность как проявление различных дестабилизирующих, дисфункциональных факторов, способных вывести из строя или нанести значительные повреждения цифровой сетевой платформе. Угроза является выражением чьего-либо намерения причинить вред [6]. Понятие «угроза» рассматривается как опасность, обусловливающая намерения субъекта с определённой вероятностью нанести ущерб / вред объекту. Опасности и угрозы – это внешние, объективные для субъекта обстоятельства, риск же является субъективно переживаемой проекцией этих обстоятельств. «Индивид учитывает лишь те вероятности, которые он себе представляет, а не те, какие существуют в действительности. При этом нет никакого основания полагать, что субъективные вероятности должны быть равны вероятностям объективным» [7, с. 217]. Риск есть ожидание проявления опасностей и угроз, постоянно присутствующее в настоящем, и страх перед возможными негативными их последствиями, проецируемый на будущее своё поведение. Поэтому будет справедливо определить риск как эспектацию человеком наступления жизненных событий, которые могут привести к деструкции сложившихся социальных практик повседневной жиз-

недеятельности [8]. Жизненные события – это тот момент, когда проявляются опасности или реализуются угрозы.

Предложим свою классификацию опасностей социотехнической конвергенции, отталкиваясь 1) от положения источника опасностей, 2) от состава цифровой сетевой платформы, которая обладает определённой структурой, и 3) от уровня субъектности опасностей, т. е. уровня влияния пользователя на процессы функционирования, возможности контролировать наступления тех или иных результатов.

Внешние и внутренние опасности для функционирования цифровых сетевых платформ

К внешним следует отнести опасности, исходящие из природной и общественно-политической среды, в которой происходит функционирование цифровых платформ. Эти опасности составляют непреодолимую силу для разработчиков, владельцев и пользователей цифровых платформ. В настоящий момент к природным опасностям следует отнести такие стихийные комплексные форс-мажорные обстоятельства, как пандемия Covid-19, а также такие антропогенные процессы, как ухудшение экологической ситуации и сокращение природных ресурсов, экономические кризисы и военные действия.

Ход процесса цифровизации может быть изменён под влиянием внутренних факторов развития общественно-политической сферы общества (например, смена власти, наличие госпрограммы цифровизации, внутренняя политика, коррупция) и путём воздействия внешних факторов (например, экономический кризис в стране и мире, санкции западных стран). Противодействие цифровизации может исходить от различных акторов политического пространства, поэтому глубокое понимание общественно-политического контекста имеет решающее значение для успеха цифровизации. Но самое страшное – это цифровизация ради самой цифровизации. Например, при проектировании и строительстве нового квартала используются цифровые технологии дополненной реальности, больших данных и искусственного интеллекта, одевая AR-очки, но при этом жилые дома связываются с остальным городом единственным шоссе. Или в медицине применяются современные средства связи, аналитические приложения, но прописываются ангажированные или несертифицированные лекарства и процедуры.

Внутренние же опасности можно классифицировать в зависимости от уровня субъектности на сервисные, интенциальные и ментальные. К сервисным опасностям следует отнести те, где нет явного присутствия человека, т. е. уровень субъектности низкий. Такие опасности носят объективный и абсолютный характер, распространяющийся на цифровую инфраструктуру платформ. Эти опасности могут быть вызваны последствиями функционирования технико-технологических систем и (или) их нарушениями. Сюда, например, относятся ошибки при сборе данных, их учёте, утрата базы данных, причиной которой становятся сбои в программном обеспечении и работе аппаратной части, а также любое иное нарушение алгоритмов работы, связанных с применением цифровыми платформами своего функционала. Появление таких опасностей вызывает проведение превентивных мероприятий, профилактику оборудования, проверку надёжности алгоритмов. Источники опасностей, возникающие по вине программно-аппаратной части цифровых платформ, менее прогнозируемы, напрямую зависят от свойств применяемых цифровых технологий.

К интенциальным опасностям относятся опасности, обусловленные преднамеренными действиями субъекта, которые могут привести к причинению ущерба как непосредственно пользователям цифровой платформы, так и их владель-

цам и/или различным социальным группам. Они связаны с неправомерным, несанкционированным доступом к информации как путем разработки специального программного обеспечения, так и путём использования технологий социальной инженерии. Интенциальные опасности создают возможности для различных преступлений и правонарушений.

Ментальные опасности – это опасности, возникающие в силу особенностей восприятия человеком мира и его поведения в цифровом мире. В этом случае человек сам своими действиями или бездействием может поставить под угрозу свою жизнедеятельность.

Рассмотрим основные опасности социотехнической конвергенции, возможность их превращения в угрозы, а также формирующиеся под их воздействием риски.

Опасность некорректного использования цифровых данных

В отличие от принятого понимания информационного общества основная идея сбора данных в цифровом обществе заключается в том, что информация накапливается и применяется в реальном мире, но обрабатывается посредством цифровых технологий в киберпространстве. Именно объемом и возможностями обработки данных и ценна та или иная цифровая платформа. Более того, формирующаяся «экономика данных» характеризуется масштабной синхронизацией баз данных, вследствие чего повышается цена ошибки утраты важной информации, так как даже один сбой способен привести не только к «обрушению» цифровой платформы, но к коллапсу всего цифрового сетевого пространства. Это особенно важно и ответственно в настоящий период, когда на государственном уровне создается единая распределённая база данных на всех граждан России [9]. Реестр граждан будет содержать как базовые (фамилия, имя, отчество, дата и место рождения и смерти, пол, реквизиты записи актов гражданского состояния о рождении и смерти, СНИЛС, ИНН, так и дополнительные (семейное положение, родственные связи, состояние здоровья и иные) сведения о физическом лице. С одной стороны, предполагается, что использование такого полного архива информации о человеке должно ускорить и улучшить качество оказания государственных услуг, но с другой – хранилище будет открыто для чиновников разного уровня, спецслужб, МФУ, словом, для всех заинтересованных сторон.

Вместе с тем в числе первостепенных сервисных опасностей функционирования подобных баз данных – это защищенность цифровой информации. Можно привести массу примеров сбоев в работе таких платформ, например в деятельности Федеральной службы судебных приставов, где технические заминки, совпадение персональных данных приводят к блокировке банковских карт граждан. Цифровая платформа должна гарантировать целостность данных, т. е. не допускать их разрушение или изменение в случае сбоев или некорректной работы непрофессионального пользователя.

Конвергенция человека и цифровой платформы стала настолько естественной, что ощущается их тесная взаимозависимость только в момент непредсказуемых сбоев. Невозможно прогнозировать, когда и в какой части социотехнических систем произойдёт разрыв и как он повлияет человека и его поведение в социуме. Таким образом, цифровизация данных граждан России создаёт реальную опасность для каждого гражданин в виде сбоя работы цифровой платформы и перманентную погруженность в рискогенную социотехническую среду.

Опасность чрезмерного цифрового надзора

Ещё четверть века назад сеть Интернет была местом, где можно было существовать под всевозможными никами, принимать новые «обличия», ведя диалоги с другими такими же анонимами. Сегодня же благодаря тому, что в любом

месте мира к каждому человеку можно получить доступ с помощью цифровых инструментов, развивается система тотального контроля за жизнедеятельностью граждан. Обратим внимание, что на любой цифровой сетевой платформе фактически имеет место полная идентификация человека, вследствие чего любое действие персонализировано, то есть можно определить, кто, что и когда делал на цифровой платформе. Информация о гражданах становится «прозрачной» для владельцев баз, а в случае взлома – и для злоумышленников. Также внедряются системы биометрии, распознавания лиц, которые позволяют идентифицировать личность человека на основе имеющихся сведений. Параллельно с этим идёт развитие системы контроля перемещения, позволяющее на основе геолокации мобильных устройств или при помощи устройств «Интернета вещей» (IoT) отследить перемещение граждан и предложить им услуги в зависимости от их текущего местоположения. А пандемия показала ещё одну возможность цифрового контроля – установление контактов конкретного человека в диапазоне от случайного пересечения до интимных отношений. Ранее задача выявления круга общения человека признавалась трудно выполнимой и финансово высокозатратной. Теперь же появление цифрового сетевого пространства делает её технически элементарной.

Безусловно, сегодня цифровой надзор предназначен для использования информации в целях защиты государственной безопасности, стимулирования производственной деятельности, повышения эффективности работы организаций. Но сам факт возможности осуществления цифрового надзора настораживает часть населения, особенно если его начинают осуществлять спецслужбы, которые считают, «чем больше граждан будут проявлять активность в Интернете, особенно в социальных сетях, тем проще собирать установочные данные, проводить оперативно-розыскные мероприятия и заниматься аналитикой» [10, с. 86]. Но это рождает сопротивление со стороны правозащитников и лидеров гражданского общества, осознающих угрозы благополучию гражданского общества [11]. Поэтому возникают опасения того, что контроль цифровой инфраструктуры государством и крупными корпорациями приведёт к эрозии демократии и гражданских свобод [11, p. 214].

Опасность непрозрачности принятия решений

Недалеко то время, когда в жизни человека появятся цифровые платформы, которые будут принимать решение о возможности продажи спиртного, необходимости замены паспорта, назначении пенсии, доступности кредита, выдаче лицензии на оружие, продлении трудового контракта, т. е. решение принимается на основе данных о человеке и той жизненной ситуации, в которую он попал. Поэтому проблема ответственности за действия систем искусственного интеллекта – самая обсуждаемая. Такие системы имеют технический потенциал к самообучению, совершенствованию и развитию, что делает их все сложнее и менее прозрачными в плане алгоритмов принятия решения. Ожидания общества таковы, что «действия ИИ должны быть прозрачными для широкого круга заинтересованных сторон, в том числе для повышения доверия граждан к ИИ и цифровым технологиям вообще» [12, с. 17]. Иначе появятся непреодолимое препятствие для цифровизации общества и реальные риски для гражданского общества [13].

Но самое главное – алгоритм будет принимать решения в нестандартной жизненной ситуации, которые раньше являлись этическим выбором лица, принимающего решения. Например, назначать или не назначать пособие на детей от 3 до 7 лет при «нулевом доходе» его родителей? Другой пример: продавать

или не продавать оружие, если человек в последнее время в цифровом сетевом пространстве явно выражает угрозы в чей-либо адрес? Пока решение может принимать оператор-человек, можно рассчитывать на сочувствие, понимание, интуицию. Машина же не склонна к сентиментальности, ее алгоритм зависит программных настроек. А поскольку корпорации, в т. ч. государственные, очень активно занимаются внедрением цифровых сервисов, то именно они в ближайшие годы будет настраивать «практику правоприменения» алгоритмов искусственного интеллекта. Это действительно серьёзная проблема, поскольку речь идёт о делегировании права принятия этического решения алгоритмам искусственного интеллекта. При этом в случае ошибки сделать ответственной интеллектуальную систему вряд ли получится. С юридической точки зрения виноват, скорее всего, будет владелец цифровой платформы, «программист» или «эксперт», создающий алгоритмы принятия решений. Но первый никакие правила принятия решений не создавал, оператор лишь закладывает правила поведения в алгоритмы цифровых платформ, определяемые экспертом, специалистом в некоторой предметной области. А эксперт основывает логику принятия решений на тех законах, нормах и правилах, которые действуют в обществе. Таким образом, в проигрыше всегда останется рядовой гражданин как самый незащищенный и некомпетентный участник процесса тотальной цифровизации.

Опасность ошибки идентификации

Необходимость цифровой идентификации постепенно укладывается в сознании людей. Все больше граждан становятся пользователями цифровых сетевых платформ, используя электронную подпись, биометрию, коды и пароли. Однако с признанием данных форм идентификации растёт озабоченность граждан по поводу возможных рисков «кражи личности», когда к персональным данным (особенно биометрическим) цифровой платформы получает доступ совершенно посторонний человек. Например, если человек давно не посещает свой аккаунт в социальной сети, мошенники могут до него добраться и украсть вместе с личными данными пользователя.

Современный «Интернет вещей», помимо потрясающих возможностей, привносит в этот цифровой мир много новых, малоизученных опасностей. Умные устройства, персональный компьютер и бытовая техника, подключённая к сети, все чаще становятся мишенью для хакеров. Из-за несовершенства и технических сбоев человек может стать заложником в собственном «умном доме». Так, осенью 2017 г. была обнаружена уязвимость в мобильном и облачном приложениях дистанционного управления домашней интеллектуальной системы, которая позволила злоумышленнику удалённо войти в облачное приложение и, завладев учётной записью, получить контроль над его устройствами. В частности, стало доступным управление пылесосом и, главное, встроенной в него видеокамерой, которая снимала видео в режиме реального времени и сохраняла его в приложении. При взломе устройств пользователя опасности подвергается персональная информация о человеке: злоумышленникам доступна информация о его местонахождении, состоянии здоровья, ведущихся разговорах, в т. ч. деловых, и т. д. [14]. Именно из-за риска постороннего вмешательства в работу миниатюрных медицинских приборов, в частности, электронного кардиостимулятора кардиолог вице-президента США Дика Чейни не одобрил его использование пациентом. Эксперты по безопасности демонстрируют, что с помощью легкодоступного оборудования, руководства для пользователя и знания кода прибора они могут взять под контроль прибор или осуществлять мониторинг посылаемых им данных [15, p. 499]. Поэтому в новом цифровом деловом мире потребуются технологии для аутентификации не только

личности людей, но и личных вещей граждан.

Опасность несанкционированного доступа и использования персональных данных

Вопрос о нарушении цифровой конфиденциальности также связан с несовершенством современных информационно-коммуникативных технологий. Спектр организаций, имеющих доступ к личной информации, расширяется, и если не управлять этим процессом должным образом, то это может подорвать доверие и репутацию цифровой платформы.

Понятие цифровой конфиденциальности лучше всего можно охарактеризовать как защиту информации о частных лицах, которая собирается от них непосредственно, от информационных датчиков или в результате аналитической деятельности. Цифровая конфиденциальность основана на том факте, что использование цифровых носителей для ведения дел, будь то личных или профессиональных, может оставить следы в цифровой форме (цифровые следы). Например, многие интернет-пользователи не осознают, что информация о них и их привычках поведения в Сети постоянно регистрируется и хранится. IP-адрес компьютера может быть прослежен до определённого пользователя, и таким образом, его привычки и предпочтения при просмотре веб-сайтов могут отслеживаться. Такая информация, как дата и время его поиска, какой браузер он использовал для доступа к веб-сайтам и даже сколько времени он просматривал веб-сайты, может храниться на серверах поисковой системы. Опасность несанкционированного использования персональных данных будет только увеличиваться с ростом числа цифровых сервисов, поскольку каждое устройство становится потенциальной точкой утечки данных. К такой «внезапной сверхпрозрачности» никто не готов.

Сегодня каждая цифровая платформа ведёт свою базу данных пользователей, хотя ее создание идёт вразрез не только с Законом «О персональных данных», но и положениями Конституции РФ о праве на неприкосновенность частной жизни, личную и семейную тайну и недопущении сбора, хранения, использования и распространения информации о частной жизни лица без его согласия [16]. Вместе с тем «манипуляции с данными обеспечивают платформе не только возможность создавать качественные платформенные инструменты взаимодействий пользователей, но и извлекать дополнительную выгоду от данных путём реализации извлечённых знаний третьим лицам, не всегда являющихся участниками платформы» [17]. Кроме того, стремление к повышению прибыли от сбора и обработки данных приводит к возникновению новой формы монополии, называемой цифровой монополией [18], которая стремится к более полному контролю сети и расширенному использованию данных, собранных прямо и косвенно в цифровых экосистемах (Amazon, Facebook). Появляются такие веб-сайты, которые специализируются на формировании профилей частных лиц, включающих не только актуальные полные имена, даты рождения, адреса, псевдонимы, изображения и карты в домах людей и многое другое, но и хранении информации, описывающей последние 10 лет жизни запрашиваемого человека. А поскольку российская программа «Цифровая экономика» в значительной степени связана с деятельностью госкорпораций, данная опасность приобретает актуальность и в плане политического контроля [19].

Такими услугами могут воспользоваться заинтересованные лица в корыстных целях, таких как дискредитация хозяина аккаунта цифровой платформы, для незаконного получение выгод от компаний/государства или мошенничество в отношении пользователя платформы для получения денежных средств граждан.

Поэтому в публичной сфере сохранность персональных данных становится основным предметом «конфликтов и противоречий основных участников в лице национальных государств, технологических компаний (включая Big Tech), коммерческих организаций, криминальных структур, институтов гражданского общества» [20, с. 148].

Так или иначе, с определённой периодичностью происходят утечки информации, даже несмотря на наличие согласия об обработке личных данных, в котором фиксируется, что организация обязуется хранить эти данные и по требованию пользователя уничтожать их. Понятно, что данные о приватной жизни пользователей стараются оберегать через внедрение систем кибербезопасности. Некоторые исследования показали, что предпринимаемые меры недостаточны и не обеспечивают необходимой защиты [21].

Осознание этой опасности всеми участниками цифрового сетевого взаимодействия может ощутимо замедлить скорость и конечные цели развития цифровых технологий, сконцентрировав большую часть усилий на разработке и реализации стратегии обеспечения кибербезопасности.

Опасность виртуализации социальных контактов

Процесс опосредования социальных контактов цифровыми информационными технологиями усиливает их виртуализацию. Значительная часть социальных коммуникаций может быть осуществлена без физического присутствия коммуникантов. Данный тип взаимодействия неизменно реализуется посредством таких технических средств, как планшет, компьютер или иное мобильное устройство с выходом в сеть Интернет. Это реализуется в интернет-магазинах, электронном банкинге, сервисах онлайн-знакомства, обучающих дистанционных курсах. Без сомнения, коммуникации в виртуальном пространстве удобны дистантностью, мобильностью, интерактивностью, мультисубъектностью, трансграничностью. Эти характеристики позволили создать совершенно новые форматы коммуникаций, изменив природу человеческих отношений. Сеть Интернет предоставляет среду, в которой люди могут изображать себя иначе, чем они есть на самом деле, а также даёт возможность в произвольный момент времени прекратить своё участие в актах коммуникации (даже на стадии расчёта за приобретённый товар или услугу). Ясно, что процесс налаживания контактов и формирования социальных связей в виртуальном сетевом пространстве требует от индивида гораздо меньше материальных затрат, физических усилий и «нервных клеток». Но в то же время виртуализация социальных коммуникаций ведёт к росту обособленности. Реальный мир быстро теряет свою привлекательность, поскольку виртуальный мир кажется все более удобным для общения в рамках любой деятельности человека.

Опасность цифрового неравенства

Цифровизация определяет включенность людей в современную жизнь, что стало особенно заметно в период нынешней пандемии и самоизоляции. Инклюзия как процесс социализации граждан подразумевает и доступность цифровых сервисов с учётом всех объективных ограничений. Таким объективным ограничением может выступать, например, технико-технологическая отсталость, которая наблюдается у определённых категорий граждан: жителей отдаленных территорий, у граждан с низким уровнем дохода, людей с ограниченными возможностями здоровья.

Так, жителям небольших хуторов, поселков или аулов нужен не просто выход в сеть Интернет, а возможность пользоваться целым рядом онлайн-сервисов. Это достигается внедрением широкополосного доступа в сеть Интернет. Но здесь проявляется другой фактор: низкий уровень дохода ведёт к тому, что человек реже использует широкополосный Интернет, а

это значительно затрудняет обратную связь при использовании цифровых сервисов. А людям с ограниченными возможностями или с особыми потребностями не всегда удобно пользоваться цифровыми сервисами, так как они создаются без учета их особенностей. Не только инвалидность, но и травмы, болезни, возрастные изменения, появление детей влияют на возможности человека ориентироваться в интернет-пространстве, пользоваться гаджетами и потреблять медиаконтент. Поэтому многим из них необходимы соответствующие пользовательские сценарии. Когда цифровые сервисы изначально проектируются с учётом различных сценариев использования, то они будут продолжать оставаться доступны человеку, даже если со временем у него изменятся возможности и потребности.

Если в обществе существуют достаточно большие группы граждан, которые имеют ограниченные возможности доступа к современным цифровым средствам коммуникации, то можно констатировать наличие «цифрового неравенства» [22]. Фактически «те, кто задействован в данной системе, получают дополнительное преимущество в виде скорости получения необходимой информации, те, кто исключен из данной системы, вынуждены затрачивать больше средств и усилий в таких поисках, что соответственно делает их менее эффективными в современном мире» [23]. При этом цифровое неравенство превращается в перманентную проблему [24]. Например, сегодня пользователь должен быть обеспечен не просто мобильным телефоном, а девайсом с расширенным функционалом, не просто доступом в сеть, а высокоскоростным Интернетом. А это значит, что мы имеем дело с «проблемой движущейся цели».

Опасность цифрового аутсайдерства

Развитие цифровых сервисов связано не только с инфраструктурой, но и с культурой пользователей, практикой использования современных цифровых сервисов, цифровой грамотностью. Намечающийся люфт между темпами развития цифровых технологий и трансформацией компетенций человека порождает опасность цифрового аутсайдерства, когда человек не находит своего места в обществе.

Отметим, пользователи даже ментально не успевают за цифровым прогрессом. У определённой части населения внутреннее растёт страх и сопротивление, когда приходится сталкиваться с цифровыми технологиями. Это может принимать форму футурофобии, что находит выражении в устойчивом предубеждении, негативном отношении к цифровым технологиям в целом или каким-то конкретным сервисам, а может и в переживании тревоги в связи с использованием технологии, которая может лишить самостоятельности, контроля над своими поступками и ответственности, сохранения частной, потаённой информации. Футурофобию отличает от других фобий то, что человек осознает неизбежность контакта с цифровыми технологиями. У него уже нет выбора, поскольку цифровизацию уже не остановить. Преодолению страха перед будущим будет способствовать цифровая компетентность. Она состоит в непрерывном овладении знаниями, умениями, навыками, формировании соответствующей мотивации для того, чтобы уверенно, эффективно, критично и безопасно применять цифровые сервисы в разных сферах своей жизнедеятельности. Именно отсутствие цифровой компетентности порождает неспособность перерабатывать большое количество информации, которая ведет к затрате большого количества личного времени при работе с сервисами.

При этом знание, как именно работает цифровая технология, решающего значения здесь не имеет. Для пользователя важны «рецепты» использования цифровых сервисов, а также ему важно понимать, насколько легко ими овладеть,

можно применить в определённой жизненной ситуации, насколько можно довериться их разработчикам и владельцам.

Опасность сегментации социально-сетевого пространства

Аккумулированная на цифровых платформах личная информация может быть использована и для манипулирования выбором и предпочтениями человека. К этому добавляется таргетирование информации на основе больших данных и «Интернет вещей», т. е. персональные гаджеты пользователей становятся ценным источником информации для формирования цифровых профилей. Не стоит также забывать, что цель любого владельца коммерческой цифровой платформы – это извлечение прибыли, а не обеспечение конституционных прав граждан в области неприкосновенности личной жизни. Поэтому каждый человек хотя бы один раз сталкивался с рекламными предложениями по телефону или электронной почте от посторонних лиц, кому явно не оставлял своих контактов и не давал согласие на обработку персональных данных. Подвергаются атакам рекламных агентов даже те люди, которые крайне осторожно и бережно относятся к распространению своих личных данных. В этом случае наблюдается так называемая персонализация контента, т. е. идёт адаптации выдачи информации с вебресурса под определённые категории интернет-пользователей на основе предсказания возможных интересов и предпочтений, которые даются на основе их персональных данных, цифрового поведения и цифровых следов.

Но цифровой мир идёт дальше. Персонализация сопровождается особым эффектом: крупные цифровые платформы окружают каждого пользователя его собственным информационным «пузырём» [25], внутри которого индивиду демонстрируется отредактированная информационная картина мира на основе анализа его пользовательской активности. Сегодня возникают технологические возможности создания индивидуальных цифровых капсул с учётом индивидуальных особенностей восприятия информации и предпочтений форм и контента её потребления [26]. По мнению А. А. Мовчан, каждый находится «в зоне комфорта собственных предубеждений», «подменяя реальность, паразитируя на страхах и слабостях людей, последние при этом расплачиваются не только потраченным временем, но и реальным положением дел в жизни своей семьи и страны» [27].

Выводы

Главное отличие цифровизации в том, что человек имеет дело не с отдельной информационно-телекоммуникационной технологией, а с комплексом цифровых и информационно-телекоммуникационных технологий, обеспечивающим создание конкретизированной и специализированной системы взаимодействия между акторами и актантами сетевого пространства. В цифровом обществе люди, IoT-устройства и цифровые платформы взаимосвязаны в киберпространстве, и по большому счету результаты, полученные с помощью цифровых сервисов, должны быть возвращены в физическое пространство для обеспечения комфортной среды обитания человека. Именно такая социотехническая конвергенция призвана разрешить основные вызовы глобального цивилизационного развития. Но её сопутствующим элементом выступает повышенная опасность, которая может сформировать рискогенное поведение пользователей цифровых платформ. В этом случае обозначенные нами опасности, которые могут привести к деструкции сложившихся социальных практик повседневной жизнедеятельности в цифровом сетевом пространстве, сильно замедлят темпы цифровизации.

Современному обществу необходимо найти способы сосуществования людей и технологий в цифровом мире, ибо цифровизация – это необратимый процесс. И не исключено, что выбора здесь попросту нет: обозначенные нами опасности идут в

одном пакете с цифровизацией. Однако, вероятнее всего, признание уязвимости цифровых платформ не приведёт к тому, что люди согласятся жертвовать своим новым технологическим комфортом, но станут искать возможности компенсации рисков и более безопасных стратегий развития цифровой техносферы.

Список литературы

1. Зотов В. В. Информационно-аналитические платформы как основа цифровизации общества // Труды 63-й Всероссийской научной конференции МФТИ. 23–29 ноября 2020 года. Гуманитарные науки и педагогика. М.: МФТИ, 2020. С. 71-72.

2. Majchrzak A., Markus M. L., Wareham J. Designing for digital transformation: Lessons for information systems research from the study of ICT and societal challenges // MIS Quarterly. 2016. Vol. 40, N 2. P. 267–277.

3. The dark side of information technology / Tarafdar M., D'Arcy J., Turel O., Gupta A. // MIT Sloan Management Review. 2015. Vol. 56, N 2. P. 61-69.

4. Kumar S., Tiwari P., Zymbler M. Internet of Things is a revolutionary approach for future technology enhancement: a review // Journal of Big Data. 2019. N 6. P.111. https://doi.org/10.1186/s40537-019-0268-2.

5. Собиров Б. Ш. Homo digital: поведение в цифровую эпоху // Modern Science. 2021. № 1-2. С. 112-116.

6. Battistelli F., Galantino M. G. Dangers, risks and threats: An alternative conceptualization to the catch-all concept of risk // Current Sociology. 2018. Vol. 67, N 1. P. 64-78. https://doi.org/ 10.1177/0011392118793675.

7. Алле М. Поведение рационального человека в условиях риска: критика постулатов и аксиом американской школы // THESIS. 1994. Вып. 5. С. 217-241.

8. Зотов В. В., Каменева Т. Н. Социокультурный риск: понятие и классификация // Риски в изменяющейся социальной реальности: проблема прогнозирования и управления: материалы Международной научно-практической конференции, Белгород, 19–20 ноября 2015 года / ответственный редактор Ю. А. Зубок. Белгород: ПТ, 2015. С. 392-396.

9. Климашевская О. В. Цифровая модернизация российского государства и общества: плюсы, вызовы и риски // Власть. 2020. Т. 28, № 1. С. 92-96. https://doi.org/ 10.31171/vlast.v28i1.7047.

10. Винник Д. В. Социальная феноменология цифровой эпохи: риторика ненависти, анонимусы, копирайт и полицейский надзор // Философия образования. 2014. № 4(55). С. 79-88.

11. Pasquale F. The Black Box Society. The Secret Algorithms That Control Money and Information. Cambridge: Harvard University Press, 2016. 320 p.

12. Этика и «цифра» — коротко о главном. Робот-врач, робот-учитель, робот-полицейский: социальные риски и отраслевые этические вызовы: аналитическая записка к тому 2 доклада «Этика и „цифра“: этические проблемы цифровых технологий». М.: РАНХиГС, 2020. 45 с.

13. Aseeva I., Budanov V. Digitalization: potential risks for civil society // Економічний часопис-XXI. 2020. Т. 186, № 11-12. С. 36-47.

14. Бевза Д. Скрытая угроза: Интернет вещей: Чем очень опасен Интернет вещей для современного общества. URL: https://www.gazeta.ru/tech/2018/01/06/11573180/iot_is_not_safe.shtml (дата обращения: 10.09.2021).

15. Clery D. Could your pacemaker be hackable? // Science. 2015. Vol. 347, is. 6221.

16. Асеева И. А. Проблема приватности в цифровую эпоху // Науковедческие исследования, 2020: ежегодник / отв. ред. Е. Г. Гребенщикова; ИНИОН РАН. М., 2020. С. 36-50.

17. Рындина С. В. Уязвимости цифровых платформ // Современные инструменты, методы и технологии управления знаниями. 2020. № 3. С. 1-5.

18. Loertscher S., Marx L. M. Digital monopolies: Privacy protection or price regulation? // International Journal of Industrial Organization. 2020. Vol. 71, N 3. P. 102623.

19. Мухаметов Д. Р. Политические риски и барьеры цифровизации // Гуманитарные науки. Вестник Финансового университета. 2020. Т. 10, № 4. С. 58-64. https://doi.org/ 10.26794/2226-7867-2020-10-4-58-64.

20. Мухаметов Д. Р. Технологии big data в политических процессах: риски и ограничения // Гуманитарные науки. Вестник Финансового университета. 2019. Т. 9, № 9. С. 143-149. https://doi.org/ 10.26794/2226-7867-2019-9-6-143-149

21. Minoli D., Sohraby K., Kouns J. IoT security (IoTSec) considerations, requirements, and architectures // Proceeding 14th IEEE annual consumer communications & networking conference (CCNC). Las Vegas, 2017. P. 1006-1007. https://doi.org/10.1109/ccnc.2017.7983271.

22. Bucy E. P. Social Access to the Internet // The Harvard International Journal of Press-Politics. 2000. Vol. 5, N 1. P. 50-61. https://doi.org/ 10.1162/108118000568967.

23. Pippa N. Digital divide: civic engagement, information poverty, and the Internet worldwide. New York: Cambridge University Press, 2001. 303 p.

24. Compaine B. M. The Digital Divide: Facing a Crisis or Creating a Myth? Cambridge: The MIT Press, 2001. 374 p.

25. Pariser E. The Filter Bubble: What The Internet Is Hiding From You. New York: Penguin Press, 2011. 294 p.

26. Володенков С. В., Артамонова Ю. Д. Информационные капсулы как структурный компонент современной политической интернет-коммуникации // Вестник Томского государственного университета. Философия. Социология. Политология. 2020. № 53. С. 188-196. https://doi.org/10.17223/1998863X/53/20.

27. Мовчан А. А. Россия в эпоху постправды. Здравый смысл против информационного шума. М.: Альпина Паблишер, 2019. 598 с.

References

1. Zotov V. V. [Information and analytical platforms as the basis for the digitalization of society]. Trudy 63-y Vserossiyskoy nauchnoy konferentsii MFTI. 23–29 noyabrya 2020 goda. Gumanitarnyye nauki i pedagogika [Proceedings of the 63rd All-Russian Scientific Conference of MIPT. November 23-29, 2020. Humanities and pedagogy]. Moscow, MIPT Publ., 2020, pp. 71-72. (In Russ.)

2. Majchrzak A., Markus M. L., Wareham J. Designing for digital transformation: Lessons for information systems research from the study of ICT and societal challenges. *MIS Quarterly*, 2016, vol. 40, no. 2, P.267–277.

3. Tarafdar M., D'Arcy J., Turel O., Gupta A. The dark side of information technology. *MIT Sloan Management Review*, 2015, vol. 56, no. 2, pp. 61-69.

4. Kumar S., Tiwari P., Zymbler M. Internet of Things is a revolutionary approach for future technology enhancement: a review. *Journal of Big Data*, 2019, no. 6, p.111. https://doi.org/10.1186/s40537-019-0268-2

5. Sobirov B. Sh. Homo digital: povedeniye v tsifrovuyu epokhu [Homo digital: behavior in the digital age]. *Modern Science*, 2021, no. 1-2, pp. 112-116.

6. Battistelli F., Galantino M. G. Dangers, risks and threats: An alternative conceptualization to the catch-all concept of risk. *Current Sociology*, 2018, vol. 67, no. 1, pp. 64-78. https://doi.org/ 10.1177/0011392118793675

7. Allé M. Povedeniye ratsional'nogo cheloveka v usloviyakh riska: kritika postulatov i aksiom amerikanskoy shkoly [Behavior of a rational person in conditions of risk: criticism of the postulates and axioms of the American school]. *THESIS*, 1994, is. 5, pp. 217-241.

8. Zotov V. V., Kameneva T. N. [Socio-cultural risk: concept and classification]. Riski v izmenyayushcheysya sotsial'noy real'nosti. Problema prognozirovaniya i upravleniya. Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii, Belgorod, 19–20 noyabrya 2015 goda [Risks in a changing social reality. The problem of forecasting and management. Proceedings of the international scientific-practical conference, Belgorod, November 19–20, 2015]; ed. by Yu. A. Zubok. Belgorod, PT Publ., 2015, pp. 392-396. (In Russ.)

9. Klimashevskaya O. V. Tsifrovaya modernizatsiya rossiyskogo gosudarstva i obshchestva: plyusy, vyzovy i riski [Digital modernization of the russian state and society: positive aspects, challenges and risks]. *Vlast' = Power*, 2020, vol. 28, no. 1, pp. 92-96. https://doi.org/ 10.31171/vlast.v28i1.7047

10. Vinnik D. V. Sotsial'naya fenomenologiya tsifrovoy epokhi: ritorika nenavisti, anonimusy, kopirayt i politseyskiy nadzor [Social phenomenology of the digital age: rhetoric of hatred, anonymus, copyright and police supervision]. *Filosofiya obrazovaniya = Philosophy of Education*, 2014, no. 4 (55), pp. 79-88.

11. Pasquale F. The Black Box Society. The Secret Algorithms That Control Money and Information. Cambridge, Harvard University Press, 2016, pp. 214-218.

12. Etika i "tsifra" – korotko o glavnom. Robot-vrach, robot-uchitel', robot-politseyskiy: sotsial'nyye riski i otraslevyye eticheskiye vyzovy: analiticheskaya zapiska k tomu 2 doklada "Etika i „tsifra“: eticheskiye problemy tsifrovykh tekhnologiy". [Ethics and "digital" – briefly about the main thing. Doctor robot, teacher robot, police robot: social risks and sectoral ethical challenges: analytical note to volume 2 of the report "Ethics and the digital: ethical problems of digital technologies"]. Moscow, RANEPA Publ., 2020. 45 p.

13. Aseeva I., Budanov V. Digitalization: potential risks for civil society. *Економічний часопис-XXI = Economic Magazine-XXI*, 2020, vol. 186, no. 11-12, pp. 36-47.

14. Bevza D. Skrytaya ugroza: internet veshchey: Chem ochen' opasen internet veshchey dlya sovremennogo obshchestva [The Latent Threat: the Internet of Things: Why the Internet of Things is very dangerous for modern society]. Available at: https://www.gazeta.ru/tech/2018/ 01/06/11573180 / iot_is_not_safe.shtml. (accessed 10.09.2021)

15. Clery D. Could your pacemaker be hackable? *Science*, 2015, vol. 347, is. 6221.

16. Aseeva I. A. [The problem of privacy in the digital age]. Naukovedcheskie issledovaniya, 2020. Ezhegodnik [Scientific research, 2020. Yearbook]; ed. by E. G. Grebenshchikova. Moscow, ISISS RAS Publ., 2020, pp. 36-50. (In Russ.)

17. Ryndina S. V. Uyazvimosti tsifrovykh platform [Vulnerabilities of digital platforms]. *Sovremennyye instrumenty, metody i tekhnolo-gii upravleniya znaniyami = Modern Knowledge Management Tools, Techniques and Technologies*, 2020, no. 3, pp.1-5.

18. Loertscher S., Marx L. M. Digital monopolies: Privacy protection or price regulation? *International Journal of Industrial Organization*, 2020, vol. 71, no. 3, pp. 102623.

19. Mukhametov D. R. Politicheskiye riski i bar'yery tsifrovizatsii [Political risks and barriers of digitalisation]. *Gumanitarnye Nauki. Vestnik Finasovogo Universiteta = Humanities and Social Sciences. Bulletin of the Financial University*, 2020, vol. 10, no. 4, pp. 58-64. https://doi.org/ 10.26794/2226-7867-2020-10-4-58-64

20. Mukhametov D. R. [Big Data technologies in political processes: risks and opportunities]. *Gumanitarnye Nauki. Vestnik Finasovogo Universiteta = Humanities and Social Sciences. Bulletin of the Financial University*, 2019, vol. 9, no. 9, pp.143-149. https://doi.org/10.26794/2226-7867-2019-9-6-143-149

21. Minoli D., Sohraby K., Kouns J. IoT security (IoTSec) considerations, requirements, and architectures. Proceeding 14th IEEE annual consumer communications & networking conference (CCNC). Las Vegas, 2017, pp. 1006-1007. https://doi.org/ 10.1109/ccnc.2017.7983271

22. Bucy E. P. Social Access to the Internet. *The Harvard International Journal of Press-Politics*, 2000, vol. 5, no. 1, pp. 50-61. https://doi.org/10.1162/108118000568967

23. Pippa N. Digital divide: civic engagement, information poverty, and the Internet worldwide. New York, Cambridge University Press, 2001. 303 p.

24. Compaine B. M. The Digital Divide: Facing a Crisis or Creating a Myth? Cambridge, The MIT Press, 2001. 374 p.

25. Pariser E. The Filter Bubble: What The Internet Is Hiding From You. New York, Penguin Press, 2011. 294 p.

26. Volodenkov S. V., Artamonova Yu. D. Informatsionnyye kapsuly kak strukturnyy komponent sovremennoy politicheskoy internet-kommunikatsii [Information capsules as a structural component of contemporary political internet communication]. *Vestnik Tomskogo gosudarstvennogo universiteta. Filosofiya. Sotsiologiya. Politologiya = Tomsk State University Journal of Philosophy, Sociology and Political Science*, 2020, no. 53, pp. 188-196. https://doi.org/10.17223/1998863X/53/20

27. Movchan A. A. Rossiya v epokhu postpravdy. Zdravyy smysl protiv informatsionnogo shuma [Russia in the era of post-truth. Common sense versus information noise]. Moscow, Alpina Publisher, 2019. 598 p.

Информация об авторах / Information about the Authors

Зотов Виталий Владимирович, доктор социологических наук, профессор, профессор департамента философии учебно-научного центра гуманитарных и социальных наук, Московский физико-технический институт (национальный исследовательский университет), Московская область, г. Долгопрудный, Российская Федерация,
e-mail: om_zotova@mail.ru,
ORCID: 0000-0003-1083-1097

Vitaly V. Zotov, Doctor of Sociological Sciences, Professor, Professor of the Department of Philosophy, Educational and Scientific Center for the Humanities and Social Sciences, Moscow Institute of Physics and Technology (National Research University), Moscow Region, Dolgoprudny, Russian Federation,
e-mail: om_zotova@mail.ru,
ORCID: 0000-0003-1083-1097

Асеева Ирина Александровна, доктор философских наук, профессор, ведущий научный сотрудник ИНИОН РАН, г. Москва, Российская Федерация,
e-mail: irinaaseeva2011@yandex.ru,
ORCID: 0000-0002-4172-7762

Irina A. Aseeva, Doctor of Philosophical Sciences, Professor, Leading Researcher at ISISS RAS, Moscow, Russian Federation,
e-mail: irinaaseeva2011@yandex.ru,
ORCID: 0000-0002-4172-7762

Буданов Владимир Григорьевич, доктор философских наук, доцент, главный научный сотрудник ИФ РАН, г. Москва, Российская Федерация,
e-mail: budsyn@yandex.ru,
ORCID: 0000-0003-2371-8659

Vladimir G. Budanov, Doctor of Philosophical Sciences, Associate Professor, Main Research Fellow IPh RAS, Moscow, Russian Federation,
e-mail: budsyn@yandex.ru,
ORCID: 0000-0003-2371-8659