

ЦИФРОВАЯ СОЦИОЛОГИЯ: НАПРАВЛЕНИЯ ИССЛЕДОВАНИЙ

Конвертация опасностей социотехнической конвергенции в риски цифровизации

УДК 316.776

DOI 10.26425/2658-347X-2022-5-2-4-20

Получено 14.03.2022

Доработано после рецензирования 20.04.2022

Принято 26.04.2022

Зотов Виталий Владимирович

Д-р социол. наук, проф. департамента философии Учебно-научного центра гуманитарных и социальных наук, Московский физико-технический институт (национальный исследовательский университет), г. Москва, Российская Федерация

ORCID: 0000-0003-1083-1097

E-mail: Om_zotova@mail.ru

Асеева Ирина Александровна

Д-р филос. наук, вед. науч. сотр., Центра научно-информационных исследований по науке, образованию и технологиям, Институт научной информации по общественным наукам Российской академии наук, г. Москва, Российская Федерация

ORCID: 0000-0002-4172-7762

E-mail: irinaaseeva2011@yandex.ru

Буданов Владимир Григорьевич

Д-р филос. наук, гл. науч. сотр., Сектора междисциплинарных проблем научно-технического развития Институт философии Российской академии наук, г. Москва, Российская Федерация

ORCID: 0000-0003-2371-8659

E-mail: budsyn@yandex.ru

Белкина Виктория Александровна

Преп. каф. философии и социологии, Юго-Западный государственный университет, г. Курск, Российская Федерация

ORCID: 0000-0002-3306-6706

E-mail: viktorija2206.1995@mail.ru

АННОТАЦИЯ

Создание цифровых сетевых платформ сопровождается неоднозначным процессом социотехнической конвергенции, в ходе которого возникают определенные опасности как факторы, дестабилизирующее функционирование цифровой платформы, и риски как ожидания наступления этих событий. Целью исследования является оценка уровня конвертации опасностей социотехнической конвергенции в соответствующие риски. Методология исследования базируется на экосистемном подходе и концепции платформенных исследований, дополненных авторами идеями социотехнической конвергенции. Для оценки конвертации опасностей социотехнической конвергенции в риски цифровизации был применен метод эмпирической верификации на базе репрезентативного социологического опроса. Итогом таксономического деления стала классификация опасностей по таким предметным областям, как: цифровые данные (опасность сбоя работы); цифровой надзор (опасность чрезмерного цифрового надзора); цифровая мораль (опасность принятия решений искусственным интеллектом); цифровая идентификация (опасность ошибки идентификации); цифровая

конфиденциальность (опасность несанкционированного использования персональных данных); цифровая коммуникация (опасность виртуализации социальных контактов); цифровая доступность (опасность цифрового неравенства); цифровые кластеры (опасность сегментации социально- сетевого пространства); цифровая компетентность (опасность цифрового аутсайдерства). Авторы приходят к выводу, что не все опасности конвертируются в риски одинаково. Сильно выраженные эксплицитные риски наблюдаются в результате конвертации опасности несанкционированного использования персональных данных. Средне выраженные эксплицитные риски появляются в случае опасности сбоя работы цифровых платформ, опасности принятия решений искусственным интеллектом, опасности ошибки идентификации, опасности цифрового неравенства. Слабо выраженные эксплицитные риски характерны для конвертации опасности чрезмерного цифрового надзора и опасности виртуализации социальных контактов. В имплицитные риски конвертируются опасность сегментации социально- сетевого пространства и опасность цифрового аутсайдерства.

Ключевые слова

Цифровизация, социотехническая конвергенция, цифровые сетевые платформы, опасности, риски, конвертация рисков, цифровое общество, платформенные исследования

Для цитирования

Зотов В.В., Асеева И.А., Буданов В.Г., Белкина В.А. Конвертация опасностей социотехнической конвергенции в риски цифровизации // Цифровая социология. 2022. Т. 5, № 2. С. 4–20.

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

© Зотов В.В., Асеева И.А., Буданов В.Г., Белкина В.А., 2022.

Статья доступна по лицензии Creative Commons «Attribution» («Атрибуция») 4.0. всемирная (<http://creativecommons.org/licenses/by/4.0/>).



DIGITAL SOCIOLOGY: RESEARCH DIRECTIONS

Converting the sociotechnical convergence hazards into the risks of digitalisation

Received 14.03.2022 Revised 20.04.2022 Accepted 26.04.2022

Vitaliy V. Zotov

Dr. Sci. (Sociol.), Prof. at the Philosophy Department of the Educational and Scientific Center for the Humanities and Social Sciences, Moscow Institute of Physics and Technology, Moscow, Russia

ORCID: 0000-0003-1083-1097

E-mail: Om_zotova@mail.ru

Irina A. Aseeva

Dr. Sci. (Philos.), Leading Researcher at the Centre for Science, Education and Technology Information Studies, Institute of Scientific Information for Social Sciences of the Russian Academy of Sciences, Moscow, Russia

ORCID: 0000-0002-4172-7762

E-mail: irinaaseeva2011@yandex.ru

Vladimir G. Budanov

Dr. Sci. (Philos.), Assoc. Prof., Main Researcher at the Interdisciplinary Science and Technology Development Branch, Institute of Philosophy of the Russian Academy of Sciences, Moscow, Russia

ORCID: 0000-0003-2371-8659

E-mail: budsyn@yandex.ru

Victoria A. Belkina

Lecturer at the Philosophy and Sociology Department, Southwest State University, Kursk, Russia

ORCID: 0000-0002-3306-6706

E-mail: viktorija2206.1995@mail.ru

ABSTRACT

The creation of digital network platforms is accompanied by an ambiguous process of sociotechnical convergence, during which certain hazards arise as factors that destabilize the functioning of a digital platform, and risks as an expectation of the occurrence of these events. The purpose of the study is to assess the level of conversion of the sociotechnical convergence hazards into the corresponding risks. The research methodology is based on the ecosystem approach and the concept of platform research, supplemented by the authors with the ideas of sociotechnical convergence. To study the conversion of the sociotechnical convergence hazards into the risks of digitalization, the method of empirical verification based on a representative sociological survey was applied. The result of the taxonomic division was the classification of hazards in such subject areas as (hazard of failure); digital surveillance (hazard of excessive digital surveillance); digital morality (hazard of decision-making by artificial intelligence); digital identification

(hazard of identification error); digital privacy (hazard of unauthorized use of personal data); digital communication (hazard of virtualization of social contacts); digital accessibility (hazard of digital inequality); digital clusters (hazard of social network segmentation); digital competence (hazard of digital outsider). The authors come to the conclusion that not all hazards are converted into risks in the same way. Strongly expressed explicit risks are observed as a result of converting the hazard of unauthorized use of personal data. Medium-expressed explicit risks appear in case of hazard of failure of digital platforms, hazard of decision-making by artificial intelligence, hazard of identification error, hazard of digital inequality. Weakly expressed explicit risks are typical for the conversion of the hazard of excessive digital surveillance and the hazard of virtualization of social contacts. The hazard of social network segmentation and the hazard of digital outsider are converted into implicit risks.

Keywords

Digitalization, sociotechnical convergence, digital network platforms, hazards, risks, risk converting, digital society, platform research

For citation

Zotov V.V., Aseeva I.A., Budanov V.G., Belkina V.A. (2022) Converting the sociotechnical convergence hazards into the risks of digitalization. *Digital sociology*, vol. 5, no. 2, pp. 4–20. DOI: 10.26425/2658-347X-2021-5-2-4-20

Acknowledgements. The research was carried out with the financial support of the Russian Foundation for Basic Research and Expert Institute for Social Research within the framework of the scientific project No. 21-011-31719 «Sociotechnical convergence in the conditions of digitalization of network spaces».

© Zotov V.V., Aseeva I.A., Budanov V.G., Belkina V.A., 2022.

This is an open access article under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).



ВВЕДЕНИЕ / INTRODUCTION

Большие возможности цифрового представления информации ведут к созданию цифровых сетевых платформ как системы взаимодействия пользователей, заинтересованных в обмене информацией о возможностях и потребностях друг друга. С самого начала в сфере экономики под цифровой платформой понималась «коммуникационная и транзакционная среда, участники которой извлекают выгоды от взаимодействия друг с другом»¹. Другими словами, это информационный ресурс, на котором было организовано взаимодействие между отраслевыми поставщиками и потребителями с целью минимизации транзакционных издержек. На сегодня именно они, выйдя за границы экономики, дают возможность человеку, не выходя из дома, совершать покупки, управлять финансами, приобретать билеты, получать услуги, участвовать в выработке решений. Под лозунгами цифровизации возможно создание совершенно нового мира, в котором будут доминировать иные, отличные от сегодняшней системы социальных ценностей и норм, экономические отношения, управленческие концепции. Но распространение цифровых сетевых платформ несет в себе определенные опасности и риски для человека, требующие осмысления и научного исследования. Современный человек имеет дело с изменением атрибутов социальности, поскольку наблюдается «перенесение значительной части социальных взаимодействий и отношений в виртуальное пространство, появление новых нечеловеческих субъектов взаимодействий» [Василенко, Мещерякова, 2021, с. 104], и соответственно, с новыми рисками и опасностями. В условиях цифровизации общества опасности, порождаемые современными технологиями, становятся в такой степени очевидными, что их последствия могут значительно превосходить описанное Джорджем Оруэллом в его антиутопии «1984». Отрицательные последствия, инициация которых связана с цифровой трансформацией экономики и общества, все чаще включаются в ландшафт опасностей социотехнической конвергенции и рисков цифровизации. Поэтому побочные эффекты, связанные с все более широким использованием цифровых сетевых платформ, требуют более тщательного анализа.

Целью исследования является оценка уровня конвертации опасностей социотехнической

конвергенции в соответствующие риски в условиях цифровизации социально- сетевого пространства.

ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ИССЛЕДОВАНИЯ / THEORETICAL AND METHODOLOGICAL FOUNDATIONS OF THE STUDY

Многие исследователи, связывая среднесрочные тренды развития общества и экономики с их процессом цифровизации, справедливо указывают на возможные опасности, угрозы и риски этого процесса [Aseeva, Budanov, 2020; Гримов, 2021; Кравченко, 2021; Кульков, 2017; Ленчук, Власкин, 2018; Мальшева, 2018; Халин, Чернова, 2018]. Цифровизация сделала крайне популярным такой изначально специфический термин индустрии информационных технологий, как «цифровая платформа». Несомненно, цифровые сетевые платформы, предполагая наличие взаимоотношений между ее владельцем и пользователями, обладают свойством системной синергетичности, которая достигается за счет сетевого эффекта [Rochet, Tirole, 2003]. Это выражается в том, что они создают вокруг себя цифровые экосистемы [Авдокушин, 2021]. От сформированности экосистемы зависит успех самой платформы. Здесь важно определить значение понятия «экосистема». На наш взгляд, это централизованная система пользователей, взаимодействующих, обменивающихся ресурсами и трансформирующих одни их виды в другие. Пользователи выступают и поставщиками контента, размещаемого на платформе, и конечными потребителями услуг различных сервисов, собранных в одном месте.

При этом не следует сбрасывать со счетов технико-технологическую составляющую цифровых сетевых платформ, которая обеспечивает ведение реестра пользователей, задание алгоритмов их взаимодействия и хранение информации об осуществленных ими онлайн-транзакциях (цифровых следов). Поскольку в основе цифровых сетевых платформ лежит взаимодействие между людьми и техносубъектами, проектирование таких систем должно осуществляться таким образом, чтобы исключить противоречие аспектов функционирования цифровых технологий и жизнедеятельности человека. Применительно к цифровизации объединение возможностей человека и цифровых технологий в одной системе для более эффективного решения определенного класса задач следует называть социотехнической конвергенцией. Именно конвергенция (от англ. converge – «сводить в одну точку», «сводить воедино»), как коэволюция человека

¹ Электронная библиотека Белорусского государственного университета (2019). Толковый словарь терминов и понятий по вопросам цифровой трансформации. Режим доступа: [https://elib.bsu.by/bitstream/123456789/236902/1/Словарь терминов и понятий по вопросам цифровой трансформации.pdf](https://elib.bsu.by/bitstream/123456789/236902/1/Словарь%20терминов%20и%20понятий%20по%20вопросам%20цифровой%20трансформации.pdf) (дата обращения: 10.03.2022).

и техники, оказывает важный синергетический эффект в развитие современного общества. Отметим, что проблемы конвергенции оказываются сегодня в центре внимания. В частности, В.Ф. Минаков, А.В. Шуваев, О.С. Лобанов [2018] вводят понятие «умные конвергентные решения», под которыми понимаются «процессы и решения, обладающие совокупностью компонентов и связей между ними сближающего характера (либо взаимопроникновением, сближением), благодаря которым обеспечиваются потребительская ценность и положительный эффект путем (за счет) производства и использования знаний, извлекаемых кибернетическими системами».

Использование экосистемного и платформенного подхода позволяет по-новому взглянуть на цифровую трансформацию и обратить внимание на опасности социотехнической конвергенции.

На сегодняшний день существуют различные взгляды относительно определения опасностей и рисков, в том числе сопутствующих цифровой трансформации. Наиболее распространенное определение опасности связывает ее с совокупностью определенных факторов и условий, которые обладают объективно существующей возможностью оказания негативного воздействия на человека, среду его обитания. Опасность в этом случае имеет отношение к объекту [Луман, 1994], то есть в нашем случае к цифровой сетевой платформе и ее составляющим. Опасность рассматривается как наличие факторов, оказывающих дисфункциональное и/или дестабилизирующее воздействие на цифровую сетевую платформу. Другими словами, эти факторы способны сорвать ее нормальное функционирование, довести до выхода из строя и уничтожения. Опасности носят объективный характер. Это внешние для человека обстоятельства, которые неизбежны. Риски же субъективны. Они создаются собственными представлениями и восприятием опасностей и угроз. «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» [Алле, 1994].

Отметим, что опасности могут быть связаны с внутренней средой цифровой экосистемы или с внешней средой (в частности, политические, экологические и иные риски). В первом случае они – результат, порожденный процессом социотехнической конвергенции. А во втором случае опасности порождены окружающей физической и социальной средой. Угроза является выражением чьего-либо намерения причинить

вред [Battistelli, Galantino, 2018]. Понятие «угроза», в общем случае, отражает опасность, обусловленную намерениями субъекта с определенной вероятностью нанести ущерб/вред объекту.

Нами была предложена своя классификация опасностей социотехнической конвергенции, построенная на основе 1) состава цифровой сетевой платформы, в структуре которой выделяется инфраструктура, пользователи и интерфейс, и 2) субъектности опасностей, понятой как уровень возможности пользователя влиять на функционирование [Зотов и др., 2021]. Классификация опасностей была осуществлена методом таксономии.

Цифровая сетевая платформа, как совокупность цифровых технологий, используется для создания специализированной системы сетевого взаимодействия представителей заинтересованных сторон в рамках определенной предметной сферы (финансы, государственные услуги, транспорт и т.д.). Ее ключевыми элементами являются непосредственно *цифровая инфраструктура* (как совокупность технологий хранения и обработки данных), *цифровые пользователи* (как заинтересованные стороны) и *цифровой интерфейс* (как совокупность правил взаимодействия пользователей и множество устройств для входа на цифровую платформу).

Цифровая инфраструктура представляет собой совокупность организационных структур и комплекс информационно-телекоммуникационных и цифровых технологий, обеспечивающих вычислительные, телекоммуникационные и сетевые мощности платформы, и построенных на их основе сервисов. Цифровая инфраструктура обеспечивает хранение больших данных и аналитическую обработку информации. Ее основа – технологии больших данных и искусственного интеллекта.

Влияние цифровизации на жизнь людей возможно только тогда, когда они станут цифровыми пользователями. Цифровой пользователь – это человек (потребитель), использующий цифровую сетевую платформу для решения стоящих перед ним задач. Как правило, он должен пройти процедуру регистрации и последующую авторизацию для доступа к информационным ресурсам и функциональным возможностям платформы. Каждый цифровой пользователь представляет системе определенного рода информацию о себе: от ФИО до банковских реквизитов, которые образуют его цифровой профиль. А та информация о нем, которая остается после посещения информационного ресурса, образует цифровые следы.

Ввод и вывод данных обеспечивается 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, предоставляемого для одного устройства или локальной сети, к беспроводным сетям по технологии Wi-Fi. Сейчас «выход в интернет» обеспечивается благодаря возможностям смартфона, планшета и других мобильных устройств. В последние годы наблюдается значительный рост использования интернета вещей (англ. Internet of Things, IoT) для входа в сеть «Интернет» [Kumar et al., 2019].

Внутренние же можно классифицировать в зависимости от уровня субъектности на сервисные, интенциальные и ментальные.

К сервисным опасностям следует отнести те, где нет явного присутствия человека. Такие опасности имеют объективный характер, поскольку вызваны дисфункциями технико-технологических систем и (или) нарушениями в их работе. Такие источники опасности совершенно не поддаются прогнозированию, и поэтому меры против них должны применяться всегда. Сюда относятся ошибки при сборе данных, их учете или расчетах, утрата базы данных, причиной которого становятся сбои в программном обеспечении и работе аппаратной части, а также любое иное нарушение алгоритмов работы, связанных с исполнением цифровыми платформами своих функций. Появление таких опасностей определяется ненадежностью аппаратной части цифровой платформы, отсутствием превентивных мероприятий, нерегулярной профилактикой оборудования, небезупречностью работы алгоритмов.

К интенциальным опасностям относятся опасности, обусловленные преднамеренными действиями субъекта, которые могут привести к причинению ущерба как непосредственно пользователям цифровой платформы их владельцам и (или) различным социальным группам социума. Именно данный вид опасностей и следует рассматривать как угрозы, которые являются главной причиной преступлений и правонарушений. Они связаны с неправомерным, несанкционированным доступом к информации как путем разработки специального программного обеспечения, так и путем использования технологий социальной инженерии.

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

Представляется возможным максимально сузить количество опасностей социотехнической конвергенции до определенной предметной области / домена (табл. 1).

Таблица 1. Классификация предметных областей опасностей социотехнической конвергенции

Table 1. Domains of sociotechnical convergence hazards's classification

Структурный элемент	Опасности		
	Сервисные	Интенциальные	Ментальные
Инфраструктура	Цифровые данные	Цифровой надзор	Цифровая мораль
Интерфейс	Цифровая идентификация	Цифровая конфиденциальность	Цифровая коммуникация
Пользователь/клиент	Цифровая доступность	Цифровая кластеризация	Цифровая компетентность

Составлено авторами по материалам исследования / Compiled by the authors on the materials of the study

Ранее проведенный анализ показал, что с функционированием инфраструктуры цифровой сетевой платформы связаны следующие предметные области опасностей социотехнической конвергенции: «цифровые данные», «цифровой надзор», «цифровая мораль». Сервисные опасности в области обработки и передачи цифровых данных проявляются как нарушение работы цифровых сетевых платформ в виде сбоя сервиса, ведущего к непреднамеренному изменению персональной информации; потери данных, разрушение цифрового профиля пользователя и возникновение ошибок при работе некомпетентного пользователя (отсутствие «защиты от дурака»). Интенциальные опасности связаны с попытками владельцев усилить цифровой надзор над своими пользователями. Это проявляется как высокая прозрачность персональных данных для владельцев цифровых платформ, попытки внедрения систем контроля перемещения (геолокации), распознавания лиц, биометрии. Ментальные опасности в области цифровой морали связаны с непрозрачностью алгоритмов принятия решений, ошибочностью принятия решений цифровым сервисом или с предвзятым отношением сервиса к проблемам/запросам человека.

С интерфейсом цифровой сетевой платформы связаны следующие предметные области опасностей социотехнической конвергенции: идентификация, конфиденциальность и коммуникация, которые соответственно носят сервисный, интенциональный и ментальный характер. В предметной области «цифровой идентификации» одной из опасностей является ошибочная идентификация пользователя, которая проявляется, прежде всего, как невозможность войти в аккаунт на цифровой платформе по своим идентификационным данным или, напротив, возможность идентификации постороннего человека как подлинного пользователя аккаунтом цифровой платформы. Сюда же следует отнести менее очевидную опасность, связанную с уязвимостью цифровых платформ со стороны интернет-вещей. Их несанкционированный, самостоятельный вход в систему для обмена информацией может также нанести вред пользователю платформы.

В предметной области «цифровой конфиденциальности» велика опасность несанкционированного использования персональных данных, которая может проявляться в виде 1) использования чужих персональных данных для незаконного получения выгоды от компаний/государства; 2) мошенничества с использованием чужих персональных данных для получения денежных средств или иных благ граждан; 3) создания поддельных аккаунтов (клонов) для ведения своей деятельности или дискредитации владельцев настоящих. В предметной области «цифровой коммуникации» следует обратить внимание на виртуализацию социальных контактов, при которой теряется ценность межличностного человеческого общения. Это выражается в замене обращения в службу поддержки общением с виртуальными помощниками (чат-ботами) или простым (авто)заполнением форм заявок/обращений со стороны клиентов.

Таблица 2. Классификация внутренних опасностей социотехнической конвергенции для составляющих цифровых платформ

Table 2. Classification of sociotechnical convergence's internal dangers for components of digital platforms

Структурный элемент	Предметные области	Опасности	Разновидности
Инфраструктура	Цифровые данные	Опасность сбоя работы цифровых сетевых платформ	Сбой сервиса, ведущий к непреднамеренному изменению персональной информации
			Потеря данных, разрушение цифрового профиля пользователя
			Отсутствие защиты от ошибок некомпетентного пользователя
	Цифровой надзор	Опасность «большого брата» или чрезмерного цифрового надзора	Прозрачность персональных данных на цифровой платформе
			Внедрение системы контроля перемещения (геолокации)
			Внедрение систем распознавания лиц
			Внедрение биометрии
	Цифровая мораль	Опасность принятия решений искусственным интеллектом	Непрозрачность алгоритмов принятия решений
			Ошибочное принятие решений цифровым сервисом
			Предвзятое отношение сервиса к проблемам/запросам пользователя
Интерфейс	Цифровая идентификация	Опасность ошибки идентификации	Невозможность войти в аккаунт на цифровой платформе по своим идентификационным данным
			Возможность использования аккаунта на цифровой платформе посторонним человеком
			Возможность нанесения вреда человеку несанкционированным входом интернет-вещей
	Цифровая конфиденциальность	Опасность несанкционированного использования персональных данных	Использование чужих персональных данных для незаконного получения выгоды от компаний/государства
			Мошенническое использование чужих персональных данных для получения денежных средств граждан
			Создание поддельных аккаунтов (клонов) для введения своей деятельности

Окончание табл. 2

Структурный элемент	Предметные области	Опасности	Разновидности
Интерфейс	Цифровая коммуникация	Опасность виртуализации социальных контактов	Замена обращения в службу поддержки общением с виртуальными помощниками (чат-ботам)
			Отсутствие человеческого общения с поставщиками услуг/товаром
Пользователь	Цифровая доступность	Опасность цифрового неравенства	Отсутствие «нормального» доступа в сеть «Интернет»
			Высокая стоимость пользования цифровыми платформами
			Отсутствие техники (смартфона, планшета, компьютера) для работы с сервисами
			Трудности использования цифровых сервисов для людей с особыми потребностями (инвалиды, пожилые, больные и т.д.)
	Цифровые кластеры	Опасность сегментации социально-сетевого пространства	Персонализация информации, рекламы товаров и услуг
			Рекомендации к добавлению в перечень контактов («в друзья», «в избранное»)
			Погружение в информационную капсулу цифровых платформ
	Цифровая компетентность	Опасность цифрового аутсайдерства	Нехватка умений и знаний пользования сервисами
			Неспособность перерабатывать большое количество информации
			Страх изменений, вызывающий внутреннее сопротивление

Составлено авторами по материалам исследования / Compiled by the authors on the materials of the study

Опасности социотехнической конвергенции тех или иных пользовательских ситуаций порождаются в следующих предметных областях: цифровая доступность, цифровые кластеры и цифровая компетентность. Охарактеризуем опасности, возникающие в данных предметных сферах. Сервисные опасности в области доступности цифровых платформ проявляются как возможность неподключения к цифровой платформе из-за отсутствия высокоскоростного доступа в сеть «Интернет» техники (смартфона, планшета, компьютера) для работы с сервисами или высокой стоимостью пользования цифровыми платформами. Кроме того, сюда следует отнести проблемы в использовании цифровых сервисов людьми с особыми потребностями (инвалиды, пожилые, больные и т.д.). Интенциональные опасности связаны с попытками владельцев осуществить сегментацию своих пользователей, привязав их к определенной цифровой экосистеме. Это проявляется как персонализация информации, рекламы товаров и услуг, навязывание определенных контактов, формирование собственной информационной (новостной) повестки, что ведет к замыка-

нию пользователя в информационной капсуле цифровых платформ. Опасности, возникающие в силу особенностей восприятия человеком мира и его поведения в цифровом мире (ментальные опасности) связаны с недостаточным уровнем цифровой компетентности и проявляются как опасность цифрового аутсайдерства. Это связано с нехваткой умений и знаний пользования сервисами, неспособностью перерабатывать большое количество информации, а также наличием футурофобии – страха перед неизбежными негативными изменениями.

Опасности и угрозы – это внешние для субъекта условия, которые неизбежны, то есть они для него носят объективный характер. Риски создаются собственными представлениями и восприятием опасностей и угроз, то есть они субъективны.

Традиционно используют два основных подхода к раскрытию термина «риск». С одной стороны, риск предстает как вероятность достижения результата в условиях влияния неопределенности, с другой – как степень потенциального негативного воздействия на человека, его здоровье, материальное благополучие, повседневное

поведение. В общем случае риск оказывается тесно связан с такими понятиями, как: «опасность», «вероятность», «неопределенность», «альтернативность». На наш взгляд, риск относится к субъекту, который принимает решение и действует в условиях проявляющихся опасностей. По мнению Н. Лумана, только в случае принятия решений в непредвиденных обстоятельствах появляется риск, поскольку человек подвергается опасностям [Luhmann, 1993, p. 23]. Таким образом, опасность касается объектов, которые не зависят от индивида. В этом случае последний не имеет возможности выбирать модели поведения или осуществлять контроль, в то время как риск связан с решением и выбором такой модели поведения. Риск – это конвертация опасностей, то есть процесс осознания и оценка уровня опасностей с позиций их влияния на самого человека, его повседневное поведение. Это может быть, например, оценка возможности попасть под машину при переходе улицы. С позиций нашего исследования риск можно определить через оценку опасности, которая с определенной вероятностью может выйти из-под контроля. Риск есть ожидание проявления опасностей, постоянно присутствующее в настоящем, и страх перед возможными негативными их последствиями, проецируемый на будущее свое поведение. Поэтому будет справедливо определить риск как экспектацию человеком проявления определенных опасностей, которые могут привести к деструкции сложившихся социальных практик повседневной жизни. А уровень осознания опасностей позволяет классифицировать риски на латентные (скрытые), имплицитные (воспринимаемые) и эксплицитные (учитываемые). Латентные риски – это объективно существующие опасности (угрозы), которые человеком не воспринимаются и не учитываются при осуществлении деятельности (то есть не прошедшие конвертацию). Имплицитные риски – это осознаваемые, человеком опасности, которые, однако, не служат источником трансформации его поведения. И наконец, эксплицитные риски – явные, открыто выраженные опасности, которые осознаются человеком и могут оказать влияние на трансформацию его поведения.

МЕТОДЫ / METHODS

В декабре 2021 г. было проведено массовое социологическое исследование «Цифровое сетевое пространство российского общества» с целью выявления возможностей, опасностей и рисков социотехнической конвергенции в условиях цифровизации сетевых пространств. Одной из задач

этого исследования стала оценка уровня конвертации опасностей социотехнической конвергенции в соответствующие риски. Генеральную совокупность исследования составило население Российской Федерации старше 14 лет. Всего было опрошено 1 000 человек, но часть анкет была исключена из обработки из-за допущенных респондентами при заполнении ошибок. В итоге выборочная совокупность составила 930 респондентов.

Социальный портрет респондента массового опроса следующий. Соотношение мужчин и женщин в выборке 42 % к 58 %. Среди опрошенных люди всех возрастов с незначительным преобладанием по удельному весу молодежи до 20 лет. В выборке представлены граждане в следующих соотношениях: до 20 лет – 19,4 %, от 21 года до 30 лет – 17,4 %; от 31 года до 40 лет – 14 %; от 41 года до 50 лет – 19,9 %, от 51 года до 60 лет – 15,2 %, старше 61 года – 14,1 %.

В целом социально-демографические характеристики респондентов совпадают с социально-демографическими характеристиками населения Российской Федерации, что подтверждает представительность полученных результатов по отношению к генеральной совокупности (всему населению страны).

В связи с эпидемиологической ситуацией техническая организация работ по проведению социологического исследования в форме массового анкетного опроса опиралась на сочетание методов: 1) онлайн-опроса с использованием интерактивного анкетного инструментария на базе сервиса Google Forms; 2) полевого опроса методом личного интервью с помощью печатной анкеты. Это позволяло снизить количество непосредственных контактов исследователя с респондентами, которое представлялось нежелательным в условиях неблагоприятной эпидемиологической обстановки из-за пандемии COVID-19, сопутствовавшей проведению полевых работ. Данные полевого опроса использовались для заполнения респондентами «вакантных» мест в половозрастных квотах выборки. Хотя вероятность возникновения погрешностей, вызванных использованием такого исследовательского инструментария, представляется сравнительно низкой, но тем не менее, такая особенность является важной в контексте описания дизайна социологического исследования.

В ходе опроса выяснялось отношение респондентов к цифровым платформам, их восприятие процессов цифровой трансформации и себя в этих процессах. Процесс конвертации опасностей социотехнической конвергенции в риски оценивался по номинальной шкале: «Да, присуще и может изменить мое отношение» (эксплицитный риск),

«Да, присуще, но на пользовании не сказывается» (имплицитный риск), «Нет, такой проблемы не существует» (латентный риск). На уровне социума будем исходить из следующих соображений. Для отнесения риска к той или иной категории простое большинство населения (50 %) должно выбрать соответствующую позицию на шкале конвертации. При относительном большинстве риск будет относиться к слабовыраженным, а при абсолютном (две трети) – сильно выраженным. Кроме того, данная шкала была дополнена позицией «Затрудняюсь ответить», учитывающей мнение людей, которые не были знакомы с проблемой или не могли дать однозначный ответ из-за противоречивого отношения к исследуемой проблеме.

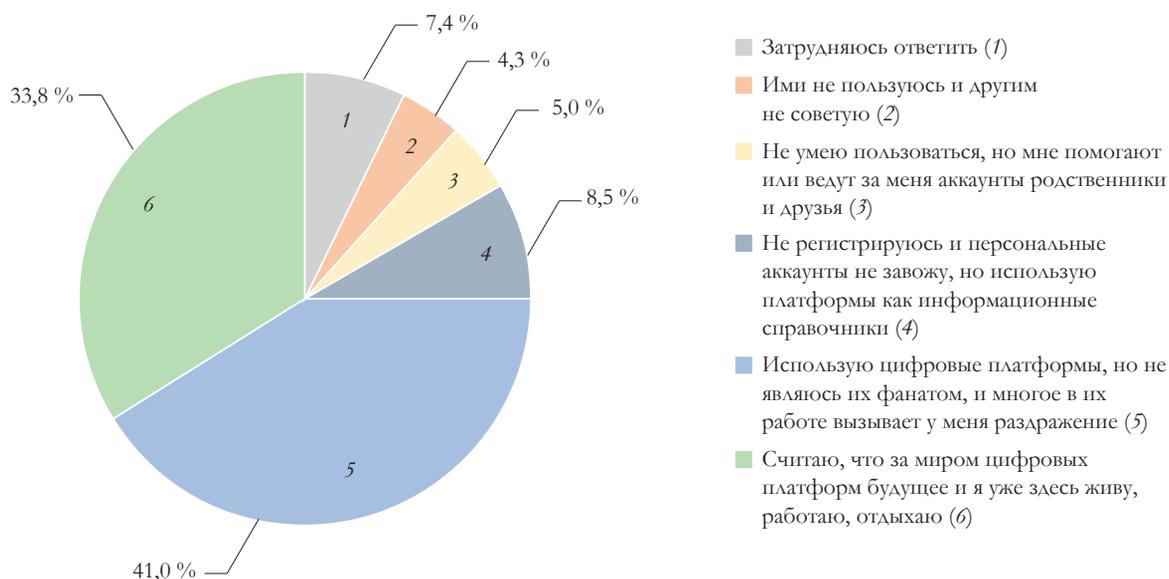
АНАЛИЗ РЕЗУЛЬТАТОВ / RESULTS ANALYSIS

Человечество вступило в эпоху цифровых перемен. В российском обществе достаточно быстрыми темпами идет проникновение цифровых технологий во все сферы жизни человека. При этом катализатором во многом стало распространение коронавирусной инфекции, которая одновременно и высветила их преимущества, и показала их недостатки [Kharlamov et al., 2021]. Каждый день новые цифровые технологии все сильнее проникают в жизнь человека. Изменения, которые наваливаются на современное общество, невозможно остановить. Они так или иначе вторгаются в жизненное пространство

человека и наводят здесь свой порядок. В результате человек нередко теряется перед их неограниченными возможностями: процесс цифровизации оказывается одновременно и увлекательным, и пугающим. По этой причине интерес вызывает оценка отношения граждан к развивающимся цифровым технологиям и в первую очередь к цифровым сервисам/платформам.

Результаты опроса показывают, что преобладающим ответом на вопрос: «Как бы Вы могли определить свое отношение к цифровым платформам?», является ответ: «Использую цифровые платформы, но не являюсь их фанатом, и многое в их работе вызывает у меня раздражение», который можно охарактеризовать как принятие данности, реальности (рис. 1). В то же время треть опрошенных имеет позитивно-оптимистический взгляд на процесс распространения цифровых сетевых платформ.

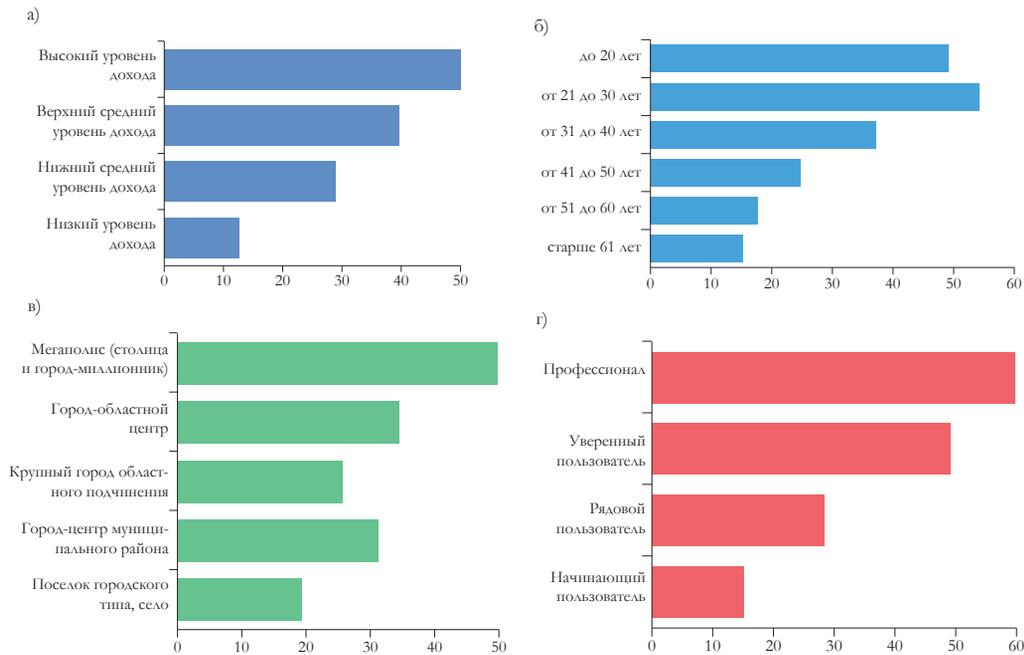
Если попытаться рассмотреть позитивно-оптимистический взгляд респондентов на процесс цифровизации в зависимости от уровня дохода, возраста, места проживания и уровня владения, то можно констатировать наличие определенных эмпирических закономерностей (см. рис. 2). Чем выше уровень дохода у респондента, чем он моложе и чем профессиональнее пользуется цифровой платформой, тем в большей мере он согласен с позицией: «За миром цифровых платформ будущее и я уже здесь живу, работаю, отдыхаю». В отношении места проживания такая закономерность не вполне очевидна. Безусловно, отличие между



Составлено авторами по материалам исследования / Compiled by the authors on the materials of the study

Рис. 1. Распределение ответов респондентов на вопрос «Как бы Вы могли определить свое отношение к цифровым платформам?»

Figure 1. Distribution of respondents' responses to the question "How could you define your attitude to digital platforms?"



Составлено авторами по материалам исследования / Compiled by the authors on the materials of the study

Рис. 2. Зависимость мнения респондентов о том, что за миром цифровых платформ будущее, от уровня дохода (а), возраста (б), места проживания (в) и пользовательского уровня (г)

Figure 2. The dependence of respondents' opinion that the world of digital platforms are the future, on the level of income, age, place of residence and user level

малым населенным пунктом (поселком городского типа / сельским поселением) и мегаполисом огромно. Но вот респонденты, представляющие все остальные города (независимо от их ранга), демонстрируют практически одинаковый выбор данной позитивно-оптимистической позиции.

Растущее влияние цифровых технологий на общество обострило две противоположные позиции относительно последствий цифровизации: технооптимистическую и технопессимистическую. Технооптимисты акцентируют внимание на положительных аспектах цифровых преобразований, а технопессимисты указывают на негативные ее стороны. Через мнение относительно определенных высказываний о современной цифровой реальности и своем поведении в ней можно попытаться оценить то, как люди относятся к технологическим изменениям: как к благу (технооптимизм) или как к злу (технопессимизм). На рисунке 3 представлен индекс согласия с утверждениями о цифровых сервисах/платформах и цифровизации общества, рассчитанный по формуле:

$$I = R_4 + \frac{1}{2} \cdot R_3 - \frac{1}{2} \cdot R_2 - R_1, \quad (1)$$

где R_4 – доля ответов «Полностью согласен»; R_3 – «Скорее согласен, чем нет»; R_2 – «Скорее не согласен, чем да»; R_1 – «Полностью не согласен».

Индекс согласия демонстрирует два интересных момента восприятия респондентами цифровой действительности и себя в этой действительности.

Во-первых, результаты опроса фиксируют очень высокие значения индекса согласия с утверждениями: «Цифровые платформы делают повседневную жизнь проще и удобнее» и «Развитие цифровых платформ позволит решить многие проблемы современного общества». Это свидетельствует о высоком уровне технооптимизма в отношении распространения цифровых платформ.

Во-вторых, фиксируется высокий индекс согласия с утверждениями: «Мне нравится быть в курсе последних технологических новинок» и «Я хотел бы учиться пользоваться цифровыми сервисами». Это говорит о высокой открытости населения цифровым инновациям.

Одновременно опрос показывает, что более половины опрошенных имеют неудачный опыт использования цифровых сервисов (54,4 %). Это вызывает тревогу у части людей (48 %) при их взаимодействии с современными цифровыми технологиями. Последнее особенно сильно проявляется в старших возрастных категориях: 58,8 % у респондентов старше 61 года против 36,8 % у респондентов младше 20 лет.

Для определения опасностей, которые возникают в процессе функционирования инфраструктуры, респондентам были перечислены опасности



Примечание. Цветами выделены позитивные (1) и негативные (2) коннотации утверждений.

Составлено авторами по материалам исследования / Compiled by the authors on the materials of the study

Рис. 3. Индекс согласия с утверждениями относительно цифровых сервисов/платформ и цифровизации общества

Figure 3. Index of agreement with the statements regarding digital services/platforms and digitalization of society

в домене «цифровые данные», «цифровой надзор» и «цифровая мораль» и задан вопрос о том, какие из них присущи цифровым платформам и могут повлиять на отношение к ним. Уровни конвертации этих опасностей в риски социотехнической конвергенции представлены на рисунке 4.

Результаты опроса показывают, что при функционировании цифровых платформ наибольшая конвертация опасностей в риски социотехнической конвергенции наблюдается для опасностей сбоя работы данных платформ (домен «цифровые данные»). Сбой сервиса, ведущий к непреднамеренному изменению персональной информации, а разрушение цифрового профиля пользователя, равно как и потеря данных, может сильно сказаться на поведении пользователей платформ. Неслучайно данная проблема

поднимается в Докладе Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека: «Оцифровка всех данных не повышает надежность хранения, а кардинально снижает ее в среднесрочном периоде, создает риски забвения и потери данных»².

Далее идут опасности принятия решений системами искусственного интеллекта. По мнению большинства опрошенных, изменить их поведение может как ошибочное принятие решений алгоритмами работы технологий искусственного интеллекта, так и предвзятое отношение этих

² Совет при Президенте Российской Федерации по развитию гражданского общества и правам человека (2021). Цифровая трансформация и защита прав граждан в цифровом пространстве: Доклад Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека. Режим доступа http://president-sovet.ru/docs/doclad_SPCh.docx (дата обращения: 10.03.2022).



Составлено авторами по материалам исследования / Compiled by the authors on the materials of the study

Рис. 4. Распределение мнений опрошенного населения об опасности функционирования цифровых платформ и возможность таких опасностей повлиять на отношение к ним

Figure 4. Distribution of the interviewed population's opinion on the hazards of digital platforms and the possibility of such hazards influencing attitudes towards them

алгоритмов к проблемам пользователя платформы (так считают 55,6 % и 51,4 % респондентов соответственно). А вот опасности чрезмерного цифрового надзора (за исключением прозрачности персональных данных на цифровой платформе) респондентов «пугают» в гораздо меньшей степени. Сегодня граждане считают «возможным передачу персональных данных в обобщенном виде для принятия управленческих решений. Половина опрошенного населения не возражает против осуществления цифрового контроля за своими действиями и перемещениями» [Зотов, 2021].

Для определения опасностей социотехнической конвергенции, связанных с интерфейсом цифровых платформ (а это домены «цифровая идентификация», «цифровая конфиденциаль-

ность» и «цифровая коммуникация»), респондентам был задан вопрос о том, какие опасности взаимодействия присущи цифровым платформам и могут повлиять на отношение к ним (рис. 5).

В предметной области «цифровая конфиденциальность» опрос фиксирует самую высокую возможность конвертации опасностей в риски. Так, возможность использования чужих персональных данных для незаконного получения выгод от компаний/государства может заставить изменить поведение 69,0 % опрошенных, создание поддельных аккаунтов (от чужого имени) для введения своей деятельности или для дискредитации его хозяина – 70,0 %, мошенническое использование чужих персональных данных для получения денежных средств граждан – 75,7 %.



Составлено авторами по материалам исследования / Compiled by the authors on the materials of the study

Рис. 5. Распределение мнений опрошенного населения об опасности взаимодействия на цифровых платформах и возможность таких опасностей повлиять на отношение к ним

Figure 5. Distribution of the interviewed population's opinion about the dangers of interaction on digital platforms and the possibility of such dangers affecting attitudes towards them

Поэтому следует признать, что отрицательной стороной развития цифровых технологий являются риски, связанные с утратой конфиденциальности персональных данных человека, поскольку цифровые следы дают беспрецедентно подробную информацию о его частной жизни. Конфиденциальность человека находится в прямой зависимости от эффективности защиты его персональных данных [Farsi et al. (ed.), 2020].

Предметная область «цифровая идентификация» характеризуется средним уровнем конвертации опасностей в риски взаимодействия на цифровых платформах. Несмотря на все достоинства технологий интернета вещей, обычных людей все же пугают их возможности. Так, 57,4 % опрошенных опасаются, что вход постороннего человека на цифровую платформу через интерфейс интернет-вещей может быть использован им во вред. Невозможность войти в аккаунт на цифровой платформе по своим идентификационным данным пугает 59,7 % респондентов. Более

всего вызывает опасение у опрошенных возможность использования личного аккаунта цифровой платформы посторонним человеком. О том, что это может сказаться на их отношении к цифровым платформам заявило 65,4 % опрошенных.

Результаты опроса показывают, что менее всего пользователи воспринимают опасности, связанные с цифровизацией коммуникаций. Так отсутствие человеческого общения с поставщиками услуг/товаров может сказаться на изменении социальных практик только для 40 % опрошенных. При этом фактором, определяющим отношение, выступает уровень навыков работы с цифровыми сервисами. Так в группе лиц, являющихся профессионалами в сфере цифровых и информационно-телекоммуникационных технологий, только 33,3 % признают отсутствие межличностного взаимодействия в качестве опасности, которая может изменить их поведение. В то время как в группе уверенных пользователей таких 37,1 %, а среди рядовых – 44,9 %. Стоит отметить, что в группе

начинающих 40,8 % опрошенных признают отсутствие межличностного взаимодействия в качестве опасности, которая может изменить их поведение. Но здесь велика доля затруднившихся ответить (каждый пятый против каждого десятого в других категориях). Описанная ситуация позволяет классифицировать риски в предметной сфере «цифровая коммуникация» как слабо выраженные эксплицитные.

Для определения опасностей, которые связаны с пользователем цифровой платформы, респондентам были перечислены опасности из домена «цифровая доступность», «цифровая кластеризация» и «цифровая компетентность», а далее предложено высказаться относительно того, какие из этих опасностей возникают в тех или иных пользовательских ситуациях и могут повлиять на отношение к ним. Уровни конвертации данных опасностей в риски социотехнической конвергенции представлены на рисунке 6.

Проведенный опрос показывает, что для опасностей социотехнической конвергенции, которые возникают в тех или иных пользовательских ситуациях на цифровых платформах, наибольшая конвертация в риски наблюдается в домене «цифровая доступность». О том, что они готовы изменить свое поведение, если будет высокая стоимость пользования цифровыми сервисами, заявили 61,8 % опрошенных. Отметим, что мнение респондентов зависит от уровня их дохода (около 70 % в группах с низким и ниже среднего доходом против 55 % в группах с высоким и выше среднего доходом). В случае отсутствия удобного высокоскоростного доступа в сеть «Интернет» готовы изменить свое отношение 55,7 % опрошенных.

Опросы показывают, что опасность сегментации социально-сетевое пространство и опасность цифрового аутсайдерства имеют меньшую рискогенную составляющую и могут рассматриваться как имплицитные риски.



Составлено авторами по материалам исследования / Compiled by the authors on the materials of the study

Рис. 6. Распределение мнений опрошенного населения об опасности тех или иных пользовательских ситуаций, возникающих на цифровых платформах, и возможность таких опасностей повлиять на отношение к ним

Figure 6. Distribution of the interviewed population's opinion about the hazards of certain user situations arising on digital platforms and the possibility of such hazards affecting attitudes towards them

Таблица 3. Уровень конвертации опасностей социотехнической конвергенции в риски цифровизации

Table 3. The level of conversion of the sociotechnical convergence hazards into the risks of digitalization

Структурный элемент	Предметные области	Опасности	Уровень конвертации риска
Инфраструктура	Цифровые данные	Опасность сбоя работы цифровых сетевых платформ	Эксплицитный
	Цифровой надзор	Опасность «большого брата» или чрезмерного цифрового надзора	Эксплицитный (слабо выраженный)
	Цифровая мораль	Опасность принятия решений искусственным интеллектом	Эксплицитный
Интерфейс	Цифровая идентификация	Опасность ошибки идентификации	Эксплицитный
	Цифровая конфиденциальность	Опасность несанкционированного использования персональных данных	Эксплицитный (сильно выраженный)
	Цифровая коммуникация	Опасность виртуализации социальных контактов	Эксплицитный (слабо выраженный)
Пользователь	Цифровая доступность	Опасность цифрового неравенства	Эксплицитный
	Цифровые кластеры	Опасность сегментации социально- сетевого пространства	ИмPLICITный
	Цифровая компетентность	Опасность цифрового аутсайдерства	ИмPLICITный

Составлено авторами по материалам исследования / Compiled by the authors on the materials of the study

В таблице 3 представлен уровень конвертации опасностей социотехнической конвергенции в риски цифровизации исходя из предложенной шкалы: латентные, имплицитные и эксплицитные.

ЗАКЛЮЧЕНИЕ / CONCLUSION

Цифровизация есть объективный и неизбежный процесс, который актуализирует проблему конвертации опасностей социотехнической конвергенции в риски.

Результаты опроса свидетельствуют о высоком уровне технооптимизма в отношении распространения цифровых платформ и высокой открытости населения цифровым инновациям. Одновременно опрос показал, что более половины опрошенных имеют неудачный опыт использования цифровых сервисов и поэтому испытывают тревогу при их взаимодействии с современными цифровыми технологиями.

Жизнь на цифровых платформах будет наполнена многими совершенно новыми опасностями и рисками, с которыми предстоит считаться человеку в своей повседневной жизни. Опасность рассматривается как наличие факторов, оказывающих на цифровую сетевую платформу дисфункциональное и/или дестабилизирующее воздействие, а риск как конвертацию опасностей, то есть

процесс осознания и оценки уровня опасностей с позиций их влияния на самого человека, его повседневное поведение. Уровень осознания опасностей позволяет классифицировать риски на латентные (скрытые), имплицитные (воспринимаемые) и эксплицитные (учитываемые).

Нами была предложена своя классификация опасностей социотехнической конвергенции, построенная на основе:

1) состава цифровой сетевой платформы, в структуре которой выделяется инфраструктура как совокупность цифровых технологий хранения и обработки данных, пользователи – как заинтересованные стороны и интерфейс – как совокупность устройств, обеспечивающих вход и взаимодействие пользователей;

2) субъектности опасностей, понятой как уровень возможности пользователя влиять на функционирование.

Итогом таксономического деления стала классификация опасностей по таким предметным областям, как: цифровые данные (опасность сбоя работы); цифровой надзор (опасность чрезмерного цифрового надзора); цифровая мораль (опасность принятия решений искусственным интеллектом); цифровая идентификация (опасность ошибки идентификации); цифровая конфиденциальность (опасность несанкционированного использования персональных данных); цифровая коммуникация (опасность виртуализации

социальных контактов); цифровая доступность (опасность цифрового неравенства); цифровые кластеры (опасность сегментации социально-сетевого пространства); цифровая компетентность (опасность цифрового аутсайдерства). На основе этой классификации и результатов эмпирической верификации (посредством репрезентативного социологического опроса граждан) была дана следующая оценка конвертации опасностей социотехнической конвергенции в риски цифровизации. В сильно выраженные эксплицитные риски конвертируется опасность несанк-

ционированного использования персональных данных; в средне выраженные эксплицитные риски – опасность сбоя работы цифровых сетевых платформ, опасность принятия решений искусственным интеллектом, опасность ошибки идентификации, опасность цифрового неравенства; в слабо выраженные эксплицитные риски – опасность чрезмерного цифрового надзора и опасность виртуализации социальных контактов. В имплицитные риски конвертируются опасность сегментации социально-сетевого пространства и опасность цифрового аутсайдерства.

СПИСОК ЛИТЕРАТУРЫ

- Авдокушин Е.Ф.* (2021). Формирование и развитие цифровых экосистем // Вопросы новой экономики. № 4 (60). С. 4–12. https://doi.org/10.52170/1994-0556_2021_60_4
- Алле М.* (1994). Поведение рационального человека в условиях риска: критика постулатов и аксиом американской школы // THESIS. Т. 5. С. 217–241. [Фр.: Allais M. (1953). Le comportement de l'homme rationnel devant le risque: critique des postulats et axiomes de l'école américaine // Econometrica, vol. 21, no. 2, pp. 503–549]
- Василенко Л.А., Мещерякова Н.Н.* (2021). Социология цифрового общества: монография. Томск: Изд-во Томского политехнического университета. 226 с.
- Гримов О.А.* (2021). Контуры цифровой реальности: теоретико-методологические аспекты // Известия Юго-Западного государственного университета. Серия: Экономика. Социология. Менеджмент. Т. 11, № 6. С. 223–232. <https://doi.org/10.21869/2223-1552-2021-11-6-223-232>
- Зотов В.В.* (2021). Демаркация публичного и частного при взаимодействии государства и граждан на цифровых сетевых платформах // Цифровая социология. Т. 4, № 3. С. 16–26. <https://doi.org/10.26425/2658-347X-2021-4-3-16-26>
- Зотов В.В., Асеева И.А., Буданов В.Г.* (2021). Цифровая сетевая платформа: классификация опасностей социотехнической конвергенции // Известия Юго-Западного государственного университета. Серия: Экономика. Социология. Менеджмент. Т. 11, № 6. С. 243–259. <https://doi.org/10.21869/2223-1552-2021-11-6-243-259>
- Кравченко С.А.* (2021). Социология цифровизации: учебник для вузов. М.: Юрайт. 236 с.
- Кульков В.М.* (2017). Цифровая экономика: надежды и иллюзии // Философия хозяйства. № 5 (113). С. 145–156.
- Ленчук Е.Б., Власкин Г.А.* (2018). Формирование цифровой экономики в России: проблемы, риски, перспективы // Вестник Института экономики Российской академии наук. № 5. С. 9–21. <https://doi.org/10.24411/2073-6487-2018-00001>
- Луман Н.* (1994). Понятие риска // THESIS. Т. 5. С. 135–160. [Нем.: Luhmann N. (1991). Der Begriff Risiko // Soziologie des Risikos / Luhmann N. Berlin; New York: Walter de Gruyter. Pp. 9–40]
- Мальшичева Г.А.* (2018). О социально-политических вызовах и рисках цифровизации российского общества // Власть. Т. 26, № 1. С. 40–46.
- Минаков В.Ф., Шуваев А.В., Лобанов О.С.* (2018). Эффект цифровой конвергенции в экономике // Известия Санкт-Петербургского государственного экономического университета. № 2 (110). С. 12–18.
- Халин В.Г., Чернова Г.В.* (2018). Цифровизация и ее влияние на российскую экономику и общество: преимущества, вызовы, угрозы и риски // Управленческое консультирование. № 10 (118). С. 46–63. <https://doi.org/10.22394/1726-1139-2018-10-46-63>
- Aseeva I., Budanov V.* (2020). Digitalization: potential risks for civil society // Economic Annals-XXI. V. 186, No. 11-12, pp. 36–47. <https://doi.org/10.21003/ea.V186-05>
- Battistelli F., Galantino M.G.* (2018). Dangers, risks and threats: An alternative conceptualization to the catch-all concept of risk // Current Sociology. V. 67, No. 1. Pp. 64–78. <https://doi.org/10.1177/0011392118793675>
- Farsi M., Daneshkhah A., Hosseinian-Far A., Jahankhani H. [ed.]* (2020). Digital Twin Technologies and Smart Cities. Cham, Switzerland: Springer International Publishing. 212 p. <https://doi.org/10.1007/978-3-030-18732-3>
- Kharlamov, A.A., Raskhodchikov A.N., Pilgun M.* (2021). Smart city data sensing during COVID-19: Public reaction to accelerating digital transformation // Sensors. V. 21, No. 12. Art. 3965. <https://doi.org/10.3390/s21123965>
- Kumar S., Tiwari P., Zymbler M.* (2019). Internet of Things is a revolutionary approach for future technology enhancement: a review // Journal of Big Data. No. 6. Art. 111. <https://doi.org/10.1186/s40537-019-0268-2>

Luhmann N. (1993). *Risk: A Sociological Theory*. Berlin; New York: de Gruyter. 236 p.

Rochet J.-C., Tirole J. (2003). Platform Competition in Two-Sided Markets // *Journal of the European Economic Association*. V. 1, No. 4. Pp. 990–1029.

REFERENCES

Allais M. (1994), “Behavior of a rational person in conditions of risk: criticism of the postulates and axioms of the American school”, *THESIS*, vol. 5, pp. 217–241. [Trans. from French: Allais M. (1953), “Le comportement de l’homme rationnel devant le risque: critique des postulats et axiomes de l’école américaine”, *Econometrica*, vol. 21, no. 2, pp. 503–549]

Aseeva I., Budanov V. (2020), “Digitalization: potential risks for civil society”, *Economic Annals-XXI*, vol. 186, no. 11-12, pp. 36–47, <https://doi.org/10.21003/ea.V186-05>

Avdokushin E.F. (2021), “Formation and development of digital ecosystems”, *Voprosy novoi ekonomiki*, no. 4 (60), pp. 4–12, https://doi.org/10.52170/1994-0556_2021_60_4

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

Farsi M., Daneshkhah A., Hosseinian-Far A., Jahankhani H. [ed.] (2020), *Digital Twin Technologies and Smart Cities*, Springer International Publishing, Cham, Switzerland, <https://doi.org/10.1007/978-3-030-18732-3>

Grimov O.A. (2021), “Contours of Digital Reality: Theoretical and Methodological Aspects”, *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Ekonomika. Sotsiologiya. Menedzhment*, vol. 11, no 6, pp. 223–232, <https://doi.org/10.21869/2223-1552-2021-11-6-223-232>

Kravchenko S.A. (2021), *Sociology of digitalization: University textbook*, Yurait, Moscow, Russia, (in Russian).

Khalin V.G., Chernova G.V. (2018), “Digitalization and its impact on the Russian economy and society: Advantages, challenges, threats and risks”, *Administrative Consulting*, vol. 10 (118), pp. 46–63, <https://doi.org/10.22394/1726-1139-2018-10-46-63>

Kharlamov A.A., Raskhodchikov A.N., Pilgun M. (2021), “Smart city data sensing during COVID-19: Public reaction to accelerating digital transformation”, *Sensors*, vol. 21, no. 12, art. 3965, <https://doi.org/10.3390/s21123965>

Kulkov V.M. (2017), Digital Economy: Hopes and Illusions, *Filosofiya khozyaistva*, no. 5, pp. 145–156.

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

Lenchuk E.B., Vlaskin G.A. (2018), “Formation of the digital economy in Russia: Problems, risks, prospects”, *Vestnik Instituta Ekonomiki Rossiyskoi akademii nauk*, no. 5, pp. 9–21. <https://doi.org/10.24411/2073-6487-2018-00001>

Luhmann N. (1993), *Risk: A Sociological Theory*, de Gruyter, Berlin, New York.

Luhmann N. (1994), “Concept of risk”, *THESIS*, no. 5, pp. 135–160. [Trans. from German: Luhmann N. (1991), Der Begriff Risiko, In: Luhmann N. *Soziologie des Risikos*, Walter de Gruyter, Berlin, New York, pp. 9–40]

Malysheva G.A. (2018), “On the socio-political challenges and risks of digitalization of the Russian society”, *Vlast*, vol. 26, no. 1, pp. 40–46.

Minakov V.F., Shuvaev A.V., Lobanov O.S. (2018), “Effect of digital convergence in economy”, *Izvestiya Sankt-Peterburgskogo gosudarstvennogo ekonomicheskogo universiteta*, no. 2 (110), pp. 12–18.

Rochet J.-C., Tirole J. (2003), “Platform Competition in Two-Sided Markets”, *Journal of the European Economic Association*, vol. 1, no. 4, pp. 990–1029.

Vasilenko L.A., Meshcheryakova N.N. (2021), *Sociology of Digital Society: monograph*, Tomsk Polytechnic University Publishing House, Tomsk, Russia (In Russian).

Zotov V.V. (2021), “Demarcation of the public and private in the interaction of the state and citizens on digital network platforms”, *Digital Sociology*, vol. 4, no. 3, pp 16–26, <https://doi.org/10.26425/2658-347X-2021-4-3-16-26>

Zotov V.V., Aseeva I.A., Budanov V.G. (2021), “Digital network platform: classification of sociotechnical convergence hazards”, *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Ekonomika. Sotsiologiya. Menedzhment*, vol. 11, no. 6, pp. 243–259, <https://doi.org/10.21869/2223-1552-2021-11-6-243-259>