УДК 004.5

В. М. Золотухин, М. В. Золотухин
Кузбасский государственный технический университет
им. Т.Ф. Горбачева, Кемерово, Россия
Томский государственный университет систем управления и радиоэлектроники
Томск, Россия

ПРОБЛЕМЫ ЦИФРОВОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ РАЗВИТИЯ ТЕХНОЛОГИЙ

В статье рассматриваются проблемы цифровой безопасности, в том числе связанные с принудительным переходом на дистанционную работу. Подчеркивается, что с процессами расширения цифрового пространства сопряжены как позитивные, так и негативные моменты, возникают социально-экономические риски, а также трансформируется сознание человека и его поведение. Акцентировано внимание, что это связано с уровнем доверия к государственным институтам, с социокультурной востребовательностью, их функциональной необходимостью в цифровых технологиях. Увеличение технологических каналов распространения информации требует адаптации человека к цифровой реальности, что влечет за собой поиск способов и механизмов обеспечения безопасности человека и идентичности в реальном мире.

Ключевые слова: информация**,** информационная безопасность**,** доверие, сознание, социокультурная среда, киберриски, цифровое пространство.

Современное урбанизированное общество невозможно представить без использования различных технологий в повседневной жизни. Информатизация, цифровизация и социальная среда тесно взаимосвязаны и переплетены между собой в рамках социокультурного пространства. С процессом расширения цифрового пространства возникают не только позитивные, но и негативные моменты, в основе которого лежит уровень доверия к цифровым технологиям со стороны человека и его окружения.

От уровня доверия к цифровым технологиям, методам и способам их внедрения, а также доступности и полезности их использования зависит трансформация сознания человека. С этим связано формирование стереотипов экономического поведения [Золотухин, 2018, Золотухин, Семина, Семина. 2020], основанного на психико-физиологических реакциях. Существенную роль играет адаптация к способам и методам получения знания, технологическим возможностям и степени их осознания, восприятия и применение в практической деятельности. При сознательном изменении стереотипов поведения и своего отношения к использованию новых техно-

логий определяется социокультурная востребовательность технологических, в том числе цифровых изменений со стороны различных субъектов.

Степень восприимчивости человеком новых технологий и возможностей расширяет зону риска их применения не только в позитивном, но и негативном аспектах. По мнению А. Пишняк и Н. Халиной «степень проникновения технологий и государственная политика в их отношении различаются, имеют место межкультурные особенности восприятия инновационных процессов» [Пишняк, Халина, 2021, С. 43]. Более того, подчеркивается социальная обусловленность инноваций, в рамках которой «простота эксплуатации включает в себя также компоненту самоидентификации («Новыми техническими средствами пользуются такие же люди, как и я»), а воспринимаемая полезность помимо прочего подразумевает престижность применения новых технологий, принадлежность к группе людей, идущих в ногу со временем» [Пишняк, Халина, 2021, С. 49]. В связи с этим возникает необходимость создания системы цифровой безопасности во всех сферах жизнедеятельности человека.

Человек в своей повседневной практике стремится создать условия для обеспечения безопасности, как самого себя, так и окружающих. Понимание и представление безопасности может быть индивидуализировано, хотя есть и объективированные критерии обеспечения безопасности. Особенно это значимо в рамках изменений (социальных, техногенных и т.д.), угрожающих нормальной жизнедеятельности человека. В то же время, существует опасность превращения безопасности в определенный «культ», ибо как отмечает А. Фатенков, «Власть имущие – повсеместно – заинтересованы не в том, чтобы поддержать гражданина в его способности самому себя защищать, а в том, чтобы отнять у него по максимуму эту способность и присвоить её себе ради собственной защищённости [Фатенков, 2021, С. 107]. Более того, «можно с уверенностью сказать, что множество типовых угроз останется неизменным, так как используемый в основе мо-

дели угроз аппарат имеет высокую степень абстракции и строится на теории графов, а не на объектах реального мира» [Егошин, 2021, С. 23].

Информационная безопасность являясь «отражением определенных интересов и ценностей», ставит проблему о легитимности и репрезентативности, состоящая «в нарастающей сложности последующего социального контроля, в том, что цифровые технологии в их натиске и тотальности превращаются в квазиприродную силу, к которой индивиды и сообщества вынуждены приспосабливаться [Грунвальд, Ефременко, 2021, С. 38]. По мнению В. И. Пржиленского появляются «такие явления как «умная толпа», государство в смартфоне. Жизнь человека трансформировалась не в соответствии с каким бы то ни было планом или проектом, но в результате сложения разнородных и разнонаправленных изменений, каждое из которых связано с использованием индивидами и коллективами электронных цифровых устройств и IT-технологий» [Пржиленский, 2021, С. 74].

Требуя новых, «калиброванных» сотрудников, в процессах цифровизации изменяется язык, «из него уходит эмоциональная окраска, синтаксис и грамматика, к сожалению, и традиционный язык национальной культуры уходит вместе с продвижением цифровой среды» [Попова, 2021, С. 53]. С точки зрения психологии, изменение форм передачи информации приводит к изменению «языковой личности» [Гейхман, Ставцева, 2016]. Это является основанием для констатации возрастания взаимосвязи транспортных сетей и сетей цифровых, что привело к сжатию пространства и времени, а также «можно считать иным модусом человеческого бытия, порождаемым новой реальностью» [Пржиленский, 2021, С. 75].

В рамках изменения социальной реальности и осознания неизбежности существования цифровой среды в повседневной жизнедеятельности необходимо постоянное повышение цифровой грамотности. Формирования цифровой культуры необходимо для минимизации возникновения и существования киберрисков. Подобные риски возникают по инициативе

самих пользователей цифровыми ресурсами, а также связаны с другими пользователями и/или организациями, предоставляемыми данные ресурсы. Иными словами, они связаны как с неосведомленностью сотрудника с работами с фишинговым ссылкам, так и с экономией на программах по информационной безопасности и обучении персонала. По мнению Н. И. Глухова и П. Н. Недосекина, «как в России, так и в странах СНГ подавляющее число источников угроз информационной безопасности приходится на рядовых работников предприятий (73/81% – соответственно Россия и СНГ) и уволенных (40/30% –соответственно Россия и СНГ)» [Глухов, Наседкин, 2021, С. 36]. Из результатов аналитических исследований за 2019 г., касающихся оценки уровня информационной безопасности в компаниях России и СНГ, следует, что: «основным источником внутренних угроз информационной безопасности на предприятиях был и остается персонал, контроль которого должен осуществляться как со стороны непосредственного руководителя, так и со стороны кадровых служб и служб безопасности» [Глухов, Наседкин, 2021, С. 40]. С этой точки зрения, угрозу как личной, так и коллективной безопасности представляют цифровые следы как следствие определенного вида деятельности. С одной стороны, по мнению Т. Г. Лешкевича, цифровизация «задает надличностные масштабы контроля и принуждения, чревата информационной перегрузкой и когнитивными деформациями, а с другой – манифестирует ценность цифровых форм познания, досуга и развлечений, обеспечивает многообразные способы коммуникации и творческого самовыражения» [Лешкевич, 2020].

Деятельность может иметь как позитивный так и негативный характер, связана с контролем и оценкой поведения, а также определением степени правомерности со стороны гражданина. Последняя имеет свою противоречивость, проявляемую в соотношении субъекта его применяющего и/ или к которому оно применяется. В рамках социального взаимодействия происходит трансформация у субъекта его идентичности [Жукова, Жуков,

2014: Казаков, 2017, Гаврилов, Гаврилов, Грицкевич, Жукова, Казаков, 2020] в рамках его социокультурной ментальности и правовой нормативности [Степанцова, 2014]. В этом случае, добавляется морально-нравственный аспект, возникающий «в рамках постчеловеческой морали: (пост)человеческого достоинства, моральной зоосолидарности, морального биоусиления» [Девятко, Катерный, Кирилина, Перов, Семенов, Соколов, Черныш, 2021, С. 32]. Более того, «личное поведение в цифровой реальности оказывается фактором оценки профессиональной деятельности, что далеко не всегда этически обосновано. Возникающие моральные проблемы требуют нормативного регулирования, зафиксированного в этических кодексах, особенно в плане профессиональной этической защиты от морально негативных явлений, которые свойственны активности деперсонифицированного «цифрового субъекта» [Девятко, Катерный, Кирилина, Перов, Семенов, Соколов, Черныш, 2021, С. 34].

Признавая, что «цифра на самом деле – это не математический нуль – это ничто, ничто человеческой пустоты, которое стремится в ней спрятать свое ничтожество» [Варава, 2021], происходит трансформация человеческого сознания [Zolotukhin, Zhukova, 2017; Zhukova, Zhukov, Zolotukhin, Kazakov, 2019] не только на индивидуальном, но и коллективном уровнях. Данный аспект, на его уровне осознания противоречив, более того «коммуникации человека, владеющего цифровыми технологиями и создающего фактически новое культурное пространство, осознаются им весьма слабо» [Ярославцева, 2020].

С увеличением каналов распространения информации, необходима адаптация человека «к новой технологической реальности» для выстраивания собственной безопасности, поскольку, по мнению «Юрия Жданова, важной проблемой цифровизации является недостоверная информация и распространение порочащих личность сведений. «Исследования показывают, что последствия так называемой «цифровой ненависти» наносят не

меньший урон, чем реальные преступлений» [Татьяна, 2022]. При этом, приходится констатировать тот факт, что «инвестиции в обновление навыков в России не только очень малы, но еще и быстро сокращаются. Скажем, вероятность переобучения работника в возрасте 50–59 лет в Скандинавских странах – выше 50 процентов, в России – не выше 10 процентов, причем львиную долю переобучающихся составляют врачи и учителя, от которых требуют прохождения соответствующих курсов, тренингов и т.д.» [Штраф, 2022].

Существуют угрозы противоправного использования цифровизации не только против отдельного субъекта, но и коллектива (социальная группа, класс, государство), что является показателем качества жизни, дифференциации уровня образования и смертности, зависящих от таких факторов как «доход (связанный, в свою очередь, с расходами на здравоохранение) и размер населенного пункта (связанный, в свою очередь, с доступностью медицинских учреждений)» [Щур, 2022]. На индивидуальном уровне, это связано с ложными отношениями «Я» и «себя» выявляются в проблеме акразии (несдержанности – отсутствия у человека способности в действиях воплощать собственное правильное знание), замеченной еще Аристотелем и не потерявшей актуальности до наших дней)» [Кожевникова, 2021]. С точки зрения государственных образований это обусловлено как наднациональным, так и внутринациональным характером, например Соцсети, для которых «нет никаких регулирующих положений, позволяющих выстраивать внутреннюю стратегию, международную стратегию» [Объединяя, 2021, С. 27]. Также, примером проявлением дискриминации может «служить привлечение Красного Креста к осуществлению этнически избирательных мероприятий в отношении цыган в Италии. Впрочем, гораздо более распространенная практика – сотрудничество правоохранительных органов с частными коммерческими организациями» [Григорьева, 2020]. Риск манипуляции субъектом связан с тем, что «основа любого искусст-

венного интеллекта и робототехники – это программное обеспечение, которое создает риски неправомерного доступа к нему с помощью вредоносных программ» [Грачева, Маликов, Чучаев, 2020, С. 203].

В рамках повседневной практики, а также правоприменения [Zolotukhin, Bikmetov, Shiller, Tarasenko, 2021], отмечается, что «аналитика инцидентов внутренней безопасности по отраслям, среди которых отмечаются следующие направления: попытки откатов (здравоохранение – 44%, ритейл – 42%, логистическая сфера – 41%, промышленность – 40%,строительство–38%, сфера ИТ – 30%) и промышленного шпионажа/работы в пользу конкурентов (ритейл – 39%, строительство – 43%, промышленность – 37%)» [Глухов, Наседкин, 2021, С. 38]. В конечном итоге это характеризует несбалансированные и противоречивые способы внедрения и использования цифровых технологий в современном мире, влияющих на мировоззренческую самоидентификацию человека и социума в целом.

Библиографический список

Варава В. Danse macabre человека цифровой эпохи. // Новый мир, 2021. № 3. С. 96. [Электронный ресурс] Режим доступа – URL http://www.nm1925.ru/Archive/Journal6_2021_3/Content/Publication6_7705/Default.aspx (дата обращения 22.01.2022 г.).

Гаврилов О. Ф., Гаврилов Е. О., Грицкевич Т. И., Жукова О. И., Казаков Е. Ф. Модусы социального взаимодействия: концепты идентичности духовного опыта, общественных преобразований. коллективная монография / Кемеровский государственный университет. – Кемерово, 2020.

Гейхман Л. К., Ставцева И. В. Межкультурная коммуникация: реальное и виртуальное // Труды Санкт-Петербургск. гос. ин-та культуры. 2016. Т. 214. С. 65–67.

Глухов Н. И., Наседкин П. Н. Аналитика внутренних угроз информационной безопасности предприятий // Доклады ТУСУР. – 2021. – Т. 24, № 1. – С. 33–41. DOI: 10.21293/1818-0442-2021-24-1-33-41.

Грачева Ю. В., Маликов С. В., Чучаев А. И. Предупреждение девиаций в цифровом мире уголовно-правовыми средствами // Право. Журнал Высшей школы экономики, 2020. – № 1. – С. 188–210.

Григорьева К. С. Этнически избирательный контроль: дисфункция правоохранительной системы или социальный институт?. The Journal of Social Policy Studies, 2020 – № 18 (2). – 299– 312. https://doi.org/10.17323/727-0634-2020-18-2-299-312

Грунвальд А., Ефременко Д. В. Цифровая трансформация и социальная оценка техники. // Философия науки и техники. 2021. Т. 26. № 2. С. 36–51. DOI: https://doi.org/10.21146/2413-9084-2021-26-2-36-51

Девятко И. Ф., Катерный И. В., Кирилина Т. Ю., Перов В. Ю., Семенов Е. В., Соколов В. М., Черныш М. Ф. Нравственность, мораль, этика: что происходит в теории и социальной практике? (круглый стол) // Социологические исследования. 2021. № 3. С. 28-43. DOI: 10.31857/S013216250014275-5.

Егошин Н. С. Модель типовых угроз безопасности информации, основанная на модели информационных потоков // Доклады ТУСУР. – 2021. – Т. 24. – № 3. – С. 21–25. DOI: 10.21293/1818-0442-2021-24-3-21-25.

Жукова О. И., Жуков В. Д. Кризис идентичности как нормообразующее становление личности. // Вестник Кемеровского государственного университета культуры и искусств, 2014. – № 29-1. С. 81–88.

Золотухин В. М. Социально-философский и культурологический аспекты экономического поведения в российской ментальности. // Вестник КемГУКИ, 2018. – № 43. – С. 36–42.

Золотухин В. М., Семина Д. И., Семина М. И. Социокультурный и аксиологический аспекты экономического поведения человека и реализация его потребностей // Вестник Кемеровского государственного университета. Серия: Гуманитарные и общественные науки. 2020. – Т. 4. – № 1. – С. 47–52. DOI: https://doi.org/10.21603/2542-1840-2020-4-1-47-52

Казаков Е. Ф. Идеальный человек и кризис идентичности. // Идеи и идеалы. 2017. – Т. 1. – № 4 (34). – С. 40–48.

Кожевникова М. Н. Феномен самообмана и проблемы человеческой зрелости. // Человек, 2021. – Т. 32. – № 4. – С. 132–148. DOI 10.31857/S023620070016691-7.

Лешкевич Т. Г. Ценностно-целевые регулятивы и эмерджентность: экзистенциальная проекция в цифровом мире. // Философия науки и техники, 2020. – Т. 25. – № 2. – С. 131–144.

Объединяя усилия во имя развития. Международное сотрудничество. // Roscongress Аналитический обзор. RC INSIDER, 2021. – С. 22–27.

Пишняк А. Халина Н. Восприятие новых технологий населением как показатель открытости к инновациям. // ФОРСАЙТ. 2021. – Т. 15 – № 1. – С. 39–54. DOI: 10.17323/2500-2597.2021.1.39.54.

Попова А. В. Цифровая социализация, теговое мышление и современный образовательный процесс в государственно правовом измерении России. // Правовое государство: теория и практика, 2021. – № 1 (63). – С. 50–69. DOI 10.33184/pravgos-2021.1.4.

Пржиленский В.И. Понятие цифровой реальности: значение и смысл // Философия науки и техники. 2021. – Т. 26. – № 2. – С. 68–80. DOI: 10.21146/2413-9084-2021-26-2-68

Степанцова Е. В. Социально-философский аспект правовых норм и их влияние на общественное согласие. // Вестник Челябинского государственного университета, 2009. – № 42 (180). – С. 148–151.

Татьяна Москалькова рассказала о плюсах и минусах цифровой эпохи на примере России. 13 января 2022 [Электронный ресурс] Режим доступа – URL https://ombudsmanrf.org/news/novosti_upolnomochennogo/view/tatjana_moskalkova_rasskazala_o_pljusakh_i_minusakh_cifrovoj_epokhi_na_primere_rossii (дата обращения 27.01.2022 г.).

Фатенков А. Культ безопасности как тоталитарная угроза // Философская антропология. 2021. – Т. 7. – № 2. – С. 104–109.

«Штраф за возраст» Директор Центра трудовых исследований НИУ ВШЭ Владимир Гимпельсон – о парадоксах отечественного рынка труда. // Огонёк" № 2 от 25.01.2021, стр. 8. [Электронный ресурс] Режим доступа – URL: https://www.kommersant.ru/doc/4640417 (дата обращения 27.01.2022 г.).

Щур А. Различия в ожидаемой продолжительности жизни по типам поселений России. // Население и общество. 2022. – №1 (106). [Электронный ресурс] Режим доступа – URL: http://www.demoscope.ru/weekly/2022/0929/population_and_society02.php (дата обращения 27.01.2022 г.).

Ярославцева Е. Потенциал цифровых технологий и проблемы творчества человека. // Вопросы философии, 2020. – Т. № 11. – С. 58–66. DOI: https://doi.org/10.21146/0042-8744-2020-11-58-66.

Zolotukhin V.M., Bikmetov R.S., Shiller V.V., Tarasenko A.A. Sociocultural aspect of criminal lam enforcement the russian mentality . Rudn conference on legal theory, methodology and regulatory practice (RUDN LTMRP conference 2021/ SHS Web of Conferences (см. в книгах). 2021. № 118. С. 02009.

Zolotukhin V. M., Zhukova O. I. Problem of relations between human and society in conditions of social transformations: RPTSS 2017 Intern. Conf. on Research Paradigsm Transformation in Social Sciences.

Zhukova O. I., Zhukov V. D., Zolotukhin V. M., Kazakov E. F. The problem of the impact of information on consciousness and human Identity. / 11 th International Scientific and Theoretical Conference – Communicative Strategies of Information Society Editors: Olga D. Shipunova, Violetta N. Volkova, Alfred Nordmann, Laurent Moccozet. 2019. С. 420-429.

V. M. Zolotukhin, M. V. Zolotukhin
T.F. Gorbachev Kuzbass State Technical University, Kemerovo, Russia
Tomsk State University of Control Systems and Radio Electronics
Tomsk, Russia

PROBLEMS OF DIGITAL SECURITY IN THE CONTEXT OF TECHNOLOGY DEVELOPMENT

The article discusses the problems of digital security, including those related to the forced transition to remote work. It is emphasized that both positive and negative aspects are associated with the processes of expanding the digital space, socio-economic risks arise, and human consciousness and behavior are transformed. It is emphasized that this is due to the level of trust in state institutions, the socio-cultural relevance, their functional need for digital technologies. The increase in technological channels of information dissemination requires human adaptation to digital reality, which entails the search for ways and mechanisms to ensure human security and identity in the real world.

Keywords: information, information security, trust, consciousness, socio-cultural environment, cyber risks, digital space.