

УДК 101.1.304.44

*М. Д. Мартынова**Национальный исследовательский Мордовский государственный университет
им. Н. П. Огарёва (Саранск, Россия), e-mail: martynovamd@mail.ru*

«Цифровое доверие» vs «недоверие» в формировании социальных отношений и практик глокального общества

Введение. Применение индивидом наработанных социальных практик в цифровой среде сталкивается с определенными трудностями, вызванными широкими возможностями «честного» и «нечестного» поведения в интернете. Высокий уровень доверия к цифровым технологиям и возможность манипулирования личными данными, стремление опираться на «экспертное мнение» и недостоверная информация, социальная потребность общения и иллюзия общения в социальных сетях, а также прочие дилеммы взаимоотношений в цифровом мире и оперировании большими данными (Big Data) создают ощущение неуверенности, неустойчивости и разобщенности в восприятии цифровой действительности. Цель статьи – выявление социального и этического аспектов феномена доверия как установки сознания, препятствий для цифрового доверия и определения путей его наработки. **Материалы и методы.** Междисциплинарный подход, опирающийся на этику в сфере информационных технологий, социологию, теорию коммуникации, позволяет проанализировать становление новых социальных практик и интерпретировать развитие ценностного отношения личности к новым реалиям жизни. **Результаты исследования.** Выявлены следующие сферы актуализации концепта «доверие» в цифровом мире: доверие к цифре и алгоритмам, доверие к «цифровому субъекту», «интернет доверия» как пространство обязательств и правил. Формирование «интернета доверия» сопряжено с осознанием всех социальных и морально-психологических проблем, связанных с процессом сочетания онлайн- и офлайн-среды в социальной практике индивида, где следует найти новые формы применения традиционных стандартов поведения. **Обсуждение и заключение.** Откладывание индивидом «на потом» рационального анализа рисков цифрового взаимодействия провоцирует создание критических для благополучия и безопасности индивида ситуаций. Издержками цифрового доверия выступают снижение безопасности и создание «ловушек» в общественных отношениях и социальных практиках. Цифровая среда создает ситуацию уязвимости индивида, что побуждает его прибегать к возможным мерам защиты. В свою очередь для эффективного функционирования и дальнейшего развития общества совершенно необходим «интернет доверия» как новая цифровая реальность.

Ключевые слова: цифровое доверие, социальные практики, «интернет доверия», конфиденциальность, автономия.

Для цитирования: Мартынова М. Д. «Цифровое доверие» vs «недоверие» в формировании социальных отношений и практик глокального общества // Гуманитарий : актуальные проблемы гуманитарной науки и образования. – 2020. – Т. 20. – № 4. – С. 445–453. DOI: 10.15507/2078-9823.52.020.202004.445-453.

Благодарность: Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-011-00710.

© Мартынова М. Д., 2020

“Digital trust” vs “Distrust” in the Formation of Social Relations and Practices of Glocal Society

Introduction. The individual’s application of established social practices in the digital environment faces certain difficulties caused by the wide opportunities for “honest” and “dishonest” behavior on the Internet. The high level of trust in digital technologies and the possibility of manipulating personal data, the desire to rely on “expert opinion” and unreliable information, the social need for communication and the illusion of communication in social networks, as well as other dilemmas of relationships in the digital world and operating with big data create a sense of uncertainty, instability and disunity in the perception of digital reality. The purpose of the article is to identify social and ethical aspects of trust phenomenon as an attitude of consciousness, obstacles to digital trust and identify ways to develop it. **Materials and Methods.** The interdisciplinary approach based on ethics of information technology, sociology, and communication theory allows us to analyze the formation of new social practices and interpret the development of a person’s value attitude to new realities of life. **Research result.** The following areas of actualization of the concept of “trust” in the digital world are identified as trust in data and algorithms, trust in “digital subject”, “Internet of trust” as a space of obligations and rules. The formation of the “Internet of trust” is associated with awareness of all social, moral and psychological problems associated with the process of combining online and offline environments in the social practice of an individual, where new forms of applying traditional standards of behavior should be found. **Discussion and Conclusion.** Postponing the rational risk analysis of digital interaction by an individual “for later” provokes the creation of situations that are critical for the individual’s well-being and security. The costs of digital trust are reduced security and creation of “traps” in public relations and social practices. Digital environment creates a situation of vulnerability of an individual, which encourages him to resort to possible measures of protection. In turn, the “Internet of trust” as a new digital reality is absolutely necessary for the effective functioning and further development of society.

Keywords: digital trust, social practices, Internet of trust, privacy, autonomy.

For citation: Martynova M. D. “Digital trust” vs “Distrust” in the Formation of Social Relations and Practices of Glocal Society. *Gumanitarian : aktual'nye problemy gumanitarnoi nauki i obrazovaniia* = Russian Journal of the Humanities. 2020; 20(4): 445–453 (In Russ.). DOI: 10.15507/2078-9823.052.020.202003.445-453.

Acknowledgements: This work was supported by the Russian Foundation for Basic Research, project No. 18-011-00710.

Введение

Стремительная цифровая трансформация всех сфер экономики создает новую экономическую и социальную среду современной жизни глобального общества. Несмотря на то что для молодежи цифровая среда вполне привычна, они родились «с кнопкой на пальце», риски и вызовы цифрового мира требуют иных социальных практик самоопределения и самоутверждения. Период изолированной жизни во время пандемии коронавируса показал, что особой проблемой для студентов при

переходе на дистанционный режим является психологическая адаптация к новым условиям. Умея выстраивать дружеские отношения и досуг онлайн, они оказались не готовы учиться онлайн, и дело здесь не только в самоорганизации.

Проблема формирования новых социальных практик в цифровом формате имеет глобальный характер локального приложения, поскольку форматы использования цифровых сервисов одинаковы во всем мире, а, например, способы сочетания двух сред – офлайн и онлайн, – безусловно, имеют

культурную специфику. Морально-психологическая готовность индивида к опоре на привычные этические правила взаимодействия в цифровой среде нередко сталкивается с определенными рисками, что формирует новый концепт «цифровое доверие». Он актуализируется в ситуациях наличия высокого уровня доверия к цифровым технологиям и характеризуется открытостью личных данных, а также широкой возможностью манипулировать этими данными. Стремление опираться на «экспертное мнение» сталкивается с недостоверностью информации, размещенной в интернете, а базовая социальная потребность общения – с иллюзией общения в социальных сетях и т. п.

Проблема цифрового доверия в первую очередь обсуждается применительно к правовому регулированию среды благополучного развития цифровых технологий в экономической сфере, безопасности ведения бизнеса в цифровом формате. Бизнес значительно зависит от поведения пользователей, их реакции на цифровую среду и отношения к ней. Цифровое доверие пользователя зависит от безопасности цифровых технологий, их надежности и обеспечения конфиденциальности личных данных. Джим Харлей выделяет условия цифрового доверия: удобство, опыт пользователя, репутация, прозрачность и целостность¹. В свою очередь Дж. Веккерт считает, что доверие пользователя в электронной среде основано не на рациональных соображениях, а на склонности видеть других агентов как заслуживающих доверия. В этом случае рациональная оценка рисков откладывается, пользователь будет оценивать результаты выбора на втором этапе. Если окажется, что виртуальная среда благоприятствует положительным результатам, возникнет подлинное доверие, основанное на убеждениях доверителя [18]. Соци-

альные и морально-психологические риски в отношении цифрового доверия у пользователей связаны с размытостью границ ответственности за конфиденциальность данных и опасностью последствий снижения защиты данных [5]. По мнению Л. Флориди, цифровое доверие определяет «цифровое благополучие» человека в разных сферах его жизни, на которые существенное влияние оказывают цифровые технологии [6]. Быстрое внедрение цифровых технологий в практику нашей жизнедеятельности изменило наши отношения с самими собой, друг с другом и с окружающей средой. В результате наше индивидуальное и социальное благополучие теперь тесно связано с состоянием нашей информационной среды и цифровых технологий, опосредующих наше взаимодействие с ней, что ставит насущные этические вопросы, касающиеся влияния цифровых технологий на наше благополучие [8]. Еще одной актуальной сферой анализа чувства доверия является отношение к искусственному интеллекту [14].

Методы

Нужно отметить, что в исследовательской литературе вопросы цифрового доверия обсуждаются применительно к принципам формирования отношений между компаниями, партнерами и клиентами, а также отношения пользователя к искусственному интеллекту. Нас же интересуют процессы формирования социальных практик и морально-психологический аспект проявления доверия к цифровому миру. Поэтому целью исследования является проведение сравнительного анализа различных точек зрения на концепт «цифровое доверие», выявление социального и этического аспектов феномена доверия как установки сознания, препятствий для цифрового доверия и определения путей его наработки.

¹ С надеждой всматриваясь вдаль. Российский выпуск 20-го опроса руководителей крупнейших компаний мира [Электронный ресурс]. – URL: <https://www.pwc.ru/ru/ceo-survey/20th-ceo-survey.pdf>.

Междисциплинарный подход, опирающийся на этику в сфере информационных технологий, социологию, теорию коммуникации, позволяет проанализировать становление новых социальных практик и интерпретировать развитие ценностного отношения личности к новым реалиям жизни.

Результаты

Концепт «доверие» в цифровом мире применим в следующих сферах: доверие к цифре и алгоритмам, доверие к «цифровому субъекту», «интернет доверия» как пространство обязательств и правил. Каждый из аспектов имеет свой масштаб проблем. Доверие к цифре связано с возможностью манипулирования персональными данными, начиная от платежных систем и заканчивая медицинскими данными, что требует безусловной конфиденциальности. Доверие к «цифровому субъекту» проявляется в процессе виртуальной коммуникации с индивидом. «Интернет доверия» – идеальный образ безопасного цифрового пространства, где соблюдаются договоренности и правила взаимодействия. Формирование «интернета доверия» сопряжено с осознанием всех социальных и морально-психологических проблем, связанных с процессом сочетания онлайн- и офлайн-среды в социальной практике индивида, где следует найти новые формы применения традиционных стандартов поведения. Новое поколение профессионалов работает с «неживыми» IT-процессами и большими данными (Big Data), за которыми стоят живые люди со своими проблемами, страхами, интересами; люди, которые могут понести значительный моральный, психологический, финансовый ущерб при некорректном обращении с цифровыми данными.

Обсуждение

Толковые словари русского языка обозначают социальную природу слова «доверие», делая акцент на добровольных взаимных обязательствах людей (С. И. Ожегов). Здесь очевидны глубокие моральные и

психологические основания этой установки сознания, которая появляется только при наличии одинаковых ценностей у взаимодействующих сторон. Необходимость доверия возникает в ситуации уязвимости и неопределенности, требует от индивида открытости другим людям, стремления опереться на авторитет, что было достаточно подробно проанализировано в трудах выдающихся психологов: С. Л. Франка, Р. Б. Шо, Э. Эриксона [1; 3; 4] – и многих других исследователей. Оно опирается на уверенность личности в порядочности и добросовестности другого субъекта взаимодействия, имеет аффективное, нормативное и рациональное основания [14]. Рациональная парадигма доверия опирается на логический выбор, стоит ли доверять другому человеку [12]. Аффективное отношение опирается на добрую волю того, кому доверяют, и сопровождается нашими ожиданиями благосклонности [9]. Нормативное измерение доверия опирается на должностное и сложившиеся правила взаимоотношений [11]. Проводя философское исследование доверия, Е. Кимолен отмечает, что цифровая среда изменила характер доверия, которое сегодня уже не основано на межличностных взаимодействиях, а полностью опосредовано технологиями [10].

Каким же образом интенция доверия реализуется в цифровом мире? Цифровое доверие – это концепция, определяющая уверенность в надежности всех компонентов цифрового взаимодействия: пользователей, процессов, устройств, технологий. Доверие цифре выбирается как наиболее простой и легкий путь поиска достоверной информации при помощи алгоритма Google. Мы больше не ищем информацию – мы «гуглим». Привычка надеяться на Google нивелирует способность человека к самостоятельному поиску информации. Показательна ситуация со студентами, которые не приучены к тщательному поиску

достоверной информации, полагаются на верхние строки поисковой выдачи Google и бессмысленно выдают исследовательские работы – курсовые и дипломные, которые так и не сформировали у них исследовательские навыки, необходимые в профессиональной деятельности.

Одна из ключевых проблем, связанная с доверием в цифровом мире, – необходимость сохранения конфиденциальности. Здесь выделяются несколько разноплановых аспектов: конфиденциальность информации, анонимность, наблюдение (слежение, пириновый надзор), автономия, дискриминация и некорректное использование информации. Исследователи подчеркивают, что дилемма доверия и конфиденциальности основана на ущемлении свободы человека, поскольку алгоритмические системы поддержки принятия решений посягают на ее ограничение [7; 8]. Самой очевидной провокацией для морального сознания индивида является система автоматизированного принятия решений. Социальные сети знают, какой контент нам подходит, чем мы интересуемся, и предлагают соответствующие источники в интернете. Достаточное количество информации и достаточная вычислительная мощность позволяют внешним системам обработки данных узнать все о наших желаниях, решениях и мнениях. Все, чем мы интересуемся в интернете, является предметом изучения алгоритмов, что позволяет им делать заключение о наших пристрастиях и потребностях и манипулировать потребительским поведением.

Алгоритмы контроля сопряжены с режимом тотальной слежки, который не только контролирует наши действия и высказывания, но и способен следить за нашими внутренними ощущениями и понимать чувства человека гораздо лучше, чем

он сам. Такие алгоритмы больших данных появились вследствие слияния двух масштабных революций – биотехнологической и информационной. Ю. Н. Харари прогнозирует, что в скором времени лечение, подбор медикаментов, рекомендации в выборе супруга и многое другое будут основаны на алгоритме больших данных, что сведет на нет свободу воли и позволит манипулировать внутренним миром человека [2, с. 76].

Проблема недоверия возникает в результате манипуляций с большими данными. Неоднократны случаи дискриминации как результат решений, принимаемых алгоритмами, в частности, по этнической принадлежности, полу или социальному статусу. Причиной дискриминации являются данные, загружаемые в DSS (Decision Support System – системы поддержки принятия решений), которые принимают решения. Так, например, в 2018 г. алгоритм набора персонала Amazon, настроенный на поиск людей, преуспевающих в компании, ввел данные на отмену выбора женских резюме². Такие примеры легли в основу панельной дискуссии «Цифровая этика – подавляют ли нас алгоритмы?» во время Берлинской недели науки в 2018 г.

Ввод корректных данных и методологическая точность исследований, осуществляемых на основе больших данных, зависят от специалистов, работающих с алгоритмами и несущих индивидуальную ответственность за потенциальную возможность дискриминации. Вследствие этого в некоторых странах предмет этики включен в университетское образование, в первую очередь в области естественных наук и инженерии, с целью изучения потенциальных этических последствий решений при разработке автоматизированных DSS.

Люди стремятся к анонимности, но постоянно растет число социальных отноше-

² Нейросеть Amazon для поиска сотрудников научилась сексизму и была закрыта [Электронный ресурс]. – URL: https://infostart.ru/journal/news/biznes/neyroset-amazon-dlya-poiska-sotrudnikov-nauchilas-seksizmu-i-byla-zakryta_922089/.

ний и практик, которые становятся источниками данных. Индивидам все труднее оставаться неидентифицируемыми, поскольку все большее число битов неидентифицированной информации может быть прикреплено к конкретному человеку с помощью кратковременного поиска и анализа. П. М. Реган, Дж. Джиси, Л. Свини и многие другие исследователи обеспокоены тем обстоятельством, что с большими данными анонимность информации о людях становится более сложной, если не невозможной, поскольку осуществляется постоянное пересохранение информации [13; 16], что делает возможным поиск информации при объединении одной базы данных с другими базами данных при использовании сложных алгоритмов.

Еще один аспект, который вызывает недоверие пользователя, состоит в том, что сбор информации об индивиде должен осуществляться с учетом его знаний и объем информации должен быть минимальным и соответствующим цели, для которой он был собран. При этом в рамках принципов справедливой информационной практики следует соблюдать уведомление, согласие, выбор и прозрачность сбора информации. На этом основаны законы о конфиденциальности и защите данных во всем мире. В случае с большими данными происходит гораздо больший сбор информации, нежели необходимо, о большем количестве аспектов жизни человека вследствие того, что она собирается из большого количества источников и без ведома человека. Если в интернете вещей покупатель может делать выбор, соглашаясь с Политикой конфиденциальности, то в сфере образования, например при сборе и использовании больших данных, вопросы уведомления, выбора, согласия и прозрачности усложняются, поскольку учет достижений обучающихся

является обязательным (цифровой след обучающегося) и исключает реальный выбор.

Угрозой доверию пользователей выступает так называемый пиринговый надзор, который включает как мониторинг деятельности индивида, так и анализ этой деятельности для определения вероятностных будущих действий. В ряде случаев это необходимо с точки зрения государственной безопасности (отслеживания сайтов экстремистской направленности). В случае масштабного применения автономия индивида подвергается манипулированию со стороны больших данных, а именно возможность управлять своей жизнью в соответствии со своими предпочтениями. Алгоритмы больших данных интернета вещей заставляют людей покупать определенные товары, выбирать определенные маршруты или рестораны. Персонализированные системы обучения так же манипулятивны, поскольку, как подчеркивает К. Н. Санстейн, пытаются апеллировать к индивидуальным способностям рефлексивного и осознанного выбора [15].

Издержками цифрового доверия выступают не только снижение безопасности, но и глубинные процессы, лежащие в основе общественных отношений и социальных практик. Цифровая среда создает ситуацию уязвимости индивида, что побуждает его прибегать к возможным мерам защиты. Например, авторизация на том или ином сайте. Отмечены случаи, что пользователи все реже указывают личную информацию при заполнении профиля. Так, например, администраторы Платформы Leader-ID отмечают, что таких большинство: данные в профиле открыты только у 23 тыс. из 750 тыс. Это всего 3 % пользователей. При этом 93 % участников готовы дать свой контакт по прямому запросу, если к ним обращается коллега или человек, с которым они были на одном мероприятии³.

³ Помню, что сидели в одном ряду [Электронный ресурс] / Платформа Leader-ID. – URL: https://leader-id.ru/?utm_source=newsletter&utm_medium=email&utm_campaign=Noyabr%27+glazami+Leader-ID.+Nachalo_6244.

Проблема интернет-доверия является широко обсуждаемой на международных форумах, поскольку проблемы кибербезопасности и фейковые новости углубляют недоверие между людьми. На Форуме по управлению интернетом The Internet of Trust (Франция, 12–14 ноября 2018 г.) Генеральный секретарь ООН А. Гутерриш обозначил такие глобальные проблемы интернета, как проблемы цифрового разрыва, влияние на человечество искусственного интеллекта и передовых технологий, кибербезопасность, гендерное равенство, последствия для устойчивого развития, и как цифровое будущее обеспечивает наши права человека, и меры, которые смогут обеспечить «интернет доверия».

Доверие к «цифровому субъекту» формируется в процессе коммуникации с индивидом, в первую очередь в социальных сетях. Все цифровые следы человека: посты, репосты, лайки, комментарии, выложенные фотографии и т. д. – складываются в «цифровой портрет» личности. Модель цифрового человека как новый культурно-антропологический вид обладает ценностями, практиками, требованиями к миру и особым набором качеств и компетенций, позволяющих выживать и быть эффективным в цифровой среде.

Общепризнано, что оцифровка меняет все аспекты человеческой жизни. Это изменение начинается с восприятия человеком самого себя как субъекта, существующего большую часть времени онлайн, чем офлайн. Это иного рода субъективация, или самопонимание, связанное с автономией человека. Р. Капурро пишет, что современный субъект встроен в глобальную сеть сетевых объектов [7]. В наше время быть человеком означает быть-в-сетевом-мире в подавляющем большинстве случаев. Сетевые объекты отличаются от объектов во внешнем мире. Простой пример: интернет вещей демонстрирует не совсем то качество продукта, нежели человек его получает в руки. Так же

и сетевой человек – человек в Сети – отличается от автономного индивида. Поведенческие реакции в Сети, самопроявление и самопрезентация обусловлены параметрами и возможностями сетевого мира.

Дополненная и виртуальная реальности становятся регулярными средами для социального взаимодействия, в результате возникает так называемое «бесшовное» смешение онлайн-информации с офлайн-реальностью. Новая привычка обычных людей отслеживать друг друга сочетается с социально-сетевыми инструментами для самопрезентации и формирования онлайн-имиджа. Интернет-пользователи учатся оптимизировать свою онлайн-личность, чтобы получить самую положительную обратную связь и избежать отрицательной обратной связи через серию проб и ошибок [17]. Человек «оптимизирует» себя в интернете, представляя себя симпатичным, одобренным членом толпы, у которого есть те же мысли, чувства, мнения, интересы и поведение, что и у других, и скрывает любые склонности, которые могут доказать обратное. Фактически происходят симуляция отношений и утрата доверия между пользователями. Реальная коммуникация продолжает оставаться значимой, признается и ценность виртуального Другого, взаимодействие с которым имеет свои правила.

Заключение

Цифровое доверие стало одной из стандартных установок сознания личности, лежащее в основе новых поведенческих стереотипов применительно к цифровой среде. Оно играет большую роль для благополучного самоосуществления индивидуума вследствие той доли времени, которое он уделяет цифровому пространству. Потребность в безопасности требует формирования новых социальных практик и паттернов поведения в Сети. Это непросто, поскольку новая среда дает новые расширенные возможности, которые часто производят неожиданный эффект.

Библиографический список

1. Франк С. Л. Духовные основы общества : сборник / сост. и авт. вступ. ст. П. В. Алексеев. – М. : Республика, 1992. – 510 с.
2. Харари Ю. Н. 21 урок для XXI века. – М. : Синдбад, 2019. – 416 с.
3. Шо Р. Б. Ключи к доверию в организации: Результативность. Порядочность. Проявление заботы : пер. с англ. – М. : Акад. нар. хоз-ва при Правительстве Рос. Федерации : Дело, 2000. – 271 с.
4. Эриксон Э. Идентичность: юность и кризис : пер. с англ. / общ. ред. и предисл. А. В. Толстых. – М. : Прогресс, 1996. – 340 с.
5. Abraham Ch., Sims R. R., Daultrey S., Buff A., Fealey A. How Digital Trust Drives Culture Change [Electronic resource]. – URL: <https://sloanreview.mit.edu/article/how-digital-trust-drives-culture-change>.
6. Burr Ch., Taddeo M., Floridi L. The Ethics of Digital Well-Being: A Thematic Review // Science and Engineering Ethics. – 2020. – Vol. 26. – P. 2313–2343.
7. Capurro R. Digitization as an Ethical Challenge. // AI & Society. – 2017. – Vol. 32. – P. 277–283.
8. Floridi L. The Onlife Initiative. The Onlife Manifesto [Electronic resource] // Floridi L. (eds). The Onlife Manifesto. – URL: https://doi.org/10.1007/978-3-319-04093-6_2.
9. Jones K. Trust as an affective attitude // Ethics. – 1996. – Vol. 107 (1). – P. 4–25.
10. Keymolen E. Trust on the line: A philosophical exploration of trust in the networked era. – Amsterdam : Wolf Legal Publishers, 2016. – 286 p.
11. McLeod C. Trust [Electronic resource] // The Stanford Encyclopedia of philosophy / ed. by Edward N. Zalta. – Metaphysics Research Lab, Stanford University, 2015. – URL: <https://plato.stanford.edu/archives/fall2015/entries/rust/>.
12. Mollering G. Trust: Reason, routine, reflexivity (1st ed.). – Bingley : Emerald Group Publishing Limited, 2006.
13. Regan P. M., Jesse J. Ethical challenges of edtech, big data and personalized learning: twenty-first century student sorting and tracking [Electronic resource] // Ethics and Information Technology. – 2019. – Vol. 21. – P. 167–179. – URL: <https://doi.org/10.1007/s10676-018-9492-2>.
14. Ryan M. In AI We Trust: Ethics, Artificial Intelligence, and Reliability [Electronic resource] // Science and Engineering Ethics. – 2020. – URL: <https://doi.org/10.1007/s11948-020-00228-y>.
15. Sunstein C. R. The ethics of nudging // Yale Journal on Regulation. – 2015. – Vol. 32 (2). – P. 413–450.
16. Sweeney L. Uniqueness of simple demographics in the US population (Laboratory for International Data Privacy, Working Paper LIDAP-WP4), 2000 [Electronic resource]. – URL: <http://dataprivacylab.org/projects/identifiability/index.html>.
17. Valkenburg P. M., Peter J., Schouten A. P. Friend networking sites and their relationship to adolescents' well-being and social self-esteem // Cyberpsychology & Behavior. – 2006. – Vol. 9 (5). – P. 584–590.
18. Weckert J. Trust in Cyberspace // Cavalier R. J. (ed.). The Impact of the Internet on Our Moral Lives. – Albany : University of New York Press, 2005. – P. 95–120.

References

1. Frank S. L. Spiritual foundations of society. Moscow, 1992, 510 p. (In Russ.).
2. Harari Yu. N. 21 lessons for the 21st century. Moscow, 2019, 416 p. (In Russ.).
3. SHO R. B. Keys to trust in an organization: Performance. Decency. Showing concern. Moscow, 2000, 271 p. (In Russ.).
4. Erikson E. Identity: youth and crisis. Moscow, 1996, 340 p. (In Russ.).
5. Abraham Ch., Sims R. R., Daultrey S., Buff A., Fealey A. How Digital Trust Drives Culture Change. <https://sloanreview.mit.edu/article/how-digital-trust-drives-culture-change>. (In Eng.).
6. Burr Ch, Taddeo M., Floridi L. The Ethics of Digital Well-Being: A Thematic Review. Science and Engineering Ethics. 2020; 26: 2313–2343. (In Eng.).
7. Capurro R. Digitization as an Ethical Challenge. AI & Society. 2017; 32: 277–283. (In Eng.).

8. *Floridi L.* The Onlife Initiative. The Onlife Manifesto. In: Floridi L. (eds). The Onlife Manifesto. Springer, Cham. 2015. https://doi.org/10.1007/978-3-319-04093-6_2. (In Eng.).
9. *Jones K.* Trust as an affective attitude. *Ethics*. 1996; 107(1): 4–25. (In Eng.).
10. *Keymolen E.* Trust on the line: A philosophical exploration of trust in the networked era. Wolf Legal Publishers. 2016, 286 p. (In Eng.).
11. *McLeod C.* Trust. In: The Stanford Encyclopedia of philosophy, edited by Edward N. Zalta. Metaphysics Research Lab, Stanford University. 2015. <https://plato.stanford.edu/archives/fall2015/entries/rust/>. (In Eng.).
12. *Mollering G.* Trust: Reason, routine, reflexivity (1st ed.). Bingley: Emerald Group Publishing Limited, 2006. (In Eng.).
13. *Regan P. M., Jesse J.* Ethical challenges of edtech, big data and personalized learning: twenty-first century student sorting and tracking. *Ethics and Information Technology*. 2019; 21: 167–179. <https://doi.org/10.1007/s10676-018-9492-2>. (In Eng.).
14. *Ryan M.* In AI We Trust: Ethics, Artificial Intelligence, and Reliability. *Science and Engineering Ethics*. 2020. <https://doi.org/10.1007/s11948-020-00228-y>. (In Eng.).
15. *Sunstein C. R.* The ethics of nudging. *Yale Journal on Regulation*. 2015; 32(2): 413–450. (In Eng.).
16. *Sweeney L.* Uniqueness of simple demographics in the US population (Laboratory for International Data Privacy, Working Paper LIDAP-WP4). 2000. <http://dataprivacylab.org/projects/identifiability/index.html>. (In Eng.).
17. *Valkenburg P. M., Peter J., Schouten A. P.* Friend networking sites and their relationship to adolescents' well-being and social self-esteem. *Cyberpsychology & Behavior*. 2006; 9(5): 584–590. (In Eng.).
18. *Weckert J.* Trust in Cyberspace. In: R. J. Cavalier (Ed.), *The Impact of the Internet on Our Moral Lives*. Albany: University of New York Press, 2005: 95–120. (In Eng.).

Поступила 09.06.2020.

Сведения об авторе

Мартынова Марина Дмитриевна – кандидат философских наук, доцент кафедры философии Историко-социологического института ФГБОУ ВО «Национальный исследовательский Мордовский государственный университет им. Н. П. Огарёва» (Саранск, Россия). Сфера научных интересов: философия образования, этика, биоэтика, этика в сфере информационных технологий. Автор более 140 научных и учебно-методических публикаций. ORCID: <https://orcid.org/0000-0003-1244-9721>.

E-mail: martynovamd@mail.ru

Submitted 09.06.2020.

About the author

Marina D. Martynova – Candidate of Philosophy, Associate Professor, Philosophy Department, History and Sociology Institute, National Research Mordovian State University (Saransk, Russia). Research interests: philosophy of education, ethics, bioethics, ethics in the field of information technology. The author of more than 140 scientific and educational publications. ORCID: <https://orcid.org/0000-0003-1244-9721>.

E-mail: martynovamd@mail.ru