Ольга Дмитриевна Шипунова

доктор философских наук,
профессор кафедры общественных наук
Гуманитарного института Санкт-Петербургского
политехнического университета Петра Великого,
Санкт-Петербург, Россия;
e-mail: o_shipunova@mail.ru

Елена Геннадиевна Поздеева

кандидат социологических наук,
доцент Высшей школы медиакоммуникаций
и связей с общественностью
Гуманитарного института Санкт-Петербургского
политехнического университета Петра Великого,
Санкт-Петербург, Россия;
e-mail: elepozd@mail.ru

Проблема доверия к смарт-технологиям в цифровом обществе

УДК: 001.8; 316.422.44
DOI: 10.24412/2079-0910-2022-4-131-145

Рассматриваются философские аспекты технологической эволюции цифрового общества, определенные трансформациями человеко-компьютерных систем и отношений. Задачи статьи связаны с анализом уровней доверия общественности к перспективе развития смарт-технологий в социальных взаимодействиях. Проблема доверия смарт-технологиям явно обозначена перспективой замещения человека в профессиональной деятельности. При этом традиционные аспекты доверия между людьми, связанные с этическими установками, дополняются проблемами доверия к интеллектуальным технологиям и «умным» роботам, включенным в институциональные и когнитивные структуры жизненного мира. Исследование уровней доверия к цифровой среде и системам с искусственным интеллектом (ИИ) опирается на методы анализа и обобщения эмпирического материала, который содержится в обзорах ВЦИОМ, составленных по опросам различных возрастных групп граждан РФ и направленных на выявление характера отношений к перспективам внедрения технологий искусственного интеллекта в социальные и профессиональные сферы деятельности. В оценке уровня доверия цифровой среде использованы данные, полученные в результате онлайн-опроса в ноябре 2021 г. (140 респондентов, пользователей сети Интернет, преимущественно студентов и молодых специалистов). На этом основании выявлены социотехнические сфе-

ры с высоким уровнем доверия смарт-технологиям, систематизированы позитивные и негативные факторы доверия к перспективе расширения функций систем с ИИ в социальных структурах. Выделен междисциплинарный характер исследования цифрового доверия, обусловленный интерактивной технологией, опосредующей социальные и профессиональные коммуникации. В дискуссионном плане рассмотрены системные факторы доверия в сетевых интеракциях, определенные такими показателями, как: отношение к цифровой среде, поведение в цифровой среде, условия надежности цифровой среды, опыт пользователя, соотносимый с восприятием цифровой среды. В заключении подчеркивается, что уровень доверия информации в сети соотносится с социальным опытом компетентных людей, однако вотум доверия в цифровой среде смещается в сторону авторитета, знакомого по сети, а также в сторону компании, владеющей сервисом.

Ключевые слова: сетевые интеракции, смарт-технологии, цифровое общество, цифровое доверие, факторы доверия, цифровая среда.

Введение

Специфика технологии жизни в обществе с развитой е-культурой определяется динамикой развития сложных человеко-машинных комплексов с дополненной реальностью. Информационно-компьютерные технологии цифровой эпохи представлены созданием виртуальных моделей любых систем в киберпространстве, способных генерировать различные варианты действий в качестве агента возможных интеракций. Интенсивное развитие е-культуры, распространение цифровых посредников, консультантов и помощников в различных сферах профессиональной деятельности, а также в повседневной жизни создает новые проблемы в системе социальных взаимодействий, становясь фактором усиления технологической зависимости человека. Жизненная стратегия и процессы социализации человека оказываются тесно связанными с вопросами ориентации в киберпространстве, а также с определенным уровнем доверия к технологическим инновациям, трансформирующим повседневные коммуникации.

Наиболее актуальной проблемой социализации на сегодняшний день представляется перспектива замещения человека в профессиональной деятельности «умными» роботами и системами. Опасения в устойчивости социальной структуры повседневной жизни вызывает не только перспектива тотальной роботизации и замещения людей в профессии, но и безопасность перемещения в физическом и социальном пространстве, поскольку система транспортных связей активно включается в интеллектуальную автоматизацию функций операторов. Обеспечение быстрой связи на основе обработки больших массивов информации в системах с искусственным интеллектом (ИИ) связывают с перспективами прогресса Индустрии 4.0 [*Al-Shoqran, Al Zubi*, 2021; *Lorne, Gogireddy*, 2021].

В системе социально-экономических отношений проблемы человеко-компьютерных взаимодействий связаны с вопросами конфиденциальности и защиты данных, которые имеют решающее значение как для поддержки доверия потребителей интеллектуальных продуктов, так и для обеспечения надежных коммерческих и производственных цепочек. Современные авторы отмечают, что цифровая трансформация в системах интеракций в той или иной степени способствует разрушению конфиденциальности, подрыву доверия к распространяемой информа-

ции, делает человека продуктом манипуляции, а не пользователем [*Osburg,* 2019]. В потребительской сфере особенно часто возникают вопросы, которые касаются доверия цифровым агентам в связи с этическими сторонами интеракций, поскольку линии подотчетности и надзора не всегда четко определены [*Martinez-Martin,* 2020].

Комплексный характер проблемы доверия в условиях технологической эволюции цифрового общества предполагает оценку риска смарт-инноваций в связи с неопределенностью и непредсказуемостью следствий их влияния на природу самого человека и его жизненного мира. На этом фоне представляется актуальным анализ факторов доверия смарт-технологиям в социальных взаимодействиях.

Цель авторов данной статьи связана с исследованием уровней доверия общественности к перспективе развития «умных» систем и технологий ИИ. В задачи статьи входит уточнение содержания понятия *цифровое доверие*. В самом широком значении цифровое доверие можно рассматривать как уверенность людей в надежности, а также безопасности цифровых технологий и систем [*Frenehard*, 2019; *Веселов,* 2020]. В узком значении цифровое доверие предполагает достаточный уровень уверенности в действиях человека (как пользователя и профессионала), в надежности процессов и технологий, что необходимо для безопасности жизни.

Обзор литературы

В современной литературе концепт *доверие* имеет несколько интерпретаций. Согласно определению Ф. Фукуямы, доверие — это возникающее у членов сообщества ожидание того, что другие его члены будут вести себя более или менее предсказуемо, честно и добросовестно, со вниманием к нуждам окружающих, в согласии с некоторыми общими нормами [*Фукуяма,* 2004]. Э. Гидденс выделяет доверие к людям и доверие к абстрактным системам в виде символических и институциональных структур [*Гидденс,* 2011]. Проблема доверия актуализируется в моделировании социальных роботов, предназначенных для интеракций с сотрудниками. Индикатором, который фиксирует уровень доверия сотрудников в этом случае, выступает внешний вид сервисного представителя (гуманоидный робот, робот-андроид, человек) [*Stock et al.,* 2019].

В англоязычной литературе употребляются термины: *digital trust* (цифровое доверие) и *the digital trust environment* (цифровая среда доверия). Ключевые параметры *цифрового доверия* предлагается связывать с надежностью, прозрачностью, безопасностью и честностью [*Building digital trust,* 2921]. В статье: [*Shipunova et al.,* 2022a] показано, что в среднем 80% молодежной аудитории доверяют информационным сервисам в системе человеко-компьютерных взаимодействий.

Роль этики в оценке *цифрового доверия* выделена в исследовании уровня доверия населения к цифровой экономике, в частности, в связи с рисками и неэффективной практикой использования данных, имеющихся в распоряжении компании [*The State of Cybersecurity and Digital Trust,* 2016].

Проблема доверия в сетевых интеракциях связывается с разрушением согласованности ментальных моделей и общей осведомленности о ситуации посредством распространения неверной информации, которая усиливает диссонирующие ментальные модели рекомендательными алгоритмами, ботами и доверенными пользо-

вателями платформы (влиятельными лицами). Развитие централизованно управляемых коммуникационных (например, *Twitter, Facebook*) и сервисных (например, *Uber, airbnb*) платформ, поисковых систем и агрегирования данных (например, *Google*), а также аналитики данных и искусственного интеллекта создали эпоху цифровых сбоев в течение последнего десятилетия. Отдельные профили пользователей создаются поставщиками платформ, чтобы зарабатывать деньги на отслеживании, прогнозировании, использовании и влиянии на предпочтения и поведение своих пользователей. Для смягчения этого процесса цифрового разрушения необходимы новые методы и подходы к централизованному управлению этими платформами, чтобы укреплять и поощрять доверие к субъектам, которые их используют [*Bunker,* 2020].

В качестве факторов, определяющих доверие пользователя к источнику информации, рассматриваются типы знания, необходимого для действия. Доверие к записям зависит от четырех типов знаний о создателе или хранителе записей: репутация, прошлые результаты, компетентность и уверенность в будущих результатах. Рамки для установления доверия развивались по мере развития технологий. Сегодня отдельные лица и организации все чаще сохраняют записи и получают к ним доступ в инфраструктуре облачных вычислений, где мы не можем оценивать наше доверие к записям исключительно на основе четырех типов знаний, использовавшихся в прошлом. В исследовании, проведенном в Университете Британской Колумбии в области природы цифровых записей и их достоверности, сделана попытка определить границы общего права, в рамках которых проверяются вопросы доверия к документальным доказательствам [*Duranti, Rogers,* 2012].

В исследовании: [*Shin,* 2019] моделируется опыт пользователей инструментов блокчейна. Оценка доверия к инструментарию блокчейна определяется через влияние на поведение пользователя факторов конфиденциальности и безопасности. В книге: [*Internet of Things,* 2021] обсуждается возможность применения технологии блокчейна для обеспечения безопасности в различных областях социальных взаимодействий. Особое внимание уделяется применению интегрированных технологий для улучшения моделей данных, интеллектуальных прогнозов. Авторы объясняют, как блокчейн может повысить конфиденциальность и безопасность данных, одновременно повышая точность и целостность данных, сгенерированных системой «Интернет вещей» (IoT), и информации, обработанной ИИ.

В условиях взаимодействия потребителей и фирм в Интернете растет роль прогноза степени их удовлетворенности. В маркетинге цифрового контента, который направлен на повышение вовлеченности и доверия потребителей к бренду, в качестве концептуальной основы выделяются функциональные, гедонистические мотивы взаимодействия [*Hollebeek, Macky,* 2019].

В анализе текущего состояния обращения к онлайн-сервисам в случае оплаты услуг поставщика выделены три ключевых аспекта проблемы доверия: популярность использования различных цифровых способов оплаты, аспекты технологического доверия и демографические данные респондентов. На основании опроса 400 респондентов был выявлен уровень технологического доверия, который свидетельствует о росте популярности конкретного цифрового способа оплаты [*Szumski,* 2020].

В литературе по электронной коммерции представлены исследования по развитию доверия посредникам на основании анализа рынка онлайн-продуктов и при-

менения этих моделей к рынкам онлайн-услуг. Отмечается, что успешная сделка по предоставлению услуг требует не только первоначального доверия, но и дальнейшего поддержания его в процессе сотрудничества между клиентами и поставщиками. Посредники по краудсорсингу стимулируют цифровых предпринимателей, создавая рынки онлайн-услуг, на которых поставщики услуг заключают контракты с клиентами по всему миру. Важной стороной цифрового предпринимательства выступает создание институциональных механизмов, которые призваны поддерживать доверие клиентов к системе онлайн-услуг. В работе: [*Wenyu, Mao,* 2018] на примере исследования деятельности крупнейшего посредника по краудсорсингу в Китае представлена модель процесса взаимодействия клиентов с поставщиками. Подчеркивается роль посредника, который использует разные наборы институциональных механизмов, инициирующих, усиливающих и поддерживающих доверие клиентов.

Социальные факторы интеллектуальной автоматизации сетевых интеракций всесторонне обсуждаются в работе: [*Acemoglu, Restrepo,* 2018]. Авторы отмечают, что недавние опросы показывают высокий уровень беспокойства по поводу воздействия «умных» технологий на систему социальных и профессиональных взаимодействий. Примеры использования агентного моделирования для прогнозирования сложных доверительных отношений рассматриваются в работе: [*Hendriks et al.,* 2021].

Проблемам исследования цифрового доверия посвящены работы: [*Hollis,* 2018; *Botsman,* 2017]. В работах: [*Blöbaum,* 2016; *Bruckes et al.,* 2019] внимание авторов уделено выявлению и анализу ключевых характеристик цифрового доверия. В работе: [*Chakravorti et al.,* 2018] авторы подчеркивают необходимость разработки комплексной системы оценок доверия к цифровым инструментам деятельности и коммуникации. Приведенные в статье данные ранжированы по четырем параметрам в границах от низкого уровня доверия (0 баллов) до высокого уровня (5 баллов). Данные по четырем аспектам цифрового доверия, зарегистрированные в 42 странах, позволяют оценить перспективы распространения «умных» технологий в широкой сфере социальных взаимодействий.

Материалы и методы

Данное исследование опирается на системную методологию в оценке факторов доверия цифровым агентам в человеко-компьютерных взаимодействиях, на методы анализа и обобщения эмпирических данных. Чтобы выделить и систематизировать индикаторы цифрового доверия, мы рассмотрели разные аспекты отношения российских граждан к «умным» технологиям в различных социальных сферах.

Авторы обращаются к статистическим данным опросов населения России, чтобы выявить социальные сферы деятельности с наиболее эффективным внедрением структур ИИ в соотнесении с индикаторами цифрового доверия. Эмпирический материал для комплексной оценки цифрового доверия граждан России составляют статистические данные ВЦИОМ по опросам населения, выявляющим отношение общественности к перспективам внедрения цифровых агентов и технологий искусственного интеллекта в социальные и профессиональные взаимодействия. Мы используем Аналитические обзоры Всероссийского центра исследования обществен-

ного мнения (ВЦИОМ)[1]. В рамках исследования отношения к цифровой среде использовались данные онлайн-опроса в ноябре 2021 г., который был направлен на выявление сервисов и ресурсов цифровой среды, вызывающих / не вызывающих доверие. Выборка была случайная, участвовали 140 респондентов, пользователей сети Интернет. Анкета в Google-форме размещена в социальных сетях, доступных молодежи (преимущественно — группы «ВКонтакте» среди студентов, молодых специалистов — выпускников вузов, а также других пользователей).

Результаты

В онлайн-опросе уровень доверия цифровой среде выявлялся по отношению к мошенничеству в сетевых интеракциях. Прямой вопрос респондентам «Насколько Вы доверяете информации, получаемой через интернет-каналы?» получил следующее распределение ответов: только около 3% полностью доверяют; 46% отметили частичное доверие; 37% — скорее недоверие; 10% — совсем не доверяют. Около 75% респондентов в той или иной мере сталкивались с интернет-мошенничеством. Почти 43% опрошенных отмечают высокую степень риска быть обманутым в интернет-среде; почти 48% высказывают мнение о средней степени риска; и 8% респондентов считают интернет-среду безопасной (рис. 1).

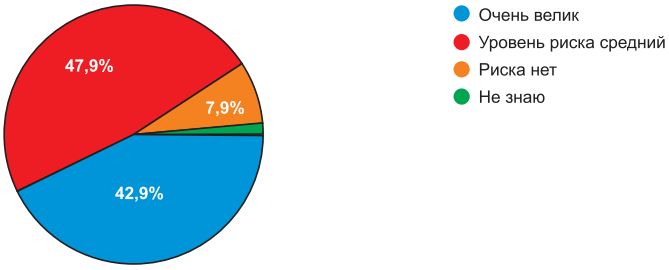

Рис. 1. Распределение ответов на вопрос о степени риска быть обманутым в интернет-среде
Fig. 1. Distribution of answers on the degree of risk of being deceived in the Internet environment

На вопрос: доверяете ли вы друзьям или подписчикам в социальных сетях (*«ВКонтакте», Facebook, Instagram, TikTok*), выяснилось, что более 70% респондентов частично доверяют и 38% — скорее не доверяют. Вопрос о доверии мобильным приложениям банков (*ВТБ, Сбер, «Альфа банк»* и др.) показал, что 30% полностью доверяют; 36% — частично доверяют; 23% — скорее не доверяют. При этом 42% респондентов указали, что имеют опыт в использовании таких сервисов, как мобиль-

[1] Искусственный интеллект: угроза или возможность? (27 января 2020). [Электронный ресурс]. Режим доступа: https://wciom.ru/analytical-reviews/analiticheskii-obzor/iskusstvennyj-intellekt-ugroza-ili-vozmozhnost (дата обращения: 19.07.2021); Роботы и работа: мифы и реальность (20 августа 2019). Режим доступа: https://wciom.ru/analytical-reviews/analiticheskii-obzor/roboty-i-rabota-mify-i-realnost (дата обращения: 19.07.2021); Роботизация работы: возможность или опасность (14 декабря 2017). Режим доступа: https://wciom.ru/tematicheskii-katalog/page-3?tx_news_pi1%5BoverwriteDemand%5D%5Bcategories%5D=142&cHash=4e7bf7a0f3e239d4c812b958a9140a74 (дата обращения: 19.07.2021).

ный цифровой ассистент (банковские ассистенты, *Siri, «Алиса», «Маруся», Google*), но при этом доверяют им 38% всех опрошенных, а 46% — не доверяют. Вывод: цифровое доверие зависит от практики пользования цифровыми услугами сервисов, от активности в цифровой среде.

Оценка степени готовности использовать системы искусственного интеллекта

По данным ВЦИОМ 2019–2020 гг. российские граждане оптимистично оценивают расширение смарт-технологий и систем ИИ. В среднем по разным возрастным группам 64–68% опрошенных респондентов не считают «умные» системы опасными для человека в перспективе. Однако для трети респондентов характерен высокий уровень недоверия к «умным» системам (см. табл. 1).

Табл. 1. Индикаторы недоверия к системам искусственного интеллекта

Table 1. Indicators of distrust to artificial intelligence systems

Индикатор негативного отношения к ИИ	**Усредненные показатели опроса в Аналитических обзорах ВЦИОМ, %**	**Причина негативного отношения к ИИ**
Недоверие к надежности работы системы	31% по данным: [*Искусственный интеллект: угроза или возможность?* 2020]	17% — техническая проблема
		8% — выход из-под контроля
		6% — человек надежнее
Недоверие к безопасности	21% по данным: [*Искусственный интеллект: угроза или возможность?* 2020]	Угроза безопасности личных данных 12% — взлом и хищение персональных данных
		9% — нарушение конфиденциальности личного пространства
Недоверие к последствиям в системе взаимодействий	37% по данным: [*Искусственный интеллект: угроза или возможность?* 2020]	16% — плохое влияние на формы общения человека и его поведение
		12% — непредсказуемость перспектив развития систем ИИ
		5% — отсутствие знаний о последствиях внедрения ИИ
Замещение в профессии	21%, по данным: [*Роботы и работа: мифы и реальность*, 2019]	Перспектива потерять работу
	62%, по данным: [*Роботизация работы: возможность или опасность, 2017*]	Считают неправильной политику замены людей роботами на рабочих местах

Результаты обобщения данных серии опросов российских граждан по проблеме доверия к смарт-технологиям в системах сетевых интеракций представлены в таблице 2 и на рисунке 2.

Табл. 2. Сферы внедрения смарт-технологии с высоким уровнем доверия к искусственному интеллекту[2]

Table 2. Areas of smart technology implementation with a high level of trust in artificial intelligence[3]

Социотехнические сферы деятельности	Доверяют ИИ, по данным опросов ВЦИОМ, %
Наука	72
Промышленность	69
Транспорт	66
Госуслуги	68
Медицина, диагностика	52

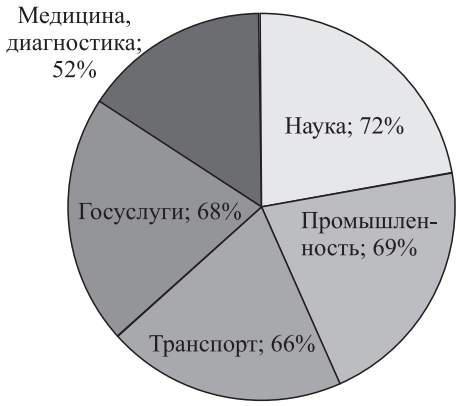

Рис. 2. Социотехнические сферы деятельности с высоким уровнем доверия смарт-технологиям[4]

Fig. 2. Sociotechnical spheres of activity with a high level of trust in smart technologies[5]

[2] Искусственный интеллект: угроза или возможность? (27 января 2020) [Электронный ресурс]. Режим доступа: https://wciom.ru/analytical-reviews/analiticheskii-obzor/iskusstvennyj-intellekt-ugroza-ili-vozmozhnost (дата обращения: 19.07.2021).

[3] Artificial Intelligence: threat or opportunity (January 27, 2020). Available at: https://wciom.ru/analytical-reviews/analiticheskii-obzor/iskusstvennyj-intellekt-ugroza-ili-vozmozhnost (date accessed: 19.07.2021).

[4] Искусственный интеллект: угроза или возможность? (27 января 2020) [Электронный ресурс].

[5] Artificial Intelligence: threat or opportunity (January 27, 2020).

Дискуссия

Условия цифрового доверия

С ростом интенсивности онлайн-взаимодействий между потребителями и компаниями возрастает роль прогнозирования удовлетворенности потребителей. В контент-маркетинге целью является повышение вовлеченности потребителей. Условия доверия бренду связывают с функциональными и гедонистическими мотивами в качестве концептуальной основы проектирования взаимодействия [*Hollebeek, Macky,* 2019; *Shipunova et al.,* 2022b]. Проблема доверия особенно актуальна при моделировании социальных роботов, предназначенных для взаимодействия сотрудников. В этом случае представитель службы *outlook* (гуманоидный робот, android, человек) является показателем, отражающим уровень доверия сотрудников.

Исследование 2021 г. по оценке цифровой готовности россиян [*Дмитриева*, 2021] выявило специфику технологического и социального цифрового доверия в зависимости от области применения интеллектуальных систем. К индикаторам технологического доверия отнесли: прозрачность процесса (знаю, как работает); безопасность моих действий, защита от ошибок; удобство, скорость и стоимость получения результата; надежность и доступность сервиса (без сбоев 24 часа в сутки); конфиденциальность моих сведений; собственный опыт. К индикаторам социального доверия отнесли: опыт близких и авторитетных людей; доверие компании владельца сервиса; собственный опыт. Авторы исследования подчеркивают: 1) чем выше уровень цифровой грамотности (от начального до продвинутого), тем слабее влияние фактора «доверие технологиям» при принятии решения использовать цифровой сервис; 2) для бизнесменов при использовании цифрового сервиса намного более сильное влияние имеет фактор социального доверия, чем для представителей остальных социальных групп; 3) для военнослужащих ярче выражен фактор доверия технологиям; 4) для учащихся (студентов) оба фактора одинаково значимы [*Там же,* 2021, с. 63]. На уровень доверия «умным» системам ИИ влияет имеющийся у пользователей опыт работы с цифровыми сервисами и базами данных.

Комплексные показатели оценки цифрового доверия

В сетевом обществе укрепление доверия к смарт-технологиям и цифровым сервисам социальных и профессиональных взаимодействий является сложным процессом. Для сравнительной оценки цифрового доверия авторы [*Chakravorti et al.*, 2018] предлагают использовать комплексные индикаторы, фиксирующие особенности поведения, отношения, окружающей среды и опыта. Центральным понятием в комплексной оценке уровня доверия выступает цифровая среда.

Доверие в отношении цифровой среды сетевых интеракций рассматривается через призму следующих показателей:

- отношение к цифровой среде;
- поведение в цифровой среде;
- условия надежности цифровой среды;
- опыт пользователя, соотносимый с восприятием цифровой среды.

Индикаторы поведения фиксируют реакции пользователя в цифровом взаимодействии, которое всегда связано с технологическими условиями работы сети и определенными навыками вхождения в сеть. Характер поведения пользователей го-

ворит об актуальной мере цифрового доверия. Безопасная работа в системе сетевых интеракций требует определенных программ и паролей. Эмпирические измерения в рамках индикатора цифрового поведения касаются определения мотива выбора сфер интернет-практики и выявления уровня цифровой грамотности пользователя.

Индикаторы отношения пользователя к цифровой среде позволяют косвенно оценить уровень доверия через исследование временных параметров сетевых взаимодействий пользователя, характеризующих его интернет-активность. С другой стороны, индикатор отношения указывает на значение конфиденциальности информации в сети. Это позволяет установить степень доверия пользователя технологической платформе или социальной сети, а также экспертным системам и цифровым посредникам в коммуникации.

Индикаторы, связанные с характеристикой цифровой среды, фиксируют факторы, гарантирующие надежность и безопасность информационного взаимодействия в сети. Три основных фактора укрепления доверия: конфиденциальность, интернет-безопасность и подотчетность. Конфиденциальность — одна из основных проблем, вызывающих беспокойство пользователей, от массового взлома конфиденциальной информации до усиления государственного и корпоративного отслеживания цифровых действий, идентификационных данных и местоположения пользователей [*Chakravorti et al.,* 2018].

Индикатор цифрового опыта пользователя характеризует интеллектуально-эмоциональный спектр восприятия сетевой технологической среды. В эмпирическом исследовании показатель качества цифрового опыта выявляется в измерении скорости и простоты использования цифровых сервисов при совершении онлайн-транзакций, связанных с идентификацией и интерфейсами. Однако усложнение систем цифровой конфиденциальности, безопасности и подотчетности может привести к негативному восприятию, снижающему доверие пользователей к онлайн-сервису. Например, введение нескольких паролей для входа в безопасный сервис может сделать пользователя менее склонным к взаимодействию в сети. Гармония индивидуального опыта действий в сети с надлежащей защитой выступает в данном случае мерой цифрового доверия.

Заключение

В настоящем исследовании проблема цифрового доверия рассматривается в узком значении с акцентом на информационной уверенности. С развитием сетевого общения доверие меняет свою форму, трансформируясь в сетевое доверие в социальных сетях, в которых личное знакомство может и не предполагаться. Расширение информационного потока приводит к тому, что переформатируется способ социальных взаимодействий. Возможности современных технологий способствуют тому, что, не обладая серьезными навыками работы в IT-сфере, более или менее продвинутый пользователь может разместить в сети любую информацию (пост, блог и т. п.), достоверность которой сложно установить.

Индикаторы доверия информации в сети сопоставимы с индикаторами социального доверия, которые характеризуются отношением к опыту близких или авторитетных людей. Новости, оценку событий современный молодой человек черпает чаще всего из окружения, которое сформировалось у него под влиянием сетевого

взаимодействия. Вопрос доверия в таком случае смещается в сторону доверия тому или иному человеку, возможно, знакомому только по сети, или компании, владеющей цифровым сервисом.

Исследование индикаторов цифрового доверия в системах человеко-компьютерных взаимодействий имеет междисциплинарный характер, обусловленный интерактивной технологией, усиливающей сложность социальных и профессиональных коммуникаций в сетевом обществе. Комплексные показатели, фиксирующие отношение доверия российских граждан к распространению смарт-технологий в социальной и профессиональной деятельности, опираются на обобщение базы данных социологических опросов населения России. Выявлено пять сфер применения ИИ в России, для которых индикатор интеллектуально-эмоционального восприятия цифровой среды показывает высокий уровень доверия «умным» технологиям.

Литература

Веселов Ю.В. Доверие в цифровом обществе // Вестник Санкт-Петербургского университета. Сер.: Социология. 2020. Т. 13. Вып. 2. С. 129–143. DOI: 10.21638/spbu12.2020.202.

Гидденс Э. Последствия современности / Пер. с англ. М.: Праксис, 2011. 352 с.

Искусственный интеллект: угроза или возможность? (27 января 2020) [Электронный ресурс]. Режим доступа: https://wciom.ru/analytical-reviews/analiticheskii-obzor/iskusstvennyj-intellekt-ugroza-ili-vozmozhnost (дата обращения: 19.07.2021).

Дмитриева Н.Е., Жулин А.Б., Артамонов Р.Е., Титов Э.А. Оценка цифровой готовности населения России: доклад к XXII Апр. междунар. науч. конф. по проблемам развития экономики и общества, Москва, 13–30 апр. 2021 г. М.: Изд. дом Высшей школы экономики, 2021. 86 с.

Роботизация работы: возможность или опасность (14 декабря 2017) [Электронный ресурс]. Режим доступа: https://wciom.ru/tematicheskii-katalog/page-3?tx_news_pi1%5Boverwrite Demand%5D%5Bcategories%5D=142&cHash=4e7bf7a0f3e239d4c812b958a9140a74 (дата обращения: 19.07.2021).

Роботы и работа: мифы и реальность (20 августа 2019) [Электронный ресурс]. Режим доступа: https://wciom.ru/analytical-reviews/analiticheskii-obzor/roboty-i-rabota-mify-i-realnost (дата обращения: 19.07.2021).

Фукуяма Ф. Доверие: социальные добродетели и путь к процветанию / Пер. с англ. М.: АСТ, 2004. 730 с.

Acemoglu D., Restrepo P. Artificial Intelligence, Automation and Work // NBER Working Paper Series. 2018. No. 24196. Available at: http://www.nber.org/papers/w24196 (date accessed: 19.07.2021).

Al-Shoqran M., Al Zub'I. S. A Review on Industry 4.0 Management for Sustainable Technologies // Artificial Intelligence Systems and the Internet of Things in the Digital Era. EAMMIS 2021. Lecture Notes in Networks and Systems / Eds. A.M. Musleh Al-Sartawi, A. Razzaque, M.M. Kamal. Vol. 239. Cham: Springer, 2021. P. 206–217. DOI: 10.1007/978-3-030-77246-8_21.

Blöbaum B. Key Factors in the Process of Trust. On the Analysis of Trust under Digital Conditions // Trust and communication in a digitized world. Models and concepts of trust research / Ed. B. Blöbaum. 2016. Cham: Springer, 2016. P. 3–25. DOI: 10.1007/978-3-319-28059-2_1.

Botsman R. What Can You Trust?: How Technology Brought Us Together — and Why It Could Drive Us Apart. UK: Penguin; USA: Public Affairs. 2017. 323 p.

Bruckes M., Westmattelmann D., Oldeweme A., Schewe G. Determinants and Barriers of Adopting Robo-advisory Services // International conference on information systems (ICIS 2019). Munich:

AIS. Available at: https://www.researchgate.net/publication/337428436_Determinants_and_Barriers_of_Adopting_Robo-Advisory_Services) (date accessed: 01.11.2021).]

Building Digital Trust: The Role of Data Ethics in the Digital Age. AccentureLabs. Available at: https://www.visionmonday.com/CMSDocuments/2019/04/Accenture-Data-Ethics-POV-WEB.pdf (date accessed: 01.11.2022).

Bunker D. Who Do You Trust? The Digital Destruction of Shared Situational Awareness and the COVID-19 Infodemic // International Journal of Information Management. 2020. Vol. 55. P. 102201. DOI: /10.1016/j.ijinfomgt.2020.102201.

Chakravorti B, Bhalla A, Chaturvedi R.S. The 4 Dimensions of Digital Trust, Chartered across 42 Countries // Harvard business review, 2018. Available at: https://hbr.org/2018/02/the-4-dimensions-of-digital-trust-charted-across-42-countries (date accessed: 01.06.2022).

Duranti L., Rogers C. Trust in Digital Records: An Increasingly Cloudy Legal Area // Computer Law & Security Review. 2012. Vol. 28. No. 5. P. 522–531. DOI: 10.1016/j.clsr.2012.07.009.

Frenehard T. Building Digital Trust: What Does It Really Mean (2019). Available at: https://blogs.sap.com/2019/10/08/building-digital-trust-what-does-it-really-mean (date accessed: 19.07.2022).

Hendriks F., Distel B., Engelke K.M., Westmattelmann D., Wintterlin F. Methodological and Practical Challenges of Interdisciplinary Trust Research // Trust and Communication / Ed. B. Blöbaum. 2021. Cham: Springer, 2021. P. 29–57. DOI: 10.1007/978-3-030-72945-5_2.

Hollis C. Let Artificial Intelligence Earn Your Trust. Forbes. 2018. Available at: https://www.forbes.com/sites/oracle/2018/03/26/let-artificial-intelligence-earn-your-trust/ (date accessed: 19.07.2022).

Hollebeek L.D., Macky K. Digital Content Marketing's Role in Fostering Consumer Engagement, Trust, and Value: Framework, Fundamental Propositions, and Implications // Journal of Interactive Marketing. 2019. Vol. 45. P. 27–41.

Internet of Things, Artificial Intelligence and Blockchain Technology / Eds. R. Lakshmana Kumar, Yichuan Wang, T. Poongodi, Agbotiname Lucky Imoize. Springer Nature Switzerland AG, 2021. DOI: 10.1007/978-3-030-74150-1.

Lorne F.T., Gogireddy M.R. Digital Social Contracts with AI Robots: Some Implications for Amazon.Com // Artificial Intelligence Systems and the Internet of Things in the Digital Era. EAMMIS 2021. Lecture Notes in Networks and Systems / Eds. A.M. Musleh Al-Sartawi, A. Razzaque, M.M. Kamal. Vol. 239. Cham: Springer, 2021. P. 78–89. DOI: 10.1007/978-3-030-77246-8

Martinez-Martin N. Chapter Three — Trusting the Bot: Addressing the Ethical Challenges of Consumer Digital Mental Health Therapy // Developments in Neuroethics and Bioethics. 2020. Vol. 3: Ethical Dimensions of Commercial and DIY Neurotechnologies / Eds. I. Bárd, E. Hildt. P. 63–91. DOI: 10.1016/bs.dnb.2020.03.003.

Osburg T. Changing Relevance of Trust in Digital Worlds // Media Trust in a Digital World / Eds. T. Osburg, S. Heinecke. Cham: Springer, 2019. P. 15–33. DOI: 10.1007/978-3-030-30774-5_2.

Shin Don D.H. Blockchain: The Emerging Technology of Digital Trust // Telematics and Informatics. 2019. Vol. 45. No. 101278. DOI: 10.1016/j.tele.2019.101278.

Shipunova O., Berezovskaya I., Pozdeeva E., Evseeva L., Barlybayeva S. Digital Trust Indicators in Human-Computer Interaction // Information Systems and Technologies. WorldCIST 2022. Lecture Notes in Networks and Systems / Eds. A. Rocha, H. Adeli, G. Dzemyda, F. Moreira. Vol. 468. Cham: Springer, 2022a. DOI: 10.1007/978-3-031-04826-5_24.

Shipunova O., Berezovskaya I., Kedich S., Popova N. Indicators of Choosing Internet User's Responsible Behavior // Proceedings of Sixth International Congress on Information and Communication Technology. Lecture Notes in Networks and Systems / Eds. X.S. Yang, S. Sherratt, N. Dey, A. Joshi. 2022b. Vol. 236. Singapore: Springer, 2022b. DOI: 10.1007/978-981-16-2380-6_85.

Stock R, Merkle M., Eidens D., Hannig M., Heineck P., Nguyen M.A., Völker J. When Robots Enter Our Workplace: Understanding Employee Trust in Assistive Robots // ICIS 2019 Proceedings. 1. Available at: https://aisel.aisnet.org/icis2019/human_computer_interact/human_computer_interact/1 (date accessed: 19.07.2022).

Szumski O. Technological Trust from the Perspective of Digital Payment // Procedia Computer Science. 2020. Vol. 176. P. 3545–3554. DOI: 10.1016/j.procs.2020.09.032.

The State of Cybersecurity and Digital Trust 2016. Identifying Cybersecurity Gaps to Rethink State of the Art. Available at: https://www.accenture.com/_acnmedia/pdf-22/accenture-data-ethics-pov-web.pdf (date accessed: 02.11.2021).

Wenyu (Derek) Du, Ji-Ye Mao. Developing and Maintaining Clients' Trust through Institutional Mechanisms in Online Service Markets for Digital Entrepreneurs: A Process Mode // The Journal of Strategic Information Systems. 2018. Vol. 27. No. 4. P. 296–310. DOI: 10.1016/j.jsis.2018.07.001.

The Problem of Trust in Smart Technologies in Digital Society

Olga D. Shipunova

Peter the Great St Petersburg Polytechnic University,
St Petersburg, Russia;
e-mail: o_shipunova@mail.ru

Elena G. Pozdeeva

Peter the Great St Petersburg Polytechnic University,
St Petersburg, Russia;
e-mail: elepozd@mail.ru

The article considers philosophical aspects of technological evolution of digital society determined by the transformation of human-computer systems and relationships. The article analyses the levels of public trust in the prospect of smart technologies development in social interactions. The problem of trust in smart technologies clearly reveals the prospective problem of replacing a person in professional activity. At the same time, the traditional aspects of trust between people related to ethical attitudes are complemented by the problems of trust in intelligent technologies and smart robots included in the institutional and cognitive structures of the life world. The study of the levels of trust in the digital environment and AI systems is based on analysis and generalization of empirical material from VCIOM reviews compiled from surveys of the Russian Federation citizens of various age groups, and is aimed at identifying the nature of attitudes to the prospects for the artificial intelligence technologies introduction into social and professional spheres of activity. In assessing the level of trust in the digital environment, the authors utilize the data of an online survey carried out in November 2021 (140 respondents, Internet users, mainly students and young professionals — university graduates). On this basis, we identify sociotechnical spheres as ones with a high level of trust in smart technologies, systematize positive and negative factors of trust in the prospect of expanding of artificial intelligence systems in social structures. It's worth to note the interdisciplinary nature of the studies of digital trust indicators, caused by an interactive technology mediating social and professional communications. As a basis for discussion, we consider the factors of trust in network interactions determined by such indicators as: attitude to the digital environment, behavior in the digital environment, conditions for the digital environment reliability, user experience correlated with the digital environment perception. In conclusion, it is emphasized that the level of trust in information on the network correlates with the social experience of experts, but the vote of confidence in the digital environment is shifting towards the authority of friends on the network, as well as towards the company that owns the service.

Keywords: network interactions, smart technologies, digital society, digital trust, trust factors, digital environment.

References

Acemoglu, D., Restrepo, P. (2018). Artificial Intelligence, Automation and Work, *NBER Working paper series*, no. 24196. http://www.nber.org/papers/w24196.

Al-Shoqran, M., Al Zub'I, S. (2021). A Review on Industry 4.0 Management for Sustainable Technologies, in A.M. Musleh Al-Sartawi, A. Razzaque, M.M. Kamal (Eds.), *Artificial Intelligence Systems and the Internet of Things in the Digital Era. EAMMIS 2021. Lecture Notes in Networks and System*s, vol. 239 (pp. 206–217), Cham: Springer. DOI: 10.1007/978-3-030-77246-8_21.

Blöbaum, B. (2016). Key Factors in the Process of Trust. On the Analysis of Trust under Digital Conditions, in B. Blöbaum (Ed.), *Trust and Communication in a Digitized World. Models and Concepts of Trust Research* (pp. 3–25). Cham: Springer. DOI: 10.1007/978-3-319-28059-2_1

Botsman, R. (2017). *What Can You Trust?: How Technology Brought Us Together — and Why It Could Drive Us Apart*, UK: Penguin; USA: Public Affairs.

Bruckes, M., Westmattelmann, D., Oldeweme, A., Schewe, G. (2019). Determinants and Barriers of Adopting Robo-advisory Services, in *International conference on information systems (ICIS 2019)*, Munich: AIS. Available at: https://www.researchgate.net/publication/337428436_Determinants_and_Barriers_of_Adopting_Robo-Advisory_Services (date accessed: 01.11.2021).

Building Digital Trust: The Role of Data Ethics in the Digital Age (2019). AccentureLabs. Available at: https://www.visionmonday.com/CMSDocuments/2019/04/Accenture-Data-Ethics-POV-WEB.pdf (date accessed: 01.11.2022).

Bunker, D. (2020). Who Do You Trust? The Digital Destruction of Shared Situational Awareness and the COVID-19 infodemic, *International Journal of Information Management*, no. 55, 102201. DOI: /10.1016/j.ijinfomgt.2020.102201.

Chakravorti, B, Bhalla, A, Chaturvedi, R.S (2018). The 4 Dimensions of Digital Trust, Chartered across 42 Countries, in *Harvard Business Review*. Available at: https://hbr.org/2018/02/the-4-dimensions-of-digital-trust-charted-across-42-countries (date accessed: 01.06.2022).

Dmitrieva, N.E., Zhulin, A.B., Artamonov, R.E., Titov, E.A. (2021). *Otsenka tsifrovoy gotovnosti naseleniya Rossii* [Assessment of the digital readiness of the population of Russia], XXII Apr. int. scientific. conf. on the problems of economic and social development, Moscow, 13–30 April. 2021, Moskva: National Research University "Higher School of Economics" (in Russian).

Duranti, L., Rogers, C. (2012). Trust in Digital Records: An Increasingly Cloudy Legal Area, *Computer Law & Security Review*, *28* (5), 522–531. DOI: 10.1016/j.clsr.2012.07.009.

Frenehard, T. (2019). *Building Digital Trust: What Does It Really Mean*, Available at: https://blogs.sap.com/2019/10/08/building-digital-trust-what-does-it-really-mean (date accessed: 19.07.2021).

Fukuyama, F. (2004). *Doveriye: sotsial'nyye dobrodeteli i put' k protsvetaniyu* [Trust: social virtues and the path to prosperity], Moskva: ACT (in Russian).

Giddens, E. (2011). *Posledstviya sovremennosti* [Consequences of modernity], Moskva: Praxis (in Russian).

Hendriks, F., Distel, B., Engelke, K.M., Westmattelmann, D., Wintterlin, F. (2021). Methodological and Practical Challenges of Interdisciplinary Trust Research, in B. Blöbaum (Ed.), *Trust and Communication* (pp. 29–57), Cham: Springer. DOI: 10.1007/978-3-030-72945-5_2.

Hollis, C. (2018). *Let Artificial Intelligence Earn Your Trust. Forbes*. Available at: https://www.forbes.com/sites/oracle/2018/03/26/let-artificial-intelligence-earn-your-trust/ (date accessed: 19.07.2021).

Hollebeek, L.D., Macky, K. (2019). Digital Content Marketing's Role in Fostering Consumer Engagement, Trust, and Value: Framework, Fundamental Propositions, and Implications, *Journal of Interactive Marketing*, vol. 45, 27–41.

Lakshmana, Kumar R., Yichuan Wang, Poongodi, T., Agbotiname Lucky Imoize (Eds.) (2021). *Internet of Things, Artificial Intelligence and Blockchain Technology*, Springer Nature Switzerland, AG 2021. DOI: 10.1007/978-3-030-74150-1.

Iskusstvennyy intellekt: ugroza ili vozmozhnost'? [Artificial intelligence: threat or opportunity?] (27 January 2020). Available at: https://wciom.ru/analytical-reviews/analiticheskii-obzor/iskusstvennyj-intellekt-ugroza-ili-vozmozhnost (date accessed: 19.07.2021) (in Russian).

Lorne. F.T., Gogireddy, M.R. (2021). Digital Social Contracts with AI Robots: Some Implications for Amazon.Com, in A.M. Musleh Al-Sartawi, A. Razzaque, M.M. Kamal (Eds.), *Artificial Intelligence Systems and the Internet of Things in the Digital Era. EAMMIS 2021. Lecture Notes in Networks and Systems*, vol. 239 (pp. 78–89), Cham: Springer. DOI: 10.1007/978-3-030-77246-8.

Martinez-Martin N. (2020). Chapter Three — Trusting the Bot: Addressing the Ethical Challenges of Consumer Digital Mental Health Therapy, in I. Bárd, E. Hildt (Eds.), *Developments in Neuroethics and Bioethics*, Vol. 3: Ethical Dimensions of Commercial and DIY Neurotechnologies (pp. 63–910). DOI: 10.1016/bs.dnb.2020.03.003.

Osburg, T. (2019). Changing Relevance of Trust in Digital Worlds, in T. Osburg, S. Heinecke (Eds), *Media Trust in a Digital World* (pp. 15–33), Cham: Springer. DOI: 10.1007/978-3-030-30774-5_2.

Robotizatsiya raboty: vozmozhnost' ili opasnost' [Robotization of work: opportunity or danger] (December 14, 2017). Available at: https://wciom.ru/tematicheskii-katalog/page-3?tx_news_pi1%5BoverwriteDemand%5D%5Bcategories%5D=142&cHash=4e7bf7a0f3e239d4c812b958a9140a74 (date accessed: 14.12.2017) (in Russian).

Roboty i rabota: mify i real'nost' [Robots and work: myths and reality] (August 20, 2019). Available at: https://wciom.ru/analytical-reviews/analiticheskii-obzor/roboty-i-rabota-mify-i-realnost (date accessed: 19.07.2021) (in Russian).

Shin Don, D.H. (2019). Blockchain: The Emerging Technology of Digital Trust, *Telematics and Informatics*, vol. 45, 101278. DOI: 10.1016/j.tele.2019.101278.

Shipunova, O., Berezovskaya, I., Pozdeeva, E., Evseeva, L., Barlybayeva, S. (2022a). Digital Trust Indicators in Human-Computer Interaction, in A. Rocha, H. Adeli, G. Dzemyda, F. Moreira (Eds.), *Information Systems and Technologies. WorldCIST 2022. Lecture Notes in Networks and Systems*, vol. 468, Cham: Springer. DOI: 10.1007/978-3-031-04826-5_24.

Shipunova, O., Berezovskaya, I., Kedich, S., Popova, N. (2022b). Indicators of Choosing Internet User's Responsible Behavior, in X.S. Yang, S. Sherratt, N. Dey, A. Joshi (Eds.), *Proceedings of Sixth International Congress on Information and Communication Technology. Lecture Notes in Networks and Systems*, vol. 236, Singapore: Springer. DOI: 10.1007/978-981-16-2380-6_85.

Stock, R., Merkle, M., Eidens, D., Hannig, M., Heineck, P., Nguyen, M.A., Völker, J. (2019). When Robots Enter Our Workplace: Understanding Employee Trust in Assistive Robots, in *ICIS 2019 Proceedings. 1.* Available at: https://aisel.aisnet.org/icis2019/human_computer_interact/human_computer_interact/1 (date accessed: 19.07.2021).

Szumski, O. (2020). Technological Trust from the Perspective of Digital Payment, *Procedia Computer Science*, *176,* 3545–3554. DOI: 10.1016/j.procs.2020.09.032.

The State of Cybersecurity and Digital Trust (2016). Identifying Cybersecurity Gaps to Rethink State of the Art. Available at: https://www.accenture.com/_acnmedia/pdf-22/accenture-data-ethics-pov-web.pdf (date accessed: 02.11.2021).

Veselov, Yu.V. (2020). Doveriye v tsifrovom obshchestve [Trust in digital society], *Vestnik Sankt-Petersburgskogo universiteta, ser.: Sotsiologya, 13* (2), 129–143 (in Russian). DOI: 10.21638/spbu12.2020.202.

Wenyu (Derek), Du, Ji-Ye, Mao (2018). Developing and Maintaining Clients' Trust through Institutional Mechanisms in Online Service Markets for Digital Entrepreneurs: A Process Mode, *The Journal of Strategic Information Systems*, *27* (4), 296–310. DOI: 10.1016/j.jsis.2018.07.001.