УДК 316.422 Вестник СПбГУ. Социология. 2020. Т. 13. Вып. 2

Результаты эмпирического исследования киберсоциального доверия среди жителей Петербурга*

Л. А. Видясова[1], *Я. Д. Тенсина*[1], *Ю. А. Кабанов*[1,2]

[1] Санкт-Петербургский национальный исследовательский университет ИТМО, Российская Федерация, 197101, Санкт-Петербург, Кронверкский пр., 49
[2] Национальный исследовательский университет «Высшая школа экономики», Российская Федерация, 190121, Санкт-Петербург, ул. Союза Печатников, 16

Для цитирования: *Видясова Л. А., Тенсина Я. Д., Кабанов Ю. А.* Результаты эмпирического исследования киберсоциального доверия среди жителей Петербурга // Вестник Санкт-Петербургского университета. Социология. 2020. Т. 13. Вып. 2. С. 236–254.
https://doi.org/10.21638/spbu12.2020.208

Доверие является важным элементом в построении информационного общества, вместе с тем все более обширное распространение и использование технологий сопровождается влиянием негативных факторов и опасений, связанных с незащищенностью некоторых каналов передачи данных, обсуждаемыми кибератаками, давлением государства на гражданские структуры, а также неопределенностью в отношении правил и норм коммуникаций нового типа. В статье приводятся результаты эмпирического исследования отношения жителей Петербурга к цифровым технологиям, а также их уровня доверия к Интернет и межличностной коммуникации. Опрос 600 респондентов был проведен в мае 2019 г. (выборка репрезентативная для населения Петербурга старше 18 лет, ошибка выборки не превышает 5 %, уровень достоверности составил 95 %). По результатам исследования было выявлено преобладание интернет-пользователей среди опрошенных респондентов, а также рост уверенности в использовании новых технологий у более молодых групп населения. В статье более детально представлены результаты исследования опыта пользователей в сфере онлайн-обучения. Анализ включенности в онлайн-обучение также продемонстрировал востребованность этих технологических решений в группе молодежи (люди до 35 лет). При этом в оценке личного опыта мнения жителей Петербурга разделились практически поровну на позитивные и негативные. На основе факторной модели выявлены три компонента, из которых складывается категория «киберсоциальное доверие»: институциональное доверие к организациям, осуществляющим свою деятельность в Интернете; транзакционное доверие к взаимодействию с другими акторами онлайн (прежде всего — к государству); информационное доверие относительно полноты, качества и достоверности информации (услуг в области информации).

Ключевые слова: социальное доверие, доверие к информационным технологиям, онлайн-образование, интернет-пользователи, киберсоциальное доверие.

Введение

В настоящее время применение новых информационных технологий приводит к созданию новых моделей коммуникации, социализации и сотрудничества, однако способствует и появлению ранее неизвестных угроз для индивидуального раз-

* Исследование выполнено за счет гранта РФФИ (проект № 18-311–20001 «Исследование киберсоциального доверия в контексте использования и отказа от информационных технологий»).

вития и общественных перемен. Некоторые исследователи отмечают, что с развитием технологий появляются не существовавшие ранее факторы маргинализации и социального исключения [1]. Кроме того, отмечается, что популярность современных средств коммуникации, их разнообразие и обновление приводят к росту ощущения неуверенности и недоверия к содержанию информации. Большинство исследований направлены на изучение доверия в сфере общественных отношений: в частности доверия к отдельным социальным институтам — в то время как вопрос доверия к новым технологиям по-прежнему остается недостаточно изученным. Кроме того, недостаточное внимание уделяется доверию как фактору, влияющему на принятие инноваций и готовность к изменениям.

По данным статистики поисковой системы «Яндекс», рынок онлайн-образования демонстрирует постоянный рост, и за последний год превысил планку в 60 %. Онлайн-образование представляет собой услуги дистанционного обучения с учителем/тьютором, а также занятия с использованием образовательных интернет-ресурсов, обучающих мобильных приложений, онлайн-тренажеров — любые формы образования с применением интернет- и видеоконтента. Сейчас ключевыми технологиями, используемыми в среде онлайн-образования, являются технологии виртуальной и дополненной реальности, использование искусственного интеллекта и машинного обучения, геймификации и т. д. В статье приводятся результаты опроса жителей Петербурга о восприятии новых информационных технологий в различных сферах, и особенное внимание уделяется доверию к цифровизации сферы образования. На основе полученных эмпирических данных строится модель киберсоциального доверия, охватывающая различные сферы использования информационных технологий.

Доверие к информационным технологиям: направления исследования

Научный интерес к общей категории доверия обоснован его ролью в формировании общественного капитала. Фундаментальная роль доверия в межчеловеческих отношениях отражена в работах К. Арроу [2], С. М. Липсет и В. Шейдер [3], Д. Р. Гибб [4], Н. Лумана [5], Б. Мишталь [6]. Ф. Фукуяма определяет доверие как основу социального капитала, которая выполняет функцию воспроизводства социальной структуры, ускоряет процессы социального обмена и способствует интеграции общества [7]. Кроме того, исследователи замечают, что в современном рыночном обществе экономическое развитие во многом обусловлено моральной составляющей общества и доверием, в частности. Ю. В. Веселов отмечает, что современное доверие производится и воспроизводится экономическими структурами (структурами обмена, рынка, стоимости и денег), в связи с чем связь экономики (рынка) и доверия гораздо более сложная, чем это понимается в экономической и социальной науке [8]. Н. Луман отмечал, что доверие делает мир более понятным и менее сложным, создавая ощущение надежности и предсказуемости, а также снижает чувство опасности и стабилизирует социальные связи [5]. В трехфакторной модели Р. Патнэма развитие социального капитала также основывается на доверии, общих нормах и социальных связях [9]. Доверие в данной модели рассматривается как основа надежности и устойчивости развития всей системы и основа эффек-

тивного взаимодействия в современном обществе. П. Бурдье и Дж. Коулмен отмечали, что доверие в современном обществе становится одним из самых важных факторов социальной интеграции общества, потенциала солидарности и развития социального капитала, где маркерами выступают общие, понятные и принимаемые ценности [10].

В научной литературе выделяют различные сферы применимости категории доверия. Например, в бизнесе доверие в деловых отношениях способствует развитию экономики, доверие в межличностных отношениях — стабильности и прогрессу, а доверие к институтам — становлению гражданского общества. Р. Коуз предположил, что снижение уровня доверия приводит к росту издержек во всех сферах жизнедеятельности общества, а рост доверия, в свою очередь, способствует снижению издержек и росту благосостояния [11]. В некоторых исследованиях рассматривается связь между конкурентоспособностью, состоянием институционального доверия и межличностным доверием. В эмпирическом исследовании Н. Я. Калюжновой выявлено, что низкий уровень конкурентоспособности экономики, качество и уровень институционального доверия достаточно тесно связаны с низким уровнем межличностного доверия в обществе [12].

В то же время доверие является фундаментальным аспектом информационно-компьютерных социальных взаимодействий. Отношения в Интернете строятся на доверии, потому что пользователи полагают, что другой пользователь сети будет действовать по предсказуемому сценарию [13]. А. Киран и П. Вербек отмечают, что вместо того, чтобы с недоверием относиться к технологиям, сложные связи между человечеством и технологией побуждают нас развивать способность активно доверять себя технологии [14].

Текущее и будущее технологическое развитие зависит от двух основных факторов: развития технологии, определяемое уровнем технологических знаний, и адаптации и принятия технологии обществом [13]. Некоторые исследователи отмечают, что доверие к информационным технологиям (ИТ) очень схоже с доверием в межчеловеческих отношениях, разница только в объекте доверия. В случае с доверием к ИТ объектом доверия выступает не конкретный человек или группа лиц, а особая технология или технологии. Независимо от того, является ли объект доверия другим человеком или информационной технологией, один доверяет другому в той степени, в которой он решает зависеть от другого, и примиряет страхи, желая стать уязвимым для другого, не контролируя другого [14]. Доверие к информационным технологиям является важной концепцией, так как на сегодняшний день люди полагаются на ИТ гораздо больше, чем когда-либо прежде.

В современном мире люди совместно формируют себя через отношения, которые у них складываются с технологиями [15]. Так, В. Фогг разработал приложения, навязывающие пользователям возможную форму поведения. Автор отмечает уникальную пригодность мобильных устройств для доверия, так как они являются нашими близкими («мы женимся на них»), они являются вездесущими, и они обладают замечательными возможностями [16].

Доверие системе является также фактором убеждения. Разработчики интернет-порталов учитывают такие функции как надежность, опыт, авторитет, чувство реальности, одобрение и т. д. Система поддержки доверия не только повышает ее уровень, но также влияет на полезность системы и обеспечивает связь пользова-

теля сети с реальным миром. Доверие, кажется, основано на развитии ожиданий, которые продолжают быть встречными. Отсутствие полной предсказуемости технологии не означает, что доверие, надежность и ответственность полностью несовместимы с технологией. Фактически доверие к технологии является формой доверия людям, которые проектируют и создают технологические артефакты [15].

В научной литературе выделяются разные подходы к достижению доверия в зависимости от системы. Например, в государственных информационных системах таким подходом является выполнение установленных процедур аттестации объектов информатизации по требованиям безопасности, а в бизнес-процессах широко используются процедуры аудита информационной безопасности [17]. Такие аспекты доверия как неотказуемость или придание юридической значимости электронному документообороту достигаются за счет использования различных видов электронной подписи.

Исследовательский интерес также направлен на изучение факторов, которые влияют на доверие к ИТ. Так, группа ученых из Грузии эмпирически проверила модель доверия к ИТ-артефактам [18]. В результате исследования было выявлено, что во многом доверие пользователей к ИТ определяется визуальной привлекательностью и навигационной структурой той или иной технологии. Кроме того, в результате сравнения доверия потенциальных пользователей Франции и Америки к технологиям мобильной коммерции было выявлено прямое влияние культуры на доверие к ИТ.

Отмечается, что риск и доверие являются немаловажными факторами в принятии пользователями электронных услуг. Д. Моу, Д. Шин и Д. Кохен провели метаанализ 67 эмпирических исследований, направленных на изучение влияния доверия и восприятия риска пользователями электронных услуг [19]. Полученные данные подтвердили, что доверие и риск важны для принятия электронных услуг, но доверие оказывает гораздо больший эффект. Авторы отмечают, что эффект влияния доверия был смягчен такими факторами, как исследуемая группа потребителей, тип электронных услуг и объект доверия. Данные метаанализа поддерживают причинную логику, которая позиционирует доверие как предшествующее восприятию риска. Риск частично опосредует влияние доверия на получение электронных услуг.

Доверие к информационным технологиям также рассматривается с точки зрения их использования в образовательном процессе. В частности, отмечается, что учителя не всегда доверяют информационным технологиям и осознают их потенциал для сферы образования [1]. В то же время среди учащихся активно появляются новые образцы коммуникации и новые типы отношений. Образование становится сложной коммуникационной системой, в которой все большее значение приобретают не только уровень и качество получаемых знаний и информации, но и используемые каналы их передачи, искажение и интерпретация, обеспечение необходимой скорости передачи и получения сообщений, наличие обратной связи. Коммуникативность как свойство социальной реальности представляет собой совокупность условий, обеспечивающих возможность установления диалога, взаимодействия между субъектами информационного процесса [20].

Маклюэн обратил внимание на то, что не только содержание, но и сама структура коммуникации влияют на общество и его культуру. Поставив в центр внима-

ния способ общения (устный, письменный, «телевизионный»), Маклюэн представил историю общества как историю коммуникации [21; 22]. Хабермас, анализируя эволюцию современного общества, определяет его как общество модернового типа, которое функционирует на стыке системы (капиталистического способа производства) и жизненного мира, при этом сферы экономики и пространство жизненного мира переплетаются таким образом, что формирование нормативных механизмов социального управления определяется взаимодействием данных подсистем [23]. Эти идеи также разделял Д. Томпсон [24], который изучал роли массовой коммуникации в обществе: изменение и сохранение традиции, трансформация способов контроля и понятий публичного и приватного, влияние на конструирование индивидуальной идентичности, участие в глобализации и т. д.

В условиях информатизации и компьютеризации социальной реальности наличие налаженных каналов трансляции и репродуцирования информации становится неотъемлемым условием коммуникации. В системе современного образования все компоненты между собой тесно взаимосвязаны, потому что коммуникация в ней представляет один из достаточно сложных видов всеобщей связи. Изучение процессов коммуникации в современном образовании дает возможность обеспечить интенсификацию учебного процесса и использовать научный потенциал коммуникативности в конкретной учебной ситуации, что позволяет вести диалог об информатизации системы образования [25].

Доверие к информационным технологиям в работах зарубежных исследователей также рассматривается в контексте «виртуальных» форм организаций и как под воздействием новых технологий выстраиваются отношениями между руководителями организации, сотрудниками и другими стейкхолдерами. Л. Бреннан и В. Джонсон анализируют, как доверие к новым технологиям влияет на управление удаленными работниками и на выстраивание виртуальных отношениях с другими организациями и клиентами [26].

Часть исследований направлена на изучение доверия информационным технологиям с точки зрения безопасности. Л. А. Грищенко отмечает, что основной задачей управления безопасностью ИТ является обеспечение приемлемого уровня доверия [27]. Правообладатели, связанные с системой ИТ, получат обоснованную уверенность в том, что оцениваемый объект будет функционировать в соответствии с намеченным и утвержденным планом, с приемлемым риском. С точки зрения безопасности это означает уверенность в осуществлении оцениваемым объектом принятой политики безопасности.

В то же время отмечается, что новые технологии создают новые возможности манипулирования, общения и взаимодействия, которые не всегда могут быть однозначны и могут приводить к росту недоверия в обществе [2]. Социальные связи в сети приводят к изменению образа жизни, переводя людей в категорию пользователей и предоставляя альтернативные варианты осуществления различных видов социальной активности, присущих им в физической реальности. Социальная активность в виртуальном пространстве приводит к киберсоциализации пользователей, трансформации их жизненных установок, их ценностно-смыслового восприятия реальности, появлению новых интересов и жизненных приоритетов, нового запроса на доверие к собеседнику и к открытости институтов гражданского общества.

Систематизируя выявленные в ходе анализа научных публикаций тенденции, можно выделить ряд параметров, характерных для изучения доверия к информационным технологиям и доверия в сфере онлайн-образования.

Говорить о доверии к информационным технологиям в обществе можно, когда мы наблюдаем:

— трансформации социальных процессов;
— формирование новых нормативных механизмов;
— выстраивание виртуальных отношений;
— существование новых манипулятивных технологий.

Доверие к образовательным технологиям есть, когда мы констатируем:

— качество знаний;
— налаженные каналы коммуникации;
— интенсификация процесса обучения;
— адаптация и принятие пользователями;
— доверие к системе образования в целом.

Для изучения отношения пользователей к информационным технологиям в сфере образования было проведено исследование среди жителей Петербурга.

Методология и методика исследования

Исследование проведено с опорой на идеи подхода SCOT (от англ. The Social Construction of Technology — социальное конструирование технологии). Базируясь на данном подходе, авторы сделали предположение об участии пользователей в тех или иных формах электронного обучения, а также о формировании киберсоциального доверия в области онлайн-образования на основе оценки данного опыта.

В рамках исследования было предложено базовое определение, согласно которому под киберсоциальным доверием понимается уверенность пользователя в предсказуемости «поведения» цифровых технологий, их надежности, в готовности пользователей делегировать ряд задач различным программно-техническим системам. В сфере онлайн-образования киберсоциальное доверие проявляется в социотехническом комплексе человеко-компьютерного взаимодействия, на формирование которого оказывают воздействие оценки предыдущего опыта по взаимодействию в сети, а также уровень доверия межличностному общению и социальным институтам, участвующим в системе онлайн образования.

В соответствии с этим, внимание исследователей было нацелено на следующие параметры электронных коммуникаций в сфере образования:

— использование информационных технологий, самооценка пользователей как опытных/неопытных;
— опыт использования различных форм онлайн-обучения, его оценка пользователями;
— субъективное доверие к формам онлайн-образования;
— различие между возрастными группами пользователей в уровне доверия.

С целью выявления маркеров социального доверия и недоверия к новым технологиям был проведен опрос жителей Петербурга. Использовалась техника личного

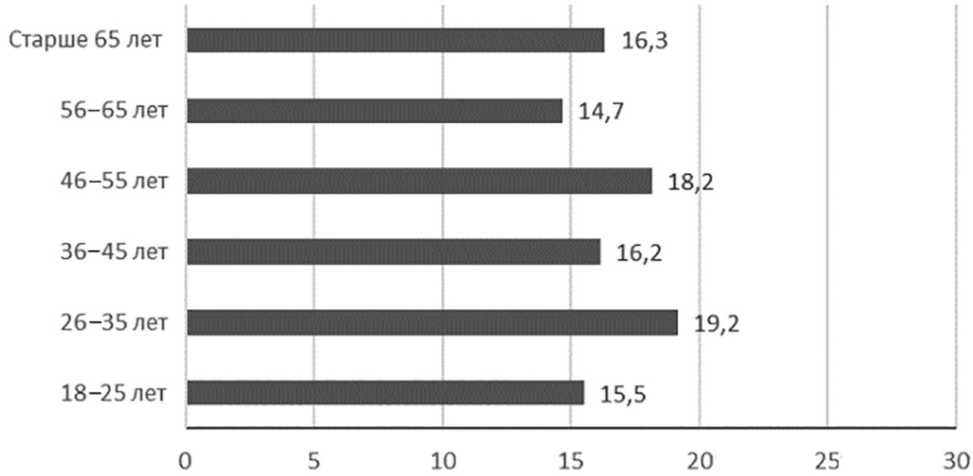

Рис. 1. Распределение респондентов по возрасту (в %), 2019 г.

И с т о ч н и к: авторские данные.

интервью. В качестве места проведения исследования были выбраны 6 многофункциональных центров (МФЦ), расположенных в самых густонаселенных районах Санкт-Петербурга. Для расчета выборочной совокупности использовались данные о численности населения, его возрастном и половом составе на сайте Управления федеральной службы статистики по Санкт-Петербургу и Ленинградской области. На основании данных о численности населения в целом был рассчитан размер выборки — 600 респондентов (выборка репрезентативная для населения Петербурга старше 18 лет). Ошибка выборки не превышает 5 %, уровень достоверности составил 95 %. Исходя из размера выборочной совокупности, была составлена квотная выборка по полу и возрасту. Население Санкт-Петербурга было разделено на шесть возрастных групп: 18–25, 26–35, 36–45, 46–55, 56–65 и старше 65 лет. В каждой возрастной группе было рассчитано процентное соотношение мужчин и женщин. Опрос проводился в мае 2019 года.

Всего в опросе приняли участие 600 человек — 46,3 % мужчин и 57,3 % женщин. Возрастная структура была представлена на рис. 1.

Дифференциация опрошенных по сферам занятости выглядит следующим образом: служащий/специалист (45 %), неработающий пенсионер (16 %), бизнесмен / руководитель высшего или среднего звена (11 %), учащийся/студент (11 %), рабочий/охранник/водитель (8 %), временно безработный (3 %), домохозяйка (3 %), другие сферы (3 %). Опросный лист составлен в форме вопросов-утверждений о личном опыте использования информационных технологий в коммуникации с органами власти, по вопросам взаимодействия в сфере образования, здравоохранения, а также для сообщения с органами власти/управления/ администрацией в сети. Для градации вариантов ответов использовалась шкала Лайкерта. В данной статье приводятся результаты исследования, связанные с использованием информационных технологий и доверием к ним в сфере образования.

Для определения конструкта киберсоциального доверия проведен факторный анализ. Для факторного анализа отобрано 13 переменных из опроса, относящихся

к тем или иным аспектам онлайн-доверия. При этом авторы не ограничились только вопросами, связанными с онлайн-образованием.

Для анализа использовался метод главных компонент. Критерием отбора компонентов выступал показатель собственного значения (eigenvalue) по критерию Кайзера: для анализа отбирались только факторы с собственным значением выше одного. В качестве методики вращения использован ортогональный метод Варимакс (Varimax method). Для оценки адекватности имеющихся данных для факторного анализа использовалась мера адекватности выборки Кайзера-Мейера-Олкина (КМО), а также критерий сферичности Бартлетта.

Результаты указанных выше тестов демонстрируют пригодность данных для факторного анализа: значение меры КМО составляет 0,812 (при допустимых значениях от 0,5 до 1), критерий Барлетта демонстрирует значимость 0,000 (хи-квадрат 3793,505, степени свободы 78). Все переменные значимо и положительно коррелируют друг с другом (значимость всех коэффициентов — на уровне 0,01), что указывает на то, что доверительное отношение к какому-либо аспекту деятельности онлайн с большой вероятностью связано с повышением доверия к другим аспектам.

На основании полученных эмпирических данных базовое определение было подвержено корректировке.

Результаты исследования

В самом начале опроса респондентов спрашивали об их опыте использования информационных технологий (ИТ) и Интернета. Данный блок вопросов был ориентирован на выявление потенциального сегмента целевой аудитории, который уже сейчас обладает необходимыми навыками для использования технологий онлайн-обучения.

Результаты опроса продемонстрировали, что большая часть респондентов (42,5 %) являются активными пользователями интернета. Однако к категории продвинутых пользователей себя отнесли только 23,3 % опрошенных. Большая часть респондентов, уверенно чувствующая себя при работе с Интернетом, относится к возрастной категории 18–25 лет (54,8 %). В то время как наименьшее количество опытных пользователей Интернета относится к возрастным группам 56–65 лет (3,4 %) и старше 65 лет (5,1 %). Мотивы для использования того или иного интернет-ресурса по мере популярности расположились в порядке убывания следующим образом:

— личная уверенность в безопасности своих данных,
— существенная экономия времени по сравнению с офлайн-процедурой,
— невозможность реализации потребности вне Интернета,
— денежная экономия,
— личный предшествующий позитивный опыт,
— рекомендация родственников, коллег, друзей.

В ходе опроса респондентам было предложено оценить несколько утверждений, касающихся форм онлайн-обучения, по шкале от 1 до 5 (где 1 — полностью не согласен, а 5 — полностью согласен). Большая часть респондентов отметили, что они не используют различные возможности онлайн-обучения (43,8 %) (см. рис. 2). Только 11,2 % опрошенных указали, что активно используют формы обучения

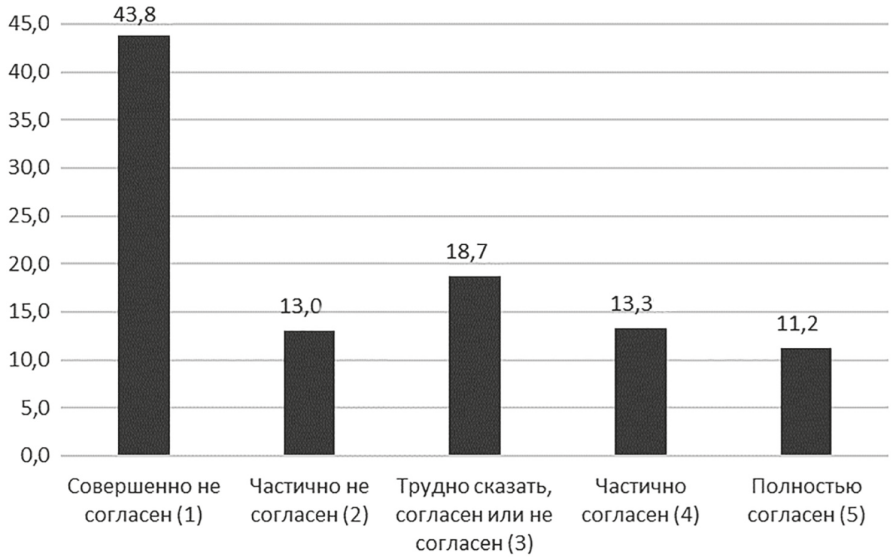

Рис. 2. Распределение ответов на вопрос «Я активно использую формы онлайн-обучения (вебинары, семинары, онлайн-курсы и другое)» по шкале от 1 до 5, 2019 г.

И с т о ч н и к: авторские данные.

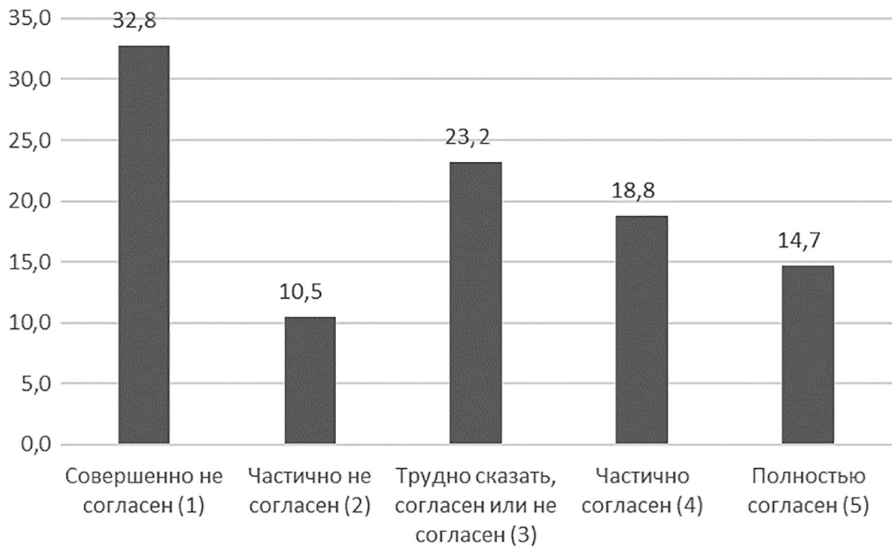

Рис. 3. Распределение ответов на вопрос «Я оцениваю свой опыт получения онлайн- обучения как позитивный» по шкале от 1 до 5, 2019 г.

И с т о ч н и к: авторские данные.

в Интернете. Анализ возрастных групп продемонстрировал, что большая часть активных пользователей относится к возрастной группе 26–35 лет (20,9 %).

Результаты опроса показали, что 33 % опрошенных жителей склонны оценивать свой опыт получения онлайн-обучения как позитивный (рис. 3). Бóльшая часть негативных оценок была оставлена представителями возрастных групп 56–

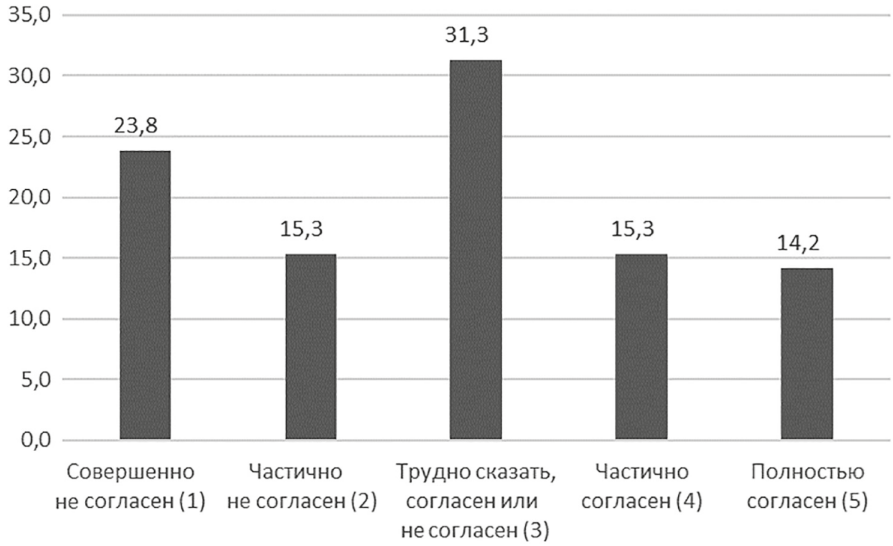

Рис. 4. Распределение ответов на вопрос «В целом я доверяю взаимодействию через Интернет для получения онлайн-обучения» — по шкале от 1 до 5, 2019 г.

И с т о ч н и к: авторские данные.

65 лет (53,4 %) и старше 65 лет (71,4 %). Наибольшую долю респондентов, рассказавших о позитивном опыте, составили представители самой молодой возрастной категории 18–25 лет (33,3 %).

Для того чтобы определить уровень доверия технологиям онлайн-обучения, респондентам было предложено оценить по шкале от 1 до 5 утверждение «В целом, я доверяю взаимодействию через Интернет для получения онлайн-обучения». Стоит отметить, что здесь не прослеживается тенденций к доверию или полному недоверию к таким технологиям. Большая часть опрошенных выбрали вариант нейтральной оценки (31,3 %), что свидетельствует о том, что граждане имеют потенциальный интерес к формам обучения в Интернете, но относятся к ним настороженно или не знакомы с примерами позитивного опыта и преимуществ онлайн-обучения (рис. 4).

Анализируя распределение ответов по возрастным группам, стоит отметить, что недоверие онлайн-формам обучения выразили преимущественно представители старших возрастных групп 56–65 лет (43,2 %) и старше 65 лет (50 %) (рис. 5). Представители более молодых групп демонстрируют скорее заинтересованность в онлайн-обучении, о чем свидетельствует невысокий процент негативных оценок.

Кроме того, в ходе исследования был оценен общий уровень доверия респондентов к общению с другими горожанами, а также уровень доверия городским властям. По данным опроса, только 23 % считают, что большинству людей в целом можно доверять. Почти треть (29 %) доверяют государственным и муниципальным властям. Своему интернет-провайдеру доверяют 35 %, российским компаниям, предлагающим товары и услуги в Интернете, — 32 %, а иностранным компаниям — 33 %. В целом, администрациям российских социальных сетей доверяют 24 % опрошенных, такие же цифры были отмечены и для иностранных социальных сетей.

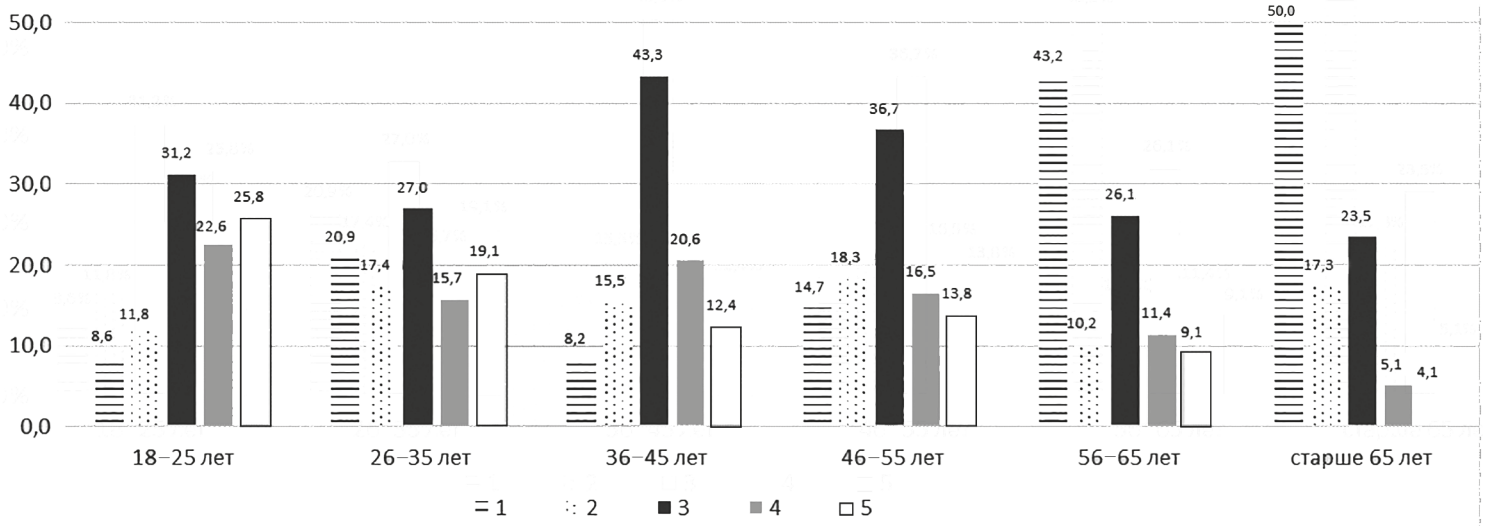

Рис. 5. Распределение ответов на вопрос «В целом я доверяю взаимодействию через Интернет для получения онлайн-обучения», 2019 г.
И с т о ч н и к: авторские данные.

В ходе опроса было обнаружено позитивное отношение респондентов к Интернету. Например, с утверждением «Я считаю, что Интернет представляет больше вреда, чем пользы» не согласны 77 %. По мнению опрошенных (75 %), обеспечение безопасности пользователей в Интернете — это прерогатива органов государственной власти. При этом меры, укрепляющие безопасность в Интернете, не должны уменьшать его открытость и свободу — так считают 77 % респондентов. Текущие меры, предпринимаемые государством по обеспечению безопасности в Интернете, считают достаточными только 44 %.

Стоит отметить, что 17 % опрошенных рассказали о том, что с ними произошли разного рода инциденты при получении онлайн-услуг в течение 2019 года. Как моральный ущерб такой инцидент оценили 10 %, и почти столько же заявили о материальном ущербе (8 %). Чуть более 15 % рассказали о подобных инцидентах при использовании интернет-банкинга, и 12 % рассказали о случаях хищения персональных данных либо иных нарушениях частной жизни через Интернет. При этом о существовании «горячих линий» и других каналов обратной связи для информирования соответствующих уполномоченных организаций об угрозах безопасности в интернете или о реально происшедших инцидентах знают 40 % опрошенных. Чуть более половины (55 %) знают о мерах, принимаемых органами власти для снижения угроз безопасности в Интернете и в сетях мобильной связи, включая защиту своих персональных данных. Примерно столько же опрошенных знают механизмы проверки безопасности интернет-ресурса и используют их.

Результаты исследования показывают, что уровень осведомленности о надежности интернет-коммуникации и возможностях защиты безопасности в сети в целом превалирует над выявленным процентом пользователей, понесших разного рода издержки от подобной коммуникации.

В результате факторного анализа было отобрано три фактора, определяющих категорию киберсоциального доверия, с собственным значением выше 1. Вместе они покрывают 64,4 % выборки, что является достаточно высоким показателем: из них первый компонент покрывает около 24,7 % выборки, второй — около 23 % и третий — около 16,5 %. Для наглядности в факторной матрице (табл. 1) приведены только те значения факторной нагрузки переменных, которые равны или выше 0,4, что означает достаточно высокую степень взаимосвязи данной переменной и фактора.

Первый фактор группирует переменные, относящиеся к доверию определенным организациям, осуществляющим деятельность в Интернете: российским и зарубежным интернет-компаниям, администрации социальных сетей, а также отчасти интернет-провайдеру (хотя факторная нагрузка последнего не такая значительная). С долей условности этот фактор можно обозначить как институциональное доверие.

Второй фактор объединяет переменные, которые прежде всего нацелены на построение доверительных отношений между различными акторами в Интернете. В частности, здесь высока факторная нагрузка таких показателей, как доверие к общению с гражданами и представителями власти в социальных сетях и на интернет-площадках, доверие к онлайн-платежам и доверие к получению электронных услуг через систему идентификации. Этот фактор условно можно обозначить как транзакционное доверие, т. е. доверие, обеспечивающие прозрачные и честные

правила взаимодействия между людьми, между гражданами и государством, а также в процессе обмена ресурсами (в том числе платежными средствами). Вместе с тем, следует отметить, что в данном факторе особенно высока роль государства как контрагента взаимодействия (в силу того, какие вопросы — переменные имеют большую факторную нагрузку).

Таблица 1. **Матрица компонентов (с учетом вращения)**

Переменные	Институциональное доверие	Транзакционное доверие	Информационное доверие
Доверие иностранным компаниям	0,851		
Доверие российским компаниям	0,834		
Доверие администрации иностранных социальных сетей	0,800		
Доверие администрации российских социальных сетей	0,731		
Доверие интернет-провайдеру	0,591	0,477	
Доверие органам государственной и муниципальной власти в социальных сетях		0,843	
Доверие органам государственной и муниципальной власти для взаимодействия в Интернете		0,755	
Доверие людям в социальных сетях		0,753	
Доверие электронной идентификации		0,666	
Доверие онлайн-банкингу		0,439	
Доверие услугам электронного здравоохранения			0,836
Доверие информации о здравоохранении в Интернете			0,776
Доверие услугам электронного обучения			0,758

И с т о ч н и к: авторские данные.

Наконец, третий фактор объединяет такие переменные, как доверие к онлайн-образованию, а также к получению услуг и информации в области здравоохранения. Объединяет эти переменные то, что здесь гражданин выступает как потребитель услуги, в основном заключающейся в получении информации — новых знаний или консультации, и ожидает ее полноты и достоверности. В связи с этим третий фактор можно обозначить как информационное доверие, хотя и с оговоркой, что речь идет об определенном наборе услуг.

Таблица 2. **Корреляционная матрица взаимосвязи факторов и переменных**

Переменные	**Институциональное доверие**	**Транзакционное доверие**	**Информационное доверие**
Женщины	0,030 (,469)	–0,044 (,286)	0,007 (,863)
Мужчины	–0,030 (,469)	–0,044 (,286)	0,007 (,863)
Возраст*	**0,108 (,008)**	**0,125 (,002)**	**0,251 (,000)**
Образование	0,051 (,216)	**0,131 (,001)**	**0,102 (,012)**
Активный интернет-пользователь	0,111 (,007)	**0,279 (,000)**	**0,223 (,000)**
Активный пользователь (получение гос. и мун. услуг)	**0,138 (,001)**	**0,350 (,000)**	**0,227 (,000)**
Активный пользователь (обращения в органы власти)	0,080 (,050)	**0,273 (,000)**	**0,289 (,000)**
Активный пользователь (соц. сети)	**0,211 (,000)**	**0,295 (,000)**	**0,238 (,000)**
Активный пользователь (интернет-банкинг)	**0,167 (,000)**	**0,212 (,000)**	**0,347 (,000)**
Активный пользователь (покупки, платежи в Интернете)	**0,165 (,000)**	**0,228 (,000)**	**0,344 (,000)**
Активный пользователь (услуги здравоохранения онлайн)	**0,109 (,000)**	**0,238 (,000)**	**0,442 (,000)**
Активный пользователь (услуги образования онлайн)	**0,152 (,000)**	**0,130 (,000)**	**0,339 (.000)**
Уровень генерализованного доверия	**0,227 (,000)**	**0,113 (,006)**	**0,162 (,000)**
Уровень доверия к органам власти	**0,363 (,000)**	**0,478 (,000)**	–0,006 (,887)
1) *Возраст кодируется в обратном порядке (младшая возрастная когорта получает более высокое значение) 2) значимость указана в скобках, жирным отмечены значимые корреляции на уровне ,001 и ,005			

И с т о ч н и к: авторские данные.

На следующем этапе был проведен корреляционный анализ полученных факторов и других переменных из опроса: (1) социально-демографических характеристик; (2) опыта использования инструментов и (3) показателей офлайн-доверия. Предварительный корреляционный анализ Пирсона (табл. 2) демонстрирует, что гендерные различия не играют значимой роли, в то время как определенную роль могут играть возраст и образование. Хотя коэффициент корреляции этих пере-

менных невелик, молодые люди и граждане с более высоким уровнем образования, в целом, склонны больше доверять новым технологиям. Положительно на факторы доверия влияет также факт активного использования интернета: как в целом, так и конкретных онлайн-инструментов: для первого фактора наиболее значимо пользование социальными сетями, для второго — государственными сервисами и социальными сетями, для третьего — телемедициной, онлайн образованием и финансово-коммерческими сервисами. Наконец, корреляционный анализ демонстрирует взаимосвязь онлайн- и офлайн-доверия, а именно значимую корреляцию между выявленными факторами, с одной стороны, и уровнями генерализованного и институционального доверия.

Выводы и обсуждение результатов

В целом, факторный и корреляционный анализ продемонстрировали валидность полученных данных для последующего глубокого исследования. На основе полученных переменных были построены обобщенные факторы, составляющие конструкт онлайн-доверия, а также получены предварительные данные о том, как эти факторы соотносятся с социально-демографическими характеристиками респондентов, их степенью пользования онлайн-технологиями и уровнем офлайн-доверия к гражданам и власти.

Таким образом, представленная факторная модель позволяет выявить некоторые теоретические ожидания относительно того, из каких компонентов может складываться киберсоциальное доверие, помимо собственно доверия к технологиям или степени владения ими. К таким компонентам можно отнести: (1) институциональное доверие к организациям, осуществляющим свою деятельность в Интернете; (2) транзакционное доверие к взаимодействию с другими акторами онлайн (прежде всего — к государству); (3) информационное доверие относительно полноты, качества и достоверности информации (услуг в области информации).

По результатам исследования было выявлено преобладание интернет-пользователей среди опрошенных, а также рост уверенности в использовании новых технологий у более молодых групп населения. Личные мотивы (экономия времени и денег), а также уверенность в безопасности интернет коммуникации являются движущими факторами к использованию онлайн услуг в различных сферах.

Анализ включенности в онлайн-обучение также продемонстрировал востребованность этих технологических решений в группе молодежи (люди до 35 лет). При этом жители Петербурга оценили свой личный опыт как позитивный и негативный практически поровну. Принимая во внимание, что личный опыт был выделен как ключевой мотив для включения в интернет-среду, можно сделать вывод о существовании барьеров в этом направлении. Эти тенденции подтверждают также данные об оценках доверия пользователей к онлайн-обучению.

По данным исследования, уровень киберсоциального доверия в области услуг онлайн-обучения не превысил 35 % респондентов в различных возрастных группах. На данном этапе формированию устойчивой уверенности у пользователей в предсказуемости и надежности работы онлайн-систем образования препятствуют, с одной стороны, недостаточная цифровая включенность людей старшей возрастной категории в процессы получения таких услуг, а с другой — кейсы негатив-

ного опыта, инциденты с персональными данными, атаки на системы финансов, о которых рассказали опрошенные, опираясь на собственный опыт.

Возвращаясь к имеющимся данным о бурном росте рынка онлайн-образования, стоит подчеркнуть возможность снижения недоверия информационным технологиям в данной области за счет разработки программ обучения людей старших возрастных групп как компьютерным навыкам, так и прохождению образовательных курсов и программ повышения квалификации онлайн. В связи с повышением пенсионного возраста в Российской Федерации и необходимостью пожилых людей оставаться востребованными на рынке труда, возможности онлайн-образования становятся все более актуальными.

Результаты, представленные в данной статье, отражают выводы по одному из направлений изучения киберсоциального доверия. Дальнейшее развитие исследовательского направления авторы видят в построении многофакторной модели киберсоциального доверия, затрагивающей онлайн-взаимодействие в сферах получения государственных услуг, экономики, образования, здравоохранения и других.

Литература

1. *Черепаняк-Вальчак М., Пежицка Э.* Доверие учителей и учащихся к применению современных технологий в процессе обучения // Научные ведомости Белгородского государственного ун-та. Серия: Гуманитарные науки. 2014. №6 (177). С. 294–299.
2. *Тульчинский Г. Л., Лисенкова А. А.* Проблема доверия и современные информационно-коммуникативные технологии // Российский гуманитарный журнал. 2016. № 2. С. 233–242.
3. *Lipset S. M., Scheider W.* The confidence gap: Business, labor and government in the public mind. New York: The Free Press, 1983.
4. *Gibb J. R.* Trust: A new view of personal and organizational development. Los Angeles: The Guild of Tutors Press, 1978.
5. *Luhmann N.* Vertrauen. Ein Mechanismus der Reduktion sozialer Komplexität. Stuttgart: Lucius&Lucius, 1973.
6. *Misztal B.* Trust in Modern Societies. Cambridge: Polity Press, 1986.
7. *Fukuyama F.* Trust: The Social Virtues and the Creation of Prosperity. New York: Free Press, 1995.
8. *Веселов Ю. В.* Доверие и справедливость: моральные основания современного экономического общества. М.: Аспект Пресс, 2011.
9. *Putnam R. D.* Bowling alone: The Collapse and Revival of American Community. New York: Simon & Schuster, 2000.
10. *Coleman J.* Foundations of social theory. Cambridge, Mass.: Belknap Press of Harvard University Press, 1990.
11. *Коуз Р.* Проблема социальных издержек. М.: Экономика, 1978.
12. *Калюжнова Н. Я.* Экономика недоверия: роль социального капитала в России // Журнал институциональных исследований. 2012. Т. 4. № 2. С. 74–82.
13. *Mayer R. C., Davis J. H., Schoorman F. D.* An Integrative Model of Organizational Trust // Academy of Management Review. 1995. Vol. 20, no. 3. P. 709–734.
14. *Kiran A. H., Verbeek P.-P.* Trusting Our Selves to Technology // Knowledge, Technology & Policy. 2010. Vol. 23, no. 3–4. P. 409–427.
15. *Дедюлина М. А.* Доверие в мире информационно-компьютерных технологий // Манускрипт. 2016. № 12-3 (74). С. 54–56.
16. *Fogg B. J.* Persuasive Technology: Using Computers to Change What We Think and Do. San Francisco: Morgan Kaufmann, 2002.
17. *Дураковский А. П., Кондратьева Т. А., Лаврухин Ю. Н., Петров В. Р.* О доверии в информационных системах на основе Интернет-технологий // Безопасность информационных технологий. 2015. Т. 22. № 1. С. 25–28.
18. *Vance A., Elie-Dit-Cosaque C., Straub D. W.* Examining Trust in Information Technology Artifacts: The Effects of System Quality and Culture // Journal of Management Information Systems. 2008. Vol. 24, no. 4. P. 73–100.

19. *Mou J., Shin D-H, Cohen J. F.* Trust and risk in consumer acceptance of e-services // Electronic Commerce Research. 2017. Vol. 17, no. 2. P. 255–288.

20. *Лысикова Н. П.* Социальные коммуникации в системе современного образования. Саратовский государственный университет: официальный сайт. URL: http//www.sgu.ru/sites/default/files/textdocsfiles/2013/07/15/lysikova_0.pdf (дата обращения: 15.10.2019).

21. *McLuhan M.* The Gutenberg Galaxy. London: Routledge and Kegan Paul, 1962.

22. *McLuhan M.* Understanding media: The extensions of man. New York and Scarborough, Ontario: McGraw Hill, 1964.

23. *Хабермас Ю.* Моральное сознание и коммуникативное действие / пер. с нем. СПб.: Наука, 2000.

24. *Thompson J. B.* The media and modernity: A social theory of the media. Cambridge: Polity Press, 1995.

25. *Симонова М. М.* Проблемы и перспективы коммуникации в современном образовании // Проблемы современного образования. 2019. № 1. С. 9–16.

26. *Brennan L. L., Johnson V. E.* Computer-mediated Relationships and Trust: Managerial and Organizational Effects. Hershey, PA: Information Science Publishing, 2007.

27. *Грищенко Л. А.* Оценка доверия к безопасности информационных технологий // Вопросы науки и образования. 2018. № 7 (19). С. 62–66.

Статья поступила в редакцию 7 ноября 2019 г.;
рекомендована в печать 9 апреля 2020 г.

Контактная информация:

Видясова Людмила Александровна — канд. соц. наук; bershadskaya.lyudmila@gmail.com
Тенсина Ярослава Дмитриевна — аналитик; tensina.yaroslava@gmail.com
Кабанов Юрий Андреевич — ст. преп., аналитик; ykabanov@hse.ru

The results of an empirical study of cyber-social trust among residents of St. Petersburg*

L. A. Vidiasova[1], *Ia. D. Tensina*[1], *Yu. A. Kabanov*[1,2]

[1] ITMO University,
49, Kronverksky pr., St. Petersburg, 197101, Russian Federation
[2] National Research University Higher School of Economics,
16, ul. Soyuza Pechatnickov, St. Petersburg, 190121, Russian Federation

For citation: Vidiasova L. A., Tensina Ia. D., Kabanov Yu. A. The results of an empirical study of cyber-social trust among residents of St. Petersbourg. *Vestnik of Saint Petersburg University. Sociology*, 2020, vol. 13, issue 2, pp. 236–254. https://doi.org/10.21638/spbu12.2020.208 (In Russian)

Trust is an important element in building an information society, however, the increasingly widespread dissemination and use of technology is now accompanied by the influence of negative factors and fears related to the insecurity of certain data transmission channels and much discussed by cyberattacks, government pressure on civilian structures, and also uncertainty about the rules and communication standards of a new type. The article presents the results of an empirical study of the attitude of St. Petersburg residents to the use of digital technologies and identifies the level of trust in the Internet and interpersonal communication. A survey of 600 respondents was conducted in May 2019 (a sample representative of the population of St. Petersburg over 18 years old, the sampling error does not exceed 4%, the confidence level was 95%).

* The study was performed with financial support by the grant from the Russian Foundation for Basic Research (RFBR) (project no. 18-311-20001): "The Research of cybersocial Trust in the context of the use and refusal of information technology".

According to the results, the prevalence of Internet users among the respondents was revealed, as well as an increase in trust in new technologies among younger groups of the population. The article presents the detailed results of the study dedicated to user experience in the field of online learning. The analysis of social inclusion in online learning has also demonstrated the relevance of these technological solutions in the group up to 35 years old. At the same time, assessments of personal experience were divided almost equally into positive and negative between residents of St. Petersburg. Based on the factor model, 3 components were identified that make up the category of cyber-social trust: institutional trust in organizations operating on the Internet; transactional trust in interacting with other online actors (primarily to the state); information trust regarding the completeness, quality and reliability of information (information services).

Keywords: social trust, trust in information technology, online education, Internet users, opinion, poll.

References

1. Cherepanyak-Valchak M., Pezhitska E. The trust of teachers and students in the use of modern technologies in the learning process. *Nauchnie vedomosti Belgorodskogo gosudarstvennogo universiteta. Ser. Gumanitarnye nauki,* 2014, no. 6 (177), pp. 294–299. (In Russian)

2. Tulchinsky G. L., Lisenkova A. A. The problem of trust and modern information and communication technologies. *Rossiiskii Gumanitarnyi Zhurnal*, 2016, no. 2, pp. 233–242. (In Russian)

3. Lipset S. M., Scheider W. *The confidence gap: Business, labor and government in the public mind*. New York, Free Press, 1983.

4. Gibb J. R. *Trust: A new view of personal and organizational development.* Los Angeles, The Guild of Tutors Press, 1978.

5. Luhmann N. *Vertrauen. Ein Mechanismus der Reduktion sozialer Komplexität*. Stuttgart, Lucius & Lucius, 1973.

6. Misztal B. *Trust in Modern Societies*. Cambridge, Polity Press, 1986.

7. Fukuyama F. *Trust: The Social Virtues and the Creation of Prosperity*. New York, Free Press, 1995.

8. Veselov Iu.V. *Trust and justice: moral foundations of a modern economic society*. Moscow, Aspekt Press Publ., 2011. (In Russian)

9. Putnam R. D. *Bowling alone: The Collapse and Revival of American Community*. New York, Simon & Schuster, 2000.

10. Coleman J. *Foundations of social theory*. Cambridge, Mass., Belknap Press of Harvard University Press, 1990.

11. Coase R. *The problem of social costs*. Moscow, Ekonomika Publ., 1978. (In Russian)

12. Kalyuzhnova N. Ya. Economics of distrust: the role of social capital in Russia. *Zhurnal institutsional'nykh issledovanii,* 2012, vol. 4, no. 2, pp. 74–82. (In Russian)

13. Mayer R. C., Davis J. H., Schoorman F. D. An Integrative Model of Organizational Trust. *Academy of Management Review*, 1995, vol. 20, no. 3, pp. 709–734.

14. Kiran A. H., Verbeek P.-P. Trusting Our Selves to Technology. *Knowledge, Technology & Policy*, 2010, vol. 23, no. 3-4, pp. 409–427.

15. Dedyulina M. A. Trust in the world of information and computer technologies. *Manuskript*, 2016, vol. 74, no. 3, pp. 54–56. (In Russian)

16. Fogg B. J. *Persuasive Technology: Using Computers to Change What We Think and Do*. San Francisco, Morgan Kaufmann, 2002.

17. Durakovsky A. P., Kondratieva T. A., Lavrukhin Yu.N., Petrov V. R. About trust in information systems based on Internet technologies. *Bezopasnost' informatsionnykh tekhnologii,* 2015, vol. 22, no. 1, pp. 25–28. (In Russian)

18. Vance A., Elie-Dit-Cosaque C., Straub D. W. Examining Trust in Information Technology Artifacts: The Effects of System Quality and Culture. *Journal of Management Information Systems*, 2008, vol. 24, no. 4, pp. 73–100.

19. Mou J., Shin D-H, Cohen J. F. Trust and risk in consumer acceptance of e-services. *Electronic Commerce Research*, 2017, vol. 17, no. 2, pp. 255–288.

20. Lysikova N. P. Social communications in the system of modern education. *Saratovskii gosudarstvennii universitet, official website.* Available at: http//www.sgu.ru/sites/default/files/textdocsfiles/2013/07/15/lysikova_0.pdf (accessed: 15.10.2019). (In Russian)

21. McLuhan M. *The Gutenberg Galaxy*. London, Routledge and Kegan Paul, 1962.
22. McLuhan M. *Understanding media: The extensions of man*. New York and Scarborough, Ontario, McGraw Hill, 1964.
23. Habermas J. *Moral consciousness and communicative action*. St. Petersburg, Nauka Publ., 2000. (In Russian)
24. Thompson J. B. *The media and modernity: A social theory of the media*. Cambridge, Polity Press, 1995.
25. Simonova M. M. Problems and prospects of communication in modern education. *Problemy sovremennogo obrazovaniia,* 2019, no. 1, pp. 9–16. (In Russian)
26. Brennan L. L., Johnson V. E. *Computer-mediated Relationships and Trust: Managerial and Organizational Effects*. Hershey, PA, Information Science Publishing, 2007.
27. Grishenko L. A. Assessment of trust in information technology security. *Voprosy nauki i obrazovaniia,* 2018, no. 7 (19), pp. 62–66. (In Russian)

Received: November 7, 2019
Accepted: April 9, 2020

Authors' information:

Lyudmila A. Vidiasova — PhD in Sociology; bershadskaya.lyudmila@gmail.com
Iaroslava D. Tensina — Analyst; tensina.yaroslava@gmail.com
Yury A. Kabanov — Senior Lecturer, Analyst; ykabanov@hse.ru