RUDN Journal of Political Science. ISSN 2313-1438 (print), ISSN 2313-1446 (online) **2022 Vol. 24 No. 3 447–459**
Вестник Российского университета дружбы народов. Серия: ПОЛИТОЛОГИЯ http://journals.rudn.ru/political-science

DOI: 10.22363/2313-1438-2022-24-3-447-459

Научная статья / Research article

Феномен «цифрового доверия» и его влияние на становление цифрового правительства в России

С.Г. Чепелюк

Московский государственный университет имени М.В. Ломоносова, Москва, Российская Федерация

sergey.chepeliuk@yandex.ru

Аннотация. В условиях развития в России проекта цифрового правительства доверие к технологическим новшествам становится темой, характеризующей качество перемен и внедрения цифровых технологий в государственное управление. Цель исследования — определить значение фактора доверия со стороны граждан для успешной реализации концепции цифрового правительства и показать, насколько он учитывается при проведении соответствующих государственных технологических реформ. В ходе исследования был рассмотрен феномен «цифрового доверия», а также проведен контент-анализ основных государственных программных и аналитических документов по реализации концепции цифрового правительства на предмет отражения в них данного феномена. На основе проведенного исследования было описано влияние доверия на эффективность реализации возможностей цифрового правительства, выявлены основные принципы формирования доверия, такие как открытость системы цифрового правительства для граждан, безопасность и надежность электронных сервисов, выстраивание двусторонней коммуникации с гражданами. Хотя некоторые из данных принципов учитываются государственными органами при формировании цифрового и электронного правительства, однако на основе исследования можно сделать вывод об отсутствии внятной стратегии формирования «цифрового доверия» в российской политике, а также системы показателей уровня цифрового доверия и мер по его повышению. Данное обстоятельство, в свою очередь, может послужить серьезным барьером на пути цифровизации государственных услуг.

Ключевые слова: цифровое правительство, цифровое доверие, кибербезопасность, цифровые услуги, государственное управление

Для цитирования: *Чепелюк С.Г.* Феномен «цифрового доверия» и его влияние на становление цифрового правительства в России // Вестник Российского университета дружбы народов. Серия: Политология. 2022. Т. 24. № 3. С. 447–459. https://doi.org/10.22363/2313-1438-2022-24-3-447-459

The Phenomenon of "Digital Trust" in the Context of Digital Government in Russia

Sergey G. Chepelyuk

Lomonosov Moscow State University, Moscow, Russian Federation

sergey.chepeliuk@yandex.ru

Abstract. In recent years new digital technologies have become an integral part of daily life of civilians, including their interaction with government. Trust in innovation in the government sector became the most important feature of the relations between government and civilians. The main purpose of this research is to explore how the factor of civil trust influences the implementation of digital technologies in government. We studied new phenomenon — "digital trust" and made content analysis of the main programmatic and analytical documents on the realization of the digital government concept. Based on the research results, we described the impact of the trust on the digital government effectiveness, and defined the basic principles of trust building, such as openness of the digital government system for citizens, security and reliability of electronic services, two-way communication with citizens. However, Russia lacks a clear strategy on how to build "digital trust" to government services. This circumstance could become a barrier for government's digitalization in the future.

Keywords: digital government, digital trust, cybersecurity, digital services, public administration

For citation: Chepelyuk, S.G. (2022). The phenomenon of "digital trust" in the context of digital government in Russia. *RUDN Journal of Political Science*, 24(3), 447–459. (In Russian). https://doi.org/10.22363/2313-1438-2022-24-3-447-459

Введение

Начало XXI в. характеризовалось постепенным падением доверия населения к государственным институтам и политикам [West, West 2005: 40] по всему миру. Подобная тенденция прослеживалась и в России. Так, если брать последнее десятилетие, то устойчивое доверие у россиян вызывают только институт Президента и армия. Правительству же доверяет меньше половины россиян [Латов 2021: 173]. В данном контексте цифровизация государственного сектора была призвана повысить эффективность, результативность и открытость правительственных структур, что впоследствии должно было бы нивелировать накопившееся недоверие к государственным структурам и государственным служащим. Однако чуда не произошло. Особенно вопрос доверия граждан по отношению к государству обострился в период пандемии COVID-19, во время которой многие процессы взаимодействия между государством, обществом и бизнесом перешли в цифровую среду. Именно доверие напрямую влияло на восприятие принимаемых государством мер по борьбе с распространением пандемии и готовность идти на личные ограничения в угоду общественному здоровью [Balog-Way, McComas 2020: 839]. Однако, по данным некоторых исследований, уровень доверия к государственной власти за время

пандемии упал более чем у 60 % россиян[1]. По данным ВЦИОМ, за время пандемии деятельность правительства одобряло менее 30 % россиян[2]. При этом исследователи отмечают, что за период пандемии многие граждане по всему миру перестали доверять новым технологиям, что стало важным глобальным вызовом [Chaudhuri 2021: 3]. Можно сказать, что на настоящем этапе внедрение новых технологий не приводит к ожидаемым результатом. С другой стороны, очевидно, что цифровизация государственного управления, в особенности перевод государственных услуг в цифровой формат с дальнейшим переходом к цифровому правительству, — общий тренд, без которого нельзя представить современное государство. Представляется важным выработать методологию анализа формирования «цифрового доверия» в гражданском обществе к цифровому правительству, а также понять возможности управления им.

Основной целью исследования является выявление влияния фактора «цифрового доверия» на проект цифрового правительства в России и оценка, насколько данный фактор учитывается при проведении технологических реформ. Автор опирается на системный и структурно-функциональный подходы, позволяющие рассматривать цифровое доверие как важное условие успешной деятельности цифрового правительства. Основной методикой исследования является контент-анализ, позволяющий показать представление о цифровом доверии в основных государственных программных документах, частных и государственных аналитических материалах.

Понятие «цифрового доверия» в политическом дискурсе

Хотя в российском политическом дискурсе термин «цифровое доверие (digital trust) появился сравнительно недавно, уже сейчас термин часто фигурирует в контексте цифрового правительства, цифровой экономики и общего прихода новых технологий в повседневную жизнь россиян.

Сам термин «доверие» имеет широкую коннотацию. Некоторые российские ученые даже склонны рассматривать категорию доверия как специфическую власть, определяющую качество взаимоотношений между обществом, бизнесом и государственными структурами [Дугин 2018: 61]. Само толкование слова «доверие» в мировой политической науке разнообразно. Так, зарубежные исследователи помимо термина доверия (trust) используют также термины «надежность» (trustworthiness), уверенность (confidence), вера (faith). В общем смысле доверие употребляется как дефиниция, описывающая состояние уверенности в том, что

[1] За время пандемии уровень доверия к государству упал у 61 % россиян // Официальный сайт сетевого издания РБК. URL: https://www.rbc.ru/society/26/05/2020/5eccff7b9a794728f8f0f327 (дата обращения: 04.04.2021).

[2] Рейтинги доверия политикам, оценки работы Президента и правительства, поддержка политических партий // Официальный сайт ВЦИОМ. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/reitingi-doverija-politikam-ocenki-raboty-prezidenta-i-pravitelstva-podderzhka-politicheskikh-partii-19022021 (дата обращения: 04.04.2021).

интересы тех, кому мы доверяем, согласованы либо совпадают с нашими интересами [Festenstein 2019: 447]. Данные дефиниции могут употребляться как в синонимичном значении, так и различаться. Доверие к правительству — важный аспект его легитимности, связанный с системной поддержкой принимаемых решений [Citrin, Stoker 2018: 50].

Кроме того, учеными принято рассматривать доверие в двух ипостасях: рациональной и эмоциональной. Рациональное доверие — доверие к тому, что объектом будут выполнены взятые на него обязательства. Эмоциональное же доверие зиждется на общности ценностей и целей, оценке доброй воли партнера [Дугин 2018: 62]. Из двух данных частей непосредственно проистекает доверие граждан к общественным и государственным институтам. При этом гражданину важнее его нормативная состоятельность (выполнение возложенных на институт функций) [Festenstein 2019: 455] и его эффективность [Малкина, Овчинников, Холодилин 2020: 82].

По сути, цифровое правительство — новый, еще не до конца сформированный государственный институт. Сама концепция образования цифрового правительства — относительно новая в отечественной политической науке и является развитием концепции электронного правительства. В общем смысле под «цифровым правительством» понимается правительство, использующее преимущества цифровых данных для оптимизации, трансформации и создания новых услуг [Василенко 2020: 225].

Если в электронном правительстве акцент делался на переводе услуг в цифровой формат, то цифровое правительство призвано изменить саму систему государственного управления. В первую очередь, это происходит за счет новых, более совершенных технологий BigData и искусственного интеллекта. Так, цифровое правительство обладает возможностью превентивного принятия решений за счет анализа данных граждан. Подобное правительство обладает рядом особенностей функционирования, среди которых гибкое (неиерархичное) управление, интерактивность, ориентированность на пользователя (ориентированность на желания пользователя и построение государственных стандартов, руководствуясь данным принципом), сильная зависимость от анализа данных при принятии решений, новый уровень привлечения IT-решений на основе открытых стандартов, открытость принятия решений, платформенность (включение в систему всех структур), ориентированность на горизонтальные структуры [Clarke 2020: 363].

Следует отметить, что в рамках концепций «электронного» и «цифрового» правительств с самого начала целью внедрения новых технологий в государственное управление становится повышение эффективности, результативности и открытости правительственных структур, что, в свою очередь, должно привести к повышению общего доверия к государственным органам со стороны граждан [Twizeyimana, Andersson 2019: 167]. Однозначность подобной цели подчеркивалась тем, что цифровые реформы долгое время носили чисто технологический характер, исключая идеологические распри [West, West 2005: 36].

Мы склонны рассматривать доверие в качестве важного структурного элемента цифрового правительства. С одной стороны, именно доверие влияет на качество проводимых цифровых изменений, с другой стороны, качество самих проводимых реформ способствует его росту.

В наиболее общем смысле «цифровое доверие» определяется как уверенность пользователей в способности людей, технологий и процессов создавать безопасный цифровой мир [Веселов 2020: 134] или как восприятие гражданином того, что элементы структуры цифрового правительства обладают атрибутами для охраны его интересов и соблюдают ряд ценностных для гражданина принципов [Venkatesh et al. 2016: 95]. В первую очередь, под «цифровым доверием» подразумевалось доверие к новым цифровым технологиям. В исследованиях доверия населения к цифровому правительству часто акцент делался на теоретические модели внедрения и распространение технологий, такие как модель принятия технологий, теория запланированного поведения, модель распространения инноваций и единая теория принятия и использования технологий [Venkatesh et al. 2016: 88]. В целом данная позиция актуальна и в настоящем времени. Так, последние исследования подтверждают, что именно доверие к технологиям (точнее — личный опыт использования данных технологий) играет ключевую роль в формировании позитивного отношения граждан к услугам цифрового правительства [Попова 2020: 43].

В дополнение некоторые зарубежные исследователи в рамках рассмотрения вопроса о доверии к цифровому правительству склонны отдельно выделять категорию надежности (trustworthiness) [Janssen et al. 2018: 648]. Понятие надежности относится к свойствам, через которые доверенное лицо (будь то другое лицо или учреждение) обслуживает интересы доверителя (гражданина или бизнеса). Надежность можно определить как убежденность в отсутствии резких изменений и «целостности» доверенного лица. Данная дефиниция напрямую связана с такими категориями, как безопасность и конфиденциальность.

Отмечается, что активное использование новых цифровых сервисов правительства гражданами положительно сказывается на политическом доверии правительству в общем (на вере граждан в то, что правительство принимает правильные решения) [Horsburgh, Goldfinch, Gauld 2011: 233]. Однако следует отметить, что на настоящий момент данная связь не является основополагающей в контексте развития цифрового правительства (например, более важную роль здесь играют такие параметры, как уровень компьютерной грамотности и уровень доходов граждан) [Pérez-Morotea, Pontones-Rosaa, Núñez-Chicharro 2020: 10]. Вместе с тем прослеживается и обратная связь, когда более высокий уровень доверия к действующей власти положительно сказывался на одобрении предоставляемых государством услуг (в том числе и цифровых) [Herian 2014: 89].

Положительное влияние на доверие к правительству цифровые сервисы могут оказать только при соблюдении определенных принципов, таких как открытость (понятность алгоритмов обработки данных пользователей, интуитивность интерфейса, доступность информации о том, куда и как переда-

ются данные пользователя) и подотчетность (возможность пользователя защитить свои права в случае ошибок сервиса) [Mahmood, Weerakkody, Chen 2020: 721]. Соблюдение именно данных принципов, по мнению как зарубежных, так и российских специалистов, обеспечит необходимый общественный контроль за деятельностью государственных органов в цифровой среде [Кочетков 2020: 15].

Основными структурными элементами цифрового доверия можно считать: 1) ожидания (доверитель рассчитывает на определенное поведение доверенного лица), 2) убежденность, веру в поведение доверенного лица, которое основывается на его компетентности, честности и доброжелательности, 3) принятие доверителем определенного риска [Нурмухаметов 2019: 11]. Некоторые ученые предлагают такие структурные элементы, как надежность источника информации, открытость структурных элементов сервисов цифрового правительства, доброжелательность интерфейсов цифрового правительства к пользователю, прозрачность, оперативность, компетентность, подотчетность, конфиденциальность [Janssen et al. 2018: 665].

Проблема доверия стала краеугольной темой не только в научном сообществе, но и для бизнеса, который опережает государство по многим вопросам цифровизации [Benay 2018: 3]. Исследованию доверия в цифровой среде посвящены многие проекты консалтинговых и аналитических агентств. Например, консалтинговая компания KPMG воспринимает цифровое доверие как «уверенность потребителей в технологиях». Специалисты KPMG приводят такие атрибуты цифрового доверия, как надежность (сервисы соответствуют запросам потребителей), авторитет (компания выполняет взятые на себя обязательства), открытость (пользователи знают, где и как используются их персональные данные), честность (соблюдение интересов потребителей), безопасность. В практической плоскости данные атрибуты выражаются в таких областях, как бренд компании, управление рисками, «гибкость» электронных сервисов компании, стандартизация сервисов, цифровая инфраструктура, безопасность и конфиденциальность[3]. Подчеркивается, что потребители в настоящее время больше фокусируются не на самих сервисах и продуктах, а на вере в сохранность их персональных данных. При этом в последние годы участились случаи утечки персональных данных, в том числе из баз данных государственных структур. Так, громкая утечка данных базы «Госуслуг» произошла в 2019 г., когда в сети оказались данные более чем 30 тысяч клиентов сервиса[4]. Уже в начале 2020 г. в открытый доступ попали данные 300 тысяч москвичей, переболевших коронавирусом. При этом причиной утечки назвали не техно-

[3] Digital Trust // Официальный сайт консалтинговой компании KPMG. URL: https://assets.kpmg/content/dam/kpmg/pdf/2015/12/digital-trust.pdf (дата обращения: 04.04.2021).

[4] СМИ узнали об утечке данных пользователей сайта госуслуг // Официальный сайт сетевого издания РБК. URL: https://www.rbc.ru/society/29/12/2019/5e08a43d9a7947345490f23e (дата обращения: 04.04.2021).

логический, а человеческий фактор[5]. В декабре 2021 г. в открытом доступе также оказался исходный код сайта «Госуслуг»[6]. С одной стороны, столь частые утечки персональных данных и ненадежность информационных систем можно обосновать техническим фактором. С другой стороны, в мире (и в особенности в России) пока не развита культура обращения с персональными данными. Данный аспект может являться серьезной проблемой и вызывать серьезные опасения при пользовании сервисами со стороны граждан.

Похожие структурные элементы выделяют и специалисты компании Deloitte. По их мнению, цифровое доверие держится на четырех столпах: этика и ответственность компаний перед клиентами, контроль конфиденциальности данных пользователей, открытость и доступность (в контексте используемых цифровых практик), безопасность и надежность. В рамках первой категории подчеркивается значимость обратной связи с пользователями и быстрое реагирование на возникающее недовольство электронными сервисами, а также значимость борьбы с недостоверной информацией об услугах и разработки методик исследования отзывов пользователей. В рамках второй категории подчеркивается значимость участия пользователей в контроле за своими данными (например, выбор пользователями данных, которые они размещают на онлайн-сервисах), принцип «экономности» и точности при сборе персональных данных пользователей. В рамках третьей категории говорится о важности легкой оценки пользователями цифровых предложений компании (их преимуществ) и возможности понимания пользователями алгоритмов, по которым работают цифровые системы. В рамках четвертой категории рассматривается важность проактивного оповещения пользователей о возможных угрозах и совершенствование средств защиты данных[7].

Консалтинговая компания Accenture заявляет, что для построения доверительных отношений с пользователями электронных сервисов компаниям необходима четкая стратегия. Данная стратегия должна основываться на стандартах открытости, конфиденциальности и безопасности работы с данными пользователей. Следует учитывать, что цифровое доверие не ограничивается программным обеспечением безопасности данных, а является более широким понятием, отражающим характеристику самой компании. В целях завоевания доверия пользователей необходимо придерживаться принципов клиентоориентированности,

[5] «Ситуация критическая»: чем грозит крупнейшая утечка данных заболевших коронавирусом // Официальный сайт сетевого издания Forbs.ru. URL: https://www.forbes.ru/tehnologii/415857-situaciya-vesma-kritichna-chem-grozit-krupneyshaya-utechka-dannyh-zabolevshih (дата обращения: 04.04.2021)

[6] «Привлечь внимание к проблеме»: кто слил исходный код «Госуслуг» и чем это грозит // Официальный сайт сетевого издания Forbs.ru. URL: https://www.forbes.ru/tekhnologii/451375-privlec-vnimanie-k-probleme-kto-slil-ishodnyj-kod-gosuslug-i-cem-eto-grozit (дата обращения: 15.01.2022)

[7] Building digital trust: Technology can lead the way // Официальный сайт консалтинговой компании Deloitte. URL: https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/Innovation/lu-building-digital-trust.pdf (дата обращения: 04.04.2021)

целостности системы (построение цифрового доверия становится миссией организации, а не отдельным элементом ее сервисов), партнерства[8].

Цифровое доверие — сложное явление, заключающееся в доверии к новой технологии, включающее в себя рациональные и эмоциональные аспекты поведения граждан. Подобное доверие является важным аспектом легитимности новых государственных цифровых институтов и должно строиться на определенных принципах, таких как открытость элементов и принципов работы, особое внимание к конфиденциальности данных пользователей, надежности и однозначности источника информации о сервисе. Соблюдение приведенных принципов и повышение доверия к цифровым сервисам может повысить доверие граждан к государству в целом.

Особенности формирования цифрового доверия к сервисам цифрового правительства

Представляется важным посмотреть, как категория доверия представлена в основных стратегических и нормативно-правовых документах России, регулирующих развитие цифрового правительства, а также в иных материалах по внедрению концепции электронного и цифрового правительства в России. Данный анализ может помочь ответить на вопрос, рассматривается ли вопрос доверия как вопрос стратегической важности и какие меры используются в целях повысить доверие граждан к цифровым сервисам государства. Среди данных документов: федеральная целевая программа «Электронная Россия» (2002–2010 гг.), «Концепция формирования в РФ электронного правительства до 2010 года», Государственная программа РФ «Информационное общество» (2011–2020 гг.), «Стратегия развития информационного общества в РФ (2008 г.)», «Концепция развития механизмов предоставления государственных и муниципальных услуг в электронном виде» (от 2013 г.) и др.

Сам термин «цифровое доверие» встречается в стратегических документах редко (упомянуто в двух документах). В государственной программе «Информационное общество» говорится об отсутствии на современном этапе доступных механизмов обеспечения доверия к электронной цифровой подписи, об отсутствии целостной системы удостоверяющих центров, а также объединения удостоверяющих центров электронной подписи в домены взаимного доверия. В связи с данными обстоятельствами поставлена задача по формированию единого пространства доверия электронной подписи, включающего инфраструктуру, систему удостоверяющих центров, систему авторизации и идентификации пользователей[9]. В государственной программе «цифровая экономика» также ста-

[8] Re-imagining Trust in the Digital Age // Официальный сайт консалтинговой компании Accenture. URL: https://www.accenture.com/_acnmedia/PDF-47/Accenture-Trust-Digital-Age.pdf (дата обращения: 04.04.2021).

[9] Распоряжение Правительства Российской Федерации от 20 октября 2010 г. № 1815-р г. Москва «О государственной программе Российской Федерации „Информационное общество (2011-2020 годы)“» // Официальный сайт Российской газеты. URL: https://rg.ru/2010/11/16/infobschestvo-site-dok.html (дата обращения: 04.04.2021).

вится задача по формированию «единой цифровой среды доверия»[10]. В первую очередь, рассматриваются вопросы совершенствования правовых механизмов регулирования цифровой среды, в том числе вопросы международного нормативного регулирования безопасности в интернет-среде. Несмотря на то, что в стратегических документах обозначены общие направления изменений, данные меры не связаны между собой. Следует отметить, что на настоящий момент не разработаны показатели повышения доверия граждан к цифровым услугам и система оценки опыта граждан во взаимодействии с цифровыми сервисами. Под вопросом остается участие граждан в управлении своими данными, в особенности при взаимодействии с сервисами правительства. Гражданский контроль за деятельностью цифрового правительства остается особенно важной сферой. Эксперты отмечают важность внесения поправок в основные нормативно-правовые акты, которые должны контролировать деятельность цифрового правительства и препятствовать превышению полномочий со стороны государственных служащих, а также обеспечить публичную дискуссию по вопросам цифрового правительства уже на уровне пилотных проектов.

Распространенной практикой является принятие нормативно-правовых актов, контролирующих общие принципы функционирования той или иной технологии. Примером такого подхода является принятая в Нидерландах Хартия 5G, контролирующая внедрение сетей 5G как в частном, так и в государственном секторах[11]. В России также вырабатываются общие принципы взаимодействия в рамках конкретных технологий. Например, в августе 2020 г. Правительством России была утверждена Концепция развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 г. Важно подчеркнуть, что в принятии подобного рода документов огромное значение имеет удовлетворение интересов всех сторон, включающих бизнес, общество и государство.

Несмотря на все трудности, Правительству России удалось создать некоторый «задел доверия» к своим цифровым решениям. Последнее исследование ВШЭ «Оценка цифровой готовности населения России», учитывающее уровень цифрового доверия, показало относительно высокий его уровень. Так 85 % взрослого населения России (от 17 до 75 лет) доверяет действующим государственным электронным сервисам. По мнению специалистов ВШЭ, показатель цифрового доверия непосредственно влияет на активность россиян в использовании цифровых сервисов[12]. В исследовании подчеркивается, что данный пока-

[10] Распоряжение Правительства РФ от 28 июля 2017 г. № 1632-р Об утверждении программы «Цифровая экономика Российской Федерации» // Официальный сайт Федерального агентства связи. URL: https://rossvyaz.gov.ru/upload/gallery/87/21087_4464749e911aff89e843adb0b71c47438 1da42b3.pdf (дата обращения: 04.04.2021).

[11] Официальный электронный ресурс организации Netherlands Digital // Хартия 5G. URL: https://www.nederlanddigitaal.nl/initiatieven/handvest-5g (дата обращения: 21.04.2020).

[12] Исследование: порядка 85 % взрослого населения доверяет цифровым госсервисам // Официальный сайт информационного агентства ТАСС. URL: https://tass.ru/ekonomika/11121571 (дата обращения: 12.04.2021).

затель на настоящем этапе может быть исчерпывающим. Для его дальнейшего роста государству необходимо выработать общую стратегию кибербезопасности и стимуляции населения к использованию новых цифровых технологий. В некоторых аналитических докладах, посвященных разным областям цифрового правительства, также отмечается важность создания мультиканального взаимодействия между государством и обществом, а также возможность для пользователя контролировать использование своих данных[13].

Заключение

Проведенное исследование показало, что цифровое доверие — сложное явление, состоящее из множества структурных элементов. Наиболее важными принципами построения данного доверия в рамках цифрового правительства является его открытость для граждан (в том числе за счет возможностей граждан контролировать распространение своих данных) (примером здесь может служить опыт Нидерландов, где в 2005 г. была принята «Хартия электронного гражданина», позволяющая гражданам выбирать каналы связи с государственными органами и получать от них информацию о передачи их личных данных), безопасность и надежность электронных сервисов (исключение критических ошибок и некорректной работы цифровых сервисов), выстраивание двусторонней коммуникации с гражданами (возможности обратной связи, активная разъяснительная работа с пользователями сервисов цифрового правительства). Некоторые из данных принципов заложены в государственные программные документы, посвященные цифровой трансформации, однако общая стратегия построения цифрового доверия не выработана. Игнорирование данной проблемы может в итоге привести к бойкотированию гражданами государственных цифровых сервисов, а также общему снижению доверия к государственным институтам.

Несмотря на общий высокий уровень доверия к сервисам цифрового правительства в России в настоящее время, под вопросом остается разработка показателей уровня цифрового доверия и дальнейших мер по его повышению.

Поступила в редакцию / Received: 13.04.2022
Доработана после рецензирования / Revised: 07.06.2022
Принята к публикации / Accepted: 15.06.2022

[13] *Буров В.В., Петров М.В., Шклярук М.С., Шаров А.В.* «Государство-как-платформа»: (кибер) государство для цифровой экономики. Цифровая трансформация // Доклад Центра Стратегических разработок. 2018. // Официальный сайт Центра стратегических разработок. URL: https://www.csr.ru/upload/iblock/313/3132b2de9ccef0db1eecd56071b98f5f.pdf (дата обращения: 12.04.2021).

Библиографический список

Василенко И.А. Особенности формирования концепции цифрового правительства в политической науке и перспективы ее реализации в России // Государственное управление. Электронный журнал ФГУ МГУ. 2020. № 82. С. 218–244.

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

Дугин Е.Я. Власть доверия и доверие власти // Власть. 2018. Т 26. № 8. С. 60–66.

Кочетков А.П. Роль цифрового правительства в повышении эффективности взаимодействия власти и гражданского общества в современной России // PolitBook. 2020. № 2. С. 6–24.

Латов Ю.В. Институциональное доверие как социальный капитал в современной России (по результатам мониторинга) // Полис. Политические исследования. 2021. № 5. С. 161–175.

Малкина М.Ю., Овчинников В.Н., Холодилин К.А. Институциональные факторы политического доверия в современной России // Journal of Institutional Studies. 2020. № 4. С. 77–93.

Нурмухаметов Р.К. К вопросу о цифровом доверии // Алтайский вестник Финансового университета. 2019. № 4. С. 8–17

Нурмухаметов Р.К., Торин С.С. Цифровое доверие (digital trust): сущность и меры по его повышению // Известия Тульского государственного университета. Экономические и юридические науки. 2020. № 1. С. 32–39

Орехова Е.А. Цифровое доверие как фактор развития в условиях турбулентности // Вестник Саратовского социально-экономического университета. 2020. № 3. С. 24–27

Попова О.В. Использование услуг цифрового правительства: фронтиры и аутсайдеры // Вестник ВГУ. Серия: История. Политология. Социология. 2020. № 2. С. 38–44.

Balog-Way D.H. P., McComas K.A. COVID-19: Reflections on trust, tradeoffs, and preparedness // Journal of Risk Research. 2020. Vol. 23, no. 7. P. 838–848.

Benay A. Government Digital: The Quest to Regain Public Trust, Toronto, Dundurn Press, 2018.

Chaudhuri A. Transformation with trustworthy digital: policy desiderata for businesses in post COVID-19 world // The EDP Audit, Control, and Security Newsletter. 2021. Vol. 63, no. 1. P. 1–8.

Citrin J., Stoker L. Political Trust in a Cynical Age // Annual Review of Political Science. 2018. Vol. 21. P. 49–70.

Clarke A. Digital government units: what are they, and what do they mean for digital era public management renewal? // International Public Management Journal. 2020. Vol. 23, no. 3. P. 358–379

Festenstein M.I. Political Trust, Commitment and Responsiveness // Political Studies. 2019. Vol. 62, no. 2. P. 446–462.

Herian M.N. Trust in Government and Support for Municipal Services // State and Local Government Review. 2014. Vol. 46, no. 2. P. 82–90.

Horsburgh S., Goldfinch S., Gauld R. Is Public Trust in Government Associated With Trust in E-Government? // Social Science Computer Review. 2011. Vol. 29, no. 2. P. 232–241.

Janssen M., Rana N.P., Slade E.L., Dwivedi Y.K. Trustworthiness of digital government services: deriving a comprehensive theory through interpretive structural modeling // Public Management Review. 2018. Vol. 20, no. 5. P. 647–671.

Mahmood M., Weerakkody V., Chen W. The role of information and communications technology in the transformation of government and citizen trust // International Review of Administrative Sciences. 2020. Vol. 86, no. 4. P. 708–728

Pérez-Morotea R., Pontones-Rosaa C., Núñez-Chicharro M. The effects of e-government evaluation, trust and the digital divide in the levels of e-government use in European countries // Technological Forecasting & Social Change. 2020. Vol. 154. P. 1–14.

Twizeyimana D.J., Andersson A. The public value of E-Government — A literature review // Government Information Quarterly. 2019. Vol. 36, no. 2. P. 167–178.

Venkatesh V., Thong J.Y. L., Chan F.K. Y., Hu P.J. H. Managing Citizens' Uncertainty in EGovernment Services: The Mediating and Moderating Roles of Transparency and Trust // Information Systems Research. 2016. Vol. 27, no. 1. P. 87–111.

West D.M., West M.M. Digital Government: Technology and Public Sector Performance. Princeton NJ, Princeton University Press, 2005.

References

Balog-Way, D.H.P., & McComas, K.A. (2020). COVID-19: Reflections on trust, tradeoffs, and preparedness. *Journal of Risk Research*, 23(7), 838–848.

Benay, A. (2018). *Government Digital: The Quest to Regain Public Trust*. Toronto: Dundurn Press.

Chaudhuri, A. (2021). Transformation with trustworthy digital: policy desiderata for businesses in post COVID-19 world. *The EDP Audit, Control, and Security Newsletter*, 63(1), 1–8.

Citrin, J., & Stoker, L. (2018). Political Trust in a Cynical Age. *Annual Review of Political Science*, 21, 49–70.

Clarke, A. (2019). Digital government units: what are they, and what do they mean for digital era public management renewal? *International Public Management Journal*, 23(3), 358–379.

Dugin, E. Ya. (2018). The power of trust and confidence in power. *The Authority*, 8, 60–66 (In Russian).

Festenstein, M.I. (2019). Political Trust, Commitment and Responsiveness. *Political Studies*, 62(2), 446–462.

Herian, M.N. (2014). Trust in Government and Support for Municipal Services. *State and Local Government Review*, 46(2), 82–90.

Horsburgh, S., Goldfinch, S., & Gauld, R. (2011). Is Public Trust in Government Associated With Trust in E-Government? *Social Science Computer Review*, 29(2), 232–241.

Janssen, M., Rana, N.P., Slade, E.L., & Dwivedi, Y.K.(2018). Trustworthiness of digital government services: deriving a comprehensive theory through interpretive structural modeling. *Public Management Review*, 20(5), 647–671.

Kochetkov, A.P. (2020) The role of digital government in improving the effectiveness of interaction between government and civil society in modern Russia. *PolitBook — Political science journal*, (2), 6–24 (In Russian).

Mahmood, M., Weerakkody, V., & Chen, W. (2020). The role of information and communications technology in the transformation of government and citizen trust. *International Review of Administrative Sciences*, 86(4), 708–728.

Majorov, A.V., Volkova, A.M., & Potapov, A.D. (2019). Digital transformation of state and municipal administration: main theses in a new technological reality. *Towards a "digital society": Expert estimates and forecasts. Expert Institute for Social Research.* Moscow: Nauka (In Russian).

Malkina, M.Yu., Ovchinnikov, V.N., & Kholodilin, K.A. (2020). Institutional Factors Influencing Political Trust in Modern Russia. *Journal of Institutional Studes*, 12(4), 77–93. (In Russian).

Nurmukhametov, R.K. (2019). To the question of digital trust. *Altai Vestnik of the Financial University*, (4), 8–17 (In Russian).

Nurmukhametov, R.H., & Torin, S.S. (2020). Digital trust: the essence and measures to increase it. *Izvestiya Tula State University*, (1), 32–39 (In Russian).

Orekhova, E.A. (2020). Digital trust as a contributor to development under uncertainty and turbulence. *Vestnik of Saratov state socio-economic university*, (3), 24–27 (In Russian).

Popova, O.V. (2020). Using digital government services: frontiers and outsiders. Proceedings of Voronezh State University, (2), 38–44 (In Russian).

Pérez-Morotea, R., Pontones-Rosaa, C., & Núñez-Chicharro, M. (2020). The effects of e-government evaluation, trust and the digital divide in the levels of e-government use in European countries. *Technological Forecasting & Social Change*, 154, 1–14.

Twizeyimana, D.J., & Andersson, A. (2019). The public value of E-Government — A literature review. *Government Information Quarterly*, 36(2), 167–178.

Vasilenko, I.A. (2020). Formation of "Digital Government" Concept in Political Science and Prospects for Its Implementing in Russia. *Public administration electronic bulletin*, 82, 218–244 (In Russian)

Veselov, Yu. V. (2020). Trust in a digital society. *Vestnik of Saint Petersburg University*. *Sociology*, 13, 129–143 (In Russian).

Venkatesh, V.L., Thong, J.Y., Chan, F.K.Y., & Hu, P.J.H. (2016). Managing Citizens' Uncertainty in EGovernment Services: The Mediating and Moderating Roles of Transparency and Trust. *Information Systems Research,* 27(1), 87–111.

West, D. M, & West, M.M. (2005). Digital Government: Technology and Public Sector Performance. Princeton NJ: Princeton University Press.

Сведения об авторе:

Чепелюк Сергей Георгиевич — аспирант кафедры российской политики Московского государственного университета им. М.В. Ломоносова. (e-mail: sergey.chepeliuk@yandex.ru) (ORCID: 0000-0002-4925-1244)

About the author:

Sergey G. Chepelyuk — Postgraduate of the Department of Russian Politics, Faculty of Political Science of Lomonosov Moscow State University (e-mail: sergey.chepeliuk@yandex.ru) (ORCID: 0000-0002-4925-1244)