Цифровое доверие как ключевой фактор в формировании датацентричного государственного управления

Е. М. Стырин, Я. А. Рыбушкина, А. Г. Санина

Национальный исследовательский университет «Высшая школа экономики»

estyrin@hse.ru, yrybyshkina@hse.ru, asanina@hse.ru

Аннотация

Государственное управление за последние годы претерпевает значительные изменения, которые были вызваны внедрением новых технологий и цифровых инструментов. Появление концепции датацентричного управления неразрывно связано с цифровой трансформацией, порождающей изменения не только в способах решения задач управления, применением цифровых инструментов, но и организации работы ведомств и взаимодействия между гражданами и государством. В этом разрезе на первый план выходит феномен цифрового доверия – новый ключ к внедрению и пониманию датацентричного управления. Данная статья представляет собой анализ существующих знаний относительно цифрового доверия, а также рассматривает барьеры и меры по внедрению датацентричного управления в России. В заключение авторы приводят способы повышения цифрового доверия на основе результатов экспертного опроса. Публикация обобщает имеющиеся сведения о цифровом доверии в научном и практическом поле и является частью комплексного исследования цифрового доверия.

Ключевые слова: датацентричное государственное управление, цифровое доверие, цифровая трансформация государственного управления, инструменты повышения цифрового доверия

Библиографическая ссылка: Стырин Е. М., Рыбушкина Я. А., Санина А. Г. Цифровое доверие как ключевой фактор в формировании датацентричного государственного управления // Государство и граждане в электронной среде. Выпуск 7 (Труды XXVI Международной объединенной научной конференции «Интернет и современное общество», IMS-2023, Санкт-Петербург, 26–28 июня 2023 г. Сборник научных статей). — СПб.: Университет ИТМО, 2024. С. 13–23. DOI: 10.17586/2541-979X-2024-7-13-23

1. Изучение датацентричного управления государством

Государственное управление, основанное на данных (датацентричное государственное управление), становится заметной международной темой исследований в области государственного управления в последние годы [1, 2, 3, 4]. За последнее время страны по всему миру разработали концепции или стратегии развития цифровой трансформации государственного сектора [5, 6, 7, 8]. При этом в стратегиях сделан упор на технологических улучшениях. Великобритания, например, ставит себе цель к 2027 году перейти на технологии 5G, чтобы большинство населения получило доступ к сигналу 5G благодаря программе «Испытания 5G и испытательные стенды» (5G Trials and Testbeds programme). Работа с технологическими решениями цифровой трансформации в государственном секторе остаётся магистральной темой для учёных и практиков, но фокус проблем смещается, поскольку происходящие цифровые изменения во многом связаны с человеческим фактором, сотрудниками и людьми, взаимодействующими с организацией [9, 10, 11].

Исследование опирается на экспертный опрос, который изучает барьеры внедрения датацентричного управления государством. Ими стали вопросы технического и технологического характера, правовых и бюрократических аспектов датацентричного управления, а также личностные и человеко-ориентированные особенности восприятия цифровых инноваций. Опрошенные эксперты и чиновники непосредственно принимают или сопровождают процесс принятия решений в переходе на датацентричное управление. Экспертный опрос, проведённый с 12 по 29 сентября 2022 г., выборка которого проходила по методу снежного кома, составил 146 экспертов. Основными критериями для участия в опросе были следующие параметры: стаж работы респондента в сфере цифровой трансформации государственного сектора должен быть не менее трех лет (главный критерий для чиновников и экспертов-практиков), а также для учёных было необходимо иметь не менее трех публикаций по теме. Проведённое опросное исследование позволит подробнее раскрыть разные аспекты формирования датацентричного управления в России.

Таблица 1. Перечень российских проблем, препятствующих внедрению модели датацентричного госуправления

Рейтинг значимости проблем, которые препятствуют внедрению в России общенациональной модели управления данными	**Значимость (в %)**
Отсутствие в органах власти общих (единых) стандартов предоставления (обмена) данных	89,1
Правовая неопределённость в сфере регулирования вопросов обмена и повторного использования данных	87,0
Отсутствие необходимого уровня навыков для работы с данными в органах власти	86,6
Бюрократические барьеры в текущей модели управления	85,4
Крупные компании не заинтересованы в обмене технологиями и инфраструктурой	84,2
Низкий уровень развития инфраструктуры размещения, обработки и использования данных	84,2
Отсутствие механизмов сотрудничества государства и бизнеса в формировании единой политики управления, основанной на данных	81,0
Противоречия (разногласия) в отраслевых и ведомственных подходах управления данными	80,6
Недопонимание органами публичной власти преимуществ и выгод от обмена данными	79,4
Отсутствие доверия к обмену данными между владельцами данных	78,9
Ограничения и неравномерность доступа к технологический инфраструктуре	78,9
Высокие затраты на разработку, внедрение и поддержание систем управления данными	78,9
Отсутствие лидеров и методологов управления на основе данных в руководстве органов публичной власти	78,5
Открытые данные фрагментированы, разрознены, малоценны	77,3
Отсутствие культуры работы с данными в органах власти	76,1
Дорогостоящий процесс подготовки (очистки, верификации, связывания) данных	74,9
Сильная зависимость от иностранных технологий и ПО	70,9
Государство не заинтересовано в предоставлении данных бизнесу и обществу	70,0
Сопротивление инновациям со стороны госслужащих	68,4
Отсутствие политической поддержки перехода к датацентричному управлению	66,8

Наиболее остро в России стоят проблемы технологического характера, правого регулирования, а также человеческого восприятия (отсутствие доверия к обмену данными между владельцами данных – см. табл. 1). Помимо этого, важно отметить бюрократические

барьеры в текущей модели управления, так как они затрудняют технологическое развитие, правовое реагирование и желание людей взаимодействовать в цифровом поле.

Эксперты также оценивали меры, которые необходимы для внедрения в России модели датацентричного госуправления (табл. 2).

Таблица 2. Перечень мер, необходимых для внедрения в России модели датацентричного госуправления

Перечень мер	Значимость (в %)
Обучение навыкам работы с данными всех сотрудников органов власти и организаций	90
Обеспечение безопасности сбора, обработки и обмена данными	95
Повышение уровня цифровой грамотности граждан	91
Утверждение отраслевых стандартов и политик по созданию системы управления данными	91
Повышение доверия к данным	91
Внедрение механизма межведомственного управления с полномочиями по обеспечению соблюдения стандартов сбора, обмена и переиспользования данных	89
Внедрение отраслевых систем бесплатного повышения компетенций по работе с данными для специалистов	85
Создание в каждом органе власти подразделения, ответственного за цифровые и технологические стандарты, за реализация инициатив в области обмена и анализа данных	81
Принятие законодательства для обеспечения функциональной совместимости определенных категорий данных	85
Создание на федеральном уровне экспертно-консультационного совета в сфере управления данными	80
Включение дифференцированного курса по анализу данных во всех вузах	78
Назначение в каждом органе власти замруководителя, отвечающего за развитие системы управления данными, создание инфраструктуры данных, аналитические и инвестиционные проекты в этой области	74
Принятие законодательства для обмена и многократного переиспользования данных	87
Реализация серии флагманских инновационных проектов по обмену данными	81
Принятие в каждом органе власти тактических планов по переходу к датацентричной модели	78
Создание саморегулируемых организаций и ассоциаций анализа передовых практик и повышения эффективности управления данными	63

Наиболее значимыми стали технологические меры, такие как обеспечение безопасности сбора, обработки и обмена данными, но при этом на первый план вышли вопросы формирования человеко-направленных аспектов доверия, таких как: повышение уровня цифровой грамотности граждан и повышение доверия к данным. Эксперты выделяют личные особенности восприятия технологий человеком как одну из ключевых задач для принятия датацентричной модели управления (обучение навыкам работы с данными всех сотрудников органов власти и организаций; повышение уровня цифровой грамотности граждан). В академическом поле личное восприятие технологий связано с феноменом цифрового доверия. Внедрение датацентричного управления необходимо рассматривать через призму цифрового доверия.

2. Роль цифрового доверия в датацентричном управлении

Взаимоотношение человека с технологией продуктивно рассматривать через понятие цифрового доверия. В российском научном поле цифровое доверие определяют как уверенность пользователей в безопасности и надёжности цифровых систем, процессов и технологий [12]. При этом использование термина «цифровое доверие» практически не встречается в стратегических документах Российской Федерации, соответственно, прямо не прописаны меры по повышению цифрового доверия граждан к технологиям, применяемым в госсекторе [13]. В этой связи стоит обратиться к международному опыту изучения цифрового доверия.

Организация экономического сотрудничества и развития (ОЭСР, OECD) отмечает отсутствие на данный момент общепринятого определения цифрового доверия, поэтому предлагает понимать его как положительный результат способности справляться с неопределённостью [7]. К тому же ОЭСР выделяет цифровое доверие с двух точек зрения: человека и организаций. С точки зрения человека, доверие в цифровую эпоху — это готовность рисковать временем, деньгами и раскрытием личных данных для участия в коммерческой и социальной деятельности, а также стать уязвимым, если покупка пойдёт не так, если его данные будут украдены или использованы для мониторинга его поведения, дискриминации или нарушения его частной жизни [14]. С точки зрения организаций, доверие также означает принятие определенного уровня риска, связанного с возможными инцидентами в области цифровой безопасности, конфиденциальности, защиты прав потребителей [7]. Для того, чтобы в полной мере воспользоваться преимуществами цифровой трансформации, частные лица, компании и правительства должны быть уверены в том, что участие в цифровой среде для осуществления своей социально-экономической деятельности принесёт больше преимуществ, чем недостатков. Негативный опыт может возникнуть из-за различных источников неопределённости, влияющих на цифровые технологии, данные и трансграничные потоки. Большинство из них связаны с потенциальными инцидентами цифровой безопасности, информационной асимметрией, дисбалансом сил или юрисдикционными проблемами, усугубляемыми цифровой средой. Это может привести к нарушению законов и нормативных актов, таких как неприкосновенность частной жизни, защита прав потребителей или безопасность продукции, призванных уменьшить эти дисбалансы и проблемы. Для обеспечения доверия крайне важно максимально смягчить подобные неопределённости. Можно заключить, что цифровое доверие тесно связано с грамотным управлением цифровыми рисками.

Стоит также отметить, что ещё в 2013 году ОЭСР было разработано руководство по доверию, которое включает в себя восемь принципов, применимых как к государственному, так и к частному сектору: (1) принцип ограничения сбора; (2) принцип качества данных; (3) принцип определения цели; (4) принцип ограничения использования; (5) принцип гарантий безопасности; (6) принцип открытости; (7) принцип индивидуального участия; (8) принцип подотчётности. Многие государства разрабатывают свои стратегии цифрового развития опираясь на эти принципы.

Можно заметить, что специалисты ОЭСР выделяют фактор цифрового доверия в решении задач поиска технологических уязвимостей, урегулирования правовых ограничений, налаживания работы с данными. При этом мало уделяется внимания социальным и человеческим барьерам, которые играют не менее важную роль.

Всемирный экономический форум (ВЭФ, World Economic Forum) определяет цифровое доверие как ожидание людей о том, что организации, предоставляющие цифровые технологии и услуги, будут защищать интересы всех заинтересованных сторон и поддерживать общественные ожидания и ценности. В этой связи ВЭФ выделяет два основополагающих типа доверия: механическое и реляционное. Механическое доверие — это средства и механизмы, которые надёжно и предсказуемо обеспечивают заранее определенные результаты. К «механическим» можно отнести применение таких

технологий, как блокчейн или практику не дискреционного раскрытия информации. Реляционное доверие тесно связано с социальными нормами и соглашениями, которые учитывают сложные реалии жизни. В контексте цифрового доверия реляционное доверие часто представляет собой общее соглашение о том, когда, где, почему и как используются технологии. Даже если все механические системы работают, при этом отдельные лица, оценивающие доверие, не верят, что организации и отдельные лица играют по одним и тем же правилам, или верят, что лица, принимающие организационные решения, не полностью учитывают интересы своих пользователей и не стремятся к их соблюдению, основное (цифровое) доверие часто разрушается [15].

В разрезе исследования применения чат-ботов в государственном секторе [16], интересно посмотреть на модель «производительность-процесс-цель» (performance-process-purpose framework). Хэнгслер и др. [17], эмпирически установили, что промышленные менеджеры и инженеры работают с этими тремя источниками доверия, чтобы повысить доверие потребителей к их машинной продукции. Модель «производительность-процесс-цель» была представлена Ли и Си [18] в 2004 году и выглядит следующим образом. Производительность — это текущая и историческое функционирование автоматизации и включает в себя такие характеристики, как надёжность, предсказуемость и способность и относится также к компетентности или способности машины достичь целей оператора. Процесс относится к алгоритмам и операциям, которые управляют поведением цифрового продукта, а также к тому, что оператор будет склонен доверять цифровому решению, если его алгоритмы могут быть понятны или если они способны достичь цели оператора в текущей ситуации. Цель – это степень, в которой цифровое решение используется в пределах и в рамках замысла разработчика и описывает, почему набор алгоритмов был разработан [18]. В данном случае видно применение определенных категорий, которые призваны описать удовлетворённость граждан (операторов), что будет напрямую влиять на их желание пользоваться цифровым продуктом. В исследовании оценки цифровой готовности населения России [19] отмечается, что «чем выше уровень цифрового доверия, тем чаще человек использует цифровые сервисы и технологии». Применение модели «производительность-процесс-цель» может повысить использование цифровых инструментов гражданами, что может положительно влиять на цифровое доверие.

Повышение уровня цифрового доверия в государственном секторе напрямую связано с работой с данными [20, 21, 22]. Исследование, проведённое Пинк и др. [23], показывает, что граждане доверяют, когда они чувствуют себя достаточно уверенными в том, что любое случайное действие смягчено привычностью процесса или места. Ощущение привычности является ключевым моментом, оно ассоциируется с рутиной. Граждане справляются с неопределённостью путём выстраивания привычных рутин деятельности. Именно эти обстоятельства создают ситуации, в которых они могут доверять, и поэтому они способны избежать чувства тревоги по поводу того, что произойдёт дальше, и имеют достаточно уверенности, чтобы использовать новые технологии. Отсутствие этой уверенности может выражаться в низкой мотивации у сотрудников работать с данными, низкой культурой цифровой грамотности, недостатком знаний о технологиях. Это напрямую влияет на уровень цифрового доверия.

Обобщая вышеизложенные концепции, можно выделить несколько ключевых аспектов цифрового доверия. Первый — технологическая уверенность в цифровых системах. Вопросы безопасности, конфиденциальности, совершенства обмена данными внутри и между структурами играют важную роль в поддержании доверия. Второй — человеческие особенности восприятия цифровых изменений. Граждане склонны бояться неизвестности, поэтому необходимо создавать привычные условия пользования технологиями и формировать уверенность в тех, кто создаёт, внедряет и пользуется цифровыми данными. Третий — отсутствие правовой неопределённости.

Цифровое доверие как предмет исследования объединяет в себе несколько выделенных выше аспектов исследования. В то же время цифровое доверие как феномен может стать

инструментом для внедрения датацентричного управления в государственном секторе. Детальное изучение взаимосвязей внутри формирования цифрового доверия, выделение ключевых характеристик, может позволить сформировать рекомендации для представителей органов власти Российской Федерации по развитию датацентричного управления.

Концепция датацентричного управления в государственном секторе включает в себя целый ряд задач, которые необходимо курировать, а также создавать среду для их исполнения. В первую очередь — это управление данными, комплекс мер, который направлен на обеспечение попадания и использования нужных данных в необходимых управленческих процессах [24]. Помимо этого, управление данными включает в себя установление единых форматов сбора и обработки данных, а также решение вопросов законодательного соответствия этих процессов [25]. Работа с данными сама по себе требует от ответственных государственных органов предоставления метаданных, чтобы пользователи могли убедиться в качестве собранных данных и областях их применения [22]. Управление на основе данных должно приводить к созданию устойчивого диалога между аналитиками и лицами, принимающими решения, чтобы оно было качественным и проносящим реальные результаты [26]. В целом использование данных в государственном управлении должно приводить к прогнозированию эффекта от вводимых мер. Аналитика может быть направлена либо на исследование возможных действий, либо на создание предписания [27]. В этой связи цифровое доверие играет ключевую роль в процессах сбора и обработки данных, соблюдения конфиденциальности и безопасности (технологическая сторона цифрового доверия), а также законности сбора данных. Отношение граждан к передаче своих данных и желание участвовать в цифровом процессе взаимодействия с органами власти, формирует базу для внедрения датацентричного государственного управления.

3. Заключение, перспективы

Цифровое доверие можно назвать определяющим звеном во внедрении модели датацентричного государственного управления. На сегодняшний день в России нет представленного перечня мер по повышению цифрового доверия. Поскольку цифровое доверие представляет собой собирательный термин, охватывающий многие зоны цифрового взаимодействия, шаги по его повышению также должны быть комплексными.

Данное исследование ограничено экспертной парадигмой изучения цифрового доверия в контексте государственного управления. В представленном исследовании формирование критериев цифрового доверия опиралось на опрос экспертов. При этом тема цифрового доверия заслуживает внимания не только специалистов в цифровизации госсектора, но и внимания психологов, антропологов и социологов, чьи исследования могут дополнить картину восприятия гражданами новых технологий и принципов работы с ними, выявить их отношение к использованию данных, а также всевозможные влияющие на доверие демографические, личностные, эмоциональные, культурные и социальные особенности граждан. В данной работе главным направлением исследования стал практический опыт управленцев, работающих с данными в государственном секторе.

Органам власти рекомендуется в первую очередь ввести в свою деятельность цифровое доверие как механизм оценки цифровых инноваций со стороны граждан. Определение феномена, а также целевых показателей по цифровому доверию как, например, доступность данных и метаданных на сайтах ведомств, требования по конфиденциальности и безопасности данных, периодический опрос граждан по вопросам использования, предоставления, хранения данных, отражающих их личные предпочтения, должны стать базой для формирования цифровых государственных инструментов, повышающих доверие к процессу цифровой трансформации государства. Формирование стратегического показателя цифрового доверия граждан к цифровому государству на федеральном уровне,

а также организация его независимого мониторинга, в частности, в вопросах управления государственными данными станут базой для внедрения системы датацентричного управления.

Государственным служащим следует информировать граждан о работе с данными и механизмах их использования в государственном секторе, чтобы снизить влияние неопределённости и неинформированности, следовательно, повысить уровень цифрового доверия к датацентричному управлению. Граждане должны знать, какие данные о них хранятся в государственных информационных системах, какие действия с данными могут осуществлять уполномоченные лица, разрешать или не позволять использовать предоставленные данные, а также какие блага они получат взамен. Следует регламентировать и стандартизировать государственные технологии сбора, хранения, обработки и использования данных, а также механизм доступа уполномоченных лиц для работы с данными. Алгоритмы, согласно которым принимаются управленческие решения, должны быть понятными, прозрачными и недискриминационными. Сохранность личных данных граждан должна стать ключевым приоритетом государственных служащих, работающих с данными. Взаимодействие между гражданами и государством все чаще будет выстраиваться на данных о них в государственных информационных системах, поэтому выстраивание цифрового доверия к работе с данными в госсекторе крайне важно.

Улучшение цифрового доверия к государственным данным и сервисам на них — непрерывный процесс, без которого будет крайне сложно продвигать новые цифровые решения, менять процессы принятия решений и доверять результатам подобных решений в государственном секторе.

Литература

[1] Attard J., Orlandi F., Auer S. Data driven governments: Creating value through open government data // Transactions on Large-Scale Data-and Knowledge-Centered Systems XXVII: Special Issue on Big Data for Complex Urban Systems. 2016. P. 84-110. URL: https://www.researchgate.net/profile/Judie-Attard-2/publication/307624050_Data_Driven_Governments_Creating_Value_Through_Open_Government_Data/links/5b03f59daca2720ba09964ff/Data-Driven-Governments-Creating-Value-Through-Open-Government-Data.pdf (дата обращения: 12.04.2023).

[2] Liang F., Das V., Kostyuk N., Hussain M. Constructing a data-driven society: China's social credit system as a state surveillance infrastructure // Policy & Internet. 2018. Vol. 10, № 4. P. 415–453. URL: https://www.researchgate.net/profile/Fan-Liang-9/publication/326817957_Constructing_a_Data-Briven_Society_China's_Social_Credit_System_as_a_State_Surveillance_Infrastructure/links/5c40df14299bf12be3cf63d5/Constructing-a-Data-Driven-Society-Chinas-Social-Credit-System-as-a-State-Surveillance-Infrastructure.pdf (дата обращения: 12.04.2023).

[3] Matheus R., Janssen M., Maheshwari D. Data science empowering the public: Data-driven dashboards for transparent and accountable decision-making in smart cities //Government Information Quarterly. 2020. Vol. 37, № 3. Art. 101284. DOI: https://doi.org/10.1016/j.giq.2018.01.006.

[4] Сидоренко Э. Л., Барциц И. Н., Хисамова З. И. Эффективность цифрового государственного управления: теоретические и прикладные аспекты // Вопросы государственного и муниципального управления. 2019. № 2. С. 93–114. URL: https://vgmu.hse.ru/data/2019/06/17/1485071385/Сидоренко,%20Барциц,%20Хисамова%202-2019.pdf (дата обращения: 12.04.2023).

[5] UK Digital Strategy URL: https://www.gov.uk/government/publications/uks-digital-strategy/uk-digital-strategy (дата обращения: 12.04.2023).

[6] United Nations Development Programme. Digital Strategy 2022–2025. URL: https://digitalstrategy.undp.org/documents/Digital-Strategy-2022-2025-Full-Document_ENG_Interactive.pdf (дата обращения: 12.04.2023).
[7] OECD. Going digital integrated policy framework // OECD Digit. Econ. Pap. URL: https://www.oecd-ilibrary.org/docserver/dc930adc-en.pdf?expires=1680803750&id=id&accname=guest&checksum=91C5D21A575EB74540A0EE814918C574 (дата обращения: 12.04.2023).
[8] USAID. Digital Strategy 2020–2024 URL: https://www.usaid.gov/sites/default/files/2022-05/USAID_Digital_Strategy.pdf.pdf (дата обращения: 12.04.2023).
[9] Moran J. W., Brightman B. K. Leading organizational change //Career development international. 2001. Vol. 6, № 2. P. 111–119.
[10] Mergel I., Edelmann N., Haug N. Defining digital transformation: Results from expert interviews. // Government information quarterly. 2019. Vol. 36 (4). Art. 101385. DOI: 10.1016/j.giq.2019.06.002.
[11] Tangi L., Janssen M., Benedetti M., Noci G. Digital government transformation: A structural equation modelling analysis of driving and impeding factors //International Journal of Information Management. 2021. Vol. 60. Art. 102356. DOI: 10.1016/j.ijinfomgt.2021.102356.
[12] Горлов К. Н., Пеньков В. Ф. Формирование доверия бизнеса и власти в условиях цифровизации российской экономики // Власть. 2021. № 3. С. 36–47. DOI: 10.31171/vlast.v29i3.8130.
[13] 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. DOI: 10.22363/2313-1438- 2022-24-3-447-459.
[14] Wachter S. Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR // Computer law & security review. 2018. Vol. 34, № 3. P. 436–449. URL: https://ora.ox.ac.uk/objects/uuid:e49c4ea8-fe71-48ac-9f85-13c3e0ede718/download_file?file_format=pdf&safe_filename=Wachter%2B07.02.18.pdf&type_of_work=Journal+article (дата обращения: 12.04.2023).
[15] World Economic Forum. Earning Digital Trust: Decision-Making for Trustworthy Technologies URL: https://www3.weforum.org/docs/WEF_Earning_Digital_Trust_2022.pdf (дата обращения: 12.04.2023).
[16] Aoki N. An experimental study of public trust in AI chatbots in the public sector. // Government Information Quarterly. 2020. Vol. 37, № 4. Art. 101490. DOI: https://doi.org/10.1016/j.giq.2020.101490
[17] Hengstler, M., Enkel, E., Duelli, S. Applied artificial intelligence and trust – The case of autonomous vehicles and medical assistance devices // Technological Forecasting and Social Change. 2016. Vol. 105. P. 105–120. DOI: 10.1016/j.techfore.2015.12.014.
[18] Lee J. D., See K. A. Trust in automation: Designing for appropriate reliance // Human Factors. 2004. Vol. 46, № 1. P. 50–80. URL: https://journals.sagepub.com/doi/pdf/10.1518/hfes.46.1.50_30392 (дата обращения: 12.04.2023).
[19] Дмитриева Н. Е., Жулин А. Б., Артамонов Р. Е., Титов Э. А. Оценка цифровой готовности населения России // К XXII Апрельской международной научной конференции по проблемам развития экономики и общества. 2021. № 17. URL: https://conf.hse.ru/mirror/pubs/share/464963752.pdf (дата обращения: 12.04.2023).
[20] Bibri S. E., Krogstie J. The emerging data–driven Smart City and its innovative applied solutions for sustainability: The cases of London and Barcelona // Energy Informatics. 2020. Vol. 3. P. 1–42. DOI: 10.1186/s42162-020-00108-6.
[21] Tremblay C. A., Mellouli S., Cheilh M., Khechine H. E-government Service Adoption by citizens: A literature Review and a High-Level Model of Influential Factors // Digital Government: Research and Practice. 2023 Vol. 4, № 2. P. 1–24. DOI: 10.1145/3580369.

[22]Macfarlane S. B., AbouZahr C. A. Matter of Trust: Data Quality and Information Integrity // The Palgrave Handbook of Global Health Data Methods for Policy and Practice. 2019. P. 427–449. DOI: 10.1057/978-1-137-54984-6_22.
[23]Pink S., Lanzeni D., Horst H. Data anxieties: Finding trust in everyday digital mess. Big Data & Society. 2018. Vol. 5, № 1. Art. 2053951718756685. DOI: 10.1177/2053951718756685.
[24]Van Donge W., Bharosa N., Janssen M. Data-driven government: Cross-case comparison of data stewardship in data ecosystems // Government Information Quarterly. 2022. Vol. 39, № 2. P. 101642. DOI: 10.1016/j.giq.2021.101642.
[25]Rosenbaum S. Data governance and stewardship: designing data stewardship entities and advancing data access // Health services research. 2010. Vol. 45, № 5. P. 1442–1455. DOI: 10.1111/j.1475-6773.2010.01140.x.
[26]Namvar M., Intezari A. Wise data-driven decision-making // Responsible AI and Analytics for an Ethical and Inclusive Digitized Society: 20th IFIP WG 6.11 Conference on e-Business, e-Services and e-Society, I3E 2021, Galway, Ireland, September 1–3, 2021, Proceedings 20. Springer International Publishing, 2021. P. 109–119. DOI: 10.1007/978-3-030-85447-8_10.
[27]Mentzas G., Lepenioti K., Bousdekis A., Apostolou D. Data-Driven Collaborative Human-AI Decision Making // Responsible AI and Analytics for an Ethical and Inclusive Digitized Society: 20th IFIP WG 6.11 Conference on e-Business, e-Services and e-Society, I3E 2021, Galway, Ireland, September 1–3, 2021, Proceedings 20. Springer International Publishing, 2021. P. 120–131. DOI: 10.1007/978-3-030-85447-8_11.

Digital Trust as a Key Factor in Building Data-driven Government

Evgeny M. Styrin, Yana A. Rybushkina, Anna G. Sanina

National Research University Higher School of Economics

Public governance has undergone significant changes in recent years. These have been caused by the introduction of new technical and technological tools. The emergence of the concept of data-driven government is inextricably linked with digital transformation. It introduces changes not only in the way management tasks are solved, drives the use of digital tools, but also in the organization of the work of departments and the interaction between citizens and the state. In this context, the phenomenon of digital trust, a new key to the implementation and understanding of datacentric governance, comes to the fore. This article presents an analysis of existing knowledge regarding digital trust, as well as examines barriers and measures for the implementation of data-driven government in Russia. The authors conclude with ways to increase digital trust based on the results of an expert survey. The publication summarizes the existing knowledge about digital trust in the scholarly and practical field and serves as part of a comprehensive study of digital trust.

Keywords: data-driven government, digital trust, digital transformation of public administration, tools for increasing digital trust

Reference for citation: Styrin E. M., Rybushkina Y. A., Sanina A. G. Digital Trust as a Key Factor in Building Data-driven Government // The State and Citizens in the Electronic Environment. Vol. 7 (Proceedings of the XXVI International Joint Scientific Conference «Internet and Modern Society», IMS-2023, St. Petersburg, June 26–28, 2023). — St. Petersburg: ITMO University, 2024. P. 13–23. DOI: 10.17586/2541-979X-2024-7-13–23

Reference

[1] Attard J., Orlandi F., Auer S. Data driven governments: Creating value through open government data // Transactions on Large-Scale Data-and Knowledge-Centered Systems XXVII: Special Issue on Big Data for Complex Urban Systems. 2016. P. 84-110. URL:

https://www.researchgate.net/profile/Judie-Attard-2/publication/307624050_Data_Driven_Governments_Creating_Value_Through_Open_Government_Data/links/5b03f59daca2720ba09964ff/Data-Driven-Governments-Creating-Value-Through-Open-Government-Data.pdf (access date: 12.04.2023).

[2] Liang F., Das V., Kostyuk N., Hussain M. Constructing a data-driven society: China's social credit system as a state surveillance infrastructure // Policy & Internet. 2018. T. 10, № 4. P. 415–453. URL: https://www.researchgate.net/profile/Fan-Liang-9/publication/326817957_Constructing_a_Data-Briven_Society_China's_Social_Credit_System_as_a_State_Surveillance_Infrastructure/links/5c40df14299bf12be3cf63d5/Constructing-a-Data-Driven-Society-Chinas-Social-Credit-System-as-a-State-Surveillance-Infrastructure.pdf (access date: 12.04.2023).

[3] Matheus R., Janssen M., Maheshwari D. Data science empowering the public: Data-driven dashboards for transparent and accountable decision-making in smart cities // Government Information Quarterly. 2020. Vol. 37, № 3. Art. 101284. DOI: https://doi.org/10.1016/j.giq.2018.01.006.

[4] Sidorenko E.L., Bartsits I.N., Khisamova Z.I. The Efficiency of Digital Pub- lic Administration Assessing: Theoretical and Applied Aspects // Public Administration Issues. 2019. № 2. P. 93–114 (in Russian). URL: https://vgmu.hse.ru/data/2019/06/17/1485071385/Сидоренко,%20Барциц,%20Хисамова%202-2019.pdf (access date: 12.04.2023).

[5] UK Digital Strategy URL: https://www.gov.uk/government/publications/uks-digital-strategy/uk-digital-strategy (access date: 12.04.2023).

[6] United Nations Development Programme. Digital Strategy 2022–2025. URL: https://digitalstrategy.undp.org/documents/Digital-Strategy-2022-2025-Full-Document_ENG_Interactive.pdf (access date: 12.04.2023).

[7] OECD. Going digital integrated policy framework // OECD Digit. Econ. Pap. URL: https://www.oecd-ilibrary.org/docserver/dc930adc-en.pdf?expires=1680803750&id=id&accname=guest&checksum=91C5D21A575EB74540A0EE814918C574 (access date: 12.04.2023).

[8] USAID. Digital Strategy 2020–2024 URL: https://www.usaid.gov/sites/default/files/2022-05/USAID_Digital_Strategy.pdf.pdf (дата обращения: 12.04.2023).

[9] Moran J. W., Brightman B. K. Leading organizational change //Career development international. 2001. Vol. 6, № 2. P. 111–119.

[10] Mergel I., Edelmann N., Haug N. Defining digital transformation: Results from expert interviews. // Government information quarterly. 2019. Vol. 36 (4). Art. 101385. DOI: 10.1016/j.giq.2019.06.002.

[11] Tangi L., Janssen M., Benedetti M., Noci G. Digital government transformation: A structural equation modelling analysis of driving and impeding factors // International Journal of Information Management. 2021. Vol. 60. Art. 102356. DOI: 10.1016/j.ijinfomgt.2021.102356.

[12] Gorlov K. N., Pen'kov V. F. Generating Confidence Between Business and Government in Conditions of Digitalization of the Russian Economy// Vlast'. 2021. № 3. P. 36-47 (in Russian). DOI: 10.31171/vlast.v29i3.8130.

[13] Chepelyuk S.G. The phenomenon of "digital trust" in the context of digital government in Russia // RUDN Journal of Political Science. 2022. Vol. 24 (3). P., 447–459 (in Russian). DOI: 10.22363/2313-1438- 2022-24-3-447-459.

[14] Wachter S. Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR // Computer law & security review. 2018. Vol. 34, № 3. P. 436–449. URL: https://ora.ox.ac.uk/objects/uuid:e49c4ea8-fe71-48ac-9f85-13c3e0ede718/download_file?file_format=pdf&safe_filename=Wachter%2B07.02.18.pdf&type_of_work=Journal+article (access date: 12.04.2023).

[15] World Economic Forum. Earning Digital Trust: Decision-Making for Trustworthy Technologies URL: https://www3.weforum.org/docs/WEF_Earning_Digital_Trust_2022.pdf (data assess: 12.04.2023).
[16] Aoki N. An experimental study of public trust in AI chatbots in the public sector. // Government Information Quarterly. 2020. Vol. 37, № 4. Art. 101490. DOI: https://doi.org/10.1016/j.giq.2020.101490
[17] Hengstler, M., Enkel, E., Duelli, S. Applied artificial intelligence and trust – The case of autonomous vehicles and medical assistance devices // Technological Forecasting and Social Change. 2016. Vol. 105. P. 105–120. DOI: 10.1016/j.techfore.2015.12.014.
[18] Lee J. D., See K. A. Trust in automation: Designing for appropriate reliance // Human Factors. 2004. Vol. 46, № 1. P. 50–80. URL: https://journals.sagepub.com/doi/pdf/10.1518/hfes.46.1.50_30392 (access date: 12.04.2023).
[19] Dmitrieva N.E., Zhulin A.B., Artamonov R.E., Titov E.A. Evaluation of digital readiness of the population of Russia // To the XXII April International Scientific Conference on the problems of development of economy and society. 2021. № 17 (in Russian). URL: https://conf.hse.ru/mirror/pubs/share/464963752.pdf (access date: 12.04.2023).
[20] Bibri S. E., Krogstie J. The emerging data–driven Smart City and its innovative applied solutions for sustainability: The cases of London and Barcelona // Energy Informatics. 2020. Vol. 3. P. 1–42. DOI: 10.1186/s42162-020-00108-6.
[21] Tremblay C. A., Mellouli S., Cheilh M., Khechine H. E-government Service Adoption by citizens: A literature Review and a High-Level Model of Influential Factors // Digital Government: Research and Practice. 2023 Vol. 4, № 2. P. 1–24. DOI: 10.1145/3580369.
[22] Macfarlane S. B., AbouZahr C. A. Matter of Trust: Data Quality and Information Integrity // The Palgrave Handbook of Global Health Data Methods for Policy and Practice. 2019. P. 427–449. DOI: 10.1057/978-1-137-54984-6_22.
[23] Pink S., Lanzeni D., Horst H. Data anxieties: Finding trust in everyday digital mess. Big Data & Society. 2018. Vol. 5, № 1. Art. 2053951718756685. DOI: 10.1177/2053951718756685.
[24] Van Donge W., Bharosa N., Janssen M. Data-driven government: Cross-case comparison of data stewardship in data ecosystems // Government Information Quarterly. 2022. Vol. 39, № 2. P. 101642. DOI: 10.1016/j.giq.2021.101642.
[25] Rosenbaum S. Data governance and stewardship: designing data stewardship entities and advancing data access // Health services research. 2010. Vol. 45, № 5. P. 1442–1455. DOI: 10.1111/j.1475-6773.2010.01140.x.
[26] Namvar M., Intezari A. Wise data-driven decision-making // Responsible AI and Analytics for an Ethical and Inclusive Digitized Society: 20th IFIP WG 6.11 Conference on e-Business, e-Services and e-Society, I3E 2021, Galway, Ireland, September 1–3, 2021, Proceedings 20. Springer International Publishing, 2021. P. 109–119. DOI: 10.1007/978-3-030-85447-8_10.
[27] Mentzas G., Lepenioti K., Bousdekis A., Apostolou D. Data-Driven Collaborative Human-AI Decision Making // Responsible AI and Analytics for an Ethical and Inclusive Digitized Society: 20th IFIP WG 6.11 Conference on e-Business, e-Services and e-Society, I3E 2021, Galway, Ireland, September 1–3, 2021, Proceedings 20. Springer International Publishing, 2021. P. 120–131. DOI: 10.1007/978-3-030-85447-8_11.