Человек и культура
Правильная ссылка на статью:
Былевский П.Г. — Социально-культурные риски «больших пользовательских данных» российских граждан // Человек и культура. – 2023. – № 4. DOI: 10.25136/2409-8744.2023.4.43896 EDN: WEVENQ URL: https://nbpublish.com/library_read_article.php?id=43896

Социально-культурные риски «больших пользовательских данных» российских граждан

Былевский Павел Геннадиевич

ORCID: 0000-0002-0453-526X

кандидат философских наук

доцент, кафедра информационной культуры цифровой трансформации; кафедра международной информационной безопасности, Московский государственный лингвистический университет

119034, Россия, Москва, г. 119034 Москва, ул. Остоженка, 36, оф. 106

pr-911@yandex.ru

Статья из рубрики "Электронная культура и интернет"

DOI:

10.25136/2409-8744.2023.4.43896

EDN:

WEVENQ

Дата направления статьи в редакцию:

24-08-2023

Аннотация: Предметом исследования являются современные социально-культурные риски граждан России как пользователей компьютерно-телекоммуникационных технологий и интернет-коммуникаций. Объектом исследования выступают такие последствия цифровой трансформации, как преимущества и угрозы автоматизации генерации, сбора и анализа «больших пользовательских данных». Актуальность темы обусловлена принятием Правительством России «Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации» 22 декабря 2022 года. Рассматриваются социально-культурные риски и угрозы, в том числе традиционным ценностям и идентичности, связанные с нахождением в «цифровой» среде и действиями пользователей. Особое внимание уделено анализу угроз российским гражданам со стороны «электронного тоталитаризма» недружественных стран и глобальных корпоративных цифровых платформ, а также возможностям противодействия. Новизна исследования социально-культурных рисков информационной безопасности в применении профильного системно-динамического культурологического подхода, эволюционного и структурно-функциональных методов. Учитывая

стремительность изменения ландшафта социально-культурных цифровых рисков в последние годы, материалами исследования служили российские научные публикации в журналах перечня ВАК (категорий К1, К2) и иностранные в международной базе Scopus (квартилей Q1, Q2) 2021–2023 гг., «переломных» для формирования современных цифровых угроз. Особым вкладом является использование наработок, полученных в ходе исследований научно-практических коммуникаций в информационной безопасности финансовой сферы, проводившихся под руководством автора в 2010–2023 гг. Результатами исследования являются выводы о необходимости учёта баланса преимуществ и угроз «цифровизации», управления социально-культурными рисками «больших пользовательских данных» в интересах российских граждан. Основным выводом является определение решающей роли в развитии и повышении общегражданской культуры информационной безопасности не только профессиональной деятельности государственных органов и профильных организаций, но и всех граждан.

Ключевые слова:

большие пользовательские данные, анализ больших данных, цифровые социокультурные риски, информационная безопасность, цифровая трансформация, цифровой тоталитаризм, традиционные ценности, социокультурная идентичность, дезинформация, манипулирование сознанием

Введение

Цифровая трансформация, универсальное повсеместное, непрерывное и всё более разнообразное применение компьютерно-телекоммуникационных технологий и интернет-коммуникаций, несёт многие возможности, неведомые прежде. Необходимым условием использования преимуществ цифровой трансформации является уже свершившееся превращение всех граждан России в пользователей компьютерно-телекоммуникационных технологий и интернет-коммуникаций. Практически все граждане круглосуточно живут в «цифровой среде», являясь как объектами, так и субъектами цифровизации, возрастает их вовлечённость и пользовательская активность. Однако «большие пользовательские данные», включая данные о гражданах, могут использоваться как для улучшения цифровых сервисов, так и для получения конфиденциальных сведений, а также для манипулирования сознанием, обмана, дезинформации, вовлечения в деструктивную деятельность.

Феномен «больших пользовательских данных» ярко и выпукло представляет тенденцию возрастания удельного веса социально-культурных факторов информационной безопасности в сравнении с техническими и прочими аспектами; необходимость выработки соответствующей массовой культуры требует научного осмысления методами культурологии. Чтобы определить эффективные средства снижения до приемлемого уровня социально-культурных рисков автоматизации генерации, сбора и анализа «больших пользовательских данных» российских граждан, в настоящей статье применяется культурологический анализ. Цель статьи заключается в установлении путей достижения оптимального баланса преимуществ и угроз «больших пользовательских данных», текущее соотношение которых является объектом исследования. Предметом исследования служат современные социально-культурные риски граждан России как пользователей компьютерно-телекоммуникационных технологий и интернет-коммуникаций.

1. Проблема баланса преимуществ и угроз «цифровых двойников» граждан

«Большие пользовательские данные» являются своего рода «цифровым двойником» каждого человека и социальных групп, материалом для автоматизированного анализа в режиме реального времени действий, предпочтений (музыкальных [1] и др.) и привычек, для «распознавания» эмоций и настроений, намерений, чувств и мыслей. Возможности их использования двойственны, грань между преимуществами и рисками цифровизации бывает очень тонкой, для различения существенных нюансов требуется высокая культура информационной безопасности, как профессиональная, так и общегражданская. Эта грань способна обретать динамику, меняться: вчерашние преимущества способны быстро и неожиданно оборачиваться новыми угрозами, достигающими критического уровня.

Стремительное развитие и всё новые применения технологий сопровождаются масштабными социально-культурными переменами и тектоническими сдвигами как на национальном уровне, так и в международных отношениях, разрушением однополярного глобализма, в том числе в области цифровых сервисов [2]. В таких современных реалиях для соблюдения необходимого баланса использования преимуществ и минимизации сопутствующих рисков цифровой трансформации, в частности, «больших пользовательских данных», проявилась необходимость в соответствующей массовой культуре безопасности. Подтверждением служит «Концепция формирования и развития культуры информационной безопасности граждан Российской Федерации», принятая 22 декабря 2022 г. Распоряжением Правительства России № 4088-р.

В обеспечении информационной безопасности велика роль соответствующей культуры граждан, их общей осторожности и отсутствия иллюзий о якобы доверенном характере интернет-среды, отсутствии в ней угроз [3]. Проецируя на компьютерно-телекоммуникационные технологии привычные реалии, сами граждане в первую очередь заботятся о защите тайны своей личной жизни (содержания переписки и переговоров, документов, фотографий, видеозаписей, данных о местоположениях, действиях, поведении и др.), понимая сопряжённые риски и угрозы репутации, клеветы, шантажа, нарушения авторских прав и т.д. По мере завершения анонимности пользователей интернета и мобильной связи повышается осторожность в отношении содержания почтовой, голосовой, видеосвязи, обмена короткими сообщениями и файлами, оценок, комментариев и собственных публикаций в интернете, разрешений внешнего доступа к приложениям и данным на своих мобильных устройствах [4].

Теоретически любые компьютерные данные могут быть определены, прямо или косвенно, как пользовательские и персонализированы (соотнесены с той или иной идентифицированной личностью) методом перекрёстного сопоставления различных баз. В рамках имеющихся данных технически возможно установить и юридически доказать, что, где и в какой момент времени делал тот или иной пользователь, группы пользователей с практически любым статистическим охватом. Для этого необходимо исследование (в случае инцидентов безопасности, тем более преступлений I расследование), выясняющее степень и характер участия в операциях с данными разработчиков, изготовителей, провайдера сервиса, пользователя и других людей. Чем большую опасность представляет инцидент информационной безопасности, чем больше ресурсов, включая специалистов самой высокой квалификации, задействовано, тем более подробной может быть детализация «авторства» или причастности к обработке конкретных граждан.

«Большие пользовательские данные» являются важной областью обеспечения информационной безопасности, как национальной, общественной, так и личной, включая необходимость безопасной общегражданской пользовательской культуры. Со стороны государства законом защищается тайна личной жизни, переписки, личные финансовые, медицинские, биометрические и другие сведения, в том числе в цифровом виде. Проводится последовательная государственная политика защиты персональных данных граждан, которая пока в основном относится только к сведениям о зафиксированных в официальных документах долговременных личных социальных статусах-идентификаторах (имя, фамилия, отчество, дата и место рождения, адрес постоянного жительства и т.д.).

Однако «большие пользовательские данные» в настоящий момент можно считать наиболее содержательными с точки зрения возможностей автоматизированного «извлечения знаний» о гражданах и наименее защищёнными от сопряжённых угроз. Пока со стороны и государства, и граждан наблюдается недооценка рисков, сопряженных с «большими пользовательскими данными». В то время, как для противодействия таким угрозам крайне важны знания граждан об их существовании, умение их распознавать, правильно реагировать, сообщать в уполномоченные организации о подобных инцидентах [5]. Проблема проясняется по мере её обострения, вызванного сохранением трансграничности интернет-коммуникаций в новых, намного менее благоприятных условиях: с 2014 года существенно сократилось международное сотрудничество в противодействии киберпреступности, трансграничная агрессивность которой резко возросла [6]. Существенно усилились угрозы и повысились риски трансграничных мошенничеств, психологических спецопераций против граждан России, кибердиверсий, антироссийских действий со стороны недружественных государств и глобальных цифровых платформ, базирующихся в США.

2. Структурно-функциональные особенности «больших пользовательских данных»

Уникальные, небывалые прежде возможности получения нужных сведений открывает автоматизация генерации и анализа данных, в частности – собственно пользовательских данных, включающих биометрические. Большие пользовательские данные – это электронное цифровое представление параметров пребывания человека как объекта и его активных действий в компьютерно-телекоммуникационных системах. Разнообразные «цифровые следы» формируют «цифрового двойника» пользователя, постоянно обновляемого в режиме реального времени. Структурно эти данные можно подразделить на два основных полярных вида (с дальнейшим детализированным ранжированием): результаты сознательных действий пользователей и данные о людях, автоматически генерируемые при нахождении в зоне действия сетевых цифровых датчиков.

Сознательные действия пользователей в цифровой среде – это их общение посредством мобильных и интернет-коммуникаций (голосовая и видеосвязь, короткие и почтовые текстовые сообщения, пересылка файлов), оценки и комментарии, создание и публикация контента на интернет-ресурсах, в социальных сетях и посредством блоггерских сервисов. Основным оборудованием при этом служат персональные компьютеры, подключенные к интернету, как настольные, так и мобильные. К пользовательским данным относится не только непосредственный сознательно создаваемый пользователем результат (текстовое сообщение, пост и т.д.), но и комплекс фиксируемых сопутствующих разнообразных технических параметров. Провайдерам интернет-сервисов, непосредственным операторам больших пользовательских данных, доступны характеристики типа, производителя, программного обеспечения,

идентификационный номер и др. используемого компьютерного устройства, а также всех совершённых с его помощью действий пользователя: перечень и время просмотра интернет-ресурсов, запущенных программ, полученные и отправленные сообщения, файлы и т.д.

Второй полюс пользовательских данных – это данные о людях, которые автоматически, без их участия, а часто и без ведома, генерируются и обрабатываются (передаются по сетям, собираются, анализируются и хранятся). Такие данные о людях генерируются «устройствами ввода» персональных компьютеров и «интернета вещей» ‖ носимых компьютеризованных устройств (гаджетов), а также датчиками «интернета вещей», промышленной и бытовой «умной» компьютерной техники [7]. Ярким примером могут служить цифровые системы видеонаблюдения в общественных местах с возможностью автоматизированного распознавания лиц и идентификации граждан [8]. Генерироваться оцифровкой, в том числе дистанционно, могут любые данные о различных параметрах человека, способные иметь решающее значение: местоположение [9], внешний вид, голос, речь и сопровождающие звуки, передвижения и действия, жесты и мимика, запахи, частота пульса и дыхания, электроэнцефалограммы и электрокардиограммы и др.

Функционально анализ пользовательских данных необходим для поддержки, оптимизации и улучшения интернет-сервисов и используемого компьютерно-телекоммуникационного оборудования. Большие пользовательские данные отличаются не столько количественными характеристиками, объёмами, сколько непрерывным потоковым характером, постоянным обновлением в режиме реального времени. Автоматизация их аналитики позволяет почти без задержек использовать результаты для обратного воздействия на пользователя (в том числе на большие социальные группы) в интерактивном режиме реального времени. Сводный анализ различных баз больших пользовательских данных позволяет их операторам (или покупателям) получать статистику, которая может включать секретные сведения, вплоть до относящихся к государственной тайне [10]. Эти возможные функции могут исполняться как в интересах пользователя и его родной страны, так и против, в разных пропорциях сочетаний преимуществ и угроз. Подобные злоупотребления со стороны организаций, предоставляющих цифровые сервисы, во многом становятся возможными из-за уязвимостей самих пользователей, недостаточной защиты ими собственных пользовательских данных.

Компьютерно-телекоммуникационное оборудование, программное обеспечение и цифровые сервисы являются только техническими средствами общения людей – социально-культурных субъектов. С точки зрения культурологии информационная безопасность обеспечивает защиту прав людей на ценности, а главный источник угроз – нарушители этих прав, люди и организации, стремящиеся получить выгоду за счёт ущерба другим. Компьютерно-телекоммуникационные технологии сами по себе нейтральны, но могут в достаточно широком диапазоне функционально использоваться людьми и для равноправного взаимовыгодного сотрудничества, и для эксплуатации, нанесения ущерба, деструктивных, противоправных действий. Столь же противоположным образом, в зависимости от социально-культурного контекста, могут применяться одни и те же «большие пользовательские данные», оборудование для их генерации и обработки. Государственная политика и общегражданская культура информационной безопасности необходимы, чтобы своевременно учитывать такие риски, прогнозировать подобные угрозы и противодействовать им.

3. Эволюционная динамика цифровых социально-культурных угроз российским

гражданам

Социально-культурные угрозы «больших пользовательских данных», как и их прежде неведомые преимущества, обусловлены технологиями автоматизированного анализа, потенциального «всезнания» обо всех и каждом, находящихся в зоне действия датчиков цифровых сетевых устройств. Простая диалектика заключается в том, что если эти технологии используются на всеобщее благо, то это преимущества, если же для причинения ущерба – то угрозы. Более сложная диалектика связана с тем, что одни люди могут извлекать выгоду за счёт причинения ущерба другим, в том числе посредством цифровых технологий – и это уже область информационной безопасности. Именно поэтому в массовой культуре очень тонкая, зыбкая и колеблющаяся грань между утопическим и антиутопическим [11] восприятием возможностей технологий «искусственного интеллекта», основанных на автоматизированном анализе «больших пользовательских данных». Цифровой «рай», в котором техника делает за человека всю работу, решает все проблемы и принимает важнейшие решения, легко оборачивается «цифровым тоталитаризмом» [12], внушающим ложные радости и иллюзорное счастье погрузившимся в убожество эксплуатируемым людям [13]. Стихийное осознание таких социально-культурных угроз способствовало различной критике и общественным кампаниям противодействия [14].

В какой степени в конкретной ситуации применение компьютерно-телекоммуникационных решений служит взаимовыгодному сотрудничеству, а в какой является инструментом разрушения, подчинения и эксплуатации, должен определять научный анализ [15]. Противодействие социально-культурным угрозам, предотвращение и минимизация ущерба ценностям относятся к культуре информационной безопасности, профильной наукой выступает культурология. Эволюционный культурологический анализ позволяет определить изменения в технологиях, сервисах, обществе и культуре, которые привели к созданию нового ландшафта социально-культурных угроз цифровой трансформации, в частности, роли «больших пользовательских данных». Структурно-функциональный анализ помогает определить перечень актуальных угроз, их мишеней и потенциальных жертв, характер и размеры ущерба, средства безопасности.

В целом успешное решение в 2000-е годы организационно-технических вопросов обеспечения информационной безопасности, включая защиту персональных данных, позволило понизить риски нарушений, ущерба от действий злоумышленников до приемлемого уровня. Цифровая трансформация, превращение практически всех граждан России в пользователей мобильных компьютерных устройств и покрытие беспроводным широкополосным доступом в интернет привело в 2010-е годы к качественному изменению ландшафта угроз, в особенности социально-культурных. Пользователями компьютерно-телекоммуникационных технологий стали все граждане, пользование интернет-сервисами превратилось в одну из первостепенных культурных потребностей, оказалось сопряжено с ценностями высокого уровня, включая традиционные, определяющие социально-культурную идентичность [16].

Особую ценность для мошенников (как и для недобросовестных специалистов по рекламе и маркетингу, включая политические) для массированных атак (фишинга) [17] приобрели базы персональных данных, использование которых помогало лучше входить в доверие к потенциальным жертвам [18]. В «Отчёте Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России 1.09.2018 – 31.08.2019)» отмечено: самой частой мишенью

злоумышленников стали не технические средства интернет-банкинга, а социально-культурные, психологические уязвимости клиентов; главным инструментом атак, вместо прежнего специализированного вредоносного программного обеспечения (банковских «вирусов»), стали мошеннические уловки («социальная инженерия»). В социальных сетях и мессенджерах начали действовать мошенники (также «телефонные») и злоумышленники, которые побуждали уязвимых пользователей к деструктивной активности [19], вовлекали в группы самоубийств, потребления наркотиков, кибербуллинга (травли), «школьных расстрелов», экстремального поведения, политического экстремизма и др.

В это время сформировался феномен «больших пользовательских данных», автоматизация тщательного и подробного отслеживания и анализа поведения личности и социальных групп, способный служить «ключом» доступа к чужим ценностям от денег до убеждений. Для операторов больших пользовательских данных, начиная с глобальных цифровых платформ и сервисов, разные форматы торговли «большими данными» своих пользователей стали одним из основных источников прибылей. Автоматизация анализа политических предпочтений и управления поведением сотрудников организаций [20], пользователей в социальных сетях привело к повышению социально-культурных рисков, став мощным инструментом управления политической мобилизацией [21], инспирирования извне государственных переворотов, известных как «цветные революции», а также скрытого внешнего влияния на внутреннюю политику государств-жертв.

Триггером, обострившим проблему социально-культурных угроз безопасности «больших пользовательских данных», стали 2020–2022 годы. Глобальные жёсткие меры карантина, введённые в 2020 году в связи с завышенными оценками угроз коронавируса, привели к скачкообразному росту количества пользователей, объёмов использования финансовых, образовательных и других дистанционных услуг, видеоконференций и мессенджеров, увеличению перечня и значимости сопряжённых ценностей. Начало Специальной военной операции на Украине в 2022 году ознаменовало обострение кризиса и повышение конфликтности международных отношений, разрушение однополярного глобализма, в том числе в области цифровых сервисов [22].

Кроме антироссийских технологических санкций недружественных государств, проявилась также социально-культурная угроза высокого уровня: глобальные цифровые платформы, в духе «цифрового тоталитаризма», ввели дискриминационную цензуру в отношение официальной российской прессы, журналистов и блогеров [23]. Пользовательские данные российских граждан, их сетевого поведения стали использоваться для изготовления и трансляции фейк-новостей, целевой дезинформации, пропаганды гендерного радикализма и «чайлдфри» [24], «культуры отмены» [25] и т.п.

Результаты

Проведённое исследование показывает сложную динамику соотношения преимуществ и социально-культурных угроз и рисков, связанную с «большими пользовательскими данными» граждан России. Выявлено, что превращение всех граждан в пользователей и объекты компьютерно-телекоммуникационных технологий в результате цифровой трансформации привело к появлению критических угроз социально-культурным ценностям. Объектами атак стали не столько технические устройства, сколько сознание и личности граждан; в роли злоумышленников и нарушителей стали выступать не только киберпреступники, но и недружественные государства, глобальные цифровые

платформы, базирующиеся в США. Злоупотребления зарубежных операторов выражаются в неконтролируемой торговле «большими пользовательскими данными» россиян, извлечении из них с помощью автоматизированного анализа конфиденциальных сведений, используемых для манипулирования сознанием и скрытого деструктивного воздействия (дезинформации) на поведение и деформацию ценностей, социально-культурной идентичности.

Главный вывод исследования: противодействие социально-культурным угрозам, снижение рисков «больших пользовательских данных» требует как целевых государственных мер в области информационной безопасности, так и развития профильной общегражданской культуры. К государственным мерам относятся развитие федерального законодательства в области технологически-инфраструктурного обеспечения цифрового суверенитета, независимости от импорта технологий, обязательства операторов данных хранить и обрабатывать данные на территории России, а также наделение государственных органов полномочиями блокировать доступ к запрещённому контенту и интернет-ресурсам, отменять регистрацию доменных имён, привлекать к ответственности нарушителей.

Прогнозируется усиление пока неразвитого государственного регулирования безопасности «больших пользовательских данных» российских граждан; предстоит развить законодательное регулирование их оборота, начатое в 2018 году федеральным законопроектом № 571124-7 «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации». Назрела необходимость повышения профильной общегражданской культуры информационной безопасности, разработка обучающих и методических материалов об угрозах, рисках и средствах обеспечения безопасности «больших пользовательских данных», а также трансляция их на массовую аудиторию образовательными организациями, прессой и социальной рекламой.

Библиография

1. Сердечный А.Л., Коденцева Н.Г., Петелин А.А., Лемешко А.А., Руженко В.Е. Анализ рисков при помощи информационной карты музыкальных предпочтений // Информация и безопасность. 2021. Т. 24. № 4. С. 601-608. DOI: 10.36622/VSTU.2021.24.4.013
2. Яковлева С.Н., Хамидулин Р.Ф. Информационные риски как угроза социальной безопасности современного цифрового общества // Известия Тульского государственного университета. Гуманитарные науки. 2022. №3. С. 67-77. DOI: 10.24412/2071-6141-2022-3-67-77
3. Wang X., Li Y., Khasraghi H., Trumbach Ch. The mediating role of security anxiety in internet threat avoidance behavior // Computers & Security. 2023. Vol. 134. DOI: 10.1016/j.cose.2023.103429
4. Rodríguez-Priego N., Porcu L., Kitchen Ph. Sharing but caring: Location based mobile applications (LBMA) and privacy protection motivation // Journal of Business Research. 2022. Vol.140. Pp. 546-555. DOI: 10.1016/j.jbusres.2021.11.022
5. Jiang T., Shen G., Guo Ch., Cui Yu., Xie B. BFLS: Blockchain and Federated Learning for sharing threat detection models as Cyber Threat Intelligence // Computer Networks. 2023. Vol. 224. DOI: 10.1016/j.comnet.2023.109604
6. Al-Kasasbeh B. Model of the information security protection subsystem operation and method of optimization of its composition // Egyptian Informatics Journal. 2022. Vol. 23. Iss. 3. Pp. 511-516. DOI: 10.1016/j.eij.2022.05.003

7. Najmi Kh., AlZain M., Masud M., Jhanjhi N., Al-Amri J., Baz M. A survey on security threats and countermeasures in IoT to achieve users confidentiality and reliability // Materials Today: Proceedings. 2023. Vol. 81, Part 2. Pp. 377-382. DOI: 10.1016/j.matpr.2021.03.417
8. Чаплыгина В.Н., Москвичев А.А. Применение лицевой биометрии для информационно-аналитической поддержки розыскных мероприятий // Криминалистика: вчера, сегодня, завтра. 2022. № 1 (21). С. 177-187. DOI: 10.55001/2587-9820.2022.29.81.016
9. Ложис З.З., Чупахин Р.В. Актуальные проблемы использования геолокационных данных при розыске несовершеннолетних, пропавших без вести // Российский следователь. 2022. № 4. С. 23-27. DOI: 10.18572/1812-3783-2022-4-23-27
10. Былевский П.Г. Пользовательские и персональные данные — анализ рисков извлечения знаний // Вопросы защиты информации. 2023. № 1 (140). С. 35-40. DOI: 10.52190/20732600_2023_1_35
11. Яковлев М.В. Государство датификации и его дисциплинарные техники: направленность социально-политической трансформации // Вестник Томского государственного университета. Философия. Социология. Политология. 2023. № 71. С. 246-259. DOI: 10.17223/1998863X/71/23
12. Бобринский Н.А. Московская карательная инновация: промежуточные итоги // Закон. 2021. № 6. С. 89-95. EDN: XGHMYM
13. Кнорре Б.К., Мурашова А.А. «В начале было слово...», а в конце будет число? Православие и антицифровой протест в России: с 1990-х до коронавируса // Мир России. Социология. Этнология. 2021. Т. 30. № 2. С. 146-166. DOI: 10.17323/1811-038X-2021-30-2-146-166
14. Iyanna Sh., Kaur P., Ractham P., Talwar Sh., Islam N. Digital transformation of healthcare sector. What is impeding adoption and continued usage of technology-driven innovations by end-users? // Journal of Business Research. 2022. Vol. 153. Pp. 150-161. DOI: 10.1016/j.jbusres.2022.08.007
15. Гайворонская Я.В. Крылья Икара: о рисках и угрозах цифровой трансформации общества // Advances in Law Studies. 2021. Т. 9. № 4. С. 81-85. DOI: 10.29039/2409-5087-2021-9-4-81-85
16. Скуднова Т.Д., Иванченко О.В. Трансформация российской идентичности в условиях социальной неопределенности: трансдисциплинарный анализ // Социально-гуманитарные знания. 2022. № 2. С. 207-215. DOI: 10.34823/SGZ.2022.2.51786
17. Завьялов А.Н. Интернет-мошенничество (фишинг): проблемы противодействия и предупреждения // Baikal Research Journal. 2022. Т. 13. № 2. DOI: 10.17150/2411-6262.2022.13(2).36
18. Frank M., Jaeger L., Ranft L. Contextual drivers of employees' phishing susceptibility: Insights from a field study // Decision Support Systems. 2022. Vol. 160. DOI: 10.1016/j.dss.2022.113818
19. Галяшина Е.И., Никишин В.Д. Деструктивное речевое поведение в цифровой среде: факторы, детерминирующие негативное воздействие на мировоззрение пользователя // Lex Russica (Русский закон). 2021. Т. 74. № 6 (175). С. 79-94. DOI: 10.17803/1729-5920.2021.175.6.079-094
20. Ogbanufe O. Enhancing End-User Roles in Information Security: Exploring the Setting, Situation, and Identity // Computers & Security. 2021. Vol. 108. DOI: 10.1016/j.cose.2021.102340

21. Денисенко П.В., Есиев Е.Т. Интернет-технологии как инструмент политической мобилизации в эпоху big data // Вопросы политологии. 2021. Т.11 . № 4 (68). С. 1115-1121. DOI: 10.35775/PSI.2021.68.4.017
22. Левашов В.К., Гребняк О.В. Актуальные изменения социальных сетей и цифровой среды в период специальной военной операции на Украине // Социальные и гуманитарные знания. 2022. Т. 8. № 2 (30). С. 204-213. DOI: 10.18255/2412-6519-2022-2-204-213
23. Ровинская Т.Л. Свобода слова в условиях цифровой диктатуры IT-корпораций // Полис. Политические исследования. 2022. № 2. С. 22-36. DOI: 10.17976/jpps/2022.02.03
24. Слышкин Г.Г., Малыгина Л.Е., Павлова Е.С. Радикальный феминный и маскулинный медиадискурс в аспекте лингвобезопасности // Верхневолжский филологический вестник. 2022. № 2 (29). С. 53-60. DOI: 10.20323/2499-9679-2022-2-29-53-60
25. Былевский П.Г., Цацкина Е.П. Феноменологический анализ явления «культура отмены» // Вестник Московского государственного лингвистического университета. Гуманитарные науки. 2022. № 2 (857). С. 162-169. DOI: 10.52070/2542-2197_2022_2_857_16

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

В рецензируемой статье «Социально-культурные риски "больших пользовательских данных" российских граждан» предмет исследования – это современные социально-культурные риски граждан России как пользователей компьютерно-телекоммуникационных технологий и интернет-коммуникаций. Цель исследования вытекает из названия работы и в работе сформулирована следующим образом: установление путей достижения оптимального баланса преимуществ и угроз «больших пользовательских данных».
Методология исследования в явном виде не обозначена. Автор использует аналитический метод как метод исследования, который используется для диагностики проблем и создания гипотез, позволяющих их решить. В работе данный метод был использован для рассмотрения проблемы баланса преимуществ и угроз «цифровых двойников» граждан, раскрытия структурно-функциональных особенностей «больших пользовательских данных», выявлении эволюционной динамики цифровых социально-культурных угроз российским гражданам.
Актуальность настоящего исследования обусловлены: во-первых, нарастающей тенденцией датафикации жизни человека; во-вторых, реально существующими угрозами информационной безопасности личности и её сознания в условиях нарастания деструктивного информационного воздействия; в-третьих, необходимостью и общественной потребностью создания основ системы парирования и локализации угроз.
Научная новизна публикации связана с обоснованием положения о том, что превращение всех граждан в пользователей и объекты компьютерно-телекоммуникационных технологий в результате цифровой трансформации привело к появлению критических угроз социально-культурным ценностям. В работе показано, что объектами атак стали не столько технические устройства, сколько сознание человека; в роли злоумышленников и нарушителей стали выступать не только киберпреступники, но и недружественные государства. Аналитическое исследование показало, что

противодействие социально-культурным угрозам, снижение рисков «больших пользовательских данных» требует как целевых государственных мер в области информационной безопасности, так и развития профильной общегражданской культуры. Можно предположить, что это, по мысли автора, и есть пути достижения оптимального баланса преимуществ и угроз «больших пользовательских данных».

Выводы, сформулированные в статье, в целом обоснованы. Содержание соответствует требованиям научного текста. Однако, стоит обратить внимание, что проблема рисков в статье не раскрыта (фактически риск в работе отождествлён с угрозами, но это далеко не так).

Данное исследование характеризуется общей последовательностью и грамотностью изложения. Статье присущ хороши уровень научной концептуализации. Она будет представлять интерес для специалистов, исследующих проблемы информационной безопасности в социокультурном контексте.

Библиография работы включает всего 25 публикаций и включает издания как на русском, так и на иностранных языках. Таким образом, апелляция к основным оппонентам из рассматриваемой области присутствует в полной мере.

Вывод: Статья «Социально-культурные риски "больших пользовательских данных" российских граждан» имеет научно-теоретическую значимость, соответствует отрасли – социологические науки. Работа может быть опубликована.