

УДК 316.7

Типология социальных рисков в системе защиты персональных данных

Сазонова Анна Львовна^(*)

an-netic@yandex.ru

SPIN-код: 5636-7087

МГТУ им. Н.Э. Баумана, Москва, Россия

Аннотация. Проанализированы различные виды социальных рисков в системе защиты персональных данных в контексте цифровизации. Основное внимание уделено социальным рискам, возникающим в процессе взаимодействия людей с цифровыми технологиями и платформами во всех сферах жизнедеятельности общества. Сформулировано определение социальных рисков на основе социологических теорий. Выявлены основания для типологии социальных рисков в изучаемой области на макроуровне, а также предложена конкретизация социальных рисков на микроуровне, в повседневных практиках пользователей цифровых платформ и сервисов. При этом отмечен комплексный характер проявления социальных рисков в системе защиты персональных данных, что требует дальнейших исследований.

Ключевые слова: персональные данные, защита персональных данных, социальные риски, цифровизация, повседневные практики

Typology of social risks in the system of personal data protection

Sazonova Anna Lvovna^(*)

an-netic@yandex.ru

SPIN-code: 5636-7087

BMSTU, Moscow, Russia

Abstract. The article analyzes various types of social risks in the system of personal data protection in the context of digitalization. The main attention is paid to social risks that arise in the process of interaction between people and digital technologies and platforms in all areas of society's life. The definition of social risks is formulated based on sociological theories. The article identifies the grounds for the typology of social risks in the studied area at the macro level, and also proposes the specification of social risks at the micro level, in the everyday practices of users of digital platforms and services. At the same time, the article notes the complex nature of the manifestation of social risks in the system of personal data protection, which requires further research.

Keywords: personal data, personal data protection, social risks, digitalization, daily practices

Введение. Современное общество характеризуется высокой степенью цифровизации, что приводит не только к новым возможностям, но и к новым угрозам. Одной из таких угроз является рост социальных рисков, связанных с защитой персональных данных в условиях активного использования цифровых сервисов. Развитие цифровых платформ сопровождается увеличением

объема хранимых данных, что делает эти платформы более уязвимыми для атак. При этом низкий уровень цифровой грамотности населения и активность кибермошенников также повышают социальные риски [1]. Понимание природы этих рисков требует не только применения социологических подходов к изучению риска и его влияния на общественные процессы, но и рассмотрения возможных вариантов типологизации новых видов риска.

Материалы и методы. Прежде всего, необходимо определить основные понятия в изучаемой области и проанализировать теоретические подходы.

Персональные данные представляют собой любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) [2]. Защита персональных данных рассматривается как многоуровневая система мер, направленных на обеспечение прав субъектов данных и предотвращение неправомерного использования их личной информации [3].

Концепция «общества риска», разработанная Э. Гидденсом [4] и Э.У. Беком получила широкое распространение в социальной философии. В основе подхода У. Бека лежит идея о том, что переход к эпохе риска является неизбежным следствием модернизации, обусловленным внутренними механизмами общественного развития. Этот процесс происходит поэтапно: сначала риск формируется как «побочный эффект» технологического и социального прогресса, а затем осознается как фундаментальная характеристика современного общества [5].

Н. Луман предложил социологическую теорию риска, согласно которой риск является не объективной реальностью, а социальной конструкцией, формируемой через коммуникацию. Н. Луман подчеркивает: «Бессмысленно говорить о том, что современная технология «рискованная». Только коммуникация о технологии, коммуникация о решениях по поводу использования/неиспользования той или иной технологии может быть «рискованной» [6].

О.Н. Яницкий, следуя концепции У. Бека, рассматривает два возможных пути адаптации к новой эпохе — креативный и деструктивный. Если первый способствует росту инновационного потенциала общества, то второй ведет к демодернизации и регрессу. По его мнению, «страны, избравшие первый путь, в конечном счете увеличивают свой креативный потенциал и жизненный ресурс»; второй же вариант сопровождается «процессами прогрессирующей демодернизации» [7]. О.Н. Яницкий также характеризует современную Россию как «общество всеобщего риска», объясняя это рядом факторов: слабая институционализация риск-рефлексии, преобладание традиционного, а не инновационного подхода к анализу рисков в научной среде, а также размывание границ между социальной нормой и девиацией в массовом сознании.

В.И. Чупров и Ю.А. Зубок также отмечают, что «Качественные изменения социальной среды, связанные с появлением глобальной угрозы для жизни человека, придали понятию «риск» новую направленность. Главным его фактором стала не внешняя угроза, а сам человек, последствия его производственной деятельности. Более того, риск приобрел глобальный характер, затронув жизненные интересы всех людей» [8].

Таким образом, современные социологи сходятся во мнении, что риск в цифровом обществе — это неотъемлемый элемент развития, формируемый самим обществом в процессе его модернизации. Он носит конструктивный или деструктивный характер в зависимости от степени осознанности, готовности к саморефлексии и способности к адаптации к новым вызовам. Исходя из рассмотренных теоретических подходов, социальные риски можно определить, как угрозы и неопределенности, возникающие в результате социальных, экономических, нормативно-правовых и технических изменений, которые влияют на структуру общества, социальные отношения и безопасность индивидов.

Результаты. Важно отметить, что данные виды социального риска — экономический, технико-технологический, нормативно-правовой и непосредственно социальный, с одной стороны, могут служить вариантом типологии, но, с другой стороны, настолько тесно переплетены, что их анализ требует перевода на уровень более конкретных повседневных практик. Риски проявляются в самых различных сферах жизнедеятельности — от образования и трудоустройства до общения в сети и потребления цифровых услуг. Эти риски не абстрактны — они конкретизируются в виде реальных угроз, с которыми сталкиваются люди в повседневной цифровой реальности. Однако такая типология может существовать лишь в рамках теоретической модели, поскольку на практике социальные риски редко можно однозначно приписать к какой-либо отдельной сфере жизнедеятельности. Это связано с тем, что социальные риски представляют собой сложные, многогранные явления, которые переплетаются между собой и часто затрагивают несколько аспектов сразу. Например, риски, связанные с защитой персональных данных, могут одновременно иметь экономическое и технологическое измерение, затрагивать вопросы социальной безопасности и требовать регулирования на нормативно-правовом уровне [9].

Поэтому кроме теоретической модели типологии рисков макроуровня необходимо выделять социальные риски в повседневных практиках. На микроуровне повседневной жизни крайне сложно описать все существующие социальные риски, связанные с защитой персональных данных, однако можно выделить наиболее распространенные угрозы.

Одним из наиболее острых рисков остаются финансовые угрозы, возникающие в результате кражи персональных данных с последующим использованием в мошеннических целях. Хищение банковской информации, оформление кредитов на имя пользователя, взлом аккаунтов и использование данных в целях обмана — все это формирует ощущение небезопасности цифровой среды.

Не менее значимым является риск утраты конфиденциальности, который охватывает широкий спектр угроз: от несанкционированного доступа к личной информации до ее использования для манипуляций, психологического давления, навязчивого таргетинга, а также дискриминации. Такие риски затрагивают фундаментальные права личности и усиливают чувство уязвимости [10].

В условиях мегаполисов все более значимой становится риск несанкционированной слежки, особенно с учетом развития технологий распознавания

лиц и сбора биометрических данных. Население испытывает обеспокоенность по поводу непрозрачности систем, которые фиксируют их перемещения, поведение и даже эмоции в общественных пространствах, включая транспорт, учреждения образования, торговые центры и улицы. Отсутствие контроля над тем, как используются эти данные, воспринимается как вторжение в личное пространство и нарушение базовых свобод [11].

Значительную роль в восприятии рисков играет репутационная угроза. Утечка или намеренное распространение их персональных данных может негативно повлиять на их общественный имидж, карьерные перспективы и личные взаимоотношения. Подобные инциденты могут не только разрушить доверие к цифровым платформам, но и вызвать психологическое напряжение.

Кроме того, среди социальных рисков все чаще обсуждается потеря автономии личности. В условиях, когда цифровые платформы собирают и анализируют огромное количество данных о поведении пользователей, молодежь сталкивается с незаметным, но систематическим влиянием на свои выборы и решения. Персональные данные используются для формирования индивидуализированной ленты новостей, рекламных предложений, рекомендаций контента и даже политических сообщений. В результате у пользователей может складываться иллюзия свободы выбора, тогда как их информационная среда уже заранее сконструирована алгоритмами на основе их же поведения в сети. Это ограничивает возможности критического мышления, сужает кругозор и способствует формированию замкнутых «информационных пузырей», в которых человек видит только то, что подтверждает его взгляды и предпочтения. Таким образом, нарушается важный принцип цифрового взаимодействия — свобода осознанного выбора и личная информационная независимость [12].

Наконец, все эти риски в совокупности ведут к снижению доверия к цифровым платформам, государственным институтам и механизмам регулирования.

Обсуждение полученных результатов. Риски в предметной области продолжают существовать и трансформироваться, что требует системной защиты и дальнейших усилий как со стороны пользователей, так и со стороны цифровых платформ для минимизации угроз и повышения доверия к цифровым сервисам.

В силу многогранности проявления социальных рисков в системе защиты персональных данных, сложности их эмпирической фиксации и несовершенства нормативно-правовой требуется дальнейшее комплексное изучение данного явления, как на макроуровне, так и в повседневных практиках населения на микроуровне.

Заключение. В результате проведенного анализа уточнено понятие «социальные риски в системе защиты персональных данных» и предложены два подхода к типологизации этих видов риска. Первый подход — теоретический, структурирует проблему защиты персональных данных на макроуровне, в рамках общественной и институциональной структуры. В соответствии с этим ос-

нованием можно выделить риски по сферам жизнедеятельности: экономические, технико-технологические, нормативно-правовые и непосредственно социальные. Второй подход конкретизирует социальные риски, проявляющиеся на микроуровне, в повседневных цифровых практиках населения. В этом случае риски приобретают форму конкретных угроз, воспринимаемых людьми как значимые и непосредственные. К числу таких рисков отнесены: финансовые угрозы, утрата конфиденциальности, массовая слежка, репутационные потери, снижение доверия к цифровым платформам и утрата автономии личности. Типологизация социальных рисков в системе защиты персональных данных требует дальнейшей научной разработки, поскольку исследования в данной предметной области позволяют использовать более эффективные способы предотвращения различного рода угроз в условиях технологического развития современного общества.

Список источников

- [1] *Цифровая самооборона*. URL: <https://wciom.ru/analytical-reviews/analiticheskii-obzor/cifrovaja-samooborona> (дата обращения 14.05.2025).
- [2] *О персональных данных*. Федеральный закон от 27 июля 2006 г. № 152-ФЗ (в ред. от 23 июля 2013 г. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения 14.05.2025).
- [3] *Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных*. Постановление Правительства РФ от 1 нояб. 2012 г. № 1119. URL: <http://government.ru/docs/all/84743/> (дата обращения 14.05.2025).
- [4] Гидденс Э. Последствия современности. *Мониторинг общественного мнения: экономические и социальные перемены*, 2010, № 6 (100), с. 169–181.
- [5] Beck U. Risk Society and the Provident State. *Risk, Environment and Modernity*. London, Sage Publications, 1998, 198 p.
- [6] Луман Н. Понятие риска. Thesis, 1994, № 5, с. 135–160.
- [7] Яницкий О.Н. Модернизация в России в свете концепции «общества риска». *Куда идет Россия? Общее и особенное в современном развитии. IV Междунар. симпозиума: матер.* Москва, Московская высшая школа социальных и экономических наук, 1997, с. 37–48.
- [8] Чупров В.И., Зубок Ю.А., Уильямс К. *Молодежь в обществе риска*. Москва, Наука, 2003, 161 с.
- [9] Сазонова А.Л., Реброва С.А. Безопасность персональных данных как новый социальный феномен. *Позиция. Философские проблемы науки и техники*, 2024, № 22, с. 86–93.
- [10] Гаврилова Ю.В., Субочева О.Н., Красулина К.Р. Социальная безопасность в киберпространстве: специфика и технологии нарушения. *Социально-гуманитарные знания*, 2023, № 12, с. 195–199.
- [11] Самойлов С.И., Сазонова А.Л. Социальные риски распространения мифов о применении технологий биометрии. *XI Энгельмейеровские чтения. Общество – человек – культура: тренды цифровизации. Всерос. науч. конф. с междунар. участием: сб. ст.* Москва, Изд-во МГТУ им. Н.Э. Баумана, 2025, с. 123–125.
- [12] Авдеева А.П., Сафонова Ю.А. Геймификация: характеристики, тренды, риски. *Вестник университета*, 2024, № 8, с. 175–184. <https://doi.org/10.26425/1816-4277-2024-8-175-184>