УДК 316.3 URL: https://ptsj.bmstu.ru/catalog/hum/socio/1071.html

СОЦИАЛЬНЫЕ РИСКИ РАЗВИТИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ОБЩЕСТВЕ ЗНАНИЙ

М.А. Сорокин sorokinma@student.bmstu.ru

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

В статье рассмотрены социальные риски развития информационных технологий в условиях глобализации и перехода к обществу знаний, в котором данные технологии служат ключевым фактором развития. Показано, что стремительный процесс цифровизации и глубокое проникновение информационно-коммуникативных технологий во все сферы жизни современного общества сопровождается значительными социальными вызовами и рисками, которые требуют пристального внимания со стороны исследователей, политиков и общественности. Проанализированы риски цифрового неравенства, перспективы и опасности потери приватности, угрозы информационной и мягкой безопасностей с учетом глобальных тенденций, нерешенности этических проблем и недостатка правового регулирования.

Ключевые слова: информационные технологии, цифровизация, общество знаний, социальные риски, цифровое неравенство, информационная безопасность, мягкая безопасность, этические и правовые риски

Введение. В современном мире, где технологический прогресс играет ключевую роль в трансформации экономических, социальных и культурных процессов, современное общество все чаще характеризуют как «общество знаний» (knowledge society). Термин «общество знаний» был зафиксирован ЮНЕСКО во всемирном докладе 2005 г. [1], по сути, ознаменовав очередную глобальную трансформацию. Согласно исследованиям организации, переход к обществу знаний определяется интенсивным развитием информационно-коммуникационных технологий (ИКТ), которые и будут обеспечивать беспрепятственную передачу нужного объема информации. В результате таких преобразований условия существования социума становятся все более зависимыми от информационных и цифровых технологий.

В научном публичном пространстве также уже сформировалась новая экономическая парадигма, когда основным ресурсом развития современного общества признаются информация, знания и инновации, а не материальные активы. Технологический прогресс именно в области информационных технологий (ИТ), искусственного интеллекта и биотехнологий определяет конкурентоспособность стран, влияя на экономический рост, структуру занято-

 ISSN 2541-8009

сти и распределение ресурсов. Вместе с тем, как отмечают современные ученые, стремительные технологические изменения создают не только новые возможности для развития общества, но и продуцируют социальные риски, такие как цифровое неравенство, потеря приватности и усиление социальной поляризации [2].

Цифровое неравенство. Одной из наиболее актуальных для современного общества угроз, связанных с интенсивным развитием ИТ, является цифровое неравенство (digital divide). Оно проявляется в отставании отдельных групп населения, регионов и целых стран по уровню цифровой грамотности, доступности компьютерной техники, Интернета, онлайн-услуг и достоверной информации. Эксперты подчеркивают, что, несмотря на огромный потенциал цифровых технологий для социального и экономического развития, лишь небольшая часть населения мира может полноценно использовать эти возможности. Проблема цифрового неравенства выходит за рамки индивидуальных трудностей и затрагивает целые страны и регионы. Уже сегодня исследователи прогнозируют, что в ближайшем будущем вместо термина «бедная страна» будет использоваться понятие «страна с дефицитом знаний». Это связано с тем, что конкурентоспособность государств все больше зависит от уровня образования и квалификации их граждан. Страны, которые не смогут инвестировать в развитие науки, технологий и образования, рискуют оказаться на периферии глобальной экономики [3].

Согласно исследованию Организации экономического сотрудничества и развития (ОЭСР) [4], цифровой разрыв усугубляет социальное и экономическое неравенство, ограничивая возможности для получения качественного образования, трудоустройства и доступа к государственным услугам. Например, в докладе Международного союза электросвязи (International Telecommunication Union — ITU) за 2022 год подчеркивается, что около 2,7 миллиарда человек по всему миру до сих пор не имеют доступа к Интернету, что создает серьезные барьеры для их интеграции в цифровую экономику. В условиях глобализации цифровой разрыв становится одной из ключевых проблем международной повестки дня. Ведущие организации, такие как ООН, Всемирный банк и Всемирная торговая организация, активно трудятся над сокращением этого разрыва, разрабатывая программы по расширению доступа к цифровым технологиям и повышению цифровой грамотности. Например, инициатива ООН «Цифровая кооперация» [5] направлена на обеспечение равных возможностей для всех стран в использовании цифровых технологий.

В целом цифровое неравенство — это не только технологическая, но и социально-экономическая проблема, которая требует комплексного подхода и международного сотрудничества. Без решения этой проблемы глобаль-

ное неравенство будет только усиливаться, что может привести к дальнейшей поляризации мира.

Российские исследователи, рассматривая специфику и тенденции становления информационного общества, фиксируют различные оценки проявления цифрового разрыва и его влияния на экономическое развитие [6–8]. Например, Л.И. Власюк в своей научной работе [8] даже назвала развитие цифровой экономики в Российской Федерации «…скорее угрозой, чем возможностью, поскольку цифровое неравенство выступает дополнительным фактором, усиливающим социально-экономическое неравенство и без того значительную дифференциацию регионов РФ по уровню развития». В частности, необходимо выделять уровни цифрового разрыва в связи со спецификой и масштабами доступа и использования ИКТ. В то же время эксперты выделяют уровни цифрового разрыва в связи со спецификой и масштабами доступа и использования ИКТ.

Цифровое неравенство между теми, кто имеет доступ к Интернету, и теми, у кого возможности использования интернет-технологий ограничены, получил название «цифровой разрыв первого уровня». В России, по мнению исследователей, данный уровень показывают устойчивую тенденцию к сокращению цифрового разрыва [9].

Второй уровень цифрового разрыва связан с возможностями, которые предоставляет выход в сеть, и тем, каким образом эти возможности используются. Важно не только, кто пользуется Интернетом, но и уровни владения пользователей специальными онлайн-навыками, способность эффективно находить информацию в Интернете, при этом уровень развития ИКТ сегодня является одним из наиболее важных показателей экономического и социального благополучия государства [9]. Международным союзом электросвязи (ITU) был введен индекс развития ИКТ (ICT Development Index) — комбинированный показатель, характеризующий достижения стран мира с точки зрения развития ИКТ. Эти показатели касаются доступа к ИКТ, использования ИКТ, а также навыков, т. е. практического знания этих технологий населением стран, охваченных исследованием [10].

Потеря приватности. Другой серьезной проблемой современного мира, напрямую связанной с развитием ИКТ, исследователи называют потерю приватности. Развитие ИТ и цифровой среды требуют от человека отказаться от приватности и принять так называемую постприватность. Иначе говоря, каждый из нас вопреки своему желанию вынужден обменивать чувствительную персональную информацию на доступ к интересующим их сервисам, а если добавить к этому и добровольное распространение личных данных в социальных сетях, то получается, что современный человек лишен приватного

 ISSN 2541-8009

пространства и возможности скрыть свою личную жизнь от глаз других людей. И как бы каждый из нас не относился к распространению собственных данных, с увеличением его «цифровых следов» пропорционально увеличивается и риск оказаться жертвой кибер-преступлений: шантажа, мошенничества, травли [11].

Несмотря на то что людей, готовых контролировать собственную приватную информацию в информационном пространстве, немного, осознанное противодействие граждан размыванию границ публичного и приватного все-таки имеет обратный социальный эффект. В современном публичном пространстве даже появилось понятие «эффект Стрэйзанд» — явления, при котором попытка скрыть или удалить определенную информацию из публичного доступа приводит к обратному результату: информация привлекает еще больше внимания и распространяется гораздо шире, чем изначально. Этот эффект назван в честь американской актрисы Барбары Стрэйзанд, которая в 2003 г. попыталась удалить фотографии своего дома, размещенные в Интернете. В результате ее иск привлек к этим фотографиям огромное внимание, и они стали гораздо более известными, чем были до этого [12].

Данный феномен только подчеркивает, насколько сложно сохранить конфиденциальность в цифровую эпоху. Даже если человек пытается защитить свои личные данные, он может непреднамеренно привлечь к ним внимание, что делает приватность еще более уязвимой. Эффект Стрэйзанд служит напоминанием о том, что в современном мире важно тщательно обдумывать последствия своих действий в Интернете, особенно когда речь идет о защите личной информации.

Потеря приватности в цифровую эпоху вскрывает еще одну из ключевых социальных уязвимостей — возможность манипуляции человеческим сознанием через анализ и использование персональных данных. Современные технологии позволяют создавать так называемого цифрового двойника — виртуальную модель личности, формируемую на основе цифровых следов, которые пользователь оставляет в Интернете. Эти данные, включая историю поисковых запросов, лайки, репосты, комментарии в социальных сетях, время, проведенное на определенных страницах, и даже просмотр мемов, становятся основой для анализа, прогнозирования и управления поведением человека. Исследования показывают, что даже незначительные на первый взгляд действия в цифровой среде могут быть использованы для создания подробного психологического портрета. Например, работа М. Косинки и других продемонстрировала, что на основе лайков в Facebook[1] можно с высокой

[1] Продукт компании Meta, признанной экстремистской организацией и запрещенной на территории РФ.

точностью предсказать личностные черты, политические взгляды, сексуальную ориентацию и даже склонность к определенным заболеваниям [13]. Это свидетельствует о том, что цифровые следы становятся мощным инструментом для манипуляции, поскольку позволяют воздействовать на пользователя с учетом его индивидуальных особенностей.

В социальных сетях, таких как Facebook, Instagram[2] и TikTok, активно используются алгоритмы, которые анализируют поведение пользователей для персонализации контента и рекламы. Однако эта персонализация может быть использована не только в коммерческих целях, но и для политического влияния. Ярким примером служит скандал с компанией Cambridge Analytica, когда данные миллионов пользователей Facebook были использованы для создания психологических профилей и таргетированной политической рекламы с целью влияния на результаты выборов [14]. Этот случай наглядно демонстрирует, как потеря приватности может привести к манипуляции общественным мнением и принятием решений. Кроме того, исследования Шошаны Зубофф в ее работе "The Age of Surveillance Capitalism" подчеркивают, что сбор и анализ данных о пользователях превратились в основу новой экономической модели, где личная информация становится товаром, а поведение человека — объектом прогнозирования и контроля [15]. Это создает угрозу не только для приватности, но и для автономии личности, поскольку решения, принимаемые на основе анализа данных, могут ограничивать свободу выбора и формировать предсказуемые модели поведения.

Согласно исследованиям в области «мягкой безопасности» [16], роль бизнеса в воздействии на людей недооценивать нельзя. Наглядным примером влияния по средствам социальных сетей являются популярный феномен — интернет-мем, который, как и термин мем, на самом деле несет в себе куда больше смысла, чем может показаться [17]. Действуя на уровне эмоций, будучи ориентированными на клиповое мышление, мемам сегодня удается эффективно действовать на потребителя, упрощая его мировоззрение, нарушая восприятие получаемой информации и, как следствие, внедряя необходимый посыл в подсознание человека. Проще говоря, интернет-мемы полноправно можно назвать «информационной бомбой».

Таким образом, потеря приватности в цифровом мире не только угрожает конфиденциальности личной информации, но и создает предпосылки для манипуляции сознанием. Цифровые следы, оставляемые пользователями, становятся инструментом для создания «цифровых двойников», которые мо-

[2] Продукт компании Meta, признанной экстремистской организацией и запрещенной на территории РФ.

 ISSN 2541-8009

гут быть использованы для прогнозирования и управления поведением. Это подчеркивает необходимость разработки более строгих мер для защиты данных и повышения осведомленности пользователей о рисках, связанных с их цифровой активностью.

Манипуляция сознанием. Еще одним социальным риском в современном информационном пространстве выступает дезинформация, которая может играть ключевую роль в формировании общественного мнения. Непреднамеренное искажение информации, вызванное, например, недостатками технологий, таких как интернет-переводчики, может привести к потере сложных грамматических конструкций, эмоционального окраса и лингвистических нюансов. Это, в свою очередь, может исказить истинный смысл передаваемой информации. Однако более серьезную угрозу представляет умышленная дезинформация, которая может включать в себя утаивание информации, направленное на манипуляцию общественным мнением. Примером такой дезинформации может служить политика китайской нейронной сети DeepSeek, которая избегает упоминаний о событиях на площади Тяньаньмэнь. Это является результатом внутренней политики Китая, но с учетом распространенности искусственного интеллекта, потенциальными потребителями искаженной информации становится значительное количество людей по всему миру.

Безусловно, в случае с ненаправленной дезинформацией отличить поддельные или недостающие сведения практически не составляет труда. Сложнее дело обстоит в том случае, когда информация замалчивается или искажается специально и, хотя целью этих действий может быть собственная выгода частной компании, ее достижение будет осуществляться в ущерб другим членам общества. За примерами далеко ходить не нужно: социальные сети часто не позволяют на своих площадках распространять статьи, публикации и посты, наносящие ущерб их коммерческим интересам, даже если законодательно они не имеют право этому препятствовать. Яркий пример тому — скандально известная зарубежная социальная сеть, запрещенная в Российской Федерации.

Наиболее опасной формой дезинформации является намеренная, целенаправленная дезинформация, которая имеет конкретное содержание и определенную целевую аудиторию. Манипуляция этого типа может представлять серьезную угрозу для развития общества и создавать риск дестабилизации обстановки в регионе или стране. Одним из наиболее известных проявлений такой практики является фальсификация истории, которая, как показывают исследования, имеет глубокие корни и не ограничивается только историческими событиями [18]. Целью вмешательства недружественных государств может быть подрыв обучаемости граждан и деформация гносеологической стратегии

исследовательского поиска. Для достижения этой цели недоброжелатели стремятся использовать различные уязвимости, такие как определение объекта воздействия, сбор данных о нем, выбор инструмента манипуляции и сама манипуляция. Отсутствие строгих правовых рамок, регулирующих эти проблемы, может способствовать реализации таких стратегий.

Современное развитие ИТ происходит настолько стремительно, что процесс формирования соответствующих этических норм и правовых рамок не успевает адаптироваться к новым вызовам. Это приводит к возникновению значительных пробелов в регулировании, что, в свою очередь, создает риски для реализации стратегических задач, таких как те, что обозначены в Стратегии развития информационного общества России [19]. При этом одной из ключевых проблем является отсутствие четких правовых границ, регулирующих внедрение и использование технологических инноваций. Эта правовая неопределенность не только затрудняет достижение целей, поставленных в стратегических документах, но и ставит под угрозу национальную безопасность.

Современная сложность разработки необходимой нормативно-правовой базы, как отмечают исследователи, усложняется рядом факторов. Во-первых, отсутствуют универсальные стандарты, регулирующие объем персональных данных, которые компании могут собирать и хранить о своих пользователях. Во-вторых, цифровое неравенство, как отмечалось выше, остается серьезной проблемой. В-третьих, невозможность полностью отфильтровать информационное пространство от вредоносного или искаженного контента. И, наконец, в виртуальной среде сложно определить границы прав и свобод отдельных лиц, что создает дополнительные правовые коллизии.

Этические нормы. Для решения этих проблем необходимо строгое определение этических норм, регулирующих применение технологий. Современные правила использования ИКТ должны не только отвечать текущим потребностям цифрового общества, но и учитывать исторические, культурные и традиционные особенности. Такой подход позволит создать устойчивую основу для будущих правовых рамок, что, в свою очередь, будет способствовать устойчивому развитию общества знаний в России [20].

Важнейшим вызовом, связанным с развитием современных информационных и цифровых технологий, становится глобальный характер проблематики социальных рисков и обусловливается транснациональной природой технологий, которые не ограничиваются национальными границами. Рассматриваемые угрозы в той или иной степени актуальны для всех государств, что подчеркивает необходимость международного сотрудничества для разработки унифицированных подходов к регулированию и минимизации данных рисков.

 ISSN 2541-8009

Однако на практике наблюдается использование технологических уязвимостей в интересах отдельных государств. В частности, страны, входящие в так называемый коллективный Запад, активно эксплуатируют слабости других государств для достижения своих внешнеполитических целей. Глобальное цифровое неравенство способствует тому, что государства, лидирующие в области цифрового развития, превращают менее развитые страны в своего рода «технологические колонии». Ярким примером может служить ситуация с распространением мобильных технологий и платформ в странах Африки. Компании из технологически развитых стран, такие как Meta[3] (ранее Facebook) и Google, активно внедряют свои услуги в регионы с низким уровнем цифровой инфраструктуры. Например, проект Free Basics от Meta предоставляет ограниченный доступ к Интернету через мобильные устройства, но при этом ограничивает пользователей только определенными сайтами и сервисами, контролируемыми компанией. Это создает зависимость от платформ, принадлежащих иностранным корпорациям, и ограничивает развитие местных цифровых экосистем [21].

Заключение. Таким образом, современное развитие ИКТ диктует необходимость прогнозирования и управления социальными рисками, продуцируемыми развивающимися новшествами ИКТ. Диагностика и управление социальными рисками в данной области позволяют синхронизировать цифровое развитие регионов, обеспечивать физическую, кибернетическую и информационную безопасность граждан, непрерывно выявлять и своевременно предотвращать новые угрозы. Это особенно важно для устойчивого развития общества знаний, где технологии должны служить человеку, а не создавать новые угрозы.

Результатом исследования можно считать проведенный комплексный анализ социальных рисков, связанных с развитием ИТ. В результате анализа была подчеркнута необходимость государственного контроля социальных рисков и аналитически определено место традиций и истории в формировании общества знаний. Статья может стать важным вкладом в дискуссию о том, как использовать потенциал ИТ для блага общества, минимизируя при этом их негативные последствия.

Литература

[1] *К обществам знаний: Всемирный доклад ЮНЕСКО*. URL: https://unesdoc.unesco.org/ark:/48223/pf0000141843 (дата обращения 11.03.2025).

[3] Признана экстремистской организацией и запрещена на территории РФ.

[2] Кастельс М. *Информационная эпоха: экономика, общество и культура*. Москва, ГУ ВШЭ, 2000.

[3] Лысак И.В. Новые образовательные технологии как средство преодоления цифрового разрыва. *Современные наукоемкие технологии*, 2017, № 7, с. 129–135. URL: https://top-technologies.ru/ru/article/view?id=36743 (дата обращения 17.03.2025)

[4] *OECD. Understanding the Digital Divide*. OECD Digital Economy Papers, no. 49. OECD Publishing, Paris. https://doi.org/10.1787/236405667766

[5] *The Age of Digital Interdependence.* Report of the Secretary-General on Digital Cooperation. New York, United Nations, 2019, 56 p. URL: https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf (accessed 17.03.2025).

[6] Усков В.С. Развитие цифровой экономики России: факторы и региональные различия. *Проблемы развития территории*, 2024, т. 28, № 1, с. 28–41.

[7] Долгих Е.А., Паршинцева Л.С. Оценка инновационного развития регионов России. *Финансы и управление*, 2024, № 3, с. 37–56.

[8] Власюк Л.И. Цифровое неравенство российских регионов: стратегические возможности и угрозы. *Экономика промышленности*, 2023, vol. 16 (1), pp. 59–68. https://doi.org/10.17073/2072-1633-2023-1-59-68

[9] Добринская Д.Е., Мартыненко Т.С. Перспективы российского информационного общества: уровни цифрового разрыва. *Вестник РУДН. Серия: Социология*, 2019, № 1, с. 108–120.

[10] *International Telecommunication Union*. Measuring the Information Society Report 2007. ICT Opportunity Index and World Telecommunication/ICT Indicators. Geneva, ITU.

[11] Чеснокова Л.В. Трансформация информационной приватности в современном цифровом обществе. *Общество: философия, история, культура*, 2024, № 5. https://doi.org/10.24158/fik.2024.5.17

[12] Ракова В.А., Дождикова Р.Н. Манипуляции с информацией: искаженное восприятие и распространение негативной информации. *Философия мира и созидания. Народное единство и историческая память. Матер. Междунар. круглых столов.* Минск, БНТУ, 2023, с. 118–121. URL: https://rep.bntu.by/handle/data/131125 (дата обращения 19.03.2025).

[13] Kosinski M., Stillwell D., Graepel T. Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences*, 2013, vol. 110 (15), pp. 5802–5805. https://doi.org/10.1073/pnas.1218772110

[14] Cadwalladr C. *The Cambridge Analytica files. The Guardian*. URL: https://www.theguardian.com/news/series/cambridge-analytica-files (accessed 19.03.2025).

 ISSN 2541-8009

[15] Hikikomori F., Zuboff S. *The Age of Surveillance Capitalism: the Fight for a Human Future at the New Frontier of Power*. New York, Public Affairs, 2019, 704 p.

[16] Ворочков А.П. «Мягкая сила» современной России: институциональный аспект. *Теории и проблемы политических исследований*, 2016, т. 5, № 5А, с. 258–275.

[17] Бурнашева М.П., Маленко С.А., Некита А.Г. Интернет-мем как инструмент манипуляции в современном культурном и информационном пространстве. Состав редакционной коллегии и организационного комитета. *Лучшая исследовательская работа. IV Междунар. науч.-исслед. конкурс: сб. тр.* Петрозаводск, Новая Наука (ИП Ивановская И.И.), 2024, с. 73–82.

[18] Балахонский В.В., Стрельченко В.И., Балахонская Л.В. Гносеологический инструментарий современных практик фальсификации истории. *Контекст и рефлексия: философия о мире и человеке*, 2024, т. 13, с. 31–37.

[19] *Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы.* URL: http://www.kremlin.ru/acts/bank/41919 (дата обращения 11.03.2025).

[20] Манжуева О.М. Информационная этика Норберта Винера. *Вестник БГУ*, 2013, № 6, с. 53–57.

[21] Toussaint N. Access granted: Facebook's free basics in Africa. *Media, Culture & Society*, 2020, vol. 42, pp. 329–348. https://doi.org/10.1177/0163443719890530

Поступила в редакцию 27.04.2025

Сорокин Михаил Артемович — студент кафедры «Системы обработки информации и управления», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Научный руководитель — Оплетина Надежда Витальевна, кандидат социологических наук, доцент кафедры «Социология и культура», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация. E-mail: opletinanv@mail.ru, SPIN-код: 4093-9386.

Ссылку на эту статью просим оформлять следующим образом:
Сорокин М.А. Социальные риски развития информационных технологий в обществе знаний. *Политехнический молодежный журнал*, 2025, № 05 (100). URL: https://ptsj.bmstu.ru/catalog/hum/socio/1071.html

SOCIAL RISKS OF INFORMATION TECHNOLOGY DEVELOPMENT IN THE KNOWLEDGE SOCIETY

M.A. Sorokin sorokinma@student.bmstu.ru

Bauman Moscow State Technical University, Moscow, Russian Federation

The article examines the social risks of information technology development in the context of globalization and the transition to a knowledge society in which these technologies are a key factor in development. It is shown that the rapid process of digitalization and the deep penetration of information and communication technologies into all spheres of modern society are accompanied by significant social challenges and risks that require close attention from researchers, politicians and the public. The risks of digital inequality, prospects and dangers of loss of privacy, threats to information and soft security are analyzed, taking into account global trends, unresolved ethical issues and lack of legal regulation.

Keywords: information technologies, digitalization, knowledge society, social risks, digital inequality, information security, soft security, ethical and legal risks

Received 27.04.2025

Sorokin M.A. — Student of Department of Information Processing and Management Systems, Bauman Moscow State Technical University, Moscow, Russian Federation.

Scientific advisor — Opletina N.V., Ph. D. (Soc.), Associate Professor of Department of Sociology and Culture, Bauman Moscow State Technical University, Moscow, Russian Federation. E-mail: opletinanv@mail.ru, SPIN-code: 4093-9386.

Please cite this article in English as:
Sorokin M.A. Social risks of information technology development in the knowledge society. *Politekhnicheskiy molodezhnyy zhurnal*, 2025, no. 05 (100). (In Russ.). URL: https://ptsj.bmstu.ru/catalog/hum/socio/1071.html

 ISSN 2541-8009