СОЦИОЛОГИЯ УПРАВЛЕНИЯ И СОЦИАЛЬНЫЕ ТЕХНОЛОГИИ
SOCIOLOGY OF MANAGEMENT AND SOCIAL TECHNOLOGIES

УДК 316.33

DOI: 10.18413/2408-9338-2026-12-4-1-0

Исследовательская статья

Гайдукова Г. Н.

Социологическая оценка специфики формирования социально-технологической безопасности крупных городов Северной Евразии

Северо-Западный институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте РФ,
Средний проспект Васильевского острова, дом 57/43,
Санкт-Петербург, 199178, Россия
gaydukova-gn@ranepa.ru

Аннотация. *Актуальность* статьи определяется тем, что современный крупный город все в меньшей степени может рассматриваться как относительно стабильная административно-территориальная единица и все в большей степени выступает как сложная социально-технологическая система, функционирующая в режиме постоянной неопределенности. Особенно остро данная проблематика проявляется в крупных российских городах Северной Евразии, где суровые климатические условия, зависимость от централизованного теплоснабжения, протяженность инфраструктур, цифровизация управления и неоднородность городского населения усиливают вероятность каскадных сбоев. *Научная проблема* исследования состоит в недостаточной разработанности интегральной концепции социально-технологической безопасности города. В существующих подходах социальные, технические, информационные и управленческие риски нередко анализируются раздельно, тогда как в реальной городской среде они образуют единую систему взаимных усилений. *Методологическую основу* статьи составляет междисциплинарная рамка социологии нестабильности, объединяющая идеи социологии риска, теории рефлексивной модерности, системного анализа, урбанистики и исследований безопасности. В работе используются концептуальный анализ категорий «социальная нестабильность», «социальная турбулентность», «социальный хаос», «социальные риски», «опасность» и «угроза», а также элементы системного и институционального подходов. *Научные результаты* исследования заключаются, во-первых, в уточнении различия между социально-технологической опасностью и социально-технологической угрозой. Опасность понимается как потенциальная возможность недостижения субъектом социального действия планируемых результатов вследствие непрофессионального применения социальных технологий или неспособности адекватно интерпретировать действия других акторов. Угроза, в отличие от опасности, предполагает адресное деструктивное воздействие, осуществляемое конкретным актором с использованием организационных, информационных, цифровых или

манипулятивных технологий. Во-вторых, показано, что ключевая уязвимость крупного города связана с разрывом между высокой взаимозависимостью инфраструктур и фрагментарностью институционального управления. В-третьих, выявлено, что экспертное сообщество оценивает уровень представлений населения и институтов о социально-технологических опасностях как недостаточный, что усиливает необходимость системного просвещения, подготовки специалистов и формирования культуры безопасности. В *выводах* обосновывается необходимость создания городской системы социально-технологической безопасности как многоуровневого институционального контура, включающего нормативно-правовую базу, техническую защиту, цифровой мониторинг, системы диспетчеризации, риск-коммуникацию, образовательные программы, контур противодействия дезинформации, независимую экспертизу и механизмы участия населения. Такая система должна быть ориентирована не только на ликвидацию последствий кризисов, но и на раннее выявление предкризисных признаков, поддержание достоверной обратной связи и повышение способности городского сообщества к рациональному совместному действию в условиях нестабильности.

Ключевые слова: крупный город; социальные технологии; социально-технологическая безопасность; социология нестабильности; социальные риски; городская устойчивость

Благодарность. Исследование выполнено за счет гранта Российского научного фонда № 25-28-02281, https://rscf.ru/project/25-28-02281/.

Информация для цитирования: Гайдукова Г. Н. Социологическая оценка специфики формирования социально-технологической безопасности крупных городов Северной Евразии // Научный результат. Социология и управление. 2026. Т. 12, № 4. С. 146-170. DOI: 10.18413/2408-9338-2026-12-4-1-0.

Research article

Galina N. Gaidukova

Sociological assessment of the specifics of the formation of socio-technological security of large cities in Northern Eurasia

North-West Institute of Management – Branch of RANEPA,
57/43 Sredny Ave., Vasilievsky Island, St. Petersburg, 199178, Russia
gaydukova-gn@ranepa.ru

Abstract. The *relevance* of this article is determined by the fact that modern large cities can increasingly be viewed as relatively stable administrative-territorial units and increasingly act as complex socio-technological systems operating in a state of constant uncertainty. This problem is particularly acute in large Russian cities in Northern Eurasia, where harsh climatic conditions, dependence on centralized heating, extensive infrastructure, digitalization of governance, and heterogeneity of the urban population increase the likelihood of cascading failures. The *scientific problem* of the study lies in the insufficient development of an integrated concept of urban socio-technological security. Existing approaches often analyze social, technical, informational, and managerial risks separately, whereas in the real urban environment they form a unified system of mutual reinforcement. The *methodological basis* of the article is the interdisciplinary framework of the sociology of instability, combining ideas from the

sociology of risk, the theory of reflexive modernity, systems analysis, urban studies, and security studies. This paper utilizes a conceptual analysis of the categories of “social instability”, “social turbulence”, “social chaos”, “social risks”, “danger”, and “threat”, as well as elements of systemic and institutional approaches. The *research's scientific results*, firstly, clarify the distinction between socio-technological danger and socio-technological threat. Danger is understood as the potential for a social actor to fail to achieve its intended results due to the unprofessional application of social technologies or the inability to adequately interpret the actions of other actors. Threat, in contrast, implies a targeted destructive impact carried out by a specific actor using organizational, information, digital, or manipulative technologies. Secondly, it is shown that the key vulnerability of a large city is associated with the gap between the high interdependence of infrastructures and the fragmentation of institutional governance. Thirdly, it was revealed that the expert community considers the public's and institutions' understanding of socio-technological hazards to be inadequate. This emphasises the need for systemic education, specialist training and the development of a safety culture. The *findings substantiate* the need to create an urban socio-technological security system as a multi-layered institutional framework, including a regulatory framework, technical protection, digital monitoring, dispatching systems, risk communication, educational programs, a framework for countering disinformation, independent expertise, and public participation mechanisms. Such a system should be focused not only on eliminating the consequences of crises but also on the early detection of pre-crisis signs, maintaining reliable feedback, and enhancing the urban community's capacity for rational, collaborative action in unstable conditions.

Keywords: large city; social technologies; socio-technological security; sociology of instability; social risks; urban resilience

Acknowledgements. The research was supported by Russian Science Foundation grant 25-28-02281, https://rscf.ru/project/25-28-02281/.

Information for citation: Gaidukova, G. N. (2026), “Sociological assessment of the specifics of the formation of socio-technological security of large cities in Northern Eurasia”, *Research Result. Sociology and Management*, 12 (4), 146-170. DOI: 10.18413/2408-9338-2026-12-4-1-0.

Введение (Introduction). Современный крупный город все чаще оказывается не только центром экономической активности, инноваций и культурной концентрации, но и пространством повышенной нестабильности. В нем одновременно сосуществуют сложные инженерные инфраструктуры, цифровые платформы управления, многообразные социальные группы, информационные потоки и институты публичной власти. Такая концентрация ресурсов и связей делает город эффективным, но одновременно и уязвимым: локальный технологический сбой, информационная провокация, кризис доверия или социально-экономическое напряжение способны быстро приобрести каскадный характер и перерасти в системную угрозу.

Особую значимость эта проблема приобретает для крупных российских городов Северной Евразии, что обусловлено сочетанием суровых природно-климатических условий, протяженных инфраструктурных сетей, высокой зависимости населения от бесперебойной работы энергетики, транспорта, связи и коммунальных систем, а также сложной историей институциональных трансформаций. Здесь социальная безопасность не может рассматриваться отдельно от технологической – устойчивость городской жизни зависит не только от качества инженерных систем, но и от уровня доверия, управленческой

координации, цифровой грамотности населения, способности институтов предупреждать и нейтрализовать угрозы.

Научная проблема состоит в том, что исследования городской безопасности нередко разделяют социальные, технологические и информационные риски, рассматривая их как относительно автономные сферы. Между тем в реальной городской среде они образуют единую систему взаимных усилений. Поэтому анализ безопасности крупных городов требует интегральной рамки, соединяющей социологию нестабильности с концепцией социально-технологической безопасности.

В социологической перспективе нестабильность следует понимать не только как временное отклонение от нормы, но и как устойчивый режим существования современных обществ. «Особенности развития современного социально-гуманитарного знания связаны с актуализацией проблемы безопасности, которая сегодня является всесторонней, приобретает глобальный и насущный характер, так как быстрыми темпами растут факторы риска и источники угроз, которые охватывают все сферы жизнедеятельности общества и социального субъекта – экономическую, политическую, социальную и духовную» (Вильданов, Хабибуллин, 2025: 15). Городские системы функционируют в условиях постоянной неопределенности, где опасности и угрозы имеют гибридный характер. Социальная опасность может быть связана с бедностью, неравенством, конфликтностью, демографическими изменениями или дефицитом доверия. Однако в условиях цифровизации эти опасности все чаще усиливаются технологическими и информационными факторами: сбоями инфраструктуры, кибератаками, дезинформацией, алгоритмическими искажениями, зависимостью от платформенных сервисов.

Кроме того, одной из особенностей развития общества в XXI веке становится увеличение возможностей применения социальных технологий для решения общественных проблем или, напротив, для их искусственного обострения. Сложившаяся ситуация является одним из следствий цифровизации/дигитализации социума, в ходе которой традиционные социальные технологии конвергируют с цифровыми. Образующиеся при этом гибриды в случае их применения нередко приводят к негативным эффектам, порождая опасности и угрозы для общества и человека, что особенно заметно в высоко урбанизированной, по определению технологичной, среде. К устранению и/или минимизации этих угроз социальные институты и граждане пока готовы мало. Возникает противоречие между неизбежностью дальнейшей технологизации социальных отношений, заключающей в себе, наряду с конструктивными результатами элементы социальных деструкций и не разработанностью концепции социально-технологической безопасности городского пространства.

Методология и методы (Methodology and Methods). Исходной рамкой анализа социально-технологической безопасности крупного города выступает социология нестабильности. Она рассматривается не как завершенная научная школа, а как междисциплинарный подход, сформированный на пересечении социологии риска, теорий поздней модерности и социальных изменений, системного анализа, урбанистики и исследований безопасности. Его центральный тезис состоит в том, что неопределенность, ускорение изменений и возможность каскадных сбоев являются не отклонениями от устойчивого порядка, а нормальными условиями функционирования современных обществ.

Основы данного подхода заложены в работах У. Бека, Э. Гидденса, Н. Лумана, М. Дуглас, А. Вильдавски, З. Баумана, Х. Розы и Ч. Перроу. У. Бек показал, что модернизация производит не только общественные блага, но и экологические, техногенные, информационные и иные риски, которые являются внутренним следствием технологического развития (Beck, 1992). Э. Гидденс связывал устойчивость современного общества с доверием к «абстрактным системам» – транспорту, энергетике, медицине,

экспертному знанию, цифровым сетям и государственным институтам (Giddens, 1990, 1991). Чем сложнее эти системы, тем сильнее зависимость от них и тем меньше возможности рядового человека контролировать их функционирование.

Принципиальное значение имеет различение риска и опасности, предложенное Н. Луманом. Если возможный ущерб приписывается принятому решению, он определяется как риск; если воспринимается как внешнее воздействие – как опасность (Luhmann, 1993). Поэтому один и тот же инфраструктурный сбой может интерпретироваться органами управления как результат рискованного решения, а населением – как навязанная извне опасность. М. Дуглас и А. Вильдавски, в свою очередь, показали, что восприятие рисков зависит не только от вероятности ущерба, но и от культуры, ценностей, институтов и распределения власти (Douglas, Wildavsky, 1982).

З. Бауман описывал современность как состояние утраты долговременной устойчивости социальных форм, институтов и идентичностей (Bauman, 2000). В крупном городе это выражается в мобильности населения, фрагментации социальных связей и снижении способности институтов обеспечивать чувство надежности. Х. Роза связывает нестабильность с социальным ускорением: технологические, политические и коммуникативные изменения происходят быстрее, чем институты успевают адаптироваться (Rosa, 2013). Концепция «нормальных аварий» Ч. Перроу дополняет эту логику: в сложно организованных и тесно связанных системах сбои становятся трудно предсказуемым следствием самой их структуры. Таким образом, кризисы встроены в развитие крупных социально-технологических систем, а не выступают исключительно внешними нарушениями порядка.

Для описания разных уровней дезорганизации необходимо разграничивать социальную нестабильность, социальную турбулентность и социальный хаос. Под социальной нестабильностью понимается состояние общества или его подсистем, характеризующееся ослаблением институтов и нормативного порядка, ростом напряженности, конфликтности и неопределенности, вследствие чего снижается способность системы к саморегуляции и предсказуемому воспроизводству. В городе нестабильность проявляется как в открытых кризисах – протестах, авариях, панике и насилии, – так и в латентном накоплении недоверия, инфраструктурного износа, цифровой зависимости, неравенства и информационной уязвимости.

Социальная турбулентность обозначает более динамичное состояние – быстрые, нелинейные, разнонаправленные и плохо прогнозируемые изменения. Э. Тоффлер связывал его с ситуацией, в которой темпы технологических и институциональных преобразований превышают адаптивные возможности человека и общества (Тоффлер, 2003, 2004, 2025). М. Кастельс показал, что сетевые структуры и глобальные потоки информации, капитала и власти выводят социальные процессы за рамки линейного национального развития (Кастельс, 2000). П. Штомпка рассматривал общество как процесс становления, уделяя особое внимание травматическим изменениям и культурной дезориентации переходных эпох (Штомпка, 1996).

Социальную турбулентность, таким образом, можно определить как многомерное состояние, возникающее в условиях ускоренных и нелинейных изменений, при котором ослабляется устойчивость институтов, норм и механизмов координации, возрастает чувствительность к внешним и внутренним воздействиям, а развитие приобретает прерывистый и трудно прогнозируемый характер.

Социальный хаос представляет наиболее радикальную степень дезорганизации, при которой нарушаются базовые механизмы координации, нормативной регуляции и институционального управления. Однако хаос не обязательно означает полное разрушение

социальной ткани: он может рассматриваться как предельное неравновесие, из которого возникают новые формы порядка (Лиотар, 1998; Делёз, 2025a, 2025b).

Ключевой характеристикой хаотического состояния является нелинейность. В нелинейной системе масштаб последствий не пропорционален силе первоначального воздействия: локальный конфликт, слух, публикация или единичный инфраструктурный сбой могут вызвать массовую мобилизацию, панику или кризис доверия, тогда как значительные управленческие усилия не всегда приводят к ожидаемому результату. Эффект определяется не только непосредственной причиной, но и состоянием системы: накопленными противоречиями, плотностью социальных связей, скоростью распространения информации и наличием скрытых точек нестабильности.

Следовательно, социальная нестабильность означает ослабление устойчивости институтов и норм; турбулентность – ускоренную и нелинейную динамику изменений; социальный хаос – радикальную перегрузку либо разрушение механизмов упорядочивания. Это разграничение необходимо для эмпирического анализа городских кризисов, сетевых конфликтов, переходных процессов и трансформаций социального порядка.

Смежной категорией являются социальные риски – вероятные неблагоприятные события и процессы, нарушающие жизненные траектории людей, воспроизводство социальных групп и устойчивость институтов. В техническом подходе риск обычно определяется как сочетание вероятности события и масштаба ущерба. В социологии учитываются также распределение последствий, принятие решений и интерпретация угроз различными социальными группами. Вопрос заключается не только в том, насколько вероятен ущерб, но и в том, кто принимает рискованные решения, кто получает выгоды, и кто несет издержки.

Социальные риски имеют преимущественно структурный характер. Хотя их последствия переживаются индивидуально – как потеря работы, ухудшение здоровья или социальное исключение, – условия их возникновения могут определяться деиндустриализацией, прекаризацией занятости, институциональной нестабильностью и неравным доступом к ресурсам. Социологический анализ тем самым переносит внимание с индивидуальной биографии на социальные механизмы производства и распределения риска.

Концепции социальной уязвимости и резильентности дополняют этот подход анализом способности индивидов и сообществ противостоять неблагоприятным воздействиям (Chambers, 2009; Moser, 1997; Cutter, 2003). Социальный риск определяется не только внешним шоком, но и дефицитом адаптационных ресурсов: низким доходом, слабыми сетями поддержки, ограниченным доступом к медицине и образованию, территориальной изоляцией или институциональной дискриминацией. Социальные риски, следовательно, представляют общественно произведенные, структурно распределенные и культурно интерпретируемые вероятности ущерба.

В исследованиях безопасности необходимо также разграничивать опасность и угрозу. Опасность – потенциальная способность явления, среды или субъекта причинить вред. Она может существовать латентно: к городским опасностям относятся инфраструктурный износ, социальная изоляция молодежи, низкое доверие к институтам и недостаточная медиаграмотность. В логике Н. Лумана опасность воспринимается как внешний источник возможного ущерба, хотя для управленческих структур она может быть результатом накопленного институционального риска (Luhmann, 1993).

Угроза представляет актуализированную опасность, для которой можно определить источник, объект, механизм и вероятные последствия. Так, низкая медиаграмотность является опасностью, а массовое распространение фейка о заражении воды – социально-информационной угрозой; изношенность коммунальных сетей – опасностью, а вероятность отключения теплоснабжения в конкретном районе – инфраструктурной угрозой. Аналогично

социальное неравенство формирует опасность, тогда как мобилизация массового конфликта после резонансного события выступает конкретной социальной угрозой.

Наконец, в соответствии с теорией секьюритизации угроза становится объектом политики безопасности не только вследствие объективных характеристик, но и благодаря ее публичному обозначению политическими, медийными или экспертными акторами (Buzan, Waever, Wilde, 1998). Поэтому анализ социально-технологической безопасности города должен учитывать одновременно объективные параметры риска, структурную уязвимость системы и дискурсивные механизмы, посредством которых отдельные явления признаются угрозами и легитимируют чрезвычайные меры реагирования.

Тем не менее, многие аспекты формирования системы безопасности изучены недостаточно. К числу их относится социально-технологическая безопасность, представляющая собой систему мер, направленных на предотвращение опасностей и угроз, обусловленных либо 1) непрофессиональным использованием социальных технологий, либо 2) неспособностью субъектов защитить себя от деструктивного социально-технологического воздействия (антитехнологий), 3) либо неудачные попытки акторов использовать антитехнологии в своих целях. В массе своей многие городские жители предрасположены становится жертвами деструктивного воздействия (мошенничество, обман и т.д.), что превращает их в объект манипуляции с помощью антитехнологий, представляющих собой практики скрытого управления людьми, лишающие их атрибута субъектности. Антитехнологии ориентированы на интеграцию факторов опасностей и угроз в состав практик управления общественными процессами.

Целью работы выступает попытка эмпирически проанализировать специфику социально-технологической безопасности крупных российских городов Северной Евразии через призму социологии нестабильности. В центре внимания находится вопрос о необходимости системного решения проблемы обеспечения городской социально-технологической безопасности, что предполагает институционализацию этой деятельности, подготовку кадров социальных технологов и развитие социально-технологической культуры населения.

Эмпирической базой выступило глубинное интервью экспертов «Оценка уровня социально-технологической безопасности в крупных городах России» (N=30), проведенного с участием автора в апреле-мае 2026 года для уточнения основных параметров концепта проектирования системы социально-технологической безопасности крупного города и показателей его оценки. Для оценки социально-технологической безопасности городов применяется целевая стратифицированная выборка из 30 экспертов, сформированная по матрице «три типа городов × шесть профессиональных сфер». Городские страты включают крупные мегаполисы (Москва, Санкт-Петербург), а также диверсифицированные региональные агломерации (Казань, Екатеринбург) и города с пространственными либо ресурсными ограничениями (Белгород, Воронеж). В каждой страте представлены специалисты в области государственного управления, ЖКХ и критической инфраструктуры, IT- и кибербезопасности, науки, социальной сферы, а также НКО и информационной среды. Критериями включения выступают не менее пяти лет релевантного опыта, непосредственное знание соответствующего города или городского типа, участие в практических проектах либо исследованиях и способность подтверждать оценки конкретными данными и кейсами. Для сочетания контекстуальной глубины и сравнительной перспективы предусматривалось участие 20 локальных и 10 межгородских экспертов. Репрезентативность выборки обеспечивалась структурной полнотой и типологической представленностью мнений, а сопоставимость – единым гайдом полуструктурированного интервью.

Ключевыми исследовательскими вопросами выступили следующие:

1) Каким образом эксперты и представители городских институтов идентифицируют и разграничивают социально-технологические опасности и социально-технологические угрозы в крупных российских городах Северной Евразии с учетом таких признаков, как наличие субъекта воздействия, его намеренность и адресность, используемые технологии и предполагаемые последствия?

2) Каким образом сочетание высокой взаимозависимости городских инфраструктур и фрагментарности институционального управления связано с возникновением и воспроизводством социально-технологических уязвимостей крупных городов в условиях нестабильности?

3) Как эксперты оценивают готовность городских институтов и населения к выявлению, интерпретации и предупреждению социально-технологических опасностей и угроз, и какие институциональные, кадровые, образовательные и коммуникационные механизмы они считают приоритетными для формирования городской системы социально-технологической безопасности?

Научные результаты и дискуссия (Research Results and Discussion). Крупные российские города Северной Евразии целесообразно рассматривать не просто как урбанизированные территории с повышенной концентрацией населения, инфраструктуры и капитала, а как сложные социально-технологические системы, в которых уязвимость возникает на пересечении пространства, климата, демографии, институционального наследия, цифровизации и информационной среды. Под Северной Евразией здесь целесообразно понимать прежде всего российское и связанное с ним постсоветское городское пространство – от крупнейших агломераций Москвы и Санкт-Петербурга до сибирских, североказахстанских и арктических центров, крупных относительно окружающей системы расселения. Это пространство нельзя считать однородным: технологическая насыщенность, муниципальная автономия, климатические условия и структура экономики Москвы, Новосибирска, Астаны, Якутска и Норильска существенно различаются. Тем не менее у этих городов обнаруживается общее противоречие между высокой взаимозависимостью городских систем и фрагментарной способностью субъектов управлять этой взаимозависимостью.

Социальные технологии, традиционно рассматриваемые как специально организованная область знаний о способах и процедурах оптимизации жизнедеятельности человека в условиях нарастающей взаимозависимости, динамики и обновления общественных процессов, использовались людьми на разных этапах истории. При этом они (о чем часто забывают исследователи) постоянно эволюционируют. Данный процесс в современном обществе многократно интенсифицировался под воздействием цифровой революции. Произошла и продолжает проявлять себя конвергенция цифровых и традиционных социальных технологий, результатом которой стала их гибридизация, выражающаяся в соединении «физических» (технических и естественно-природных), социальных и информационно-коммуникационных (цифровых) процедур и операций.

«Современные социальные технологии представляют собой сложно структурированные комплексы алгоритмически выстроенных, синхронизированных “физических”, социальных и информационно-коммуникационных (цифровых) процедур и операций, разработанных и используемых для оптимизации общественных процессов» (Бабинцев, 2026: 215). Поскольку в эти технологиях ведущую роль играет цифровой компонент, их можно определить как инфосоциальные.

Благодаря развитию информационных систем, они становятся максимально доступными для городских жителей, удобны и эффективны при компетентном применении. Отражением этого процесса стало, в частности, оформление нейроурбанистики как самостоятельного направления в теории практике современного урбанизма. Но, способствуя

улучшению качества городской среды, как и любая другая общественная практика, социально-технологический подход к решению городских проблем одновременно порождает комплекс опасностей и угроз. При этом абсолютное большинство респондентов отмечают актуальность проблематики опасностей и угроз, связанных с неспособностью социальных институтов и граждан:

–профессионально применять социальные технологии (19 экспертов выбрали вариант ответа «актуально» и 11 – «скорее актуально, чем не актуально»): *«проблема состоит не столько в отсутствии социальных технологий, сколько в дефиците компетенций, позволяющих применять их профессионально. На практике управленческие решения нередко основываются на интуиции, краткосрочных политических интересах или механическом заимствовании готовых моделей без предварительной диагностики социальной среды»; «социальная технология эффективна только тогда, когда определены ее цели, целевые группы, критерии результативности и возможные побочные эффекты. Если эти элементы отсутствуют, технологическое воздействие превращается в набор несогласованных мероприятий и само может стать источником социальной нестабильности»*;

–противостоять воздействию манипулятивных технологий (24 и 6 экспертов соответственно): *«современные манипулятивные технологии действуют не только через распространение заведомо ложной информации. Значительно чаще используются эмоциональная поляризация, селективная подача фактов, создание искусственного ощущения общественного консенсуса и алгоритмическое усиление конфликтного контента»; «институты, как правило, реагируют уже на последствия информационного воздействия, тогда как сами манипулятивные кампании проектируются заранее и быстро адаптируются к реакции аудитории. В результате возникает устойчивое временное преимущество субъектов манипуляции»*;

–распознавать социальные технологии и антитехнологии – 19 и 9 экспертов соответственно: *«основная трудность заключается в отсутствии общепринятых критериев разграничения социальной технологии и антитехнологии. Один и тот же инструмент может использоваться как для общественно полезной мобилизации, так и для манипуляции, исключения отдельных групп или искусственного конструирования конфликта. Поэтому оценивать необходимо не только сам инструмент, но также цели, процедуру его применения и последствия»*; 2 считают, что «скорее не актуально, чем актуально»: *«не всякое технологически организованное воздействие следует интерпретировать как угрозу. Оценка должна зависеть от целей, степени прозрачности, добровольности участия и возможности граждан отказаться от воздействия»*;

–эффективно использовать цифровые и информационные ресурсы в социальной деятельности (22 и 8 экспертов соответственно): *«формальный доступ к цифровым ресурсам еще не означает способности эффективно использовать их в социальной деятельности. Пользователь должен уметь оценивать надежность источников, сопоставлять данные, понимать ограничения цифровых платформ и осознавать, каким образом алгоритмы влияют на отбор информации»; «организации нередко осуществляют цифровизацию существующих процедур, не меняя их содержания. В результате цифровые инструменты не повышают качество социальной деятельности, а лишь ускоряют воспроизводство прежних управленческих ошибок»*;

–формировать критическое мышление у населения для противодействия манипуляциям (22 и 8 экспертов соответственно): *«критическое мышление не следует сводить к общей недоверчивости или отрицанию официальных источников. Оно предполагает проверку происхождения информации, различение факта и интерпретации, анализ аргументации и готовность пересмотреть собственную позицию при появлении новых доказательств»; «противодействие манипуляциям должно строиться не только на опровержении*

отдельных ложных сообщений. Необходима систематическая образовательная работа, формирующая у населения устойчивые процедуры проверки информации и понимание механизмов воздействия на когнитивные и эмоциональные реакции»;

–оперативно адаптироваться к новым социальным технологиям – 21 и 6 экспертов соответственно: *«темпы распространения новых социальных технологий превышают скорость, с которой государственные, образовательные и правовые институты способны разрабатывать нормы их применения. Поэтому институциональная реакция часто носит запаздывающий и фрагментарный характер»; «адаптация не должна пониматься как безусловное принятие каждой технологической инновации. Она включает экспериментальную апробацию, оценку рисков, подготовку специалистов и создание механизмов отказа от технологии, если ее социальные издержки превышают ожидаемые преимущества»*; ; 2 считают, что «скорее не актуально, чем актуально»: *«проблема адаптации к новым социальным технологиям может быть несколько преувеличена: институты адаптируются к инновациям постепенно, а попытка регулировать каждое новшество на ранней стадии способна затормозить полезные эксперименты»*;

–обеспечивать цифровую безопасность личных данных (29 и 1 экспертов соответственно): *«защита персональных данных становится базовым условием институционального доверия. Утечка данных наносит не только материальный ущерб отдельному человеку, но и снижает готовность граждан пользоваться цифровыми государственными и социальными сервисами»*;

–предвидеть долгосрочные последствия социальных инноваций – 22 и 7 экспертов соответственно: *«социальные инновации обычно оцениваются по краткосрочным показателям – охвату, скорости внедрения или снижению издержек. При этом недостаточно учитываются отсроченные эффекты: трансформация норм, изменение структуры занятости, усиление неравенства и формирование зависимости от технологической инфраструктуры»*; 1 считает, что «скорее не актуально, чем актуально»: *«долгосрочные последствия социальных инноваций принципиально трудно прогнозировать. Поэтому вместо стремления к исчерпывающему предвидению продуктивнее создавать механизмы постоянного мониторинга и оперативной коррекции решений»*;

–взаимодействовать с ИИ-системами в социальном контексте (19 и 11 экспертов соответственно): *«компетентное взаимодействие с ИИ предполагает понимание того, что система не является нейтральным источником знания. Ее ответы зависят от обучающих данных, архитектуры модели, поставленной задачи и критериев, заданных разработчиком»; «в социальной сфере искусственный интеллект может повысить скорость обработки информации и обеспечить персонализацию услуг, но окончательная ответственность за решения, затрагивающие права и возможности человека, не должна передаваться алгоритму»*.

Полученные оценки позволяют реконструировать общую позицию экспертного сообщества как признание системного дефицита социально-технологической компетентности. По мнению экспертов, опасность обусловлена не отдельными технологиями как таковыми, а несоответствием между высокой скоростью их распространения и ограниченной способностью социальных институтов и граждан распознавать механизмы воздействия, профессионально применять цифровые инструменты, защищать персональные данные и оценивать отсроченные последствия инноваций. Наиболее выраженный консенсус наблюдается в отношении цифровой безопасности персональных данных: все 30 экспертов отнесли проблему к актуальной в той или иной степени, причем 29 выбрали безусловно положительную оценку. Существенное согласие также выявлено применительно к противодействию манипулятивным технологиям, формированию критического мышления, эффективному использованию цифровых ресурсов и взаимодействию с ИИ-системами. В

совокупности эти оценки указывают на необходимость перехода от реактивной модели устранения последствий к превентивной модели управления, включающей технологическую экспертизу, сценарное прогнозирование, развитие медиаграмотности и институциональную подотчетность.

В качестве основных причин актуализации в современных условиях социально-технологических опасностей и угроз экспертами были названы интенсивное развитие цифрового пространства (*«цифровая среда развивается быстрее, чем общество успевает осмыслить последствия ее распространения. Новые платформы и каналы коммуникации становятся массовыми еще до того, как формируются устойчивые нормы их использования и механизмы ответственности»; «современное цифровое пространство резко снижает стоимость производства и распространения недостоверного контента. Если раньше для проведения масштабной информационной кампании требовались значительные организационные ресурсы, то сегодня часть этих задач может быть автоматизирована»*), усложнение манипулятивных техник (*«манипуляция стала менее заметной. Она все реже строится на прямой лжи и все чаще – на смешении достоверных фактов, эмоциональных интерпретаций и умолчаний. Формально отдельные элементы сообщения могут быть правдивыми, но общая картина при этом оказывается искаженной»; «основным объектом воздействия становится не столько мнение человека по отдельному вопросу, сколько его эмоциональное состояние. Тревога, возмущение и ощущение срочности снижают вероятность критической проверки информации и повышают готовность делиться ею»*), а также отставание институциональных механизмов, когда социальные институты (власть, образование, НКО) не успевают адаптировать нормы и практики к темпам технологических изменений (*«технологические изменения происходят в режиме почти непрерывного обновления, тогда как государственное регулирование требует длительных процедур согласования. В результате нормативная база нередко описывает уже сложившиеся практики, а не предупреждает новые риски»; «институциональная реакция преимущественно носит постфактумный характер: сначала возникает новая угроза, затем она получает общественный резонанс и только после этого начинается поиск правовых и организационных решений»*) – Рисунок 1.

По мнению экспертов, актуализация социально-технологических угроз обусловлена не отдельными технологическими нововведениями, а рассогласованием между скоростью цифровой трансформации и адаптационными возможностями социальных институтов. Расширение цифрового пространства сопровождается алгоритмизацией информационных потоков, снижением стоимости производства контента и ростом возможностей его персонализации. Одновременно усложняются манипулятивные техники: прямое распространение ложных сведений дополняется эмоциональным фреймированием, селективным представлением достоверных фактов и имитацией массовой поддержки. Институциональные механизмы реагирования при этом характеризуются временным запаздыванием, недостаточной межсекторной координацией и дефицитом компетенций. Таким образом, социально-технологическая опасность возникает на пересечении технологической доступности инструментов воздействия, социальных уязвимостей аудитории и ограниченной способности институтов к опережающей адаптации.

Рисунок 1. Распределение ответов респондентов на вопрос: «Если Вы считаете проблему опасностей и угроз актуальной, то каковы основные причины ее актуализации? (укажите не более трех вариантов ответа)», множественный выбор, чел.[1]
Figure 1. Respondents' answers to the question: “If you consider the problem of dangers and threats to be relevant, what are the main reasons for its relevance? (Indicate no more than three answer options)”, persons

При этом социально-технологическая опасность представляет собой ситуацию, заключающую в себе возможность недостижения субъектом социального действия планируемых им результатов, либо утраты занимаемых позиций в социуме вследствие непрофессионального применения социальных технологий или неспособности адекватно интерпретировать аналогичные действия контрагентов. Опасность, как правило, не ориентирована на конкретных субъектов и актуализируется в ходе предпринимаемых ими действий. Напротив, социально-технологическая угроза проявляется в неспособности противостоять деструктивному социально-технологическому воздействию других акторов (мошенничество, манипуляции, информационный прямой и косвенный контроль), всегда носит адресный характер и инициируется тем или иным актором-оппонентом в связи как с действием, так и с бездействием ее адресата.

В предложенной понятийной рамке социально-технологическая опасность не тождественна ни природной опасности, ни технической неисправности. Она возникает тогда, когда неблагоприятное условие соединяется с дефицитом способности распознать проблему, согласовать действия, достоверно информировать население и применить технологии предупреждения или компенсации ущерба. Социально-технологическая угроза предполагает дополнительный признак – наличие актора, который намеренно использует организационные, информационные, правовые или цифровые технологии для деструктивного воздействия. Поэтому таяние мерзлоты само по себе является климатической опасностью, неспособность города организовать мониторинг деформаций превращает его в

[1] Сумма ответов превышает 100%, так как респонденты могли выбирать несколько вариантов.

социально-технологическую опасность, а сознательное сокрытие данных о деформациях ради продолжения эксплуатации объекта уже может рассматриваться как угроза. Аналитически опасность зависит от экспозиции города, его уязвимости, степени взаимозависимости систем и дефицита коллективной способности к действию; угроза – от намерения актора, его ресурсов, доступа к уязвимой системе и возможности скрывать или легитимировать свое воздействие.

К ключевым особенностям проявления социально-технологических опасностей и угроз применительно к крупным городам России экспертами были отнесены: высокая плотность населения, что увеличивает риск быстрого распространения социальных конфликтов и дезинформации через цифровые платформы; концентрация уязвимых групп в городской среде (мигранты, молодёжь, пожилые, малообеспеченные слои – все они сосуществуют в ограниченном пространстве, что усиливает риски социальной напряжённости); дефицит компетенций по управлению социально-технологическими рисками (Рисунок 2).

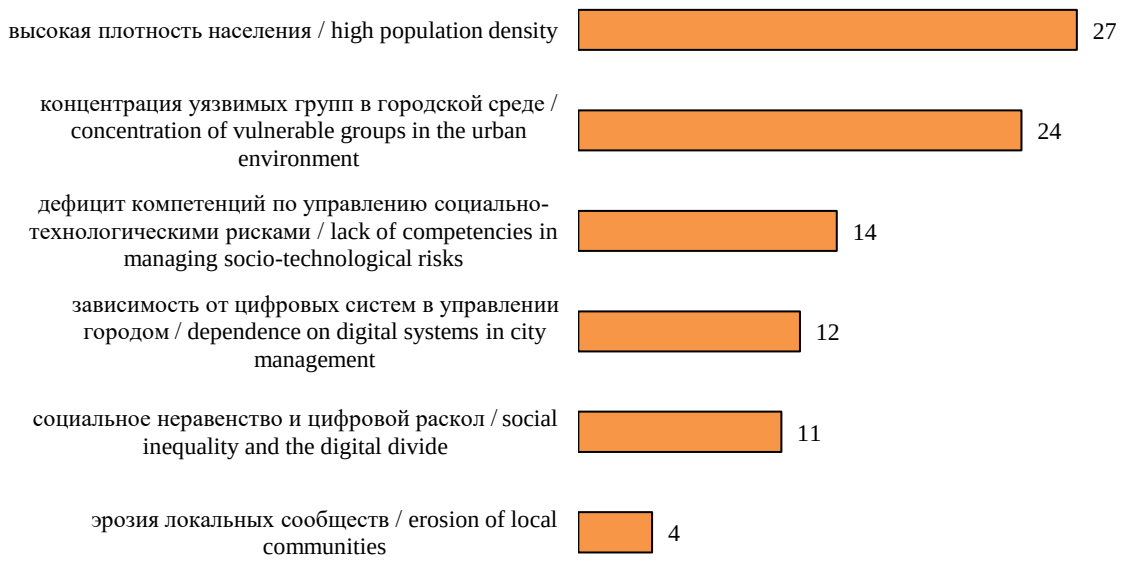

Рисунок 2. Распределение ответов респондентов на вопрос: «Можно ли, на Ваш взгляд, выделить какие-либо особенности проявления социально-технологических опасностей и угроз применительно к крупному городу России? (укажите не более трех вариантов ответа)», чел.[1]

Figure 2. Respondents' answers to the question: “In your opinion, is it possible to identify any particular features of the manifestation of socio-technological dangers and threats in relation to a large Russian city?”, persons

Фундаментальная опасность крупного города Северной Евразии состоит в несоответствии между физической интегрированностью инфраструктуры и организационной раздробленностью управления. Теплоснабжение, электроснабжение, связь, транспорт, больницы и платежные сервисы образуют не отдельные отрасли, а сеть взаимозависимых сетей. Модель С. Булдырева и соавторов показывает, что в таких системах даже ограниченный первоначальный сбой способен вызвать нелинейный каскад отказов в сопряженных сетях (Buldyrev, Parshani, Paul, 2010). Для североевразийского города эта абстрактная закономерность особенно существенна из-за централизованного

[1] Сумма ответов превышает 100%, так как респонденты могли выбирать несколько вариантов.

теплоснабжения, длительных отопительных сезонов и наследия крупных технических комплексов. Этнографическое исследование С. Кольера показывает, что постсоветская коммунальная инфраструктура одновременно является технической системой и институтом социальной политики: через тарифы, бюджетные обязательства и режимы подключения она распределяет не только тепло, но и социальную защищенность (Collier, 2011).

Социально-технологическая опасность здесь возникает, если коммунальные предприятия, муниципальные администрации, медицинские учреждения и операторы связи не имеют совместимых протоколов реагирования, общего представления о состоянии сети и защищенных каналов связи с населением. Особое значение имеет организационная культура: если сообщения о дефектах воспринимаются как угроза репутации руководства, система начинает накапливать скрытые отклонения. Небольшие аварии формально устраняются, но не превращаются в знания, меняющие регламенты. Социально-технологической угрозой та же взаимозависимость становится при целенаправленном воздействии на слабое звено: кибератаке на подрядчика, распространении ложного сообщения об аварии или эвакуации, создании искусственного дефицита информации либо намеренном нарушении координации между службами. Целью такого воздействия необязательно является физическое разрушение инфраструктуры; достаточно вызвать недоверие к официальным сообщениям и заставить людей действовать несогласованно.

Для арктических и субарктических городов физические процессы деградации мерзлоты образуют особенно наглядную связку природной и социально-технологической опасности. Пространственное моделирование показывает, что к середине XXI века значительная доля инфраструктуры в области распространения вечной мерзлоты окажется под повышенным риском повреждения (Hjort, J., Karjalainen, O., Aalto, 2018). Дмитрий Стрелецкий и соавторы отдельно оценили последствия этого процесса для зданий и инфраструктуры российских регионов на мерзлоте: (Streletskiy, Suter, Shiklomanov, 2019).

Однако социально-технологическая сторона риска определяется не температурой грунта как таковой, а тем, кто и как измеряет осадки фундаментов, кому принадлежат данные, существуют ли независимый аудит и процедура остановки эксплуатации, способен ли город переселять людей и обеспечивать резервные коммуникации. Опасность возрастает, когда мониторинг разделен между компаниями и ведомствами, а расходы на предупреждение ущерба несет один субъект, тогда как выгоду от продолжения эксплуатации получает другой. Угроза возникает, если заинтересованный актор сознательно занижает оценки, дискредитирует независимых экспертов, манипулирует общественными обсуждениями или использует административную зависимость жителей для блокирования сообщений о риске. Таким образом, климатический процесс становится средством деструктивного воздействия не сам по себе, а через управление информацией и зависимостями.

Не менее существенна деградация механизмов обратной связи между населением и институтами управления. Для крупного города жалоба, общественное обсуждение, журналистское расследование и сообщение работника о нарушении представляют собой сенсоры, без которых управляющий субъект теряет сведения о реальном состоянии системы. А. Желнина на материалах г. Санкт-Петербурга и г. Выборга показывает, что городская апатия может быть не исходным свойством граждан, а социально производимым результатом повседневного опыта: люди усваивают, что участие не приносит результата и что безопаснее не вмешиваться (Zhelnina, 2020). В рассматриваемой рамке это социально-технологическая опасность, поскольку субъект постепенно утрачивает способность к коллективному действию даже тогда, когда формальные каналы участия существуют. Если же консультации проектируются так, чтобы имитировать участие, заранее исключать нежелательные позиции и производить формальное согласие, они приобретают свойства

антитехнологии: институциональная форма обратной связи используется для блокирования самой обратной связи.

Особая группа опасностей связана с миграцией и социальной неоднородностью мегаполисов. Крупный город зависит от мобильного труда, но часто не создает понятной и доступной системы правовой навигации, языковой адаптации и проверки документов. Этнографическое исследование Мадлен Ривз в Москве показывает, что граница между «настоящим» и «поддельным» документом может производиться непрозрачными бюрократическими практиками, а не только поведением самого мигранта (Reeves, 2013). Социально-технологическая опасность состоит в том, что жители не могут надежно установить свой статус, получить достоверную консультацию и защититься от мошенничества. Это создает готовую инфраструктуру для угроз: вымогательства, целенаправленного распространения этнических слухов, провокации конфликтов и политической мобилизации через конструирование образа «опасной группы». Антитехнология здесь действует посредством социальной классификации: сложная городская проблема объясняется присутствием выбранной категории людей, после чего агрессия направляется не на источник проблемы, а на символически назначенную цель.

Информационная среда крупных городов характеризуется сочетанием традиционных СМИ, муниципальных каналов, платформ, районных сообществ и закрытых чатов. Ее опасность заключается не просто в наличии ложных сообщений, а в разрыве между скоростью распространения информации и скоростью институциональной проверки. Эмпирическая работа Д. Стукала, С. Сановича, Р. Бонно и Дж. Такера демонстрирует возможность выявлять политических ботов и подтверждает наличие автоматизированного вмешательства в публичную коммуникацию: (Stukal, Sanovich, Bonneau, Tucker, 2017). Кроме того, «в условиях острых международных противоречий, социально-политической нестабильности и конфликтов злонамеренное использование всё более совершенных технологий искусственного интеллекта (ИИ) представляет растущую угрозу информационно-психологической безопасности общества и, как следствие, для политических, социальных, экономических, культурных процессов и деятельности государственных и негосударственных институтов» (Пашенцев, Кузнецов, Чебыкина, 2025: 125). Исследование Е. Головченко, М. Хартманн и Р. Адлера-Ниссен на материале информационного конфликта вокруг Украины показывает более сложную картину, в которой дезинформацию распространяют не только централизованные операторы, но и гражданские «кураторы» контента, включенные в сетевой конфликт: (Golovchenko, Hartmann, Adler-Nissen, 2018). Поэтому само наличие множества сходных публикаций еще не доказывает существование единого центра управления, но позволяет исследовать координацию, временные паттерны и повторяющиеся нарративы.

Для города опасны ложные сообщения о заражении воды, работе больниц, дефиците топлива, действиях этнических групп или порядке эвакуации. Если администрация не имеет заранее подготовленного протокола проверки, а население не знает, какой канал считать первичным источником, даже стихийный слух способен произвести ущерб. Угрозой является намеренная фабрикация такого слуха, его координированное распространение через боты, псевдолокальные сообщества и поддельные документы, а также подавление корректирующей информации. Фактчекинг после публикации здесь недостаточен, поскольку негативный эффект может наступить до появления опровержения. Экспериментальные исследования превентивного обучения, включая игру «Go Viral!», показывают, что краткое знакомство с приемами эмоциональной манипуляции, ложной экспертности и конспирологического связывания событий способно повысить устойчивость к дезинформации в разных культурных контекстах (Basol, 2021). Социально-технологическая опасность, следовательно, состоит также в неспособности локализовать такие контртехнологии под языки, проблемы и реальные медиаканалы конкретного города.

Цифровизация городского управления усиливает двойственность социальных технологий. Камеры, биометрическая идентификация, цифровые пропуска, предиктивная аналитика и приложения обратной связи могут сокращать время реакции на аварии, но одновременно концентрируют данные и власть «классификации». Опасность появляется при непрозрачности алгоритма, отсутствии процедуры обжалования, низком качестве данных и зависимости гражданина от автоматического решения. Ошибочная запись способна ограничить доступ к услуге, а человек не всегда понимает, какой субъект отвечает за исправление ошибки.

Наиболее общей социально-технологической опасностью крупных городов Северной Евразии является, таким образом, потеря достоверной отрицательной обратной связи. Город остается управляемым, пока сведения об аварии, заболевании, конфликте или злоупотреблении могут пройти снизу вверх, быть проверены независимым способом и вызвать изменение решений. Опасность появляется, когда субъект не способен построить такую цепочку; угроза – когда другой актор сознательно загрязняет ее ложными сигналами, блокирует сообщения, фабрикует согласие или перенаправляет недовольство на ложную цель. Наиболее уязвим поэтому не обязательно технологически отсталый город, а город, в котором внешне развитые цифровые и административные системы не допускают проверки собственных ошибок.

При исследовании конкретного случая отрицательный эффект нельзя автоматически считать доказательством угрозы. Для такого вывода необходимо установить целевой объект воздействия, выбор соответствующего инструмента, координацию действий, устойчивое продолжение практики после того, как вред стал известен, а также попытки скрыть авторство или представить воздействие как естественный ход событий. Если эти признаки не обнаружены, корректнее говорить о социально-технологической опасности, организационной неспособности или непреднамеренном побочном эффекте. Такое различение принципиально: оно не позволяет объяснять любой городской кризис злым умыслом, но одновременно делает видимыми случаи, когда инфраструктурная зависимость, цифровая платформа, корпоративная социальная политика или общественное участие целенаправленно обращаются в антитехнологии.

При этом экспертное сообщество, определяя характерный для большинства типичный уровень представлений о социально-технологических опасностях и угрозах в крупных городах, в большинстве своем определяют его как низкий (Рисунок 3), что наглядно демонстрирует необходимость формирования и развития системы социально-технологической безопасности крупных городов.

Анализ экспертных оценок позволяет предположить, что типичный уровень представлений жителей крупных городов о социально-технологических угрозах характеризуется не столько полным отсутствием осведомленности, сколько ее фрагментарностью, ситуативностью и слабой возможностью перевода в практические действия. Граждане чаще распознают отдельные, широко освещаемые угрозы, однако не всегда понимают взаимозависимость технологических, информационных, институциональных и поведенческих факторов. Эксперты связывают уязвимость населения с дефицитом навыков верификации информации, отсутствием устойчивых алгоритмов поведения, переносом ответственности на государство и цифровые платформы, а также с недостатком доверия к официальным каналам коммуникации. При этом оценки указывают на социальную и территориальную неоднородность уровня готовности. Следовательно, формирование социально-технологической безопасности крупных городов требует перехода от эпизодического информирования к комплексной системе мониторинга, риск-коммуникации, практического обучения и межведомственного взаимодействия.

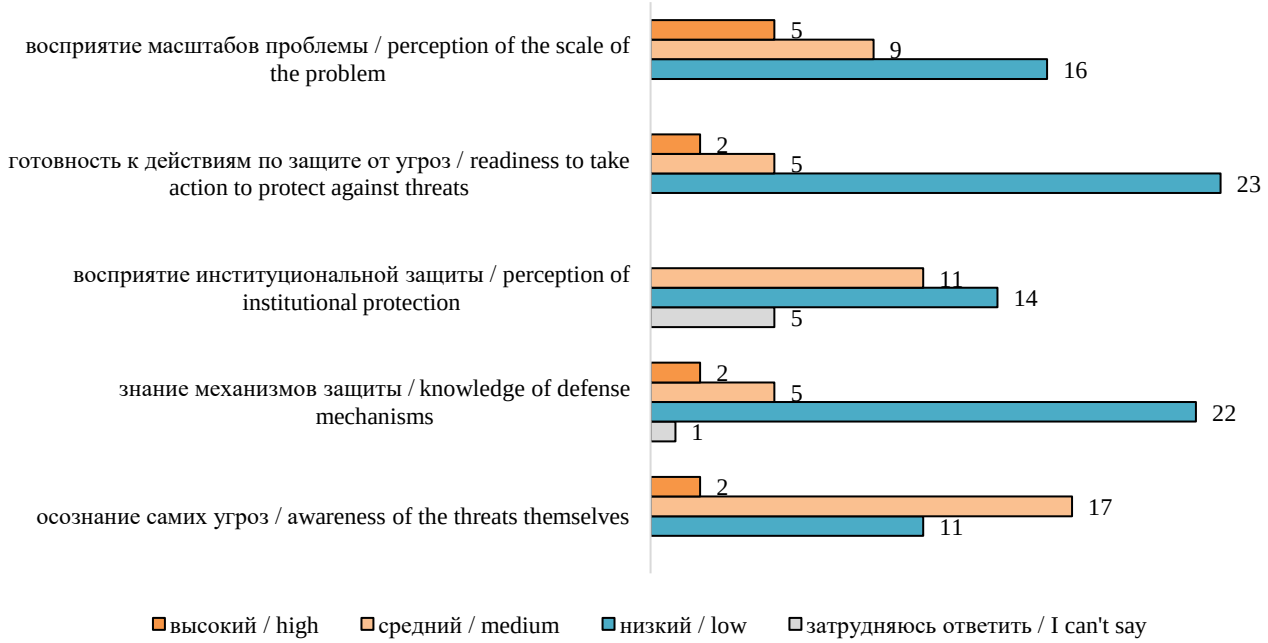

Рисунок 3. Распределение ответов респондентов на вопрос: «Как бы Вы определили типичный уровень представлений о социально-технологических опасностях и угрозах в крупных городах, характерный для большинства?», чел.
Figure 3. Respondents' answers to the question: “How would you define the typical level of understanding of socio-technological dangers and threats in large cities, characteristic of the majority?”, persons

Социально-технологическая безопасность рассматривается нами как система социальных институций[1], совместная деятельность которых позволяет оптимальным образом минимизировать деструктивные по отношению к региональному сообществу или его отдельным элементам опасности и угрозы, либо устранить их последствия путем применения алгоритмически выстроенных процедур и операций. Для крупных городов Северной Евразии такая система является не факультативным управленческим дополнением, а условием сохранения городской жизнеспособности.

Необходимость такой системы вытекает из самой природы современных урбанизированных рисков, что было отмечено всеми опрошенными экспертами. Классическая работа Чарльза Перроу о «нормальных авариях» (Perrow, 1999) показывает, что в сложных и тесно связанных системах крупные сбои могут возникать не из-за одного грубого нарушения, а из-за непредсказуемого взаимодействия множества технических и организационных факторов. Для города Северной Евразии эта логика особенно значима, потому что городские системы жизнеобеспечения здесь не просто сложны, но и климатически нагружены. Исследования взаимозависимостей критической инфраструктуры показывают, что энергетика, связь, водоснабжение, транспорт и управление образуют систему, где нарушение одного элемента способно распространяться по цепочке (Rinaldi, Peerenboom, Kelly, 2001). Следовательно, социально-технологическая безопасность должна быть направлена не на изолированное тушение отдельных аварий, а на управление переходами между техническим, социальным, информационным и институциональным контурами кризиса.

[1] Институция – система основанных на действующих социальных нормах правил, регулирующих поведение людей в какой-либо сфере жизни.

Возможность построения такой системы связана с тем, что необходимые научные, организационные и технологические основания уже существуют. Во-первых, современная теория устойчивости дает язык для описания того, что именно надо защищать. «Устойчивость системы – это не простое возвращение к прежнему состоянию, а способность сохранять функции в условиях возмущений и перестройки» (Holling, 1973). В обзоре определений городской устойчивости авторы подчеркивают, что городская устойчивость включает способность города выдерживать, адаптироваться и трансформироваться при шоках и хронических стрессах (Meerow, Newell, Stults, 2016). Для крупных городов Северной Евразии это означает, что целью должна быть не иллюзия полного предотвращения всех угроз, а создание институциональной способности обнаруживать, локализовать, компенсировать и осмысленно преодолевать сбои.

Во-вторых, существует развитая теория риск-управления и риск-коммуникации. Управление сложными рисками требует соединения экспертной оценки, участия заинтересованных сторон, прозрачной коммуникации и легитимных процедур принятия решений (Renn, Walker, 2010). Значит, система социально-технологической безопасности должна быть не закрытым штабом, который «знает лучше всех», а многоуровневым механизмом, где научная экспертиза, муниципальное управление, операторы инфраструктуры, школы, медиа, НКО, бизнес и районные сообщества включены в единую процедуру распознавания и обработки угроз.

В-третьих, возможность обеспечивается развитием цифровых инструментов мониторинга и моделирования. Спутниковые данные, городские сенсоры, геоинформационные системы, цифровые двойники инфраструктуры, анализ обращений граждан, мониторинг погодных и экологических параметров позволяют строить раннее предупреждение не только по факту аварии, но и по признакам приближения кризиса. Цифровые двойники выступают действенным способом соединять модели города с потоками данных и управленческими решениями (Batty, 2018). Однако для социально-технологической безопасности важно подчеркнуть, что цифровой двойник сам по себе не решает проблему. Он становится элементом безопасности только тогда, когда включен в алгоритм институционального действия: сигнал обнаруживается, проходит верификацию, получает классификацию по типу риска, сопоставляется со сценариями, передается ответственным субъектам, сопровождается публичным сообщением, затем проверяется по обратной связи и фиксируется в базе уроков.

Именно такой алгоритм должен стать ядром системы. В нормальном режиме город непрерывно собирает сигналы из физической среды, инфраструктуры и социальной коммуникации. Эти сигналы проходят проверку достоверности: инженерную, экспертную, статистическую, территориальную, медиалогическую. После этого событие классифицируется как обычное отклонение, локальная опасность, потенциальный каскадный сбой или целенаправленная социально-технологическая угроза. Далее включается сценарное моделирование: какие районы, группы, сети и службы будут затронуты, каковы критические сроки, где возможны вторичные эффекты. Затем выбирается протокол действия: ремонт, эвакуация, адресная помощь, ограничение движения, санитарные меры, информационное предупреждение, опровержение фейка, подключение волонтеров, перевод служб в особый режим. После выполнения протокола система собирает обратную связь, сравнивает прогноз с реальным ходом событий и корректирует процедуры. Такой алгоритм не является только программным кодом; это социальная технология, то есть формализованный порядок совместного действия институтов.

С точки зрения экспертов, обязательными элементами системы социально-технологической безопасности выступают: нормативно-правовая база (совокупность законов, регламентов и контрольных механизмов, обеспечивающих правовое регулирование защиты данных и ИТ-инфраструктуры); техническая защита (комплекс технологических

решений для предотвращения несанкционированного доступа, утечек и сбоев); образование и просвещение (программы повышения цифровой грамотности населения и специалистов); технологические инновации (передовые решения для прогнозирования и нейтрализации угроз); системы диспетчеризации и координации действий; системы оценки и управление биолого-социальными угрозами (Рисунок 4). К желательным были отнесены: институциональные механизмы (структуры и процедуры координации между ведомствами и обществом); инфраструктура доверия (меры по обеспечению прозрачности и подотчётности цифровых систем); вовлечение населения и развитие социальной инфраструктуры.

Рисунок 4. Распределение ответов респондентов на вопрос: «Если необходимо создание в крупных городах РФ системы социально-технологической безопасности, то какие элементы должна включать в себя эта система?», чел.

Figure 4. Respondents' answers to the question: " If it is necessary to create a social and technological security system in large cities of the Russian Federation, what elements should this system include?", persons

Таким образом, институционально систему социально-технологической безопасности можно представить как городской контур социально-технологической безопасности, где центральное место занимает не один «главный орган», а связка нескольких функций. Нужен городской или агломерационный центр анализа рисков, который соединяет данные о климате, инфраструктуре, здоровье населения, транспорте, экологии и информационной

среде. Нужен независимый научно-экспертный контур при участии университетов и исследовательских организаций, потому что доверие к решениям возрастает, когда они опираются не только на административную вертикаль, но и на проверяемую экспертизу. Нужен коммуникационный центр, который умеет говорить с населением до кризиса, во время кризиса и после него, причем не бюрократическим языком, а понятными сообщениями с указанием источников, неопределенностей и практических действий. Нужна сеть районных посредников: школ, поликлиник, управляющих компаний, библиотек, волонтерских групп, местных медиа, домовых и родительских чатов. Именно они превращают городскую безопасность из абстрактной политики в повседневную практику.

Особое значение имеет контур противодействия дезинформации. Он не должен сводиться к цензуре или механическому удалению сообщений, потому что такая стратегия часто только усиливает недоверие. Более продуктивна модель «эпистемической инфраструктуры» – город заранее создает проверяемые каналы информации, обучает жителей базовым процедурам проверки, публикует открытые данные, объясняет границы неопределенности и быстро реагирует на ложные сообщения. Исследования показывают, что психологическая инокуляция, то есть предварительное знакомство людей с типичными приемами манипуляции, повышает устойчивость к дезинформации (Roozenbeek, Linden, Nygren, 2020), а даже простое переключение внимания пользователя на точность информации может снижать распространение ложных сообщений (Pennycook et al, 2021). Поэтому в крупном городе нужны образовательные симуляторы, школьные и студенческие модули медиаграмотности, муниципальные фактчекинговые протоколы, боты предварительной проверки сообщений и публичные разборы резонансных фейков (т.к. «распространение противоречивых версий событий дезориентирует аудиторию, подрывая доверие к информационному контенту в целом» (Казун, 2025: 46)). Но все это должно быть встроено в общую систему доверия, иначе фактчекинг будет восприниматься как еще один голос в конфликте.

Важным условием возможности является полицентричность управления. Если вся безопасность строится только как вертикальная команда сверху вниз, система становится хрупкой: она медленно видит локальные сигналы, хуже учитывает контекст районов и провоцирует зависимость населения от указаний. В работах о полицентрическом управлении демонстрируется, что сложные коллективные проблемы лучше решаются через сочетание разных центров принятия решений, взаимного контроля и локального знания (Ostrom, 2010). Для крупного города это особенно важно: муниципальная власть должна задавать стандарты и обеспечивать координацию, но школы, больницы, коммунальные службы, научные организации, бизнес и местные сообщества должны обладать собственными процедурами обнаружения, сообщения и первичного реагирования. Тогда город становится не пирамидой, а сетью с устойчивыми узлами.

Однако возможность построения системы не означает ее автоматической реализуемости. Главные препятствия лежат не столько в отсутствии технологий, сколько в институциональной фрагментации. Данные часто принадлежат разным ведомствам и компаниям, стандарты несовместимы, ответственность размыта, стимулы к сокрытию проблем сильнее стимулов к раннему предупреждению, а публичная коммуникация включается уже после того, как доверие подорвано. Поэтому построение системы социально-технологической безопасности должно начинаться с изменения логики управления: от реагирования на чрезвычайную ситуацию к постоянной работе с предкризисными признаками; от ведомственной закрытости к совместимым данным; от разовой кампании к непрерывному обучению; от монологической пропаганды к доказательной коммуникации; от контроля населения к партнерству с ним.

Для крупных городов Северной Евразии такая система должна иметь региональный масштаб. Город не заканчивается административной границей: его безопасность зависит от пригородов, трасс, железных дорог, аэропортов, электросетей, водосборов, промышленных площадок, лесных массивов, миграционных потоков и цифровых платформ. Поэтому социально-технологическая безопасность должна строиться как агломерационная и межрегиональная. Это делает возможным создание сетей обмена сценариями, протоколами, картами рисков, образовательными модулями и результатами учений между городами.

Заключение (Conclusions). Необходимость системы социально-технологической безопасности определяется переходом городских рисков в режим каскадности и гибридности. Опасности уже не существуют отдельно как «природные», «технические», «социальные» или «информационные»: они переходят друг в друга. Угроза же возникает тогда, когда деструктивный актор целенаправленно использует эту связанность, превращая технический сбой в кризис доверия, социальное напряжение – в конфликт, неопределенность – в управляемую панику. Возможность построения системы безопасности определяется тем, что уже существуют научные модели устойчивости, риск-управления, полицентрического управления, цифрового мониторинга, фактчекинга и образовательной инокуляции против манипуляций. Главная задача теперь – собрать их в институционально оформленный городской механизм.

Такая система будет эффективной только при одном принципиальном условии: она должна минимизировать не только ущерб, но и произвол. Социально-технологическая безопасность не должна превращаться в тотальную систему наблюдения и подавления неопределенности. Ее смысл – не в том, чтобы заменить общество управляемой массой, а в том, чтобы повысить способность городского сообщества к рациональному совместному действию в условиях холода, риска, давления и информационной нестабильности. Для крупных российских городов Северной Евразии это, по существу, новая форма городской цивилизационной устойчивости: способность сохранять инфраструктуру, доверие, знание и солидарность тогда, когда внешняя среда и деструктивные акторы пытаются разрушить связи между ними.

Перспективы дальнейших исследований связаны прежде всего с переходом от общей концепции социально-технологической безопасности к ее эмпирической и методической операционализации. Необходимо разработать систему показателей, позволяющих измерять не только техническую надежность городской инфраструктуры, но и качество отрицательной обратной связи, скорость выявления слабых сигналов, уровень доверия к официальным каналам, устойчивость информационной среды, готовность населения к кооперации и способность институтов к самоисправлению. Без таких индикаторов социально-технологическая безопасность остается важной, но преимущественно теоретической рамкой.

Важной исследовательской задачей является моделирование гибридных угроз, возникающих на стыке технических, социальных и информационных процессов. Перспективными здесь могут быть сценарный анализ, агент-ориентированное моделирование, городские цифровые двойники, деловые игры и образовательные симуляторы. Однако такие инструменты должны учитывать не только материальные потоки и инфраструктурные зависимости, но и поведение граждан, динамику доверия, распространение слухов, медиапотребление, реакцию локальных сообществ и особенности риск-коммуникации.

Особого внимания требует изучение правовых и этических границ систем городской безопасности. Будущие исследования должны ответить на вопрос, каким образом можно совмещать мониторинг рисков, анализ больших данных и профилактику дезинформации с защитой гражданских прав, прозрачностью алгоритмов и общественным контролем. Иными

словами, перспективной становится не только инженерная или управленческая, но и нормативная теория социально-технологической безопасности, способная отличать легитимное предупреждение угроз от избыточного административного вмешательства.

Список литературы

Бабинцев В. П. Социальные технологии в социологическом и «несоциологическом» измерении // Вестник Российского университета дружбы народов. Серия: Социология. 2026. Т. 26, № 1. С. 215-223. DOI: 10.22363/2313-2272-2026-26-1-215-223. EDN: QEKZOB.

Вильданов Х. С., Хабибуллин И. Г. Социальная безопасность и духовный суверенитет современного российского общества в условиях ментальных войн // Общество: философия, история, культура. 2025. № 12. С. 14-22. DOI: 10.24158/fik.2025.12.1. EDN: QTFNKH.

Делез Ж., Гваттари П.-Ф. Анти-Эдип. Капитализм и шизофрения. Т. 1. Москва: Рипол-Классик, 2025. 512 с.

Делез Ж., Гваттари П.-Ф. Тысяча плато. Капитализм и шизофрения. Т. 2. Москва: Рипол-Классик, 2025. 768 с.

Казун А. Д. «Очернить светлое и чистое, обелить темное и грязное»: представления россиян о потенциальных рисках фейковых новостей // Интеракция. Интервью. Интерпретация. 2025. Т. 17, № 3. С. 35-54. DOI: 10.19181/inter.2025.17.3.2. EDN: ZQUXKW.

Кастельс М. Информационная эпоха: экономика, общество и культура. Москва: ГУ ВШЭ, 2000. 608 с.

Лиотар Ж.-Ф. Состояние постмодерна. Москва: Ин-т эксперим. социологии; Санкт-Петербург: Алетейя, 1998. 159 с.

Пашенцев Е. Н., Кузнецов П. В., Чебыкина В. А. Злонамеренное использование искусственного интеллекта и угрозы информационно-психологической безопасности для Ирана: многоуровневая реальность. Восток (Oriens). 2025. № 3. С. 125-136. DOI: 10.31696/S086919080033177-1. EDN: ZMIMPA.

Тоффлер Э. Шок будущего. Москва: АСТ, 2025. 544 с.

Тоффлер Э. Третья волна. Москва: АСТ, 2004. 781 с.

Тоффлер Э. Метаморфозы власти. Москва: АСТ, 2003. 669 с. ISBN: 5-17-004183-7. EDN: QOCCFP.

Штомпка П. Социология социальных изменений. Москва: Аспект-пресс, 1996. 414 с.

Bauman Z. Liquid Modernity. Cambridge: Polity Press, 2000.

Basol M., Roozenbeek J., Berriche M., Uenal F., McClanahan W., van der Linden S. Towards psychological herd immunity: Cross-cultural evidence for two prebunking interventions against COVID-19 misinformation // Big Data & Society. 2021. Vol. 8. DOI: 10.1177/20539517211013868. EDN: NQUVWB.

Batty M. Digital twins // Environment and Planning B: Urban Analytics and City Science. 2018. Vol. 45, No. 5. Pp. 817-820. DOI: 10.1177/2399808318796416.

Beck U. Risk Society: Towards a New Modernity. London: Sage, 1992.

Buldyrev S., Parshani R., Paul G. et al. Catastrophic cascade of failures in interdependent networks // Nature. 2010. Vol. 464. Pp. 1025-1028. DOI: 10.1038/nature08932.

Buzan B., Wæver O., de Wilde J. Security: A New Framework for Analysis. Boulder: Lynne Rienner Publishers, 1998.

Chambers R. Vulnerability, Coping and Policy (Editorial Introduction) // IDS Bulletin. 2009. Vol. 37. Pp. 33-40.

Collier S. J. Post-Soviet Social Neoliberalism Social Modernity Biopolitics. Princeton: Princeton University Press, 2011. DOI: 10.23943/princeton/9780691148304.001.0001.

Cutter S. The Vulnerability of Science and the Science of Vulnerability // Annals of the Association of American Geographers. 2003. Vol. 93. Pp. 1-12. DOI: 10.1111/1467-8306.93101. EDN: MEUSTY.

Douglas M., Wildavsky A. Risk and Culture: An Essay on the Selection of Technological and Environmental Dangers. Berkeley: University of California Press, 1982.

Giddens A. The Consequences of Modernity. Stanford: Stanford University Press, 1990.

Giddens A. Modernity and Self-Identity. Stanford: Stanford University Press, 1991.

Golovchenko Y., Hartmann M., Adler-Nissen R. State, media and civil society in the information warfare over Ukraine: Citizen curators of digital disinformation // International Affairs. 2018. Vol. 94. Pp. 975-994. DOI: 10.1093/ia/iiy148. EDN: ERFBWD.

Hjort J., Karjalainen O., Aalto J. et al. Degrading permafrost puts Arctic infrastructure at risk by mid-century // Nature Communications. 2018. Vol. 9. P. 5147. DOI: 10.1038/s41467-018-07557-4. EDN: ANNAYC.

Holling C. S. Resilience and Stability of Ecological Systems // Annual Review of Ecology, Evolution, and Systematics. 1973. Vol. 4. Pp. 1-23. DOI: 10.1146/annurev.es.04.110173.000245.

Luhmann N. Risk: A Sociological Theory. Berlin; New York: De Gruyter, 1993.

Meerow S., Newell J. P., Stults M. Defining urban resilience: A review // Landscape and Urban Planning. 2016. Vol. 147. Pp. 38-49. DOI: 10.1016/j.landurbplan.2015.11.011.

Moser C. Confronting Crisis in Angyalföld, Budapest, Hungary. Michigan: World Bank, 1997.

Ostrom E. Beyond Markets and States: Polycentric Governance of Complex Economic Systems // American Economic Review. 2010. Vol. 100, № 3. Pp. 641-672. DOI: 10.1257/aer.100.3.641.

Pennycook G., Epstein Z., Mosleh M., Arechar A. A., Eckles D., Rand D. G. Shifting attention to accuracy can reduce misinformation online // Nature. 2021. Vol. 592. Pp. 590-595. DOI: 10.1038/s41586-021-03344-2. EDN: VQQDWP.

Perrow C. Normal Accidents: Living with High-Risk Technologies. Princeton: Princeton University Press, 1999.

Renn O., Walker K. Global Risk Governance: Concept and Practice Using the IRGC Framework. Dordrecht: Springer Netherlands, 2010.

Reeves M. Clean Fake: Authenticating Documents and Persons in Migrant Moscow // American Ethnologist. 2013. Vol. 40. DOI: 10.1111/amet.12036.

Rinaldi S. M., Peerenboom J. P., Kelly T. K. Identifying, understanding, and analyzing critical infrastructure interdependencies // IEEE Control Systems. 2001. Vol. 21, № 6. DOI: 10.1109/37.969131.

Roozenbeek J., van der Linden S., Nygren Th. Prebunking interventions based on the psychological theory of «inoculation» can reduce susceptibility to misinformation across cultures // HKS Misinformation Review. 2020. Vol. 1. DOI: 10.37016/mr-2020-008. EDN: QESJPI.

Rosa H. Social Acceleration: A New Theory of Modernity. New York: Columbia University Press, 2013.

Streletskiy D. A., Suter L. J., Shiklomanov N. I. et al. Assessment of climate change impacts on buildings, structures and infrastructure in the Russian regions on permafrost // Environmental Research Letters. 2019. Vol. 14, № 2. 025003. DOI: 10.1088/1748-9326/aaf5e6. EDN: AHATIK.

Stukal D., Sanovich S., Bonneau R., Tucker J. Detecting Bots on Russian Political Twitter // Big Data. 2017. Vol. 5. Pp. 310-324. DOI: 10.1089/big.2017.0038.

Zhelnina A. The apathy syndrome: How we are trained not to care about politics // Social Problems. 2020. Vol. 67, № 2. Pp. 358-378. DOI: 10.1093/SOCPRO/SPZ019. EDN: SRIGCY.

References

Babintsev, V. P. (2026), “Social technologies in the sociological and “nonsociological” dimensions”, *RUDN Journal of Sociology,* 26 (1), 215-223, DOI: 10.22363/2313-2272-2026-26-1-215-223, EDN: QEKZOB. (In Russian)

Vildanov, Kh. S. and Khabibullin, I. G. (2025), “Social Security and Spiritual Sovereignty of Modern Russian Society in the Context of Mental Wars”, *Society: Philosophy, History, Culture,* (12), 14-22, DOI: 10.24158/fik.2025.12.1, EDN: QTFNKH. (In Russian)

Delez, Zh., Gvattari, P.-F. (2025), *Anti-Edip. Kapitalizm i shizofreniya* [Anti-Oedipus. Capitalism and Schizophrenia], 1, Ripol-Klassik, Moscow, Russia. (In Russian)

Delez, Zh., Gvattari, P.-F. (2025), *Tysyacha plato. Kapitalizm i shizofreniya* [A Thousand Plateaus. Capitalism and Schizophrenia], 2, Ripol-Klassik, Moscow, Russia. (In Russian)

Kazun, A. D. (2025), “To Tarnish the Pure and Illuminate the Tainted: Russian Perceptions of the Potential Risks of Fake News”, *Interaction. Interview. Interpretation,* 17 (3), 35-54, DOI: 10.19181/inter.2025.17.3.2, EDN: ZQUXKW. (In Russian)

Kastels, M. (2000), *Informatsionnaya epoлpa: ekonomika, obshhestvo i kultura* [The Information Age: Economy, Society, and Culture], GU VShE, Moscow, Russia. (In Russian)

Liotar, Zh.-F. (1998), *Sostoyanie postmoderna* [The state of postmodernism], In-t eksperim. sociologii, Moscow, Russia. (In Russian)

Pashentsev, E. N., Kuznetsov, P. V. and Chebykina, V. A. (2025), "Malicious Use of Artificial Intelligence and Threats to Iran's Psychological Security: A Multi-Level Reality", *Vostok (Oriens),* (3), 125-136, DOI: 10.31696/S086919080033177-1, EDN: ZMIMPA. (In Russian)

Toffler, E. (2025), *Shok budushhego* [Future shock], AST, Moscow, Russia. (In Russian)

Toffler, E. (2004), *Tretya volna* [The third wave], AST, Moscow, Russia. (In Russian)

Toffler, E. (2003), *Metamorfozy vlasti* [Метаморфозы власти], AST, Moscow, Russia, ISBN: 5-17-004183-7, EDN: QOCCFP. (In Russian)

Shtompka, P. (1996), *Sotsiologiya sotsialnykh izmeneniy* [Sociology of social change], Aspekt-press, Moscow, Russia. (In Russian)

Bauman, Z. (2000), *Liquid Modernity,* Polity Press, Cambridge.

Basol, M., Roozenbeek, J., Berriche, M., Uenal, F., McClanahan, W. and van der Linden, S. (2021), "Towards psychological herd immunity: Cross-cultural evidence for two prebunking interventions against COVID-19 misinformation", *Big Data & Society,* 8, DOI: 10.1177/20539517211013868, EDN: NQUVWB.

Batty, M. (2018), "Digital twins", *Environment and Planning B: Urban Analytics and City Science*, 45 (5), 817-820, DOI: 10.1177/2399808318796416.

Beck, U. (1992), *Risk Society: Towards a New Modernity,* Sage, London.

Buldyrev, S., Parshani, R., Paul, G. et al. (2010), "Catastrophic cascade of failures in interdependent networks". *Nature,* 464, 1025-1028, DOI: 10.1038/nature08932.

Buzan, B., Waever, O., and de Wilde, J. (1998), *Security: A New Framework for Analysis*, Lynne Rienner Publishers, Boulder.

Chambers, R. (2009), "Vulnerability, Coping and Policy (Editorial Introduction)", *IDS Bulletin,* 37, 33-40.

Collier, S. J. (2011), *Post-Soviet Social Neoliberalism Social Modernity Biopolitics*, Princeton University Press, Princeton NJ, DOI: 10.23943/princeton/9780691148304.001.0001.

Cutter, S. (2003), "The Vulnerability of Science and the Science of Vulnerability", *Annals of The Association of American Geographers – ANN ASSN AMER GEOGR,* 93, 1-12, DOI: 10.1111/1467-8306.93101, EDN: MEUSTY.

Douglas, M. and Wildavsky, A. (1982), *Risk and Culture: An Essay on the Selection of Technological and Environmental Dangers,* University of California Press, Berkeley.

Giddens, A. (1990), *The Consequences of Modernity,* Stanford University Press, Stanford.

Giddens, A. (1991), *Modernity and Self-Identity,* Stanford University Press, Stanford.

Golovchenko, Y., Hartmann, M. and Adler-Nissen, R. (2018), "State, media and civil society in the information warfare over Ukraine: Citizen curators of digital disinformation", *International Affairs,* 94, 975-994, DOI: 10.1093/ia/iiy148, EDN: ERFBWD.

Hjort, J., Karjalainen, O., Aalto, J. et al. (2018), "Degrading permafrost puts Arctic infrastructure at risk by mid-century", *Nat Commun,* 9, 5147, DOI: 10.1038/s41467-018-07557-4, EDN: ANNAYC.

Holling, C. S. (1973), "Resilience and Stability of Ecological Systems", *Annual Review of Ecology, Evolution, and Systematics,* 4, 1-23, DOI: 10.1146/annurev.es.04.110173.000245.

Luhmann, N. (1993), *Risk: A Sociological Theory,* De Gruyter, Berlin, New York.

Meerow, S., Newell, J. P., and Stults, M. (2016), "Defining urban resilience: A review", *Landscape and urban planning,* 147, 38-49, DOI: 10.1016/j.landurbplan.2015.11.011.

Moser, C. (1997), *Confronting Crisis in Angyalföld, Budapest, Hungary*. World Bank, Michigan.

Ostrom, E. (2010), "Beyond Markets and States: Polycentric Governance of Complex Economic Systems", *American Economic Review,* 100 (3), 641-72, DOI: 10.1257/aer.100.3.641.

Pennycook, G., Epstein, Z., Mosleh, M., Arechar A. A., Eckles, D., and Rand, D. G. (2021), "Shifting attention to accuracy can reduce misinformation online", *Nature*, 592, 590-595, DOI: 10.1038/s41586-021-03344-2, EDN: VQQDWP.

Perrow, C. (1999), *Normal Accidents: Living with High-Risk Technologies,* Princeton University Press, Princeton.

Renn, O. and Walker, K. (2010), *Global Risk Governance: Concept and Practice Using the IRGC Framework*, Springer Netherlands, Dordrecht.

Reeves, M. (2013), "Clean Fake: Authenticating Documents and Persons in Migrant Moscow", *American Ethnologist*, 40, DOI: 10.1111/amet.12036.

Rinaldi, S. M., Peerenboom, J. P. and Kelly, T. K. (2001), "Identifying, understanding, and analyzing critical infrastructure interdependencies", *IEEE Control Systems*, 21(6), DOI: 10.1109/37.969131.

Roozenbeek, J., van der Linden, S. and Nygren, Th. (2020), "Prebunking interventions based on the psychological theory of "inoculation" can reduce susceptibility to misinformation across cultures", *HKS Misinfo Rev*, 1, DOI: 10.37016/mr-2020-008, EDN: QESJPI.

Rosa, H. (2013), *Social Acceleration: A New Theory of Modernity*, Columbia University Press, New York.

Streletskiy, D. A., Suter, L. J., Shiklomanov, N. I. [et al.] (2019), "Assessment of climate change impacts on buildings, structures and infrastructure in the Russian regions on permafrost", *Environmental Research Letters*, 14 (2), 025003, DOI: 10.1088/1748-9326/aaf5e6, EDN: AHATIK.

Stukal, D., Sanovich, S., Bonneau, R. and Tucker, J. (2017), "Detecting Bots on Russian Political Twitter", *Big Data*, 5, 310-324, DOI: 10.1089/big.2017.0038.

Zhelnina, A. (2020), "The apathy syndrome: How we are trained not to care about politics", *Social Problems*, 67 (2), 358-378, DOI: 10.1093/SOCPRO/SPZ019, EDN: SRIGCY.

Статья поступила в редакцию 12 июня 2026 г. Поступила после доработки 18 августа 2026 г. Принята к печати 10 сентября 2026 г.
Received 12 June 2026. Revised 18 August 2026. Accepted 10 September 2026.

Конфликты интересов: у автора нет конфликта интересов для декларации.
Conflicts of Interest: the author has no conflict of interest to declare.

Гайдукова Галина Николаевна, кандидат социологических наук, доцент доцент кафедры менеджмента Факультета экономики и финансов Северо-Западного института управления – филиала Российской академии народного хозяйства и государственной службы при Президенте РФ г. Санкт-Петербург, Россия.
Galina N. Gaidukova, Candidate of Sociological Sciences, Associate Professor, Associate Professor of the Department of Management, Faculty of Economics and Finance, North-West Institute of Management, Branch of the Russian Academy of National Economy and Public Administration under the President of the Russian Federation, St. Petersburg, Russia.