

Научная статья

УДК 338.49, 338.24

JEL R58

DOI 10.25205/2542-0429-2023-23-2-108-125

Риски умного города

Елена Алексеевна Костина

Институт экономики и организации промышленного производства СО РАН,
Новосибирск, Россия

ovs.elena@gmail.com, <https://orcid.org/0000-0002-3103-1382>

Аннотация

Одним из направлений городского развития в настоящий момент является концепция умного города. Применение современных информационно-коммуникационных технологий в городской среде позволяет повысить комфортность жизни, эффективность управления городским пространством, приводит к устойчивому развитию и рациональному потреблению ресурсов. Однако, как и у других подходов, существует ряд рисков, связанных с ускоренным и масштабным внедрением современных технологий и неготовностью общества к их восприятию. Цифровизация не должна быть самоцелью, необходим комплексный подход к решению задач. Данная работа посвящена исследованию рисков, связанных с внедрением на практике положений концепции умного города. Среди рисков были выделены технологические (отсутствие или несовершенство отечественных технологических решений в данной сфере, угрозы кибербезопасности: риски нестабильности системы и утечек данных), экономические (низкая эффективность внедряемых инноваций, рост цифрового неравенства), управленческие (неготовность властей техническая и психологическая, потеря городской аутентичности), институциональные (отставание законодательства от практики применения современных технологий, наличие конфликта интересов между общественными и частными коммерческими интересами), связанные с человеческим капиталом (неготовность населения к использованию технологий, риск технократического подхода к внедрению концепции) и экологические. Несмотря на то что в литературе больше внимания уделено технологическим рискам умного города, также важны прочие риски (экономические, управленческие и т. д.). Данные риски тесно связаны между собой и оказывают существенное влияние на процесс цифровой трансформации городской среды, могут замедлить его или снизить эффективность. Поэтому необходимо учитывать их при планировании внедрения и развития умного города.

Ключевые слова

умный город, цифровизация, риски, кибербезопасность, экономическая эффективность, цифровое неравенство, технологический суверенитет

Источник финансирования

Работа выполнена по плану НИР ИЭОПП СО РАН Проект 5.6.1.5. «Теория и методология исследования устойчивого развития компаний высокотехнологичного и наукоемкого сектора экономики

© Костина Е. А., 2023

в контексте глобальных вызовов внешней среды, технологических, организационных и институциональных сдвигов» № 121040100260-3

Для цитирования

Костина Е. А. Риски умного города // Мир экономики и управления. 2023. Т. 23, № 2. С. 108–125. DOI 10.25205/2542-0429-2023-23-2-108-125

Risks of the Smart City Concept

Elena A. Kostina

Institute of Economics and Industrial Engineering SB RAS
Novosibirsk, Russia

ovs.elena@gmail.com, ORCID: 0000-0002-3103-1382

Abstract

The concept of smart city is one of the most popular directions of urban development nowadays. The use of modern information and communication technologies in the urban environment improves the comfort of life, the efficiency of urban space management, leads to sustainable development and rational consumption of resources. However, like other approaches, there are risks associated with the accelerated and large-scale introduction of modern technologies and the unpreparedness of society to accept them. Digitalization should not be the aim, government should use an integrated approach. This work is devoted to the study of the risks of introducing the concept of a smart city. There are technological risks (absence or imperfection of domestic technological solutions in this area, cybersecurity threats: risks of system instability and data leaks), economic (low efficiency of implemented innovations, growing digital divide), managerial (technical and psychological unpreparedness of the authorities, loss of urban authenticity), institutional (legislation behind the practice of applying modern technologies, the presence of a conflict of interest between public and private commercial interests), related to human capital (unpreparedness of the population to use technology, the risk of a technocratic approach to the implementation of the concept) and environmental risks. Although the literature has given more attention to the technological risks of a smart city, other risks (like economic, managerial, etc.) are also important. These risks are closely related and have a significant impact on the process of digital transformation of the urban environment, which may slow it down or reduce its effectiveness. Therefore, it is necessary to take them into account when planning the implementation and development of a smart city.

Keywords

smart city, digitalization, risks, cybersecurity, economic efficiency, digital divide, technological sovereignty

Funding

The research was carried out according to the plan of research work of IEIE SB RAS, project ‘Theory and methodology of research into sustainable development in the economic sector of high-tech and science-based companies in the context of global external challenges, technological, organizational, and institutional shifts’, No. 121040100260-3.

For citation

Kostina E. A. Risks of Smart City Concept. World of Economics and Management, 2023, vol. 23, no. 1, pp. 108–125. (in Russ.) DOI 10.25205/2542-0429-2023-23-2-108-125

Введение

По прогнозу ООН, к 2050 г. в городах будет проживать более 68 % населения¹. По всему миру идет поиск способов совершенствования городского управления и повышения комфортности городской среды. Активное развитие и внедрение информационно-коммуникационных технологий в городское пространство способствует созданию «умных городов».

Большое количество стран по всему миру активно занимаются как внедрением отдельных проектов, так и масштабным усовершенствованием городов. Так, в Индии с 2015 г. реализуется программа по модернизации и цифровизации 100 городов “100 Smart Cities Mission”. В результате запуска данной программы произошло повышение инвестиционной привлекательности городов и повышение их комфортности. В Китае к концу 2019 г. более 500 городов приступило к реализации проектов умного города, сейчас они находятся на разной степени готовности. Крупные города США также являются активными игроками на рынке умных городов и традиционно входят в рейтинг самых умных городов планеты².

В России в 2018 г. был утвержден ведомственный проект по цифровизации городского хозяйства «Умный город» в рамках национального проекта «Жилье и городская среда» и национальной программы «Цифровая экономика». В российском законодательстве представлено следующее определение: «Умный город – это подход к развитию города, использующего цифровые инструменты для повышения уровня жизни, качества услуг и эффективности управления, при обязательном удовлетворении потребностей настоящего и будущих поколений во всех актуальных аспектах жизни.»³.

Чтобы не отстать в конкурентной борьбе от других городов и более эффективно функционировать, город должен модернизироваться с использованием современных цифровых технологий и ориентироваться на устойчивое долгосрочное развитие. Однако остается вопрос, как не попасть в ловушку цифровизации. Умные города как сложные системы из множества элементов требуют особого подхода, стратегии к управлению и несут собственные, уникальные риски. Риски могут быть связаны с цифровизацией, с отсутствием высококвалифицированных специалистов, с отставанием в данной сфере институциональной среды, со сложностью экономического анализа отдачи от внедрения той или иной технологии и т. д.

Состояние исследований. Выполненный автором библиографический анализ по публикациям, включенным в базу Scopus издательства Elsevier⁴, подтвердил, что тема рисков умного города развивается с определенным лагом, относительно темы умного города. При этом в последние годы наметился устойчивый тренд по росту интереса к данной теме и в общем пуле исследований про умные города доля рисков выросла до 19 % к 2022 г. (рис. 1).

¹ UN, Department of Economic and Social Affairs, 2018. Revision of World Urbanization Prospects // <https://www.un.org/development/desa/publications/2018-revision-of-world-urbanization-prospects.html>

² Smart City Observatory. Smart City Index 2021 // https://www.imd.org/smart-city-observatory/home/#_smartCity

³ Приказ Минстроя России от 25 декабря 2020 г. № 866/пр «Об утверждении Концепции проекта цифровизации городского хозяйства “Умный город”»

⁴ Рассматривались статьи, размещенные на сайте <https://www.sciencedirect.com/>

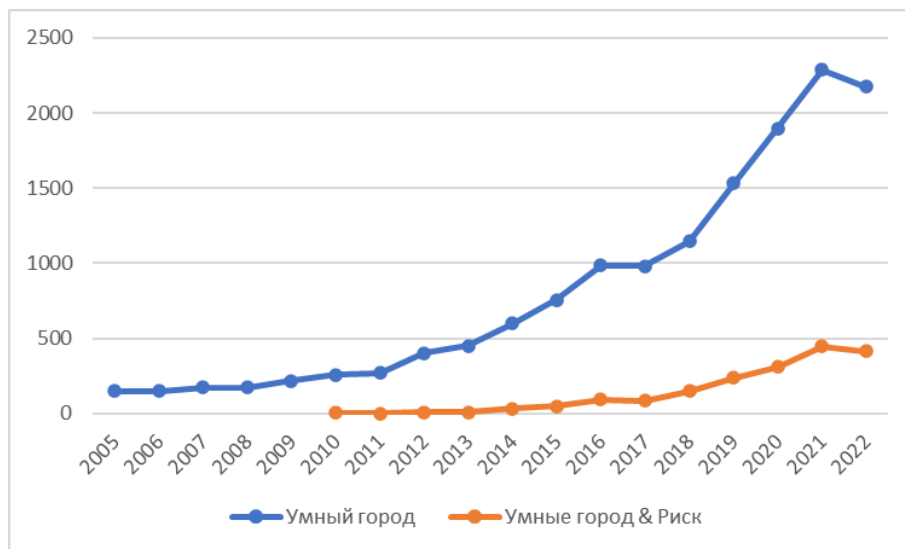


Рис. 1. Статьи по темам «Умный город» и «Умный город & Риск»
Fig. 1. Articles on the topics “Smart City” and “Smart City & Risk”

Исследование ключевых слов показывает, что большинство исследований сосредоточено на рисках применения определенных технологий – ГИС, большие данные, искусственный интеллект и т. д., мало исследований, связанных с социально-экономическими и управленческими рисками.

Ряд авторов провел систематический анализ рисков, возникающих в умном городе. Предлагаются различные типологии рисков, которые зависят от позиций авторов. Fahim Ullah с соавт. выделили три категории рисков – риски, связанные с технологиями (например, IoT, блокчейн, общедоступный Интернет), организацией (например, управлением облачными технологиями) и внешней средой (прочие) [1]. Другой коллектив исследователей [2] в своей обзорной работе выделяют риски, которые имеют технический и нетехнический характеры. Автор [3] констатирует, что большинство исследователей сосредоточивает свое внимание на технологических рисках, упуская из рассмотрения организационные, возможно из-за сложности их определения и анализа, а также наличия психологической составляющей. Однако риски, связанные с организацией и управлением, не менее важны, а некоторые авторы даже считают их более существенными [4].

Существует пул исследований, посвященных рискам цифровизации по отдельным видам технологий. Например, авторами [5] отмечены риски энергетических систем; [6] определили пять видов уязвимостей IoT в умных городах; [7] изучают проблемы и возможности технологии блокчейна, чтобы проиллюстрировать применение технологии блокчейна в масштабах умного города и связанные с этой технологией риски и т. д. Наиболее часто выделяемыми проблемами, возникающими в умном городе, являются обеспечение кибербезопасности и конфиденциальности данных [2, 8, 9], но круг проблем существенно шире.

Таким образом, несмотря на наличие исследований по рискам умного города, данная тема является актуальной и требует дальнейшего изучения. Цель данной работы – обобщение и систематизация рисков реализации концепции умного города с учетом практического опыта внедрения данной концепции и обобщения ряда существующих работ отечественных и мировых исследователей. Автором выделены технологические, экономические, управленческие, институциональные, экологические и риски, связанные с человеческим капиталом (рис. 2).



Рис. 2. Схема рисков, предлагаемая автором
Fig. 2. Risk Diagram

К технологическим рискам были отнесены риски, связанные с зависимостью от иностранных технологических решений и несовершенством либо отсутствием существующих отечественных решений, с угрозой кибербезопасности функционирования системы, отдельно выделяется проблема устойчивости системы и проблема утечки данных; к экономическим отнесены низкая эффективность внедряемых инноваций, рост цифрового неравенства; к управленческим – неготовность властей к использованию технологий умного города, потеря городской аутентичности; к институциональным – отставание законодательства, конфликт интересов бизнеса и государства, связанный со сосредоточением больших данных у коммерческих компаний; к рискам, связанным с человеческим капиталом – неготовность населения к использованию технологий, риск технократического подхода к внедрению концепции; и экологические риски. Данный список не полный и включает лишь наиболее актуальные, на взгляд автора, риски. К рассмотрению

не принимались чисто технические риски, связанные с применением отдельных технологий. Также следует учитывать, что приведенные риски характерны в большей степени для уже существующих городов, которые проходят цифровую трансформацию, а не для умных городов с «нуля», таких как Сонгдо (Южная Корея), Масдар (ОАЭ), Иннополис (Россия) и пр. Для городов с «нуля», как показывает практика, главным риском является непривлекательность для населения в качестве постоянного места проживания из-за отсутствия работы, мест для комфортного общения, культурных мероприятий, исторической привлекательности и т. д.

Технологические риски:

1. Зависимость от иностранных технологических решений.

Данная проблема стала особенно актуальна в 2022 г., когда введение новых международных санкций привело к существенному сокращению рынка высоких технологий в России и уходу крупных технологических компаний. Количество технологических санкций выросло со 128 в 2021 г. до 1914 только в I квартале 2022 г. [10]. Существенно выросли риски использования иностранных технологических решений и сузились возможности доступа к ним, а также к необходимым электронным компонентам. Это привело к пониманию необходимости обеспечения технологического суверенитета.

С учетом высокого уровня цифровизации государственных услуг (Россия входит в число стран-лидеров по цифровой трансформации правительства и цифровизации государственных услуг по результатам международного рейтинга GovTech Maturity Index, рассчитанного Всемирным банком)⁵ и успешного внедрения систем умного города по всей территории страны, важно не оказаться в заложниках в сложившейся ситуации и не остаться без критически важного оборудования и программного обеспечения. Даже при наличии всех прав на программное обеспечение или лицензий на товар можно остаться без технической поддержки или обслуживания.

Также преодоление санкционного давления приводит к дополнительным затратам и замедляет инновационную активность, что является важной составляющей умного города. Использование программного обеспечения с открытым кодом, что могло существенно экономить издержки (например, открытой платформой для моделирования городов (OPUS) по моделированию городского пространства на основе модели UrbanSim, которой пользуются некоторые города Европы, Америки и Африки и чье финансирование осуществляется за счет нескольких грантов, в том числе Национального научного фонда США, Агентства по охране окружающей среды США, Федерального управления автомобильных дорог США, сейчас является слишком рискованным, так как информация будет известна широкому кругу лиц. Помимо этого, санкции привели к оттоку высококвалифицированных специалистов, в том числе в сфере IT, что снижает как возможности создания технологичных продуктов и услуг, так и снижает человеческий капитал в умных городах и, как следствие, спрос на умные технологии в городской среде.

⁵ World Bank. GovTech Maturity Index, 2022 Update : Trends in Public Sector Digital Transformation, <https://openknowledge.worldbank.org/handle/10986/38499>

Автор [10] предлагает различные решения по нивелированию негативного воздействия санкций, например, развитие сотрудничества с КНР, привлечение кадров из дружественных стран, легализацию параллельного импорта, введение контрсанкций в сфере сырьевых поставок для высокотехнологичных отраслей, стимулирование кооперации науки и МСП-бизнеса. Все чаще в исследованиях звучит необходимость проводить целенаправленную стратегическую политику по созданию технологического суверенитета, в том числе путем наращивания человеческого капитала в данной сфере [11]. И хотя принимаются серьезные усилия в данном направлении, в частности создана Межведомственная комиссия СБ РФ по вопросам обеспечения технологического суверенитета в сфере IT-инфраструктуры⁶, предстоит еще много работы.

Кроме того, можно разделить технологии умного города на категории в зависимости от важности, «некритически важные» (например, технологии умного дома) можно приобретать у дружественных стран, достигнув таким образом не абсолютного, а «достаточного» технологического суверенитета. В то же время, например, интеллектуальная транспортная система должна быть полностью создана на отечественном оборудовании и программном обеспечении.

При этом есть и успешные примеры импортозамещения, когда российские компании имели трудности с выводом продукции на рынок, а санкционные ограничения открыли им возможности для занятия ниши на рынке, например, компания «СРТ», разработавшая протокол радиосвязи, «Элтекс», разработчик и производитель телекоммуникационного оборудования, в том числе для умного дома.

2. Угроза кибербезопасности – риски нестабильности системы.

Умные города – это сложная система, состоящая из нескольких уровней цифровых систем от датчиков и сенсоров на нижних уровнях до работы с большими данными и искусственным интеллектом, и объединяющая различные инфраструктурные системы, такие как энергетика, здравоохранение, транспорт, водоснабжение, очистка сточных вод и т. д. Все эти системы используют современные высокотехнологичные решения для повышения эффективности, устойчивости и удобства. Однако это же представляет и слабость умного города, так как блокировка систем управления в результате хакерской атаки, вируса, системной ошибки может напрямую повлиять на безопасность города. А поскольку многие системы связаны между собой, то падение одного элемента может вызвать каскадную реакцию, которая может привести к сбою во всей городской инфраструктуре и системах связи. Эксперты по кибербезопасности сочли внештатные ситуации в области аварийного оповещения, уличного видеонаблюдения и интеллектуальных светофоров наиболее рискованными в умном городе [12].

Развитие кибербезопасности не поспевает за стремительным внедрением технологий в умные города [13]. При этом отмечается рост риска кибератак [10]; в РФ в 2022 г. отражено более 50 тыс. кибератак, по словам главы Минцифры Максута Шадаева.

⁶ Указ Президента Российской Федерации от 14.04.2022 № 203 «О Межведомственной комиссии Совета Безопасности Российской Федерации по вопросам обеспечения технологического суверенитета государства в сфере развития критической информационной инфраструктуры Российской Федерации» <http://publication.pravo.gov.ru/Document/View/0001202204140035>

Авторы [14] считают, что главное слабое звено для умных городов – это безопасность и достоверность данных. Умный город работает на основе больших данных, но кибератака может изменить или уничтожить ряд данных, недействительные отчеты приведут к неверному управлению системами, авариям. Другой проблемой является недостаточность тестирования применяемых технологий на кибербезопасность [15].

Представим несколько исторических примеров. В 2021 г. во Флориде, США, в результате кибератаки постороннее лицо смогло изменить концентрацию химических веществ в местной системе водоснабжения. В 2017 г. программа-вымогатель NotPetya распространилась по всему миру и затронула сектор транспорта и логистики. В 2018 г. в городе Ноксвилл, штат Теннесси, а также в ряде других городов США, муниципальные сети были атакованы вирусами-вымогателями. В 2020 г. Chrysler отозвал около 1,4 млн своих автомобилей, поскольку была обнаружена уязвимость интеллектуальной системы управления – автомобили можно было взломать удаленно через Интернет, в том числе можно было глушить двигатель и отключать тормоза.

Основными направлениями решения проблемы кибербезопасности является прежде всего осознание необходимости работы в данном направлении, регулярные обновления протоколов безопасности, наличие соответствующих компетенций у госслужащих. В США, например, в Массачусетском технологическом институте, есть специальные программы по подготовке специалистов в области кибербезопасности, включая и технологии умного города. Подобные программы есть и в РФ, например, в НГТУ есть несколько программ обучения по данному направлению, например, «Безопасность значимых объектов критической информационной инфраструктуры». Также важным направлением является создание стандартов, авторы [4] нашли 93 стандарта, относящихся к умному городу, из них 13 по кибербезопасности. Однако исследования [4, 16] показали, что большинство рассмотренных ими городов пренебрегают мерами безопасности и внедрением стандартов.

3. Угроза кибербезопасности – утечки данных.

Другой угрозой кибербезопасности является возможные утечки данных. Умный город генерирует большие данные и на их основе принимает более взвешенные и оперативные решения. Однако повсеместное внедрение цифровых технологий чревато возможными утечками данных, в том числе личных. Разные устройства имеют разную степень защиты, особенно под угрозой мобильные смарт-устройства с IoT [17], при низкой степени защиты возможна слежка за людьми, перехват конфиденциальной и личной информации. Как для web-сайтов было введено согласие на файлы cookie (как часть Директивы об электронной конфиденциальности), так и для устройств в области IoT необходим подобный документ.

Помимо прочего, возможность утечки данных снижает открытость жителей к умному городу. Исследователи отмечают разное отношение в зависимости от типа данных и цели их сбора: они в большей степени готовы делиться обезличенной информацией, предназначенной для решения конкретных городских проблем [18]. Важно информировать жителей о целях сбора информации и предпринимаемых мерах защиты.

Далеко не всегда сбор всех доступных данных с датчиков является правильной стратегией. Чтобы не было утечек информации и не надо было беспокоиться о конфиденциальности, порой стоит пойти на минимизацию данных – собирать только необходимые, а не весь возможный массив информации. Например, при подсчете трафика удалять изображения, оставляя только число проехавших машин. Тогда не будет проблем с возможным взломом или рассекречиванием информации, отслеживания перемещений конкретных лиц. Помимо прочего, это существенно сократит затраты на обработку и хранение информации.

Наличие открытых данных является важной частью умного города. При этом все больше городов приходит к открытым базам данных с обезличенной информацией, собираемой с датчиков и камер умного города и из административных источников. Аналоги есть, например, в Барселоне, Чикаго, Ньюкасле, где на ГИС-платформе можно видеть состояние города онлайн, а также есть массив постоянно обновляемых данных. Данные связаны с состоянием окружающей среды, транспорта, новых событий, парковки и т. д. Кроме того, общественность таким образом проинформирована о количестве и месте расположении камер и датчиках, а также о цели их установки.

В Барселоне и Амстердаме запущен проект DECODE – жители городов имеют возможность отслеживать свои личные данные в открытом доступе, удалять их при желании, а также активно участвовать в городском управлении и получать услуги.

Ключевым моментом в уменьшении риска утечки данных является работа над системами кибербезопасности умного города, а также строительство доверительных прозрачных отношений, чтобы население было уверено в конфиденциальности личной информации, что предоставленные данные никуда не исчезнут и не попадут не в те руки. При этом так как широкое распространение эти технологии получили совсем недавно, еще не выработаны механизмы в области безопасности и защиты конфиденциальности.

Экономические риски:

1. Низкая эффективность внедряемых инноваций.

В отношении городских технологий определить экономическую эффективность сложно. Их внедрение должно повышать общественное благосостояние, устойчивость функционирования городской инфраструктуры и улучшить качество жизни горожан, что трудно оценить в денежном эквиваленте. Крупные инфраструктурные проекты сопряжены с высокими первоначальными затратами, значительными технологическими рисками и долгосрочным горизонтом окупаемости, что также затрудняет привлечение инвестиций [19]. Например, в Новосибирске пытались провести конкурс на концессионное соглашение по умным остановкам, что позволило бы обновить, привести к единообразию остановки общественного транспорта в городе. Однако затем конкурс отменили, в том числе из-за сомнительной эффективности и ненужного удорожания: «умный» блок на одну остановку стоит дополнительные 500 тыс. руб., что при переоборудовании 250 остановок существенно увеличивает стоимость проекта. Кроме того, оборудование таких остановок камерами и передача данных с камер в местный центр обработки данных МВД могло существенно повысить безопасность в городе, однако пока этого

нет в заявленных требованиях к остановкам. Наконец, как показывает опыт уже существующих теплых остановок, они становятся местами притяжения и проживания лиц без определенного места жительства. Важным является и вопрос альтернативной стоимости – за цену одной умной остановки можно установить несколько новых обычных остановок, что чрезвычайно важно в условиях ограниченного бюджета.

Сюда же можно отнести и проблему неоднородности инфраструктуры – города создавались в течение длительного периода времени и инфраструктура «унаследована» от предыдущих технологических укладов, поэтому внедрение новых технологий в нее может быть затруднено, экономически неэффективно. Вопрос это не только технический, но и организационный.

2. Усиление цифрового неравенства.

Отдельные ученые акцентируют внимание на то, что современные технологии могут усиливать цифровое неравенство из-за отсутствия у наиболее незащищенных групп населения доступа к компьютеру, Интернету, возможности улучшить свою компьютерную грамотность.

Для проверки гипотезы о наличии цифрового неравенства автором данной статьи были проведены расчеты на примере города Новосибирска. Результаты подтвердили гипотезу о цифровом неравенстве, что выразилось в лучшем доступе к городскому portalу у более обеспеченного населения [20].

Другой парадоксальной мыслью является то, что городские порталы, где можно поделиться своей проблемой, снижают гражданскую активность – власти решают текущую проблему обратившегося гражданина, не решая при этом проблемы в целом, но дальше действовать данный конкретный человек уже не будет.

Управленческие риски:

1. Неготовность властей: техническая и психологическая.

Исследователи перечисляют ряд проблем, с которыми можно столкнуться при внедрении технологий умного города: отсутствие интеграции и совместимости между государственными системами, отсутствие стандартизации [21], отсутствие поддерживающей инфраструктуры, недоступность универсальных стандартов и т. д. [22]. Все это осложняет создание и внедрение единой системы управления умным городом и повышает требования к квалификации сотрудников муниципалитета и разработчиков оборудования и программного обеспечения. Сложность заключается и в междисциплинарности проектов. При этом в России успешно преодолевают данный барьер, на правительственном уровне созданы разные организации, например, АНО «Цифровая трансформация», работа проводится в министерствах и на местном уровне. В Новосибирской области есть 2 министерства, занимающихся цифровизацией.

Помимо этого, как и население, местные власти могут считать построение умного города менее приоритетным и важным, чем решение насущных проблем, хотя создание умного города как раз может способствовать быстрому обнаружению проблем и даст возможность превентивно реагировать. Исследователь [23] подчеркивает нежелание властей делиться своими полномочиями, когда речь заходит о привлечении населения к управлению городом, хотя современные тех-

нологии позволяют устраивать опрос широких масс населения, принимать их мнение во внимание. Кроме того, разные показатели эффективности для разных уровней власти – это как повышение качества жизни граждан, так и чисто номинальные показатели, и в зависимости от них и выстраиваются приоритеты работы.

2. Потеря городской аутентичности.

Набор готовых решений легче внедрить, проще состыковать получаемые большие данные, легче контролировать на федеральном уровне. Но такая унификация несет в себе и плюсы и минусы. Потребности города существенно отличаются в зависимости от размера, климата, структуры экономики и многого другого. Таким образом, внедрение стандарта с точки зрения эффективности и затрат будет существенно отличаться от города к городу.

Кроме того, как указывают отдельные исследователи-урбанисты, целью городских властей должно быть позиционирование своего города в международной конкуренции городов за счет усиления сильных сторон города и специализации [24]. Автор [25] критикует растущую между городами конкуренцию за специалистов, компании и туристов за счет вытеснения местных сообществ.

В качестве примера можно привести администрацию города Санкт-Петербурга, которая ведет грамотную политику по сохранению культурного наследия, признавая его одним «из главных оснований для национального самоуважения и признания мировым сообществом».⁷ Историческая застройка Петербурга является его визитной карточкой, а современные урбанистические решения гармонично вписываются в существующий исторический ландшафт.

Другим примером является создание уникального исторического образа в г. Рыбинске. Там власти обязали размещать вывески в историческом центре только в «дореволюционном» стиле⁸. И даже курьеры сервиса доставки еды носят специальную ретро-форму, включающую шинель и фуражку. Такая политика муниципальных властей привела к росту туристического потока в город.

Институциональные риски:

1. Отставание законодательства.

Правовому регулированию требуется время, чтобы догнать инновации, законодательно оформить применение новых технологий. Наиболее ярко данную проблему можно проиллюстрировать на примере беспилотных автомобилей. В 2021 г. в Москве разрешили тестирование беспилотных автомобилей в очерченной зоне, а на 19 улицах беспилотные такси имеют право перевозить людей и багаж. При этом правовое регулирование высокоавтоматизированных транспортных средств (ВАТС) находится на начальном уровне. Пока представлен только проект закона «О высокоавтоматизированных транспортных средствах», ожидается что он вступит в силу только в 2025 г. В настоящее время идет эксперимент по опытной эксплуатации ВАТС на дорогах общего пользования, регулируемый Постановлением Правительства РФ № 1415 от 26.11.2018. В случае

⁷ Петербургская стратегия сохранения культурного наследия (постановление Правительства Санкт-Петербурга от 01.11.2005 № 1681). https://www.gov.spb.ru/gov/otrasl/c_govcontrol/peterburgskaya-strategiya-sohraneniya-kulturnogo-naslediya/

⁸ Градостроительство и архитектура г. Рыбинска <http://rybinsk.ru/gradostro>

дорожно-транспортного происшествия ущерб должен возмещать владелец средства, а если это связано с конструкторскими недостатками, то владелец может переадресовать претензии производителю. Однако такая система не совершенна, может привести к большому числу правовых коллизий и требует совершенствования. Авторы [7, 26] отмечают также отставание правовой системы в сфере проблем безопасности и конфиденциальности при использовании технологий.

2. Наличие конфликта интересов между общественными и частными коммерческими интересами.

Умный город в настоящее время – быстроразвивающийся рынок с большими возможностями, инвестиции в технологии умного города достигнут 327 млрд долл. к 2025 г. (по сравнению с 96 млрд долл. в 2019 г.), согласно исследованию, проведенному консалтинговой фирмой Frost & Sullivan. Критика начальной технокентричной постановки концепции умного города была в том числе связана с ростом власти корпораций и технических гигантов, которые активно продвигали создание умного города, преследуя при этом свои цели. Автор [27] указывает, что когда частные компании предоставляют общественные услуги, то зачастую наблюдается пренебрежение общественными и гражданскими потребностями, декларируется прибыль превыше всего. Автор [4] также подчеркивает наличие конфликта интересов между городскими властями, жителями и коммерческими партнерами в умном городе. Последние в первую очередь заинтересованы в получении прибыли, необходим контроль, чтобы компании не концентрировали свои усилия только на обеспеченных районах (например, при предоставлении услуг кикшеринга).

При этом после масштабной критики и перехода к «умному городу 2.0», где во главу угла ставятся интересы жителей и идет ориентация на их потребности, данная проблема стала менее острой.

Риски, связанные с человеческим капиталом:

1. Неготовность населения к использованию технологий.

Важным моментом, активно обсуждаемым в литературе, является восприятие населением и властями новых технологий. Технологии существуют не в вакууме, их применение предполагает определенный уровень знаний, наличие навыков и инструментов.

В России 73,6 % городских домашних хозяйств в 2019 г. обладали персональным компьютером, 77,7 % имели доступ к сети Интернет. При этом доля респондентов, которые указывают причиной неиспользования сети Интернет в домашних хозяйствах «недостаток навыков для работы в сети Интернет» составляет 32,5 %, также среди популярных причин – «высокие затраты подключения» (20,8 %) и «отсутствие технических возможностей подключения» (7,3 %).⁹ Соответственно, для части населения покрытие всей территории города сетью 5G или бесплатный Wi-Fi попросту неактуальны. Авторы [4] подчеркивают отноше-

⁹ Информационное общество в Российской Федерации. 2020: статистический сборник [Электронный ресурс] / Федеральная служба государственной статистики; Нац. исслед. ун-т «Высшая школа экономики». Электрон. текст дан. (33,6 Мб). М.: НИУ ВШЭ, 2020. // <https://rosstat.gov.ru/storage/mediabank/lqv3T0Rk/info-ob2020.pdf>

ние местных жителей к данной проблеме, которые считают, что, потратив средства и время, местные власти не успевают решить более насущные проблемы. Авторы [28] подчеркивают, что многие жители воспринимают высокотехнологичные решения как абстракцию, а не ближайшее будущее. Нужен некоторый временной лаг, чтобы население восприняло и привыкло к прорывным технологиям, чтобы технология вошла в привычку.

Чтобы упростить принятие технологий, во многих городах идет повышение осведомленности жителей о новых городских технологиях и повышается компьютерная грамотность населения. В некоторых городах, в том числе и в РФ, данную проблему учитывали и организовывали, например, бесплатные компьютерные курсы. В Барселоне при внедрении проекта создания умного округа «22@» проводили специальные бесплатные курсы, чтобы научить население пользоваться всеми внедряемыми технологиями.

Таким образом, одним из возможных решений снижения сопротивления со стороны общественности является работа с населением, информирование об инициативах и анализ обратной связи. При этом жители должны видеть, что их мнение важно и оно учитывается, например, при проведении открытых слушаний или голосования за городские проекты. Бывают и негативные примеры, например голосование за талисман для «Новогодней столицы России» в 2022 г., где в результате протестного голосования побеждал орангутан и власти просто закрыли голосование досрочно.

2. Риск технократического подхода к внедрению инноваций.

Технологии играют важную роль в процессе создания городов будущего, однако необходимо помнить об устойчивом, комфортном для жизни, экологичном, низкоуглеродном развитии города при планировании его развития. Цифровизация и внедрение современных технологий не должно быть самоцелью. Уверенность в современных технологиях может завести в ловушку, когда все возникшие проблемы решаются исключительно техническим способом, забывая о творческой, этической и прочих сторонах. Уже есть критика в излишней технократичности проводимой в России политики умных городов [29] либо отдельных применяемых технологий [30].

Экологические риски

Хотя технологии решают многие проблемы, их высокая скорость развития приводит к экологическим проблемам. На цифровой сектор сейчас все большая доля потребления электроэнергии, например, только на ЦОД в Дании к 2030 г. будет приходиться более 15 % потребления электроэнергии¹⁰, а на сектор банковских услуг тратится больше электроэнергии, чем на сектор золотодобывающей промышленности¹¹. Годовой мировой объем e-waste в 2021 г. составил около

¹⁰ Data centers will increase Denmark's carbon footprint <https://www.datacenterdynamics.com/en/news/data-centers-will-increase-denmarks-carbon-footprint/>

¹¹ Банковская система потребляет в два раза больше энергии, чем Биткоин. Исследование компании Galaxy Digital <https://vc.ru/crypto/247069-bankovskaya-sistema-potrebyaet-v-dva-raza-bolshe-energii-chem-bitcoin-issledovanie-kompanii-galaxy-digital>

57 миллионов метрических тонн. Электронные отходы составляют только 2 % потоков твердых отходов, однако они представляют собой около 70 % опасных отходов, которые попадают на свалку¹².

Короткие циклы технологических инноваций также приводят к образованию большого количества электронных отходов, создавая проблемы устойчивого развития. Например, быстрый рост блокчейн-технологий первоначально привел к росту потребления электроэнергии для проведения, по сути, бессмысленных расчетов. Затем, когда майнить стало экономически невыгодно, образовался излишек видеокарт, что усугубило проблемы с электронным мусором.

Кроме того, некоторые современные технологии оказываются не такими «зелеными», как ожидалось. Тут можно вспомнить сложности с утилизацией солнечных батарей и лопастей ветряных мельниц.

Заключение

Город – это сложная экосистема, поэтому найти универсальное решение пути его развития невозможно. В городе переплетаются интересы различных сторон, наблюдается высокая зависимость между сторонами и сложность взаимосвязи. Необходимо помнить об уникальности каждого города и подстраиваться под нужды и характеристики каждого города. Цифровизация городского хозяйства является необходимым шагом, однако для улучшения городского пространства нужно не просто внедрение новейших технологий, а комплексная работа в разных сферах с учетом ограниченности ресурсов. Существует ряд рисков при реализации концепции умного города, они делают города более уязвимыми и затрудняют внедрение концепции умного города. В данной работе на основе обобщения исследовательских работ и практики создания умных городов в мире выделены и типологизированы риски умного города.

В настоящее время вопросы, связанные с технологическим суверенитетом и кибербезопасностью умного города в России, стоят крайне остро. Угрозы могут быть связаны как с целенаправленными атаками, так и случайным отказом оборудования или сбоям программного обеспечения. Это может привести к проблемам с водоснабжением, энергоснабжением, сбоях в работе экстренных служб и т. д., при большом масштабе проблем может быть каскадное обрушение системы. Кроме того, политика умного города создает риски для конфиденциальности жителей в умном городе из-за работы с большими данными. Помимо этого, в статье приведены другие риски, в том числе управленческие, институциональные и прочие – эти риски менее изучены, однако также важны. Приведенные риски тесно переплетаются друг с другом и усиливают друг друга, поэтому требуются системные решения для устранения данных рисков. Это позволит сделать город более комфортным, удобным и привлекательным для жизни.

Осознание указанных в данной статье сложностей может быть полезным для властей при формировании стратегии создания умных городов, как на федеральном, так и на муниципальном уровне. Типология рисков поможет сформулировать более комплексную и долгосрочную стратегию умного города.

¹² Экологический пресс-центр. <http://ecopress.center/page4843325.html>

Список литературы

1. **Ullah F.** et al. Risk management in sustainable smart cities governance: A TOE framework // *Technological Forecasting and Social Change*. 2021. T. 167. C. 120743.
2. **Al Sharif R., Pokharel S.** Smart city dimensions and associated risks: Review of literature // *Sustainable Cities and Society*. 2022. T. 77. C. 103542.
3. **Ahad M. A. et al.** Enabling technologies and sustainable smart cities // *Sustainable cities and society*. 2020. T. 61. C. 102301.
4. **Mondschein J., Clark-Ginsberg A., Kuehn A.** Smart cities as large technological systems: Overcoming organizational challenges in smart cities through collective action // *Sustainable Cities and Society*. 2021. T. 67. C. 102730.
5. **O'Dwyer E.** et al. Smart energy systems for sustainable smart cities: Current developments, trends and future directions // *Applied energy*. 2019. T. 237. C. 581–597.
6. **Kitchin R., Dodge M.** The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention // *Journal of urban technology*. 2019. T. 26. №. 2. C. 47–65.
7. **Xie J.** et al. A survey of blockchain technology applied to smart cities: Research issues and challenges // *IEEE communications surveys & tutorials*. 2019. T. 21. №. 3. C. 2794–2830.
8. **Vitunskaitė M.** et al. Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership // *Computers & Security*. 2019. T. 83. C. 313–331.
9. **Li Z.** et al. Assessing and mitigating cybersecurity risks of traffic light systems in smart cities // *IET Cyber-Physical Systems: Theory & Applications*. 2016. T. 1. №. 1. C. 60–69.
10. **Шкодинский С. В., Кушнир А. М., Продченко И. А.** Влияние санкций на технологический суверенитет России // *Проблемы рыночной экономики*. 2022. №. 2. C. 75–96.
11. **Ештокин С. В.** Сквозные технологии цифровой экономики как фактор формирования технологического суверенитета страны // *Вопросы инновационной экономики*. Учредители: ООО «Триумф-Регион». 2022. T. 12. №. 3. C. 1301–1314.
12. **Frick K. T.** et al. The cybersecurity risks of smart city technologies: What do the experts think? // *white paper, CLTC White Paper Series*. – UC Berkeley, 2021.
13. **Chen D., Wawrzynski P., Lv Z.** Cyber security in smart cities: a review of deep learning-based applications and case studies // *Sustainable Cities and Society*. 2021. T. 66. C. 102655.
14. **Li W., Song H., Zeng F.** Policy-based secure and trustworthy sensing for internet of things in smart cities // *IEEE Internet of Things Journal*. 2017. T. 5. №. 2. C. 716–723.
15. **Al Dairi A.** et al. Cyber security attacks on smart cities and associated mobile technologies // *Procedia Computer Science*. 2017. T. 109. C. 1086–1091.
16. **Angelidou M.** Four European smart city strategies // *Int'l J. Soc. Sci. Stud*. 2016. T. 4. C. 18.

17. **Lv Z.** et al. AI-empowered IoT security for smart cities // *ACM Transactions on Internet Technology*. 2021. Т. 21. №. 4. С. 1–21.
18. **Van Zoonen L.** Privacy concerns in smart cities // *Government Information Quarterly*. 2016. Т. 33. №. 3. С. 472–480.
19. **Rivada A.** et al. Report on Non-technical Barriers and Legal and Normative Issues (No. D1. 13) // Valladolid, Spain: Fundación CARTTF. 2016.
20. **Костина Е. А., Костин А. В.** Барьеры использования сервисов обратной связи на муниципальном уровне // *Журнал Сибирского федерального университета. Гуманитарные науки*. 2023. Т. 16. №. 3. С. 468–480.
21. **Perera C.** et al. Sensing as a service model for smart cities supported by internet of things // *Transactions on emerging telecommunications technologies*. 2014. Т. 25. №. 1. С. 81–93.
22. **Sovacool B. K., Del Rio D. D. F.** Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies // *Renewable and sustainable energy reviews*. 2020. Т. 120. С. 109663.
23. **Пироцкая А. В.** Концепция «умного города» в представлении экспертов и жителей: проблемы и противоречия в реализации концепции // *Мир экономики и управления*. 2020. Т. 20. №. 2. С. 178–196.
24. **Van der Heiden N.** Urban foreign policy and domestic dilemmas: insights from Swiss and EU city-regions. ECPR Press. 2010.
25. **Hollands R. G.** Critical interventions into the corporate smart city // *Cambridge journal of regions, economy and society*. 2015. Т. 8. №. 1. С. 61–77.
26. **Hamilton E.** The Benefits and Risks of Policymakers' Use of Smart City Technology // *Mercatus Center Paper*. 2016.
27. **Hollands R. G.** Will the real smart city please stand up? Intelligent, progressive or entrepreneurial? // *city*. 2008. Т. 12. №. 3. С. 303–320.
28. **Воробьева О. В., Манжула Е. А., Яшина А. В.** Умный горожанин в умном городе: обзор подходов в России и за рубежом // *International Journal of Open Information Technologies*. 2019. Т. 7. №. 5. С. 59–65.
29. **Ли Ш.** Проблемные аспекты формирования в России «умных городов» // *Journal of Economic Regulation (Вопросы регулирования экономики)*. 2019. Т. 10. №. 2. С. 113–120.
30. **Степнов И. М., Ковальчук Ю. А.** Экономические ловушки внедрения искусственного интеллекта // *Экономика. Налоги. Право*. 2020. Т. 13. №. 2. С. 92–102.

References

1. **Ullah F. et al.** Risk management in sustainable smart cities governance: A TOE framework // *Technological Forecasting and Social Change*. 2021. Vol. 167. P. 120743.
2. **Al Sharif R., Pokharel S.** Smart city dimensions and associated risks: Review of literature // *Sustainable Cities and Society*. 2022. Vol. 77. P. 103542.
3. **Ahad M. A. et al.** Enabling technologies and sustainable smart cities // *Sustainable cities and society*. 2020. Vol. 61. P. 102301.

4. **Mondschein J., Clark-Ginsberg A., Kuehn A.** Smart cities as large technological systems: Overcoming organizational challenges in smart cities through collective action // *Sustainable Cities and Society*. 2021. Vol. 67. P. 102730.
5. **O'Dwyer E. et al.** Smart energy systems for sustainable smart cities: Current developments, trends and future directions // *Applied energy*. 2019. Vol. 237. P. 581–597.
6. **Kitchin R., Dodge M.** The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention // *Journal of urban technology*. 2019. Vol. 26. No. 2. P. 47–65.
7. **Xie J. et al.** A survey of blockchain technology applied to smart cities: Research issues and challenges // *IEEE communications surveys & tutorials*. 2019. Vol. 21. No. 3. P. 2794–2830.
8. **Vitunskaitė M. et al.** Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership // *Computers & Security*. 2019. Vol. 83. P. 313–331.
9. **Li Z. et al.** Assessing and mitigating cybersecurity risks of traffic light systems in smart cities // *IET Cyber-Physical Systems: Theory & Applications*. 2016. Vol. 1. No. 1. P. 60–69.
10. **Shkodinsky S. V., Kushnir A. M., Prodchenko I. A.** Influence of sanctions on the technological sovereignty of Russia // *Problemy rynochnoj ekonomiki*. 2022. No.2. P. 75–96.
11. **Eshtokin S. V.** End-to-end technologies of the digital economy as a factor in the formation of the country's technological sovereignty // *Voprosy innovacionnoj ekonomiki* 2022. T. 12. No. 3. P. 1301–1314.
12. **Frick K. T. et al.** The cybersecurity risks of smart city technologies: What do the experts think? White paper, CLTC White Paper Series. UC Berkeley, 2021.
13. **Chen D., Wawrzynski P., Lv Z.** Cyber security in smart cities: a review of deep learning-based applications and case studies // *Sustainable Cities and Society*. 2021. Vol. 66. P. 102655.
14. **Li W., Song H., Zeng F.** Policy-based secure and trustworthy sensing for internet of things in smart cities // *IEEE Internet of Things Journal*. 2017. Vol. 5. No. 2. P. 716–723.
15. **AlDairi A. et al.** Cyber security attacks on smart cities and associated mobile technologies // *Procedia Computer Science*. 2017. Vol. 109. P. 1086–1091.
16. **Angelidou M.** Four European smart city strategies // *Int'l J. Soc. Sci. Stud*. 2016. Vol. 4. P. 18.
17. **Lv Z. et al.** AI-empowered IoT security for smart cities // *ACM Transactions on Internet Technology*. 2021. Vol. 21. No. 4. P. 1–21.
18. **Van Zoonen L.** Privacy concerns in smart cities // *Government Information Quarterly*. 2016. Vol. 33. No. 3. P. 472–480.
19. **Rivada A. et al.** Report on Non-technical Barriers and Legal and Normative Issues (No. D1. 13) // Valladolid, Spain: Fundación CARTTE. 2016.
20. **Kostina E. A., Kostin A. V.** Barriers to the use of feedback services at the municipal level. *Journal of Siberian Federal University. Humanities & Social Sciences*. 2023. Vol. 16, Is. 3. P. 468–480.

21. **Perera C. et al.** Sensing as a service model for smart cities supported by internet of things // Transactions on emerging telecommunications technologies. 2014. Vol. 25. No. 1. P. 81–93.
22. **Sovacool B. K., Del Rio D. D. F.** Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies // Renewable and sustainable energy reviews. 2020. Vol. 120. P. 109663.
23. **Pirotskaya A.** The Smart City Concept in the Experts' and Residents' Perception: Problems and Contradictions in the Concept Implementation. World of Economics and Management. 2020. Vol. 20(2). P. 178–196. DOI 10.25205/2542-0429-2020-20-2-178-196
24. **Van der Heiden N.** Urban foreign policy and domestic dilemmas: insights from Swiss and EU city-regions. ECPR Press, 2010.
25. **Hollands R. G.** Critical interventions into the corporate smart city // Cambridge journal of regions, economy and society. 2015. Vol. 8. No. 1. P. 61–77.
26. **Hamilton E.** The Benefits and Risks of Policymakers' Use of Smart City Technology // Mercatus Center Paper. 2016.
27. **Hollands R. G.** Will the real smart city please stand up? Intelligent, progressive or entrepreneurial? // city. 2008. Vol. 12. No. 3. P. 303–320.
28. **Vorobieva O. V., Manzhula E. A., Yashina A. V.** A smart city dweller in a smart city: a review of approaches in Russia and abroad. International Journal of Open Information Technologies. 2019. T. 7. No. 5. C. 59–65.
29. **Li Sh.** Problematic aspects of the formation of “smart cities” in Russia // Journal of Economic Regulation. 2019. T. 10. No. 2. C. 113–120.)
30. **Stepnov I. M., Kovalchuk Yu. A.** Economic traps of the introduction of artificial intelligence // Ekonomika. Nalogi. Pravo. 2020. T. 13. No. 2. C. 92–102.

Информация об авторе

Костина Елена Алексеевна, младший научный сотрудник Института экономики и организации промышленного производства
SPIN: 1138836
Scopus AuthorID: 57892887800

Information about the Author

Elena A. Kostina, junior researcher of the Institute of Economics and Industrial Engineering
SPIN: 1138836
Scopus AuthorID: 57892887800

*Статья поступила в редакцию 25.04.2023;
одобрена после рецензирования 25.05.2023; принята к публикации 25.05.2023*
*The article was submitted 25.04.2023;
approved after reviewing 25.05.2023; accepted for publication 25.05.2023*