

Выводы

Пример референдумов в Швейцарии как способов принятия государственных решений эффективен в условиях, сложившихся в данном государстве, но он также показывает универсальный образец реального участия граждан в управлении государством, диалога населения и органов государственной власти. Хотя большинство референдумов и проводится по инициативе органов государственной власти, но осуществляются и референдумы по инициативе избирателей. Референдум в этом государстве является одним из важнейших государственно-правовых институтов, проведение которого стало неотъемлемым атрибутом повседневной жизни граждан.

Более того, швейцарский опыт наглядно показывает, что такие формы консультаций с народом при разумном применении и с учетом национальных законодательных традиций могут быть весьма перспективны и эффективны для других стран.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Аксёнов, И. В. Референдум как институт политической партии: опыт Швейцарии / И. В. Аксёнов // Дискурс-Пи. – 2022. – Т. 19. – № 2. – С. 118–137.
2. Ауэр, Андреас. Референдумы в Швейцарии. / Андреас Ауэр // Сравнительное конституционное обозрение. – 2004 – № 3. – С. 152–155.
3. Окунькова, Л. А. Конституции государств Европы : в 3-х т. – Т. 3 / под ред. Л. А. Окунькова. – М. : Норма, 2001. – 792 с.
4. Самородова-Богацкая, Л. В. Эволюция института референдума и народной инициативы в Швейцарии: историко-правовой подход (Федеральный уровень) / Л. В. Самородова-Богацкая // Труды Института государства и права Российской академии наук. – 2014. – № 4. – С. 135–148.
5. Салова, С. А. Референдум в Швейцарии. / С. А. Салова // Актуальные проблемы права, экономики и управления. – 2014. – № 10. – С. 96–98.

УДК 004

С. Н. Бордак

Учреждение образования

«Гомельский государственный медицинский университет»,

г. Гомель, Республика Беларусь

ЦИФРОВИЗАЦИЯ: РИСКИ И УГРОЗЫ

Введение

Мир стоит на пороге четвертой промышленной революции, в основе которой лежит цифровая трансформация: наличие глобальной цифровой связи, снижение затрат на обработку и хранение данных высокой плотности, стремительный рост пользователей цифровыми технологиями. На смену эпохе глобализации идет эпоха турбулентного хаоса, беспорядка и нарастающих рисков.

Цель

Систематизировать риски и угрозы цифровой трансформации общества.

Термином «цифровизация» обозначают комплекс экономических, управленческих, социальных процессов, связанных с активным использованием и широким распространением в современной жизни цифровых, компьютерных, информационных, электронных, сетевых, телекоммуникационных технологий. Термин «цифровые технологии» используется для обозначения последних достижений в области цифровых технологий и сквозных цифровых технологий. Цифровой революцией называют современный этап развития IT-технологий и сети Интернет и связывают ее с цифровизацией

производства, что выражается в создании глобальных промышленных сетей с использованием искусственного интеллекта, распространением интернета вещей, сервисов автоматической идентификации, сбора и обработки глобальных баз данных, облачных технологий, социальных сетей, создании принципиально новых механизмов взаимодействия человека и машины [1, с. 13].

К проявлениям цифровизации относятся сквозные цифровые технологии, затрагивающие разные отрасли деятельности и влияющие на развитие цифровой экономики (большие данные, новые производственные технологии, промышленный интернет, искусственный интеллект, технологии беспроводной сети, компоненты робототехники и сенсорики, квантовые технологии, системы распределенного реестра, технологии виртуальной и дополненной реальности). Под цифровой экономикой понимают экономику, существенным элементом которой является использование информационных технологий. Цифровая экономика пронизывает все сферы общественной и экономической жизни большинства стран мира, воздействуя на различные сферы мирового и национального хозяйства: банковскую систему, торговлю, энергетику, транспорт, образование, здравоохранение и др. [2, с. 77].

Таким образом, будем использовать термин «цифровизация» для обозначения всех процессов цифровой трансформации общества и его отдельных институтов за счет внедрения информационных и сквозных цифровых технологий. Цифровые технологии развиваются настолько стремительно, что мы не успеваем отреагировать на них, осознать их сущность и угрозу, которую они в себе заключают (становятся инструментом тотального контроля, вмешательства в частную жизнь, распространения ложной информации, совершения правонарушений и др.). Систематизируем основные риски и угрозы цифровой трансформации общества. Я. В. Гайворонская [3, с. 27] разделяет все потенциальные угрозы цифровизации на гипотетические (возможные в перспективе на высоком уровне технологического развития) и реальные (очевидные и существующие в современном обществе на имеющемся уровне технологического развития). Гипотетические угрозы связаны с потенциально возможным проявлением и распространением искусственного интеллекта, с возможным противостоянием человека и искусственного интеллекта. К ним относится конфликт искусственного интеллекта с ноосферой, невозможность предугадать возможные угрозы и риски, связанные с данной технологией в будущем. Прогнозируемые угрозы в сфере искусственного интеллекта в основном касаются этических вопросов.

Реальные угрозы проявляются на современном этапе технического развития и требуют решений, они более актуальны. Все реальные угрозы связаны с проблемами безопасности личности, бизнеса, общества и государства в цифровой среде. К ним относятся: незащищенность персональных данных в киберпространстве и неспособность современных правовых средств осуществить регулирование и защиту общественных отношений; интеллектуализация военной робототехники и связанные с этим последствия (угроза потери контроля над военными компьютерными системами); изменение рынка труда и технологическая безработица; распространение киберпреступности и неспособность правоохранительных органов обеспечить безопасность личности в интернет-пространстве; отсутствие правового регулирования Интернета и механизмов действенного государственно-правового контроля в интернет-среде и др.

Отдельно выделяются гносеологические проблемы цифровизации. Например, угрозы классическим научным теориям и моделям, лежащим в основе действующих в настоящее время политических, правовых, экономических и др. социальных институтов.

В современных условиях основное внимание следует обратить на предотвращение реальных угроз цифровизации [3, с. 28]. Выделим группы проблем экономической безопасности цифрового общества: системные (касаются экономики в целом или ее значительных частей: зависимость от цифровых технологий других государств, отсутствие собственной элементарной базы, проблема «цифрового неравенства»); структурные (изменения отдельных социальных институтов или системообразующих процессов в обществе: существенные изменения на рынке труда и рост безработицы); отраслевые (отсутствие цифровых решений для отдельных отраслей, отсутствие собственной платежной системы); проблемы деятельности отдельных предприятий (экономическая безопасность конкретных участников бизнеса: кража корпоративных данных, промышленный шпионаж, хакерские атаки, недостаточная обеспеченность цифровыми технологиями и компетентными кадрами); проблемы цифровой безопасности отдельных граждан (кража, манипулирование личными данными) [4].

Согласно А. И. Пискунову, критерием классификации глобальных вызовов и угроз цифровой трансформации общества является определение сфер распространения потенциальных угроз. Вызовы и угрозы цифровизации разделены на пять групп. Первая группа – угрозы, которые могут спровоцировать социальную и экономическую нестабильность (технологическая безработица и ее проявления); вторая группа – угрозы разрыва в уровнях технологического развития между странами, различными экономическими группами в зависимости от доступа к эффективности использования интеллектуальных ресурсов; третья группа – связана с вероятностью техногенных катастроф, неспособностью человека лидировать в принятии управленческих решений по сравнению с интеллектуальными системами; четвертая группа – экологические риски и угрозы (интенсификация производства может привести к существенным изменениям климата); пятая группа – угрозы снижения уровня национальной безопасности страны (риски усиления терроризма, сложность обеспечения конфиденциальности информации, угроза создания новых моделей кибероружия) [5, с. 12]. Глобальная киберпреступность и кража данных в современных условиях представляет огромную угрозу и опасность. Персональные данные могут попасть в руки мошенников через кибератаки, через утечку информации из-за слабой защиты хранилища данных. Серьезными становятся риски, связанные с порчей и утратой информации из-за вирусных заражений коммуникационных каналов и баз данных [6]. Негативные последствия могут быть катастрофическими: от хищения данных, потери интеллектуальной собственности, порчи репутации компании и коммерческих убытков до остановки производств, техногенных и экологических катастроф [5, с. 11].

Автоматизация производственных процессов и массовое внедрение таких технологий, как цифровые платформы big Data, 3D – печать, роботизация и интернет вещей приведут к тому, что цифровые преобразования станут одним из главных драйверов экономического роста в мире. «Главный мотив для ускорения перехода к цифровой экономике состоит в потребностях национальной обороны, в способности предупредить или ликвидировать угрозы национальной безопасности в случае, если потенциальный противник обладает такими средствами нападения, которые действующие в настоящее время информационно-технологические системы не могут обнаружить и нейтрализовать при существующем уровне развития информационных технологий или масштабов их развития (применения)» [2, с. 77–78].

И. Ю. Ткаченко, анализируя вопросы цифровых изменений в жизнедеятельности мирового сообщества, указывает на некоторые их негативные последствия для человека, общества и национальных экономик: 1) феномен «психологического цифрового

рабства» (зависимость от работы цифровых устройств вызывает нервное беспокойство, если вдруг что-то перестает функционировать); 2) самоизоляция в системе «человек-компьютер», уход в жизнь в сети, в виртуальную реальность (в результате происходит утрата многих жизненно важных навыков деятельности, умения коммуницировать с другими людьми, растет социальный эгоизм, возможность не следовать нормам социальной морали, сокращается или полностью исчезает личное пространство); 3) гендерное расслоение, отрыв молодого поколения с цифровыми навыками от старшего поколения, не обладающего такими навыками; 4) превращение человека в бездумного потребителя и пользователя (онлайн-покупки); 5) исчезновение многих рабочих мест и потенциальная массовая «технологическая» безработица среди высококвалифицированного населения (востребованными становятся специальности, требующие компетенции в цифровом поле – специалисты по работе в социальных сетях); 6) неравный доступ к технологиям и углубление технологического разрыва между странами и внутри стран (богатые и образованные имеют хороший доступ к цифровым ресурсам, для малообеспеченных неадекватный доступ к технологиям может помешать овладеть техническими навыками, имеющими решающее значение для успеха в современной экономике); 7) киберугрозы относятся к числу наиболее вероятных и ощутимых угроз наднационального масштаба. Интернет является привлекательной целью для киберпреступников и шпионажа. Такие технологии, как искусственный интеллект, интернет вещей, блокчейн (механизм базы данных, позволяющий организовать открытый обмен информацией в рамках бизнес-сети), становятся объектом для киберпреступлений на уровне личности, бизнеса и государственной политики. Возникает противоречие между приоритетом краткосрочных национальных интересов, которые воплощаются в меры борьбы за национальный киберсуверенитет, и необходимостью выработки глобальной стратегии противодействия киберпреступлениям на наднациональном уровне [2, с. 80–84]. «Развитие информационных технологий – противоречивое явление. С одной стороны, такие технологии открывают новые возможности для интеллектуальной деятельности человека и существенным образом меняют окружающий человека мир; с другой – создают новые проблемы и новые социальные риски, к числу которых относится проблема информационной безопасности» [7, с. 56]. Новые тенденции в развитии цифрового мира создают новые риски для информационной безопасности государства. Под информационной безопасностью понимается состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной среде.

В Республике Беларусь в марте 2019 г. утверждена концепция информационной безопасности, провозгласившая информационный суверенитет, уважение цифрового суверенитета других стран и проведение мирной внешней информационной политики. 14 февраля 2023 г. подписан Указ №40 Президента Республики Беларусь «О кибербезопасности». 22 февраля 2023 г. утверждена концепция информационной безопасности Союзного государства, главной целью которой является защита национальных интересов государств – участников Договора о создании Союзного государства в информационной сфере. Концепция определяет основы для формирования согласованной государственной политики и развития общественных отношений в области обеспечения информационной безопасности, а также выработке мер по совершенствованию систем обеспечения информационной безопасности государств – участников Договора о создании Союзного государства. Речь идет о разработке концепции коллективной информационной безопасности Союзного государства, совместном противодействии современным информационным вызовам и угрозам, повышении защищенности ин-

формационной инфраструктуры государств – участников, их критически важных объектов, а также о борьбе с деструктивным воздействием на информационные ресурсы.

Выводы

Цифровые технологии меняют мир и помогают значительно повысить производительность труда, снизить затраты времени, энергии и ресурсов в ключевых сферах жизни. Однако, помимо преимуществ, у цифровизации есть и недостатки. Основной проблемой цифровизации на современном этапе является обеспечение безопасности личности, бизнеса, общества и государства. В процессе разворачивания нового технологического уклада все страны мира столкнутся с неоднозначными последствиями цифровизации, представляющими собой вызовы. Залогом устойчивости перед любыми внешними угрозами выступает укрепление внутреннего единства, политических сил, гражданского общества.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Карцхия, А. А. Цифровая революция: новые технологии и новая реальность / А. А. Карцхия // Правовая информатика. – 2017. – № 1. – С. 13-18.
2. Ткаченко, И. Ю. Проблемы развития цифровых технологий / И. Ю. Ткаченко // Российский внешнеэкономический вестник. – 2018. – № 9. – С. 76–87.
3. Гайворонская, Я. В. Риски и угрозы цифровизации / Я. В. Гайворонская // Advances in Studies. – 2020. – Vol. 8, Special iss. – P. 25–32.
4. Попов, Е. В. Проблемы экономической безопасности цифрового общества в условиях глобализации / Е. В. Попов, А. А. Семячков // Экономика региона. – 2018. – № 14 (4). – С. 1088–1101.
5. Пискунов, А. И. Вызовы, угрозы и ожидания цифровизации для промышленных предприятий // Организатор производства. – 2019. – № 27 (2). – С. 7-14.
6. Стерлядев, Р. К. Искусственный интеллект в аспекте ноосферы : почти фантастика? / Р. К. Стерлядев, Т. Д. Стерлядева // Вестник ПНИПУ. Культура. История. Философия. Право. – 2017. – № 2. – С. 61–65.
7. Бордак, С. Н. Виртуальная реальность как социокультурный феномен информационного общества / С. Н. Бордак // Материальные и духовные измерения культуры : сборник научных статей / редкол. : В. Н. Калмыков (гл. ред.) [и др.] ; М-во образования Республики Беларусь, Гом. гос. ун-т им. Ф. Скорины. – Гомель : ГГУ им. Ф. Скорины, 2017. – С. 54–58.

УДК 004:[316.2 + 614.2]

С. Н. Бордак

Учреждение образования

«Гомельский государственный медицинский университет»,

г. Гомель, Республика Беларусь

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ СОВРЕМЕННОГО ОБЩЕСТВА И ЗДОРОВЬЕ ЧЕЛОВЕКА

Введение

Активное внедрение цифровых технологий в повседневную и профессиональную деятельность современного человека привело к изменению его образа жизни. Высокий уровень комфорта, быстрый доступ к любой информации, широкие возможности для саморазвития значительно упрощают жизнь, экономят время на решение производственных и бытовых проблем, но сопровождаются появлением серьезных угроз для здоровья человека.