

5. Постановление Правительства РФ от 23 июня 2020 г. № 906 «О реестре социально ориентированных некоммерческих организаций» – ИБ «Консультант Плюс»: Законодательство / Российское законодательство (ВерсияПроф) (дата обращения 24.02.2021).

Всероссийский научно-исследовательский институт по проблемам гражданской обороны и чрезвычайных ситуаций МЧС России (ФЦ), Москва

T. E. Kholodkova

IMPROVING THE REGULATORY FRAMEWORK FOR THE DEVELOPMENT OF COOPERATION BETWEEN THE MINISTRY OF EMERGENCY SITUATIONS OF RUSSIA AND VOLUNTARY ORGANIZATIONS OF THE RUSSIAN FEDERATION

The article provides suggestions for improving the regulatory framework in the field of voluntary (volunteer) activities.

All-Russian Research Institute for Civil Defense Problems and emergencies (FC), Moscow

УДК 338.24

А. М. Карпович

ЦИФРОВАЯ ЭКОНОМИКА И ВОЗНИКАЮЩИЕ ПРИ ЕЕ РАЗВИТИИ РИСКИ

В статье рассматриваются основные риски, возникающие в экономике при её цифровизации. Отдельное внимание уделено действиям, позволяющим уменьшить негативный эффект перехода. Необходимо наличие качественного прогнозирования имеющихся тенденций развития, как экономического, так и социального характера.

Появление информационных (компьютерных) технологий в нашей жизни привело к формированию нового общества. Получив название «постиндустриального», это общество стало постепенно формироваться во всем мире независимо от уровня развития государства и общества. Процесс внедрения информационных технологий в экономику и жизнь общества заключается не только в самом процессе замены старых технологий более новыми и совершенными технологиями. Первоначально процесс информатизации заключался в замене одних технологий более новыми, но при этом это было лишь количественное изменение. Медленные средства связи заменились более быстрыми и компактными устройствами. Однако скорость появления новых технологий и их массовость привели к качественному ускорению имеющихся изменений. Причем, эти изменения показали и то, что наряду с положительным эффектом они несут и негативную составляющую.

Формирование новой цифровой реальности требует изменения жизни современного общества, как обязательного условия стабильности жизни общества. Человеку необходимо приспособиться к новым условиям, что является достаточно сложной задачей. В прошлые века изменение жизни общества происходило в течение продолжительного периода времени. Современный человек рождается в одних условиях, взрослеет в других и заканчивает ее в третьих.

Современный человек уже привык тому, что его окружают различные элементы цифровой экономики – оплата услуг без визита в отделения банка, заказ вещей и продуктов в интернет-магазинах и многое другое. Информационные системы, используемые различными государственными и коммерческими организациями, не требуют зачастую участия людей в своей работе. Новая реальность уже воспринимается как данность нашей жизни.

Основным риском внедрения информационных технологий является кадровая проблема. Кадры являются базой работы всех информационных систем. Новая информационная система в процессе ее разработки, внедрения и эксплуатации требует наличия специфических кадров. Организация при переносе своей деятельности в информационную сферу получает значительную экономию на аренде помещений, зарплате персонала и многое другое. При этом уменьшение имеющегося офисного персонала выразилось в необходимости найма новых сотрудников. Новые сотрудники, разрабатывающие и обслуживающие информационную систему, характеризуются наличием большого количества специфических умений и навыков. Необходимое количество грамотного персонала просто физически отсутствовало на рынке труда.

Фактически, организация осуществляет замену среднеквалифицированного персонала на высококвалифицированный персонал. Среднеквалифицированный персонал значительно проще обучить или найти уже обученный на рынке труда. Необходимо также учесть и то, что высококвалифицированный персонал может уйти в иностранные компании, которые всегда имеют более высокий уровень оплаты труда.

Развитие средств коммуникаций привело к тому, что высококвалифицированный персонал может работать в иностранных компаниях даже без переезда на новое место работы. Для работника это даже более предпочтительно, так как высокая заработная плата и низкий уровень цен повышает значимость работы за пределами бывшего постсоветского пространства.

Итогом этих процессов становится то, что работу информационных систем начинают обеспечивать программисты с низким уровнем квалификации. Ведь высококвалифицированный специалист получал свою квалификацию на протяжении нескольких лет. Тогда как замена ему нужна как можно быстрее. Соответственно новый специалист имеет меньшую квалификацию, меньшие запросы. Однако при этом возрастает проблема безопасности работы, как отдельной информационной системы, так и всей отрасли в целом.

Подготовка новых специалистов требует нескольких лет, но информационные системы уже существуют и их необходимо эксплуатировать. При этом нельзя не исключать того, что после окончания обучения специалист не перей-

дет на новую более высокооплачиваемую должность, но не в своей компании [1].

Следующей проблемой является то, что обыкновенный бизнес и бизнес на цифровых технологиях имеют различные места приложения. Традиционный бизнес использует информационные технологии как отражение своей деятельности. Фактически, информационные процессы в традиционной компании лишь дублируют и значительно упрощают существующие процессы. Например, компания осуществляет некоторую деятельность по своим обязательствам путем различных переводов, оплат. Информационные технологии используются после осуществления различных действий. Если происходит какой-либо форс-мажор и данные исчезают, то деятельность компании не сильно пострадает, так как будет необходимо лишь их повторно ввести в систему.

Для компаний, которые работают на цифровых технологиях, потеря данных может стать причиной значительных финансовых потерь и даже банкротства. Причем, будет отсутствовать даже сама возможность восстановления работы, так как будут отсутствовать ее аналоги на нецифровых носителях. Сама по себе информационная технология в данном случае является ядром бизнеса, а не некоторой служебной функцией.

Следующей проблемой является безопасность. Появление так называемого «интернета вещей» позволяет нам значительно улучшить нашу жизнь. Управление различными приборами и устройствами оптимизируют наши ресурсы. Следствием этого является необходимость установки различных контролирующих модулей в наши устройства. Получаемая и обрабатываемая этими устройствами информация при недостаточном уровне безопасности может попасть в руки злоумышленников для их последующего использования. Причем безопасность этой информации не может быть обеспечена даже корпорациями, которые затрачивают миллиарды на защиту данных [2].

С каждым годом возрастает актуальность проблемы искусственного интеллекта. Все новые и новые системы используют элементы искусственного интеллекта в решении различных задач. Распознавание графической и голосовой информации, сканирование окружающей действительности, анализ деятельности пользователя и многое другое. Получение контроля над системами искусственного интеллекта даже на современном уровне их развития может нанести колоссальный вред, как отдельному человеку, так и различным компаниям. Искусственный интеллект в развитой цифровой экономике открывает большое поле для использования полученной информации в неблагоприятных сферах [3].

Нельзя не упомянуть использование искусственного интеллекта в гражданской или военных сферах. Современная гражданская инфраструктура в развитых странах контролируется при помощи различных систем, которые могут быть подвергнуты атакам. Удар с помощью систем искусственного интеллекта, которые ориентированы на поиск уязвимостей и нанесение урона, имеет более разрушительный эффект на инфраструктуру. Причем, нанесенный урон может

превышать в финансовом значении урон от военных действий, ведущихся на этой территории [4].

Проблема безопасности различных информационных систем была и остается достаточно острой. Ежегодно регистрируются сотни и тысячи вирусов и вредоносных программ. Периодически по компьютерам пользователей сокрушительным валом проходят эпидемии вредоносных программ, которые обошли защиту пользователя. Соревнование компьютерных злоумышленников и защиты от них идет на протяжении долгих лет и окончания не видно. Каждая новая «прорывная» технология исследуется на поиск уязвимостей, которые постоянно находятся. [5].

Проблема существования человеческой личности при внедрении цифровой экономики является достаточно серьезной и актуальной. Декларируемая анонимность в сети позволяет осуществлять манипуляцию общественным сознанием в интересах конкретных групп и государств. Свобода слова в сети Интернет в последние годы является выражением, которое вызывает лишь грустную улыбку. Сеть Интернет, которая десятилетия назад представляла собой площадку для открытого общения и обмена мнениями превратилась в полностью контролируемую среду. «Частные компании», которые вольно трактуют свои правила в интересах конкретных социальных или политических групп превращают огромные информационные ресурсы в полностью тоталитарные сообщества, запрещающие любые отличные точки зрения.

Высокий уровень открытости различных цифровых сообществ стал источником информации, которая в большинстве своем является негативной. Контроль предоставления информации пользователю привел к появлению новых видов войн – информационных, которые несут урон, сопоставимый с реальными военными действиями.

Процесс перехода различных отраслей экономики в цифровой формат является перспективным делом. Информационные технологии позволяют провести оптимизацию деятельности различных процессов, получить экономию ресурсов, повысить управляемость различных организаций. Положительные эффекты от использования информационных технологий наблюдаются независимо от вида собственности и размера организации. Вместе с тем, цифровизация экономики ведет к появлению различных проблем, которые необходимо нивелировать различными способами. Система государственного управления должна формировать структуры, которые будут ориентированы на прогнозирование возможных рисков, а также уменьшение их вреда. Безопасность информационной системы должна быть не дополнительным модулем, а одной из обязательных функций.

Литература

1. Андрияшин, Ю. Н. О целях, возможных рисках и последствиях «цифровой экономики» [Электронный ресурс]. – Режим доступа: <http://reosh.ru/you-n-andriyashin-o-celyax-vozmozhnyx-riskax-i-posledstviyax-cifrovoj-ekonomiki.html>.
2. Ахромеева, Т. С. Стратегии и риски цифровой реальности [Электронный ресурс] / Т. С. Ахромеева, Г. Г. Малинецкий, С. А. Посашков. – Режим доступа: <http://sec.chgik.ru/ctrategii-i-riski-tsi-frovoy-realnosti>.

3. Дубровский Д. И. Электронная культура. Кто против? / Д. И. Дубровский // Фило-софские науки. – 2017. – № 2. – С. 50–57.

4. В. Жмудь, А. Ляпидевский, В. Аврамчук, О. Стукач, Н. Roth. Возможные техноло-гические барьеры для развития технологии промышленного интернета вещей и пути их пре-одоления. Автоматика и программная инженерия. 2019. №2 (28). С. 50–61.

5. Майер-Шёнбергер В., Кукьер К. Большие данные: Революция, которая изменит то, как мы живем, работаем и мыслим / Пер. с англ. - М.: Издательство «Манн, Иванов и Фер-бер», 2014. - 240 с.

Белорусский государственный аграрный технический университет, Минск

A. M. Karpovich

THE DIGITAL ECONOMY AND THE RISKS ARISING FROM ITS DEVELOPMENT

The article discusses the main risks that arise in the economy during its digitalization. Special attention is paid to actions that reduce the negative effect of the transition. It is necessary to have a qualitative forecast of the existing development trends, both economic and social.

Belarusian state agrarian technical university, Minsk

УДК 930.85+340.1:908

В. А. Карпиевич

ФОРМИРОВАНИЕ ПРЕДСТАВЛЕНИЯ О БЕЗОПАСНОСТИ ЖИЗНЕДЕЯТЕЛЬНОСТИ: ИСТОРИКО-ПРАВОВОЙ АСПЕКТ

В статье рассматриваются вопросы формирования представления общества и го-сударства о безопасности жизнедеятельности. Рассмотрено становление правовых норм, регламентирующих безопасность от огня.

По мере развития человеческого общества отношение к чрезвычайным ситуациям (ЧС) менялось. Приходило и осознание того, что культура безопас-ности жизнедеятельности становилась повседневной потребностью. Можно выделить три уровня формирования этой потребности:

- житейский;
- общественно-бытовой;
- социально-правовой.

Житейский уровень начал формироваться в период первобытнообщинно-го строя. На житейском уровне люди научились соблюдать простейшие прави-ла при использовании в своих целях тех или иных стихий. Так, человек понял, что огонь может сжечь все вокруг или причинить боль. Вода может затопить жилище, испортить продукты или домашний скarb. Ветер может погасить до-машний очаг, разрушить жилище.