ГОСУДАРСТВО И ГРАЖДАНСКОЕ ОБЩЕСТВО: ПОЛИТИКА, ЭКОНОМИКА, ПРАВО

DOI: 10.17805/zpu.2019.3.15

Цифровое общество: новые возможности — новые угрозы

А. В. Костина

Московский гуманитарный университет

Формирование цифрового общества является стратегической целью развития России, экономическая устойчивость и национальная безопасность которой напрямую зависят от степени ее конкурентоспособности. Сегодня одним из приоритетов информационного развития является такая цифровая технология, как технология Интернета вещей, способствующая созданию «интеллектуальной окружающей среды». Актуальность этой технологии определяется не только ее применимостью в потребительских бытовых условиях («умный дом», «умный город»), но главным образом — возможностью создания систем, в которых интеллектуальные устройства, объединенные в сети, совместно с людьми-операторами осуществляют работу в средах, опасных или недоступных для человека, — в космосе, на больших глубинах, в ядерных установках, трубопроводах и т. п. Однако применение этой технологии имеет и «побочные эффекты» — нанесение физического ущерба человеку через вживленные в его тело чипы, внедрение в систему управления домом и городским хозяйством в целях выведения из строя объектов и коммунальных систем. Наиболее тяжелые последствия имеют проникновения в системы крупных промышленных объектов, управление которыми осуществляется в автоматическом режиме через Интернет. Именно поэтому внедрение цифровых технологий требует анализа рисков и угроз как экономике, так и человеку и обществу.

Ключевые слова: цифровое общество; Интернет; Интернет вещей; облачные вычисления; кибербезопасность; умный город; разрушительные технологии; информационная безопасность

ВВЕДЕНИЕ

Одной из основных тенденций социально-экономического развития России является формирование в России информационного общества. Несмотря на то что процессы вхождения в «общество знаний» имеют особенности, отраженные в различных национальных концепциях, общим является признание государствами международных принципов, определенных Окинавской хартией глобального информационного общества (2000 г.), Декларацией принципов «Построение информационного общества — глобальная задача в новом тысячелетии» (2003 г.), Планом действий Тунисского обязательства (2005 г.). Основная цель Стратегии развития информационного общества в Российской Федерации — в соответствии с принципами, продекларированными на Всемирной встрече на высшем уровне по вопросам информационного

общества (Женева, 2003 г.), определяется как «создание условий для формирования в Российской Федерации общества знаний» (Стратегия развития ... : Электронный ресурс).

Важно то, что первые прогнозы относительно формирования цифрового общества были связаны с теорией индустриализма, сформулированной в 1950–1960-е гг. Р. Ароном и У. Ростоу и разделявшей все развитие человечества на три эпохи — доиндустриальную, индустриальную и постиндустриальную (или информационную). Концепция представляла достаточно стройную модель, описывавшую стадии цивилизационного развития человечества по пути технологического прогресса и их параметры — основной производственный ресурс, тип производственной деятельности, характер базовых технологий. Было показано, что существенные социальные изменения в информационном обществе связаны с экономическими трендами, где конвейерное производство, направленное на выпуск стандартизированных изделий, уступает место индивидуализированным продуктам, что отражается в стремлении общества не к стандартизации, а к персонализации социальных стратегий.

Однако классики индустриализма, а затем — постиндустриализма (включая чуть позже проявивших себя теоретиков информационного общества) Д. Белл, Дж. Нейсбит, Дж. Бенингер, Т. Стоуньер, М. Маклюэн, Э. Тоффлер, М. Кастельс, Е. Масуда описывали то общество, которое только формировалось, и из его наблюдаемых проявлений они могли фиксировать только отдельные тенденции, связанные с усилением роли информации и знания в этом обществе, а также компьютеризацию экономики и ее переход от крупномасштабного индустриального производства к экономике «знаний» и экономике «услуг». При этом информация рассматривалась одновременно как экономическая категория и как общественное благо, направленная на преобразование в прогрессивном направлении всех сфер социокультурной жизни.

Несмотря на то что принципы и основы Интернета были заложены сетью ARPANET, созданной еще в 1969 г., доступ к ней был закрыт, и влияния на общество и все сферы его развития эти разработки не оказывали. И только с появлением раннего варианта Интернета — сети NSFNET, появившейся в 1984 г., стало очевидно, что основой информационного общества станут сетевые технологии, стремительное развитие которых — наряду с цифровыми технологиями — создаст новую основу для трансформации моделей деятельности в области экономики, бизнеса, науки, культуры.

Целью данной статьи является определение тех сложностей в социально-гуманитарной сфере и тех «побочных эффектов», которые возникают при использовании новых информационных технологий.

ЦИФРОВАЯ ЭКОНОМИКА: НОВЫЕ ТЕХНОЛОГИИ

Конвергенция концепций «всепроникающих компьютерных систем» и «интеллектуальной окружающей среды» (Pervasive Computing, Ubiquitous Computing, Ambient Intelligence) стала почвой Интернета будущего, включающего в себя помимо нынешнего Интернета людей (Internet of People, IoP) еще и Интернет медиаконтента (Internet of Media, IoM), Интернет сервисов (Internet of Services, IoS), Интернет вещей (Internet of Things, IoT) (Черняк, 2013: Электронный ресурс).

Технология Интернета вещей (Internet of Things, IoT) основана на принципе накопления разнообразных, не дифференцированных и не структурированных данных — это «концепция вычислительной сети, соединяющей вещи (физические предметы), ос-

нащенные встроенными информационными технологиями для взаимодействия друг с другом или с внешней средой без участия человека» (Стратегия развития ... : Электронный ресурс). Фактически точное — на середину 1920-х гг. в полном смысле слова прогностическое — описание Интернета вещей представил еще Никола Тесла, проводивший эксперименты с беспроводной передачей энергии: «Когда беспроводные технологии достигнут подлинного развития, вся Земля превратится в единый огромный мозг, все вещи станут частью единого целого, и доступ к этому мозгу человек будет иметь с помощью прибора, похожего на современный телефон, каждый сможет носить его в кармане» (цит. по: Лукьянова, 2014: 4).

Первыми вещами, содержащими признаки интеллектуальных технологий, стали приборы с датчиками, отключающими их при бездействии, сначала в 1984 г. — самовыключающиеся утюги, в 1994 г. — электрочайники с контактной площадкой. Создание тех вещей, которые позволяют соотносить их с Интернетом вещей, стало возможно с развитием микроэлектроники и главное — сетевых технологий (началом их истории стал управляемый по Сети тостер, сделанный в 1990 г. Джоном Ромни). Само же понятие Internet of Things было предложено в 1999 г. Его автор Кевин Эштор, основатель исследовательского центра Auto-ID Center в Массачусетском технологическом институте (MIT), в полной мере не осознавал, какой технологический и социальный феномен он обозначил. Применение термину нашлось тогда, когда команда разработчиков из MIT вела проект для компании Procter&Gamble. Его содержание было связано с описанием товаров на складе, имеющих беспроводные метки, позволяющие центрам системы взаимодействовать друг с другом без участия человека[1]. Описание феномен Интернета вещей получил в том же году в книге Нейла Гершенфельда «Когда вещи начинают думать».

Фактически Интернет вещей означает формирование такого мира, в котором объединяются субстанциональные феномены (мир физических вещей) и функциональные, символические (цифровой мир, дублирующий физические вещи в виртуальном пространстве через систему сервисов и приложений). При этом информация от вещей, имеющих уникальные (Unique Identifier) или виртуальные идентификаторы (Virtual Identifier), связанная с событиями в физическом мире (к примеру, с температурным режимом, освещенностью, перемещением, энергопотреблением и т. п.), оценивается цифровыми аналогами, учитывающими данные и полученные ранее сведения и принимающими на основе их решения (выключения, включения, изменения режима функционирования и т. п.). При этом вещи проявляют способность к самостоятельной взаимной адресации и созданию мультипротокольных сетей связи. Одним из ярких примеров подобного взаимодействия является феномен «атакующего роя», представляющего собой согласованные действия дронов, объединяемых в группу с общим информационным полем, где каждая единица выполняет общую задачу, согласуя свои действия с другими элементами системы.

Несмотря на то что технология Интернета вещей (Internet of Things, IoT) только начинает активно внедряться в повседневные практики, последствия вполне ощутимы (Ивлиев, 2015).

Одним из примеров является концепция «умного города», становящаяся одной из актуальных, так как к середине XXI в. в городах будет проживать более 70% людей на земле. «Умный город» представляет собой внедрение в городскую жизнь технологий, использование всевозможных устройств, в том числе беспилотных автомобилей, навигаторов, приложений для парковок, Wi-Fi, электрифицированных остановок с Ин-

тернетом, интернет-магазинов, систем видеонаблюдения и распознавания лиц, систем слежения за степенью освещенности улиц, за состоянием окружающей среды, а в домах — за степенью отапливаемости помещений и пр. В системе «умного дома» приборы следят за чистотой воздуха и температурным режимом, включением приборов — пылесосов, электро- и СВЧ-плит.

К этому же разряду относится и такой стремительно развивающийся сегмент Интернета вещей, как body-net, представляющий собой систему встроенных в тело человека чипов, контролирующих и регулирующих его жизнедеятельность, используемых для диагностики и лечения, подключенных к Интернету. Уже активно раскупаются очки Google glass, в США продано огромное число индивидуальных медицинских приборов и имплантатов, подключенных к Интернету. Писатель-футуролог Брюс Стерлинг описывает Интернет вещей в своей книге «Будущее уже началось»: «У вас нет "душевой кабины". Но у вас есть стандартная система повседневного ухода за телом, которая каждое утро, умывая вас, тщательно проверяет все индексы и показатели вашего самочувствия и внешнего вида. Зубная щетка анализирует состояние ротовой полости, осуществляя учет живущих там микроорганизмов. Ваш туалет — самая сложная периферия в доме. Она предоставляет вам самую полную информацию о метаболических процессах в вашем организме — обо всех веществах, которые попадают туда и оттуда выводятся, а также обо всем, что с ними в вашем теле происходит» (Стерлинг, 2005: 10). Подобные устройства передают данные о состояниях и желаниях человека — например, чувства голода — в соответствующие инстанции, например в магазины, которые обеспечат человека пищей, отвечая на его потребности. Еще один элемент Интернета вещей — Интернет животных, где камеры наблюдения и встроенные чипы позволяют наблюдать за поведением питомцев в отсутствие человека.

Повсеместная цифровизация среды и самого человека существенно отразится на его жизни: основной, а порой единственной, формой социальных контактов останутся контакты в социальных сетях. «Умный дом» останется домом, но не собственным, а арендуемым — наподобие апарт-отелей. Человек перестанет заботиться о своем домашнем имуществе и даже одежде — при помощи 3D-принтеров можно будет в любом месте напечатать костюм. В еще одном прогнозе звучит отказ от собственности в пользу аренды — и в отношении квартиры, и в отношении вещей, начиная от машины и завершая посудой.

Особой актуальностью в цифровой экономике начинают обладать те технологии, которые могут быть оперативно представлены провайдером для обеспечения сетевого доступа к определенным вычислительным ресурсам (серверам, сетям передачи данных, устройствам хранения данных). Эта технология, получившая название *облачных вычислений*, определяется как «информационно-технологическая модель обеспечения повсеместного и удобного доступа с использованием сети "Интернет" к общему набору конфигурируемых вычислительных ресурсов ("облаку"), устройствам хранения данных, приложениям и сервисам, которые могут быть оперативно предоставлены и освобождены от нагрузки с минимальными эксплуатационными затратами или практически без участия провайдера» (Стратегия развития ... : Электронный ресурс).

Технология облачных вычислений внедряется начиная с 2006 г., хотя ее идея была сформулирована в 1970 г. Дж. Ликлайдером, одним из создателей ARPANET. Согласно Ликлайдеру, подключение к сети позволит ее пользователям получать как информацию, так и программы. Идея получила развитие в работах Джона Маккарти, пока-

завших, что вычислительные мощности могут выступать в качестве предоставляемой услуги (сервиса). Рынок, связанный с распространением этой технологии, стремительно растет. В 2017 г. аналитическая компания Gartner представила данные исследования затрат потребителей и компаний на публичные облака, которые в 2016 г. составили 209,2 млрд долл. против 175 млрд долл. в 2015 г., а также данные рынка продажи IaaS-решений, которые выросли на 56% до 25,3 млрд долл., чему способствовали «высокопроизводительные нагрузки, вроде искусственного интеллекта, Интернета вещей и аналитики»[2]. Рост на 23% в 2016 г. был продемонстрирован сегментом SaaS (программное обеспечение как услуга), объем которого составил 38,6 млрд долл. В два с лишним раза в 2016 г. вырос рынок PaaS-решений (платформа как услуга), объем которого составил 7,2 млрд долл. «Доходы в сегментах облачной рекламы, BPaaS-сервисов (бизнес-процессы как услуга) и услуг облачного управления и безопасности составили 90,3, 40,8 и 7,2 млрд долларов соответственно»[3].

Архитектуру облачных вычислений составляют три способа развертывания облачных служб: общедоступное облако (владение и управление осуществляется сторонними поставщиками облачных служб, «которые предоставляют свои вычислительные ресурсы (серверы и хранилище) через Интернет»[4]; закрытое или частное облако (владение и управление осуществляется одной компанией или организацией, а инфраструктура «разворачивается в частной сети»[5]; гибридное облако, сочетающее принципы общедоступного и частного.

В качестве основных преимуществ облачных вычислений эксперты называют оптимизацию затрат на приобретение, настройку, эксплуатацию оборудования и программного обеспечения; скорость получения объемов вычислительных ресурсов; гибкость при регулировании вычислительной мощности; высокая производительность; надежность — резервное копирование данных; безопасность — широкий набор техник контроля, защищающих данные, приложения и инфраструктуру от потенциальных угроз[6].

Для «расширения облачных функций хранения, вычисления и сетевого взаимодействия, в которой обработка данных осуществляется на конечном оборудовании (компьютеры, мобильные устройства, датчики, емарт-узлы и другое) в сети, а не в “облаке”» (Стратегия развития ... : Электронный ресурс), применяется информационно-технологическая модель системного уровня *туманных вычислений*.

Ведущая их концепция — построить систему связей между облачными вычислениями и Интернетом вещей, которая обеспечивает обработку данных не столько на «облачном» уровне, куда уходят данные, сколько в первую очередь на локальном — в районе «границы», в сети. Эта концепция позволяет обеспечить скорость операций по обработке данных, которые будут осуществляться сетевыми соединениями с низкой задержкой. Концепция туманных вычислений является одной из недавних разработок, однако она нашла применение в проектах, носящих в значительной степени экспериментальный характер. Среди них — проекты, требующие высокой скорости обработки данных, которая не может быть обеспечена трафиком данных в «облако» и обратно. Это обработка информации городов в отдаленных регионах (в рамках проекта «умный город», направленного в том числе на снижение расходов коммунальных систем); связь между автомобилями без водителей и между беспилотными самолетами, где данные должны обрабатываться в режиме реального времени; система распознавания лиц, обеспечивающая безопасность при помощи высокой пропускной способности в режиме реального времени[7].

ЦИФРОВАЯ ЭКОНОМИКА: НОВЫЕ РИСКИ

Несмотря на безусловную экономическую эффективность и необходимость внедрения новых цифровых технологий, нельзя забывать, что они выступают в качестве источника основных информационных угроз, оценка которым дана в Доктрине информационной безопасности Российской Федерации (Доктрина информационной ... : Электронный ресурс). В документе отмечаются тенденции повышения «сложности, увеличения масштабов и роста скоординированности компьютерных атак на объекты критической информационной инфраструктуры, усиления разведывательной деятельности иностранных государств в отношении Российской Федерации» (там же); возрастания в зарубежной прессе объема материалов с предвзятой оценкой отечественной государственной политики; усиления активности террористических и экстремистских организаций по использованию механизмов информационного воздействия; роста компьютерной преступности. Фиксируется стремление отдельных государств использовать технологическое превосходство для доминирования в информационном пространстве, невозможность осуществить справедливое управление безопасным и устойчивым функционированием сети Интернет в связи с существующим в настоящее время распределением ресурсов между странами.

Развитие цифровых технологий является серьезным вызовом национальной безопасности России, в том числе вызовом потери суверенитета. В Послании Федеральному Собранию Президента России 2016 г. отмечалась необходимость формирования собственных информационных технологий в целях сохранения независимости. Эта позиция определяется тем, что в настоящее время примерно 85% процессоров и 75% программного обеспечения, реализуемого на мировом рынке, производится американскими или находящимися под их юрисдикцией компаниями. Причем большинство этих компаний в рамках сотрудничества со спецслужбами США изначально закладывают в эту продукцию возможность несанкционированного проникновения — это, в частности, различные логические «бомбы» и неактивированные вирусы, способные вывести компьютер из строя в любой момент. Причем программные платформы могут использоваться для кибершпионажа и кибероперациий, носящих разрушительный характер. Исследователи проблемы высказывают точку зрения о том, что зарубежные производители программного обеспечения, связанного с новейшими технологиями, навязывают российской экономике «консервирующую» динамику, направленную на установление стойкого отставания российской экономики и фиксацию лидерства западных производителей в границах этого стратегического направления IT-рынка (Ларина, Овчинский, 2014: 156–157).

С целью внедрения собственных разработок в национальные экономики Группа Всемирного банка (World Bank Group) в 2016 г. предложила им рекомендации по развитию информационно-коммуникационных технологий, расширению возможностей доступа к ним как граждан, так и организаций, снятию цифровых барьеров, активизации внедрения цифровых технологий в сферу государственного управления[8]. Фактически это означает стремление к расширению контроля над национальными государствами и их цифровыми активами через использование типового программного обеспечения. Это можно рассматривать как реализацию политики «мягкой силы», и для России такой путь не приемлем, так как он означает ее переход в позицию объекта воздействия, пользователя чужих технологий, а также предполагает отказ от собственных разработок и их перемещение под чужую юрисдикцию. В условиях цифровой конкуренции вопросом выживания становится способность России к генерации инновационных (цифровых, био-, нано-, квантовых) технологий.

Цифровое общество предполагает, что все данные, активно функционирующие в обществе и государстве, предстают как оцифрованные. Те данные, которые не подвергаются оцифровке, в процесс информационного обращения включены не будут — они останутся на периферии и будут не востребованы совсем или востребованы ограниченным числом людей, имеющих к ним физический доступ. Поэтому оцифровке подлежит вся информация, генерируемая сегодня, а также то, что составляет так называемое наследие — в первую очередь историко-культурное. В оцифрованном виде предстает и вся информация, связанная с работой учреждений, государственных органов, производств, компаний, частных лиц.

В связи с этим определяются те сферы экономики и общественного развития, которые находятся в зоне риска и которые заложены в самой природе сетевых технологий. Так, компанией SRI Consulting Business Intelligence под эгидой Национального совета по разведке США, координирующего деятельность разведки в различных странах и сферах промышленного производства, еще в 2008 г. был опубликован документ Disruptive Civil Technologies («Разрушительные гражданские технологии»). В нем рассматриваются шесть технологий в перспективе 2025 г. с потенциальными последствиями для США: «Биотехнологии, Материалы для хранения энергии, Биотопливо и биологические химикаты, Чистые угольные технологии, Сервисная робототехника, Интернет вещей» (Disruptive, 2008). Как считают авторы разработки, среди названных технологий наибольшие потенциальные угрозы представляют те, которые являются сетевыми. А если иметь в виду то, что все названные технологии не только управляются с помощью локальных сетей, но и подключаются к глобальной, они предстают в качестве технологии Интернета вещей, используют Большие данные и осуществляют операции с помощью облачных вычислений. Это подтверждает и прогноз разработчиков, согласно которому к 2025 г. все окружающие нас предметы, в первую очередь в названных сферах, могут стать узлами Интернета вещей[9]. Масштаб внедрения этих потенциально разрушительных технологий очень велик уже сегодня, к 2020 г., как считают аналитики компании Cisco, на Интернет вещей будет приходиться более 70% интернет-трафика и 50 млрд IP-адресов, принадлежащих в большей степени не столько пользователям, сколько промышленным и инфраструктурным объектам.

Есть ли побочные эффекты внедрения Интернета вещей? Их немало. К примеру, юридические проблемы: определение вины в ситуации, когда беспилотный автомобиль сбивает человека, или в том случае, когда техника дает неверное решение и запирает дом с людьми при низкой температуре или недостаточном количестве воздуха. Наряду с безусловно положительным эффектом передоверия наблюдения за собственным физическим состоянием есть и отрицательный: система body-net может или ошибиться при принятии решения, или в нее может кто-нибудь внедриться и ввести данные, направленные на ухудшение состояния человека вплоть до его гибели. Прецедент вынесения приговора, связанного с убийством через Интернет, контролирующий функционирование кардиостимулятора, уже имел место в судебной практике США. Существуют и более простые, но не менее актуальные юридические проблемы, связанные с правовыми вопросами маркировки и прозрачного трансграничного перемещения. Как считают специалисты, в России первым шагом «в обеспечении прав и обязанностей в части цифровых активов мог бы стать Цифровой кодекс» (Агеев и др., 2017: 123).

Однако наибольшую опасность представляет применение этой технологии в системе крупных промышленных объектов, управление которыми осуществляется в автоматическом режиме. Ежегодное количество кибератак на промышленные объекты

(электростанции, жилищно-коммунальные комплексы и т. п.) разных стран стремительно растет. Причем это касается и таких особых объектов, как электростанции и атомные промышленные установки.

В январе 2003 г. в США была заражена вирусом Slammer и обрушена сначала корпоративная сеть атомной электростанции в штате Огайо, а затем система мониторинга безопасности и охлаждения станции, которая была восстановлена только через шесть часов. Вирусный червь Stuxnet в сентябре 2010 г. поразил около 30 тыс. компьютерных систем промышленных объектов Ирана и вывел из строя более 1,3 тыс. центрифуг по обогащению урана в Натанзе. Власти Ирана обвинили во взломе спецслужбы США. Еще одна троянская программа, в 20 раз превосходящая Stuxnet, — Flame была направлена на тестирование уязвимостей и кражу данных с целью перехвата физического управления объектами.

В декабре 2014 г. в Южной Корее через рассылку по корпоративной почте писем, содержащих вирус, хакерами была взломана внутренняя сеть оператора Hydro and Nuclear Power Co Ltd. Требование взломщиков было связано с остановкой реакторов на АЭС «Кори» и «Вольсон». Власти страны обвинили во взломе КНДР. В апреле 2016 г. в Германии вирусами W32.Ramnit и Conficker были атакованы компьютеры АЭС «Гундреммингенн» энергетической компании RWE. Поражение компьютеров не несло в себе угрозы для основных систем АЭС, так как ее компьютеры не были подключены к Сети[10]. Однако, как утверждают авторы Wall Street Journal, «самоорганизующиеся программы-импланты смогут выводить из строя объекты, никак не подключенные к Интернету, а функционирующие в закрытых сетях», используя для проникновения акустическую и оптическую среду (Ларина, Овчинский, 2014: 54). Благодаря материалам Э. Сноудена, стало известно о программе GENIE, к концу 2013 г. поразившей более 85 тыс. стратегических серверов (там же: 39).

«Кибератаки на ядерные объекты являются реальностью», — сказал на саммите по ядерной промышленности Анно Кайзерски, вице-председатель рабочей группы по киберугрозам. — Это не фантастика, это не гипотетическая ситуация, это то, что происходит в реальной жизни, и последствия нападений могут быть значительными и отражаться, например, в повреждении оборудования»[11]. По статистике, число кибератак с каждым годом становится все больше, а сами атаки — все более интенсивны. Согласно данным Лаборатории Касперского, которая представила статистику опросов 962 компаний по всему миру, в 2017 г. число кибератак на промышленные объекты возросло на 40%, а число их жертв составило 28% предприятий. Хотя бы один инцидент был зафиксирован в 87% предприятий. По словам директора по развитию бизнеса безопасности критической инфраструктуры Лаборатории Касперского Андрея Суворова, «кибератаки на промышленные системы управления становятся бесспорной угрозой номер один, так как имеют непосредственное влияние на непрерывность бизнеса и дорогостоящие основные активы производственной компании»[12]. Конечно, кибератаки не всегда наносят ущерб производственной безопасности, угрожая катастрофическими последствиями, но всегда наносят репутационный ущерб и потенциальную утрату конфиденциальных данных, выступая подчас проявлением недобросовестной конкуренции. Среди российских компаний число жертв кибератак меньше, чем общемировое, — 22% против 28%, их наличие подтвердили представители предприятий «Северсталь», «Норникель»[13].

Такие же пессимистические прогнозы специалисты строят в отношении облачных вычислений, настолько же ненадежных для размещения конфиденциальных данных

и решения критически важных задач. Руководитель IT-издания Strategic News Service Марк Андерсон считает, что риски, связанные с облачными технологиями, столь высоки, что их необходимо учитывать руководителям крупных компаний, и вскоре можно ожидать череды катастроф, связанных с сервисами-провайдерами, предоставляемыми через Интернет: «Это может быть катастрофа типа выхода из строя, или катастрофа, связанная с безопасностью, — сказал он. — В любом случае, это будет достаточно масштабное событие. Это будет такое бедствие, которое позволит вам сказать (если вы определяете IT-политику компании): “Вот почему я не стал связываться с облачными вычислениями. ...По моим догадкам, по-настоящему безопасного “облака” не будет никогда”»[14].

Эти наблюдения подтвердил директор подразделения облачных и виртуальных сервисов компании Cisco Systems Крис Хофф: «Облака не делают приложения отказоустойчивыми» — и напомнил ситуацию с потерей данных на сервисе закладок Magnolia[15]. Между тем, риски не останавливают компании, прибегающие к технологии облачных вычислений, так как преимущества оказываются гораздо более существенными, чем риски.

ЗАКЛЮЧЕНИЕ

Обобщая, отметим, что информационное общество, обладающее цифровой экономикой, — это реальность сегодняшнего дня. От успешности вхождения в информационное общество, от эффективности внедренных цифровых технологий, равно как от обеспечения информационной безопасности и кибербезопасности, от развития человека в этом типе общества зависит будущее нашей страны. Именно на обеспечение безопасности граждан и государства, повышение роли России в мировом гуманитарном и культурном пространстве, развитие свободного, устойчивого и безопасного взаимодействия граждан и организаций, органов государственной власти Российской Федерации, органов местного самоуправления, повышение эффективности государственного управления, развитие экономики и социальной сферы направлена Стратегия развития информационного общества в Российской Федерации (Стратегия развития ... : Электронный ресурс). В Стратегии делается акцент на том, что информационное общество — это не только цифровые технологии, но и развитие человека, это такое общество, «в котором информация и уровень ее применения и доступности кардинальным образом влияют на экономические и социокультурные условия жизни граждан» (там же).

Цифровое общество, таким образом, осмысливается в Стратегии не только в категориях экономических и технологических, но и в социокультурных. Изменяется сам характер труда и всей системы экономики, направленной на уникальные предложения, создание которых обеспечивается не наличием больших капиталов, а наличием креативных идей. Именно этот аспект учитывается в определении информационного общества как общества знаний, в котором «преобладающее значение для развития гражданина, экономики и государства имеют получение, сохранение, производство и распространение... информации с учетом стратегических национальных приоритетов Российской Федерации» (Стратегия развития ... : Электронный ресурс). И одними из наиболее важных приоритетов являются те, что связаны с развитием человека и общества, с обеспечением суверенности личности, с сохранением приватности персональной информации и персональных данных, с защитой общества от манипуляционных стратегий. Эти приоритеты являются столь же важными, как и те, что связаны с развитием самих цифровых технологий и цифровой экономики.

ПРИМЕЧАНИЯ

[1] Internet of Things: как простые вещи становятся умнее [Электронный ресурс] // Itmo.news. URL: http://news.ifmo.ru/ru/archive/archive2/news/4942/ (дата обращения: 05.06.2019).

[2] Мировой рынок облачных вычислений [Электронный ресурс]. URL: http://integral-russia.ru/2017/04/13/mirovoj-rynok-oblachnyh-vychislenij/ (дата обращения: 05.06.2019).

[3] Там же.

[4] Что такое облачные вычисления? [Электронный ресурс] // Microsoft Asure. URL: https://azure.microsoft.com/ru-ru/overview/what-is-cloud (дата обращения: 05.06.2019).

[5] Там же.

[6] Там же.

[7] Облачные туманные вычисления [Электронный ресурс]. URL: https://www.xelent.ru/blog/ezhik-v-tumane/ (дата обращения: 05.06.2019).

[8] Цифровые дивиденды. Доклад о мировом развитии 2016 [Электронный ресурс] // World Bank Group. URL: https://openknowledge.worldbank.org/bitstream/handle/10986/23347/210671 RuSum.pdf (дата обращения: 05.06.2019).

[9] Disruptive Civil Technologies (2008) Six Technologies with Potential Impacts on US Interests out to 2025 [Электронный ресурс] // National Intelligence Council. URL: https://fas.org/irp/nic/disruptive.pdf (дата обращения: 05.06.2019).

[10] Федуненко Е., Чернышева Е. (2017) Кибератаки на ядерные объекты. История вопроса [Электронный ресурс] // Коммерсантъ. № 10. 20 января. С. 9. URL: https://www.kommersant.ru/doc/3196397 (дата обращения: 05.06.2019).

[11] Хакеры атакуют все больше и больше ядерных объектов [Электронный ресурс] // Энергетика. ТЭС и АЭС. URL: http://tesiaes.ru/?p=15658 (дата обращения: 05.08.2019).

[12] Число целевых кибератак на промышленные предприятия возросло на 40% [Электронный ресурс] // SecurityLab.ru. URL: https://www.securitylab.ru/news/491150.php (дата обращения: 05.06.2019).

[13] Там же.

[14] Харьковский А. «Катастрофа облачных вычислений» в 2010 г.? [Электронный ресурс] // 3Dnews. URL: https://3dnews.ru/news/ikatastrofa_oblachnih_vichisleniii_v_2010_g/ (дата обращения: 05.06.2019).

[15] Там же.

СПИСОК ЛИТЕРАТУРЫ

Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы (утв. Указом Президента РФ от 9 мая 2017 г. № 203) [Электронный ресурс] // Президент России. URL: http://www.kremlin.ru/acts/bank/41919 (дата обращения: 05.06.2019).

Доктрина информационной безопасности Российской безопасности (утв. Указом Президента РФ от 5 декабря 2016 г. № 646) [Электронный ресурс] // Гарант. URL: https://www.garant.ru/products/ipo/prime/doc/71456224/ (дата обращения: 05.06.2019).

Агеев, А. И., Аверьянов, М. А., Евтушенко, С. Н., Кочетова, Е. Ю. (2017) Цифровое общество: архитектура, принципы, видение // Экономические стратегии. № 1. С. 114–125.

Ивлиев, С. Н. (2015) Интернет вещей. Новые угрозы информационной безопасности // Проблемы и перспективы развития отечественной светотехники, электротехники и энергетики. Материалы XII Всероссийской научно-технической конференции с международным участием в рамках III Всероссийского светотехнического форума с международным участием / отв. ред. О. Е. Железникова. Саранск : Мордовский государственный университет имени Н. П. Огарева. 542 с. С. 435–441.

Ларина, Е., Овчинский, В. (2014) Кибервойны XXI века. О чем умолчал Эдвард Сноуден. М. : Книжный мир. 349 с.

Лукьянова, Н. А. (2014) Интернет вещей: семиотическая конвергенция естественного и искусственного в коммуникациях // Информационное общество. № 3. С. 4–9.

Стерлинг, Б. (2005) Будущее уже началось: Что ждет каждого из нас в XXI веке? : пер. с англ. М. : У-Фактория. 263 с.

Черняк, Л. (2013) Интернет вещей: новые вызовы и новые технологии [Электронный ресурс] // Открытые системы. №4. URL: https://www.osp.ru/os/2013/04/13035551 (дата обращения: 05.06.2019).

Дата поступления: 06.06.2019 г.

DIGITAL SOCIETY: NEW OPPORTUNITIES — NEW THREATS

A. V. Kostina
Moscow University for the Humanities

The formation of a new society is a strategic target of the development of Russia, whose economic stability and national security depend directly on the degree of its competitiveness. Today, one of the priorities of informational development is the digital technology of the Internet of things, which promotes the creation of "intelligent environment". The topicality of this technology is determined not only by its applicability in consumer household conditions ("smart home', "smart city"), but mainly by the possibility to create systems, in which human-operated networks of intelligent devices work in dangerous or inaccessible environments: space, deep sea, nuclear facilities, pipelines, etc. However, there are "side effects" to the application of this technology: physical harm to the person done by implanting chips; intrusion in the house management and municipal services and facilities aimed at inactivating facilities and public utility systems. Intrusion in large scale industrial facilities automatically operated through the Internet has the most disastrous consequences. Therefore, the implementation of digital technologies requires an analysis of risks and threats it poses both to the economy, and the human and society.

Keywords: digital society; Internet; Internet of things; cloud computing; cybersecurity; smart city; destructive technologies; information security

REFERENCES

Strategiia razvitiia informatsionnogo obshchestva v Rossiiskoi Federatsii na 2017–2030 gody (utv. Ukazom Prezidenta RF ot 9 maia 2017 g. № 203). *Prezident Rossii* [online] Available at: http://www.kremlin.ru/acts/bank/41919 (access date: 05.06.2019). (In Russ.).

Doktrina informatsionnoi bezopasnosti Rossiiskoi bezopasnosti (utv. Ukazom Prezidenta RF ot 5 dekabria 2016 g. №646). *Garant* [online] Available at: https://www.garant.ru/products/ipo/prime/doc/71456224/ (access date: 05.06.2019). (In Russ.).

Ageev, A. I., Aver'ianov, M. A., Evtushenko, S. N. and Kochetova, E. Iu. (2017) Tsifrovoe obshchestvo: arkhitektura, printsipy, videnie. *Ekonomicheskie strategii*, no. 1, pp. 114–125. (In Russ.).

Ivliev, S. N. (2015) Internet veshchei. Novye ugrozy informatsionnoi bezopasnosti. In: *Problemy i perspektivy razvitiia otechestvennoi svetotekhniki, elektrotekhniki i energetiki. Materialy XII Vserossiiskoi nauchno-tekhnicheskoi konferentsii s mezhdunarodnym uchastiem v ramkakh III Vserossiiskogo svetotekhnicheskogo foruma s mezhdunarodnym uchastiem* / ed. by O. E. Zheleznikov. Saransk, Mordovskii gosudarstvennyi universitet imeni N. P. Ogareva. 542 p. Pp. 435–441. (In Russ.).

Larina, E. and Ovchinskii, V. (2014) *Kibervoiny XXI veka. O chem umolchal Edvard Snouden.* Moscow, Knizhnyi mir. 349 p. (In Russ.).

Luk'ianova, N. A. (2014) Internet veshchei: semioticheskaia konvergentsiia estestvennogo i iskusstvennogo v kommunikatsiiakh. *Informatsionnoe obshchestvo*, no. 3, pp. 4–9. (In Russ.).

Sterling, B. (2005) *Budushchee uzhe nachalos': Chto zhdet kazhdogo iz nas v XXI veke?* : transl. from Engl. Moscow, U-Faktoriia. 263 p. (In Russ.).

Cherniak, L. (2013) Internet veshchei: novye vyzovy i novye tekhnologii. *Otkrytye sistemy*, no. 4 [online] Available at: https://www.osp.ru/os/2013/04/13035551 (access date: 05.06.2019). (In Russ.).

Submission date: 06.06.2019.

Костина Анна Владимировна — доктор философских наук, доктор культурологии, профессор, директор Института фундаментальных и прикладных исследований Московского гуманитарного университета; академик Международной академии наук (г. Инсбрук, Австрия). Адрес: 111395, Россия, г. Москва, ул. Юности, д. 5. Тел.: +7 (499) 374-75-95. Эл. адрес: Anna_Kostina@inbox.ru

Kostina Anna Vladimirovna, Doctor of Philosophy, Doctor of Culturology, Professor, Director, Institute of Fundamental and Applied Studies, Moscow University for the Humanities, Member, International Academy of Sciences (Innsbruck, Austria). Postal address: 5, Yunosti St., Moscow, Russian Federation, 111395. Tel.: +7 (499) 374-75-95. E-mail: Anna_Kostina@inbox.ru