ФЕДЕРАЛЬНОЕ АГЕНТСТВО НАУЧНЫХ ОРГАНИЗАЦИЙ

ВСЕРОССИЙСКИЙ ИНСТИТУТ НАУЧНОЙ И ТЕХНИЧЕСКОЙ ИНФОРМАЦИИ
РОССИЙСКОЙ АКАДЕМИИ НАУК
(ВИНИТИ РАН)

НАУЧНО • ТЕХНИЧЕСКАЯ ИНФОРМАЦИЯ

Серия 1. ОРГАНИЗАЦИЯ И МЕТОДИКА ИНФОРМАЦИОННОЙ РАБОТЫ

ЕЖЕМЕСЯЧНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ СБОРНИК

Издается с 1961 г. **№ 5** **Москва 2020**

ОБЩИЙ РАЗДЕЛ

УДК 338.2 : [004:002]

О.В. Сюнтюренко

Риски развития цифровой экономики: информационные аспекты*

Обсуждается многоаспектная проблема выявления, оценки и минимизации угроз и рисков разработки и применения новых технологий в рамках Четвертой производственной революции, стержневым элементом которой являются информационные технологии. На основе системного подхода, с использованием методов наукометрии и многомерного анализа данных, анализируется ряд новых технологических направлений, потенциально порождающих наиболее опасные риски для экономики и социума, зачастую не осознаваемых даже в профессиональном сообществе. Сформулированы некоторые выводы, рекомендации, первоочередные и наиболее актуальные задачи разработки междисциплинарной проблемы рисков развития цифровой экономики.

Ключевые слова: *цифровая экономика, киберугрозы, информационные технологии, сетевая инфраструктура, интернет вещей, риски, робототехника, биокиберги, цифровое неравенство, социальное программирование, информационная безопасность*

DOI: 10.36535/0548-0019-2020-05-1

* Статья подготовлена в рамках работ по гранту РФФИ № 20-07-00014 «Разработка методологии использования наукометрических данных для решения задач целеполагания, прогнозирования и управления научными исследованиями».

ПРОБЛЕМА МИНИМИЗАЦИИ РИСКОВ РАЗВИТИЯ ЦИФРОВОЙ ЭКОНОМИКИ

В настоящее время мировая экономика фактически вступила в фазу Четвертой промышленной революции (в политических декларациях и СМИ под лозунгом «Цифровая экономика»). Она характеризуется широким производственным применением целого ряда новых кластеров технологий – прежде всего это технологии Интернета вещей, интеллектуальная робототехника, технологии обработки Больших Данных, 3D-принтинг, нанотехнологии и нанобиосенсорика, искусственный фотосинтез, умные сети электроснабжения, биотехнология (включая генную инженерию и регенеративную медицину), новые материалы с заранее спроектированными свойствами, мобильный широкополосный Интернет. Информационные технологии, информатика являются основой становления и интеграции отдельных технологических кластеров в формирующемся базовом промышленном комплексе нового технологического уклада. Уже сейчас можно констатировать максимально широкое «вплетение» цифровых информационных технологий в ткань любых производственных, технологических, образовательных и управленческих процессов. На основе глобальной сети Интернет создается единая цифровая среда (инфраструктура) с подключением к ней машин и оборудования, объектов инфраструктуры, транспорта, логистических цепочек, организаций, а также людей.

Правительства многих стран, в том числе и Российской Федерации, разрабатывают и финансируют программы по перестройке своих экономик в соответствии с тенденциями и требованиями цифровой реальности. По версии международного индекса сетевой готовности, представленной в докладе «Глобальные цифровые технологии» Всемирного экономического форума за 2016 г., Россия значительно отстает от мировых лидеров, занимая «по готовности к цифровой экономике» 41-е место, а по экономическим и цифровым результатам использования цифровых технологий – 38-е место. Осознавая важность этой проблематики для развития страны, Правительством РФ была разработана и в июле 2017 г. утверждена Программа «Цифровая экономика Российской Федерации» [1], в которой поставлена задача ускоренного движения по пути инновационного развития как главного средства выживания в условиях глобальной конкуренции. Инновации становятся важнейшим направлением современного промышленного производства, а интенсификация инновационной деятельности в научно-промышленной сфере – приоритетной задачей экономического развития (ежегодный оборот на мировом рынке высоких технологий и наукоемкой продукции в несколько раз превышает оборот рынка сырья, включая нефть, газ и нефтепродукты). При этом возможные негативные последствия использования новых технологий отходят на второй план или вообще не рассматриваются. Однако все технологии и виды современной техники имеют как положительные, так и отрицательные для общества последствия и несут в себе технологические, экологические, экономические и социальные риски [2, 3].

Исторический ход научно-технического и индустриального развития показал невозможность предвидеть весь спектр его негативных последствий для человечества. С процессами формирования нового технологического уклада связана фундаментальная неопределенность, поскольку общество, во-первых, просто не готово к столь масштабному расширению пределов возможного, а во-вторых, уже явные возможности влекут за собой и опасные последствия, большинство из которых все еще относится к сфере незнания. В ряде случаев возникает необходимость принимать решения по тем вопросам, по которым – казалось бы – их в принципе принять невозможно. Риск при этом сопряжен с возможным, но в момент принятия решения еще неявным ущербом, по характеру и масштабам которого иногда вовсе нельзя сделать никаких серьезных предположений. Например, только сравнительно недавно стали ясны отдаленные негативные последствия масштабного использования антибиотиков и диоксида титана, применяемого в пищевой и фармацевтической промышленности [4].

Оценка позитивных и негативных последствий развития той или иной технологии, например, для окружающей среды, часто затрудняется недостатком или вообще отсутствием информации и необходимых для принятия решений знаний, что, естественно, увеличивает опасность появления негативных последствий новых технологий. Наиболее показательной в данном случае является нанотехнология, где установки, предназначенные для проведения научных экспериментов, одновременно становятся оборудованием для нанофабрикации. Ученые еще сами до конца не выяснили природу изучаемых ими явлений, а нанопродукты все больше и больше заполняют современный рынок.

Таким образом, по мере развития цифровой экономики, особую важность и актуальность приобретает проблема (междисциплинарная по своему характеру) выявления, оценки и минимизации угроз и рисков разработки и применения новых, и в первую очередь информационных, технологий. Современные представления о риске отличаются многообразием. Существует множество определений риска, в основном в финансово-экономической сфере. Представляется, что в рамках настоящей статьи наиболее приемлемым (и кратким) является следующее определение: «Риск – это потенциальная возможность получить в условиях осознаваемой и будущей неопределенности заранее неизвестный результат негативного характера» [5]. Следует подчеркнуть, что информационная неопределенность (отсутствие информации о возможных состояниях системы, о внешней среде и т.п.) и есть среда появления риска.

Вопрос о классификации и систематизации рисков – это сложная методологическая проблема. При постановке задачи оценки рисков очевидна необходимость стратификации рисков по значимости потенциальных негативных последствий, в первую очередь –

социального характера. Целесообразна кластеризация рисков по сферам предметной деятельности (финансы, военное дело, образование, промышленность и т.д.). В сфере экономики и финансов возможна оценка риска как ожидаемой величины потерь (для каждой *k*-й группы рисков) в виде функции $r_k = f(Dp_k)$, где D – финансовая оценка потерь, а p_k – вероятность реализации риска. В общем случае уровень риска зависит от ряда параметров (зачастую неявных). Теоретический и практический интерес представляет получение количественной оценки уровня риска. При применении *i*-й новой технологии уровень риска может, в общем случае, определяться эмпирическим выражением $r_i = f(S_i, W_j, H_j, D)$, где S_i – стратификационный уровень значимости негативных последствий; W_j – *j-я* сфера предметной деятельности, где используется новая технология; H_i – энтропия среды, определяемая как $H_i = \log p_i$, где – вероятность реализации риска; D – объем вероятных финансовых потерь [5].

В общем случае однозначное и точное описание будущих состояний социотехнических систем, в состав которых входят новые технологии, часто остается недостижимым. Это обусловлено рядом причин, которые действуют и изолировано, и в комплексе: недостаточностью наших знаний; критически большим числом факторов, определяющих динамику исследуемого (прогнозируемого) процесса; открытым и эмерджентным характером изучаемых систем. Сложность современных социотехнических систем связана в первую очередь не с техническими, а с социальными факторами. В этом и состоит особенность очередного витка эволюции сложности технических систем в условиях роста технологических рисков. Система становится настолько сложной, что не в состоянии не только управлять своей деятельностью и развитием, но и предсказывать негативные сценарии такого развития и способы их преодоления. И здесь уже часто не работает традиционное математическое моделирование. Необходимо принимать во внимание, что при использовании математических вычислений учитываются лишь те отношения, которые доступны математической обработке, т. е. могут быть количественно выражены или выразимы. Кроме того, определение вероятности того или иного события, которое может привести к аварии, катастрофе, другим негативным последствиям, затрудняется тем, что это событие часто лежит за пределами познаваемого, а его последствия измеряются (оцениваются) не только в аспекте принесенного материального ущерба (как показали Чернобыльская катастрофа и авария на АЭС Фукусима).

Многоаспектная проблема выявления, качественной и/или количественной оценки рисков, разработки подходов к их минимизации является чрезвычайно важной междисциплинарной и, в определенной степени, трансдисциплинарной проблемой. В рамках настоящей статьи рассматривается, на содержательном уровне, ограниченный континиум зачастую неявных рисков и угроз использования новых информационных технологий, значимых с точки зрения возможных негативных последствий научно-технического и индустриального развития цифровой экономики.

СТРУКТУРНЫЙ АНАЛИЗ ПОТЕНЦИАЛЬНЫХ РИСКОВ

Борьбу с угрозами и минимизацию рисков необходимо начинать с их выявления, классификации, ранжирования и оценки (количественной и/или качественной). В короткой статье невозможно уделить достаточного внимания всему множеству {IT-рисков}. Далее с системных позиций проанализируем ряд новых развивающихся технологических направлений {A,B,C,D,E,F,G,H,I}, потенциально порождающих наиболее опасные риски для экономики и социума, зачастую не вполне осознаваемые даже в профессиональном сообществе.

A. По интенсивности и широте проникновения во все сегменты научно-промышленной сферы интернет-технологии сегодня занимают главенствующее место. Развитие интернет-технологий сопровождается расширением континиума риск-факторов. Необходимо также отметить выраженный тренд роста деструктивных сетевых социальных структур. Наиболее значимые риск-факторы связаны с быстрым развитием так называемого Интернета вещей (*IoT – Internet of Things*).

По существу *IoT* – это сеть физических предметов (вещей), которые оснащены встроенной технологией взаимодействия друг с другом и внешней телекоммуникационной средой. Именно *IoT* обеспечивает лавинообразное увеличение доли автоматически генерируемых данных в глобальной цифровой среде.

Создание и развитие таких сетей рассматривается как технология, способная перестроить как экономические, так и общественные процессы посредством исключения из части действий и операций необходимость участия человека [6]. По данным кампании *Strategy Analitics* [7], количество *IoT*- устройств в мире достигло 22 млрд в 2018 г. По результатам прогнозных исследований кампании *Amason*, в США в 2020 г. будет 25 млрд подключенных устройств (энергетических установок, общественных зданий, плотин, дамб, роботов, медицинских имплантов, городской и транспортной инфраструктуры и т.п.). Для большинства из них уровень защищенности близок к нулю. К 2025 г. число таких устройств вырастит до 50 млрд (с минимум 2500-3025 млрд связей ежедневно – согласно закону Меткалфа [8]). По оценкам специалистов, технология Интернет вещей уже к 2022 г. приведет к созданию телекоммуникационных сетей такой сложности и запутанности, что они будут не только не управляемыми, но и априори ненадежными. Проблема осложняется тем, что в последнее десятилетие активно развивается глобальная широкополосная сеть Интернет, которая теперь рассматривается как перспективный базовый элемент информационной инфраструктуры. Глобальная сеть, включающая разнообразные сегменты: иерархические и одноранговые сети, коммуникации по оптоволоконным сетям и подключение через ретрансляторы и спутники, чрезвычайно уязвима. В связанной цифровой среде даже

незначительные сбои, отказы, нештатные состояния различных приборов, датчиков, программного обеспечения могут привести к целому каскаду непредсказуемых негативных последствий. В 90-х годах прошлого века именно эти факторы-детерминанты стали одной из основных причин отказа от реализации США Программы СОИ. Согласно исследованиям, проведенным в Массачусетском технологическом институте, веерные отключения и отказы в результате ошибок и несовершенства *software* станут повседневной практикой и будут измеряться десятками и сотнями в год [9].

Таким образом, основные потенциальные риски IoT для экономики и социума состоят не столько в его преднамеренном использовании злоумышленниками, а сколько в самом факте его существования и дальнейшего развития.

B. По данным Международной федерации робототехники (*International Federation of Robotics – IFR*), объем мирового рынка промышленных роботов в 2018 г. достиг рекордных 422 тыс. единиц, что на 6% больше показателей годичной давности [8]. Примерно 30% продаж промышленных роботов в мире пришлось на китайский рынок по итогам 2018 г. Такие данные приводят в *IFR* в июле 2019 г. Ожидается, что к 2020 г. Китай войдет в десятку самых автоматизированных наций мира. К этому времени количество роботов на производстве должно возрасти до 150 единиц [10]. Кроме того, Китай планирует продать в общей сложности 100 тыс. промышленных роботов местного производства [11]. При этом США производят ~ 75% мирового выпуска роботов, оснащенных вычислительным интеллектом и способных к многофункциональной деятельности. По экспоненте растет число транспортных и бытовых роботов. В цифровой экономике именно человек становится наиболее непредсказуемым, а значит ненадежным звеном автоматизированных производств. Уже в настоящее время роботы вызывают страх у рабочих, юристов, работников транспорта, торговли, представителей других профессий с повторяющимися операциями [6]. Международная консалтинговая компания *McKinsey* предсказывает, что около 20% рабочей силы по всему миру – или 800 млн рабочих – могут потерять работу из-за автоматизации процессов [9]. В будущем до 15 млн. россиян могут лишиться работы, которая не требует серьезной квалификации, т.к. их профессия вымрет. Об этом заявил член комитета Государственной Думы РФ по труду, социальной политике и делам ветеранов Олег Шеин порталу «URA.RU» (04.08.2019). В этой связи следует отметить, что, несмотря на масштабность и важность проблемы, в научном сообществе, в настоящее время, не разрабатываются какие-либо подходы и методы оценки рисков и оценки (переоценки) ценности человеческого капитала с учетом трендов процесса роботизации хотя бы на период до 2025 г.

С учетом современных тенденций следует констатировать, что весьма динамично актуализируются риски, обусловленные ростом социальной напряженности (в различных социальных слоях) вследствие быстрого прогресса робототехники. Технологическая безработица уже в глобальной «повестке дня».

C. В перспективе весьма вероятной следует рассматривать ***актуализацию рисков, связанных с конвергенцией биомедицинских и компьютерных технологий.*** В интервале 15-25 лет синтетическая биология, генетическая инженерия, практическое применение нанороботов, способных действовать внутри кровеносной системы человека, совершенно поменяют лицо медицины. На горизонте 15-25 лет реальностью станет биотехнологическая интеграция человека и искусственного интеллекта, формирование своего рода биокибергов. Искусственный интеллект, который превзойдет человека – упрощение сложного феномена. Психика человека, его интеллект работает одновременно в трех сферах: цифровой, аналоговой или модальной, и образной. Воображение, распознавание закономерностей и сложные формы коммуникаций – это когнитивные области, где у людей до сих пор имеется неоспоримое преимущество, которое наверняка сохранится и в будущем. Таким образом, «синтезированные люди» будут обладать высокими креативными способностями, крепким здоровьем и высокой трудоспособностью в течение многих десятков и, возможно, сотен лет. Это будет новый вид людей, живущих в полной, включая цифровую и дополненную, реальности, здоровых и работоспособных от рождения до смерти. Этот новый человеческий вид будет неразрывно связан с искусственным, вычислительным интеллектом (прямой интерфейс мозг-компьютер), базами данных различного целевого назначения, системами поддержки принятия решений и распознавания.

Развитие синтетических технологий создания биокибергов (суперлюдей) неизбежно трансформирует современную человеческую цивилизацию, т.е. возникнет новая, нечеловеческая цивилизация с непредсказуемыми рисками и, возможно, глобальными негативными последствиями для антропосферы (ноосферы) в целом.

D. Объем генерируемой и передаваемой в мировых сетях информации экспоненциально растет и специалисты констатируют нарастающие информационные перегрузки. Д. Боуден и Л. Робинсон в исследовании 2008 г., названном «Темная сторона информации: перегрузка, тревожность и другие парадоксы и патологии» [12] определили информационную перегрузку как «состояние цивилизации, при котором объем потенциально полезной и актуальной информации, превышает возможность ее обработки средним человеком (т.е. когнитивные способности) и становится помехой, а не подспорьем». Наглядным примером информационной перегрузки являются оценочные данные *Alphabeth* (группы компаний, в которую входит и Google): от начала цивилизации и до 2003 г. было создано около 5 экзабайт ($5 \cdot 10^9$ Гб) информации; сейчас человечество создает столько данных всего за 2 дня.

Огромное количество информации зачастую ведет к невозможности ее воспринять и усвоить. Объективно существует противоречие между ограниченными психофизиологическими возможностями по-

требителя информации по восприятию новых знаний и большими потоками насущно необходимой научно-технической и экономической информации. Перегруженность информацией приводит к снижению когнитивных (познавательных) функций мозга (возникает также информационно-коммуникативная зависимость). Вследствие этого человеку приходится постоянно делать выбор в огромном многообразии новой информации. Проблема переизбытка информации несет в себе также и другую проблему, именуемую «информационным шумом». Перенасыщение каналов восприятия детерминирует способность индивидуального сознания справиться хотя бы с первичным анализом массивов поступающей информации. Следующий аспект «информационного шума» – это потеря определенного рабочего времени и интеллектуальных ресурсов человека, затраченных при поиске необходимых данных или же в процессе их сортировки и анализа, ведущих, в итоге, к переутомляемости. Специалист, стремящийся иметь информацию о всех новых достижениях в своей области, должен тратить до трети своего рабочего времени на её поиск, анализ и изучение, иначе существует опасность непроизводительных затрат до 45% средств, выделенных на исследования и/или разработку. Следует отметить, что в настоящее время теория научно-технической информации не располагает методами индустриальной интеграции знаний, представленных в разнородных источниках. Именно это определяет тенденции развития информационно-поисковых систем и технологий аналитической обработки данных.

По данным *IDC* (*International Data Corporation*), в американских компаниях сотрудники, имеющие дело с информацией, в среднем тратят 14,5 часа в неделю на обработку электронной почты, 9,6 часа – на поиск документов и 9,5 часа – на их анализ [13]. Однако лавинообразное нарастание количества информации не столько характеризует прогресс информационных технологий, сколько отражает их проблемы. В 2016 г. в англоязычном Интернете в течение года не было ни одного посетителя (посещения) на более чем 89% сайтов, а в 2018 г. – уже почти на 90%. Сходные процессы идут и в научном сфере. В настоящее время более 94% статей, опубликованных в научных журналах, ни разу не цитировались в других источниках. Почти 90% научных публикаций имели не более пяти прочтений [14].

Таким образом, вследствие нарастающей информационной перегрузки возрастают риски торможения научно-технического прогресса, так как даже важнейшие научные открытия и инновационные разработки могут оказаться просто незамеченными научно-технологическим сообществом.

E. Информационно-цифровое неравенство представляет собой сложную проблему, которая имеет социально-экономические, политические и культурные аспекты.

Из-за постоянного развития информационных технологий информационно-цифровое неравенство является актуальной и динамической проблемой. Развитие информационно-коммуникационных технологий дает толчок интеграционным процессам в экономике и обществе, но в то же время усиливаются процессы поляризации различных групп населения, регионов и стран. Возникает опасность формирования новой «информационной элиты», а также увеличения определенной страты людей, оказавшихся в маргинальном положении по отношению к информационно-компьютерным технологиям. Основными факторами риска, способствующими появлению информационно-цифрового неравенства, являются: недостаточно развитая информационно-коммуникационная инфраструктура; высокая стоимость интернет-услуг; низкий уровень развития образования и информационной культуры населения; отсутствие социальной поддержки в освоении информационных технологий; слабая мотивация и готовность разных групп населения к использованию информационно-компьютерных технологий.

Проблема информационно-цифрового неравенства, в ближайшей перспективе будет быстро нарастать и активно проявит себя, прежде всего в экономическом и социальном аспектах. Основания для такого вывода дает анализ тенденций развития глобального процесса информатизации, а также степени его воздействия на положение той или иной страны в мировом сообществе [15-17]. Этот анализ показывает, что в геополитическом плане процесс информатизации осуществляется крайне неравномерно и резко усиливает технологическую стратификацию стран мирового сообщества. Выступая в качестве мощного катализатора научно-технического прогресса, информатизация существенным образом ускоряет развитие передовых стран, обрекая тем самым другие страны на все большее и большее отставание. Именно поэтому принимать меры по ослаблению негативных последствий развития глобальной проблемы информационного неравенства необходимо уже сегодня, так как информационное неравенство усиливает социальное расслоение общества и поэтому является угрозой для его стабильности. Исторический опыт свидетельствует о том, что усиление любых форм социального неравенства опасно для развития общества, так как именно оно является первопричиной многих социальных и международных конфликтов. Поэтому своевременное осознание обществом новой для него глобальной проблемы — информационного неравенства – является одной из важных задач мирового сообщества.

Следует констатировать, что развитие цифровой экономики неизбежно обострит проблему информационно-цифрового неравенства и, как следствие, проблему экономического неравенства, что будет приводить к возникновению рисков, обусловленных ростом социальной и политической напряженности.

F. По мере становления цифровой экономики все более начинает осознаваться новый (и, возможно, самый опасный) вид угроз – разрушение способов и форм идентификации личности в результате длительного информационно-психологического воздействия – так называемая консциентальная война (от лат. *conscientia* – сознание) [18–20], что означает переструктуризацию внутреннего мира личности (социальное программирование).

В рамках процессов глобализации и становления цифровой экономики мир вступил в новый этап борьбы – конкуренцию не только технологий, товаров и услуг, но и форм и методов организации общественного сознания. С этой целью используют массовую культуру, транслируемую средствами массовой информации (в том числе и Интернет) и разрушающую ценности традиционного общества, т.е. используют информационное оружие, для которого нет преград в век спутниковой глобальной связи. Предметом трансформирующего воздействия являются определенные типы сознания, имея в виду, прежде всего, его традиционные, этические, культурные, религиозные аспекты и ценности. В результате длительного информационно-психологического воздействия определенные типы сознания могут быть изменены, стерты, перестать существовать. Традиционные типы сознания – объекты воздействия (поражения) в консциентальной войне – должны быть вытеснены за рамки цивилизационно допустимых и приемлемых. Это происходило и раньше, когда один тип сознания вытеснял другой (как, например, христианство сменило язычество). Но с развитием информационных технологий эта конкуренция и борьба принимают тотальный характер. Очень важно понимать, что изменение и/или уничтожение определенных типов сознания предполагает разрушение и переорганизацию общностей, которые конституируют эти типы сознания [16]. Можно выделить несколько основных технологий социального программирования, которые ориентированы на трансформацию (или разрушение) сознания. Во-первых, дезинтеграция и примитивизация информационно-коммуникативной среды, где функционирует и развивается сознание, приводит к понижению уровня ее организации. Во-вторых, распространение образов и текстов, разрушающих работу сознания на основе специальных методов (психотехнологий) по каналам коммуникаций. Сейчас сформировалась устойчивая тенденция, у все более растущей доли пользователей, замены понятийно-логического мышления образно-ассоциативным (клиповым). Клиповый тип мышления на порядок повышает внушаемость людей их склонность к некритическому восприятию информации. В-третьих, разрушение способов и форм идентификации личности по отношению к фиксированным общностям, что приводит к смене форм самоопределения и к деперсонализации.

В социальном программировании используются также стереотипы и привычки, особенности восприятия, характеристики психических состояний (тревожность, агрессия) и т.п. Основной вектор – это целенаправленное изменение общественного сознания и поведенческих предпочтений больших групп с использованием активных методов, в том числе психометрических алгоритмов. Деструктивные социальные сети, новые технологии мультимедиа и виртуальной реальности вовлекают человека в новые формы существования и в определенной мере могут оказывать воздействие на формирование личности. Как результат – рост угроз социальной и личностной дезадаптации и разрушение психики человека. Возрастает уровень угроз деформации общественной нравственности и морали. Как экспериментально показал российский нейропсихолог и нейрофизиолог С.В. Савельев, автоматизация познавательной поведенческой активности ведет к морфологическим изменениям в головном мозге. Вследствие высокой пластичности мозга церебральное закрепление алгоритмического поведения может происходить в значительно более сжатые временные периоды, чем считалось ранее [21, 22].

Все это, в итоге, ведет к росту рисков целенаправленного негативного воздействия современной цифровой сетевой среды (инфосферы) на когнитивные способности и поведение людей.

G. По мере развития цифровой экономики неизбежно будут расти риски, обусловленные все более широким использованием цифровых технологий в сфере вооружений и, прежде всего, в военно-космической области. Основные риски связаны с тем, что существуют фундаментальные причины, в силу которых программное обеспечение нельзя сделать настолько надежным, чтобы не сомневаться в том, что не возникнут нештатные ситуации и несанкционированного применения ракетно-ядерного оружия. Причем уровень угроз растет с ростом масштабов и сложности военных системотехнических комплексов. В настоящее время проблема усугубляется активной разработкой и широким внедрением суперкомпьютерных технологий, роботизированных систем и систем искусственного интеллекта в различные военно-технические комплексы.

О высоком уровне потенциальных угроз и рисков свидетельствует тот факт, что, по появившейся информации, в Китае по решению руководства, начиная с 2007 г. проводится оцифровка массивов знаний, инженерной и конструкторской документации по всем ключевым технологиям и научным направлениям. КНР создает крупнейшую в мире базу семян и генного материала не только по сельскохозяйственным животным, птицам и рыбам, но и в целом генную библиотеку обитателей Земли [14].

По сути, с учетом рисков санкционированного и/или несанкционированного применения ядерного оружия, речь идет о беспрецедентном проекте создания хранилища знаний, технологий, биоматериалов, которое гипотетически может понадобиться выжившим после катастрофы китайцам.

H. Наряду с интенсивным развитием информационных систем и сетей передачи данных все более актуальной становится проблема обеспечения информационной безопасности.

Широкое применение современных информационных технологий потенциально создает предпосылки таких угроз, как утечки, хищения, утраты, искажения, подделки, копирования и блокирования информации и, как следствие – экономического, экологического, социального и других видов ущерба [17, 23–25]. В разных странах регулярно регистрируются попытки несанкционированного проникновения в информационные системы органов государственной власти и управления, факты кражи и уничтожения экономической и финансовой информации, программного обеспечения систем электронных платежей и т.д. Несанкционированно вторгаясь в компьютерные сети, нарушители

способны не только копировать хранящуюся в них информацию, но и вводить в них вирусы, разрушающие прикладные (или системные) программы, которые срабатывают спустя определенное время (или при возникновении определенных условий), что значительно усложняет их обнаружение. Такие действия могут приводить к функциональному нарушению информационных систем, систем защиты критической инфраструктуры, объектов управления, возникновению социальной напряженности (например, в случае утечки и несанкционированного использования персональных данных, лжеминирования авиационного и железнодорожного транспорта и т.п.). По оценочным данным компании *Positive Technologies*, в 2018 г. статистика киберугроз имела следующий вид: доля целенаправленных атак составила 62%; доля атак, направленных на кражу персональных данных, – 30%, учетных данных – 24% и данных платежных карт – 14%; вредоносный *softwer* используется в 56% кибератак [26].

Информационная безопасность фактически становится одной из характеристик информационных систем и технологий. С позиций информатики здесь следует выделить два аспекта. Во-первых, реализация функций защиты требует все увеличивающихся информационных и вычислительных ресурсов, что влечет временные задержки и снижение производительности поиска и обработки информации. Во-вторых, быстрый рост глобальной сети, количества компьютерных систем, лавинообразный рост цифровых данных объективно влекут возрастание рисков и различного рода угроз целостности информации.

Помимо этого специалисты отмечают тревожную закономерность быстрого нарастания рисков, связанных с тем, что отдельный человек или малая группа могут получить и даже разработать оружие массового поражения (например, программируемые биовирусы, кибероружие, нановооружение и др.). Следует отметить, что современные методы и средства компьютерного моделирования позволяют значительно сокращать цикл «исследование – разработка» (за счет виртуализации лабораторных исследований и натурных испытаний). По мере развития цифровой экономики физический объем ущерба, который теоретически способен нанести всего один человек или небольшая группа, становится все больше и больше.

С высокой степенью вероятности можно прогнозировать, что такие факторы, как внедрение новых информационных технологий (в том числе суперкомпьютинга и систем искусственного интеллекта), расширение мировой сети телекоммуникаций, развитие семантического Интернета и массмедиа будут все более актуализировать проблему роста традиционных угроз и рисков в цифровой сетевой среде.

I. Риски развития цифровой экономики в России имеют определенную специфику.

1. ***Постоянным и высоким фактором риска в сфере энергетики, промышленности, телекоммуникаций является широкое использование импортной электронной элементной базы.*** Значительны риски, связанные с использованием в сложных системах и критических приложениях импортной микроэлектроники. По разным оценкам, до 75% реализуемого на мировом рынке программного обеспечения (в первую очередь, системного software – ОС и СУБД) и 85% процессоров производится компаниями под американской юрисдикцией. Ряд крупных IT-компаний встраивают в производимые чипы целевые закладки в интересах спецслужб. Принципиальные схемы и исходные коды «зашитого» в чипах программного обеспечения известны только фирме разработчику. По некоторым оценкам существует потенциально высокий уровень рисков нарушения функционирования для ~90% отечественных энергосетей (невосстановимое отключение системы, перехват управления энергосистемой и т. п.) как из-за атак компьютерных вирусов (типа *Dugu* или *Stuxnet*), так и от внешних несанкционированных действий, осуществляемых за пределами их возможного обнаружения и идентификации. Прецеденты – длительное нарушение функционирования энергосетей на Кубе в 2012 г. и в Венесуэле в 2019 г.

2. Критически важные для безопасности *RuNet* ресурсы и функции управления инфраструктурой (корневые серверы системы доменных имен, распределение адресного пространства, маршрутизация трафика) находятся и осуществляются за пределами России. ***Риски неустойчивой работы Интернета на территории России в случае недружественных целенаправленных действий достаточно высоки.*** Доступ (к сайту) может быть заблокирован на любом этапе: корневые серверы могут неправильно перевести адрес сайта в машинную форму, не отвечать на запросы, физически отключить сегмент сети от Интернета. Таким образом *RuNet* может быть заблокирован целиком. Прецедент – отключение Сирии от Интернета в 2012 г. [15]. Именно в силу этих причин гипотетически существуют риски отключения российского сегмента Интернета от международных платежных систем *Visa* и *Mastercard*, а также от международной межбанковской системы передачи информации и совершения платежей *SWIFT*. Экономические последствия вывода *RuNet* из строя будут катастрофичными, несопоставимыми по тяжести с любыми санкциями. Страна не просто вернется в технологическое прошлое – этот возврат будет сопровождаться выводом из строя, в частности, авиа- и железнодорожного сообщения, системы безналичных платежей и коммуникаций, включая сотовую связь. Американские компании являются производителями львиной доли повсеместно используемых мультиплексоров, маршрутизаторов, серверной инфраструктуры. Некоторые страны, например Китай, осознавая риски уязвимости интернет-трафика, приступили к созданию национальных сегментов Интернета. Ставя вопрос о полном отказе от пользования системами *Microsoft*, Китай добился передачи ему исходного программного кода операционной системы *Windows*, а также исходных текстов программного обеспечения маршрутизаторов фирмы *Cisco*, которые обеспечивают работу большинства мировых сетей и серверов (и, кстати, производятся в Китае) [27]. Следует также отметить, что практически все ведущие компании, специализирующиеся на разработке программных

решений по информационной безопасности сети Интернет, имеют американскую юрисдикцию так же как и все крупнейшие провайдеры (*Twitter*, *Google*, *Amazon*, *eBay*, *Facebook* и др.) [16].

НЕКОТОРЫЕ ВЫВОДЫ И АКТУАЛЬНЫЕ ЗАДАЧИ

Цифровая экономика и лежащие в ее основе технологии обладают огромным и уже бурно реализующимся потенциалом влияния на жизнь человека и общества. Является ли это влияние заведомо позитивным; помогает ли оно автоматически выходу на траектории устойчивого развития цивилизации, не содержит ли в себе развитие новых технологий (прежде всего информационных) дополнительных источников неустойчивости и *рисков* – эти вопросы приобретают все большую актуальность в условиях кризисной динамики мировой экономики и политической турбулентности в системе международных политических отношений.

По мнению многих экспертов [14, 17], одной из междисциплинарных сверхзадач XXI века является управление *риском* и безопасностью сложных систем в экономике и социуме. Сформулируем некоторые выводы, рекомендации, первоочередные и наиболее актуальные задачи разработки проблемы рисков развития цифровой экономики.

1. Четкое осознание основных целей и задач: а) раннее предупреждение *рисков* новых технологий и их конвергентных вариантов; б) разработка методологии их многокритериальной оценки (по сегментам экономики); в) разработка рекомендаций и комплексных мер по минимизации *рисков* и улучшение основы поиска решений (с позиций междисциплинарного и трансдисциплинарного подхода).

2. Разработка методов классификации и систематизации рисков на основе таксономии. Потребность в таксономии в данном случае возникает из-за сложности предметной области, не позволяющей провести ее систематизацию на основе некоторой достаточно просто выводимой классификации объектов, ее составляющих [28]. Роль таксономии рисков на этапах создания и реализации технологий состоит в том, что она должна позволять разным категориям специалистов, экспертов, программистов оценивать риски в самых разных аспектах: а) по значимости потенциальных негативных последствий; б) по различным факторам риска (сложности, времени и др.); в) по структурным и функциональным составляющим; г) по категориям потерь.

3. Разработка принципов, методов и рекомендаций по определению и оценке рисков на основе системного подхода, системного анализа, методов социотехнического проектирования, социальной инженерии, имитационного моделирования, теории «нечетких» множеств (с использованием технологии *Big Data*).

4. Создание международной системы сбора (и БнД), анализа и систематизации данных по реализовавшимся рискам, прежде всего связанных с управлением больших системотехнических комплексов (таких как Чернобыль, Фукусима, Шушенская ГРЭС и т.п.). Организация международного сотрудничества и обобщение международного опыта, ознакомление с уже имеющимися результатами исследований в этой области, организация конструктивного взаимодействия и совместной работы с зарубежными междисциплинарными группами ученых по данной проблематике.

ЗАКЛЮЧЕНИЕ

Несколько выходя за рамки рассматриваемой проблематики, хотелось бы сделать три замечания более общего характера.

1. В научных публикациях и СМИ постоянно используется термин «четвертая производственная (промышленная) революция», своеобразным синонимом которого является термин «цифровая экономика». Строго говоря, данный термин не вполне корректен. Важнейшей характеристикой современной мировой экономики является долговременное падение многофакторной эффективности производства, а любая производственная революция предполагает ускорение темпов роста производительности труда и эффективности производства. Этого в последние 20 лет не произошло. Среднегодовые темпы роста производительности труда в 2009–2017 годы были ниже, чем в период с 2000 по 2008 год, а в 2010-х гг. они были в свою очередь ниже средних показателей за последние 20 лет XX в. Это верно не только для глобальной экономики в целом, но и для таких экономически развитых стран как США, Германия, Великобритания. Франция, Япония [14, 29].

2. С начала 70-х гг. прошлого века из пятилетия в пятилетие снижаются темпы экономического роста, повышения эффективности производства (прежде всего производительности труда) и нормы прибыли. Несмотря на наращивание энерго- и механовооруженности, повсеместное внедрение информационных технологий, переломить тенденцию к снижению темпов роста производительности труда и многофакторной эффективности производства так и не удалось. В значительной степени это связано с постоянным неуклонным падением эффективности добычи энергии, а соответственно и снижением энергоэффективности производства. Сопоставительный анализ энергоемкости производства основных видов продукции в натуральном выражении показывает, что в процессе замены рабочей силы (как фактора производства) роботами она только растет. Ключевой показатель энергоэффективности – *EROEI* (*Energy returned on energy investement*) – соотношение полученной к затраченной энергии или энергетическая рентабельность [14, 30, 31]. Этот показатель характеризует отношение количества пригодной к использованию энергии, полученной из определенного источника, к количеству энергии, затраченной на получение этого энергетического ресурса. Если $EROEI \leq 1$, то источник энергии не может быть экономически выгодным в использовании. Падение *EROEI* не может быть компенсировано развитием интернет-технологий, внедрением роботов или обработкой больших данных. В структуре цифровой экономики развитие атомной энергетики также имеет свои риски и детерминанты. Основные опасения по поводу современной ядерной энергетики породили

аварии на АЭС Три-Майл-Айленд (США) в 1979 г., Чернобыле в 1986 г. и на Фукусиме в 2011 г. Катастрофа на Фукусиме разрушила миф об энергетических реакторах с нулевым риском. Но кроме значительных рисков для безопасности, эти реакторы имеют проблемы с утилизацией отходов и перекачивают огромное количество воды. Другой важный момент заключается в том, что основным источником топлива для современных атомных реакторов служит Уран-235, запасов которого вряд ли хватит на ближайшее столетие. Будущее с управляемым термоядерным синтезом, над технологиями стабильного использования которого работают ученые уже более 60 лет, представляется сейчас более чем призрачным [32].

По экспертным оценкам, снижение энергоэффективности на горизонте по крайней мере до 2035 г. будет иметь безусловно непрерывный и всеобъемлющий характер. Оно будет происходить темпами, не позволяющими повышать общую эффективность производства за счет внедрения новых технологий.

Таким образом, значимым риск-фактором является то, что долговременное снижение *EROEI* на фоне накладывающихся друг на друга финансово-экономического, природно-климатического и технологического кризисов, возможно на интервале 15-20 лет, вынудит глобальную цифровую экономику перейти к фазе сжатия со значительными отрицательными темпами роста, т.е. абсолютным сокращением производства и потребления товаров и услуг.

3. Стихийное, неуправляемое техническое развитие, преследующее цели экономического роста, может привести к тому, что на определенном этапе техника для своего дальнейшего формирования потребует больше затрат, чем может позволить себе человечество – или отрицательные последствия технологических решений остановят рост, или же, наконец, возникнут проблемы, не имеющие технического решения. Взаимоотношения общества, природы и техники в современных условиях характеризуются приближением к порогу качественных изменений, сам процесс которых может оказаться неконтролируемым и необратимым.

СПИСОК ЛИТЕРАТУРЫ

1. Национальная Программа «Цифровая экономика Российской Федерации»; утверждена распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р. – URL: static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf
2. Bechmann G. Risk and Rationality in a Future-oriented Society // Rationality in an Uncertain World / eds. G. Banse, I. Hronszky, G. Nelson. – Berlin: Edition Sigma, 2005. – P. 59-75.
3. Lenk H. Global TechnoScience and Rensponsibility. Schemes Applied to Human Values, Technology, Creativity and Globalisation. – Berlin: LIT, 2007.
4. Сюнтюренко О.В., Ефременко Д.В. Проблемы информационно-аналитического обеспечения социальной оценки технических и технологических рисков // Научно-техническая информация. Сер. 1. – 2017. – № 10. – С. 1-10; Syuntyurenko O.V., Efremenko D.V. Aspects of Analytical Information Support of the Social Assessment of Technical and Technology Risks // Scientific and Technical Information Processing. – 2017. – Vol. 44, № 4. – P. 227-235.
5. Сюнтюренко О.В. Социальные и экономические риски развития информационных технологий // Научно-техническая информация. Сер. 1. – 2012. – № 6. – С. 1–5; Syuntyurenko O.V. The Social and Economic Risks of the Development of Information Technologies // Scientific and Technical Information Processing. – 2012. – Vol. 39, № 2. – P. 113-116.
6. Бриньолфсон Э., Макафи Э. Вторая эра машин. Работ, прогресс и процветание в эпоху новейших технологий / пер. с англ. П. Миронова. – М.: АСТ. 2017 – 384.
7. Петров В.Ю., Рудашевская Е.А. Технология «интернета вещей» как перспективная современная информационная технология // Фундаментальные исследования. – 2017. – № 9-2. –
8. С. 471-476.
9. Закон Меткалфа сорок лет спустя после рождения Ethernet // Открытые системы. СУБД, 2014 – № 01. – URL: https//www.osp.ru/05/2014/01/13039684
10. Что такое интернет вещей. – URL: www.tadviser.ru/index.php/Статья: Что_такое_ интернет_вещей_(Internet_of_Things,_IoT)
11. Промышленные роботы. – URL: www.tadviser.ru/index.php/Статья: Промышленные_ роботы
12. Международная федерация робототехники представила список самых роботизированных стран мира. – URL: https://rb.ru/story/countrits-with-greaest-density-of-robots/
13. Факты и только факты: информационная перегрузка. – URL: http://lpgenerator.ru/blog/2014/01/07/fakty-i-tolko-fakty-informacionnaya-peregruzka/
14. Сюнтюренко О.В. Факторы-детерминанты неэффективного использования информационных ресурсов в научно-технической деятельности // Научно-техническая информация. Сер.1. – 2017. – № 7. – С. 1-12; Syuntyurenko O.V. Determinants of the Ineffective Use of Information Resources in Scientific and Technological Activities // Scientific and Technical Information Processing. – 2017. – Vol. 44, № 3. – P. 159-169.
15. Ларина Е.С., Овчинский В.С. Час волка. Введение в хронополитику. («Коллекция Изборского клуба») – М.: Книжный мир, 2019. – 416 с.
16. Как отключили Интернет в Сирии. – URL: d-russia.ru/otklyuchenie-strany-ot-interneta-precedent-byl.html
17. Сюнтюренко О.В. Сетевые технологии информационного противоборства и манипуляции общественным сознанием // Научно-техническая информация. Сер. 1. – 2015. – № 10. – С. 1-7; Syuntyurenko O.V. Network Technologies for Information Warfare and Manipulation of Public Opinion // Scientific and Technical Information Processing. – 2015. – Vol. 42, № 4. – P. 205-210.
18. Малинецкий Г.Г. Сценарии, стратегические риски, информационные технологии // Информа-

ционные технологии и вычислительные системы. – 2002. – № 4. – С. 83-108.
19. Громыко Ю. Оружие, поражающее сознание, – что это такое? // Альманах «Россия-210». – М., 1997.
20. Смирнов И., Безносюк Е., Журавлев А. Психотехнологии. – М., 1996. – URL: http://www.pereplet.ru/text/grom0.html.
21. Горохов В.Г., Сюнтюренко О.В. Технологические риски: информационные аспекты безопасности общества // Программные системы и вычислительные методы. – 2013. – № 4(5). – С. 344-353.
22. Савельев С.В. Социальная психология в действии! – URL: www.felicided.ru/2012/05/blog-post_3554.html
23. Савельев С.В. Нищета мозга. – М.: ВЕДИ, 2014. – 192 с.
24. Хоффман Л.Дж. Современные методы защиты информации. – М.: Советское радио, 1980. – 263 с.
25. Смолян Г.Л. Сетевые информационные технологии и проблемы безопасности личности // Вестник РФФИ. – 1999. – № 3(17). – С.: 63-68.
26. Siountiourenko O. The Problems of Providing Information Security: The Case of Information Infrastructure // Studies in Eastern Europe. Technological and Environmental Policy / ed. Gerhard Banse. – Berlin, 2007. – P. 163-178. 4
27. Актуальные киберугрозы – 2018. Тренды и прогнозы. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018/
28. Сюнтюренко О.В. Цифровая среда: тренды и риски развития // Научно-техническая информация. Сер. 1. – 2015. – № 2. – С.1-7; Syuntyurenko O.V. The Digital Environment: The Trends and Risks of Development // Scientific and Technical Information Processing. – 2015 – Vol. 42, № 1. – P. 24-29.
29. Советский энциклопедический словарь. – М.: Советская энциклопедия, 1982.
30. Замедление темпов роста в развитых странах: основные причины. – URL: https://popecon.ru/573-zamedlenie-ekonomicheskogo-rosta-v-razvityh-stranah-osnovnye-prichiny.html
31. EROI и пирамида энергетических потребностей человечества. – URL: https://horeseman5th.wordpress.com/источникие/eroi-и-пирамида-энергетических-нужд/
32. EROEI. – URL: https://habr.com/ru/post/100525/
33. Пара слов об управляемом термоядерном синтезе. – URL: https://pikabu.ru/story/para_slov_ob_upravlyaemom_termoyadernom_sinteze_6305487

Материал поступил в редакцию 03.02.20.

Сведения об авторе

СЮНТЮРЕНКО Олег Васильевич – доктор технических наук, профессор, ведущий научный сотрудник ВИНИТИ РАН, Москва
e-mail: olegasu@mail.ru