УДК 338 65.012

Информационные технологии в экономике: тенденции и проблемы непредвиденных последствий

© В.Г. Родионова

МГТУ им. Н.Э. Баумана, Москва, 105005, Россия

Рассмотрены тенденции и проблемы использования информационных технологий в отраслях российской экономики. Статистические данные показывают рост удельного веса отраслевых промышленных организаций, применяющих преимущественно локальные системы на основе информационных технологий. В отраслях финансов, банков, платежных системах, торговле и сфере досуга цифровые технологии распространяются наиболее динамично, но сопровождаются непредвиденными последствиями, эффекты которых получили название «цифровые войны».

***Ключевые слова**: информационные технологии (IT), цифровые (информационные) войны, закон непредвиденных последствий, статическая эффективность, динамическая эффективность.*

Введение. Составной частью формирующихся предпосылок для перехода российской экономики к пятому и шестому технологическим укладам являются IT-технологии, основывающиеся на использовании компьютерного программирования и Интернета. Несомненным подтверждением тому служит сформировавшийся и успешно развивающийся отечественный рынок спроса и предложения информационных технологий. Во-первых, структуры этого рынка интенсивно прирастают «машинно-компьютерными» техническими средствами разнообразного назначения и использованием Интернета. Во-вторых, растет численность соответствующих IT-компаний и их специалистов, выполняющих отраслевые запросы экономики по аналоговому и современному цифровому программированию основной и вспомогательной деятельности деловых компаний. В общей отраслевой системе российской экономики спрос на информационные технологии исходит от отраслевых фирм как в материальном производстве, так и в сфере услуг. Исходя из спроса складывается предложение информационных технологий IT-компаниями как организационно сформированными отраслевыми структурами различного масштаба. Информационные технологии органично дополняют их основную экономическую деятельность, либо присутствуя на рынке относительно автономно в виде специализированных IT-компаний, либо функционируя в качестве внутрифирменных подразделений в составе деловых промышленных, торговых, банковских компаний или государственных учреждений.

Профессиональная локализация сфер специализированной IT-деятельности представлена высококвалифицированными специалистами цифрового программирования, использующими технические средства программирования и коммуникации.

В сфере данного рынка применяются стандартные и специфические способы конкуренции IT-структур, осуществляющих узкопрофессиональную задачу, — изобретение новейших информационно-коммуникативных технологий для создания, хранения, обработки информации и обмена ею с внешней экономической средой. В современной экономике именно эти функции служат ускорению любых деловых процессов фирм и учреждений. IT-специалисты по компьютерной технике и программированию оказывают мощное влияние на облик большинства отраслей, поскольку привносят информационно-цифровые методы в процессы движения экономических потоков товаров, услуг и денежно-финансовых ресурсов, способствуя их переходу от статической к динамической эффективности.

На уровне *микроэкономики* информационные технологии привносят в первичные звенья новые алгоритмы предпринимательства, информационный инжиниринг, автоформализацию (автоструктурирование) деловых процессов. Информация из внешней среды трансформируется и включается в предпринимательские процессы, повышает информационную составляющую эффективности материального и нематериального производств, качество предлагаемых товаров и услуг.

На уровне *макроэкономики* влияние информационных технологий диктует необходимость выбора направления развития экономической системы, согласованного с глобальными процессами трансформации ее структуры, в том числе за счет новых внешних ресурсов, включая не только ресурсы планетарного масштаба, но и поиск ресурсов в процессе освоения пространства ближнего космоса.

В итоге развитие многих отраслей экономики подвергается эволюционным изменениям, которые способствуют снижению издержек производства и хозяйствования в любой сфере деятельности, улучшают структуру и методы управления ими.

Информационные технологии указывают точки бифуркации, т. е. новые направления или ранее не существовавшие изменения в развитии экономических процессов. Основу этих процессов составляют применение и постоянное обновление информационной инфраструктуры, т. е. высокотехнологичного компьютерного приборостроения, устройств мобильной связи, создания и использования технических средств и систем освоения ближнего космического пространства.

Основные виды информационных и коммуникационных технологий (ИКТ) как фактор динамической эффективности отраслей экономики. Статическая эффективность (*static efficiency*) —

возможность *экстенсивного* экономического роста за счет вовлечения дополнительного количества имеющихся в наличии традиционных средств, ресурсов и неизменных технологий. Динамическая эффективность (*dynamic efficiency*) — способность *к интенсивному* экономическому росту в условиях ограничения или исчерпания традиционных ресурсов за счет качественных факторов, т. е. внедрения нововведений и технологических изменений.

В настоящее время динамическая эффективность достигается на основе использования IT-технологий, средств микроэлектроники для сбора, хранения, обработки, поиска, передачи и представления данных, текстов, образов и звука в экономике. Этой цели подчинено формирование информационной сети Интернет и взаимодействующих локальных сетей электронно-вычислительных машин (ЭВМ). Их расположение возможно в любых локальных и глобальных масштабах, но при этом они должны взаимодействовать по каналам дальней связи (коммутируемым или выделенным), предоставляемым телефонными компаниями или другими организациями связи.

Масштаб современных информационных и коммуникационных технологий, используемых организациями в российской экономике, показан на основе приведенных в табл. 1 статистических данных [1].

Таблица 1

Удельный вес организаций, использовавших информационные и коммуникационные технологии (% от общего числа обследованных организаций)

	2008	2009	2010	2011	2012
Удельный вес организаций, использовавших: – персональные компьютеры;	99,2	98,9	99,6	99,5	99,2
– ЭВМ других типов;	19,4	22,8	25,3	23,9	24,6
– локальные вычислительные сети;	68,8	69,5	81,4	81,0	85,2
– электронную почту;	84,3	87,1	88,6	90,6	93,7
– глобальные информационные сети:	84,6	86,6	89,2	92,7	94,6
из них — сеть Интернет;	84,2	86,3	89,2	92,6	94,6
имевших веб-сайты в сети Интернет	25,4	26,2	30,4	37,3	44,6

Виды и системы использования информационно-коммуникационных технологий в российских компаниях. Интернет, как множество независимых компьютерных сетей, соединяет пользователей для обмена информацией по стандартным открытым протоколам. На основе широкополосного доступа (ШПД) в Интернет, обес-

печивающего скорость передачи данных 256 кбит/с и выше, предоставляется возможность обмена информацией, использования идентичных технических и программных средств, методов и ресурсов. Общедоступность Интернета достигается также благодаря специализированным (корпоративной или ведомственной) сетям — Интранету, Экстранету и локальным вычислительным сетям.

Интранет как распределенная корпоративная вычислительная сеть базируется на технологиях Интернета и предназначена для обеспечения доступа сотрудников к корпоративным информационным электронным ресурсам.

Экстранет — расширение Интранета, содержащее выделенные области, к которым разрешен доступ внешним пользователям (например, частичное предоставление внешним пользователям доступа к корпоративным данным о движении их заказов или о наличии продукции на складе).

Локальная вычислительная сеть соединяет две или более ЭВМ (возможно, разного типа), а также принтеры, сканеры, системы сигнализации (охранной, пожарной) и другое производственное оборудование и периферийные устройства, расположенные в пределах одного или нескольких соседних зданий, и не использует для этого средства связи общего назначения.

В последние годы для отечественной экономики было создано более 1 138 передовых, новых производственных технологий с обслуживанием их информационно-коммуникационными системами. В их числе:

- по проектированию и инжинирингу — 191–272 вида; по производству, обработке и сборке деталей — 18;
- по автоматизированной транспортировке, а также погрузочно-разгрузочным операциям — более 405; технологиям автоматизированного наблюдения и/или контроля — более 128; в сфере связи и управления — около 154; в производственно-информационных системах — более 50;
- по интегрированному управлению и контролю — от 37 до 57 разновидностей.

В ресурсных компаниях базовых отраслей экономики цифровые технологии охватывают также внутрикорпоративное взаимодействие и мобильность сотрудников через локальные социальные сети (электронная почта, видеоконференции, другие виды мобильного обмена сообщениями). Предусмотрен также безопасный доступ к основным информационным данным. В табл. 2 представлено отраслевое использование информационных технологий в российской экономике [2].

Таблица 2

Удельный вес организаций, использовавших сеть Интернет для связи с поставщиками и потребителями товаров (работ, услуг), по видам экономической деятельности (% от общего числа обследованных организаций соответствующего вида деятельности)

	Организации, использовавшие сеть Интернет	
	для размещения заказов на товары (работы, услуги)	для получения заказов на выпускаемые товары (работы, услуги)
Всего	**100**	**100**
В том числе в отраслях: – добыча полезных ископаемых;	1,2	1,0
– обрабатывающие производства;	5,3	12,4
– производство и распределение электроэнергии, газа и воды;	3,1	4,9
– строительство;	2,2	3,9
– оптовая и розничная торговля; ремонт автотранспортных средств, мотоциклов, бытовых изделий и предметов личного пользования;	5,6	12,1
– гостиницы и рестораны;	0,5	1,6
– транспорт и связь;	6,4	9,1
– финансовая деятельность;	3,0	6,5
– операции с недвижимым имуществом, при аренде и предоставлении услуг;	10,9	13,4
– государственное управление и обеспечение военной безопасности; обязательное социальное обеспечение;	29,6	9,8
– высшее профессиональное образование;	1,6	1,3
– здравоохранение и предоставление социальных услуг	20,0	14,0

Удельный вес компаний, использующих ИКТ, зависит от уровня их текущих и капитальных затрат на закупку вычислительной техники и программного обеспечения, оплату услуг связи, обучение сотрудников или оплату услуг сторонних организаций и специалистов, а также прочих сопряженных расходов.

Так, в отраслях добычи сырьевых ресурсов, в частности на месторождениях нефти и газа, внедрение и освоение систем цифрового моделирования используется для сокращения затрат на разведку ме-

сторождений, применения более эффективных технологий добычи и повышения коэффициента извлечения сырьевого продукта. Предварительное цифровое моделирование применяется до начала разработки месторождений на основе единых стандартов IT-систем по модели *Accentur*, например в компании «ЛУКОЙЛ Оверсиз Холдинг ЛТД» для централизованного управления компанией «ЛУКОЙЛ» и подразделениями, представляющими ее интересы в ряде стран Средней Азии, Ираке, Венесуэле и Западной Африке.

В большинстве сырьевых добывающих отраслей нефти и газа частично или полностью осуществлена автоматизация с помощью АСУ ТП — автоматизированных систем управления технологическими процессами. Они представляют собой множество датчиков для сбора информации при непосредственном производстве — процессе добычи сырья. Как правило, это данные для контроля давления, влажности, наличия примесей и их концентрации в основном продукте, скорости движения механизмов, электромагнитного излучения и пр. АСУ ТП объединяется с цифровой трансформацией системы управления производственным процессом, т. е. корпоративным планированием и управлением ресурсами для общего повышения эффективности и качества управленческих решений.

В энергетике, металлургии и тяжелой промышленности масштабы цифровой трансформации еще незначительны, они используются для сбора и анализа информации для принятия решений, обработки больших массивов информации о технологических процессах. Цифровые технологии здесь также способствуют повышению скорости и улучшению качества управления. Цифровизация позволяет предсказывать изменения в объемах работ, информирует о скачках потребления электроэнергии и при необходимости способствует корректированию ее генерации. Например, в цифровых сетях счетчики *Smart Grid* автоматически обнаруживают нестандартное поведение потребителей энергетических ресурсов, способствуют регулированию сезонности в их потреблении, осуществлению корректировки ценовой политики и учету «географии» местоположения клиентских фирм.

Особенно высок спрос на ИКТ в телекоммуникационных отраслях, сфере визуальных развлечений и отдыха, кино- и шоу-бизнесе. Эти отрасли относятся к группе наиболее доступных для внедрения цифровых технологий. Во многом именно благодаря им наиболее высока скорость внедрения технологий компьютерного дизайна и программирования. В этом заключается основа роста качества и эффективности их услуг для населения, а также доходов.

В отраслях материального производства, особенно в обрабатывающих производствах, уровень спроса и возможности использования цифровых технологий значительно ниже, хотя именно для них эта задача особо актуальна.

Перечень примеров следования за передовыми цифровыми технологиями пополняют пока преимущественно фармацевтические компании, используя аналитику производства медицинских и индивидуальных диетических продуктов.

Остальные группы отраслей материального производства не изобилуют примерами выпуска качественного ассортимента продукции, конкурентная способность которой не соответствует предъявляемым потребностям на внутреннем и тем более мировых рынках. Использование современных технологий особенно важно для таких отраслей, как «малое» машиностроение, приборостроение и инструменты, химическая промышленность, где компаниям предстоит налаживать взаимодействие со своими партнерами на основе платного онлайнового портала для управления заказами, повышения конкурентоспособности продукции и выхода на мировые рынки.

В сферах транспортных услуг, туризма и отдыха, в средних и дорогих сегментах жилищного строительства, мобильного банковского обслуживания спрос на ИКТ обеспечивает высокую динамическую эффективность развития предпринимательства. Аналитики этого сектора экономики считают, что для закрепления на данных рынках услуг необходимо трансформироваться в цифровое предприятие, реагирующее на изменения в настроениях потребителей, выпускающее персонифицированные товары и услуги. Одновременно необходимо отслеживать в реальном времени внутрифирменные финансовые показатели и регулировать свои бизнес-процессы. «Цифровой или мертвый» [3] — это девиз и краткая формула для частных компаний, стремящихся к эффективному взаимодействию предпринимательства и потребителей в отраслях сферы потребительского спроса на транспортные услуги, жилищное строительство, торговые услуги, услуги туризма и пр.

Необходима особо высокая скорость освоения ИКТ, чтобы соответствовать запросам клиентов. Цифровые технологии и широкополосный доступ в Сеть способствуют повсеместной активизации предпринимательства на основе использования рекламы в Интернете и других средствах массовой информации. Задачу — следовать за «белым кроликом» цифровых технологий и IT-обслуживания потребителей товаров и услуг — решают более 580 000 компаний этого сектора экономики. Реклама служит основой и двигателем интернет-торговли, она способствует стремительному развитию потребительских рынков, современных форм доставки товаров.

Особенности предложения ИКТ на отечественном рынке. Их можно проиллюстрировать на примере достаточно крупной отечественной фирмы — *Cognitive Technologies* [4]. В настоящее время здесь официально трудятся 835 человек, не считая офшорных программистов. В начале 1990-х гг. эта компания предлагала своим кли-

ентам лишь аппаратно-программные комплексы. Новый этап деятельности начался в 2002 г., когда структуру рынка изменили финансисты: они стали относиться к софту как к высокоприбыльному, очень удобному для работы и полезному продукту. Этот период закончился примерно в 2009 г. Период профессионального развития начался, когда рынку потребовались системные, большие финансовые работы и участие в федеральных целевых программах. Позже произошла узкая специализация на ключевых продуктах *Cognitive Technologies.* Ими стали системы электронного документооборота, оптического распознавания символов, информационно-аналитические; разработки в области искусственного интеллекта и т. д. Направление, называемое документооборотом, включает целый ряд продуктов: системы управления предприятием, *CRM (Clients Relations Management),* систему управления взаимоотношениями с клиентами и многое другое. Если посмотреть на оценочные коэффициенты, то у *business software* они сейчас одни из самых высоких. У этого бизнеса много клиентов, хороший инвестиционный потенциал, он наиболее понятен для инвесторов и перспективен.

По существу, специализация компании сводится к следующим основным направлениям работы.

Первая тема IT-проектов — система электронных закупок во всех ее видах. Президент РФ В.В. Путин допустил к эксперименту по созданию электронных торговых площадок три проекта: единую электронную торговую площадку — ЕЭТП, площадки Сбербанка («Сбербанк-АСТ» — «Ведомости») и Агентства по государственному заказу Республики Татарстан. Через год состоялся конкурс, и три экспериментальные площадки вошли в число победителей. В настоящее время такого сайта, как *zakupki.gov.ru*, нет ни в США, ни в Европе, считает глава компании О. Ускова.

IT-решение, которое легло в основу российской системы госзакупок, оказалось уникальным. С одной стороны, эта система обладает всеми признаками банковской: возможность совершать платежи, закрытость, электронная подпись и т. д.; с другой, поскольку поставщики отбираются открытым способом, — это, по сути, открытый портал. Совместить эти две функции в одной системе — задача очень непростая, она решается до сих пор, и вопрос кибертерроризма сохраняет актуальность. Через площадки электронных закупок проходят триллионы рублей, каждый день проводятся тысячи торгов, и за каждыми торгами стоит совокупность разных интересов. Поэтому защита данных — отдельная задача, которая во всем мире решается очень сложными путями. Идея этой системы — полная анонимность: ни заказчик, ни участники конкурса не должны знать, кто участвует в торгах, а видят только их номера. Но где-то внутри системы все равно лежит таблица, в которой записано, кто стоит под номером 1,

а кто — под номером 99, и на сером рынке эта информация очень востребована. Технологических решений, достойных серьезного внимания, два: *Cognitive Technologies* и «Сбербанк-АСТ». Именно этими технологиями обеспечиваются защита от взлома и противодействие *DDoS*-атакам кибератившистов со всего мира.

Следующее направление — разработки *Cognitive Technologies* в области искусственного интеллекта. Искусственный интеллект — это моделирование работы мозга, поступления в мозг информации, т. е. сенсорного восприятия — зрения, осязания и т. д. С 2000 г. появилась задача — научиться работать с объемным зрением. Ее поставили отечественные заказчики из оборонки, которым требовалась такая система для самолетов-беспилотников с 3D-зрением. Компания занималась этим почти 10 лет и сейчас оформляет шесть международных патентов, поскольку направление переходит в коммерческий режим. Одновременно идут переговоры с автопроизводителями по созданию системы беспилотного управления автомобилями. Это будет не продукт, а технология. Израильская компания *Mobileye* еще в 2002 г. разработала плату, которая вставляется в автомобиль и решает определенные задачи управления. *Cognitive Technologies* делает нечто более высокоуровневое — чисто софтверное решение, и при этом ставится задача полного безопасного управления автомобилем. Создать полный беспилотник — это фактически решение «под ключ»: сел в точке А — и доехал до точки Б. Среди реальных конкурентов остается лишь вышеназванная израильская компания.

С искусственным интеллектом связано и такое направление, как электронный документооборот (например, система «Е1 Евфрат»). Это предложение для клиентов из сферы *SMB* (средний и малый бизнес), т. е. компания предлагает IT-модель перехода от управления документооборотом к управлению бизнесом, созданию системы поддержки принятия решений.

По инициативе *Cognitive Technologies* появилось общественное объединение — Национальная ассоциация инноваций и развития информационных технологий (НАИРИТ), возникшее благодаря взаимодействию с Президентом РФ В.В. Путиным по вопросам развития инновационной экономики. Компанией были сделали бесплатные сервисы по поддержке патентования — интеллектуальная сеть «Кулибин».

Следующее направление работы компании — экспертные системы поддержки принятия решений, что также связано с системами искусственного интеллекта. Суть их сводится к *Big Data*: потребитель должен уметь работать с бесконечно большим объемом информации, чтобы принимать правильные решения.

Содержание выполняемых коллективом *Cognitive Technologies* проектов показывает [4], что на долю заказов от государства приходится едва ли не половина выполняемых проектов. На втором

месте (13 %) — проекты для функциональных структур сферы денежного обращения, банков и финансовых структур; на сферу промышленности приходится 11 % IT-проектов; на энергетику — 2 %; образование и страхование — по 3 %; здравоохранение — 4 %; торговлю и телекоммуникации — по 6 %.

Приведенные на рис. 1, 2 диаграммы иллюстрируют основное содержание проектов компании *Cognitive Technologies* (консолидированная отчетность по группе за 2012 г. характеризуется годовой общей выручкой в объеме 1,12 млрд руб. и чистой прибылью 173 млн руб.) [4].

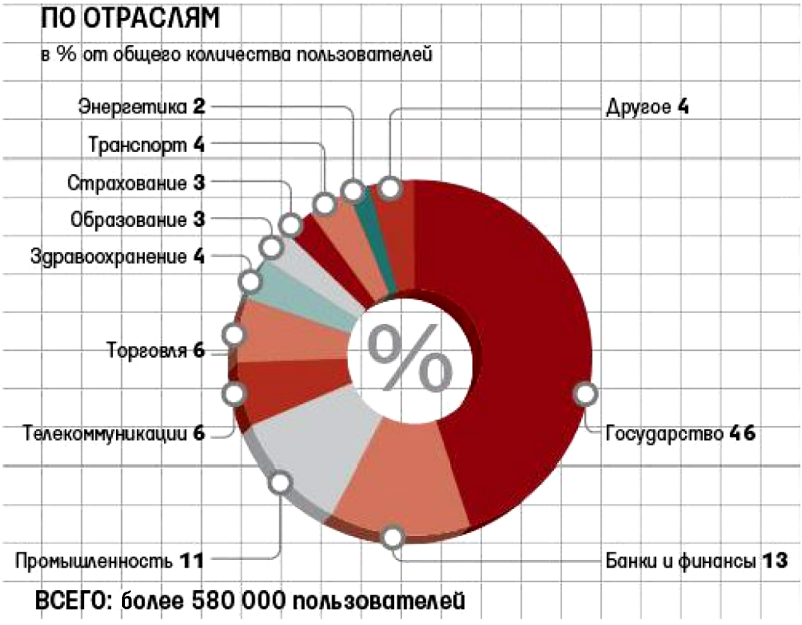

Рис. 1

Закон непредвиденных последствий: информационные технологии и статистика киберинцидентов. Разработка ряда проектов требует информационной защиты баз данных о потенциале или данных о конкурентных преимуществах компаний.

Программируемый «продукт» информационных технологий по преимуществу имеет нематериальную форму, если не считать его произведенную «компьютерно-машинную» основу и материализованные носители «записи» соответствующих программ, кодов, паролей и т. п. Восприятие неосязаемости, виртуальности Интернета замещено его осмыслением в качестве «Сети», т. е. предметной системы электронного взаимодействия реального компьютерного «железа» с его программным обеспечением (ПО).

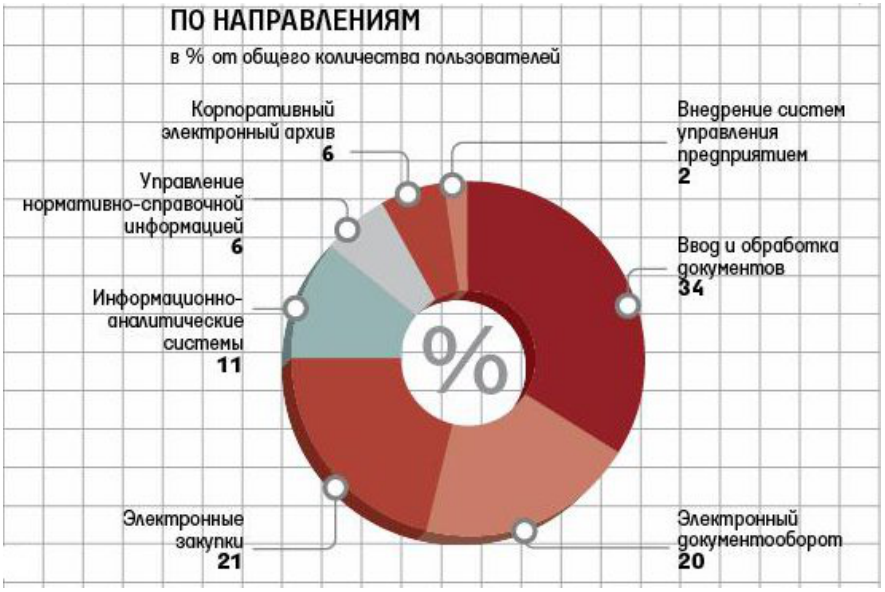

Рис. 2

Редкая возможность уникального совмещения виртуального и реального в таком явлении, как Интернет и компьютер с его ПО, способствовала своеобразному проявлению закона непредвиденных последствий. Сущность закона заключается в свойствах некоторых явлений порождать неожиданные эффекты в дополнение к тем, которые считались однозначными или единственно возможными. На всех предшествующих технологических укладах методы стимулирования прогресса содержали в себе непредвиденные эффекты влияния на экологию и социальную сферу. Интернет и связанные с ним технологии достаточно длительное время считались лишь способом ускорения трансляции таких ценных форм потребительских благ, как сигнал, звук, изображение, и улучшения их качества. Уникальность Интернета и информационных технологий очевидна и неоспорима. Но сравнительно долгое время их эффекты явно не приносили доходов, сопоставимых с уникальностью используемого явления. Дело не только в том, что процесс использования электронных устройств и создания компьютерных программ не сопряжен с особо дорогостоящими капиталоемкими затратами. Деятельность специалистов IT-сферы также не столь трудоемка, хотя и требует образования, интеллектуальных усилий, систематизации знаний и особых навыков, в том числе интуиции при поиске экономических сфер применения «продуктов» компьютерного программирования. Итог «продуцирования» также зачастую оказывался гипотетическим, непредсказуемым по причине неопределенности отрасли его применения. Апробировались на выгодность применения компьютерного программи-

рования такие сферы, как телекоммуникационные и другие визуальные формы развлечений, шоу-бизнес, реклама.

Успех, реальный экономический эффект в форме доходов от применения Интернета и IT-«продукта» происходит по мере его использования в качестве рыночного ресурса: во-первых, по мере формирования рынка продаж электронного «железа» для формирования инфраструктуры доступа в сеть Интернет; во-вторых, по мере формирования унифицированных условий взаимной выгодности — извлечения доходов как для разработчиков, так и для пользователей IT-продукта; в-третьих, существенным условием послужило создание электронных платежных систем с одновременным превращением формы «живых» денег и бумажных «платежек» в электронную форму банковских пластиковых карт для обслуживания расчетов и транзакций. Особенность этого условия состоит в том, что стала очевидной возможность ускоренной трансляции — перемещения (в том числе трансграничного) как неосязаемых, так и осязаемых ценностей, представленных товарными и денежно-финансовыми потоками. Одновременно возникло также «непредвиденное последствие» — проблема защиты потоков ценностей от несанкционированного присвоения их «продвинутыми» киберактивистами с помощью своих, особо замысловатых, IT-программ.

Статистические данные [6] о темпах роста киберинцидентов позволяют утверждать, что Интернет, будучи виртуальной сферой стремительного распространения информационных технологий, становится инструментом для «продуцирования» пользователями не только позитивных, но и непредвиденных негативных эффектов. Подобные эффекты принято называть объективным действием закона непредвиденных последствий, сопровождающих нововведения, в том числе такие, как информационные технологии. «Внешние эффекты», или чистые издержки информационных технологий, сопровождаются потенциально возможными экономическими потерями от несанкционированного «взлома» киберактивистами систем защиты, проникновения в информационные базы данных с целью хищения денежно-финансовых средств. Многообразные негативные аспекты «внешних эффектов», непредвиденных последствий использования IT-технологий в преступных целях проявляются как в глобальной, так и в национальной системах коммуникаций. Регулирующие ограничения для пользователей Интернета, в том числе в качестве сферы применения информационных технологий для незаконных операций, способны привести к организационным трансформациям и ограничительному регулированию деятельности в этой сфере. Специалисты и обычные пользователи осознают потенциальную возможность и нежелательность таких ограничений. Ограничительные меры способны «расчленить» и превратить глобальную Сеть в малоэффективные ав-

тономные национальные сети, где доступ к иностранным ресурсам будет существенно ограничен [5].

Однако факты, касающиеся незаконной деятельности киберактивистов, действительно производят удручающее впечатление. В настоящее время виртуальная сфера и используемые с помощью Интернета информационные технологии приобретают вид относительно самостоятельной сферы, с помощью которой киберпреступность наносит финансово-экономический ущерб и создает труднорешаемые проблемы и в национальных масштабах, и в глобальной системе стран. Информация о подобных инцидентах поступает с частотой, подобной сводке с какого-нибудь фронта военных действий.

Основой киберпреступности служат те же IT-технологии, но для создания альтернативных, особо «продвинутых» методов цифрового программирования с целью противоправных проникновений, «взлома» и кибератак на различные информационные базы данных. Примечательно, что особо чувствительной сферой выступает денежно-финансовый сектор. Кибератаки здесь связаны с возможностями использования IT-технологий для мошеннических операций, вымогательства или прямого присвоения персональных и корпоративных денежно-финансовых средств или информации об иных ресурсах. Целью преступного использования IT-технологий могут быть программы и операции, связанные с попытками «отмывания» преступных доходов, уклонения от налогов, несанкционированного проникновения в клиентские ресурсы банков, национальных и глобальной платежных систем. Об этом сообщает 91 % пользователей Интернета, подтверждающих как минимум разовую ежегодную попытку вирусной атаки. Остальные 9 % подтверждают факт целевых попыток взлома внутренних систем защиты в компаниях и банках. Так, например, компания *Hold Security* сообщает о сотнях миллионов инцидентов, связанных с хищениями электронных учетных записей и пополнении ими «черного рынка» (в течение нескольких недель подобных случаев набирается до 360 млн). Эксперты указанной компании полагают, что злоумышленники-киберактивисты могут получить доступ к любому сервису, имеющему онлайн-авторизацию. Подобные негативные аспекты проявляются во всё более широких социально-экономических сферах.

В результате нарастает общее недоверие пользователей к сетям, поскольку увеличиваются риски противоправных инцидентов, снижается безопасность интернет-сервисов.

Специалисты «Лаборатории Касперского» в области антивирусной защиты отмечают, что активное использование цифровых устройств наряду с позитивом защиты создает такие возможности для хищения данных, которые в ближайшем будущем способны заменить инсайдерскую разведку. Основой для подобных утверждений

стали данные компании *Kaspersky Security Bulletin* о том, что только в 2013 г. заблокировано на компьютерах и мобильных устройствах пользователей 5,18 млрд атак. «Коллекция» мобильных вирусов насчитывает 148 778 образцов, из числа которых обновлено 104 427 [6]. В течение последних месяцев 2013 г. появилось 19 966 модифицированных телефонных вредоносных кодов, что составляет почти 50 % их объема за весь 2012 г. Особенно интенсивно развивается вредоносное вирусное влияние на персональные компьютеры. Их нарастающему распространению и популярности киберактивисты ежесуточно «адресуют» около 315 000 новых образцов вирусов.

Негативные эффекты IT-технологий приобретают вид цифровых войн, вследствие чего, по мнению аналитиков IT-аутсорсинговых компаний (например, компании *Maykor*), Интернет становится слишком опасным [7].

Цифровые войны и их атакующие представители. На форуме «Открытые инновации», проходившем 1–5 ноября 2013 г., состоялась дискуссия на тему «Киберопасность: как защитить инновации от преступников», где директор антивирусной компании *F-Secure* Микко Хиппонен (Финляндия) также подтверждает фактическое нарастание киберугроз, характеризуя их как потенциальную возможность возникновения цифровых войн. По его мнению, выбор методов защиты зависит от понимания характера преступных целей, ради которых осуществляются кибератаки [8].

Так, трояны-вымогатели — это разновидность киберактивистов, именуемых в интернет-сообществе практически обычными криминальными структурами. Их особенность лишь в том, что они действуют в виртуальном пространстве. Зачастую криминальной целью их «деятельности» является добыча продукции интеллектуальной собственности, связанной со сферой развлечений: новая музыка, кино, сенсационные материалы для средств массовой информации и т. п. Но конечная цель и «демонстрация» этого вида деятельности сводится либо к прямому завладению чужими деньгами, либо к добыче информации о способах завладения ими. К этой же группе относятся противоправные действия, предпринимаемые электронной разведкой, осуществляемой спецслужбами в рамках соответствующих структур государства. Они представлены либо в форме сбора и накопления информации о движении потоков денежных средств, что формулируется в виде благовидных фискальных и подобных целей, либо эта деятельность «по умолчанию» сопровождается и неофициально дополняется коррупционными целями. Фактически этот вид деятельности также провоцирует цифровые войны, поскольку предполагает разработку и применение ответных мер электронной защиты или противодействия информационным методам слежения.

Банковские трояны — другая группа киберактивистов, заражающих компьютеры и ворующих информацию о наличии и движении потоков денег. Они атакуют не банк, а его клиентов с целью завладения их средствами путем переадресации и перевода денег через платежную систему с банковского счета клиента на мошеннические счета криминальных структур. В последнее время особенностью их «работы» является «игра по-крупному», т. е. атакуются не только клиентские счета, но и непосредственно собственные ресурсы банковских учреждений. Интенсификация такого рода атак связана с тем, что клиентские системы дистанционного банковского обслуживания оказались эффективнее защищены. В то же время защита внутренней сети и собственных ресурсов банков требует достаточно дорогостоящей модернизации технологий электронной защиты, стоимость которых варьирует от нескольких миллионов до нескольких десятков миллионов рублей. В 2013 г. более 150 тыс. банковских карт было «скромпрометировано» установленными в банкоматах мошенническими скимминговыми устройствами [9].

Кейлоггеры, или клавиатурные шпионы, — еще одна разновидность киберпреступных структур. Их компьютерные программы разработаны с целью воровства денежных средств владельцев электронных карт банковских клиентов. Компьютерные разработки кейлоггеров способны записывать нажатие клавиш в момент пользования банкоматами, платежными терминалами и иными электронными устройствами банковской инфраструктуры. Запись нажатия клавиш владельцем в момент пользования электронной картой позволяет копировать зашифрованные коды, пароли, номера электронных кредиток и иных личных данных клиентов банка для несанкционированного доступа и прямого воровства наличных денежных средств или их безналичного электронного перевода на счета клавиатурных кейлоггеров. Этот распространенный способ мошенничества называют также скимингом. Злоумышленники крепят к считывающему аппарату банкомата прибор, копирующий данные пластиковой карты клиента банка. Мошенники могут также подглядывать пин-код, используя для этого веб-камеру (за день таким образом можно собрать до сотни данных и остаться незамеченным ни для банков, ни для охраны зданий, где установлены банкоматы). Имея данные карт и пин-код, мошенники либо перепрограммируют любую карту и с ее помощью уже снимают деньги в банкомате, либо списывают средства через Интернет в любой, сколь угодно отдаленной, стране. По данным *Group-IB*, в России мошенничество в сфере интернет-банкинга в 2011 г. достигало 490 млн долл., в 2012 г. было небольшое снижение — до 446 млн долл. Значительную часть составляют потери, понесенные из-за краж со счетов юридических лиц при помощи хакерских атак. Кстати, электронных денег было похищено намного меньше — в

2012 г. только 23 млн долл., а значит, физические лица в меньшей степени интересуют мошенников. По оценкам *Group-IB,* у физлиц в 2012 г. похищено 307 млн руб. По данным Банковской школы (ВШЭ), с банковских карт незаконно снимают до 17 млрд руб. Но сколько именно было похищено с банковских карт клиентов, доподлинно не знает никто. Обобщенную статистику о киберпреступлениях трудно понять, т. к. МВД ее не оценивает в денежном выражении, а заявления потерпевших зачастую попросту не регистрирует.

Ботнеты — еще одна разновидность преступной деятельности, целью которой выступает вирусное инфицирование компьютеров. Специфика методов этой разновидности преступлений состоит в том, чтобы одновременно осуществлять «двойную операцию»: рассылку спама и блокировку работы атакуемого сайта. Преследуется цель «положить» сайт компании (например, интернет-магазина) и блокировать его работу до тех пор, пока владельцы сайта компании не заплатят выкуп за отмену атаки. Аналогичным атакам подвергаются также сайты компаний, для порталов которых критичен фактор времени (торги на электронных торговых площадках, ставки спортивных игр, продажа авиабилетов на текущие рейсы и т. п.). Мошеннические атаки ботнетов вынуждают владельцев официальных сайтов подобных компаний быстро удовлетворять требования вымогателей для сокращения потенциального ущерба, определяемого угрозой проигрыша в условиях ограниченного времени проведения торгов на электронных площадках, изменений результатов спортивных или азартных игр, задержки авиарейсов и т. п.

Хакеры от группировок ботнетов заражают также компьютеры пользователей, заходящих и часто посещающих некоторые, например новостные, сайты. Здесь целью вирусной атаки может оказаться любой сайт со многими посетителями.

Ботнеты, как и другие трояны-вымогатели, блокируют электронные системы до тех пор, пока не будет выполнено требование компьютерных преступников по переводу средств на указанные ими счета. Некоторые трояны настолько сильны, что разблокировать деловую информацию предпринимательских компаний зачастую невозможно, не заплатив по требованиям хакеров. В настоящее время одним из наиболее известных троянов-вымогателей является *Cryptoloker*, который действует массово, но относительно мелкими вымогательствами в пределах 300 долл. за разблокировку информации деловой компании. До настоящего времени данную группировку практически не удается нейтрализовать.

К способам «работы» киберпреступников относятся такие, как установление троянами своих программ на банкоматы и *POS*-терминалы; используются также установки фальшивых *POS*-терминалов в торговых точках для кражи и передачи данных платежных карт; растут

хищения с банковских счетов вследствие заражения мобильных устройств пользователей.

BitCoin Miner — одна из новейших разновидностей цифровых систем, созданных в 2006–2009 гг. для «продуцирования» и использования в платежной системе виртуальной валюты нескольких модификаций. Система двухкомпьютерных программ *BitCoin Miner* основывается на использовании умноженной процессорной мощности, которая может быть достигнута объединением нескольких персональных компьютеров *(pool).* Одна из компьютерных программ *BitCoin Miner* предназначена для майнинга *(mining),* т. е. «продуцирования» виртуальной валюты и ее хранения в электронном кошельке игрока-владельца; другая — для использования в платежной системе накопленных виртуальных денег (*BitCoin, Litecoin* и пр.) [10].

Накопленные единицы виртуальной криптовалюты могут использоваться в операциях обмена (интернет-трейдинг) практически на любую реальную валюту (в том числе доллары, евро, российские рубли и др.) на виртуальной обменной бирже валют. График торгов на обменной виртуальной бирже обновляется ежечасно.

Возможно также использование криптовалют типа биткоин, лайткоин и др. (*BTC, LTC*) для расчетов и платежей как в системе интернет-магазинов, так и в стационарной торговле разнообразными товарами и услугами. В столицах и провинциальных городах многих странах мира (от Лондона, Парижа и Москвы до Владивостока, Токио, Нью-Йорка и др.) применялась возможность использования виртуальной валюты при наличии у пользователя обычного персонального компьютера, доступа в Интернет и, разумеется, соответствующего навыка работы в подобных цифровых программах.

Каждое из перечисленных направлений кибератак заслуживает особого анализа для выработки применяемых мер защиты, их координации и оценки результативности.

Примечание. «Чтобы оценить масштаб проблемы, Центробанк ввел новую форму отчетности для банков для отражения всех инцидентов с денежными переводами, — пояснила «Эксперт Online» первый вице-президент Российского клуба финансовых директоров Тамара Касьянова. Но проблема в том, что многим банкам невыгодно показывать слабость своих систем защиты перед регулятором, который к тому же публикует итоги мониторинга, а это уже имиджевые потери. В итоге только 100 банков из более чем тысячи в июле-декабре прошлого года вообще заявили о таких инцидентах. Лишь у 3 % банков оказалось число таких инцидентов более 100, у остальных — якобы единицы».

В цифровых войнах достаточно затруднительно выявление сферы и источника происхождения киберпреступлений. Сфера происхождения хакерских атак интернациональна — это территория практически

большинства стран мира. К ним относятся Англия, Финляндия, Ирландия, Канада, Италия, страны СНГ, Балтии, Румыния, Китай, Бразилия, а также Саудовская Аравия, где сравнительно недавно была арестована крупная «интернациональная» группа киберактивистов. В основном они «специализировались» на краже номеров кредиток и рассылке спама. Но подобные виды мошенничества труднодоказуемы, и наказание за них чаще всего оказывается незначительным. Киберпреступники стараются не привлекать внимание правоохранительных органов тех стран, в которых они проживают. Например, российские хакеры не инфицируют компьютеры на территории России во избежание отслеживания и ареста российской полицией. Это обычная практика для хакеров всех стран.

Противодействие цифровым войнам ведется по нескольким основным направлениям. Одни из них ориентированы на усиление IT-методов защиты, в частности, с помощью облачных технологий, другие — на поиск оптимальных законодательных мер регулирования Интернета в отдельных странах, а также на формирование межгосударственной политики противодействия киберпреступности в глобальном масштабе. Однако и те и другие методы имеют свои недостатки. Так, главные претензии к облачным технологиям связаны с безопасностью (достаточно ли надежно защищены данные в облаке? И нет ли вероятности того, что сам владелец дата-центра решит воспользоваться доверенными ему данными?). Возникновение облачных технологий в некоторой мере означает моральное старение способов использования существующей информационной инфраструктуры с ее программными платформами и ПО. Их новизна заключается в обновлении функций предложения и использования уже известных IT-технологий, поскольку перечисленные сервисы позволяют пользователям с выгодой для себя «замещать» информационную инфраструктуру их собственных компьютеров, программно-аппаратные платформы и программное обеспечение. Недостатки облачных технологий, по существу, сводятся к следующему. Во-первых, существует некоторая зависимость пользователей облачных услуг от их поставщиков, что напоминает своеобразный вид монополизма. Во-вторых, известно, что при хранении данных на собственном компьютере пользователь в любое время может отключиться от Сети и очистить систему с помощью антивируса. А облачные услуги хотя и повышают степень сохранности пользовательских данных от компаний, но не гарантируют 100-процентную защиту от кибератак. Объективно это гарантировать невозможно, и потенциал риска несанкционированного проникновения полностью не устраняется. Следовательно, для поставщика услуг, как и для их потребителя, сохраняется необходимость всегда находиться онлайн. В-третьих, в дальнейшем возможна монетизация ресурса (т. е. ком-

пания вполне может начать взимать плату за предоставление тех или иных услуг или их совокупности). Использование технологий частного облака может применяться для снижения рисков благодаря шифрованию и иным существующим способам электронной защиты, в том числе бизнес-критичных данных. При этом особо уязвимыми могут быть данные, хранящиеся в так называемом публичном облаке единого информационного пространства.

Что касается законодательно-правовых ограничений, то с ними связано не меньше проблем. Эти меры требуют рассмотрения других аспектов и изучения достаточно обширного материала, анализа специфики задач и оценок эффективности соответствующих структур и выполняемых ими функций. Подобный анализ должен быть предметом отдельного исследования деятельности соответствующих правовых структур и законодательных основ их деятельности. К таким структурам относятся, например, Межведомственная рабочая группа по противодействию киберпреступлениям в сфере экономики; межправительственная Группа разработки финансовых мер борьбы с отмыванием денег в глобальных масштабах (ФАТФ); «Стратегии XXI» как новая идеология развития IT-технологий. Предпринимаются меры ограничительного регулирования оборота электронных денег, предложенные соответствующим комитетом Госдумы РФ по финансовому рынку; регулирования национальных и глобальной сетей Интернет и др.

Сфера IT-технологий, как правило, настороженно реагирует на формирование законодательных, административно-правовых мер вмешательства и регулирования ее деятельности. В качестве альтернативы этой сферой вырабатываются свои, все более изощренные, методы и программы электронно-цифровой защиты.

Перечисленные меры требуют более глубокого анализа, широкого обсуждения научной общественностью и могут быть заявлены в качестве отдельной темы публикации.

ЛИТЕРАТУРА

[1] *Российский статистический ежегодник.* URL: http://www.gks.ru/bgd/regl/b13_13/ IssWWW.exe/ Stg/d3/19-01.htm (дата обращения 03.09.2014).

[2] Россия в цифрах. 2012 г. *Российский статистический ежегодник*, с. 319–320. URL: http://www.gks.ru/bgd/regl/b13_13/IssWWW.exe/ Stg/d3/19-11.htm (дата обращения 03.09.2014).

[3] Рагимова С. Цифровые технологии для бизнеса. *Тематическое приложение «Коммерсант»*, 2013, № 61, 12 октября, с. 3–4.

[4] Ускова О. *Ведомости*, 2014, № 6 (3510), 20 января, с. 8–9. URL: http://www.Vedomosti.ru

[5] Алексеев М. Фонд содействия развитию технологий и инфраструктуры Интернета. *РБК daily*, 2013, № 230 (1763), 11 декабря, с. 1, 8. URL: http://www.rbcdaily.ru

[6] Гостев А. Лаборатория Касперского — Kaspersky Security Bulletin. *РБК daily*, 2013, № 230 (1763), 11 декабря, с. 1, 8. URL: http://www.rbcdaily.ru
[7] Юзбекова И., Волков Д. Интернет стал слишком опасным. *РБК daily*, 2013, № 230 (1763), 11 декабря, с. 1, 8. URL: http://www.rbcdaily.ru
[8] Хиппонен М. Киберопасность: как защитить инновации от преступников. *РБК daily*, 2013, № 204 (1737), 5 ноября, с. 9. URL: http: //www.rbcdaily.ru
[9] Терновская Т. Хакеры стали играть по-крупному. *РБК daily*, 2013, № 236 (1769), 19 декабря, с. 8. URL: http: //www.rbcdaily.ru/finance/56294999029525
[10] *Виртуальная биржа — обменник криптовалют*. URL: http://www.relay.rutvnet.ru; www.Litecoin.org.ru

Статья поступила в редакцию 05.09.2014

Ссылку на эту статью просим оформлять следующим образом:
Родионова В.Г. Информационные технологии в экономике: тенденции и проблемы непредвиденных последствий. *Гуманитарный вестник*, 2014, вып. 5.
URL: http://hmbul.bmstu.ru/catalog/ecoleg/econom/201.html

Родионова Валентина Георгиевна — канд. экон. наук, доцент МГТУ им. Н.Э. Баумана. Лауреат премии Правительства РФ (2002). Соавтор проекта программы и современного стандарта экономического образования. Соавтор учебников «Экономика» кафедры «Экономическая теория» и «Микроэкономика» Финансовой академии при Правительстве РФ, автор учебных пособий «Макроэкономика», «Микроэкономика», «Экономическая теория» и др. (28 учебно-методических и научных работ). Область научной деятельности и научных интересов: инновации и IT-технологии как фактор динамической эффективности экономики. e-mail: avroro2@mail.ru

Information technology in the economy: trends and issues of unintended consequences

© V.G. Rodionova

Bauman Moscow State Technical University, Moscow, 105005, Russia

The tendencies and problems of using information technology in the sectors of the Russian economy are considered. Statistical data show an increase in the share of industrial organizations, using mainly local systems based on the information technologies. In the fields of finance, banking, payment systems, commerce and leisure industry digital technology are spreading most rapidly, but are being accompanied by unforeseen consequences, the effects of which have been called "digital war".

***Key words**: information technology (IT), digital (information) wars, law of unforeseen consequences, static efficiency, dynamic efficiency.*

REFERENCES

[1] *Rossiyskiy statisticheskiy ezhegodnik* [Statistical Yearbook of Russia]. Available at: http://www.gks.ru/bgd/regl/b13_13/IssWWW.exe/Stg/d3/19-01.htm (accessed on 03.09.2014).

[2] *Rossiyskiy statisticheskiy ezhegodnik* [Statistical Yearbook of Russia], pp. 319–320. Available at: http://www.gks.ru/bgd/regl/b13_13/IssWWW.exe/Stg/d3/19-11.htm (accessed on 03.09.2014).

[3] Ragimova S. Tsifrovye tekhnologii dlya biznesa [Digital Technologies for Business]. *Topical annex "Kommersant"*, 2013, no. 61, October 12, pp. 3–4.

[4] Uskova O. *Vedomosti — Bulletin*, 2014, no. 6 (3510), January 20, pp. 8–9. Available at: http://www.Vedomosti.ru

[5] Alekseev M. *RBK daily*, 2013, no. 230 (1763), December 11, pp. 1, 8. Available at: http://www.rbcdaily.ru

[6] Gostev A. *RBK daily*, 2013, no. 230 (1763), December 11, pp. 1, 8. Available at: http: //www.rbcdaily.ru

[7] Yuzbekova I., Volkov D. *RBK daily*, 2013, no. 230 (1763), December 11, pp. 1, 8. Available at: http: www.rbcdaily.ru

[8] Khipponen M. *RBK daily*, 2013, no. 204 (1737), November 5, pp. 9. Available at: http: //www.rbcdaily.ru

[9] Ternovskaya T. *RBK daily*, 2013, no. 236 (1769), December 19, pp. 8. Available at: http: www.rbcdaily.ru/finance/ 56294999029525

[10] *Virtualnaya birzha — obmennik valut* [Virtual Exchange — Cryptocurrency exchanger]. Available at: http: www.relay.rutvnet.ru; www.Litecoin.org.ru

Rodionova V.G., Ph. D., assoc. professor of the Economics Department at Bauman Moscow State Technical University. Awarded with the prize of the Government of the Russian Federation (2002). Co-author of the draft program and modern standard for the economic education. Co-author of the textbook "Economics" of the Economics Department and textbooks of the Finance Academy under the Government of the Russian Federation ("Microeconomics"); the author of electronic publications and printings of textbooks, "Macroeconomics", "Microeconomics". Research interests: innovations and IT-technologies as a factor in the dynamic efficiency of the economy. 28 educational and scientific papers are published. e-mail: avroro2@mail.ru