

Информационные технологии: асоциальные факторы риска

IT: Asocial Risk Factors

Інформаційні технології: асоціальні фактори ризику

*О. С. Булычева,
Фирма «ІС», Москва, Россия
О. В. Сютюренко
ВИНИТИ РАН, Москва, Россия*

*Olga Bulycheva
IC Company, Moscow, Russia
Oleg Syuntuurenko
All-Russian Institute of Scientific and Technical Information
of the Russian Academy of Sciences,
Moscow, Russia*

*О. С. Буличова,
Фірма «ІС», Москва, Росія
О. В. Сютюренко
ВІНІТІ РАН, Москва, Росія*

Показана актуальность проблемы потенциальных негативных последствий применения информационных технологий в социальной, экономической, научно-технической сферах. Проблема ИТ-рисков является часть более общей проблемы технологических рисков в целом. Сформулированы цели и задачи социальной оценки техники и социотехнического проектирования и как нового междисциплинарного научного направления. Показано, что информационная неопределенность является средой появления риска. Сформулированы актуальные задачи разработки проблематики рисков развития информационных технологий.

Actual problem of potential negative consequences of IT use in social, economic, and science and technical sphere is described. The problem of IT risks is a part of general problem of technological risks. The aims and purposes of social evaluation of technology, and social and technical design as a new interdisciplinary scientific field are described. It is shown that informational uncertainty is environment for risk appearance. Actual purposes of development of problems of IT development risks are stated are defined.

Показана актуальність проблеми потенційних негативних наслідків застосування інформаційних технологій в соціальній, економічній, науково-технічній сферах. Проблема ІТ-ризиків є частиною більш загальної проблеми технологічних ризиків в цілому. Сформульовано цілі та завдання соціальної оцінки техніки і соціотехнічного проектування як нового міждисциплінарного наукового напрямку. Показано, що інформаційна невизначеність є середовищем появи ризику. Сформульовано актуальні завдання розробки проблематики ризиків розвитку інформаційних технологій.

Информационное общество и лежащие в его основе технологии обладают огромным и уже бурно реализующимся потенциалом влияния на жизнь человека и общества /2/. Является ли это влияние заведомо позитивным; помогает ли оно автоматически выводу на траектории устойчивого развития цивилизации; не содержит ли в себе развитие информационно-коммуникационных технологий дополнительных (новых) источников неустойчивости и *рисков*? Эти вопросы приобретают все большую актуальность глобального характера в условиях нарастающего мирового экономического кризиса.

Проблема *рисков* развития информационных технологий является частью более общей проблемы технологических *рисков* в целом /10/. Исследование технологических *рисков* традиционно считалось прерогативой конкретных научно-технических дисциплин, связанных с созданием и исследованием новой техники и технологий. Ситуация в последние десятилетия, однако, кардинально изменилась. Это связано, прежде всего, с тем, что *риски* от внедрения и эксплуатации сложных

технических систем перестали быть, строго говоря, техническими, а стали социотехническими. Все виды современной техники, однако, имеют как положительные, так и отрицательные для общества последствия и несут в себе технологические, экологические и социальные *риски*. Ветряные электростанции портят ландшафт, создают шум и низкочастотные вибрации в почве, мешают перелетам птиц. Гидроэлектростанции повреждают планктон и мешают нересту рыб, и, как показала авария на Шушенской ГРЭС, могут стать причиной серьезных техногенных катастроф.

Природные катастрофы ведут к техногенным катастрофам, а техногенные катастрофы становятся социальными катастрофами. Это показала авария на Фукусиме. До сих пор на первый план выступал человеческий фактор – ошибки операторов, недоработки конструкторов и т.п. Теперь стало очевидно, что дело не только в этом. Непредсказуемыми и часто необратимыми оказываются последствия искусственного вторжения в естественную сферу. Атомная техника, химическая технология и геновая инженерия особенно глубоко внедряются в природные процессы и структуры, создавая новые комбинации чуждых «первичной» природе материалов, элементов и организмов. Человечество не в состоянии прогнозировать в долгосрочной перспективе ни климатические изменения, ни возможные природные катаклизмы, что увеличивает вероятность техногенных катастроф, вызванных природными катастрофами. Изменение соотношения социальных и технологических перемен в современном обществе вызывает рост осознания технологических *рисков*, связанных с внедрением и эксплуатацией сложных системотехнических комплексов, электростанций, производства потенциально токсичных субстанций, возрастанием ощущения экологических угроз со стороны неконтролируемо разрастающихся масштабов фактически новой индустрии, системной составляющей которой являются информационные технологии.

Современные представления о *риске* отличаются многообразием. Понятие «риск» впервые было определено в словаре В. И. Даля. Существует множество определений *риска*, в основном в финансово-экономической сфере.

В рамках данной работы авторы считают наиболее приемлемым (и кратким) следующее определение: *Риск – это потенциальная возможность получить в условиях осознаваемой и будущей неопределенности заранее неизвестный результат негативного характера.*

Необходимо подчеркнуть, что информационная неопределенность (отсутствие информации о возможных состояниях системы, о внешней среде и т.п.) является средой появления *риска*. Проблемы разработки и функционирования программно-математического обеспечения в принципе отличаются от большинства технических проблем. Основной фактор *риска* связан с тем, что существуют фундаментальные причины, в силу которых программное обеспечение нельзя сделать настолько надежным, чтобы можно было не сомневаться в том, что не возникнут нештатные ситуации и несанкционированная работа систем. При этом *риски* растут с ростом масштабов и сложности системотехнических комплексов.

Применение современных информационных технологий потенциально создает предпосылки *риска* утечки, хищения, утраты, искажения, подделки, копирования и блокирования информации и, как следствие, экономического, экологического, социального и других видов ущерба [1,6]. В разных странах регулярно регистрируются попытки 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 как самих информационных систем и систем защиты, так и объектов управления.

По данным компании «eMarketer» пользователями Интернета в 2012 г. станут 43% россиян (~59 млн. чел.), заходящие в Сеть хотя бы раз в месяц. Информатизация общества порождает много новых и тревожных проблем в социальной сфере. Использование информационных технологий в политической области существенно влияет на практику демократии, изменяет отношения между властью и гражданами, порождает новые необычные проблемы (политические манипуляции через Интернет) и знаменует наступление эпохи «компьютеризованной политики».

Изначальная интерактивность Интернета и появление так называемых социальных сетей способствует развитию таких явлений, как сектантское проповедничество, появление юношеских суицидальных групп (например, «ВКонтакте»), распространение мистических и эзотерических учений и практик, магии, целительства и т.п. Новые технологии мультимедиа и виртуальной реальности вовлекают человека в новые формы существования и в определенной мере могут оказывать воздействие на формирование личности. Как результат, происходит рост *риска* социальной и личностной дезадаптации и разрушения психики человека. Возрастают *риски* деформации общественной нравственности и морали, вызванные неконтролируемым распространением в сети Интернет непристойных, порнографических видеоматериалов. Интернет служит весьма удобной площадкой для подготовки и осуществления информационно-террористических и информационно-криминальных действий. Распространяются пропагандистские материалы преступных организаций, рецепты изготовления взрывчатых и ядовитых веществ, оружия, наркотических и психотропных средств, рост «темного флешмоба». Отсутствие географических границ, трудно определяемая национальная принадлежность объектов сети, возможность анонимного доступа к ее ресурсам – все это повышает *риски* уязвимости общественной и личной безопасности.

Проблема минимизации *рисков* внедрения информационных технологий является, в определенном смысле, частью более общей проблемы социальной оценки научно-технического развития. Следует констатировать, что на современной стадии научно-технического развития естественнонаучное знание не способно все предвидеть, что можно лишь предусмотреть определенную степень *риска* новых, в частности, информационных технологий и необходим так называемый «сценарный подход» для реализации которого недостаточно лишь естественнонаучных и технических знаний, но необходимы также социально-гуманитарные знания и методы. Социальная оценка научно-технического развития проводится сегодня во многих развитых западноевропейских странах, где она институализирована в виде различных организационных форм при парламентах или правительствах, с целью научной поддержки принимаемых решений в области научно-технической политики /5/. Цели и задачи социальной оценки научно-технического развития:

- раннее предупреждение *рисков* новых технологий и техники;
- разработка проблематики их оценки;
- предупреждение и преодоление конфликтов;
- разработка рекомендаций по минимизации *рисков* и улучшению основы поиска решений (с позиций междисциплинарного и трансдисциплинарного подхода).

В Евросоюзе функционирует сетевая структура оценки техники (www.netzwerk-ta.net), куда входят различные организации Германии, Австрии, Швейцарии, которые провели в течение последних нескольких лет четыре конференции по данной проблематике. Последняя конференция, проходившая в Берлине в 2010 г., была посвящена, в основном, методологическим проблемам оценки технологических *рисков* /8/. Следует отметить, что, по мнению многих экспертов, одной из междисциплинарных сверхзадач XXI века является управление *риском* и безопасностью сложных систем. Отчасти в этой связи компьютерное моделирование, прогнозирование, применение высокопроизводительных вычислительных систем стало одним из основных направлений в ведущих странах мира /4/.

Наиболее актуальными задачами в разработке проблемы рисков развития ИТ представляются следующие:

- I. Разработка методов классификации и систематизации *рисков* применения информационных технологий на основе таксономии. Роль таксономии *рисков* на этапах разработки и реализации технологий состоит в том, что она должна позволять разным категориям специалистов, экспертов, программистов оценивать *риски* в самых разных аспектах: по значимости потенциальных негативных последствий; по различным факторам *риска* (сложности, времени и др.); по структурным и функциональным составляющим системы; по категориям потерь.
- II. Разработка принципов, методов и рекомендаций определения и оценки *рисков* (2) на основе системного подхода, системного анализа, методов социотехнического проектирования, имитационного моделирования, теории «нечетких» множеств.

III. Исследование и мониторинг негативных политико-правовых последствий информатизации, таких как: усиление социально-политического контроля над обществом и личностью; появление «компьютерного бюрократизма»; широкое распространение компьютерной преступности; информационные воздействия, деформирующие нормы морали и нравственности.

IV. Исследование и производство отечественного программного обеспечения, в том числе на основе «облачных вычислений», а также с открытым исходным кодом, и сокращение технологической зависимости (и *рисков*) России в этой области.

В заключение, несколько выходя за рамки рассматриваемой проблематики, хотелось бы сделать одно замечание более общего характера. Россия не является лидером в сфере информационных технологий. С учетом нарастающих тенденций объединения информационных и вычислительных ресурсов многих стран в глобальные сети следует иметь ввиду возможность трансформации традиционных проблем *рисков* ИТ (в первую очередь, компьютерных систем критических приложений) в проблему минимизации *рисков* от «компьютерного силового давления» /9/. Очевидно, что отказ от интеграции и возможностей использования глобального информационного пространства в постиндустриальных условиях формирования информационного общества невозможен. В то же время, неконтролируемая интеграция в глобальную телекоммуникационную (информационную, вычислительную) инфраструктуру без комплексного решения проблем компьютерных *рисков* может привести к далеко идущим последствиям, связанным с утратой национальной информационной независимости (последним ярким примером является неудача со станцией «Фобос-грунт» в 2011 г., стоимостью 5 млрд. руб., из-за использования импортных чипов). Поэтому стратегия развития информационной инфраструктуры и информационных технологий в нашей стране должна сочетать максимальное использование возможностей поиска, обмена, обработки информации в сетевых пространствах с минимизацией *рисков* негативного влияния на отечественные научно-технические информационные ресурсы, крупные проекты и программы, прежде всего, в сфере высоких технологий.

Литература

1. Смолян Г.Л. Сетевые информационные технологии и проблемы безопасности личности// Вестник РФФИ. 1999. № 3(17). С.: 63–68.
2. Сюттюренко О.В. Информационное общество и информатизация науки// Вестник РФФИ. 1999. № 3(17). С.: 4–7.
3. Малинецкий Г.Г. Сценарии, стратегические риски, информационные технологии// Информационные технологии и вычислительные системы. 2002. № 4. С.:83–108.
4. Сюттюренко О.В. Инфраструктурные вопросы развития и использования высокопроизводительных вычислений в научных исследованиях// Информационные технологии и вычислительные системы. 2002. № 4. С.:77–82.
5. Горохов В.Г. Философия техники как теория технической деятельности и проблемы социальной оценки техники// Философские науки. 2006. № №1,2,3,4.
6. 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.
7. Булычева О.С., Сюттюренко О.В. Техничко-экономические аспекты программного обеспечения с открытым кодом// Материалы XV конференции представителей региональных научно-образовательных сетей. RELARN-2008, 1–8 июня. – М.: Ассоциация РЕЛАРН, 2008. – С.: 107–110.
8. В.Г. Горохов, А.С. Сидоренко, Роль теоретических исследований в развитии новейших технологий// Вестник РАН. 2009. Том 79. № 9. С.:807–815.
9. Сюттюренко О.В., Борисова Л.Ф. Проблемы информационного обеспечения научно-инновационной сферы: новые концептуальные подходы// Научно-техническая информация. Сер.1. 2009. № 4. С.: 9–12.
10. Горохов В.Г. До и после Чернобыля: технический оптимизм и социальный пессимизм// Философские науки. 2011. № 6.С.:25–33.