

Горохов В.Г., Сюттюренко О.В. 

---

## ТЕХНОЛОГИЧЕСКИЕ РИСКИ: ИНФОРМАЦИОННЫЕ АСПЕКТЫ БЕЗОПАСНОСТИ ОБЩЕСТВА

***Аннотация:** Технологический риск понимается по-разному не только в различных областях, но и в рамках одной области техники. Проблема технологических рисков в области информационных технологий в современном обществе знания приобретает ярко выраженный социальный характер. Информатизация, конвергенция компьютерных, телекоммуникационных технологий и мультимедиа обеспечивают принципиально новый уровень цивилизационного развития, все более влияя на жизнь человека и общества. 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 новых источников неустойчивости и угроз. Все эти вопросы требуют специального в том числе и социально-гуманитарного исследования и обсуждения. Строящееся общество знаний принципиально амбивалентно. Современное общество становится полем перманентного экспериментирования с новыми информационными технологиями, следствия которого могут быть не только позитивными, но и негативными как для общества в целом, так и для отдельных его граждан.*

***Ключевые слова:** технологические риски, информационная безопасность, общество знания, информационные технологии, негативные последствия, экспертократия, технократия, информатика, информационное общество, интернет*

Технологический риск понимается по-разному не только в различных областях, но и в рамках одной области техники [16]. Причем риск новых технологий часто не осознается сразу и требуется определенный период времени для выявления точек риска. В особенности это относится к новейшим информационным технологиям, часто первоначальное эйфорическое отношение к которым по прошествии определенного времени сменяется резко критическим осознанием последствий их применения и главное социальной и психологической зависимости от них. Например, совершенно очевидно, что свободный доступ к информации приводит к разрушению тоталитарной системы и уничтожению основы для доминирования технократии, поскольку основой их является исключительное право правящей элиты на владение недоступной другим информацией, которая проходит по, так называемым, закрытым каналам. По открытым же каналам цир-

## Технологические риски: информационные аспекты безопасности общества

---

кулирует или неполная или заведомо фальсифицированная информация. Такая ситуация, однако, приводит, в конечном счете, к потере даже высшими эшелонами власти информирования о реальном положении дел в обществе. Информатизация, конвергенция компьютерных, телекоммуникационных технологий и мультимедиа обеспечивают принципиально новый уровень цивилизационного развития, все более влияя на жизнь человека и общества. 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 угроз мировому сообществу (и национальной безопасности России). Эти вопросы приобретают все большую актуальность в условиях устойчивых тенденций глобализации мировой экономики (и перманентного мирового экономического кризиса), бурного развития информационных технологий, масс-медиа и сетевой информационной среды [1].

Таким образом, свободный доступ к информации и участие населения в обсуждении крупных технических проектов, с одной стороны, создает условия для преодоления господства экспертократии. Но, с другой стороны, появляются новые возможности возрождения технократического мышления в электронном обществе: манипулирование общественным мнением через электронные средства масс-медиа и Интернет, тенденциозное представление и искажение информации, спекуляция на «чувствах» среднестатистического гражданина и доверии к науке и средствам массовой информации, подтасовка «фактов» и создание иллюзии их «научного» обоснования и т.п. 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 [2-5]. В разных странах регулярно регистрируются попытки проникновения в информационные системы органов государственной власти и управления, факты несанкционированного распространения и использования персональных данных, кражи и уничтожения экономической и финансовой информации, программного обеспечения систем электронных платежей. 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, объектов управления, возникновению социальной напряженности (по данным компании «Marketer» пользователями Интернета являются ~ 60 млн. россиян, заходящих 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, в сети «ВКонтакте»), распространение мистических и эзотерических учений и практик, магии, целительства и т.п. Новые технологии мультимедиа (игры) 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 разрушения психики человека. Возрастает уровень угроз деформации общественной нравственности и морали, вызванный 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» /6/. Отсутствие географических границ, трудно определяемая национальная принадлежность объектов сети, возможность анонимного доступа к ее ресурсам – все это повышает уровень уязвимости общественной и личной безопасности.

Сейчас все более актуализируется проблем потенциальных угроз использования информационных технологий в военно-космической области (прежде всего в программах ПРО и СОИ). Проблемы разработки и функционирования программно-математического обеспечения в принципе отличаются от большинства технических проблем. Основной фактор угроз безопасности связан с тем, что существуют фундаментальные причины, в силу которых программное обеспечение нельзя сделать настолько надежным, чтобы можно было не сомневаться

## Технологические риски: информационные аспекты безопасности общества

---

ся в том, что не возникнут нештатные ситуации и несанкционированное применение ракетно-ядерного оружия. Причем уровень угроз растет с ростом масштабов и сложности военных системотехнических комплексов. В настоящее время проблема усугубляется как бурным развитием новых сетевых технологий, так и активной разработкой и внедрением роботизированных систем и систем искусственного интеллекта в различных военно-технических системах. В последнее время все более начинает осознаваться новый (и, возможно, самый опасный) вид угроз – разрушение способов и форм идентификации личности в результате длительного информационно-психологического воздействия, т.н. консциентальная война (от латин. *conscientia* – «сознание») [9], что означает переструктуризацию внутреннего мира личности. В современном однополярном мире США в своей геополитической стратегии с целью установления цивилизационного контроля над другими странами и культурами используют массовую культуру, транслируемую средствами массовой информации и разрушающую ценности традиционного общества, т.е. используют информационное оружие, для которого нет преград в век спутниковой глобальной связи. В рамках процессов глобализации консциентальная война предполагает, что мир вступил в новый этап борьбы – конкуренции форм организации сознаний, где предметом поражения и уничтожения являются определенные типы сознаний. В результате длительного информационно-психологического воздействия определенные типы сознаний должны быть стерты, перестать существовать. А носители этих сознаний, наоборот, могут быть сохранены, если они откажутся от форм сознания – объектов разрушения и поражения. Типы сознаний – объекты поражения в консциентальной войне – должны быть вытеснены за рамки цивилизационно допустимых и приемлемых форм. Это происходило и раньше, когда один тип организации сознания вытеснял другой (как, например, христианство сменило язычество). Но с развитием информационных технологий эта конкуренция и борьба принимает тотальный характер. Очень важно понимать, что уничтожение определенных типов сознания предполагает разрушение и реорганизацию общностей, которые конституируют данный тип сознания [9]. В современной научной, научно-популярной литературе имеется целый ряд публикаций, посвященных эффективным разновидностям консциентального оружия, разрабатывающихся в XX веке и эффективно применяющихся на практике.

В современной консциентальной войне можно выделить несколько основных технологий, которые ориентированы на поражение и разрушение сознания.

Во-первых, посредством дезинтеграции и примитивизации информационно-коммуникативной среды, где функционирует и развивается сознание, достигается понижение уровня ее организации. Во-вторых, на основе специальных технологий (психотехнологий) по каналам коммуникации распространяют образы и тексты, которые разрушают работу сознания. В-третьих, технологии, нацеленные на разрушение способов и форм идентификации личности по отношению к фиксированным общностям, что приводит к смене форм самоопределения и к деперсонализации. . В основном с коммерческими целями (реклама) широко используются технологии второго типа – неосознаваемого внушения во время общения индивида с компьютером или телевизором. В это время его внутренний мир открыт и совершенно незащищен, в него можно вводить незаметно для человека необходимую манипулятору информацию без его ведома, которая усваивается им, как пища, и становится своей, т.е. определяет его потребности, желания, вкусы, взгляды, картину мира [10]. По оценкам отечественных и зарубежных специалистов, сеть Интернет как среда поиска и обмена информацией все более приобретает роль глобального инструмента ведения психологической войны. Технологии третьего типа становятся средством разработки и использования нового инструмента массового воздействия, оно наиболее часто и эффективно используется. Фактически социум существует в ситуации его постоянного и тотального давления. Данный тип воздействий по смене и трансформации типов имидж-идентификаций и аутентизации весьма эффективно осуществляют средства массовой информации, в первую очередь телевидение. Вследствие этого гипотетически существует тоталитарный сценарий развития информационного общества, при котором с помощью уже имеющихся и новых информационных технологий может быть установлен тотальный контроль за распределением и потреблением информации, а также за личностью, вмешательство в частную сферу государства или криминальных структур, установление диктата транснациональных корпораций по отношению к объединениям граждан и даже национальным государствам [11].

Современное общество становится полем перманентного экспериментирования с новыми информационными технологиями, следствия которого могут быть не только позитивными, но и негативными как для общества в целом, так и для отдельных его граждан, которые поневоле становятся подопытными субъектами и объектами различных злоупотреблений. В глобальном информационном обществе, с одной стороны, неизмеримо возрастают возможности быстрого рас-

## Технологические риски: информационные аспекты безопасности общества

---

пространения информации и возможности реагирования на нее, а с другой – развиваются новейшие также информационные средства подтасовки или одностороннего выгодного для технократического лобби представления данных. Такого рода технократическую тенденцию Х. Ленк называет «системной технократией» [15, р. 145]. Ленк связывает ее с господством включенной в новейшие средства электронной коммуникации бюрократии, что сигнализирует приход электронного «старшего брата» и становится реальной опасностью для дальнейшего демократического развития общества. Здесь он указывает на одну из важнейших проблем – несанкционированного коммерческого и общественного использования персональных данных, что составляет угрозу личностной сфере [14, с. 73-74]. В условиях тоталитарного режима сама идея политической, юридической и даже моральной ответственности не могла возникнуть. Любая информация, как о позитивных, так и негативных следствиях внедрения новейших технологий объявляется секретной и никогда не разглашается средствами массовой информации. Если же такая информация все же попадает к журналистам, она подвергается жесткой цензуре, прежде чем сможет быть опубликованной. В демократическом обществе появляется возможность публикации такого рода информации, но технократическое лобби именно в условиях становления нового информационного общества получает в свое распоряжение различные (в том числе и электронные) возможности дезавуировать эту информацию, объявить ее политически или научно нерелевантной. Обычному гражданину, однако, очень трудно понять научные и технические детали сложных проектов, отличить важные данные от неважных, правдивую информацию от полуистинной или ложной. Проблема усложняется еще и тем, что сами ученые и инженеры недостаточно информированы о социальных, политических, экологических, нравственных и т.п. следствиях внедрения их проектов. Для этого требуются проводить специфические исследования и особые специалисты, причем не только из научно-технической, но и социально-гуманитарной сферы. Развитие информационного общества требует и новых форм участия общественности в принятии политических решений, причем информационное общество создает не только новые возможности для расширения такого участия, но для манипуляции распространяемой через Интернет, телевизионные каналы и т.д. информацией и с ее помощью общественным мнением.

Теоретическая информатика и континуум информационных технологий образует сегодня целый узел дисциплин, начиная от когнитивных наук с преимущественно психологической ориентацией и кончая системно ориентирован-

ной кибернетикой, от нейронауки до технических наук. Появились ростки Семантического Интернета, то есть Интернета следующего поколения с преобладанием семантических принципов управления и поисков контента – ONTONET [12]. Возможности ONTONET существенно шире semanticWeb, поскольку не ограничиваются только Интернет сетевым обеспечением, а предполагает глобалистическое семантическое управление на единой онтологической платформе обширными разнообразиями компьютерно-сетевых решений. Необходимо также отметить выраженный тренд роста деструктивных сетевых социальных структур. Перед современным обществом стоят жизненно важные задачи адаптации человека к условиям существования и деятельности в информационной среде, характер взаимодействия с которой претерпевает существенные изменения на всех уровнях. Для их решения необходимо понимать информационные процессы в обществе, информационную сущность происходящих социально-экономических преобразований, причем все это на общем фоне смены доминирующих технологических укладов. Следует констатировать, что общественная проблематика, связанная с информатизацией общества, информационной безопасностью, развитием информационных технологий, не является больше национальной, она становится проблематикой всего мирового сообщества. Данный факт накладывает особый отпечаток на обсуждение проблем информационной безопасности (в широком смысле этого слова) и ответственности ученых, инженеров и политиков за эту безопасность. В настоящее время становится все более очевидной необходимость разработки принципиально новых подходов, концепций, моделей по обеспечению взаимодействия человека с информационной средой.

Итак, строящееся сегодня общество знаний принципиально амбивалентно. С одной стороны, общество знаний рассматривается как производное от информационного общества, когда в центр внимания попадают вновь возникающие возможности производства и доступности информации, которые дают новые информационные и коммуникационные технологии. С другой стороны, становящееся общество знаний должно быть рассмотрено с точки зрения возникающих при этом рисков, т. е. одновременно как общество риска, что требует сделать больший упор на обсуждение проблем последствий такого все возрастающего базирования на научном знании многих общественных областей. Таким образом в становящемся глобальном информационном обществе (или как его иногда называют «обществе знаний») появляются новые возможности возрождения технократического мышления: манипулирование общественным мнением через

## Технологические риски: информационные аспекты безопасности общества

электронные средства массовой информации и Интернет, тенденциозное представление и искажение информации, спекуляция на «чувствах» среднестатистического гражданина и доверии к науке и к средствам массовой информации, подтасовка «фактов» и создание иллюзии их «научного» обоснования и т.п. Поэтому в информационном обществе есть настоятельная необходимость и возможность борьбы с этими технократическими тенденциями с помощью тех же мультимедийных средств, просвещения населения и гуманитарного образования, организации институтов относительно независимой оценки науки и техники и проведения системной оценки научных и технических разработок и хозяйственных проектов, а также осуществления междисциплинарного прогнозирования их развития.

### Библиография:

1. Сюттюрэнко О.В. Социальные и экономические риски развития информационных технологий// Научно-техническая информация. Сер.1. 2012. № 6. С. 1-5.
2. Хоффман Л.Дж. Современные методы защиты информации// М.: Советское радио, 1980.-263 с.
3. Батулин Ю.М. Проблемы компьютерного права.-М: Юрид. лит., 1991.-272 с.
4. Смолян Г.Л. Сетевые информационные технологии и проблемы безопасности личности// Вестник РФФИ. 1999. № 3(17). С. 63-68.
5. 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.
6. Темная сторона флешмоба [Электрон. ресурс]. – URL: <http://www.metronews.ru/novosti/temnaja-storona-fleshmoba/ТpolbВ---m0VnuDmSIgzIk/>
7. Малинецкий Г.Г. Сценарии, стратегические риски, информационные технологии// Информационные технологии и вычислительные системы. 2002. № 4. С. 83-108.
8. Сюттюрэнко О.В. Инфраструктурные вопросы развития и использования высокопроизводительных вычислений в научных исследованиях// Информационные технологии и вычислительные системы. 2002. № 4. С. 77-82.
9. Громыко Ю. Оружие, поражающее сознание,-что это такое?//Альманах «Россия-2010». М., 1997. Смирнов И., Безносюк Е., Журавлев А. Психотехнологии. М., 1996.
10. Смирнов И., Безносюк Е., Журавлев А. Психотехнологии. М., 1996.
11. Горохов В.Г. Философия и история науки: Учебное пособие.-Дубна: ОИЯИ, 2012.-212 С. – ISBN 978-5-9530-0328-5
12. Дементьев И.О. Интеллектуализация глобальных телекоммуникационных систем с использованием семантических сетей//Искусственный интеллект: философия, методология, инновации. Материалы III Всероссийской конференции студентов, аспирантов и молодых ученых МИРЭА, 11-13 ноября 2009 г.

13. 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.
14. Ленк Х. Размышления о современной технике.-М.: Аспект-Пресс, 1986. — 183 с. — (Программа «Высшее образование»). — ISBN 5–7567–0052–8.
15. Lenk H. Global TechnoScience and Responsibility. Schemes Applied to Human Values, Technology, Creativity and Globalisation. Berlin: LIT, 2007.
16. Бехманн Г., Горохов В.Г. Социально-философские и методологические проблемы обращения с технологическими рисками в современном обществе (Дебаты о технологических рисках в современной западной литературе) // Воросы философии, 2012, № 7 и 8.

### References:

1. Syuntyurenko O.V. Sotsial'nye i ekonomicheskie riski razvitiya informatsionnykh tekhnologii// Nauchno-tekhnicheskaya informatsiya. Ser.1. 2012. № 6. S. 1-5.
2. Khoffman L.Dzh. Sovremennye metody zashchity informatsii// M.: Sovetskoe radio, 1980.-263 s.
3. Baturin Yu.M. Problemy komp'yuternogo prava.-M: Yurid. lit., 1991.-272 s.
4. Smolyan G.L. Setevye informatsionnye tekhnologii i problemy bezopasnosti lichnosti// Vestnik RFFI. 1999. № 3(17). S. 63-68.
5. Siountiurenko 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.
6. Temnaya storona fleshmoba [Elektron. resurs]. – URL: <http://www.metronews.ru/novosti/temnaya-storona-fleshmoba/TpolbB---m0VnuDmSIgzIk/>
7. Malinetskii G.G. Stsenarii, strategicheskie riski, informatsionnye tekhnologii// Informatsionnye tekhnologii i vychislitel'nye sistemy. 2002. № 4. S. 83-108.
8. Syuntyurenko O.V. Infrastrukturnye voprosy razvitiya i ispol'zovaniya vysokoproizvoditel'nykh vychislenii v nauchnykh issledovaniyakh// Informatsionnye tekhnologii i vychislitel'nye sistemy. 2002. № 4. S. 77-82.
9. Gromyko Yu. Oruzhie, porazhayushchee soznanie,-chto eto takoe?//Al'manakh «Rossiya-2010». M., 1997. Smirnov I., Beznosyuk E., Zhuravlev A. Psikhotekhnologii. M., 1996.
10. Smirnov I., Beznosyuk E., Zhuravlev A. Psikhotekhnologii. M., 1996.
11. Gorokhov V.G. Filosofiya i istoriya nauki: Uchebnoe posobie.-Dubna: OIYaI, 2012.-212 С. – ISBN 978-5-9530-0328-5
12. Dement'ev I.O. Intellektualizatsiya global'nykh telekommunikatsionnykh sistem s ispol'zovaniem semanticheskikh setei.//Iskusstvennyi intellekt: filosofiya, metodologiya, innovatsii. Materialy III Vserossiiskoi konferentsii studentov, aspirantov i molodykh uchennykh MIREA, 11-13 noyabrya 2009 g.

13. Syuntyurenko O.V., Borisova L.F. Problemy informatsionnogo obespecheniya nauchno-innovatsionnoi sfery: novye kontseptual'nye podkhody// Nauchno-tekhnicheskaya informatsiya. Ser.1. 2009. № 4. S. 9-12.
14. Lenk Kh. Razmyshleniya o sovremennoi tekhnike.-M.: Aspekt-Press, 1986. — 183 s. — (Programma «Vysshee obrazovanie»). — ISBN 5–7567–0052–8.
15. Lenk H. Global TechnoScience and Responsibility. Schemes Applied to Human Values, Technology, Creativity and Globalisation. Berlin: LIT, 2007.
16. Bekhmann G., Gorokhov V.G. Sotsial'no-filosofskie i metodologicheskie problemy obrashcheniya s tekhnologicheskimi riskami v sovremennom obshchestve (Debaty o tekhnologicheskikh riskakh v sovremennoi zapadnoi literature) // Vorosy filosofii, 2012, № 7 i 8.