УДК 101.1:316

РЕСУРСЫ СНЯТИЯ РИСКОГЕННЫХ СИТУАЦИЙ: СЕТЕВОЙ МОНИТОРИНГ

Ю.М. Михайлов

ФГБОУ ВПО « Тверской государственный технический университет», г. Тверь

Поднимается проблема внедрения информационно-технологических ресурсов в организациях с преобладанием сетевых технологий в процессе управления. Анализируя очевидные достоинства сетевых технологий, автор выявляет социальные и культурные противоречия, связанные с их использованием. Сетевые технологии, нацеленные по своей сути на минимизацию рисков, в частности связанных с «человеческим фактором», на деле оказываются сопряженными с новыми рисками. В этом контексте сетевой мониторинг показывается как важный ресурс исчисления и предупреждения рисков.

Ключевые слова: *сетевое общество, риск, рискогенная ситуация, сетевые технологии управления, сетевой мониторинг.*

Тема риска заняла устойчивое место в теоретических разработках природы современного информационного общества. Проблематизируя вопросы, связанные с риском, исследователи приходят к мысли о необходимости интерпретации этого понятия в контексте конвенционализма знания [2, с. 127–136; 5, с. 277–283], доверия в условиях глобализации [4, с. 4–7], коммуникативной компетентности [8, с. 4–14], сетевых технологий в условиях неопределённости [9, с. 109–116] и других аспектах.

Современное информационное общество в результате стремительного распространения интернет-технологий начинает приобретать ярко выраженный *сетевой* характер. Такое сетевое общество с его многосложными и скоростными коммуникациями многократно усиливает социальную и культурную напряженность, обусловленную нарастанием неопределенности и неоднозначности как глубинных свойств рискогенности. С одной стороны, сетевой контекст делает современное общество более «открытым», а с другой – более «незастрахованным». Существование человеческого сообщества становится похожим на жизнь «без гарантий», где степень защищенности индивида и целого сообщества явно убывает по мере возрастания числа выборов и необходимости их постоянной интерпретации.

Глобальные цифровые сети создают технологическую основу современного информационного общества, которое по форме приобретает все более и более сетевой характер. Формирующийся новый тип информационного общества характеризуется тем, что важным ресурсом жизнедеятельности индивида и общества становятся не просто знания как таковые, а знания, организованные для использования в *информационных сетях*. «Владение территорией мало что значит без контроля за

Научная библиотека ТвГУ

проходящими через нее потоками и точками доступа к нам», – пишет американский исследователь У. Митчелл [7, с. 19]. Интенсивное влияние сетевых технологий отчетливее всего проявляется в контексте коммерциализации Интернета и продолжает усиливаться за счет исторического резонанса, создаваемого такими процессами, как интернационализация, глобализация и интеграция мировой экономики. В результате современное общество превращается в общество «всеобщей коммуникации» [3, с. 7]. Автор этого понятия Дж. Ваттимо считает, что такое общество постоянно предъявляет человеку самые разнообразные требования, заставляет его жить по принципу «колебания множественности» [там же, с. 14, 101]. В таком контексте проблематика риска приобретает новые специфические черты, отчётливо иллюстрируемые на уровне реализации сетевого мониторинга.

Понятие «риск» имеет важное значение как для отдельного индивида, так и для общества в целом. Этимология этого термина неоднозначна. По одной из версий, «риск» происходит от староитальянского *risicare* – «отваживаться», а в поздней латыни появляется как *risigus*. Этимологический словарь У. Скита указывает на связь данного слова с испанским *risco* – «крутая обрывистая скала, с которой у моряков было связано представление об опасности». Близким является также испанское слово *arriesgar* – «решиться на связанный с опасностью поступок» или буквально – «идти против скалы». В XVI в. эти выражения появляются также в португальском языке при описании путешествий мореплавателей, которые, открывая новые континенты, подвергались серьёзному риску [6, с. 8].

Издавна понимание риска находилось во взаимном пересечении с понятием опасности. Например, китайский иероглиф, обозначающий риск, состоит из двух символов: один указывает на угрозу, другой – на возможность. Мысль о том, что риск представляет собой и то и другое, многим кажется противоречивой. В сознании западного человека риск ассоциируется главным образом с переживанием опасности или угрозы, а также со страхом утраты чего-либо [там же, с. 10].

Сегодня понятие риска приобретает все большую интерпретативность: 1) потенциальная, численно измеримая *возможность* неблагоприятных ситуаций и последствий в виде какого-либо ущерба, связанная с неопределенностью; 2) вероятностное *событие*, связанное с неопределенностью, которое негативно влияет на проект; 3) взвешенная линейная *комбинация* вариации и ожидаемой величины (математического ожидания) распределения всех возможных исходов; 4) *действие*, выполняемое в условиях выбора, когда в случае неудачи существует возможность оказаться в худшем положении, чем до выбора; 5) вероятная *опасность*, действие наудачу в надежде на счастливый исход (словарь Ожегова) и др. [1, с. 20]. Как видим, в большинстве современных

Научная библиотека ТвГУ

определений отмечается, что риск – это прежде всего характеристика неопределенности.

Выглядит продуктивной исследовательская позиция, согласно которой риск рассматривается одновременно и как *опасность*, т. е. возможные негативные события, которые могут привести к снижению эффективности процессов управления и качества деятельности, угрозе безопасности, возникновению потерь и убытков, и как *действие*, направленное на привлекательную цель, достижение которой сопряжено с элементом неопределенности, опасности, угрозой потери или возможностью неуспеха.

Рискогенная ситуация – это ситуация, содержащая риск уже в самом своем зарождении. Исследователи классифицируют рискогенные ситуации по ряду признаков: по степени риска (ситуации с низким, средним и катастрофически высоким уровнем риска; по частоте проявления (разовые, повторяющиеся и регулярные); по природе проявления опасности (техногенные, природные и смешанные); по сфере проявления (экологические, политические, социальные, экономические, профессиональные); по возможности прогноза (прогнозируемые и не прогнозируемые); по степени зависимости от субъекта риска (не зависящие и зависящие от человека); по прогнозу результативности (позитивные и негативные); по возможности контроля (контролируемые и не контролируемые); по уровню динамики (быстро развивающиеся и медленно развивающиеся). Однако приходится признать, что никакая классификация не может иметь всеобъемлющего характера, поскольку любая рискогенная ситуация вкраплена в определенный социокультурный контекст, где сразу же приобретает свои неповторимые специфические очертания.

Следует различать два рода рискогенных ситуаций: однозначно неблагоприятные и вероятностно неблагоприятные. В первом случае неизбежно следует некая потеря или неуспех, независимо от исхода альтернативы. Во втором случае речь идет о рискованных ситуациях, которые могут привести в равной мере к получению выигрыша и ущерба. В связи с этим чаще всего используется определение, согласно которому риск понимается как возможность неблагоприятного исхода в условиях неопределенности.

В контексте сетевого мониторинга назрела задача *исчисления рисков*, т. е. выработки способности обращения к неопределенному будущему. Риск берет свое начало в процессе принятия решений, следовательно, неизбежно всплывает и проблема социальной ответственности. Проблема «некалькулируемости» последствий риска и его размеров с особой яркостью выявляется в недостатке ответственности за них. За социальные риски ответственны люди, фирмы, государственные учреждения и политики. Социальные корни риска блокируют «экстернализацию» проблемы ответственности. Здесь мы имеем дело с историческим синтезом природного и социального, где даже естественные катастрофы

Научная библиотека ТвГУ

(например, наводнения, оползни) на деле оказываются сопряженными с результатами деятельности человека.

В современном сетевом обществе используются довольно разнообразные ресурсы снятия ситуаций риска, среди которых: дублирование коммуникационных связей; «разнесение» центров сбора и хранения информации; обучение персонала; «обучение» сети (например, уже практикуется внедрение проектов по интеллектуальному поиску в Интернете (Apolo, Чойстер), действующих по принципу: чем больше прогоняется информации, тем «умнее» становится машина) и другие возможности преодоления опасности. На фоне всего перечисленного весьма продуктивным ресурсом снятия рискогенных ситуаций выглядит *сетевой мониторинг*.

Исследователи в целом трактуют понятие «мониторинг» (от англ. monitor – контролироватъ, проверять) как специально организованное, систематическое наблюдение за состоянием объектов, явлений и процессов с целью контроля за ними, оперативного выявления факторов внешнего воздействия, оценки и прогноза [11]. Понятие «сетевой мониторинг» чаще всего используется специалистами по IT-технологиям, в представлении которых это наблюдение за аппаратным и программным состоянием сети, информационным трафиком, наличием уязвимостей сети с целью обеспечения ее оптимальной загрузки, сохранности информации, модернизации и защиты от вредоносных программных воздействий [12].

В целом солидаризируясь с такой интерпретацией сетевого мониторинга, считаем продуктивным расширить это понятие, добавив такую его характеристику, как коммуникативные возможности расширения властно-управленческих решений и ответных реакций на них со стороны персонала. Таким образом, сетевой мониторинг может включать в себя следующие компоненты: наблюдение, контроль, оценку и корректировку в системе сетевого управления. *Наблюдение* осуществляется за аппаратным и программным состоянием сети, информационным трафиком, наличием уязвимостей сети с целью обеспечения ее оптимальной загрузки, сохранности информации, модернизации и защиты от вредоносных программных воздействий. *Контроль* предполагает внешнюю фиксацию властно-управленческих коммуникаций внутри сети и реакцию на формы управленческого воздействия. *Оценка* заключается в выявлении значимости возможных ресурсов предупреждения и снятия фактора риска. *Корректировка* в системе сетевого управления сводится к оперативному изменению планов в соответствии с изменяющимися условиями их реализации.

В производственном процессе большинства современных крупных предприятий используются *сетевые технологии*. Под таковыми понимаются автоматические системы управления производством, построенные в основном на использовании интернет-технологий. Сетевые системы управления производством обычно имеют разветвленную

Научная библиотека ТвГУ

структуру, большое количество модулей, выполняющих различные функции, сложную организацию взаимодействия различных модулей системы. По этой причине возникает большое количество рисков, связанных с персоналом, обслуживающим и использующим данные системы. Получается, что очевидные достоинства и позитивные возможности, предоставляемые этими системами (скорость информации, быстрота принятия решений, прозрачность управления и др.), оказываются сопряженными и с новыми рисками.

Причины нарушения функционирования сети классифицируются следующим образом: природные явления (например, ураган Сэнди в октябре 2012 г.); техногенные воздействия (катастрофа на Саяно-Шушенской ГЭС в августе 2009 г.); террористическая деятельность (взрыв башен-близнецов в Нью-Йорке в сентябре 2001 г.); отказ оборудования (авария в энергосистемах США и Канады в августе 2003 г.); риски от вредоносного программного обеспечения (глобальная эпидемия вредоносных программ в 2005 г.). Особое место среди причин занимают психофизические и социально-культурные свойства работника, именуемые в литературе как «человеческий фактор». Яркой иллюстрацией служат примеры аварий на Чернобыльской АЭС в СССР и на АЭС «Фукусима-1» в Японии, где возникновение аварийной ситуации было связано не только с факторами стихийного бедствия и ошибок в проектировании обеих станций, но и с неправильными действиями сотрудников.

Справедливости ради следует признать тот факт, что уже само наличие сети является критическим условием функционирования любой организации, где практически весь производственный процесс «завязан» на использовании сетевых технологий. Когда информационные ресурсы систем учета, планирования, управления персоналом, а также все коммуникации полностью размещены в сети, возникает опасность, что неплановые отключения могут практически блокировать деятельность организации или значительно снизить ее эффективность. Риски зарождаются на всех стадиях реализации сетевого управления: на этапе проектирования систем, их внедрения в эксплуатацию и использования. Специалисты по программному обеспечению обычно закладывают общестатистические свойства системы без учета потребностей организаций и специфики работы тех людей, которые будут использовать искомую проектируемую систему. Услуги по перенастройке системы под конкретного потребителя стоят дорого, часто ограничены как функционалом системы, так и отсутствием достаточного количества специалистов, обладающих такими навыками. К тому же сами потребители «сетевого» продукта, планирующие проектирование или настройку сетевых систем, часто подходят к этому вопросу без достаточной мотивации. В результате при введении системы в производство неизменно проявляются недостатки, которые практически невозможно устранить или их устранение сопряжено с явными финансовыми и временными затратами [10].

Научная библиотека ТвГУ

Процесс непосредственного перехода организации на сетевую систему управления является серьезной и нередко длительной рискогенной ситуацией, аккумулирующей в своем зародыше сразу несколько факторов риска. Во-первых, временной риск, когда динамика процесса может растянуться на многие месяцы и даже годы. Во-вторых, риск наличия скрытых недостатков, когда по ходу внедрения системы выявляются системные сбои, которые не были проработаны и устранены на первых двух этапах: во время проектирования и опытной эксплуатации. В-третьих, риск, связанный с приобретением оборудования (отдельных рабочих станций, пропускной способности сети, серверного оборудования и др.), которое не всегда соответствует требованиям программного обеспечения. При всей важности перечисленных факторов, усиливающих рискогенность непосредственного перехода организации на сетевую систему управления, главным является человеческий фактор. Парадокс состоит в том, что сетевые технологии, в своей основе призванные минимизировать степень зависимости процесса от субъекта риска, на деле увеличивают его. Персонал организаций, переходящих на сетевую систему управления, обычно воспринимает это новшество не как систему, которая облегчит и упростит их работу, а как очередную дополнительную нагрузку. Каждый работник в силу своей профессиональной подготовки, возраста или способности и готовности к переобучению реагирует на внедрение сетевых технологий по-разному: одни быстро включаются в суть действия системы, другие оказываются не в состоянии работать с системой и увольняются, третьи (и таких оказывается большинство!) начинают работать, минимально используя возможности сети, допуская при этом небрежность и большое количество ошибок.

С внедрением сетевых технологий меняется и уровень компетентности специалиста: работники, которые хорошо справлялись со своими обязанностями до внедрения системы, переходят в разряд плохих специалистов, потому что не могут работать в режиме «он-лайн». Например, кладовщица, которая всю жизнь проработала на складе и всегда содержала его в идеальном состоянии, с введением системы электронного учета переходит в разряд некомпетентных или даже ненужных работников, а ее место занимает бойкий молодой «пользователь сети», способный вести электронный каталог складского учета, однако не пронизанный духом этого трудового поста.

Как отмечают практики, внедрение сетевой системы управления в работу организаций на начальном этапе нередко сопровождается недовольством и сопротивлением со стороны персонала. При благоприятном исходе со временем перечисленные факторы риска минимизируются. Однако нередко встречаются ситуации, когда число недостатков программного обеспечения и оборудования не только не сокращается, а, наоборот, со временем увеличивается. В таком случае внедрение сетевых технологий остается устойчивым «враждебным» очагом в сознании

Научная библиотека ТвГУ

работников. Если почитать форумы в Интернете с отзывами пользователей о различных сетевых системах управления производством, то положительные реакции встречаются чрезвычайно редко. По сети «гуляют» чаще всего отрицательно ироничные отзывы. Например, афористично выглядит отзыв: «SAP – это месть Гитлера за Сталинград». Так иронично характеризуют пользователи одну из наиболее крупных сетевых систем управления, созданную международной корпорацией SAP AG со штаб-квартирой в Германии, которую используют ОАО «Газпром», ОАО «РЖД», ОАО «Российские сети» и другие достаточно крупные отечественные организации [там же].

Обучение сотрудников организации, работающих с сетевой системой управления, также представляет своего рода риск. Если количество сотрудников, работающих в режиме «он-лайн», исчисляется сотнями или даже тысячами, а само виртуальное предприятие территориально разбросано по разным регионам, странам и даже континентам, то централизованная подготовка каждого работника становится затруднительной и в финансовом, и в организационном плане. В ответ на этот «вызов» сетевого общества находятся другие, более приемлемые способы обучения. Например, многие фирмы обязывают работников заниматься самообучением, для чего создается сетевое хранилище инструкций по различным направлениям функционирования системы. Поскольку в нем могут быть сотни различных инструкций, выбрать самые необходимые из них для человека, приступившего к самообучению, представляется довольно сложной задачей, особенно тогда, когда качество самих инструкций оставляет желать лучшего. Внешне положительная практика «научился сам – обучи другого» может скрывать некий внутренний конфликт: человек, научившись выполнять какой-либо «функционал» системы по неправильному алгоритму, начинает транслировать свои ошибочные навыки другим работникам; его неподготовленность может повлечь за собой ошибки в работе или создать ситуацию неполного использования функционального потенциала системы. Правильно организованный сетевой мониторинг способен минимизировать риск, связанный со снижением компетентности пользователей сетевой системы управления.

Важный фактор риска, проявляющийся практически в любой организации, связан с «перехлестом» должностных функций. С целью ускорения производственной деятельности и обеспечения максимизации отчетности работникам поручается не свойственный им функционал. Например, специалисты технических служб вынуждены оформлять платежные документы, осуществлять бухгалтерские проводки, вести складской учёт и т. д. В результате работник, занимающийся не свойственной ему деятельностью и не имеющий специальной подготовки в этом направлении, допускает значительно большее количество ошибок в работе, а скорость выполнения данных операций снижается. Соответственно, отвлекаясь на непрофильную работу, специалист уделяет меньше

Научная библиотека ТвГУ

времени деятельности, к которой он профессионально подготовлен и где может работать с максимальной эффективностью.

Обычно при построении сетевой системы управления предприятием стараются добиться максимального охвата снимаемых и учитываемых системой параметров деятельности организации. Соответственно, все эти параметры должны быть занесены каким-либо образом в систему. Одна их часть автоматически «считывается» различными электронными приборами, другая – заносится в систему вручную. Возникает эффект «двойного» делопроизводства. На основании требований различных регламентирующих документов, требований финансовой и налоговой отчетности, требований охраны труда и других инстанций все параметры дублируются и на бумажном носителе. К примеру, бухгалтерская отчетность организации полностью ведется в электронном виде: движение документов легко отслеживается, персонал, работающий с документами, входит в систему под личным паролем. Однако в силу такой бюрократической подотчетности все бухгалтерские документы параллельно дублируются и на бумажном носителе, подписываются ответственными лицами и вновь сдаются в бухгалтерию, где сканируются и заносятся в систему уже в виде электронных скан-копий. Налицо парадокс: введение сетевой системы управления производством не только не снижает, но и, наоборот, увеличивает объем человеческого труда.

В качестве вывода отметим, что сетевое общество, выступая, по сути, творением человека, определенным образом является «рисковым». Неоднозначность и неопределенность – эти свойства являются глубинными основаниями рисковости. Рисковость в организации сетевого управления кроется в объективной и субъективной неопределенности, границы которой распространяются от первоначального замысла до конечного результата. Неопределенность может принять любое истинное значение в диапазоне от «запланированной выгоды» до «фактической потери». Поскольку рискогенных ситуаций полностью избежать невозможно, надо *уметь «пребывать» в них* – рефлексировать, предвосхищать, держаться интервалов надежности. В связи с этим фактор риска обязывает быть осмотрительным, вдумчивым, рассчитывать заранее социальную рентабельность. Практика принятия решений показывает, что результаты, с одной стороны, во многом зависят от компетенции управленцев и исполнителей, с другой – от непрограммируемых уклонений или предопределенных событий, момент наступления которых нельзя спрогнозировать.

При всех очевидных достоинствах сетевых технологий (увеличение скорости передачи информации, быстрота и прозрачность принятия решений, редуцирование делопроизводства и др.) невозможно избежать социальных и культурных противоречий, связанных с их использованием. Сетевые технологии, нацеленные по своей сути на минимизацию рисков, в частности связанных с «человеческим фактором», на деле оказываются сопряженными все с новыми и новыми рисками. В этом кон-

Научная библиотека ТвГУ

тексте сетевой мониторинг является важным ресурсом снятия рискогенных ситуаций, т. е. исчисления и предупреждения рисков. Сетевой мониторинг с его прогностикой, опирающейся на предметно-профессиональную организацию, позволяет избежать непродуманной инициативы. Поэтому расчеты и проницательность в сфере сетевого управления становятся взаимодополнительными и взаимозависимыми.

Организация «сетевых» предприятий выглядит довольно противоречиво. Сколь бы ни были совершенны сетевые технологии, роль человека труда остается по-прежнему важной (его теоретические знания, понимание ответственности, степень его квалификации и компетентности, его мотивация и его поведение). Да, современный человек – это уже часть сети, но он не электронный киборг, в нем всегда присутствует «самость», автономность и творчество. В условиях повышения глобальных и локальных рисков главной задачей становится не только их минимизация, но и трансформация в новые производственные и повседневные возможности.

Список литературы

1. Авдошин С.М., Песоцкая Е.Ю. Информатизация бизнеса. Управление рисками. М., 2011.
2. Бехманн Г., Горохов В.Г. Социально-философские и методологические проблемы обращения с технологическими рисками в современном обществе // Вопросы философии. 2012. № 7–8. С. 127–136.
3. Ваттимо Дж. Прозрачное общество. М., 2001.
4. Евстифеева Е.А., Столяр В.Ю. Управление глобальным риском и доверие // Вестн. Твер. гос. ун-та. Сер.: «Философия». 2008. № 7. С. 4–7.
5. Ильин В.В. Социальный риск // Ильин В.В. Философия. Ростов/н/Д, 2006. Т. 2. С. 277–283.
6. Клири Ш., Мальре Т. Глобальные риски. Деловой успех в неспокойные времена: пер. с англ. М., 2011.
7. Митчелл У. Я++: Человек, город, сети: пер. с англ. М., 2012.
8. Михайлова Е.Е. Особенности коммуникативных компетенций в информационном обществе // Вестн. Твер. гос. ун-та. Сер.: «Философия». 2011. № 3–4. С. 4–14.
9. Рубцова Н.Е., Балакшина Е.В. Психологические ориентиры профессиональной подготовки специалистов в области страхового бизнеса // Новое в психолого-педагогических исследованиях. 2010. № 4. С. 110–116.
10. http://lurkmore.to/SAP/
11. http://vslovare.ru/slovo/monitoring
12. http://endace.ru/solutions/Monitoring

Научная библиотека ТвГУ

RESOURCES OF RISK-GENERATING SITUATIONS ELIMINATION:NETWORK MONITORING

Y.M. Mikhaylov

Tver State Technical University, Tver

Issues of implementing information technology resources into the organizations with the predominance of network technologies in the management process are discussed in the article. Analyzing the obvious advantages of network technologies, the author reveals their social and cultural contradictions. Network technologies, aimed at the risks minimization related to “a human factor”, in reality are able to produce new risks. In this context, network monitoring is interpreted as an important resource of risks calculation and prevention.
***Key words**: network society, risk, risk-generating situation, network management technologies, network monitoring.*

Об авторе:

МИХАЙЛОВ Юрий Михайлович – аспирант кафедры психологии и философии ФГБОУ ВПО «Тверской государственный технический университет», Тверь. E-mail: ymm67@yandex.ru

Author information:

Mikhaylov Yuri Mikhaylovich – Ph.D. student of the Dept. of Psychology and Philosophy of Tver State Technical University, Tver. E-mail: ymm67@yandex.ru

Научная библиотека ТвГУ