ВЕСТНИК ИТАРК

№1 2011

ISSN 2224-0873

ИТ-Ассоциация Республики Коми

Государственное автономное учреждение Республики Коми
«Центр информационных технологий»

ВЕСТНИК ИТАРК

Журнал основан в 2011 году
Выходит 2 раза в год

№1 (1), 2011

Адрес редакции:
167000, г.Сыктывкар, ул. Интернациональная, д.108-А.
Тел.: 8912 14295 31, 89087191111
E-mail: journal@itark.ru
Сайт: http://www.vestnik.itark.ru

Содержание

К читателю

Уважаемые читатели!

Вы держите в руках первый выпуск научного журнала «Вестник ИТАРК». Учредителями данного периодического научного издания являются некоммерческое партнерство «ИТ-Ассоциация Республики Коми» и государственное автономное учреждение Республики Коми «Центр информационных технологий».

Цель создания журнала – предоставить научному и экспертному сообществу в области информационных технологий площадку, где они могли бы озвучивать проблемы, делится опытом решения задач в области информационных технологий. К сожалению, в настоящее время сложилась ситуация недостатка периодических научных изданий, где эксперты и ученые в области информационных технологий могли бы публиковать результаты своих научных трудов. Редакционная коллегия журнала «Вестник ИТАРК» ставит перед собой амбициозную задачу – попасть в кратчайшее время в список журналов из списка Высшей аттестационной комиссии.

Каждый выпуск журнала будет разбиваться на разделы: Электронное правительство, Информационные технологии в отраслях народного хозяйства, Защита информации в информационных системах и пр. Состав и объем разделов будет меняться от выпуска к выпуску и будет зависеть от авторов статей. В связи с задачами, которые решает журнал «Вестник ИТАРК», все статьи будут подвергаться рецензированию. К рецензированию будут приглашаться эксперты ведущих центральных вузов и научных институтов страны, а также специалисты-практики.

Приглашаем авторов к сотрудничеству с журналом!

С уважением и надеждой на плодотворное сотрудничество, редакционная коллегия научного журнала «Вестник ИТАРК».

Информационное общество и электронное правительство

УДК 316.4

БАЗИСНЫЕ ТРАНСФОРМАЦИИ СОВРЕМЕННОГО ОБЩЕСТВА: глобальные трансформации в сфере производства и информационное общество

А.В. Селютин[1]

Аннотация: На основе проведенного теоретического анализа существующих концепций информационного общества показано, что в содержании самого понятия информационного общества с момента его появления произошли значительные изменения, которые косвенно отражают трансформации сознания в связи с изменившейся ролью информации в жизни общества.

Ключевые слова: информационное общество, исторический и философский экскурс.

Под базисными трансформациями современного общества мы понимаем трансформации, происходящие в таких сферах общественной жизни, как производство, обмен и потребление, поскольку именно эти сферы и их взаимоотношения определяют экономические основания социальной жизни. Особенностью современного этапа общественного развития является то, что происходящие в нем глобальные трансформации затрагивают глубинные, базисные основания общества, начиная со сферы производства.

Рубеж третьего тысячелетия ознаменовался для человечества очередным витком научно-технической революции, который выразился во внедрении во все сферы общественной жизни информационно-коммуникационных технологий и развитии глобальной компьютерной сети - Интернета. Бурное развитие этих технологий составило фундамент для перехода к информационному обществу - новой ступени в развитии современной цивилизации, отличительной чертой которой является появление принципиально нового производственного ресурса. Этим новым ресурсом стала информация.

Нельзя не заметить, что данное состояние общества наглядно демонстрирует всю условность разграничений между различными сферами совместной деятельности людей. Используемая в современном производстве информация по своему происхождению является продуктом духовного производства (в первую очередь, науки), но, образуя ресурсную основу материально-производственной сферы, она, в свою очередь, порождает новые трансформации во всех остальных сферах, включая организационную, социальную и духовную.

С этим связана многоаспектность информационного общества как социального феномена, что на уровне научного и философского теоретического дискурса получает отражение в наличии различных подходов к изучению этого феномена.

Не случайно концепт «информационное общество» стал исторически первой формой концептуализации глобальных трансформация современности.

Соответствующий термин был впервые употреблен» американским экономистом Ф. Махлупом во второй половине XX века в работе «Производство и применение знания в США» в контексте исследования информационного сектора экономики на примере США). До этого момента для охвата явлений, характеризующих современное состояние общества

[1] Администрация Главы Республики Коми

в экономически развитых странах, использовалось понятие «постиндустриальное общество». В современной философии и других социальных науках понятие «информационное общество» быстро развивается в качестве концепции нового социального порядка, существенно отличающегося по своим характеристикам от предыдущего. Первоначально постулируется понятие «посткапиталистического» - «постиндустриального общества», в границах которого в отраслях экономики начинает преобладать производство и распространение знания, и, соответственно, появляется новая отрасль - информационная экономика. Быстрое развитие последней обусловливает ее контроль за сферой бизнеса и государства. Выделяются организационные основы этого контроля, в применении к социальной структуре означающие возникновение класса меритократии. Производство информации и коммуникация становятся централизованным процессом. В конечном счете, основным ресурсом нового постиндустриального порядка определяют информацию. Таким образом, в первых теоретических концепциях, посвященных анализу информационного общества (Ф.Махлуп, Д.Белл, А.Турен) главным предметом исследования становится экономика как сфера социума наиболее быстро подвергшаяся изменениям в результате становления информационного общества.

Трансформация традиционного социального порядка в новый, возникающий вследствие эволюции информации в ведущую производительную силу социума, приводит к изменению дискурса по данной проблеме: экономические и технологические концепции информационного общества дополняются социологическими и социально-философскими исследованиями. Одна из наиболее интересных и разработанных философских концепций информационного общества принадлежит известному японскому ученому Е. Масуде, стремящемуся осмыслить грядущую эволюцию социума.

Как научное понятие «информационное общество» не имеет единого, общепризнанного определения. В книге «Виртуальный новый мир», подготовленной к парламентской Ассамблее Совета Европы 1997 года, дано определение информационного общества как «общества, основанного на информации»[2]. В кратком словаре по социологии информационное общество определено как «общественное устройство, основным фактором развития которого признается создание и использование индустрии информации (компьютеров, микроэлектроники, коммуникационно-вычислительных сетей, национальных и межнациональных баз данных); разновидность теории постиндустриального общества»[3]. В другом словаре дано следующее определение: «Информационное общество – одно из наименований постиндустриального общества, характеризующееся резким изменением и повышением роли и значения информационных технологий»[4]. Энциклопедический словарь «Культура» представляет информационное общество как «общество, в котором информация и уровень ее использования кардинальным образом влияет на экономическое развитие и социокультурные изменения в обществе: в экономической сфере – информация превращается в товар, в социальной — она становиться главным фактором изменения качества жизни»[5].

Всемирная философская энциклопедия определяет понятие информационного общества как понятие, «фактически заменившее в конце 20 века термин постиндустриальное общество»[6]. Действительно, концепция информационного общества

[2] См.: Вартанова Е. Информационное Общество и СМИ Финляндии в европейской перспективе. М.: МГУ, 1999. – С. 37.

[3] Краткий словарь по социологии/автор-состовитель П.Д.Павленок. — М.:Инфра-М, 2000. – С 72.

[4] Тадевосян Э.В. Словарь-справочник по социологии и политологии. – М.: Знание, 1996. – С. 93.

[5] Хоруженко К.М. Культура. Энциклопедический словарь. – Ростов-на-Дону.: Феникс, 1997. – С. 180.

[6] Всемирная энциклопедия. Философия/Главн.науч.ред. и сост. А.А. Грицанов. – М.: Харвест, Современный литератор, 2001. – С. 42.

в современной социологии направлена на осмысление нового социального порядка, проявляющегося на уровне социальной структуру. При этом вопрос о соотношении понятий «постиндустриальное общество» и «информационное общество» решается по-разному. Можно выделить три разных подхода к его решению: согласно первому подходу термин «информационное общество» есть не что иное, как синоним термина «постиндустриальное общество», в рамках второго подхода индустриальное общество выступает в качество одной из разновидностей постиндустриального общества или один из этапов его развития. Представители четвертого подхода выводят информационное общество за рамки постиндустриального общества, представляя его в качестве новой ступени развития общества, следующей за постиндустриальным обществом. Данные разночтения не представляются существенными с точки зрения целей и задач настоящего исследования. Главное – это зафиксировать существенный признак индустриального общества, который состоит в том, что в этом состоянии общества достигнуты технические возможности для протекания высокоскоростных коммуникационных процессов, благодаря чему котором информация становится основным ресурсом и в то же время основным продуктом жизнедеятельности общественного производства.

Впервые идея информационного общества была сформулирована на рубеже 60-х – 70-х гг. XX века. Термин «информационное общество» ввел профессор Токийского технологического института Ю.Хаяши. Характеристики информационного общества были представлены в отчетах ряда организаций японскому правительству, где описывалась компьютеризация общественных процессов, способствующая обеспечению доступа всех социальных групп к источникам информации и избавлению человека от рутинной работы посредством достижения высокого уровня автоматизации производства как главного условия перехода к информационному обществу.

Большой вклад в обоснование концепции информационного общества внес японский профессор И.Масуда, автор труда «Информационное общество как постиндустриальное общество»[7]. В этой работе информационное общество рассматривалось главным образом в экономическом контексте. По мнению И.Масуда, в условиях формирования информационного общества должна измениться сущность самого производства, продукт которого станет более «информационно емким», благодаря чему «производство информационного продукта, а не продукта материального будет движущей силой образования и развития общества»[8]. В то же время И.Масуда уделяет большое внимание и социальным последствиям перехода к информационному обществу, говоря о глубокой трансформации человеческих ценностей, которая по его мнению, должна привести к бесклассовому обществу. В котором будут разрешены все социальные конфликты: «это будет общество согласия, с небольшим правительством и государственным аппаратом»[9]. В целом разработка японского варианта концепции информационного общества осуществлялась с целью решения задач экономического развития Японии, что обусловило его прикладной характер.

На западе концепцию информационного общества разрабатывали также: М.Кастельс, Ф.Уэбстер, Э.Гидденс, Ю.Хабермас, Д. Мартин, Г. Молитор, А. Тоффлер, Д.Белл, З.Бжезинский, А.Кинг, Д.Несбит, А. Турен, П. Дракер, М.Маклюэн и др.

Д.Белл в 1973 г. в книге «Наступление постиндустриального общества. Опыт социального прогноза» показал, что термин «информационное общество» есть не что иное, как новое название постиндустриального общества, поскольку информация является в этом обществе основой социальной структуры. «В наступающем столетии решающее значение для экономической и социальной жизни, для способов производства

[7] Masuda Y. The Informational Society as Post-Industrial Society. World Future Society, 1981.

[8] Ibid. – P. 29.

[9] Ibid. – P. 46.

знания, а также для характера трудовой деятельности человека приобретет становление нового социального уклада, зиждущегося на телекоммуникациях»[10].

Классическая характеристика информационного общества, оформившаяся на рубеже 60-х – 70-х г.г. XX века, представленная именами Д. Белла, О. Тоффлера, А. Турена, включала следующие основные моменты. Во-первых, обоснование перехода экономических и социальных функций от капитала к информации, и вследствие этого, соединение науки, техники и экономики; увеличение информоемкости производимых продуктов, сопровождающееся увеличением доли инноваций, маркетинга и рекламы в их стоимости; высокий уровень автоматизации производства, освобождающий человека от рутинной работы и т.п. – как базовые характеристики общественного производства. Во-вторых, не собственность, а уровень знаний и информации становятся главными факторами социальной дифференциации. В основе этого процесса, как считает Д. Белл, лежит рост сферы услуг за счет сферы материального производства, вызывающий, в свою очередь, преобладание в высших социальных эшелонах людей, специализирующихся на выработке кодифицированного (т.е. систематически организованного) знания. Данный тип профессионального труда неотделим от большего удельного веса в нем всевозможных инноваций, что предъявляет повышенные требования к уровню знаний работника. В жизни современного общества, по его мнению Д.Белла, решающее значение приобретают инновации и социального контроля за изменениями. Именно изменение в осознании природы инноваций обусловливает ценность теоретического знания. Закономерным следствием этого становится, по мнению Белла, формирование новых социальных элит, на основе образования. Согласно Д. Беллу, симбиоз социальных организаций и информационных технологий создает возможность внедрения новых информационных технологий не только в промышленное производство, но также в социальную сферу, что выражается в создании интеллектуальных технологий – в частности, алгоритмов действий по принятию управленческих решений, выбора в неопределенной ситуации или в ситуации риска и т.п. В результате этих процессов, как считает Д.Белл, возникнет новая рациональность будущего информационного века, основанная не на классической идее «общественного договора» или «социального согласия», а на интеллектуальных технологиях, которая позволит осуществиться мечте об рациональной устройстве социальной жизни.

Классики теории индустриального общества предсказывали закат «индустриальной цивилизации», приход «общества информации и услуг», выделение «информационного производства» в важнейший национальный продукт. Так, Э.Тоффлер видел в средствах коммуникации главный двигатель человеческого прогресса на протяжении всей его истории, Д.Белл предсказывал внедрение информатизации в развитие всех сторон жизни общества на основе компьютерных технологий и даже утверждал, что в будущем рынок будет заменен организованным обменом на основе компьютерных сетей.

Однако реальное развитие информационного общество показало, что это общество характеризуется не только и не столько возможностями накопления и переработки информации, как это представлялось представителям классического подхода, сколько новыми формами коммуникации. В этих принципиальных изменениях процесса коммуникации в современном мире выделяют ряд оснований в том числе: глобализацию средств массовой информации и коммуникации, которая задает, по выражению Э. Гидденса, «мировой информационный порядок»; возможную потерю научным дискурсом своего привилегированного положения; обострение традиционных проблем коммуникации, таких, например, как проблема доверия/недоверия к передаваемой информации. Все эти изменения привели к сближению понятий коммуникации и развития социальных структур. Яркими примерами подобного подхода могут служить концепции И. Лумана и М. Кастельса.

[10] Белл Д.Социальные рамки информационного общества. М.: Харвест, 1980. – С. 45.

Таким образом, не информация, а коммуникация оказывается центральным звеном информационного общества. Поскольку в условиях становления информационного общества содержанием всех отношений между людьми по поводу воспроизводства общественной жизни является информационное взаимодействие, обмен информацией, ее накопление, производство, анализ, отбор и потребление, развитие как общественного производства, так и социальной структуры общества, его социальных институтов и процессов определяется уровнем состоянием коммуникации. Эта идея развивается в трудах многих специалистов, занимающихся исследованиями информационного общества.

Еще в середине 70-х гг. группа французских специалистов провела фундаментальное комплексное исследовании, результаты которого представлены в книге С.Нора и А.Минка «Компьютеризация общества. Доклад Президенту Франции»[11]. Одним из выводов исследования является тезис о том, информационное общество будет менее четко социально структурировано, чем общество индустриальное, при этом одним из факторов этих структурных изменений послужит отношение различных социальных групп к тенденции упрощения языка, связанной, в частности, с особенностями электронно-опосредованной коммуникации. В то же время компьютеризация будет способствовать преодолению культурного неравенства между отдельными социальными группами посредством унификации языка.

В книге С.Нора и А.Минка «Компьютеризация общества. Доклад президенту Франции»[12] утверждается, что белловский постиндустриалистский подход «продуктивен в отношении информации, управляющей поведением производителей и покупателей», но «бесполезен при столкновении с проблемами, выходящими за сферу коммерческой деятельности и зависящими от культурной модели»[13] .

Подчеркивая важность прогнозирования культурных конфликтов в информационном обществе, авторы доклада президенту Франции полагали, что информационное общество будет менее четко структурировано и более полиморфно, чем общество индустриальное. Одним из факторов полиморфизма, считают они, будет отношение различных групп к тенденции упрощения языка, связанной, в частности, с соображениями эффективности баз данных и других электронно опосредованных коммуникаций. Таким образом, предлагая единый язык, компьютеризация способствует преодолению культурного неравенства. Вместе с тем, считают авторы, хотя такой упрощенный язык будет совершенствоваться и становиться пригодным для все более развитых диалогов, он будет все же встречать сопротивление. Приемлемость этого кодифицированного языка будет зависеть от культурного уровня субъектов, что обусловит дискриминационный эффект телематики (слово «телематика» вводится для обозначения процессов конвергенции компьютерной техники с техникой средств связи). «Более чем когда-либо язык становится ставкой культуры. Оппозиционные группы будут бороться за его присвоение»[14] .

Главный редактор Международной энциклопедии по коммуникации Э.Барнув пишет о «центральном положении коммуникации в человеческой истории»[15]. Д.Тапскотт, выделяя признаки информационного общества, подчеркивает, что информационное общество – это общество знаний, производящее интеллектуальные изделия, причем используя цифровую форму представления объектов. Наблюдая становление

[11] Nora S., Minc A. The Computerization of Society. A Report to the President of France. – L.: Cambridge, 1980.

[12] Nora S., Minc A. The Computerization of Society. A Report to the President of France. – L.: Cambridge, 1980.

[13] Ibid. P. 134.

[14] Ibid . P . 131.

[15] Цит. по: Соколов А.В. Общая теория социальной коммуникации: Учеб. пособие. – СПб.: Изд-во Михайова В.А, 2002.

информационного общества, «мы наблюдаем некоторые его внешние проявления, но не представляем, чем оно является на самом деле. Соединяя наличествующие фрагменты теории и разрозненные эмпирические данные с фактами изменения социальных отношений, мы пытаемся составить картину грядущей цифровой эры. И под эту гипотетическую картину подгадываем правовую базу, систему образования, духовные ценности. Стремимся подогнать всю систему функционирования социума под нечто умозрительное, приблизительно угадываемое по опыту прошлых информационных революций»[16] .

Большинство теоретиков информационного общества провозглашает его самой прогрессивной формой организации жизнедеятельности людей, реализацией идей идеального общества, развиваемых великим утопистами прошлого – Т.Кампанеллой, Т.Мором и др. Бернд-Петер Ланге и Анетте Барон, характеризуя переход от индустриального к информационному обществу, отмечают, что «использование новых информационных и коммуникационных технологий и новые области их применения на основе мультимедиа – работа на дому, покупка товаров через информационную сеть, обслуживание клиентов в режиме реального времени, кабельное ТВ и т.д. – изменяют нынешнее индустриальное общество. Поэтому символичным представляется и будущее информационное общество, в котором большая часть работающего населения занята в области производства, обработки, управления и обмена информацией. Производство и распределение товаров все больше становятся зависимыми от эффективной информационной и коммуникационной сети. Общество пользователей встанет перед необходимостью создания так называемых «информационных магистралей» [17]. А информационная доступность приведет к изменению экономической структуры индустриального и обслуживающего (постиндустриального) общества в структуру общества информационного.

Значительные уточнения претерпела и такая характеристика информационного общества, как ведущая роль знания в качестве основы социальной стратификации. Стала очевидной необоснованность отождествления Д. Беллом понятий знания и информации. Сегодня скорее приходится говорить о степени доступа к информационным кодам или доступности источников информации как основании социальной стратификации, чем о степени овладения тем или иным теоретическим знанием.

Ряд возражений против классической позиции Д. Белла состоит в том, что процесс коммуникации в мире электронных технологий с преобладанием готового программного обеспечения и соответствующим требованием все менее специализированных знаний, возносит на лидирующие социальные позиции определенный тип людей – обладающих разнообразием и гибкостью когнитивных стилей[18]. И в целом, не уровень знания, а характер отношения к информации становится основанием нового социального неравенства.

Что касается такой характеристики информационного общества, как возможность алгоритмизации и программирования социальных процессов, то на смену идее о грядущей интеллектуальной рациональности человека информационного века пришло утверждение его принципиальной иррациональности, незавершенности, неопределенности.

В итоге приходится признать, что от классических концепций информационного общества на сегодняшний день остались фактически лишь фундаментальный тезис о том, что том, что происшедшие технологические изменения в области создания, передачи и

[16] Тапскотт Д. Электронно-цифровое общество. Пер. англ. – М.: Рефл-бук, 1999.- С. 54

[17] Цит. по.: Шеремет А.Н. Интернет как средство массовой коммуникации: социологический анализ. Дис. ... канд. социол. наук. – Екатеринбург, 2003. – С.39.

[18] См.: Остапенко И.А. Гендерная идентичность и самопрезентация в Интернет-коммуникации (Социально-философский анализ). Дис. ... канд. филос. наук. – Ростов н/Д, 2004.

хранения информации неизбежно влекут за собой изменения в социальных характеристиках общества, порождают определенные социальные процессы и рано или поздно получают выражение на уровне социальной структуры.

В России проблемы развития информационного общества стали предметом исследований, результаты которые представлены в работах И.С.Мелюхина, Д.В.Иванова, С.Э.Зуева, В.В.Емелина, П.Г.Арефьева, И.В.Алексеевой, Р.И.Цвылева и т.д. Р.Ф.Абдеевым была предложена концепция возникновения информационного общества, согласно которой эволюция информационной структуры человеческой цивилизации представляет собой сужающуюся спираль с переменным шагом, построенную в трехмерном пространстве, в координатах информации и с введением параметров времени и прогресса[19]. Непосредственными поводами возникновения информационного общества считает Р.Ф.Абдеев быстрое возрастание роли информационных ресурсов и коммуникаций в жизни общества в результате свершившейся революции в сфере информационных технологий, приведших к целому ряду разнообразных последствий, от появления новых профессий и серьезного изменения социальной структуры общества до возникновения новых стилей в городской архитектуре.

В целом информационное общество представляет собой единое компьютеризированное и информационное сообщество людей, деятельность которых сосредоточена главным образом на обработке информации, информационные технологии приобретая глобальный характер, охватывает все сферы деятельности человека. Различного рода системы на базе микропроцессорной технологии, компьютерных сетей, информационной технологии, телекоммуникационной связи, Интернет являются материальной и технологической базой информационного общества, обеспечивающие движение информационных потоков.

Инфраструктуру информационного общества составляет новая техника, «интеллектуальная», а не «механическая» по своей природе. Важной характеристикой информационного общества является симбиоз информационных технологий и социальной организации.

Основным принципом создания технической базы становления информационного общества является развитие глобальной информационной инфраструктуры – «огромной коммуникационной сети, которая навсегда изменит образ жизни людей во всем мире, изменит то, как они учатся, работают и связываются друг с другом. Эта глобальная сеть позволит людям в самой отдаленной деревне получить доступ к самой современной библиотеке. Она позволит врачам на одном континенте обследовать пациентов на другом континенте. Она позволит семье, живущей в Северном полушарии, поддерживать связь с родственниками в Южном полушарии. И эта сеть укрепит сознание совместной ответственности всех людей на земле за судьбы нашей маленькой планеты»[20] .

К числу стран, в которых наблюдается стремительное развитие глобальных компьютерных сетей, относятся США, Япония, Англия, Германия, страны Западной Европы. В этих странах инвестиции и поддержка инноваций в информационной индустрии, развитие компьютерных систем и телекоммуникаций стали ведущим направлением государственной политики, что способствует созданию технической базы формирования информационного общества. «Компьютерные технологии и информационные сети, являются символами нового общества, приходя на смену фабрикам – символам индустриального общества»[21]. С развитием и распространением

[19] См: Абдеев Р.Ф. Философия информационной цивилизации. – М.: Дело, 1994.- С. 59.

[20] Тревоги мира. Социальные последствия глобализации мировых процессов. Доклад ЮНРИСД, М.: Научно-исследовательский институт социального развития при ООН, 2004. – С. 2.

[21] Тоффлер Э. Шок будущего. М.: АСТ, 2001. – С. 34.

Интернета способности индивидов и социальных групп получать информацию значительно расширились.

В настоящее время наблюдается компьютеризация всех сфер общественной деятельности и повседневной жизни человека. Помимо количественного роста и высоких темпов проникновения компьютерных технологий во все сферы жизнедеятельности индивидов и социальных групп, с развитием Интернета происходит приумножение числа способов применения персональных компьютеров. Из вычислительной машины компьютер превратился в универсальное устройство, способное служить средством труда в различных профессиях как технических, так и гуманитарных, а также средством обучения, общения, развлечений.

Влияние информационных технологий на общественные процессы связано также со стремительным падением стоимости компьютерных и Интернет-технологий. Одним из основополагающих принципов создания технической базы формирования информационного общества является открытый доступ к глобальной информационной инфраструктуре. Согласно известному закону Меткалфа мощность компьютерной сети увеличивается в пропорции, равной квадрату числа ее пользователей. Иными словами, чем больше людей присоединяется к Интернет, тем в большей степени вырастет число людей, которые хотели бы пользоваться этой системой: так, если число людей, пользующихся системой, удваивается, то число возможных вариантов соединения людей и объединения их талантов и идей увеличивается в четыре раза «Закройте людям доступ к сети – и она потеряет свою ценность. Дайте людям доступ – и получаемая каждым выгода будет резко возрастать»[22].

Благодаря распространению и развитию информационных и телекоммуникационных технологий человек получает возможность активно участвовать в политической, государственной, экономической, образовательной, социальной жизни общества. Поэтому в информационном обществе более интенсивно, чем в индустриальном обществе, происходит распадение социума на два класса: класс интеллектуалов, носителей знаний, и класс тех, кто не входит в новую информационную экономику. Жесткость этого разделения обусловлена тем что в принципе информационный класс имеет возможность создать готовую продукцию фактически без применения труда людей[23].

Являясь новым средством опосредования деятельности, Интернет-технологии являются средством опосредования внутреннего мира человека, что находит отражение в формировании своего рода «компьютерном сознании»[24] . По данным психологов, они изменяют даже психологические характеристики субъекта компьютеризированной деятельности на уровне субъекта деятельности, субъекта познания, субъекта общения, вызывая различного рода изменения в познавательной, мотивационной, эмоциональной сферах личности[25].

На сегодняшний день во всех ведущих странах мира, использующих информационные технологии в национальных интересах, разрабатываются и действуют государственное программы по вхождению в глобальное информационное общество. Эти программы, содержат ответы на три основополагающих вопроса: а) цель создания в стране информационного общества; б) определение средств и путей достижения этой

[22] Тревоги мира. Социальные последствия глобализации мировых процессов. Доклад ЮНРИСД, М.: Научно-исследовательский институт социального развития при ООН, 2004.

[23] Ракитянский Н.М. Россия и вызовы глобализации//Социс. 2002. № 4. – С.60.

[24] Тихомиров О.К. Психологические аспекты процесса компьютеризации. М: Дело, 1993. – С. 8.

[25] Кузьмина К.Е. Влияние компьютеризированной деятельности на межличностные отношения в юношеском возрасте. 3-я Российская конференция по экологической психологии (15-16 сентября 2003 г., Москва). Секция 10. Психологические аспекты Интернет-среды. Доклад. – С.1.

цели, направленных на расширение сферы применения информационных технологий, упрощение доступа к информации, создание политических, экономических, культурных и правовых условий, способствующих усилению равномерности национального информационного пространства; в) распределение политических, экономических, финансовых и организационных ролей и ответственности между участниками – государством, обществом, бизнесом[26]. 22 июля 2000 года в Окинаве президенты восьми ведущих индустриальных стран мира подписали Хартию Глобального Информационного Общества с целью развития мировой экономики и переходу к новой фазе развития общества. В документе отражаются многообразные аспекты сущности и становления информационного общества. Основополагающая роль в развитии глобального информационного общества возлагается на международную компьютерную сеть Интернет.

В настоящее время существуют две наиболее успешно действующих и опробованных в мире моделей вхождения в информационное общество: калифорнийской (США), где ведущую роль играет бизнес, и финской, раскрывающей взаимодействие бизнеса, гражданского общества и государства.

Финская модель разработана совместно социологом и руководителем одной из старейших фирм Интернет-провайдеров в Финляндии М.Бееком и П.Химаненом – финским социологом, соавтором книги «Информационное общество и государство благосостояния: Финская модель» информационного общества», (совместно с М.Кастельсом). Предпринятый Финляндией опыт успешного взаимодействия государства, гражданского общества и бизнеса по переходу к новым информационным технологиям, продемонстрировал возможность иной по сравнению с калифорнийской, более сбалансированной модели эффективной информационной трансформации. В рамках этой модели государство, будучи общественным институтом, не ориентированным на получение прибыли, стимулирует и обеспечивает воспроизводство интеллектуального потенциала, финансируя сферы образования, научные и инновационные центры в качестве сфер социального роста, а также поддерживает необходимый уровень экономической, структурной, коммуникационной и информационной равномерности в обществе. Бизнес служит реализации, обмену и распространению готового информационного продукта, эффективным каналом связи между потребителями и производителями, важным средством конкурентного развития. Общество в лице негосударственных некоммерческих организаций формирует политические рамки взаимодействия государства и бизнеса, являясь барометром всего процесса. Благодаря реализации этой концепции Финляндия стала на сегодняшний день одним из лидеров глобального информационного общества[27].

В связи с проблемами формирования информационного общества в России представляют интерес выводы В.А.Ядова, обобщившего многолетнюю дискуссию социологов по теоретико-методологическим основаниям изучения России как трансформирующегося общества с учетом специфики развития российского социума. В частности, В.А.Ядов отмечает, что спецификой характеристикой России является информационная пассивность граждан. Долгие годы основной чертой советской информационной среды являлась ведомственная закрытость. Режим секретности значительной части социально значимой информации породил глубоко укоренившийся коммуникационный барьер, нежелание ни делиться информацией ни получать ее. Поэтому становление информационного общества требует изменения национального

[26] Глинчикова А.. Россия и информационное общество. М.: АСТ, 2002. – С 32

[27] Вартанова Е. См.: Информационное Общество и СМИ Финляндии в европейской перспективе. М.: МГУ, 1999.

менталитета, что в свою очередь, требует продолжительных и целенаправленных усилий по изменению состояния общественного сознания.

На основе проведенного теоретического анализа существующих концепций информационного общества мы приходим к выводу, что в содержании самого понятия информационного общества с момента его появления произошли значительные изменения, которые косвенно отражают трансформации сознания в связи с изменившейся ролью информации в жизни общества. Если классики теории постиндустриального общества, вводя в употребление понятие информационного общества, считали основополагающим принципом этого общества производство информации и информационный обмен, то, по мере усложнения информационных процессов и появления качественно новых форм информационного обмена, формировалось понимание того, что главной отличительной характеристикой информационного общества является возникновение принципиально новых форм коммуникации.

Это, в свою очередь, порождает такие явления в сфере сознания, как снижение ценности рационального знания, усиление роли субъективных факторов в структуре информационных потоков, повышение значимости обратной связи в коммуникационных взаимодействиях. В результате этих трансформаций уже не информация, а коммуникация оказывается центральным звеном информационного общества. В этих условиях сознание общества становится менее жестко структурированным, более мобильным и полиморфным, что отражается на всех сферах общественной жизни. Так, в организационной сфере вследствие происходящих трансформаций главным основанием социальной стратификации становится уже не доступ к материальным и финансовым ресурсам, а доступность коммуникативных полей.

Наиболее серьезные трансформации претерпевает материально-производственная сфера социальной деятельности. Главным принципом создания технической базы информационного общества становится развитие глобальной информационной инфраструктуры Интернет. Однако развитием технических возможностей Интернета не ограничивается содержание этого процесса, важнейшей его составляющей являются люди, участвующие Интернет-коммуникациях и тем самым создающие коммуникативное пространство информационного общества, в чем проявляется воздействие базисных трансформаций, происходящих в производственно-экономической сфере на все остальные сферу жизни общества.

Библиографический список

1. Вартанова Е. Информационное Общество и СМИ Финляндии в европейской перспективе. М.: МГУ, 1999. – С. 37.
2. Глинчикова А.. Россия и информационное общество. М.: АСТ, 2002.
3. Тревоги мира. Социальные последствия глобализации мировых процессов. Доклад ЮНРИСД, М.: Научно-исследовательский институт социального развития при ООН, 2004.
4. Ракитянский Н.М. Россия и вызовы глобализации//Социс. 2002. № 4. – С.60.
5. Тихомиров О.К. Психологические аспекты процесса компьютеризации. М: Дело, 1993. – С. 8.
6. Кузьмина К.Е. Влияние компьютеризированной деятельности на межличностные отношения в юношеском возрасте. 3-я Российская конференция по экологической психологии (15-16 сентября 2003 г., Москва). Секция 10. Психологические аспекты Интернет-среды. Доклад. – С.1.
7. Тоффлер Э. Шок будущего. М.: АСТ, 2001.

8. Остапенко И.А. Гендерная идентичность и самопрезентация в Интернет-коммуникации (Социально-философский анализ). Дис. ... канд. филос. наук. – Ростов н/Д, 2004.
9. Абдеев Р.Ф. Философия информационной цивилизации. – М.: Дело, 1994.
10. Соколов А.В. Общая теория социальной коммуникации: Учеб. пособие. – СПб.: Изд-во Михайова В.А, 2002.
11. Тапскотт Д. Электронно-цифровое общество. Пер. англ. – М.: Рефл-бук, 1999.

A.V.Selyutin

BASIC TRANSFORMATION OF MODERN SOCIETY: GLOBAL TRANSFORMATIONS IN THE SPHERE OF PRODUCTION AND THE INFORMATION SOCIETY

Abstract: Based on the theoretical analysis of the existing concepts of information society shows that the content of the concept of information society since its inception there have been significant changes, which indirectly reflect the transformation of consciousness because of the changing role of information in society.

Keywords: information society, the historical and philosophical digression.

УДК 316.4

МОДЕЛЬ SAAS И ЭЛЕКТРОННОЕ ПРАВИТЕЛЬСТВО

Д.А.Беляев[28]

Аннотация: В статье рассматривается современная технология предоставления услуг в электронном виде SaaS. Анализируется уровень использования и проблемы внедрения облачных вычислений на современном ИТ-рынке России.

Ключевые слова: программное обеспечение как услуга, электронное правительство, облачные вычисления.

В последнее время всё чаще говорят о модели SaaS. Что же это такое и где её можно применить? Если касаться определения этой модели, то SaaS — это сокращенная аббревиатура от англоязычного словосочетания Software as a Service. Software as a service (SaaS) дословно переводится как «программное обеспечение как услуга» .

Это модель предложения программного обеспечения потребителю, при которой поставщик разрабатывает веб-приложение, размещает его и управляет им (самостоятельно либо через третьих лиц) с целью и возможностью использования заказчиками через Интернет. Заказчики платят не за владение программным обеспечением как таковым, а за его использование (напрямую через web-браузер, через API, доступный через веб или веб-службы). Модель SaaS позволяет получать преимущества коммерческой лицензии программного обеспечения, эксплуатации без сложностей сопровождения/администрирования и невысокой стоимости владения.

Многие виды программного обеспечения хорошо подходит для SaaS. Примерами могут служить управление клиентских отношений (CRM), видео конференций, управление персоналом (HR), управление проектами, электронная почта. Модель SaaS отличается от более ранних моделей тем, что SaaS решения были разработаны специально для доступа через Internet с помощью web-браузера. SaaS приложения обычно лицензируются по количеству пользователей, иногда с относительно небольшим минимальное количество пользователей.

Основными характеристиками модели SaaS являются:

• сетевой доступ и работа, коммерческого (не разработанного под конкретного клиента) программного обеспечения;

• все функции сосредоточены на одном Internet-ресурсе, что позволяет пользователям работать удаленно через Internet;

• централизованное обновление устраняет необходимость загрузки патчей или обновлений.

Если говорить о сферах применения этой модели, то они достаточно широки. Это и бизнес, и отрасли образования и науки, а также управление государственными и муниципальными услугами посредством технологий электронного правительства.

И.О. Щёголев, министр связи и массовых коммуникаций и известный сторонник новейших технологий, на конференции в МГУ 25 мая 2011 года сообщил, что особое внимание в процессах построения электронного правительство уделяется использованию именно модели SaaS. «При использовании этой модели каждый регион не должен создавать у себя систему с нуля. Он получает и инфраструктуру, и программное обеспечение, и конкретные решения в качестве услуги», — отметил министр. Игорь Щёголев подчеркнул, что затраты на создание системы с нуля на порядок отличаются от покупки услуги.

[28] Министерство образования Республики Коми

По словам главы Минкомсвязи, уже появляется набор участников рынка, работающих с единой платформой. Эти компании могут приходить на места и предлагать регионам решения по переводу государственных услуг в электронный вид.

«Рынок подстраивается под предложенную модель, — убежден министр. — У нас уже нет россыпи несочетаемых решений, у нас есть решения, которые стыкуются с центральной платформой. Они взаимозаменимы, и те, кто внедряет эти решения, могут выбрать наиболее подходящее».

Также И.О. Щёголев отметил, что электронное правительство с точки зрения гражданина в первую очередь означает возможность обратиться всего один раз к общеправительственному порталу для получения информации и услуги. «Человек должен обращаться к правительству, а не к отдельным ведомствам или чиновникам», — подчеркнул глава Минкомсвязи.

Некоторое время назад сообщалось об облачных технологиях, которые всё чаще используются в ИТ-задачах. По различным статистическим данным в настоящее время число компаний, платящих за облачные сервисы, составляет 29%. К 2014 году их число увеличится до 39%. Существуют разные прогнозы относительно рынка услуг облачных вычислений, варьирующиеся от 30 млрд. до 300 млрд. долл. в год. Так, исследователи известной аналитической компании Forrester считают, что в данной экономически нестабильной ситуации предсказать объем рынка чрезвычайно трудно. Тем не менее, если принимать во внимание даже самые скромные прогнозы, в которых фигурируют 30–40 млрд. долл., можно утверждать: будущее — за облачными вычислениями.

То, что будущее в ИТ-сфере именно за «облаками», подтверждает и Минкомсвязи РФ в лице министра. Недавно он встречался с представителями корпорации Microsoft. Основной темой встречи стало развитие облачных технологий и их использование для государственных нужд.

Глава Минкомсвязи России напомнил, что в России электронное правительство строится на основе облачных технологий. Узловые точки с большими серверными мощностями — «центральные облака» — расположены в некоторых крупных регионах. «С точки зрения построения электронного правительства мы по части использования облачных технологий продвинулись дальше, чем Соединённые Штаты», — заявил глава Минкомсвязи.

Глава Минкомсвязи России обратил снимание на то что, отдельной темой для обсуждения и совместной работы могла бы стать тема защиты персональных данных. «На следующем этапе мы могли бы инициировать международную конференцию с участием экспертов для обсуждения этих тем», — подытожил он.

В ходе встречи была затронута тема подготовки молодых специалистов в области интернет-технологий. И.О. Щёголев подчеркнул своевременность и перспективность этого направления и предложил специалистам компании «Майкрософт», которые в настоящее время работают по программе сотрудничества со «Сколково», разработать параллельный стратегический проект по созданию факультета компьютерного инжиниринга в одном из российских вузов.

Особое внимание в рамках встречи было уделено обсуждению концепции построения российской Национальной программной платформы, создание которой запланировано в рамках государственной программы Российской Федерации «Информационное общество (2011-2020 годы)». Результатом данного проекта будет создание комплекса преимущественно отечественных программных решений, построенных на базе единых технологий, позволяющих осуществлять разработку новых программных продуктов методом компоновки и настройки уже готовых программных модулей, а также новых подсистем, создаваемых для расширения функционала платформы.

И.О. Щёголев отметил, что министерство изначально оппонировало сторонникам так называемого «китайского пути», подразумевающего создание собственной

операционной системы. «То, что касается программной платформы, в нашем случае в большей степени пересекается с темой свободного программного обеспечения», — пояснил он. «Я бы обратился к слову «платформа». Именно платформа может стать прогрессивной и многообещающей базой для взаимодействия России и «Майкрософт», — подчеркнул министр.

Он напомнил, что до сих пор многие российские компании в качестве оффшорных задач создавали продукты, которые потом входили в качестве части в конечный продукт «Майкрософт». «Если «Майкрософт» сможет предложить платформу, при которой наши компании могли бы приходить не с частичными решениями, а с готовым продуктом — это было бы более выгодно для всех» — добавил И.О. Щёголев.

Российское правительство ежегодно тратит на внедрение информационных технологий в органах власти около 80 млрд руб. Однако российские министерства и ведомства неэффективно расходуют бюджетные средства, убежден вице-премьер РФ С.Б. Иванов. Он заявил об этом на прошедшем в Москве заседании совета генеральных и главных конструкторов, ведущих ученых и специалистов в области высокотехнологичных секторов экономики.

«Мы тратим из федерального бюджета на информатизацию расширенного правительства 80 млрд руб. в год. Это огромные деньги», — признал С.Б. Иванов. Он отметил, что, несмотря на такое финансирование, из года в год при составлении федерального бюджета ряд федеральных министерств и ведомств обращаются с просьбами о выделении дополнительных денег на развитие информационных технологий. По его словам, ряд органов власти без указания сверху начали внедрять информационные технологии, в том числе — облачные вычисления.

«Фрагментарно это у нас уже начинает происходить, причем естественным путем, без принятия каких-либо правительственных решений, постановлений и вообще вмешательства бюрократии в этот процесс. Это просто жизненная необходимость», — пояснил Иванов.

К использованию облачных технологий перешли такие структуры, как Роскосмос, Федеральная налоговая служба, а также «Росатом» и АФК «Система». «Они понимают, что огромные массивы информации, когда хранятся в одном месте, создают очевидные риски, — подчеркнул Сергей Иванов, говоря об использовании облачных вычислений. — По сути, это напоминает простой человеческий принцип: не кладите яйца в одну корзину».

Так, например, в начале этого года ОАО «Российские космические системы» создало совместно с компанией «Оверсан» облако корпоративного уровня. «Первое российское облако инфраструктурного уровня — одна из немногих коммерчески успешных российских инноваций, которые так нужны современной России, вставшей на путь модернизации, — отметил на заседании конструкторов генеральный конструктор „Российских космических систем“ Ю. Урличич. — Этот продукт является готовым инфраструктурным ядром для целого ряда социально значимых проектов и программ государства».

По словам директора департамента техподдержки и аутсорсинга компании «АйТи» В. Ермолова, в последние год-два сама тема облаков стала одной из самых популярных на отечественном рынке. «Поэтому можно с большой долей уверенности говорить и о том, что востребованность таких технологий растет», — сказал В. Ермолов ComNews. А с точки зрения главы представительства компании VMware в России и СНГ А. Антича, все больше клиентов осознают финансовые, экологические и организационные преимущества, которые предоставляют бизнесу виртуализация и облачные вычисления: «Серверная виртуализация стала мейнстримом и в России».

Однако, по словам вице-премьера, российские госструктуры неэффективно расходуют бюджетные средства на развитие ИТ. «Анализируя средства, потраченные государством за последние годы, и комплексную отдачу, связанную с такими вещами, как

электронное правительство, электронные услуги для населения, мы видим, что массивы ряда ведомств не стыкуются между собой, средства расходуются неэффективно», — сетует С.Б. Иванов.

В этой связи, по его словам, Минкомсвязи дано жесткое поручение не пропускать в Минфин без своего согласия заявки министерств и ведомств на развитие внутриведомственных информационных технологий, в том числе облачных. «Иначе у нас тонки слоем деньги распределяются, а толку — чуть», — предупредил вице-премьер.

По мнению вице-премьера, российская высокотехнологичная продукция не востребована на мировом рынке из-за отсутствия информационной поддержки и электронного сопровождения. «К сожалению, пока многие российские предприятия в вопросе информационной поддержки своей продукции существенно отстают от западных конкурентов и поэтому зачастую проигрывают им тендеры на поставку высокотехнологичной продукции», — сказал он, добавив, что правительство уже предпринимает меры для изменения сложившейся ситуации (в частности, утвержден перечень технологических платформ по информационно-коммуникационным технологиям).

С.Б. Иванов отметил, что рост экономики и развитие общества в современном мире напрямую зависят от внедрения передовых информационных технологий. Логичным этапом эволюции информационных технологий является появление облачных вычислений. «По оценкам специалистов, внедрение подобных технологий способно значительно повысить уровень использования вычислительных ресурсов, — отметил Сергей Иванов. — Сейчас этот показатель составляет примерно 20%, а в перспективе его можно будет поднять до 80% или даже 85%».

Таким образом, резюмируя сказанное, можно сделать следующие выводы:

- в современной России все четче проявляется стремление к использованию облачных вычислений, причем это движение осознано не только представителями бизнес структур, но и правительством страны на самом высоком уровне;
- происходит централизация распределения бюджетных средств на ИТ.

Библиографический список

1. Демидов А. Про SaaS в России: от А до Я. Эл. Ресурс. Режим доступа: http://www.cloudzone.ru/articles/analytics/25.html. Дата доступа: 01.07.2011.
2. На международной конференции в МГУ обсуждают инновации в государственном управлении. Эл. Ресурс. Режим доступа: http://www.msunews.ru/news/2647. Дата доступа 15.06.2011.
3. Капустина Т. Иванов недоволен ИТ. Эл. Ресурс. Режим доступа: http://www.comnews.ru/index.cfm?id=62271. Дата доступа: 01.07.2011.

D.A.Beljaev

MODEL SAAS AND THE ELECTRONIC GOVERNMENT

Annotation: In article the modern technology of granting of services in electronic form SaaS is considered. Level of use and a problem of introduction of cloudy calculations in the modern IT Market of Russia is analyzed.

Keywords: the software as service, the electronic government, cloudy calculations.

УДК 316.4

КОГНИТИВНОЕ МОДЕЛИРОВАНИЕ СОЦИАЛЬНО-ЭКОНОМИЧЕСКИХ РЕЙТИНГОВ РЕГИОНОВ

И.И.Лавреш[29]*, В.В.Миронов*[30]*, А.В.Смирнов*[31]

Аннотация: В работе рассмотрена методология когнитивного моделирования. При помощи выбранной методологии моделирования были созданы рейтинги по трем перспективным направлениям социально-экономического развития Республики Коми: рейтинг инвестиционного климата регионов, рейтинг информатизации регионов, рейтинг туристической привлекательности регионов.

Ключевые слова: когнитивный анализ, социальные системы, рейтинг, математическое моделирование

I. В настоящее время анализ рейтингов социально-экономических систем является важным инструментом принятия управленческих решений в области региональной политики. Рейтинги позволяют определить сильные и слабые стороны региона и выработать меры по комплексному улучшению ситуации.

Большинство социально-экономических систем являются слабоструктурированными. Это накладывает ограничение на полноту информации, которой обладает лицо, принимающее решение. Наличие обратных связей и сложных транзитивных зависимостей, действующих в системе, может привести к ее контр-интуитивному поведению.

Другим фактором, затрудняющим понимание социально-экономических систем, являются их постоянно изменяющиеся условия при ограниченном времени принятия решений. Таким образом, подготовку и принятие решений в задачах управления слабоструктурированными системами, следует рассматривать как сложный интеллектуальный процесс разрешения проблем, несводимый исключительно к рациональному выбору [1]. В целях поддержки принятия решений может использоваться подход когнитивного моделирования.

Методология применения когнитивного подхода в управлении слабоструктурированными системами была предложена американским политологом Робертом Аксельродом [2] и в настоящее время активно развивается в Институте проблем управления им. В. А. Трапезникова РАН [3]. Ключевое понятие когнитивного подхода – когнитивная карта.

Когнитивная карта – ориентированный взвешенный граф, в котором вершины соответствуют факторам системы, а дуги взаимосвязям между ними:

$$G =< V, E >,$$

где G – взвешенный орграф, в котором V - множество вершин $v_i \in V, i = \overline{1,n}$, являющихся факторами системы, E – множество дуг $e_{ij} \in E, \quad i,j = \overline{1,n}, \quad i \neq j$ отражают отношения между вершинами v_i и v_j.

Когнитивная карта показывает только факт наличия влияний факторов друг на друга. Для определения характера связей, важности факторов и уточнения параметров системы необходимо перейти на следующий уровень моделирования – создать когнитивную модель [4].

[29] ГАУ РК «Центр информационных технологий Республики Коми»
[30] ФГБОУ ВПО «Сыктывкарский государственный университет»
[31] ФГБОУ ВПО «Сыктывкарский государственный университет»

Когнитивная модель – функциональный граф исследуемой системы, в котором вершины соответствуют факторам системы, а дуги отражают функциональную зависимость между ними.

Распространен подход моделирования, в соответствии с которым исследуется распространение импульса по системе. Импульс интерпретируется как внешнее воздействие на систему, а ребрам присваиваются коэффициенты сопротивляемости прохождению импульса [5].

Компьютерная реализация когнитивной модели подразумевает программное воплощение модели в одной из сред моделирования, позволяющее автоматизировать процесс исследования системы.

Преимущества применения когнитивного подхода в создании рейтингов:

- Наглядность представления взаимосвязей между факторами и средства когнитивной графики облегчают работу экспертов.
- Высокая скорость разработки моделей.
- Небольшая численность команды разработчиков.
- Наличие большого количества инструментальных средств когнитивного моделирования.
- Возможность усовершенствования рейтинговой методологии с помощью средств когнитивного анализа.

Алгоритм когнитивного моделирования рейтингов:

- Формулировка цели и задач моделирования.
- Изучение предметной области и исследование выбранной социально-экономической системы.
- Сбор, анализ и систематизация статистических данных, необходимых для моделирования.
- Построение когнитивной карты.
- Определение агрегированных индикаторов.
- Разбиение модели на подсистемы.
- Последовательная декомпозиция полученных подсистем до первичных статистических показателей.
- Определение взаимосвязей между факторами.
- Создание когнитивной модели.
- Определение направленности связей (положительные или отрицательные) когнитивной карты.
- Определение типов связей между факторами (линейные, полиномиальные, s-образные, …).
- Определение интенсивности (силы) связей между показателями.
- Выделение факторов, которыми возможно управлять.
- Реализация компьютерной модели.
- Выбор инструментальной среды моделирования.
- Перенос модели в выбранную среду.
- Ввод статистических данных.
- Проведение предварительного эксперимента.
- Проверка адекватности модели.
- Моделирование и составление рейтинга.
- Обработка результатов.
- Формулировка выводов и рекомендаций в соответствии с поставленной целью.

Создание социально-экономических рейтингов на основе когнитивных карт имеет некоторые особенности:

- Рейтинги, как правило, имеют иерархическую структуру;

- Для составления рейтинга требуется небольшое число агрегированных индикаторов (чаще всего - один);
- Необходимость вычисления результатов за один временной промежуток, но для большого числа объектов;
- Для создания когнитивной карты требуются обширные знания в предметной области, поэтому непременными атрибутами когнитивного моделирования являются консультации с экспертами и экспертные оценки. Помощь экспертов требуется во время большинства этапов разработки когнитивной модели: от определения структуры системы и причинно-следственных связей факторов до экспертного оценивания силы и направленности их влияния.

Эксперты и разработчики когнитивных карт вносят в них свои субъективные представления о моделируемой системе, что несет значительные риски снижения качества модели. Необходимо вовремя их обнаруживать и реагировать на угрозы, связанные с человеческим фактором.

Поэтому следующим этапом разработки является проверка достоверности полученной когнитивной модели. Для этого применяются критерии достоверности модели: когнитивной ясности математической модели, полноты влияний на фактор, соразмерности объемов понятий факторов и нарушения транзитивности казуальных влияний [6].

Существуют методы экспертной верификации, позволяющие существенно повысить качество когнитивной модели. Они включают как анализ по предопределенным критериям, так и экспертный анализ без предварительных критериев. К предопределенным критериям исследования когнитивных карт можно отнести: критерий монотонности причинно-следственных зависимостей, критерий отсутствия дублирующих влияний, критерий отсутствия ложной транзитивности, критерий полноты влияний внешний среды и др. [7]

С помощью диаграмма активности [8] можно продемонстрировать (Рис. 1) разделение ролей процесса моделирования между разработчиком модели, экспертом и исследователем.

Для проведения эксперимента над моделью необходимо разработать механизмы обработки результатов и обратной связи между экспериментатором и моделью. Для этого применяются различные статистические методы, варьирование параметров и анализ чувствительности модели.

Одной из основных проблем является выбор подходящей среды моделирования. Существует множество систем компьютерной реализации когнитивных моделей. К ним можно отнести разработанные в Институте проблем управления РАН системы [9]: «Ситуация», «КУРС», «Компас», «Компас-2», «КИТ», «Канва». В Брянском государственном техническом университете создана система «Игла», в Волгоградском государственном техническом университете – «Стратег».

Так же имеется возможность создавать когнитивные модели в средах имитационного моделирования и системной динамики: AnyLogic, Vensim, PowerSim, iThink. В них ограниченны возможности использования лингвистических переменных и нечетких вычислений, однако их функционал достаточен для большинства задач. Некоторые из программ имитационного моделирования включают внутренний язык программирования, позволяющий создавать различные пользовательские интерфейсы и средства обработки результатов.

При помощи выбранной методологии моделирования были созданы рейтинги по трем перспективным направлениям социально-экономического развития Республики Коми:

- Рейтинг инвестиционного климата регионов;
- Рейтинг информатизации регионов;
- Рейтинг туристической привлекательности регионов.

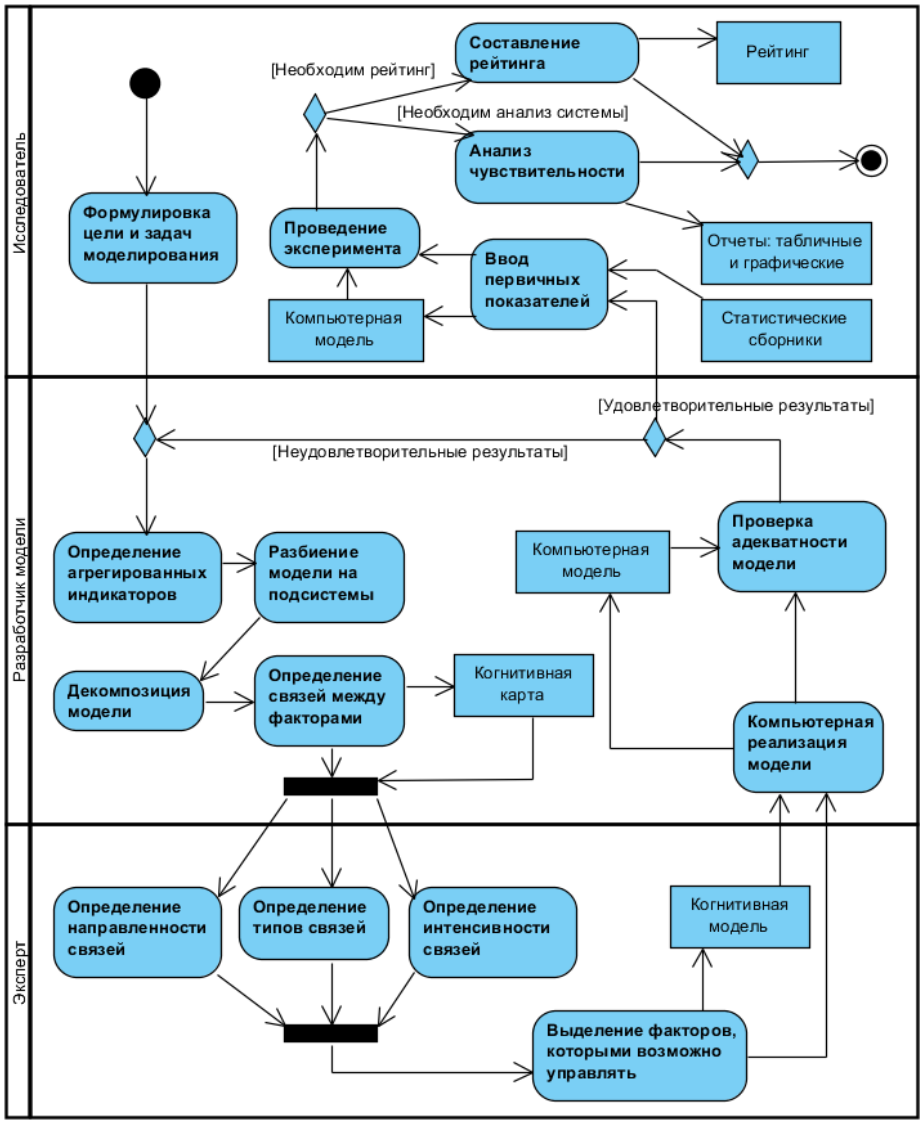


Рис. 1. Диаграмма активности когнитивного моделирования.

II. В современных условиях, улучшение инвестиционного климат региона является важнейшей целью региональной политики. Для повышения конкурентоспособности Республики Коми необходимы серьезные капитальные вложения в экономику региона. Выявление и анализ факторов, влияющих на привлекательность региона в глазах инвесторов, должны привести к более глубокому пониманию инвестиционных процессов. А решения, принятые при понимании скрытых и обратных связей системы – к росту производства, сферы услуг и созданию в Республике Коми инновационной экономики.

Таблица 1. Подсистемы модели инвестиционного рейтинга.

Инвестиционный потенциал	Инвестиционные риски
Инновационный потенциал Институционный потенциал Инфраструктурный потенциал Потребительский потенциал Производственный потенциал Ресурсно-сырьевой потенциал Трудовой потенциал Финансовый потенциал	Законодательные риски Криминальные риски Политические риски Социальные риски Финансовые риски Экологические риски Экономические риски

Инвестиционный рейтинг – количественный показатель инвестиционной привлекательности региона. Это главный интегральный индикатор модели. В инвестиционный рейтинг входят инвестиционный потенциал (позитивное влияние) и инвестиционные риски (негативное влияние). Их можно разделить (Табл. 1) на 8 и 7 групп соответственно [10].

Не все группы факторов одинаково влияют на итоговый результат. С помощью экспертного оценивания были получены веса, соответствующие силе связей между подсистемами и агрегированными показателями. С учетом вышесказанного, можно произвести декомпозицию модели на три уровня (Рис. 2).

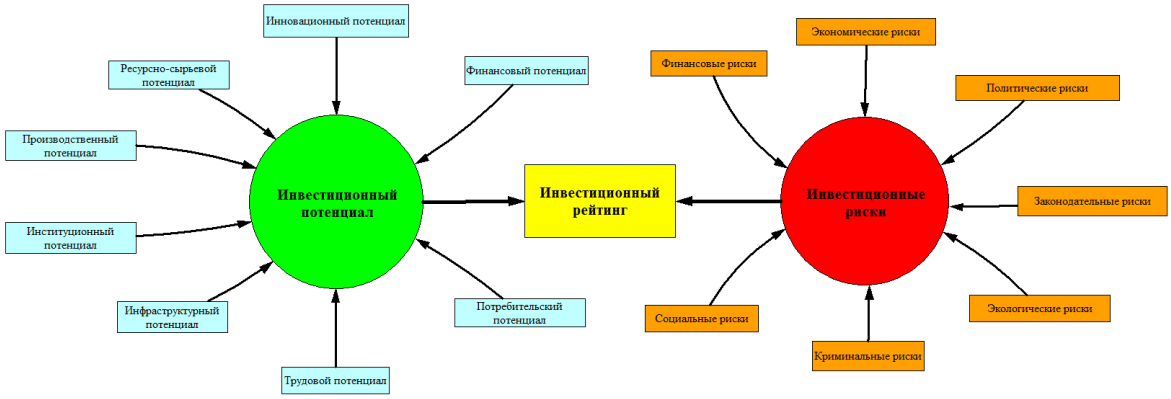


Рис. 2. Структура инвестиционного рейтинга.

В ходе дальнейшей разработки модели была произведена декомпозиция полученных подсистем на 105 базовых социально-экономических факторов, определены взаимосвязи между ними и получены экспертные оценки их весовых коэффициентов. Структура одной из подсистем модели представлена на рис. 3. Некоторые факторы модели влияют сразу на несколько подсистем. Они требуют особого внимания, поскольку могут сделать поведение исследуемой системы непредсказуемым.

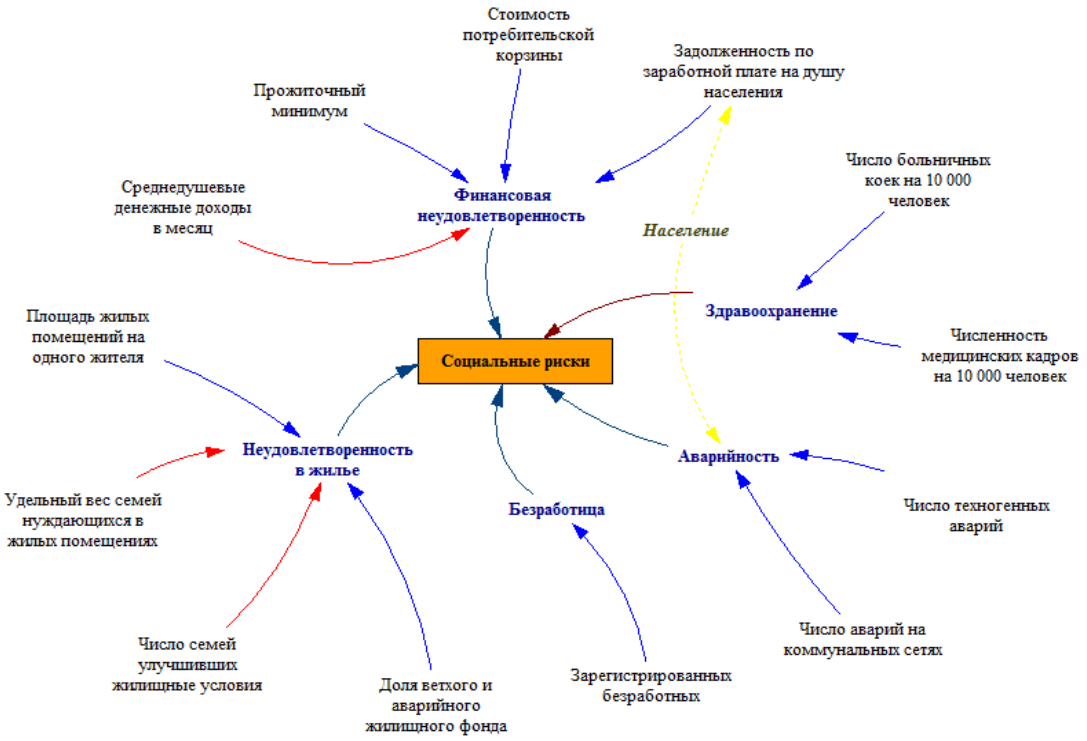


Рис. 3. Социальные риски региона.

При публикации инвестиционных рейтингов принято указывать значения инвестиционного потенциала и рисков отдельно [11], а не вычислять их средневзвешенное значение. В ходе предварительного эксперимента были получены значения основных индикаторов инвестиционного климата региона. Дальнейшие исследования позволят определить наименее и наиболее эффективные области социально-экономического развития региона в целях совершенствования экономики и повышения инвестиционной привлекательности.

III. Следующая модель создана для поддержки принятия управленческих решений в области информатизации региона. Сегодня интернет и информационные технологии имеют большое значение для развития гражданского общества. Сфера информационных технологий имеет сложную структуру, динамично развивается и требует детального изучения.

Рейтинг информатизации регионов совмещает в себе как уровень использования в регионе информационных технологий бизнесом и населением [12], так и оценку степени внедрения ИТ в региональных и муниципальных органах власти. Важнейшим фактором при этом является качество [13] электронного правительства региона [14] (число и степень внедрения электронных услуг, инфраструктура и техническое обеспечение электронного правительства).

Таблица 2. Подсистемы модели рейтинга информатизации.

Факторы развития информационного общества	Использование информационных технологий	Уровень внедрения электронного правительства
ИТ – инфраструктура Человеческий капитал Деловой климат	ИТ в бизнесе ИТ в здравоохранении ИТ в культуре ИТ в домохозяйствах ИТ в органах власти	Муниципальные услуги Государственные услуги Инфраструктура ЭП Техническое обеспечение ЭП

Структура рейтинга информатизации (Табл. 2) позволяет всесторонне проанализировать состояние информационных технологий в регионе и его готовность к информационному обществу.

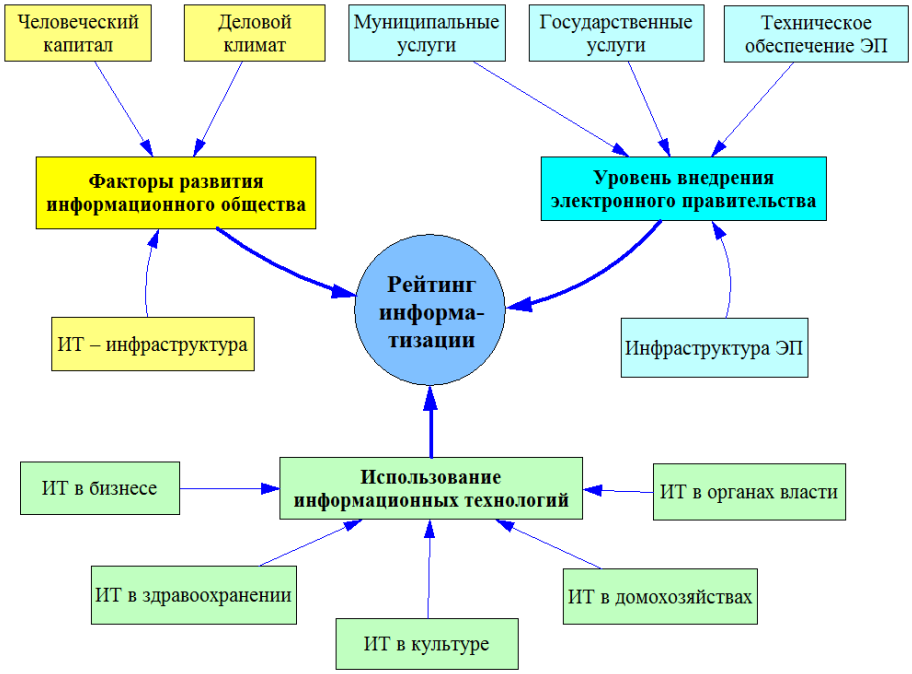


Рис.4. Структура рейтинга информатизации в Vensim.

IV. Одна из основных задач, стоящих перед Республикой Коми в ближайшее десятилетие – многократный рост потока туристов в регион [15]. В связи с этим, необходимо определить направления, по которым Республика Коми отстает от других регионов и пути улучшения ситуации.

При составлении туристического рейтинга важно учесть как природные условия региона, так и развитие туристической инфраструктуры и сервиса (Табл. 3). На развитие туризма сильно влияет безопасность в регионе: уровень преступности, транспортные аварии, число пожаров и др. Не меньшую значимость имеют и туристическая репутация региона, наличие объектов Всемирного наследия, природных памятников, заповедников и национальных парков.

Таблица 3. Подсистемы модели туристического рейтинга.

Природно-климатические условия	Инфраструктура	Культура и развлечения	Торговля и услуги
Природные условия Климатические особенности Экологическая ситуация	Связь и коммуникации Транспорт Безопасность	Культура Отдых Развлечения	Торговля Услуги Цены

Особенность рейтинга туристической привлекательности в разнонаправленном влиянии многих факторов на различные виды туризма (летний и зимний, рекреационный и деловой). Поэтому выбрана структура рейтинга, в которой факторы имеют разные веса в рамках различных подсистем и итоговый результат вычисляется с учетом популярности в РФ того или иного вида туризма. Так, степень урбанизации, благоприятно влияющая на деловой туризм, может отрицательно сказаться на оздоровительном.

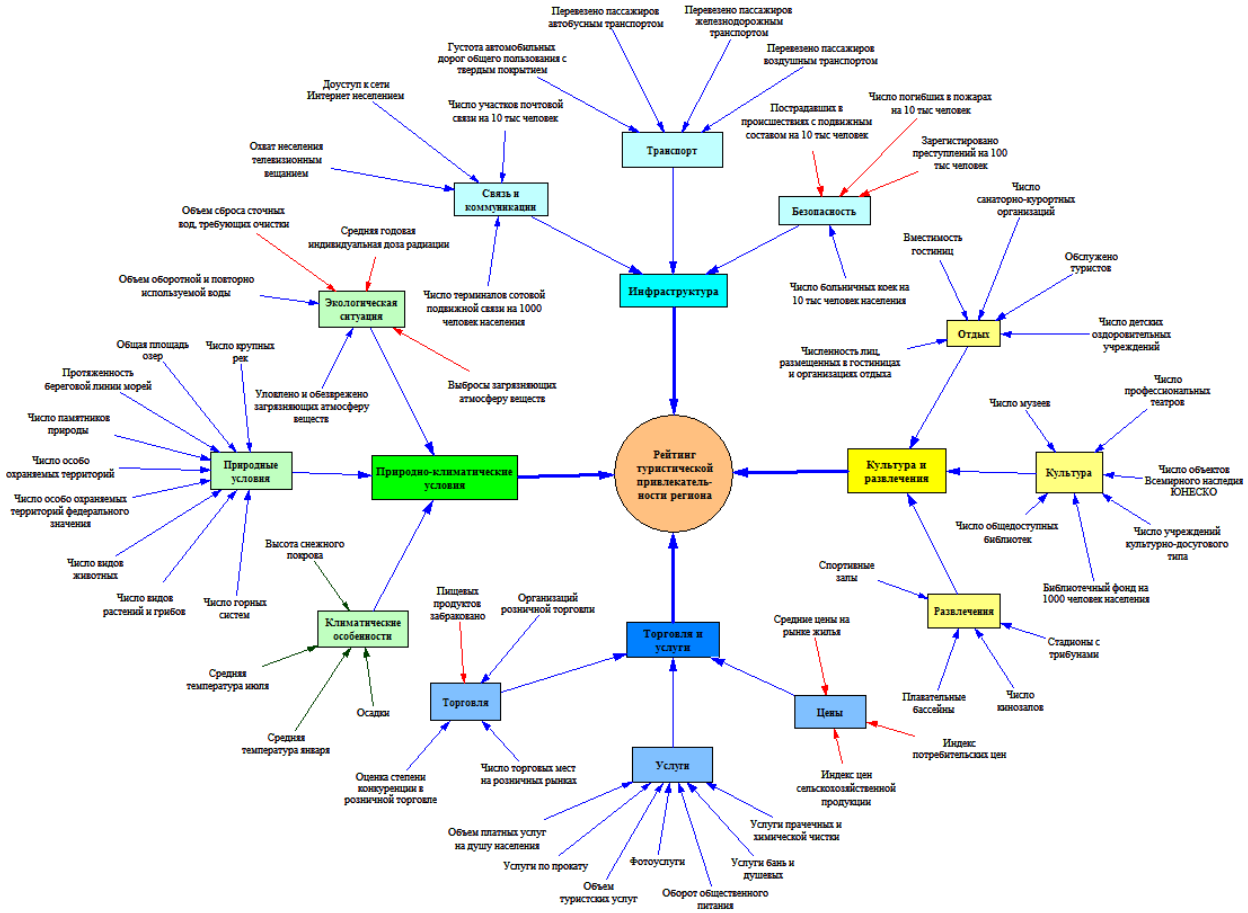


Рис.5. Туристический рейтинг в Vensim.

Статистические данные для показателей рейтингов были получены из общероссийского [16] и территориальных [17] статистических сборников Федеральной службы государственной статистики РФ.

V. В процессе использования рейтингов на основе когнитивных карт были получены оценки социально-экономических систем, смоделированы различные варианты влияния изменения показателей на значения региональных рейтингов.

В результате проделанной работы создан продукт, позволяющий моделировать инвестиционный климат региона, составлять рейтинги инвестиционной привлекательности и способствовать принятию качественных управленческих решений в области инвестиционной политики. Созданные модели могут использоваться при принятии решений в области социально-экономической политики региона.

Можно выделить некоторые наиболее перспективные направления дальнейшего развития подхода, рассматриваемого в статье:

- Ежегодная публикация рейтингов регионов, построенных в соответствии с полученной методологией.
- Применение сходной методологии при моделировании других социально-экономических систем (например, образование, здравоохранение, экология, предпринимательство и др.).
- Создание рейтингов районов в пределах субъекта РФ.
- Интеграция в модели структуры распределения бюджетных средств и прогнозирование влияния бюджетирования на состоянии систем. Такой прогноз позволит определить наиболее сильные и слабые направления внутренней политики региона.
- Совершенствование средств анализа чувствительности и обработки результатов моделирования.
- Введение в модель лингвистических переменных и алгоритмов нечеткого вывода. Это позволит более адекватно использовать при моделировании экспертные оценки социально-экономических показателей.
- Создание более развитого и эргономичного интерфейса модели.
- Использование других методологий моделирования (в частности агентного и системодинамического), а так же их совмещение для дальнейшего исследования систем.
- Создание комплекса программ для поддержки принятия управленческих решений в области социально-экономической политики региона.

Библиографический список

4. Авдеева З.К., Коврига С.В., Макаренко Д.И., “Когнитивное моделирование для решения задач управления слабоструктурированными системами (ситуациями)”, УБС, 16 (2007), 26–39
5. Axelrod R. The Structure of Decision: Cognitive Maps of Political Elites. – Princeton. University Press, 1976
6. Максимов В.И. Когнитивный анализ и управление развитием ситуаций. – Материалы 1-й международной конференции в 3-х томах/ Под. Ред. В.И. Максимова. – М., 2001.
7. Максимов В.И., Корноушенко Е.К., Качаев С.В. Когнитивные технологии для поддержки принятия управленческих решений // Технологии информационного общества 98. М.: ИПУ РАН, 1999.
8. Кочкаров А.А., Салпагаров М.Б., “Когнитивное моделирование региональных социально-экономических систем”, УБС, 16 (2007), 137–145

9. Абрамова Н.А., Коврига С.В., “Некоторые критерии достоверности моделей на основе когнитивных карт”, Пробл. управл., 2008, № 6, 23–33
10. Абрамова Н.А., “Экспертная верификация при использовании формальных когнитивных карт. подходы и практика”, УБС, 30:1 (2010), 371–410
11. Буч Г., Рамбо Дж., Джекобсон А.. Язык UML. Руководство — 2-е изд. — М., СПб.: ДМК Пресс, Питер, 2004. — 432 с.
12. Кулинич А.А., “Компьютерные системы моделирования когнитивных карт: подходы и методы”, Пробл. управл., 2010, № 3, 2–16
13. Марченко Г., Мачульская О. Исследование инвестиционного климата регионов России: проблемы и результаты/Вопросы экономики.-1999.-№9-С.69-79
14. Рейтинг инвестиционной привлекательности регионов России. Рейтинговое агентство «Эксперт РА» http://www.raexpert.ru/ratings/regions/ratingclass/
15. Индекс готовности регионов России к информационному обществу 2004‑2005 / Под ред. Т.В. Ершовой, Ю.Е. Хохлова и С.Б. Шапошника. — М.: Институт развития информационного общества, 2005. — 212 с.
16. Методика составления Рейтинга субъектов РФ по уровню внедрения Электронного правительства. http://gosman.ru/electron?news=17324
17. Распоряжение Правительства Республики Коми от 16.08.2010г. №361-р "Об утверждении Концепции информатизации Республики Коми". http://rkomi.ru/content/4854/361-p.doc
18. Гайзер В.М.. Стратегия: «От мечты к реальности - 10 лет пути». http://rkomi.ru/content/6017/2011.01.13_Стратегия%20В.Гайзера.doc
19. Российский статистический ежегодник. 2010: Стат.сб./Росстат. М., 2010. 813 с.
20. Статистический ежегодник Республики Коми. 2010: Стат.сб./Комистат. Сыктывкар, 2010. 502 с.

I.I. Lavresh, V.V. Mironov, A.V. Smirnov

COGNITIVE MODELING SOCIO-ECONOMIC TIMES REGIONAL

Annotation: The paper considers the methodology of cognitive modeling. With the chosen modeling methodology ratings were established in three promising areas of socio-economic development of the Komi Republic: the rating of the investment climate regions, the rating information regions, the rating of tourist attraction areas.

Keywords: cognitive analysis, social system, the rating of the mathematical modeling

Информационные технологии в образовании

УДК 681.3

МОДЕЛИРОВАНИЕ И ОЦЕНКА СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРИМЕРЕ ФГБОУ ВПО «Сыктывкарский государственный университет»

В.В.Миронов[32]*, И.А.Носаль*[33]

Аннотация: В работе рассматриваются вопросы моделирования систем обеспечения информационной безопасности, строятся модели таких систем. Приводятся результаты моделирования систем обеспечения информационной безопасности на примере ФГБОУ ВПО «Сыктывкарский государственный университет» в виде числовых оценок и даются рекомендации по совершенствованию названной системы.

Ключевые слова: моделирование, система, информационная безопасность.

Успешность современной компании во многом зависит от эффективности использования информационных технологий. Все набирающая обороты информатизация вносит свои коррективы в постановку задачи создания систем защиты информации. Кроме того, что информация стала самостоятельным активом, нуждающимся в защите, она сама по себе может имеет различный статус и отличительные характеристики в зависимости от состояния: информация ограниченного доступа, информация, требующая обеспечения постоянной доступности или целостности, защита информации в состоянии обработки, передачи и хранения и так далее, что обеспечить бывает достаточно сложно. Для обеспечения информационной безопасности какого-либо объекта информатизации необходимо придерживаться комплексного подхода.

Создание систем защиты с учетом особенностей защищаемого объекта и принципов информационной безопасности (ИБ), учитывая при этом системность требований по защите, достаточно сложный процесс, поэтому, как и в любой другой науке для этих целей применяется моделирование. Необходимость создания моделей систем обеспечения ИБ (СОИБ) и моделирования процессов ИБ связана также с тем, что оценка (например: эффективности управления, функционирования) СОИБ - системная задача, требующая анализа и синтеза исходных данных, гипотез, теорий, знаний специалистов, а построение модели системы позволяет использовать эту модель для оценки.

Объектом исследования являются модели СОИБ и методики их оценки. Предмет исследования - СОИБ конфиденциального сегмента ИС Сыктывкарского госуниверситета. Цели работы можно сформулировать следующим образом:

1. Создать модель системы обеспечения информационной безопасности, провести ее анализ.

2. Провести оценку СОИБ конфиденциального сегмента ИС Сыктывкарского государственного университета и дать рекомендации по ее улучшению.

Для достижения целей были поставлены следующие задачи:

1. Провести анализ существующих методик и моделей оценки СОИБ.
2. Подготовить методику оценки СОИБ на основе известных методик оценки.
3. Подготовить методику обработки экспертной информации.
4. Провести исследование и оценку СОИБ.

[32] ФГБОУ ВПО «Сыктывкарский государственный университет»
[33] ФГБОУ ВПО «Сыктывкарский государственный университет»

5. Обработать результаты и дать оценку СОИБ и рекомендации по улучшению СОИБ.

Системная классификация моделей ИБ в настоящее время не произведена, возможно, ввиду малого числа таких моделей или недостаточности данных, поэтому хотелось бы представить свою классификацию моделей (см. рис. 1) .

Перейдем теперь к разработке модели и методики оценки СОИБ на основе известных моделей. В качестве базовой выберем модель трехмерной матрицы. Модель создавалась в целях научного обеспечения процесса создания систем защиты информации за счет правильного выбора вариантов технических решений. Для этого требуется составить такое представление об информационной безопасности чтобы охватить все аспекты проблемы и все связи между ними. Чтобы реализовать подход системности в модели предлагается представить ее в виде трехмерной матрицы, направления координат которой (основы, этапы, направления) отвечают на вопросы:

1. Из чего состоит СОИБ? (основы)
2. Для чего предназначена? (направления)
3. Как работает? (этапы)

Под основами понимается законодательная, нормативно-правовая и научная база; структура и задачи органов (подразделений), обеспечивающих безопасность ИТ; организационно-технические и режимные меры и методы (политика информационной безопасности); программно-технические способы и средства.

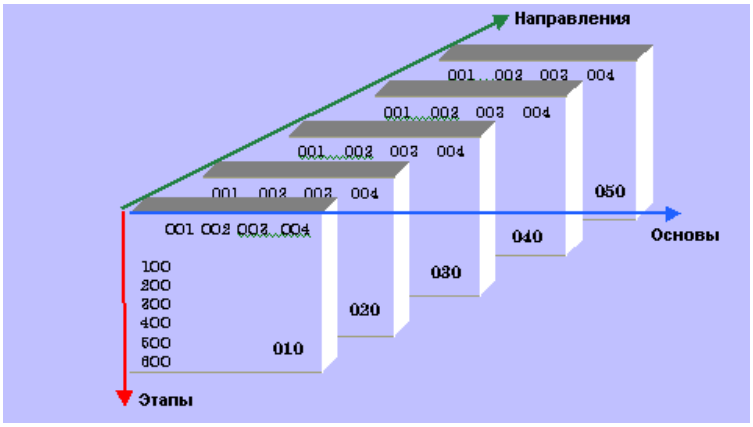


Рис.1. Трехмерная матрица.

В общем случае, учитывая типовую структуру ИС и исторически сложившиеся виды работ по защите информации, предлагается рассмотреть следующие направления:защита объектов ИС; защита процессов, процедур и программ обработки информации; защита каналов связи; подавление побочных электромагнитных излучений; управление системой защиты.

На основе проведенного анализа существующих методик (последовательностей) работ по созданию СОИБ, выделяются следующие этапы: определение информационных и технических ресурсов, а также объектов ИС подлежащих защите; выявление полного множества потенциально возможных угроз и каналов утечки информации; проведение оценки уязвимости и рисков информации (ресурсов ИС) при имеющемся множестве угроз и каналов утечки; определение требований к системе защиты информации; осуществление выбора средств защиты информации и их характеристик; внедрение и организация использования выбранных мер, способов и средств защиты; осуществление контроля целостности и управление системой защиты. Особенность рассматриваемой модели в том, что она является не только концепцией, но и реальным инструментом оценки и построения СОИБ, благодаря тому, что приводится не только схема взаимосвязи различных составляющих ИБ в виде трехмерной таблицы (матрицы), но и предлагается собственная методика проведения оценки СОИБ с использованием этой матрицы. Ответы на вопросы анкеты, построенной по матрице, позволяют сформировать некое представление о состоянии дел по защите информации в конкретной ИС и может выступать в роли руководства по созданию СОИБ.

Если все элементы матрицы заполнить соответствующими оценками (собрать их предлагается экспертным путем), то после обработки результатов можно будет судить об эффективности создаваемой или уже функционирующей СОИБ, оценить эффективность

принимаемых решений и выбрать рациональный вариант технической реализации СОИБ. Таким образом, эту модель можно рассматривать не только на уровне концепции, но и как практический применимый инструмент оценки СОИБ.

Объект исследования. Объектом моделирования данной работы является СОИБ, реализуемая для выделенной информационной системы Сыктывкарского государственного университета. Данная информационная система концентрирует в себе всю наиболее значимую и конфиденциальную информацию, обрабатываемую в ФГБОУ ВПО «Сыктывкарского государственного университета», поэтому обеспечение ее безопасного функционирования является важной задачей для организации. Поскольку информационная система содержит такие категории информации конфиденциального характера как коммерческая тайна и персональные данные, к созданию системы защиты подходили с учетом соответствующих требований законодательства.

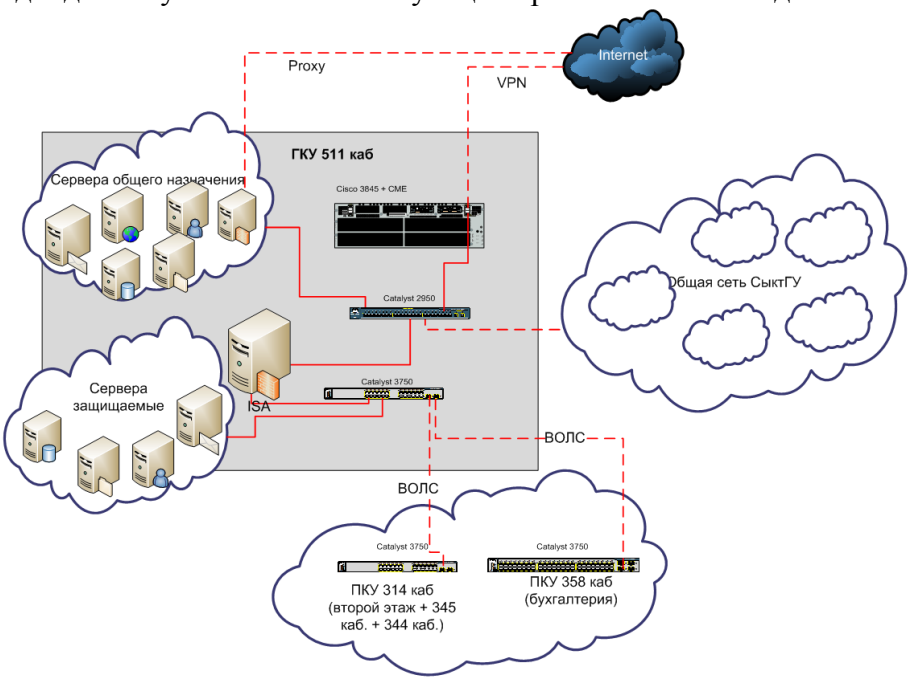


Рис. 2. Логическая схема ИС Сыктывкарского государственного университета.

Создание и функционирование СОИБ регламентировано в таких документах как «Положение о системе защиты закрытых цифровых информационных ресурсов в Сыктывкарского государственного университета от 12.10.2006», «Перечень сведений конфиденциального характера Сыктывкарского государственного университета», «Инструкция пользователя автоматизированного рабочего места информационной системы персональных данных (АРМ ИСПД)», «Инструкция администратора информационной системы персональных данных», «Регламент доступа в помещения, в которых ведется обработка ПД».

В конфиденциальной подсистеме присутствуют следующие ИС [56]:

1. Система расчета и начисления зарплаты сотрудникам «Зарплата» и «Расчет заработной платы».
2. Система ведения бухгалтерского учета «Комплексная бухгалтерия».
3. Система ведения штатного расписания «Штаты».
4. Система ведения кадрового учета «Кадры».
5. Система организации приемной компании «Абитуриент».
6. Система организации учебного процесса и учета выпускников «Контингент-Сессия».
7. Система расчета стипендии «Стипендия».
8. Система автоматизации учета и выдачи дипломов «КиберДИПЛОМ».
9. Система расчета квартплаты за общежитие «Квартплата».

10. Система материального учета на платформе 1С: Предприятие 7.7.

11. ИС учета клиентов института дополнительного профессионального образования.

12. Автоматизированная библиотечная информационная система «Руслан».

Таблица 1. Информационные ресурсы конфиденциальной подсистемы Сыктывкарского государственного университета

ИС учебного характера	**ИС с бухгалтерской информацией**
Система организации приемной компании "Абитуриент"	Система расчета и начисления зарплаты сотрудникам "Зарплата" и "Расчет заработной платы"
Система организации учебного процесса и учета выпускников "Контингент-Сессия"	Система ведения бухгалтерского учета "Комплексная бухгалтерия".
Система автоматизации учета и выдачи дипломов "КиберДИПЛОМ"	Система ведения штатного расписания "Штаты"
ИС учета клиентов института дополнительного профессионального образования	Система расчета стипендии "Стипендия"
Автоматизированная библиотечная информационная система "Руслан"	Система расчета квартплаты за общежитие "Квартплата"
	Система материального учета на платформе 1С: Предприятие 7.7

Таблица 4. Допуск сотрудников отделов к ИС

ИС учебного характера	Отделы имеющие допуск
«Абитуриент»	Центральная приемная комиссия, Финансово-аналитический отдел, Отдел реализации
«Контингент-Сессия»	Учебный отдел, Отдел нормативно-документационного обеспечения учебного процесса, Центр содействия занятости учащейся молодежи и трудоустройства выпускников, Финансово-аналитический, Расчетный, Операционный отдел и Отдел реализации, Отдел магистратуры и аспирантуры, Отдел воинского учета и бронирования, Отдел документационного обеспечения образовательных программ
«Кибер ДИПЛОМ»	Отдел документационного обеспечения образовательных программ
Клиенты ИДПО	Институт дополнительного профессионального образования
«Руслан»	Научная Библиотека
«Зарплата»	Операционный и Расчётный отделы
«Комплексная бухгалтерия».	Все отделы Управления бухгалтерского учёта и финансового контроля, Финансово-аналитический отдел
«Штаты»	Финансово-аналитический отдел
«Стипендия»	Расчётный отдел
«Квартплата»	
1С: Предприятие 7.7	Материальный отдел

Поскольку ставилась задача провести оценку СОИБ Сыктывкарского государственного университета с учетом особенностей защищаемой информационной системы, при этом придерживаясь системности требований по защите и их связей (как в

Кубе МакКамбера или трехмерной матрице Домарева), было решено разработать собственную модель оценки на основе уже известных моделей с применением известных методик оценки. В качестве каркаса собственной модели была выбрана трехмерная матрица, состоящая из измерений: активы, составляющие защиты, этапы построения защиты.

Идентификация активов – данный этап лежит в основе, поэтому является залогом успешных дальнейших действий. Главное в этом процессе – определиться с глубиной детализации и определить характер актива: ценность, чувствительность, имеющиеся меры защиты. Установление границы помогает четко определить – какие из перечисленных активов должны быть учтены при рассмотрении результатов анализа рисков.

В итоге: активы были идентифицированы с использованием методики "Facilitated Risk Analysis Process (FRAP)" разработанной Томасом Пелтиером (Thomas R. Peltier) [40]. В соответствии с ней, определение защищаемых активов производится с использованием опросных листов, изучения документации на информационную систему, использования инструментов автоматизированного анализа (сканирования) сетей.

После проведенного исследования в форме консультаций со специалистами системы и изучения соответствующей документации были выделены следующие направления защиты:

1. Защита ИС учебного характера при хранении: RAID, контроль целостности, разграничения доступа.
2. Защита ИС учебного характера при обработке: защита ОС, СУБД, СЗИ (SecretNet, S-Terra, антивирус), ActiveDirectory и программ обработки информации, электронный документооборот.
3. Защита ИС учебного характера при передаче: защита каналов внешнего обмена/передачи информации (локальная сеть, интернет, электронная почта, ЭЦП), за исключением физической охраны.
4. Защита БД с бухгалтерской информацией при хранении.
5. Защита БД с бухгалтерской информацией при обработке.
6. Защита БД с бухгалтерской информацией при передаче.
7. Защита информационных ресурсов в бумажном виде при хранении.
8. Защита информационных ресурсов в бумажном виде при обработке.
9. Защита информационных ресурсов в бумажном виде при передаче.
10. Физическая охрана ключевых узлов ИС (помещений и оборудования).
11. Управление СОИБ.

Всего было получено 11 направлений, группируя которые, можно получить картину состояния защиты персональных данных в учебном отделе, персональных данных и бухгалтерской информации в бухгалтерии, сетевой защиты в целом и в каждом из сегментов отдельно, состояние защищенности информации в электронном и бумажном виде.

Составляющие защиты по классической трехмерной матрице:

1. Нормативно-правовая и научная база.
2. Структура и задачи органов.
3. Организационные меры и методы (политика безопасности).
4. Программно-технические способы и средства защиты информации

совпадают во многом с одним из измерений Куба МакКамбера – защитные меры:

1. Персонал.
2. Политики и практики.
3. Технологии.

В итоге было принято решение применять составляющие защиты по трактовке Джона МакКамбера, где персонал - обеспечение того, чтобы как пользователи ИС, так и администраторы осознавали свою роль и обязанности в отношении защиты ИС; политики

и практики – процедуры административного управления, организационное обеспечение ИБ; технологии – программно и аппаратно базированные решения по защите.

Перейдем к рассмотрению *этапов.* Во всех прогрессивных стандартах и методиках ИБ организации представляет собой взаимосвязь двух направляющих: СОИБ и системы управления СОИБ. Создание СОИБ является никогда не заканчивающимся цикличным процессом, который имеет определенные этапы. Идея заимствована из циклической модели Деминга (PDCA) «…- планирование – реализация – проверка – совершенствование – планирование -…», которая является основой модели менеджмента стандартов качества ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 27001–2006 и созданный на его основе стандарт ЦБ РФ СТО БР ИББС-1.0-2008. По стандарту ISO/IEC 27000 – 2009 выделяются необходимые четыре группы процессов: планирование СОИБ организации; реализация СОИБ организации; мониторинг и анализ СОИБ; поддержка и улучшение СОИБ. Анализируя оригинальное построение трехмерной матрицы, можно заметить, что в качестве «этапов» матрицы выбрано несколько процессов, которые хорошо раскрывают этап «планирования» в модели Деминга, и всего один процесс, относящийся к реализации и один к контролю СОИБ, что не может не сказаться на адекватности оценки СОИБ. Совершенствование СОИБ – важный этап, который не стоит пропускать, в том числе для обеспечения уверенности в том, что хороший практический опыт организации документируется, становится обязательным к применению, а СОИБ становится лучше. Также для выбора этапов применялся ГОСТ Р ИСО/МЭК 13335-3 – 2007. Таким образом, были выделены следующие этапы:

1. Определение информации, подлежащей защите (идентификация и оценка активов).
2. Выявление угроз и каналов утечки информации, оценки уязвимости (с учетом существующих защитных мер).
3. Проведение оценки рисков.
4. Определение требований к защитным мерам и средствам.
5. Осуществление выбора СОИБ и защитных мер (определение защитных мер, структура безопасности ИТ, идентификация и анализ ограничений).
6. Проверка приемлемости и принятие рисков.
7. Внедрение и использование выбранных мер и средств.
8. Контроль и управление защитой.

Применение разработанной оценочной модели. Используя сформированные в предыдущем разделе метрики в трех измерениях, была составлена анкета, состоящая из 264-х вопросов. Для каждого вопроса экспертам было предложено не только ответить на него (столбец «Оценка выполненности требования»), но и выставить оценку важности самого вопроса (столбец «Важность требования»). При ответе требовалось выставлять оценки в соответствии с приведенной ниже лингвистической шкалой.

Таблица 2. Шкала качественной оценки

Числовое значение	**Качественная характеристика**
1	Полностью удовлетворяет, в полной мере, максимально важно
0,7	Почти удовлетворяет, почти достаточно, достаточно важно
0,5	Удовлетворяет в основном, удовлетворительно
0,3	Не удовлетворяет, не достаточно, не очень важно
0	Полностью не удовлетворяет, отсутствует, абсолютно не важно

Баллы выставлялись экспертами интуитивно и могли быть промежуточными на этой шкале. К примеру, *0.8* – если ответ ближе к «Почти удовлетворяет» или *0.9*, если ближе к «Полностью удовлетворяет», но недостаточно.

В качестве метода опроса был выбран метод «экспертной оценки», в котором принимало участие определенное количество экспертов, где каждый из экспертов

отдельно от остальных отвечал на вопросы анкеты на основе своего опыта в исследуемой области.

В качестве экспертов были привлечены сотрудники отделов Сыктывкарского государственного университета, которым было поручено проведение мероприятий по организации информационной безопасности выделенной ИС и которые принимали в этом активное участие. В экспертизе приняло участие восемь специалистов разной профессиональной подготовки, степени участия в проекте и авторитетом в области ИБ.

Кроме того, каждому из требований было присвоено свое весовое значение – важность требования, необходимое для того, чтобы позволить не включать в оценку те требования, которые не характерны для исследуемой СОИБ. Это значение присваивалось требованиям в процессе опроса методом «мозговой штурм», в котором принимали участие эксперты с наиболее высоким авторитетом в области ИБ. путем синтеза экспертной информации.

Для получения оценок с учетом важности требования использовались взвешенные средние

$$\bar{x} = \frac{\Sigma_{i=1}^{n} x_i n_i}{\Sigma_{i=1}^{n} n_i} .$$

Здесь n_i – вес i-го элемента, x_i – экспертная оценка данного элемента. Значения весов получены экспертным путем.

Поскольку необходимо было сформировать общую оценку СОИБ, данные экспертов необходимо было агрегировать в одну анкету, при этом учитывая авторитет каждого эксперта в области ИБ и достоверность его оценки. Для этого была проведена предварительная обработка экспертных оценок.

Обработка экспертных оценок. После окончания анкетирования результаты опроса по каждому из экспертов были проверены на корреляцию с результатами других участников с целью выявить тех участников опроса, чьи мнения резко отличаются от большинства, что может свидетельствовать о некомпетентности или необъективности эксперта и необходимости его исключения, а также выявить группы экспертов с высокой согласованностью (высокой корреляцией) мнений. Для подсчета корреляции была использована формула

$$r_{xy} = \frac{n\Sigma(x_i \times y_i) - \Sigma x_i \times \Sigma y_i}{\sqrt{\left(n\Sigma x_i^2 - (\Sigma x_i)^2\right) \times \left(n\Sigma y_i^2 - (\Sigma y_i)^2\right)}} ,$$

где x_i и y_i – сравниваемые количественные признаки, n – число сравниваемых наблюдений.

Таблица 3. Корреляционная матрица оценок экспертов

	Э №1	Э №2	Э №3	Э №4	Э №5	Э №6	Э №7	Э №8
Э №1	1							
Э №2	0.407	1						
Э №3	0.361	0.758	1					
Э №4	0.515	0.330	0.370	1				
Э №5	0.123	0.260	0.290	0.160	1			
Э №6	0.934	0.438	0.399	0.559	0.164	1		
Э №7	0.369	0.464	0.522	0.356	0.238	0.391	1	
Э №8	-0.175	-0.310	-0.018	-0.034	-0.120	-0.194	-0.218	1

После вычислений, были получены данные приведенные в таблице 3, по которым можно судить о степени согласованности мнений всех экспертов. Для того чтобы убедится, что линейная корреляционная связь между оценками двух экспертов действительно существует (т.е. при другом отборе невозможно исчезновение согласованности), проводилась оценка значимости всех коэффициентов корреляции. Результат анализа значимости коэффициентов корреляции представлен в таблице. Те значения r, которые признаны не значимыми, выделены красным цветом. Как можно заметить, практически

все результаты экспертов достоверны, за исключением Эксперта № 8 и нескольких результатов у Эксперта № 5.

Направления >>>				**010**	**020**	**030**	**040**	**050**	**060**	**070**	**080**	**090**	**0 10 0**	**0 11 0**	
<<< Этапы		**<<< Основы**		Защита ИС учебного характера			Защита ИС с бухгалтерской информацией			Защита информационных ресурсов в бумажном виде			Физ.охрана	Управление СОИБ	**<<<Оценки**
				хранение	Обработка	передача	хранение	обработка	передача	хранение	обработка	передача			
100	Идентификация активов	Кадры	**101**	**0.70**	**0.85**	**0.82**	**0.75**	**0.83**	**0.78**	**0.58**	**0.58**	**0.58**	**0.68**	**0.65**	**0.71**
		Политики и практики	**102**	**0.75**	**0.65**	**0.68**	**0.63**	**0.67**	**0.85**	**0.63**	**0.60**	**0.57**	**0.75**	**0.57**	**0.67**
		Технологии	**103**	**0.42**	**0.43**	**0.47**	**0.50**	**0.52**	**0.60**	**0.42**	**0.55**	**0.52**	**0.48**	**0.48**	**0.49**
200	Модель угроз	Кадры	**201**	**0.83**	**0.83**	**0.83**	**0.83**	**0.83**	**0.83**	**0.83**	**0.83**	**0.83**	**0.83**	**0.83**	**0.83**
		Политики и практики	**202**	**0.70**	**0.70**	**0.70**	**0.68**	**0.68**	**0.70**	**0.68**	**0.68**	**0.68**	**0.70**	**0.70**	**0.69**
		Технологии	**203**	**0.30**	**0.35**	**0.30**	**0.30**	**0.35**	**0.30**	**0.30**	**0.30**	**0.00**	**0.30**	**0.37**	**0.29**
300	Оценка рисков	Кадры	**301**	**0.75**	**0.75**	**0.75**	**0.75**	**0.75**	**0.75**	**0.75**	**0.75**	**0.75**	**0.75**	**0.75**	**0.75**
		Политики и практики	**302**	**0.50**	**0.45**	**0.35**	**0.50**	**0.50**	**0.55**	**0.55**	**0.55**	**0.55**	**0.45**	**0.55**	**0.50**
		Технологии	**303**	**0.28**	**0.28**	**0.28**	**0.28**	**0.28**	**0.33**	**0.33**	**0.33**	**0.33**	**0.33**	**0.33**	**0.31**
400	Определение требований	Кадры	**401**	**0.83**	**0.79**	**0.69**	**0.80**	**0.74**	**0.69**	**0.70**	**0.70**	**0.76**	**0.86**	**0.69**	**0.75**
		Политики и практики	**402**	**0.63**	**0.62**	**0.50**	**0.62**	**0.63**	**0.57**	**0.63**	**0.62**	**0.63**	**0.58**	**0.57**	**0.60**
		Технологии	**403**	**0.47**	**0.49**	**0.49**	**0.49**	**0.49**	**0.47**	**0.46**	**0.44**	**0.00**	**0.44**	**0.46**	**0.43**
500	Осуществление выбора	Кадры	**501**	**0.50**	**0.50**	**0.58**	**0.53**	**0.53**	**0.58**	**0.50**	**0.50**	**0.50**	**0.50**	**0.53**	**0.52**
		Политики и практики	**502**	**0.64**	**0.66**	**0.56**	**0.63**	**0.63**	**0.64**	**0.61**	**0.59**	**0.60**	**0.60**	**0.61**	**0.62**
		Технологии	**503**	**0.73**	**0.70**	**0.67**	**0.75**	**0.70**	**0.67**	**0.70**	**0.70**	**0.00**	**0.67**	**0.62**	**0.63**
600	Осуществление выбора	Кадры	**601**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**
		Политики и практики	**602**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**
		Технологии	**603**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**
700	Внедрение и использование	Кадры	**701**	**0.80**	**0.75**	**0.58**	**0.78**	**0.72**	**0.68**	**0.63**	**0.63**	**0.63**	**0.65**	**0.68**	**0.69**
		Политики и практики	**702**	**0.60**	**0.57**	**0.52**	**0.60**	**0.57**	**0.57**	**0.57**	**0.57**	**0.57**	**0.60**	**0.57**	**0.57**
		Технологии	**703**	**0.53**	**0.53**	**0.50**	**0.57**	**0.53**	**0.57**	**0.60**	**0.57**	**0.00**	**0.60**	**0.53**	**0.50**
800	Усовершенствование	Кадры	**801**	**0.67**	**0.65**	**0.70**	**0.67**	**0.67**	**0.72**	**0.58**	**0.58**	**0.65**	**0.58**	**0.62**	**0.64**
		Политики и практики	**802**	**0.62**	**0.62**	**0.62**	**0.62**	**0.62**	**0.62**	**0.72**	**0.72**	**0.72**	**0.67**	**0.67**	**0.65**
		Технологии	**803**	**0.42**	**0.42**	**0.42**	**0.42**	**0.42**	**0.42**	**0.42**	**0.42**	**0.00**	**0.42**	**0.42**	**0.38**
Оценки >>>				**0.53**	**0.52**	**0.50**	**0.53**	**0.53**	**0.54**	**0.51**	**0.51**	**0.41**	**0.52**	**0.51**	

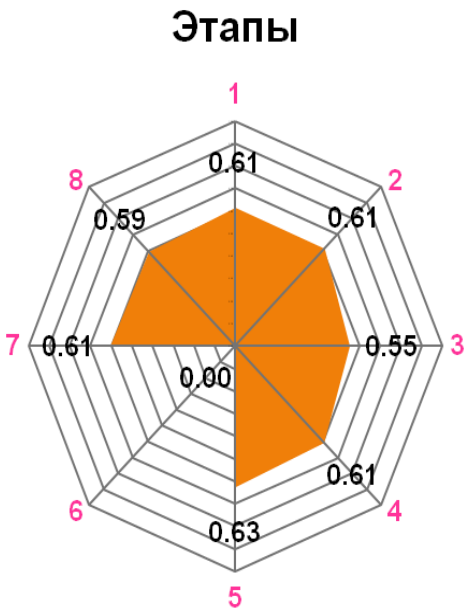
Далее, оценивая степень корреляции, была сформирована группа экспертов с высокой корреляцией мнений и группа с низкой корреляцией. К группе с низкой корреляцией относятся Эксперт № 8 и Эксперт № 5. В результате было принято решение исключить результаты группы экспертов с низкой корреляцией из эксперимента, а группа экспертов с высокой корреляцией была разбита на две подгруппы:

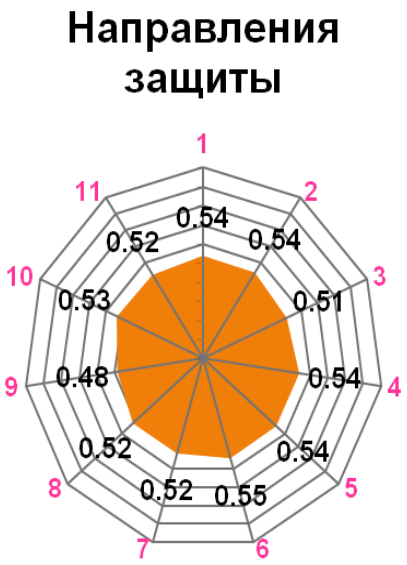
Группа 1: Эксперт № 1, Эксперт № 6 (зеленый маркер) и

Группа 2: Эксперт № 2, Эксперт № 3 и Эксперт № 7 (синий маркер),

внутри которых хорошо прослеживается корреляция между экспертами, а между экспертами из разных групп таковая практически отсутствует. В итоге была получена одна обобщенная оценка и две оценки от двух групп.

По результатам исследования была составлена трехмерная матрица, отражающая оценку экспертами СОИБ Сыктывкарского государственного университета.



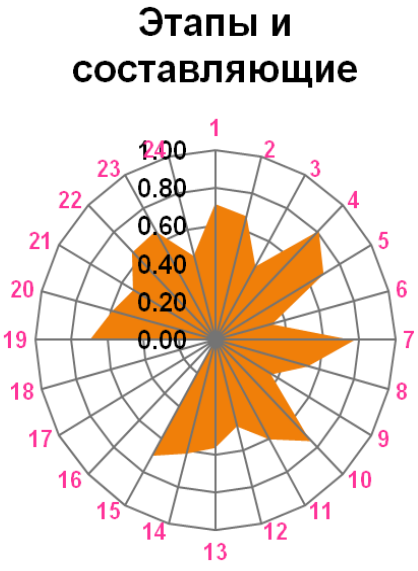


Заключение. Во-первых, следует сказать о том, что различные срезы матрицы в своем сочетании дают огромный массив данных. Сочетая, группируя и анализируя требования и блоки требований можно получить информацию по любым вопросам, касающимся СОИБ.

Рассматривая матрицу в срезе этапов построения СОИБ (см. рис.8), более всего выделяется шестой этап. Этот этап был упущен при создании СОИБ в Сыктывкарского государственного университета.

В итоге общая оценка СОИБ равна *0.52*, что соответствует вербальной характеристике «удовлетворительно, удовлетворяет в основном».

В качестве результатов оценки по разработанной модели можно дать следующие рекомендации: довести до конца этап внедрения организационных и технических мер защиты, ввести процедуру мониторинга и контроля изменений, ввести обязательные периоды проверки работоспособности и достаточности СОИБ, а по результатам разрабатывать план усовершенствования СОИБ. Прежде чем осуществлять какие-либо внедрения СЗИ, необходимо провести оценку остаточных рисков – чтобы без лишних затрат определить будет ли получен ожидаемый результат.



Требуется разработать процедуры безопасного

пользования мобильными устройствами. Большим недостатком является также отсутствие во всех процессах, процедурах и документах, касающихся учебного процесса, взгляда касающегося информационной безопасности. Конечно это титанический труд – переработать все существующие документы и практики с учетом ИБ, тем не менее, это является важной частью построения СОИБ.

Следует учитывать требования безопасности при создании и выборе программных продуктов для обработки информационных ресурсов, внимательнее подходить к написанию ТЗ на разработку ПО.

Библиографический список:

1. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения Введ. 01.10.2009. – М.: Стандартинформ, 2009

2. ГОСТ Р 51897-2002 Менеджмент риска. Термины и определения; Введ. 01.01.2003- М.:Госстандарт России, 2002 -26 с.

3. ГОСТ Р ИСО/МЭК 13335-1 – 2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий; Введ. 01.06.2007. – М.: Стандартинформ, 2006 -23с.

4. ГОСТ Р ИСО/МЭК 27001—2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. –Взамен ГОСТ Р ИСО/МЭК 17799—2005; Введ. 27.12.2006 - М, 2008 -26 с. (ISO/IEC 27001:2005 «Information technology — Security techniques — Information security management systems — Requirements»).

5. Федеральный закон Российской Федерации «О коммерческой тайне», № 98-ФЗ от 29.07.2004 г.

6. Федеральный закон Российской Федерации «О персональных данных», № 152-ФЗ от 27.07.2006.

7. Девянин, П.Н. Модели безопасности компьютерных систем: Уч.пос./ П.Н.Девянин. – М.:Издательский центр «Академия», 2005. – 144 с.

8. McCumber J. A Structured Methodology. Assessing and Managing Security Risk in IT Systems/J. McCumber//Publisher: Auerbach Publications; 1 edition (June 15, 2004) . – Режим доступа: https://buildsecurityin.us-cert.gov/swa/downloads/ McCumber.pdf. Дата последнего доступа 12.05.2010

9. Introduction Information Systems Audit and Control Association (ISACA) Jan 2009 “An Introduction to the Business Model for Information Security”//Режим доступа: http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=48017. Дата последнего доступа 12.05.2010

10. Домарев, В.В. Безопасность информационных технологий. Системный подход - Киев: ООО ТИД «Диасофт», 2004.-992 с. Режим доступа: http://www.security.ukrnet.net/d-book-2/ch_06.pdf. Дата последнего доступа 12.05.2010

11. Information Security Forum. Standard of Good Practice 2007 (ISF “SoGP”) - Information Security Forum Limited (01.05.2007) // Режим доступа: www.securityforum.org. Дата последнего доступа 12.05.2010

12. Aceituno V. Information security management maturity model (ISM3) v2.10//Stansfeld E. - ISM3 Consortium.

13. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена заместителем директора ФСТЭК России 15.02.2008.

14. Базовая модель угроз безопасности информации в ключевых информационных инфраструктурах, утверждена заместителем директора ФСТЭК России 18.05.2007.

15. Корт С.С. Теоретические основы защиты информации: Учебное пособие. – М.: Гелиос АРВ, 2004. – 240 с.

16. Moore A., Ellison R., Linger R. Attack Modeling for Information Security and Survivability // Software Engineering Institute, Technical Note CMU/SEI-2001-TN-01, March 2001.

17. ГОСТ Р ИСО/МЭК 15408 Общие критерии оценки безопасности информационных технологий, принят постановлением Госстандарта России от 4.04.2002 г. № 133-ст; Введ. 01.01.2004.

18. Нестеров, С.А. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft/С.А.Нестеров// Режим доступа: - http://www.intuit.ru/department/itmngt/riskanms. Дата последнего доступа 05.05.2010

V.V.Mironov, I.A.Nosal

MODELLING AND ESTIMATION OF SYSTEM OF MAINTENANCE OF INFORMATION SECURITY ON EXAMPLE SYKTYVKAR STATE UNIVERSITY

Annotation: In article questions of modeling of systems of maintenance of information security are considered, models of such systems are under construction. Results of modeling of systems of maintenance of information security on example Syktyvkar state university in the form of numerical estimations are resulted and recommendations about perfection of the named system are made.

Keywords: modeling, system, information security.

УДК 681.3

К ВОПРОСУ О ПОСТРОЕНИИ СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УЧЕБНОМ ЗАВЕДЕНИИ

А.А.Будина[34]*, В.В.Миронов*[35]

Аннотация: в статье рассматриваются вопросы построения системы менеджмента информационной безопасности в высшем учебном заведении. В качестве методики использовался стандарт ГОСТ Р ИСО/МЭК 27001—2006. Приводится типовая модель угроз безопасности и выработаны рекомендации по проектированию и построению системы защиты информации учреждения.

Ключевые слова: стандарты информационной безопасности, менеджмент информационной безопасности.

Информация - основополагающий ресурс в деятельности любой организации. Поэтому крайне важно защищать критичные для учреждений информационные ресурсы. Информация может быть представлена в различной форме, в том числе устной, письменной, может передаваться как в процессе разговора, так и по электронным каналам связи, либо посредством обычной почты. Она также может быть представлена на бумажном носителе, либо хранится на электронном. В зависимости от типа передаваемой информации, а также вида ее представления, информация, как актив организации, должна быть защищена. Защита активов организации является существенным фактором для поддержания делового имиджа, рентабельности, соответствия требований федерального законодательства.

В этом случае защита информации представляет собой комплекс средств, методов и мер, позволяющий минимизировать актуальные для организации угрозы, обеспечить непрерывность рабочего процесса и увеличить степень доверия к ее деятельности.

Защита информации важна для предприятий как государственного, так и частного сектора, а также для защиты ценных инфраструктур внутри самой организации. В обоих секторах деятельности защита информации будет работать как инструмент для достижения целей, например, как элемент управления, или как инструмент для снижения разнообразных угроз и рисков. В плане частного сектора защита информации (первостепенно – коммерческая тайна и персональные данные) и первую очередь будет направлена на реализацию политики получения прибыли и, в таком случае, непосредственной защите активов, непосредственно влияющих на достижение этой цели. В государственном секторе защита информации направлена на сохранение некоторой конфиденциальной информации (первостепенно – защита персональных данных и государственная тайна).

Комплексная защита информации достигается реализацией соответствующей системы менеджмента информационной безопасности, принятием комплекса организационных и технических мер, направленных на достижение целей организации, ведением непосредственного контроля за состоянием системы защиты информации на предприятии, выявлением недостатков и совершенствовании принятых мер. Эти элементы построения системы защиты необходимо создать, внедрить, постоянно контролировать, анализировать и улучшать, по необходимости, с целью обеспечить выполнение конкретных задач защиты и деятельности учреждения.

[34] ФГБОУ ВПО «Сыктывкарский государственный университет»
[35] ФГБОУ ВПО «Сыктывкарский государственный университет»

Однако, следует помнить, что процесс защиты должен быть интегрирован в общую систему управления организацией и быть прозрачным для бизнес-процессов, быть пропорциональным затратам на эту систему и ценности защищаемой информации.

С целью обеспечения комплексности при создании системы защиты можно определить следующий алгоритм выработки профиля защиты [1]:

1. Определить источники требований защиты;
   1.1. Требования федерального законодательства;
   1.2. Стратегия и цели организации;
   1.3. Требования самой организации к безопасности;
2. Определить риски в организации, которые состоят в следующем:
   2.1. Идентификация активов;
   2.2. Выявление актуальных угроз безопасности защищаемой информации;
   2.3. Определение уязвимостей системы;
   2.4. Выявление критичного воздействия на систему на основании выявленных угроз и рисков;
3. Определить отправные точки системы защиты информации;
4. Определить цели защиты информации необходимые для достижения требуемого уровня безопасности;
5. Определить менеджмент защиты информации в организации:
   5.1. Распределение обязанностей между сотрудниками организации;
   5.2. Определение направлений защиты информации в организации;
   5.3. Контроль за обеспечением безопасности в организации;
   5.4. Выявление недостатков в существующей системе защиты информации на предприятии;
   5.5. Совершенствование и улучшение действующей системы защиты для достижения целей организации;
6. Разработать внутренние принципы управления системой защиты информации и организационных документов, регламентирующих режим конфиденциальности;

На основании этого в любом учреждении должна быть построена единая политика безопасности, регламентирующая порядок обеспечения и соблюдения введенного режима.

В качестве объекта исследования будем рассматривать учебное заведение высшего профессионального образования - университет. В нем присутствует две категории субъектов: сотрудники и обучающиеся и фигурируют такие виды конфиденциальной информации как коммерческая тайна и персональные данные. Уже на основании этого необходимо отталкиваться от соответствующих требований федерального законодательства и остальных нормативных документов, закрепленных законодательно и регламентирующих порядок обработки с этими типа информации. Следующий список нормативно-правовых актов описывает названный порядок:

1. «Трудовой кодекс Российской Федерации» от 30.12.2001 N 197-ФЗ (принят ГД ФС РФ 21.12.2001);
2. «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 N 195-ФЗ (принят ГД ФС РФ 20.12.2001);
3. «Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ (принят ГД ФС РФ 24.05.1996);
4. Федеральный закон от 27.07.2006 №152 «О персональных данных»;
5. Федеральный закон от 27.07.2006 №149 «Об информации, информационных технологиях и защите информации»;
6. Федеральный закон от 08.08.2001 №128 «О лицензировании отдельных видов деятельности»;
7. Федеральный закон от 29.07.2004 №98 «О коммерческой тайне»;

8. Постановление Правительства РФ от 17.11.2007 N 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
9. Постановление Правительства РФ от 15.09.2008 N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
10. Другие нормативно-правовые акты.

Поскольку университет является государственным образовательным учреждением, то основными целями в области защиты информации в нем является выполнение требований федерального законодательства.

Итак, первый этап алгоритма построения комплексной системы защиты информации выполнен: были определены основные субъекты защиты и приведен перечень нормативно-правовых актов, регламентирующих работу с ней.

На втором этапе определяются информационные риски. Процесс расчета риска и управления им в организации можно представить в схеме [2]:

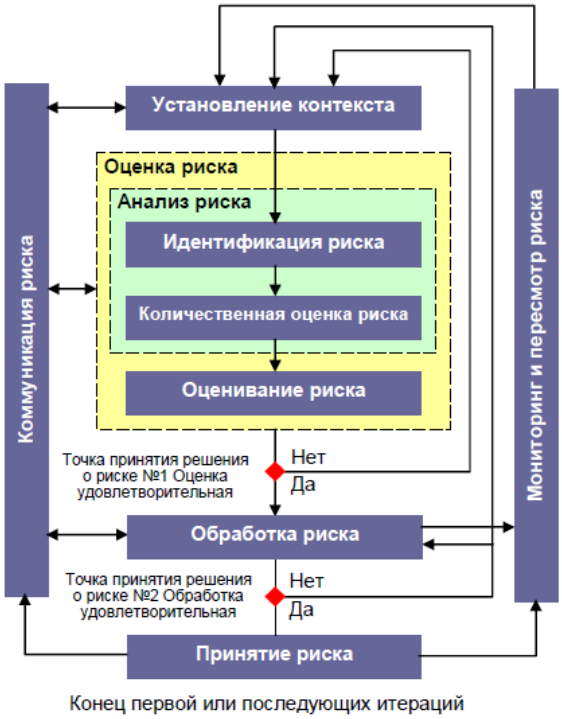


Рисунок 1. Процесс менеджмента риска информационной безопасности.

Этот этап начинается с оценки информационных активов объекта защиты. Основными активами обычно являются базовые процессы и информация о деятельности учреждения в области применения. В данном случае - университет. Например, с использованием методики FRAP. В результате анализа были выявлены следующие направления [5]:

1. Защита ИС учебного характера при хранении;
2. Защита ИС учебного характера при обработке: защита ОС, СУБД, СЗИ, AD и программ обработки информации, электронный документооборот;
3. Защита ИС учебного характера при передаче: защита каналов внешнего обмена/передачи информации (локальная сеть, интернет, электронная почта), за исключением физической охраны;
4. Защита БД с бухгалтерской информацией при хранении;
5. Защита БД с бухгалтерской информацией при обработке;
6. Защита БД с бухгалтерской информацией при передаче;
7. Защита информационных ресурсов в бумажном виде при хранении;

8. Защита информационных ресурсов в бумажном виде при обработке;
9. Защита информационных ресурсов в бумажном виде при передаче;
10. Физическая охрана ключевых узлов ИС (помещений и оборудования).

Для качественной оценки рисков использовалась следующая шкала соответствия (Таблица 1):

Таблица 1. Качественные показатели

Числовое значение	**Качественная характеристика**
1	Полностью удовлетворяет, в полной мере, максимально важно
0,7	Почти удовлетворяет, почти достаточно, достаточно важно
0,5	Удовлетворяет в основном, удовлетворительно
0,3	Не удовлетворяет, не достаточно, не очень важно
0	Полностью не удовлетворяет, отсутствует, абсолютно не важно

В результате получилась модель защиты, которую схематично можно представить в виде трехмерной оценочной матрицы с показателями защищенности по выделенным направлениям защиты в университете (Таблица 2).

На базе этой модели уже можно наглядно увидеть существующие угрозы по выделенным направлениям. Их можно оценить по качественным показателями итоговых оценок таблицы, приняв некоторую «среднюю» величину, ниже которой показатели не удовлетворяют требованиям защищенности. В результате можно получить некоторую типовую модель угроз и выявить критичные направления [2]:

Таблица 3. Типовая модель угроз

Вид	**Угрозы**	**Происхождение**		
		Случ.	Умыш.	Прир.
Физический ущерб	Пожар	+	+	-
	Ущерб, причиненный водой	+	+	-
	Загрязнение	+	-	-
	Крупная авария	+	-	-
	Разрушение оборудования или носителей	+	+	-
Природные Явления	Климатическое явление	-	-	+
	Метеорологическое явление	-	-	+
Утрата важных сервисов	Авария системы кондиционирования воздуха или водоснабжения	+	+	-
	Нарушение энергоснабжения	+	+	+
	Отказ телекоммуникационного оборудования	+	+	+
Помехи вслед. излуч.	Электромагнитное излучение	+	+	+
	Тепловое излучение	+	+	+
	Электромагнитные импульсы	+	+	+
	Перехват компрометирующих сигналов помех	-	+	-
	Дистанционный шпионаж	-	+	-
	Прослушивание	-	+	-
	Кража носителей или документов	-	+	-
	Кража оборудования	-	+	-
Компрометация информации	Поиск повторно используемых или забракованных носителей	-	+	-
	Раскрытие	+	+	-
	Данные из ненадежных источников	+	+	-
	Преступное использование аппаратных средств	-	+	-
	Преступное использование программного	+	+	-

	обеспечения			
	Определение местонахождения	-	+	-
Технические неисправности	Отказ оборудования	+	+	-
	Неисправная работа оборудования	+	+	-
	Насыщение информационной системы	+	+	-
	Нарушение функционирования программного обеспечения	+	+	-
	Нарушение сопровождения информационной системы	+	+	-
Несанкционирован. действия	Несанкционированное использование оборудования	-	+	-
	Мошенническое копирование программного обеспечения	-	+	-
	Использование контрафактного или скопированного программного обеспечения	+	+	-
	Искажение данных	+	+	-
	Незаконная обработка данных	-	+	-
Компрометация функций	Ошибка при использовании	+	-	-
	Злоупотребление правами	+	+	-
	Фальсификация прав	+	+	-
	Отказ в [произведении] действий	+	+	-
	Нарушение работоспособности персонала	+	+	+

Особое внимание следует уделять человеческим источникам угрозы и классифицировать их отдельно [3].

На следующем этапе проектирования системы защиты предполагается рассмотреть отправную точку построения. Здесь рассматривается наличие базовых средств, систем, мер и методов защиты, имеющихся в организации на данный момент и соотнести их с выявленными угрозами, уязвимостями и рисками. Далее смотрятся источники требований защиты, определенных для организации на первом этапе. Результатом этапа должна стать разница между имеющейся системой защиты и требуемой системой в соответствии с источниками требования.

Должны быть проработаны такие направления при проектировании и построении системы защиты как:

1. Единая политика в области защиты информации университета;
2. Внутренняя организация защиты информации в учреждении;
    a. Распределение обязанностей
    b. Соглашение о конфиденциальности
    c. Аудит системы защиты информации в учреждении
3. Учет защиты информационных активов при работе с третьими сторонами;
4. Безопасные зоны (физическая защита)
    a. Контролируемая зона и физический периметр
    b. Средства управления физическим доступом в контролируемую зону
    c. Защита офисов, комнат и средств обработки информации
5. Защита технического оборудования
    a. Расположение защиты оборудования
    b. Обслуживание оборудования
6. Менеджмент средств связи и операций
    a. Защита от злонамеренного кода
    b. Резервное копирование информации
    c. Средства управления сетью

d. Защита съемных носителей информации
e. Политика и процедуры обмена информацией
f. Электронный обмен сообщениями
g. Информационные системы

7. Управление доступом
   a. Единая политика управления доступом
   b. Регистрация пользователей
   c. Наделение правами пользователей
   d. Единая политика управления паролями
   e. Политика чистого стола и чистового экрана
   f. Аутентификация пользователя при внешних соединениях
   g. Идентификация оборудования в сетях
   h. Защита портов
   i. Разделение в сетях
   j. Управление сетевыми соединениями и маршрутизацией
   k. Идентификация и аутентификация пользователей
   l. Ограничение доступа к информации
   m. Изоляция критичных информационных систем
8. Требования к защите приобретенных и разработанных информационных систем
9. Менеджмент произошедших инцидентов в системе безопасности;
   a. Отчеты о произошедших событиях
   b. Отчеты о выявленных недостатках действующей системы защиты информации

Результатом станет полноценная картина состояния системы защиты. Можно построить диаграмму соответствия для наглядного примера оценки защищенности:

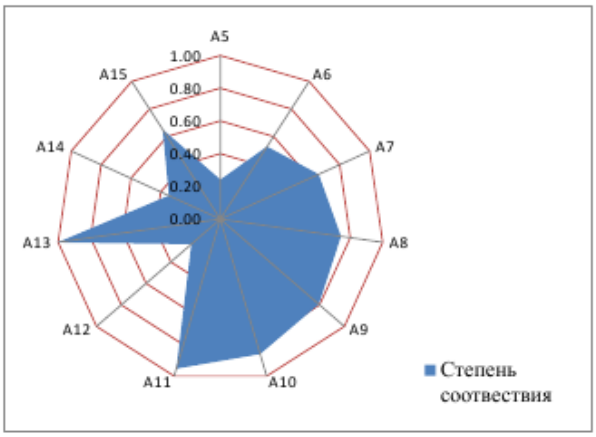


Рисунок 2. Оценка соответствия.

Теперь можно сформулировать основные направления, нуждающееся в доработке и улучшении:

1. Политика безопасности
2. Организация информационной безопасности
3. Управление активами
4. Правила безопасности, связанные с персоналом
5. Физическая защита и защита от воздействия окружающей среды
6. Управление средствами коммуникаций и их функционированием
7. Контроль доступа
8. Разработка, внедрение и обслуживание информационных систем
9. Управление инцидентами информационной безопасности
10. Управление непрерывностью рабочего процесса
11. Соответствие требованиям.

На заключительном этапе должна быть определена система менеджмента информационной безопасности университета. Должна быть проработана система оповещения об инцидентах, например, централизованная система сбора log-файлов, либо периодический мониторинг отчетов системы. Также следует проработать систему периодической проверки и тестирования действующих методов защиты для выявления их актуальности работоспособности, оценки их соответствия предъявляемым требованиям организации.

В конечном итоге должна быть спроектирована полноценная система организационной документации, рассматривающей разнообразные аспекты защиты выделенной критичной для организации информации. Она должна включать в себя положения, инструкции, регламенты, внутренние методики, применяемые в рабочем процессе.

В итоге, будет пройдена первая итерация цикла Демминга [1], и, как результат этой итерации, получен проект комплексной защиты критичной информации.

Библиографический список

1. ГОСТ Р ИСО/МЭК 27001—2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. –Взамен ГОСТ Р ИСО/МЭК 17799—2005; Введ. 27.12.2006 - М, 2008 -26 с. (ISO/IEC 27001:2005 «Information technology — Security techniques — Information security management systems — Requirements»).

2. ISO/IEC 27004:2009 Information technology — Security techniques — Information security management — Measurement 07.12.2009, 55 page.

3. ISO/IEC 27005:2008 Information technology — Security techniques — Information security risk management

4. ISO/IEC 27002— Security techniques — Information security risk management

5. Носаль И.А. Моделирование и оценка системы обеспечения информационной безопасности на примере ГОУ ВПО «Сыктывкарского государственного университета». Выпускная квалификационная работа. Сыктывкарского государственного университета. Сыктывкар, 2010. 81 с.

6.

A.A.Budina, V.V.Mironov

TO THE QUESTION ON CONSTRUCTION OF SYSTEM OF MANAGEMENT OF INFORMATION SECURITY IN EDUCATIONAL INSTITUTION

Annotation: in article questions of construction of system of management of information security in a higher educational institution are considered. As a technique the standard of ISO/IEC 27001:2005 was used. The typical model of threats of safety is resulted and recommendations about designing and construction of system of protection of the information of establishment are developed.

Keywords: information security standards, information security management.

Защита информации в информационных системах

УДК 316.4

ИНФОРМАЦИОННАЯ И ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ В УСЛОВИЯХ ИНФОРМАЦИОННОГО ОБЩЕСТВА

П.Ю. Филяк[36]

Аннотация: В статье рассматривается вопросы информационной и экономической безопасности в условиях информационного общества. Решению проблем информационной и экономической безопасности и комплексному решению данных проблем в настоящее время придается большое значение, поскольку достижение указанных целей не нуждается в доказательстве их актуальности.

Ключевые слова: информационная безопасность, экономическая безопасность, информационное общество.

Информационное общество - общество, в котором большинство работающих занято производством, хранением, переработкой и реализацией информации, характеризуется высокой степенью востребованности защиты информации и информационных продуктов, как совокупности данных, сформированной производителем для распространения в вещественной или невещественной форме.

Совершенно очевидно, что данные, информация, информационные продукты, информационные ресурсы, информационные технологии, информационные процессы, информационные системы и прочие составляющие информатизации являются предметом повышенного интереса для субъектов экономики в конкурентной среде, а информационная и экономическая безопасность, органично дополняя друг-друга, являются тесно и неразрывно связанными как в понятийном отношении, так и в предметной области и в правоприменительной сфере.

При рассмотрении проблем обеспечения информационной и экономической безопасности необходимо учитывать объективные условия, факторы и динамику современного общества, а также существующие реальные и потенциальные угрозы. В частности, - развитие правового государства, обеспечение прав граждан на получение информации, открытость в освещении событий, информационный взрыв, с одной стороны, с другой стороны, - право граждан на неприкосновенность частной жизни и собственности, угрозы мирового терроризма, обострение конкурентной среды в экономике и других сферах, отстаивание собственных экономических интересов субъектами экономики, стремление к технологическому лидерству и прочие реальные угрозы личности и обществу. Наличие указанных выше факторов создает две противоречащие друг-другу тенденции – тенденция к открытости и тесной интеграции в вопросах экономики и информационного обеспечения и тенденция возрастания роли и значимости экономической и информационной безопасности.

Эти две, казалось бы, совершенно противоположные тенденции на самом деле не являются антагонистическими, а составляют единое целое, требуя неотъемлемого друг от друга рассмотрения, совершенствования подходов и методов решения двуединой задачи.

Данную проблему наглядно иллюстрирует внедрение технологий «облачных вычислений», или «облачных технологий» и информационных технологий «аренды». Указанные технологии в условиях динамично развивающихся аппаратных средств, программного обеспечения и современных телекоммуникаций являются очень

[36] АОУ ВПО «Коми республиканская академия государственной службы и управления»

привлекательными с точки зрения получения максимального функционального эффекта при минимуме экономических затрат. «Общественные облака» и «аренда» очень выгодны в первую очередь небольшим организациям – из сферы малого и среднего бизнеса, но с точки зрения экономической и информационной безопасности не могут выдержать серьезной критики, поскольку обеспечение режима конфиденциальности информации и информационной безопасности отдается практически полностью «на откуп» поставщику данных услуг. Администратор (супервизор) поставщика услуг (провайдера) в этом случае по сути дела имеет неограниченный доступ к коммерческой, технологической, личной и иной информации потребителя услуг которой он оперирует. Фактически, единственным механизмом обеспечения защиты информации потребителя услуг от аутсайдеров является юридический механизм, - на уровне взаимных договоров или договоренностей сторон, предусматривающий выполнение условий обеспечения информационной безопасности для потребителя услуг (пользователя).

Несколько проще обстоит проблема в случае организации «частных облаков», но в этом случае особого внимания заслуживает проблема защиты информации в отношении инсайдеров, особенно для больших корпораций.

Таким образом, многие современные перспективные информационные технологии не могут быть использованы в предварительно предполагаемых масштабах по причине того, что в рамках данных проектов подходы к обеспечению защиты информации на текущий момент не отражают уровень предъявляемых требований по информационной безопасности. В этой связи значительная часть потенциальных клиентов может отказаться от предлагаемых новых эффективных решений в пользу традиционных более дорогостоящих, «заплатив» тем самым за обеспечение безопасности информации.

Требования и стандарты.

Новая парадигма управления предполагает системный и процессный подход к решению возникающих проблем, что в свою очередь предусматривает целеполагание, оценку ситуации, определение круга проблем, необходимых для решения поставленных задач, их структуризацию.

Отправной точкой для решения проблем информационной безопасности являются стандарты информационной безопасности. Стандарты это тот фундамент, на котором должна строиться концепция информационной безопасности любой организации и последующая реализация данной концепции, а также подходы к решению возникающих текущих проблем. В противном случае обеспечение информационной безопасности не будет комплексным и будет представлять собой постоянный процесс решения частных задач и «улучшений», не обеспечивая полноценную реализацию поставленной задачи.

Несколько сложнее обстоит дело с комплексным решением проблем экономической безопасности и, тем более, интегрированости с информационной безопасностью, поскольку на настоящий момент нет стандартов экономической безопасности. Тем не менее, существуют стандарты системы менеджмента качества, в которых основное внимание нацелено на обеспечение качества менеджмента, как системы, в которой рассматривается и информационная безопасность и оцениваются риски.

Решению проблем информационной и экономической безопасности и комплексному решению данных проблем в настоящее время придается большое значение, поскольку достижение указанных целей не нуждается в доказательстве их актуальности. Стандартизация в этом направлении идет по пути корреляции внутренних стандартов государства с международными стандартами, что в условиях укрепления международных экономических связей и международной интеграции является важным фактором построения эффективного взаимовыгодного взаимодействия и сотрудничества, создания новых технологий и повышения эффективности экономики, предотвращения существующих и потенциальных угроз в условиях современного индустриального и информационного общества.

P.Y. Filyak

INFORMATION AND ECONOMIC SECURITY IN THE INFORMATION SOCIETY

Abstract: This article discusses the issues of information and economic security in the information society. Problem-solving information and economic security and a comprehensive solution to these problems now is important, since the attainment of these goals does not require proof of their relevance.

Keywords: information security, economic security, the information society.

УДК 004.056

О НЕКОТОРЫХ АСПЕКТАХ ОБЕСПЕЧЕНИЯ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Д.А.Беляев[37]*, Д.Н.Едомский*[38]

Аннотация: В статье рассматриваются отдельные вопросы обеспечения организационно-технической защиты информации. Характеризуется модель нарушителей системы персональных данных.

Ключевые слова: персональные данные, модель нарушителя, информационная безопасность.

В последние годы проблемам защиты персональных данных уделяется достаточно много внимания. Предмет защиты персональных данных определяется как комплекс мер технического, организационного и административно-правового характера, направленных на защиту сведений, относящихся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных) [1].

Вместе с тем, научно-теоретическая база в части защиты персональных данных в Российской Федерации находится в самом начале своего развития [2]. Проблематика вопроса защиты персональных данных, по нашему мнению, включает в себя необходимость постановки и решения соответствующих задач по нескольким основным направлениям:

- организационно-техническая защита персональных данных;
- нормативно-правовое обеспечение персональных данных.

Можно описать несколько проблем организационно-технического обеспечения защиты персональных данных.

Во-первых, если говорить об организационно-технической защите персональных данных, то в настоящее время недостаточно развит аппарат составления и применения на практике такого важного инструмента как модель нарушителя, неполный вариант которой есть, например, в «Базовой модели угроз» [3].

Модель нарушителя определяет:

- категории (типы) нарушителей, которые могут воздействовать на объект (персональные данные);
- цели, которые могут преследовать нарушители каждой категории, их возможный количественный состав, используемые инструменты, принадлежности, оснащение, оружие и др.;
- типовые сценарии возможных действий нарушителей, описывающие последовательность (алгоритм) действий групп и отдельных нарушителей, способы их действий на каждом этапе.

Модель нарушителей системы персональных данных должна иметь разную степень детализации в зависимости от масштабов предприятия, организации, учреждения, а также отраслевой принадлежности, категории и класса персональных данных.

Содержательная модель нарушителей системы персональных данных должна отражать систему принятых взглядов (и документально закреплённых положений, инструкции и прочих материалов) на контингент потенциальных нарушителей. Кроме этого, модель нарушителей должна включать в себя возможные причины и мотивацию их

[37] Министерство образования Республики Коми
[38] ФГБОУ ВПО «Сыктывкарский государственный университет

действий, преследуемые цели и общий характер действий в процессе подготовки и совершения акций воздействия на персональные данные.

Сценарии воздействия нарушителей определяют классифицированные типы совершаемых нарушителями акций с конкретизацией алгоритмов и этапов, а также способов действия на каждом этапе.

В модели воздействия нарушителей может применяться математический инструментарий, который представляет собой формализованное описание сценариев в виде логико-алгоритмических последовательностей действий нарушителей, количественных значений, параметрически характеризующих результаты действий, и функциональных (аналитических, численных или алгоритмических) зависимостей, описывающих протекающие процессы взаимодействия нарушителей с элементами объекта и системы охраны. Именно этот вид модели может быть использован для количественных оценок уязвимости объекта и эффективности охраны.

Таким образом, модель нарушителя позволяет формально описать возможного «злоумышленника», зная которого можно построить эффективную систему защиты. Разработка модели нарушителей наиболее актуальна сегодня, когда широкое распространение получают различные вирусные и хакерские утилиты, которые легко найти в сети Интернет и воспользоваться ими.

Заметим, что типовую модель нарушителей системы защиты персональных данных можно представить в разрезе следующих потенциальных злоумышленников, аналогично [4]:

- разработчик;
- обслуживающий персонал (системный администратор, сотрудники обеспечения информационной безопасности);
- пользователи;
- сторонние лица.

Во-вторых, в системах защиты персональных данных на большинстве предприятий в настоящее время наблюдается ситуация несоответствия фактических параметров используемых информационно-коммуникационных устройств тем параметрам, которые указаны в имеющихся на предприятии документах. Например, такие идентификаторы как IP-адреса, пароль пользователя и инвентарные номера компьютеров, на которых осуществляется обработка персональных данных, должны взаимно-однозначно соответствовать друг другу.

В-третьих, количество специальных технических средств, применяемых для защиты персональных данных, можно снизить путём осуществления организационных методов. К примеру, при монтаже локальной вычислительной сети все телекоммуникационные устройства можно расположить в специальных коробах. В этом случае можно ежедневно осуществлять контроль целостности коробов, а также выявление несанкционированных подключений к сети. Для выполнения этих действий достаточно вменить в должностную инструкцию одного из сотрудников предприятия данную функцию контроля физической целостности локальной вычислительной сети. Если организовать такой контроль, то не будет необходимости применения активных и пассивных линий защиты сети и линий электропитания. Как следствие, общим эффектом будет снижение совокупной стоимости владения системой защиты персональных данных.

В-четвертых, многие предприятия осуществляют хозяйственную деятельность в арендуемых помещениях и не могут организовать пропускной режим в соответствии с действующими правилами защиты персональных данных. Выход из ситуации видится в том, что необходимо четко прописывать режим работы сотрудников, осуществляющих обработку персональных данных, в должностных инструкциях. Например, вменить в ответственность сотруднику контроль за тем, чтобы монитор был расположен таким образом, чтобы не было видовой утечки информации. Также при нахождении посторонних лиц в помещениях, где обрабатываются персональные данные, сотрудник

вместо сворачивания файла в панель задач операционной системы может просто отключить монитор.

В-пятых, сегодня предприятия самостоятельно решают, в каких программах осуществлять обработку персональных данных. При этом может сложиться ситуация, когда предприятие своевременно не проконтролировало наличие актов (сертификатов) соответствия на используемое программное обеспечение в части отсутствия недокументированных и недекларированных возможностей (НДВ), в том случае, когда это необходимо. Если осуществлять полноценную сертификацию программных средств (или их проверку на отсутствие НДВ и возможностей несанкционированного доступа), то это очень дорого. Как следствие, предприятие может вынужденно нарушить закон. Решением проблемы могло бы стать наличие специализированных центров мониторинга соответствия реализуемых в России программных продуктов (где так или иначе предусмотрена обработка персональных данных) законодательству.

Библиографический список

1. Постановление Правительства Российской Федерации от 17 ноября 2007 г. N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных".

2. Назаров И.Г., Язов К.Ю., Остроухова Е.С. Особенности организации обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных // Информация и безопасность. 2009. № 1. с 71-76.

3. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.).

4. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации (утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.).

D.A. Belyaev, D.N. Edomsky

ABOUT SOME ASPECTS OF MAINTENANCE OF ORGANIZATIONAL-TECHNICAL PROTECTION OF THE PERSONAL DATA

Annotation: In article individual questions of maintenance of organizational-technical protection of the information are considered. The model of infringers of system of the personal data is characterized.

Key words: Personal data, model of the infringer, information security.

К сведению авторов журнала «Вестник ИТАРК»

Журнал публикует научно-аналитические обзоры (объем до 25 м.с.), оригинальные статьи (до15 м.с.) и краткие сообщения (до 6 м.с.) теоретического и экспериментального характера по проблемам в области информационных технологий и информационной безопасности. К публикации также принимаются комментарии к ранее опубликованным работам, информация о научных конференциях, рецензии на книги, хроника событий научной жизни. Статьи должны отражать результаты законченных и методически правильно выполненных работ.

Решение о публикации принимается редакционной коллегией журнала после рецензирования, учитывая новизну, научную значимость и актуальность представленных материалов. Статьи, отклоненные редакционной коллегией, повторно не рассматриваются.

Общие требования к оформлению рукописей

Статьи должны сопровождаться направлением научного учреждения, где была выполнена работа. В необходимых случаях должно быть приложено экспертное заключение. Организация, направляющая статью, как и автор(ы), несет ответственность за её научное содержание, достоверность и оригинальность приводимых данных. Изложение материала статьи должно быть ясным, лаконичным и последовательным. Статья должна быть хорошо отредактирована, тщательно проверена и подписана всеми авторами (автором) с указанием (полностью) фамилии, имени, отчества, домашнего адреса, места работы, служебного и сотового телефонов и e-mail.

В редакцию подается рукопись статьи в двух экземплярах – на бумаге и на диске в редакторе Word под Windows. Электронная и бумажная версии статьи должны быть идентичны. Текст должен быть набран на компьютере (шрифт Times New Roman, кегль 14) в одну колонку через 1,5 интервала на бумаге форматом А4. По всей статье шрифт должен быть одинаковым. Поля страниц оригинала должны быть не менее: левое – 25 мм, верхнее – 20 мм, правое – 10 мм, нижнее – 25 мм. Объем иллюстраций (таблицы, рисунки, фото) в статье не должен превышать 8-10, а список литературы -15 наименований. Количество иллюстраций в кратких сообщениях не должно превышать, соответственно, 5.

Первая страница рукописи оформляется следующим образом: в начале статьи указывается индекс Универсальной десятичной классификации (УДК); затем прописными буквами печатается название статьи, которое должно быть максимально кратким (информированным) и не содержать сокращений; далее следуют инициалы и фамилии авторов. Отдельной строкой дается название учреждения и города (для иностранных авторов – также страны). Ниже печатается электронный адрес для переписки. При наличии авторов из нескольких организаций необходимо арабскими цифрами указать их принадлежность. Через один полуторный интервал следует краткая аннотация (8-10 строк), в которой сжато и ясно описываются основные результаты работы. После аннотации через полуторный интервал приводятся ключевые слова (не более 6-8). Далее идут название статьи, аннотация и ключевые слова на английском языке.

Текст статьи состоит, как правило, из введения, основного текста, заключения (резюме) и списка литературы. В статье, описывающей результаты экспериментальных исследований рекомендуется выделить разделы: «Материал и методы», «Результаты и обсуждение». Отдельно прилагаются подрисуночные подписи.

Во введении (заголовком не выделяется) в максимально лаконичной форме должны быть изложены цель, существо и новизна рассматриваемой задачи с обязательным кратким анализом данных наиболее важных и близких по смыслу работ других авторов. Однако введение не должно быть обзором литературы. В разделе «Материал и методы» должны быть четко и кратко описаны методы и объекты исследования. Единицы измерения следует приводить в международной системе СИ. Подробно описываются только оригинальные методы исследования, в других случаях указывают только суть

метода и дают обязательно ссылку на источник заимствования, а в случае модификации – указывают, в чем конкретно она заключается.

При первом упоминании терминов, неоднократно используемых в статье (однако не в заголовке статьи и не в аннотации), необходимо давать их полное наименование, и сокращение в скобках, в последующем применяя только сокращение. Сокращение проводить по ключевым буквам слов в русском написании. Все используемые, включая общепринятые, аббревиатуры должны быть расшифрованы при первом упоминании. Все названия видов флоры и фауны при первом упоминании в тексте обязательно даются на латыни с указанием авторов.

В разделе «Результаты и обсуждение» полученные данные приводят либо в табличной форме, либо на рисунках, без дублирования одной формы другой, и краткого описания результатов с обсуждением в сопоставлении с данными литературы.

В тексте цитированную литературу приводить только цифрами в квадратных скобках. Список литературы должен быть представлен на отдельной странице и составлен в порядке упоминания источников в тексте в соответствии со следующими правилами описания. Журнальные публикации: фамилии и инициалы всех авторов, полное название статьи журнала, название журнала (в соответствии с рекомендованным ВИНИТИ списком сокращений), год, том, выпуск (номер), страницы (первая и последняя). Книги: фамилии и инициалы всех авторов, полное название книги, инициалы и фамилии редакторов, город, год, страницы (если ссылка не на всю книгу) или число страниц в книге. Сборники: фамилия и инициалы авторов, полные названия статьи и сборника, первая и последние страницы. Если сборник содержит материалы конференций, необходимо указать их форму (труды, доклады, материалы) и название конференции. Диссертации: фамилия и инициалы автора, полное название диссертации, на соискание какой степени, каких наук, город, институт, в котором выполнена работа, год. Ссылки на авторефераты допускаются в исключительных случаях с указанием фамилии и инициалов автора, полного названия работы, места и года защиты, общего количества страниц. Ссылки на неопубликованные работы не допускаются.

Библиографический список оформляется по нижеприведенным примерам (следует обратить особое внимание на знаки препинания):

1. *Иванов И.И.* Название статьи // Название журнала. 2005. Т.41. № 4. С. 18-26.
2. *Петров П.П.* Название книги. М.: Наука, 2007. Общее число страниц в книге (например, 180 с.) или конкретная страница (например, С. 75.).
3. *Казаков К.К.* Название диссертации: Дис. «…». канд. биол. наук. М.: Название института, 2002. 164 с.
4. *Мартынюк З. П.* Патент RU № 92963 на полезную модель " Фотограмметрическое средство измерений объемов круглых лесоматериалов при проведении погрузо-разгрузочных работ". Патентообладатель(и): Учреждение Российской академии наук Институт биологии Коми научного центра Уральского отделения РАН.

При наличии четырех авторов в списке литературы указываются все, а более четырех – только первые три, а далее пишется «и др.».

Для статей журналов, имеющих русскую и английскую версию, необходимо давать в списке литературы двойную ссылку (под одним номером), например:

1. *Иванов И.И., Петров П.П.* Название статьи // Название журнала. 2008. Т. 47. № 1. (8-18). *Ivanov I., Petrov P.* Article name // Magazine name. 2008. T. 47. № 1. (4-15).

При несоблюдении этих перечисленных правил статья не рассматривается редакционной коллегией, а возвращается авторам на доработку.

Все статьи проходят рецензирование и в случае необходимости возвращаются авторам на доработку. Рецензирование статьи закрытое. Возможно повторное и параллельное рецензирование. Редакционная коллегия оставляет за собой право

редактирования статьи. Статьи публикуются в порядке очередности, но при этом учитывается их тематика и актуальность. Редакционная коллегия сохраняет первоначальную дату поступления статьи, а, следовательно, и очередность публикации, при условии возвращения ее в редакционную коллегию не позднее, чем через 1 месяц. Корректуру принятой в печать статьи редакционная коллегия иногородним авторам рассылает по e-mail. Автор в течение 7-10 дней должен вернуть ее в редакционную коллегию или передать правку по указанному телефону или электронному адресу (e-mail) редакционной коллегии. В случае отклонения материала рукописи, приложения и дискета не возвращаются.

Требования к электронной версии статьи

При подготовке материалов для журнала с использованием компьютера рекомендуются следующие программы и форматы файлов.

Текстовые редакторы: Microsoft Word for Windows. Текст статьи набирается с соблюдение следующих правил:

- набирать текст без принудительных переносов;
- разрядки слов не допускаются;
- уравнения, схемы, таблицы, рисунки и ссылки на литературу нумеруются **в порядке их упоминания в тексте;** нумеровать следует лишь те формулы и уравнения, на которые даются ссылки в тексте;
- в числовых значениях **десятичные разряды отделяются запятой**;
- вставка символов **Symbol.**

Графические материалы: *Растровые рисунки* должны сохраняться только в формате TIFF с разрешением 300 dpi (точек на дюйм) для фотографий и не менее 600 dpi (точек на дюйм) для остальных рисунков (черно-белый). Использование других форматов нежелательно.

Векторные рисунки (не диаграммы) должны предоставляться в формате программы, в которой они созданы: CorelDraw. Adobe Illustrator. Если использованная программа не является распространенной, необходимо сохранить файлы рисунков в формате Enhanced Windows Metafile (EMF) или Windows Metafile (WMF).

Диаграммы: Рекомендуется использовать Microsoft Excel, Origin для Windows (до версии 6.0).

Рукописи статей **только простым письмом** направлять по адресу:
Ответственному секретарю редакционной коллегии журнала «Вестник ИТАРК»
Лавреш Ивану Ивановичу
167000, г. Сыктывкар, ул. Интернациональная, д. 108

Тел. (факс) (8212) 22-31-11
E-mail: journal@itark.ru

Contents

Журнал издается под руководством ИТ-ассоциации Республики Коми

Редакционная коллегия:

Редакция:

Республика Коми, г.Сыктывкар, ул. Интернациональная, 108-А.
Контактный телефон 8-9121429531, факс – (88212) 22-31-11,
Электронная почта – journal@itark.ru
Сайт – http://www.vestnik.itark.ru

Сдано в набор 21.07.2011 Подписано к печати 30.07.2011 Формат бумаги 70×100 1/16
Офсетная печать Усл. печ. л. 15 Усл.-кр.отт. 12,5 тыс.
Уч.изд.л. 17 Бум.л.10
Тираж 200 экз. Заказ 8745

ISSN 2224-0837