

Федеральное агентство по образованию

Государственное образовательное учреждение
высшего профессионального образования
«Санкт-Петербургский государственный
инженерно-экономический университет»



**СОВРЕМЕННЫЕ
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ОБРАБОТКИ
И ЗАЩИТЫ ИНФОРМАЦИИ**

Сборник научных трудов



Санкт-Петербург
2009

УДК 378.001.658.011.56

ББК 32.97

С56

Утверждено редакционно-издательским советом СПбГИЭУ

Рецензенты:

кафедра комплексного обеспечения информационной безопасности
СПбГУВК (зав. кафедрой д-р техн. наук, проф. А. П. Ныроков),
д-р техн. наук, проф. Э. А. Пиль (ПГУПС)

Редакционная коллегия:

д-р техн. наук, проф. В. Л. Горохов (отв. ред., СПбГИЭУ); канд. экон.
наук, доц. Е. Б. Попов (зам. отв. ред., СПбГИЭУ), канд. техн. наук, доц.
Ф. Ф. Павлов (чл. редкол., СПбГИЭУ)

Одобрено к изданию научно-техническим советом СПбГИЭУ

С56 **Современные информационные технологии обработки
и защиты информации : сб. науч. тр. / редкол.: В. Л. Горохов
(отв. ред.) [и др.]. – СПб. : СПбГИЭУ, 2009. – 161 с.**

ISBN 978-5-88996-972-3

В сборнике, подготовленном на кафедре вычислительных систем и программирования СПбГИЭУ, рассматриваются проблемы применения информационных технологий в различных сферах, а также проблемы защиты информации.

Сборник предназначен преподавателям, аспирантам, магистрам, студентам, а также всем, кто интересуется проблемами применения современных технологий обработки и защиты информации.

УДК 378.001.658.011.56
ББК 32.97

ПРЕДИСЛОВИЕ

Переход к информационному обществу вызвал бурное развитие технологий обработки и передачи информации во всех сферах жизнедеятельности. При этом возникают проблемы обеспечения надежности и безопасности информационных систем, особенно при использовании компьютерных сетей передачи данных.

В представленном сборнике рассматриваются теоретические и практические вопросы применения новых информационных технологий в различных отраслях народного хозяйства, а также вопросы защиты целостности и конфиденциальности данных в информационных системах.

Сборник состоит из двух разделов.

В первом разделе анализируются современные технологии обработки информации; рассматриваются вопросы бизнес-планирования, определения структуры расходов, моделирования банковской деятельности, использования нейронных сетей; оцениваются СММ моделирования, конструирование компьютерных метафор для систем когнитивной машинной графики.

Во втором разделе рассматриваются основные технологии защиты данных, учета рисков; изучаются концепция иерархии угроз, основные алгоритмы защиты, обеспечение безопасности информации при работе в компьютерных сетях.

Редакционная коллегия

Раздел I

ТЕХНОЛОГИИ ОБРАБОТКИ ИНФОРМАЦИИ

УДК 378.001.658.011.56

Х. И. Аминов

Санкт-Петербургский государственный
инженерно-экономический университет

МОДЕЛИРОВАНИЕ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ

Моделирование занимает важное место в управлении современным банком. Вопросами моделирования банковской деятельности начали заниматься с 1888 г., когда впервые была опубликована классическая работа Ф. Эджуорта. С тех пор вышло много работ, связанных с моделированием банковской деятельности. Надо отметить, что, несмотря на большое количество работ, проблема моделирования банковской деятельности остается актуальной [1; 2; 3].

По принятой на Западе теории банковской фирмы [3] выделяют полные и частичные модели.

Полные модели должны объяснить решения об активах и обязательствах банка (и их взаимодействие, если оно есть) и размеры фирмы. Полная модель банковской фирмы также должна предусматривать одновременное определение структуры активов, структуры пассивов и размеры фирмы.

Частичные модели, или, как их еще называют, портфельно-теоретические модели, концентрируются либо на отборе активов, либо на управлении обязательствами. Они являются частичными, потому что анализируют только часть поведения банковской фирмы.

Среди российских публикаций выделяются другие классификации моделей банковской деятельности; в частности, в работе [2] рассматривается следующая классификация:

- модели банка как финансового посредника;
- производственно-организационные модели банковской деятельности;
- модель банка как совокупность стохастических финансовых потоков.

Модель банка как финансового посредника описывает деятельность банков с точки зрения выполнения ими функций финансового посредника.

Производственно-организационная модель банковской деятельности приближает математические модели банков к традиционным моделям производственных предприятий и организаций, т. е. эта модель представляет банк как некоторый абстрактный объект, характеризующийся входными и выходными параметрами, а также функцией, которая их связывает. Преимуществом этой модели является сопоставление теории финансово-банковских институтов с классической теорией фирмы.

Модель банка как совокупность стохастических финансовых потоков более подробно описывает процессы, протекающие внутри финансовых институтов.

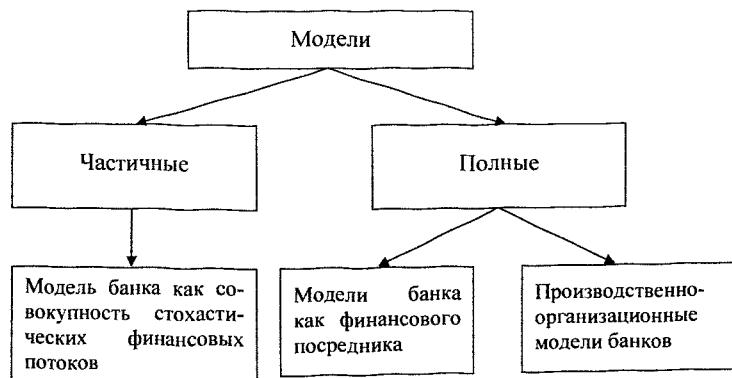
Надо отметить, что модели банка как финансового посредника и производственно-организационные модели банковской деятельности можно отнести к полным моделям, а модель банка как совокупность стохастических финансовых потоков отнести к частичным.

Классификация моделей кредитного портфеля представлена на рисунке.

Также можно выделить конкретные модели, предлагаемые российскими авторами; в частности, среди частичных моделей можно выделить следующие [1; 2; 3]:

- оптимальная модель стратегии развития коммерческих банков (В. А. Васильева);
- стохастическая модель динамики объемов банковских депозитов «до востребования» (И. В. Вишняков);
- модель оптимизации кредитной политики банка и предприятия (Ю. Н. Иванов, В. Симунек, Р. А. Сотникова);

– модель управления ликвидностью банка (А. И. Екушов, Д. В. Романюк).



Среди полных моделей наиболее интересны следующие:

- модель управления ликвидностью банка при случайно колеблющихся ставках процентов (М. Ю. Андреев, М. Г. Поспелов);
- модель деятельности банка при отсутствии инфляции и экономического роста (С. М. Гуриев, И. Г. Поспелов);
- модели дефолта российских банков (Пресетский).

Эта классификация не может представить всю полноту моделей банковской деятельности. Банк является сложным объектом, поэтому невозможно выделить один подход или одну модель, которая могла бы описать всю банковскую деятельность.

Литература

1. Аңыз С. М., Орзебеков Н. А. Об одном подходе к построению математических моделей для оптимизации банковской деятельности. Новосибирск, 2004. (Препринт/РАН. № 147. Сиб. отд. Институт математики).
2. Конюховский П. В. Микроэкономическое моделирование банковской деятельности. СПб.: Питер, 2001.
3. Синки Дж. Ф., м.л. Управление финансами в коммерческих банках: Пер. с англ. 4-го перераб. изд. / Под ред. Р. Я. Левиты, Б. С. Пинскера. М.: Catallaxy, 1994.

УДК 378.001.658.011.56

И. А. Брусакова, В. Н. Бугорский

Санкт-Петербургский государственный
инженерно-экономический университет

ОСНОВНЫЕ ЭТАПЫ РАЗРАБОТКИ БИЗНЕС-ПЛАНА СОЗДАНИЯ ПРОВАЙДЕРСКОЙ ФИРМЫ

При создании провайдерской фирмы необходимо иметь в виду, что, для того чтобы удовлетворять потребности конечного пользователя в услугах Интернет, фирме необходимо сначала купить доступ в Интернет.

Крупные компании в России продают такой доступ. Например, ОАО «Ростелеком» – крупнейшая компания связи в России, имеет сети связи, охватывающие множество городов и несколько международных каналов подключения к зарубежным сетям. Такие компании (их называют uplink-провайдерами или операторами связи) не занимаются предоставлением услуг конечным пользователям.

В свою очередь uplink-провайдеры могут входить в телекоммуникационные холдинги, например в ОАО «Связьинвест» – один из крупнейших телекоммуникационных холдингов в мире, установленный капитал которого образован акциями акционерных обществ электросвязи, созданных в процессе приватизации государственных предприятий электросвязи.

Телекоммуникационные холдинги, компании и крупные провайдеры владеют физическими линиями связи (телефонные сети, оптоволоконные кабели, связь через спутники и т. д.).

Местные провайдеры могут создавать крупные сети в пределах одного города, но прокладывать линии связи на большие расстояния самостоятельно им невыгодно, дешевле и проще купить доступ к таким линиям.

Для предоставления услуг доступа конечным пользователям необходимо оборудование – модемные стойки, серверы доступа. Приходится покупать телефонные линии и номера у телефонных компаний и т. д.

Зарубежные государства с самого начала отнесли Интернет-сервисы к услугам добавленной стоимости, позволив провайдерам

развиваться по своему усмотрению, а в России Интернет был отнесен к услугам связи со всеми вытекающими последствиями: обязательным получением лицензий, согласованием проектов и сертификацией используемого оборудования.

Поскольку развитие законодательной базы не успевает за экономическими и правовыми отношениями в сфере высоких технологий, условия предоставления услуг провайдера не регламентированы законом. Каждый провайдер при предоставлении услуг подключения, например, по выделенной линии, представляет свой вариант типового договора, в который уже вносятся поправки в соответствии с конкретными пожеланиями клиентов.

При подключении местного провайдера к региональному подписывается провайдерское соглашение, описывающее права и обязанности провайдеров по отношению друг к другу.

Провайдеры в большей мере зависимы от внешних факторов, таких как введение повременной оплаты за телефон, отключение энергоснабжения, аварии каналов, вмешательство государственных и правоохранительных органов в свою деятельность, изменения в законодательстве.

Бизнес-план является рабочим инструментом, используемым во всех сферах предпринимательства; он описывает процесс функционирования фирмы, показывает, как достичь своих целей, в частности повышения прибыльности ее работы.

Бизнес-план является постоянным документом, систематически обновляется (в него вносятся изменения, связанные с переменами, происходящими как внутри фирмы, так и на рынке, где существует фирма), определяет стратегию развития фирмы, базируется на общей концепции развития фирмы, дает технико-экономическое обоснование конкретным мероприятиям.

Бизнес-план позволяет решать целый ряд экономико-организационных задач, основными из которых являются:

- обоснование экономической целесообразности выбора направлений развития фирмы;
- расчет ожидаемых финансовых результатов деятельности, в первую очередь объемов продаж, прибыли, доходов на капитал;
- определение намечаемого источника финансирования для реализации выбранной стратегии;
- подбор работников, которые способны реализовать данный план.

Бизнес-план состоит из ряда разделов, в которых даются характеристика продукции, оценка рынков сбыта, анализ конкуренции на рынке, оценка рисков, а также рассматривается план производства, организационный план, финансовый план и т. д.

Содержание резюме бизнес-плана провайдерской фирмы. Бизнес-план начинается с резюме, которым практически завершается работа по его написанию. Таким образом, резюме создается после того, как проработаны все вопросы, связанные с созданием провайдерской фирмы. Объем резюме должен быть небольшим (до 4 машинописных страниц). В резюме должны быть отражены финансовые результаты проекта.

Будущие кредиторы и инвесторы должны получить из резюме полную информацию по интересующим их вопросам. Для этого в резюме можно выделить следующие подпункты:

- основная идея проекта;
- цели бизнес-плана;
- способы и средства достижения целей;
- сроки и этапы реализации проекта.

Содержание названных подпунктов должны быть представлены в резюме бизнес-плана провайдерской фирмы для конечного пользователя.

Идея бизнеса состоит в создании фирмы Интернет-провайдера, т. е. фирмы, занимающейся оказанием услуг доступа в мировую сеть Интернет. Например, предполагается, что данная фирма будет обслуживать конечных пользователей Санкт-Петербурга и в дальнейшем – Ленинградской области, исходя из того, что в среднем за неделю к Интернет-страницам обращаются около полутора миллиона человек в этом регионе.

Создаваемая фирма на первом этапе должна предоставлять услуги неограниченного доступа в Интернет по домашней сети для физических и юридических лиц. В дальнейшем сектор услуг может быть расширен.

Целями бизнес-плана являются:

- создание экономически устойчивой провайдерской компании, услуги которой будут пользоваться достаточно большим спросом за счет их высокого качества и низкой стоимости;
- создание возможностей для развития номенклатуры предлагаемых услуг, таких как:

веб-дизайн – выделение специализированного отдела в компании, занимающегося разработкой, поддержкой и сопровождением сайтов и баннеров для юридических и физических лиц; веб-хостинг – размещение сайтов и поддержка виртуальных серверов на сервере фирмы; создание в рамках фирмы виртуального магазина электронной коммерции; разработка специальных программ подключения для юридических лиц, нуждающихся в высокой скорости передачи данных; – вхождение в число крупнейших фирм-поставщиков услуг Интернета по домашним сетям;

- обеспечение требуемой рентабельности фирмы;
- возвращение взятых кредитов в оговоренные сроки.

Содержание раздела бизнес-плана «Продукция провайдерской фирмы». С этого раздела начинается основная часть бизнес-плана. Здесь описываются те услуги, которые собирается предложить провайдер потенциальным покупателям (конечным пользователям), а также дается основная информация по провайдерской фирме, которая помогает доказать потенциальному инвестору, что она способна осуществить производство заявленных услуг.

Удовлетворение потребностей человека в оперативной информации и общении является целью предоставления сетевых услуг. Интересы пользователей русскоязычных ресурсов Интернета могут быть охарактеризованы следующим составом:

- общественно-политические новости;
- деловые новости;
- погода;
- наука;
- путешествия, отдых;
- искусство;
- поиск работы;
- спорт;
- электронная коммерция, электронный бизнес;
- медицина;
- дистанционное обучение и образование;
- межличностные коммуникации;

- промышленность;
- IP-телефония и др.

Для удовлетворения потребностей конечных пользователей в соответствии с их интересами провайдерская фирма должна иметь соответствующие производственные фонды, располагать соответствующими нематериальными активами (лицензии, программные средства и т. п.).

Содержание раздела бизнес-плана «Маркетинговый план и исследование рынка». В рамках раздела маркетингового плана и исследования рынка можно выделить следующие основные подразделы:

- рынки сбыта;
- сегментация;
- прогнозы объемов продаж;
- ценообразование;
- анализ конкурентов;
- реклама;
- продвижение;
- стимулирование продаж;
- рынок ресурсов.

Бизнес Интернет-провайдера отличается отсутствием сезонности, что делает его особенно привлекательным, хотя могут происходить незначительные колебания численности конечных пользователей.

Трудности вхождения в информационный рынок для создаваемой провайдерской фирмы вызваны тем, что:

- крупные и состоявшиеся фирмы имеют гораздо более дешевые порталы связи с Интернетом, и соответственно, меньшие издержки;
- пользователи привержены компаниям, которые их устраивают и с которыми они уже работают.

Статистика показывает, что пользователь остается верен своему первому провайдеру либо провайдеру, услуги которого отличаются приемлемым соотношением «цена – качество». Таким образом, новая компания может сделать следующие рекламные ходы для привлечения потребителей:

- установить более низкие цены на подключение и более низкую абонентскую плату, чем у других домашних сетей в данном

районе; это могло бы заинтересовать клиентов, собирающихся впервые подключиться к сети Интернет по домашней сети;

– предложить абонентам других сетей бесплатно перейти на обслуживание в свою компанию (т. е. не взимая с них повторной платы за подключение).

В настоящее время рынок провайдинговых услуг в Санкт-Петербурге представлен достаточно большим количеством компаний. Таким образом, набрать портфель конечных пользователей в размере 5 000–10 000 физических лиц особых трудностей не составит.

Учитывая сущность оказываемых услуг и отсутствие нацеленности фирмы на узкий сегмент рынка, представляется целесообразным придерживаться массового подхода к оказанию услуг.

В ценообразовании предполагается придерживаться политики проникновения на рынок, что очень важно в условиях конкуренции. Низкие цены (в сочетании с высоким качеством) привлекут клиентов, а компания увеличит свою долю на рынке.

В части рекламной политики планируется прибегнуть, например, к следующим методам:

- реклама в журналах;
- реклама в газетах, а также в изданиях, распространяющихся бесплатно;
- реклама в городском транспорте;
- реклама в Интернете;
- рекламные плакаты в различных магазинах и точках, где будут продаваться Интернет-карты.

Рекламная кампания будет проводиться интенсивно на начальной стадии развития предприятия.

В дальнейшем фирма может производить реализацию услуг через собственную сбытовую сеть и/или авторизованных дилеров.

Содержание раздела бизнес-плана «Производственный план». Основная задача данного раздела бизнес-плана – доказать потенциальным партнерам, что фирма в состоянии производить необходимое количество информационных услуг в установленные сроки и с требуемым качеством.

Для реализации поставленной цели предприниматель при составлении бизнес-плана показывает, как будут решаться проблемы, связанные с помещениями, оборудованием, персоналом и т. д. По своей сути рассматриваемый раздел является технико-экономическим обоснованием разрабатываемого бизнес-плана.

При этом должны быть выделены следующие важные подразделы:

- способ производства, технология;
- производственные площади;
- оборудование;
- поставщики;
- потребность в оборотных средствах;
- общие затраты;
- заработка плата;
- смета затрат.

Провайдеру необходимо купить широкий канал в Интернете по оптовым ценам и распродать его конечным пользователям в виде узких каналов по розничным ценам. Ширина канала, выделенная пользователю, определяет, насколько быстро происходит обмен потоками данных между пользователем и сетью. Фирма-провайдер должна оценить ширину канала доступа в сеть.

Следует привести информацию об арендодателе и арендной плате. Следует также определить состав оборудования, приобретаемого или арендуемого фирмой-провайдером.

Содержание раздела бизнес-плана «Организационный план». После ответа на вопрос, как будут решены проблемы, связанные с производством услуг, важно решить проблему набора сотрудников и планирования их работы. Поэтому в данном разделе бизнес-плана обосновывается организация управления производственной деятельностью провайдерской фирмы, описываются квалификационные требования к специалистам и их состав.

Рассматриваемый раздел содержит следующие основные подразделы:

- организационная структура фирмы;
- организационно-правовая форма;
- менеджеры;
- персонал;
- законодательная база (регулирующая данный вид деятельности);
- стимулирование работы персонала.

Организационная структура создаваемой фирмы определяется составом и объемом информационных услуг.

В качестве примера на рисунке приведена организационная структура средней провайдерской фирмы.



Примерная организационная структура средней провайдерской фирмы

Одновременно с разработкой оргструктуры следует решить вопрос о выборе организационно-правовой формы провайдерской фирмы.

При определении состава и структуры привлекаемых к работе специалистов, руководящего и обслуживающего персонала необходимо руководствоваться объемом и видами информационных услуг, предлагаемых фирмой-провайдером. Надо помнить, что качество оказываемых услуг существенно зависит от квалификации работников фирмы.

Содержание раздела бизнес-плана «Оценка рисков». Каждому предпринимателю необходимо предусмотреть возможные трудности и заранее разработать стратегии их преодоления. При этом важно обосновать степень существующего риска.

Угроза может исходить от конкурентов, собственных просчетов при осуществлении производственной деятельности, маркетинговой политики и при подборе руководящих кадров. К рискам также относится вероятность пожаров и землетрясений, забастовок, межнациональных конфликтов.

Для более полной оценки рисков предлагается выделить количественные и качественные критерии. Качественные оценки рисков характеризуются:

- наименованием риска;
 - причиной риска;
 - влиянием риска на ожидаемую прибыль;
 - методами предотвращения риска и др.
- Количественные оценки рисков характеризуются:
- ранжированием риска;
 - весом рисков;
 - балльной оценкой рисков по видам и др.

Под риском может пониматься опасность того, что цели, поставленные в проекте, могут быть не достигнуты полностью или частично.

Если рассматриваемый проект охватывает несколько стадий, то оценку риска целесообразно проводить по ним (например, по подготовительной и стадии функционирования).

По характеру воздействия риски могут быть разделены на простые и составные. Составные риски являются композицией простых, каждый из которых рассматривается как простой риск. Простые риски определяются как инвариантные (независимые) по отношению к другим рискам.

Для оценки вероятности воздействия рисков используются мнения экспертов. Разработчиками проекта составляется перечень первичных рисков по всем стадиям проекта. Каждому эксперту предоставляется этот перечень для оценки вероятности наступления рисков, руководствуясь некоторой системой оценок:

- 0 – риск рассматривается как несущественный;
- 25 – риск, скорее всего, не реализуется;
- 50 – о наступлении события ничего определенного сказать нельзя;

- 75 – риск, скорее всего, проявится;
- 100 – очень большая вероятность реализации риска.

Оценки приоритетов должны отражать важность каждого отдельного события для всего проекта. После определения вероятностей по простым рискам проводится интегральная оценка риска по двум последовательным этапам, но перед этим рассматриваются простые риски для каждой стадии.

Для получения оценки объединенных рисков используется процедура взвешивания.

Все простые риски могут быть ранжированы по степени важности (по приоритетам). Риски первого приоритета имеют больший вес, чем риски второго, и т. д.; все риски с одним и тем же приоритетом имеют равные веса, а сумма весов всех простых рисков должна быть равна единице. Суммарная балльная оценка каждого простого риска легко вычисляется, если определены: величина приоритета, средняя оценка экспертов и вес для каждого простого риска.

Например, величина риска, связанного с появлением непредвиденных затрат, рассчитанная в табл. 1, составляет 5,25 и получена перемножением средней оценки экспертов и веса этого риска.

Веса каждого простого риска рассчитываются исходя из приоритетов, им присвоенных, и общего количества наименований рисков. Оценка составного риска представляет собой сумму оценок простых рисков, входящих в составной.

С помощью балльных оценок рисков выявляют перечень наиболее значимых рисков и проводят мероприятия по уменьшению их последствий для реализации бизнес-проекта. Необходимо отметить, что перечень рисков может быть дополнен или, наоборот, некоторые риски следует из него исключить как нетипичные для провайдерской фирмы.

В качестве условий предотвращения рисков могут быть рекомендованы следующие мероприятия:

- страхование имущества и ответственности работников провайдерской фирмы. Детальная проработка подготовительной стадии проекта с целью снижения значимых рисков;
- заключение долгосрочных контрактов с поставщиками с четкими условиями и штрафными санctionями;
- использование механизмов страхования рисков и др.

Таблица 1

Оценка простых и составных рисков

Наименование рисков	Эксперты			Средняя оценка экспертов	Приоритет риска	Вес риска	Балльная оценка риска
	Эксперт 1	Эксперт 2	Эксперт 3				
Риски на подготовительной стадии							
Непредвиденные затраты	50,00	50,00	75,00	58,33	1	0,09	5,25
Риски на стадии функционирования							
Финансово-экономические риски							
Неустойчивость спроса	50,00	75,00	50,00	58,33	1	0,09	5,25
Появление альтернативного продукта	50,00	75,00	50,00	58,33	2	0,04	2,32
...
...
Рост налогов	50,00	25,00	50,00	41,67	3	0,01	0,42
Социальные риски							
Трудности с набором квалифицированной рабочей силы	75,00	50,00	50,00	58,33	2	0,04	2,33
Отношение местных властей	25,00	25,00	0,00	16,67	2	0,04	0,67
...
...

Окончание табл. 1

Наименование рисков	Эксперты			Средняя оценка экспертов	Приоритет риска	Вес риска	Балльная оценка риска
	Эксперт 1	Эксперт 2	Эксперт 3				
Недостаточный уровень заработной платы	0,00	25,00	25,00	16,67	2	0,04	0,67
Технические риски							
Нестабильность работы оборудования	25,00	0,00	25,00	16,67	3	0,01	0,17
...
...
Отсутствие резерва мощности	50,00	50,00	50,00	50,00	2	0,04	2
Экологические и другие риски							
Вредность производства	50,00	25,00	0,00	25,00	3	0,01	0,25
...
...
				I	Некоторое число		

Содержание раздела бизнес-плана «Финансовый план». Важнейшим разделом разрабатываемого документа является финансовый план. Он формируется с целью обеспечения потребности фирмы в денежных ресурсах и достижения (поддержания) устойчивого финансового состояния.

Необходимо выделить следующие основные подразделы:

- источники собственных средств;
- источники заемных средств;
- прогноз объемов реализации продукции;
- общие затраты;
- заработка плата;

- налоги и отчисления в бюджет;
- отчет о движении денежных средств (простой и дисконтированный);
- график безубыточности;
- отчет о прибылях и убытках.

Следует особо отметить, что структуризация разделов бизнес-плана позволяет реализовать такие основополагающие требования, как достаточность и доступность для восприятия (при наличии четкой структуры потенциальному партнеру, в т. ч. и инвестору, легче принять правильное решение о сотрудничестве).

При формировании финансового плана необходимо определить размеры собственных средств, вкладываемых в дело, а также источники заемных средств с указанием размеров необходимых кредитов.

Прогноз объемов реализации информационной продукции следует сделать на 1-й год с разбивкой на месяцы, а затем на последующие 2–4 года. На больший период времени этот прогноз составлять не следует.

Необходимо определить объемы реализации продукции провайдинговой фирмы в стоимостном выражении от величины затрат и, наконец, планируемой прибыли. Результаты расчетов затрат, доходов и прибыли фирмы могут быть сведены в таблицу (табл. 2), и эта таблица, по сути дела, объединяет в себе прогноз продаж и план по прибыли.

По той же форме можно предоставить данные по нескольким планируемым периодам (2–4 года).

Используя сведения из баланса фирмы и данные прогноза объемов реализации продукции и затрат, можно определить уровень общей рентабельности провайдерской фирмы (табл. 3).

В этом разделе следует также представить смету заработной платы, отчет о прибылях и убытках провайдерской фирмы, сводный баланс активов и пассивов и график достижения безубыточности.

Этот раздел может быть дополнен вопросами, связанными со стратегией финансирования бизнес-проекта. Например, уточняется план получения средств, их форма, период возврата капитала, величина прибылей.

Таблица 2
Прогноз реализации продукции на 1-й год деятельности фирмы

Наименование продукта (услуги)	Цена продукта (услуги), у. е.	Планируемый период (1 год)							
		1-й месяц				2-й месяц			
		Объем продукции, ед. изм.	Выручка, у. е.	Общие затраты, у. е.	Балансовая прибыль, у. е.	Чистая прибыль, у. е.	Объем продукции, ед. изм.	Выручка, у. е.	...
Предоставление трафика	6,0	1 000	6 000	4 000	2 000	1 540	2 000	1 200	...
Разработка сайтов для конечных пользователей	500	15	7 500	5 000	2 500	1 970	5	2 500	...
...
...

Таблица 3
Определение уровня общей рентабельности

Наименование показателей	1-й год	2-й год	3-й год
Балансовая прибыль, у. е.	27 000	42 000	63 000
Среднегодовая стоимость ОПФ и нормируемых оборотных средств, у. е.	32 000	34 000	41 000
Рентабельность фирмы, %	85	126	154

Часто задают вопрос: что нужно сделать, какие документы необходимо собрать, чтобы стать Интернет-сервис-провайдером?

Чтобы стать провайдером, следует как минимум:

- получить (купить, арендовать) высокоскоростные международные каналы связи;
- подключиться к провайдерам других уровней;
- заключить договоры с основными провайдерскими фирмами об обмене трафиком.

УДК 378.001.658.011.56

И. А. Брусакова, В. И. Фомин

Санкт-Петербургский государственный
инженерно-экономический университет

**МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ ПО НАПРАВЛЕНИЮ
«ПРИКЛАДНАЯ ИНФОРМАТИКА»:
ВАРИАНТЫ ПОСТРОЕНИЯ**

В соответствии с требованиями к уровню подготовки магистра по направлению 080800 – «Прикладная информатика» магистерская диссертация должна представлять собой законченную теоретическую или экспериментальную научно-исследовательскую работу, связанную с решением актуальных задач, определяемых особенностями подготовки по конкретной магистерской программе направления «Прикладная информатика». Требования к структуре, содержанию и объему магистерской диссертации определяются вузом на основании Государственного образовательного стандарта высшего профессионального образования по направлению 080800 и методических рекомендаций учебно-методического объединения (УМО) по образованию в области прикладной информатики.

Как представляется, могут быть отмечены следующие особенности формирования требований к магистерской диссертации по рассматриваемому направлению:

– наличие по ограничению квалификационной работы магистра (ограничения «снизу», обусловленные требованиями к выпускным квалификационным работам (ВКР) бакалавра и специалиста; ограничения «сверху», обусловленные требованиями к диссертации на соискание ученой степени кандидата наук);

– возможность предоставления в качестве магистерской диссертации как теоретической, так и экспериментальной научно-исследовательской работы, что заведомо допускает различные варианты структуры, содержания и объема ВКР для магистра;

– возможность реализации нескольких (различных) магистерских программ в рамках направления «Прикладная информатика»,

что, несомненно, предполагает особенности построения магистерской диссертации по этим программам.

С учетом вышеизложенного в рамках магистерской программы «Прикладная информатика (в аналитической экономике)» могут быть предложены следующие базовые варианты построения магистерских диссертаций.

Вариант 1. Теоретическая научно-исследовательская работа, содержащая:

– анализ и выявление экономико-организационных проблем в выбранной предметной области, требующих применения научных математических средств для успешного решения;

– анализ состояния научной проработки выявленных проблем (наличие соответствующих моделей, методов, инструментальных средств, оценка их эффективности для решения выявленных проблем, сопоставительный анализ различных известных подходов и т. д.);

– выявление научных проблем, требующих решения применительно к выбранной предметной области, предложения по путям разработки соответствующих научных методов, моделей (адаптация существующих методов к предметной области; применение научных методов, не применявшимся до сих пор для рассматриваемой предметной области; разработка новых методов и моделей и т. д.);

– предложения по возможным вариантам решения рассматриваемой научной проблемы (отдельные модели, соображения по их модификации; определение научного аппарата, с помощью которого могут быть получены искомые решения, и т. п.).

Данный вариант магистерской ВКР может рассматриваться как аналитическая и постановочная научно-исследовательская работа. Такая работа, по существу, представляет собой первую часть кандидатской диссертации, которая в дальнейшем может быть подготовлена в рамках обучения в аспирантуре.

Вариант 2. Теоретическая научно-исследовательская работа, аналогичная в своей аналитической и постановочной части первому варианту, но отличающаяся двумя моментами:

– сосредоточением внимания при анализе на более узком вопросе, затрагивающем лишь некоторые аспекты экономических

проблем в выбранной предметной области, а также ограничением научной постановки каким-либо частным вопросом научных (математических и инструментальных) методов решения указанной проблемы;

– доведением до конкретного решения выбранной научной проблемы (моделирование известной модели применительно к новой предметной области; решение какого-либо частного вопроса в рамках предлагаемых модификаций или разработки математических моделей и т. п.).

Данная версия ВКР также может рассматриваться как своеобразный задел для кандидатской диссертации, отличающийся от полномасштабной диссертации прежде всего локальностью (узостью) решаемой научной проблемы, которая представляет собой одну из «подпроблем», разрабатываемых в рамках кандидатской диссертации проблем.

Вариант 3. Экспериментальная научно-исследовательская работа, содержащая:

– анализ и выявление экономико-организационных проблем в выбранной предметной области, требующих изменения научных, математических или инструментальных средств для их успешного решения;

– обзор и анализ состояния научной проработки выявляемых проблем и выбор на основе сопоставительного анализа математической модели метода (группы моделей, ансамбля методов) для решения выявленных проблем в выбранной предметной области;

– сбор необходимых данных, проведение необходимых в соответствии с выбранными методами (моделями, методиками) расчетов, анализа, обоснования решений для выбранной предметной области;

– анализ результатов, полученных на основе применения известных научных моделей, методов, методик, оценка их адекватности поставленным задачам;

– оценка экспериментального применения известных методов, методик, предложения по их изменению в аналогичных ситуациях, по совершенствованию известных методик и т. п.

Данный вариант магистерской ВКР также может рассматриваться в качестве предварительной работы, позволяющей на основе экспериментальной проверки известных моделей, методов, методик поставить вопрос об их развитии и совершенствовании в рамках кандидатской диссертации.

Вариант 4. Экспериментальная научно-исследовательская работа, содержащая:

– анализ и выявление экономико-организационных проблем выбранной предметной области, требующих применения инструментальных средств (прежде всего программно-технических) для их успешного решения;

– анализ известных инструментальных средств для решения выявленных экономико-организационных проблем, оценка их эффективности для рассматриваемой области, сопоставительный анализ известных средств;

– описание разработанных (моделированных) в рамках магистерской диссертации инструментальных средств, описание их экспериментальной проверки для выявления и решения экономико-организационных проблем, оценка адекватности полученных результатов, оценка эффективности предложенных инструментальных средств, границ применимости и т. д.

Данный вариант магистерской диссертации также может рассматриваться в качестве задела для кандидатской диссертации (в частности, по научной специальности «Математические и инструментальные средства экономики»).

В части требований к оформлению магистерской диссертации целесообразно принять за основу требования межгосударственного стандарта ГОСТ 7.32–2001 «Отчет о научно-исследовательской работе. Структура и правила оформления» (введен в действие с 1 июля 2002 г. взамен ГОСТ 7.32–91).

Предлагаемые варианты построения магистерской диссертации могут быть приняты за основу требований вуза к магистерской диссертации по направлению «Прикладная информатика». Список вариантов носит предварительный характер и может расширяться и уточняться по мере получения практического опыта написания и защиты магистерской ВКР.

УДК 378.001.658.011.56

В. Н. Бугорский, А. Г. Сергиенко

Санкт-Петербургский государственный
инженерно-экономический университет

ОСОБЕННОСТИ МОДЕЛИРОВАНИЯ ПРОГНОЗА КОТИРОВОК ЦЕННЫХ БУМАГ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННЫХ СЕТЕЙ

В последнее десятилетие наблюдается устойчивый рост популярности технического анализа – набора эмпирических правил, основанных на различного рода индикаторах поведения рынка. Технический анализ сосредотачивается на индивидуальном поведении финансового инструмента вне его связи с остальными ценными бумагами. Но технический анализ очень плохо работает там, где нужно прогнозировать направление цены. Поэтому все большую популярность приобретает нейросетевой анализ, поскольку, в отличие от технического, он не предполагает никаких ограничений на характер входной информации. Это могут быть как индикаторы данного временного ряда, так и сведения о поведении других рыночных инструментов. В связи с этим нейросети активно используют брокеры, для которых особенно важны корреляции между различными рынками. Кроме того, нейросетевые технологии успешно применяются в самых различных областях – экономике, медицине, технике, геологии, физике, решая задачи прогнозирования, классификации, управления и др. [5].

Предсказание финансовых временных рядов – важный элемент любой финансовой деятельности. Сама идея осуществления торгов ценными бумагами – покупка или продажа сейчас с целью получения дохода в будущем – основывается на идее прогнозирования будущего. Соответственно, предсказание финансовых временных рядов лежит в основе деятельности всей финансовой индустрии – всех бирж и небиржевых систем торговли ценными бумагами.

На практике известно, что 99% всех сделок – спекулятивные, т. е. направлены не на обслуживание реального товарооборота, а заключены с целью извлечения прибыли. Все биржевые операции основаны на предсказаниях изменения курсов участниками сдел-

ки, причем предсказания участников каждой сделки противоположны друг другу. Таким образом, объем спекулятивных операций характеризует степень различий в предсказаниях участников рынка, т. е. реально – степень непредсказуемости финансовых временных рядов.

Нейросетевое моделирование в чистом виде базируется лишь на данных, не привлекая никаких априорных соображений. В этом его достоинство и одновременно – его недостаток. Например, может не хватить имеющихся данных для обучения, размерность потенциальных входов может оказаться слишком велика и др. [3].

Прежде чем использовать модель нейросети для прогнозирования котировок, необходимо подготовить данные для анализа. На практике предобработка данных может стать наиболее трудоемким элементом нейросетевого анализа. Причем знание основных принципов предобработки данных не менее, а, может быть, и более важно, чем знание собственно нейросетевых алгоритмов.

Известен ряд случаев, в которых на изменение котировок ценных бумаг часто влияют другие, неэкономического характера факторы, которые зачастую определяют резкие скачки в изменении цен: высказывания известных политиков, вооруженные конфликты и др. Кроме того, не всякая входная или выходная переменная может иметь численное выражение. Соответственно, такие переменные следует закодировать – перевести в численную форму, прежде чем осуществлять нейросетевую обработку. В связи с этим нейронные сети могут учитывать данные факторы, представляя их влияние в численной форме, что также подчеркивает значимость и высокую эффективность нейросетевых технологий [1].

Как входами нейросети, так и выходами могут быть совершенно разные величины. Очевидно, что результаты нейросетевого моделирования не должны зависеть от единиц измерения этих величин. Чтобы сеть трактовала их значения единообразно, все входные и выходные данные должны быть приведены к единому единичному масштабу. Кроме того, для повышения скорости и качества обучения полезно провести дополнительную предобработку данных, выравнивающую распределение значений еще до этого этапа обучения.

Однако для хорошего прогноза нужно пользоваться качественно подготовленными данными. Существуют различные методы

подготовки данных для анализа. Наиболее часто в качестве входных параметров используют значения котировок ценных бумаг за временной период.

В связи с тем, что между последовательными значениями курсов имеется большая корреляция, а их изменения, как правило, гораздо меньше по амплитуде, чем сами котировки, то в другом случае в качестве входов и выходов нейросети используются не сами значения котировок, а изменения значений котировок. Таким образом можно увеличить интервал прогнозирования значений цен в силу того, что граница изменений цен на порядок меньше, чем граница самих значений цен (рисунок).

Между тем, для повышения качества обучения следует стремиться к статистической независимости входов, т. е. к отсутствию подобных корреляций. Поэтому в качестве входных переменных логично выбирать наиболее статистически независимые величины.

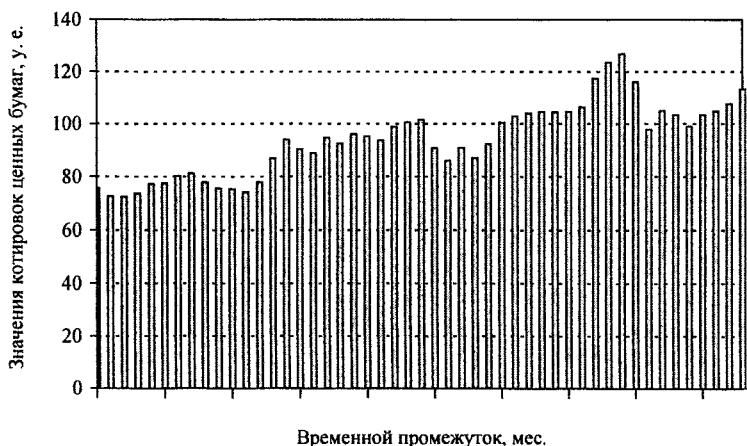
Последний выбор эффективен особенно для длительных временных рядов. В этом случае простые разности в разных частях ряда будут иметь различную амплитуду. Напротив, отношения последовательных котировок не зависят от единиц измерения и будут одного масштаба, несмотря на различные единицы измерения. В итоге большая стационарность ряда позволит использовать для обучения большую историю и обеспечит лучшее обучение [2].

Очевидно, что чем дальше в прошлое уходит история ряда, тем меньше деталей его поведения влияет на результат предсказаний. Следовательно, надо найти такое представление динамики ряда, которое имело бы избирательную точность: чем больше временной промежуток – тем меньше деталей при сохранении общего вида кривой.

Архитектура нейросети зависит от поставленной задачи, в большинстве случаев используются сети типа «многослойный перцептрон» [4].

Поскольку прогнозирование никогда не сможет полностью уничтожить риск при принятии решений, необходимо явно определять неточность прогноза. Обычно принимаемое решение определяется результатами прогноза (при этом предполагается, что прогноз правильный) с учетом возможной ошибки прогнозирования [1].

Гистограмма значений котировок ценных бумаг



Гистограмма изменений значений котировок ценных бумаг



Гистограмма значений и гистограмма изменений значений котировок ценных бумаг

Таким образом, нейросети являются прогрессивным элементом построения и анализа модели прогнозирования котировок ценных бумаг, имеющими большое прикладное значение как в экономике, так и во многих других областях науки. Их уникальность заключается еще и в том, что аналитику не требуется обширных знаний в нейросетевых алгоритмах и теории статистики, а значит использование нейросетевых методов прогнозирования доступно не только для брокеров, но и для обширного круга людей, не специализирующихся на биржевых торгах.

Литература

1. Бестенс Д., Ван ден Берг В., Вуд Д. Нейронные сети и финансовые рынки: принятие решений в торговых операциях. М.: ТВП, 1997.
2. Терехов С. А. Вейвлеты и нейронные сети: [Электронный ресурс]: alife.narod.ru/lectures/wavelets2001/index.html
3. Введение в теорию нейронных сетей: [Электронный ресурс]: www.orc.ru/~stasson/neurox.html
4. Введение в сети встречного распространения: [Электронный ресурс]: www.intuit.ru/department/ds/neuronnets/6/
5. Масалович А. Нейронные сети в России за полчаса до весны: [Электронный ресурс]: www.icmm.ru/~masich/win/lexion/neituss.htm

УДК 378.001.658.011.56

**В. Л. Горохов, П. Террикорпи,
Ю. В. Барышев**

Санкт-Петербургский государственный
инженерно-экономический университет

КОНСТРУИРОВАНИЕ КОМПЬЮТЕРНЫХ МЕТАФОР НА ОСНОВЕ ФЕНОМЕНОЛОГИЧЕСКИХ ОНТОЛОГИЙ ДЛЯ СИСТЕМ КОГНИТИВНОЙ МАШИННОЙ ГРАФИКИ

Введение. Проблемы эффективной организации наблюдений и мониторинга астрофизических и космологических объектов как сложных систем изучаются и решаются сегодня на международном

и национальном уровнях [1–15]. Информационное обеспечение таких наблюдений требует развития нового поколения информационно-аналитических систем – ИАС (интеллектуальные информационные системы – ИИС), обеспечивающих интеллектуальную поддержку принимаемых решений в соответствии с результатами мониторинга. Серьезная особенность объектов мониторинга как сложных систем состоит в глубокой априорной неопределенности характеристик состояния этих систем [2; 12–14].

В настоящее время отсутствуют информационные системы аналитического типа для интеллектуальной поддержки принятия решений по результатам мониторинга, работающие в условиях значительной (глубокой) неопределенности состояния таких сложных систем.

Создание подобных программных продуктов требует практического освоения целого комплекса достижений в области математической статистики, теории нечетких множеств, когнитивной машинной графики, когнитивной психологии и, прежде всего, – теории познания (гносеологии).

В данной работе делается попытка изложения ряда достижений в перечисленных областях с учетом инженерной специфики их возможного применения. Работа опирается на возможности использования этих достижений на уже действующих программных средствах интеллектуальной поддержки принимаемых решений в задачах управления сложными системами с глубокой априорной неопределенностью. Это в первую очередь системы, использующие когнитивную машинную графику (системы SWOT, PEST-анализа, системы динамической визуализации многомерных данных X-Gobi, SW, SCV и т. д.).

Внимание концентрируется на принципиальных философских идеях и понятиях, освоение которых позволит эффективно и рационально использовать все возможности новых информационных технологий в практике управления сложными системами.

1. Идея отражения феноменологических онтологий в когнитивных образах. Разработанный в когнитивной машинной графике и теории баз данных набор понятий, включающих понятия онтологии, семантики, ноэмы когнитивного образа данных (попрежних объектом мониторинга и отражающих его фундаментальные свойства), построен на глубоких аналогиях между зада-

чами поддержки принятия решений в условиях глубокой априорной неопределенности и познавательными процессами, описываемыми в теории познания. Этот набор понятий дает возможность модернизировать интеллектуальные интерфейсы современных систем поддержки принятия решений и систем машинной графики. Появляется возможность формирования новых идей, методологий и основанных на них методик работы с интеллектуальными интерфейсами.

Использование данного подхода в сочетании с перспективным медиа-оборудованием открывает принципиально новые возможности конструирования технических средств для стимуляции творческих возможностей человека – оператора (такие средства получили название техногностических систем).

Современные объекты космического мониторинга представляют собой столь сложные и малоисследованные объекты, что неизбежно для их изучения требуется активизация не только конкретных теоретических парадигм, но и подключение всего комплекса гносеологических концепций лица, принимающего решения (ЛПР), его научной и эстетической интуиции, всего комплекса эмпирических знаний и навыков. Ярким примером подобных задач являются задачи наблюдательной космологии. Здесь ЛПР имеет дело с целым комплексом научных теорий и философских взглядов, которые необходимо учитывать при организации и проведении мониторинга. Весь комплекс взглядов исследователя можно представить в виде феноменологических онтологий (в стиле Э. Гуссерля, М. Хайдеггера, Ж. П. Сартра). Их онтологии включают в себя широкий спектр и более традиционных философских взглядов – так что естествоиспытатель имеет широкие возможности для классификации и выбора своих философских предпочтений. Необходимость такого подхода к современным научным исследованиям фундаментального характера указывают как философы науки (К. Поппер, Л. Витгенштейн, Р. Карнап, Б. Рассел и др.), так и сами естествоиспытатели (В. Гайзенберг, Р. Хойл, Р. Пенроуз, Ж. Пиаже, Г. Селье и др.).

В данной работе предлагается идея связи и отражения феноменологических онтологий в когнитивные образы, образованные на основе многомерных данных мониторинга или космического эксперимента. При этом здесь главное – предложить метафорическую

модель, связывающую объекты реального мира с теоретическими представлениями современной науки, с одной стороны, и онтологическими моделями философии – с другой. Полезность метафор в теории познания и науке как «моста» между научной интуицией и рациональным знанием отмечена в трудах С. С. Гусева.

1.1. Этапы отражения феноменологических онтологий в когнитивные образы. Очевидно, что естественнонаучная теория предполагает объекты, которые отражаются в теории как реально существующие. Совокупность (универсум) подобных объектов и образует онтологию этой теории. Обычно в этой связи говорят об онтологических допущениях языка теории. К сожалению, в стандартной семантике, по мнению многих исследователей, какой-либо определенный модус существования вообще не фиксируется. Традиционно считается, что семантика имеет дело с отношением наших утверждений к действительности, а онтология есть теория представления этой действительности. Поэтому, используя логическую семантику, необходимо учитывать возможность строгой фиксации всего набора нюансов, связанных с возможными трактовками феномена сознания и интеллекта разными исследователями (пользователями систем интеллектуальной поддержки принимаемых решений).

Таким образом, развитие систем искусственного интеллекта поставило логическую семантику (особенно алгебраическую) в положение наиболее актуального и интенсивно развивающегося раздела логики. Использование средств логической семантики как инструмента для формулировки гносеологически более тонкой понятийной структуры для систем добывания (Data Mining) и хранения научных знаний позволяет исследователю более детально формулировать его интуитивные, эмпирические и философские взгляды на объект исследования. Формулировки, выраженные в терминах логической семантики, обеспечивают возможность оригинальным и вполне рациональным образом повлиять на интерпретацию зрительных образов в системах когнитивной визуализации данных научных наблюдений (и мониторинга). Другими словами, это дает возможность изучения различных представлений и концепций предметной области, обогащения ее новыми видами объектов, в том числе и на основе когнитивных образов.

Например, идеи виртуальных наблюдательных систем. Для современных компьютерных технологий (когнитивная машинная графика и системы виртуальной реальности) необыкновенно важной является предметная область, включающая в себя действительные, возможные и виртуальные объекты. «Возможный» здесь означает «возможный относительно некоторой априорной теории». «Виртуальный» же можно понимать как идеальный (абстрактный, эйдетический) объект. Примеры таких объектов: бесконечность в обычной теории действительных чисел, бесконечно удаленная точка в проективной геометрии, виртуальные классы в теории множеств и т. п.

«Мыслимость» возможных объектов в подобного рода семантике может означать ситуацию их истолкования как объектов нашего внимания (интенциональных объектов), на которые направлено наше сознание. В этом случае действительные объекты составляют подмножество интенциональных объектов.

Так, в случае модальной логики операторы возможности и необходимости представляют собой интенциональные операторы, а возможные миры, понимаемые как различные собрания объектов с дополнительной структурой или без нее, можно считать интенциональными состояниями. Такой подход может оказаться особенно плодотворным при постановке космологических наблюдений, когда надо учитывать при планировании наблюдений весь «набор» теорий и философских установок в отношении крупномасштабной структуры Вселенной.

Для анализа и систематизации подобных «наборов» целесообразно использовать разработанную В. Л. Васюковым теорию предметной области – *формальную онтологию*, в которой исследуются формальные структуры объектов и возможные отношения между ними. Полезность таких теорий заключается в развитии новых систем онтологических объектов, с одной стороны, и в возможности создания программных средств поддержки визуализации таких объектов (на основе экспериментальных данных) – с другой. По сути, речь идет о развитии идей байесовской логики и статистики за счет новых открытий в гносеологии (феноменология, когнитивность, формальная онтология, логическая семантика, логика имен Лесневского).

Понятие интенциональности, так необходимое для выяснения различия между возможными и мыслимыми объектами, возникло в феноменологии. Как отмечает Васюков, обращение логиков (а за ними и специалистов по созданию систем искусственного интеллекта и систем интеллектуальной поддержки решений) к феноменологии в этом контексте носит обоснованный характер, ибо принимаемый ими понятийный аппарат давно уже (и гораздо лучше) разработан в рамках феноменологии.

Согласно терминологии, предложенной Васюковым, далее расширение парадигмы формальной онтологии обозначается термином «формальная феноменология», ибо такое название с самого начала побуждает действовать с учетом вклада феноменологических идей в проводимые исследования.

Как отмечает Васюков, формальная феноменология не призвана подменить собой «традиционную» феноменологию. Ее цель – создание нового раздела логических и компьютерных исследований: построение новых компьютерных метафор, логических систем и основанных на них программных систем поддержки интеллектуальных решений, использующих идеи феноменологии. Здесь речь идет прежде всего о процессах отображения логической структуры феноменологических конструкций, порожденных когнитивной графикой в сознании ЛПР с помощью языков неклассической логики.

Особенность такого отображения заключается в том, что фактически оно является переводом, который носит двухступенчатый характер: логическая структура (содержание) феноменологических концепций переводится вначале на неформальный язык содержательной семантики разрабатываемых исчислений.

Дальнейшая строгая синтаксическая передача этих концепций – это уже некоторая «кодификация» связей данной структуры с помощью формального языка. На основе этого формального языка возможна разработка интеллектуальных программных интерфейсов для поддержки принятия решений в отношении сложных систем (например, космологических моделей) в условиях глубокой априорной неопределенности их поведения. Однако прежде всего требуется перевод феноменологических концепций на неформальный язык содержательных семантик.

Таким образом, можно сформулировать основной тезис новой идеологии формирования графических интерфейсов систем

поддержки интеллектуальных решений в условиях априорной неопределенности объектов и условий наблюдения. Проектирование и эксплуатация графических интерфейсов систем анализа экспериментальных данных и мониторинга сложных объектов должно начинаться с построения феноменологически ориентированных процедур выявления логических структур в когнитивных образах многомерных данных эксперимента и в отображении этих логических структур феноменологических конструкций на неформальный язык содержательной семантики с учетом и при поддержке возможностей когнитивной визуализации этих конструкций.

Подобный неформальный язык содержательной семантики, ориентированный на возможности визуализации когнитивных образов данных эксперимента, позволит учитывать и интерпретировать эти данные с учетом рациональных моментов философских учений, разработанных такими феноменологами, как Э. Гуссерль, А. Мейнинг, К. Твардовский, Р. Ингарден, Ж. П. Сартр.

Принципиальные особенности этих философских учений, переведенные на язык содержательной семантики, позволят при создании программных интерфейсов систем поддержки принятия решений *отразить весьма важные философские установки* лиц, принимающих решения. Напомним, что естествоиспытатели при интерпретации данных эксперимента всегда используют определенные познавательные (философские) установки, которые неизбежно связаны с определенными философскими системами. Эта связь в любом случае установлена основоположниками той или иной естественнонаучной парадигмы. А последователи парадигмы используют эту связь (порой неосознанно), применяя научные методики конкретной парадигмы.

Эти философские установки, естественно, оказывали (и оказывают) во многом решающее значение на механизм принятия решений и при этом абсолютно никак не контролировались и часто не осознавались естествоиспытателями (см. работы Марио Бунге).

Теперь появилась возможность с помощью таких интеллектуальных интерфейсов объективировать ранее практически «неувидимые», но «могучие» стимулы (те самые познавательные установки), возникающие у лиц, принимающих решения. Еще раз подчеркнем, что сами ЛПР подчас не отдают себе отчета в той роли, кото-

ную оказывают на них эти философские установки в процессе принятия решений.

Между тем предлагаемая идеология работы с графическими интерфейсами заставляет пользователя обратить свое внимание на эти установки, ибо они определяют характер выделения и селекции структур на когнитивных образах и фиксируются программными средствами. Кроме того, эти философские установки могут служить и в качестве аргументов, проясняющих мотивы принимаемых решений. Они смогут быть приведены в стройную систему аргументации принимаемых решений в условиях глубокой априорной неопределенности.

Подчеркнем, что отображения логической структуры феноменологических конструкций в интерфейсах первоначально будут носить когнитивный, графический характер.

Дальнейшее развитие выдвинутых идей основывается на анализе философских аспектов данной предметной области, который позволяет формировать научные метафоры, приводящие к феноменологическим структурам и отождествлению этих структур средствами когнитивной машинной графики. Результатом когнитивного машинного анализа данных наблюдений будет являться система логических высказываний на языке логики имен Лесневского, которая будет иметь естественнонаучную интерпретацию в данной предметной области. Для исследователей, имеющих разные гносеологические установки, разумеется, эти системы высказываний будут отличаться. Однако теперь эти отличия строго кодифицированы и декларированы и возможная научная дискуссия будет конструктивно направлена на обсуждение гносеологических установок исследователей. Тем самым снимается целый ряд современных проблем интерпретации наблюдательных данных в космологии и квантовой физике. Для выяснения взаимосвязей между различными построенными системами можно применять снова средства когнитивной машинной графики или современные средства логической семантики и формальной феноменологии.

Авторы выражают надежду, что эти исследования помогут в дальнейшем строгой синтаксической «кодификации» связей логических структур наблюдательных данных с онтологическими схемами физических теорий на основе разнообразных методов современной неклассической логики. Таким образом, появятся строгие математи-

ческие модели не только для теоретических онтологических структур, но и для структур многомерных наблюдательных данных. Есть надежда, что такие математические модели структур многомерных данных наблюдений в условиях глубокой априорной неопределенности (многообразия Грасмана) естественным образом послужат новым стимулом для развития математической теории эксперимента, которая сейчас успешно описывает контролируемые и управляемые научные эксперименты в рамках гауссовых моделей.

Далее в данной работе делается попытка впервые построить компьютерную метафору онтологических структур, для семантики которых характерны предметные области, в которых приходится иметь дело с принципиально разными теоретическими подходами и гносеологическими установками. Речь идет прежде всего о наблюдательной проверке космологических моделей. Это как раз тот случай, когда естествоиспытатель имеет дело с интенциональными объектами.

Здесь возможны два варианта.

1. Имеется многомерный массив уже проведенных наблюдений (например, глубокие космологические обзоры) и требуется соопоставить эти многомерные данные с различными теоретическими схемами на предмет выбора той теоретической схемы, которая дает наилучшие соответствия с наблюдательными данными. При этом нужно учесть и возможные различия в гносеологических установках ученых, проводящих сопоставление.

2. Планируется проведение наблюдений, выявляющих ту теоретическую схему, которая будет описывать многомерные наблюдательные данные и подтверждать (фиксировать) такой элемент логической структуры теории, который отсутствует в альтернативных проверяемых теоретических схемах (критический эксперимент). Имеются в виду критические тесты релятивистской космологии и тесты физики гравитационного взаимодействия. Очевидно, что здесь ситуация повторяется: опять разные теоретические схемы (разные онтологии) и разные гносеологические установки, которые надо учитывать при постановке экспериментов.

1.2. Проблемы формализации феноменологических конструкций онтологических систем. Как отмечалось выше, современная наука и технология втягивают в орбиту производственной и научной деятельности принципиально новые типы объектов,

требующие развития новых стратегий обращения с ними [1–3; 7–9; 12–14].

Речь идет об объектах, представляющих собой саморазвивающиеся сложные системы, характеризующиеся синергетическими эффектами, развитие которых всегда сопровождается особыми состояниями неустойчивости, и, как следствие этого, – априорной неопределенностью своих характеристик. Современная практика мониторинга сложных систем уже давно показала, что наряду с методами робастного наблюдения целесообразно активно использовать интуицию и эвристический опыт лица, принимающего решение (ЛПР), которые дополняют робастные решения. Фрагменты таких сложных систем можно, безусловно, причислять к эрготехническим (человеко-машинным) системам. Хорошо известно, что саморазвивающиеся синергетические эрготехнические системы характеризуются принципиальной открытостью и не обратимостью процессов (В. Ф. Венда). Увы, для них (систем мониторинга) само человеческое действие не является чем-то внешним, а как бы включается в систему, видоизменяя каждый раз поле ее возможных состояний. В этом смысле человек не только представляет ее составную часть, но и изменяет ее с использованием фантастического потенциала человеческого сознания. И теперь появилась возможность объективно это учитывать.

Перед естествоиспытателем (ЛПР) в процессе принятия интеллектуальных решений возникает проблема выбора некоторой линии развития из множества возможных путей эволюции сложных систем. Причем этот выбор необратим и обычно не может быть детально просчитан. Интуитивное восприятие этих систем и проблем выбора для ЛПР неизбежно связано с онтологическими моделями этих систем. Это и есть тот резерв, из которого ЛПР черпает вдохновение в процессе принятия решений. Часто это происходит на интуитивном уровне и не осознается ЛПР как рациональный процесс. Между тем в настоящее время появляется возможность отчасти объективировать этот процесс, пользуясь языком содержательной семантики и когнитивными образами.

Таким образом, описание состояния этих сложных систем неизбежно связано с неформальным языком содержательной семантики, который в свою очередь связан с определенными онтологическими структурами, наиболее адекватными этим объектам с точки

зрения ЛПР. В связи с этим требуется дать краткое описание типовых компьютерных метафор, отражающих особенности возможных онтологических систем, сформированных к настоящему времени в философии.

Разумеется, философы формировали варианты онтологических систем под давлением прежде всего естествоиспытателей. Более того, наиболее глубокие онтологические системы разрабатывались учеными, которые одновременно были выдающимися естествоиспытателями и философами.

Традиция отталкивается от Аристотеля, Лейбница, Декарта, Паскаля и продолжается Кантом, Брентано, Кантором, Гильбертом, Фреге, Махом, Бриджменом, Гуссерлем, Вейлем, Расселом, Гайзебергом и т. д.

Такой подход в настоящее время уже опровергается технически в индустрии добывания знаний (Data Mining) и в современных системах управления сложными системами ERP, OLAP, BMP. «Добывание», фиксация, «усвоение» эмпирического опыта рассматриваются в таком перспективном направлении информатики, как инженерия знаний. Именно в этом направлении активно используются достижения когнитивной психологии, эпистемологии и математических средств реляционной алгебры. Инженерия знаний успешно продемонстрировала, что для привлечения и стимуляции интуитивных знаний, безусловно, требуются новые технические средства. Это прежде всего системы когнитивной машинной графики и системы виртуальной реальности [20–24]. Помимо технических средств, требуются и разрабатываемые ниже компьютерные метафоры, отражающие различные онтологические структуры, которые порождаются в сознании ЛПР при попытках описания предметных областей в идеологии Data Mining. Но прежде всего надо для дальнейшей работы более корректно определить понятие онтологии.

Для правильного формирования метафор приведем наиболее распространенные определения онтологии, принятые в философии.

Прежде всего, онтологию можно понимать как теорию того, что есть, теорию бытия. Онтология рассматривает полный универсум, включающий все предметы, являющиеся возможными. С данной точки зрения это общая теория отношений, общая теория вещей и свойств, или теория ситуаций, событий и процессов.

Заметим, что многие онтологические типы явно подразумевают нелогические аспекты анализа. Наиболее удачные классификации типов онтологии предлагает Р. Поли.

1. *Онтология объектов и свойств*. Основывается на номинальной предикации. Такая онтология была отражена в работах Аристотеля. Предполагается соответствие между лингвистической и онтической формами (наложение языковой решетки на мир). Лингвистические варианты в перспективе моделирования представлены в работах Рудольфа Карнапа.

2. *Стратифицированная онтология*. Описывает мир в категориях зависимости. Первичная внутренняя дифференциация определяется по вопросу принятия или опровержения различия между общей и локальной онтологией. С философской точки зрения подобной онтологией является феноменологическая онтология Гуссерля, Шелера, Ингардена и Гартмана. Если зависимость между слоями (стратами) описывается с помощью отношений, то получаем семантику Тарского, если зависимость описывается с помощью функции, получаем семантику Фреге и Черча. Отражением такого подхода в физике и математике являются общая теория систем, теория катастроф и термодинамика.

3. *Онтология событий*. Основывается на вербальной и невербальной предикации. Онтология такого типа изучается в работах Гегеля, Уайтхеда (монизм). Объектами онтологии являются динамические сущности. В современной физике это теория динамических систем, включая теорию относительности и квантовую теорию поля.

4. *Комбинаторная онтология*. Описывает универсум как композицию элементов и комбинацию элементов. Если комбинация является следствием внешних факторов и все элементы комбинируются, то получаем комбинаторную логику Черча и Карри. Это пример синтетического подхода. Из философов эту онтологию развивал Лейбниц и Л. Витгенштейн.

5. *Трансформационная онтология*. Синтетичность здесь достигается только как совокупность состояний или модификаций. Это онтология развивающаяся (например, в работах Спинозы). Из физиков такую онтологию развивал Эйнштейн. Его трактовка квантовой механики и ОТО оказалась весьма уязвимой с точки зрения некоторых физиков.

6. *Онтология ментальных конструкций*. Описывает ментальную активность непосредственного созерцания, не рассматривает «факты» внешнего мира (интуиционизм Брауэра). Похоже, многие современные физики-теоретики стоят на этих позициях (Хоукинг, Пенроуз, Виттен и др.).

Что касается формальной онтологии, то, по сложившейся традиции, термин «формальная онтология» имеет два различных значения.

Следуя аналитической традиции, формальная онтология является теорией бытия с точки зрения формальной логики, т. е. теория бытия в рамках и на языке элементарных формальных теорий.

Научная теория полагает некоторые объекты существующими. Универсум таких объектов составляет онтологию этой теории – обычно в этой связи говорят об онтологических допущениях языка теории. Например, широко известный критерий У. Куайна «Быть – значит быть значением связанной переменной» определяет онтологию узкого исчисления предикатов с помощью операции квантификации.

Но следует учесть, что само по себе экзистенциальное прочтение квантора существования не фиксирует какой-либо определенный модус существования. Здесь мы сталкиваемся с тем обстоятельством, что в соответствии с критерием Куайна нам придется считать возможные миры частью онтологии. Если бы мы попытались говорить лишь об онтологии относительно каждого возможного мира, то мы ничего не смогли бы сказать об *онтологии совокупности всех возможных миров*.

Пытаясь преодолеть эти трудности, У. Куайн выдвигает в качестве противовеса понятию «онтология» понятие «идеология», или «концептуальное содержание». Под *концептуальным содержанием теории* понимается определенная часть концептуальной системы, используемой для познания реального мира, та часть, которую мы обязаны принять в предположении истинности теории.

Необходимость использования такого термина как *концептуальное содержание* становится понятной, когда мы имеем дело с проблемой сравнения теорий.

Точно так же возникает вопрос о смысле эквивалентности индивидов предметных областей в случае эквивалентности теорий с

разными предметными областями. По-видимому, **концептуальное содержание** характеризует выразимость свойств и отношений индивидов из принимаемой онтологии, и поэтому не является частью онтологии. Важно, что концептуальное содержание позволяет отдельно сравнивать между собой возможные миры (в космологии это сравнение различных вариантов метавселенных) и миры, в отношении которых возможны или планируются астрофизические наблюдения. Важно отметить, что только мир, в отношении которого поставлены эксперименты или наблюдения, с точки зрения естествознания можно трактовать как реальный мир.

Заметим, что сам термин «концептуальное содержание» указывает на определенную субъективность, поскольку мы не всегда имеем семантические средства для выделения объектов реального мира из совокупности объектов возможных миров.

Именно здесь в поддержку семантическим средствам можно предложить средства когнитивной машинной графики для объектизации и визуализации объектов реального мира из совокупности объектов возможных миров.

Заметим, что в стандартной семантике какой-либо определенный модус существования вообще не фиксируется. Как справедливо указывают Васюков и Бессонов, истолкование квантора существования «...как выражающего именно реальное, материальное существование является ошибкой (причем весьма распространенной)». Один из создателей логической семантики А. Тарский утверждал, что онтология как общая теория предметов «вряд ли как-либо связана с семантикой». Это неудивительно, если вспомнить, что семантика имеет дело с отношением наших утверждений к действительности, а онтология есть теория представления этой действительности. Поэтому в семантической теории Тарского не предполагается, что в качестве объектов предметной области в логической семантике должны рассматриваться обязательно реально существующие предметы. Для теоретической физики такая позиция начинает доминировать в работах Хоукинга, Пенроуза, Виттена. Данная позиция имеет право на существование при условии ее правильного толкования. Здесь можно и нужно различать реально существующий мир и возможные миры, как их можно трактовать с точки зрения теоретической физики и математики. Разумеется, возможна и точка зрения Фреге об объективном существовании математиче-

ских объектов, но и она находит свое место в перечисленных выше онтологических типах.

На возникающий при этом вопрос, какие же предметы определяют логические понятия, Тарский отвечает следующим образом: «те и только те логические понятия являются логическими, которые определяют объекты, инвариантные относительно любого взаимно-однозначного отображения «мира» (или «универсума рассуждения», или «класса всех индивидов») на себя». Таким образом, ответ Тарского носит чисто формальный характер; его не интересует природа логических сущностей, являются ли они физическими, ментальными, принадлежат ли они к платоновскому миру идей, Фрегевским «мыслям» и т. п. Ответ подразумевает онтологию, носящую также чисто формальный характер.

По мнению этих авторов, Тарский не проводит четкого разграничения между логическими понятиями и логическими сущностями.

Если рассматривается лишь одна предметная область, то логические понятия и логические сущности жестко связаны, поскольку для каждого логического понятия существует единственная логическая сущность, подпадающая под это понятие. Если же допускаются возможные изменения предметной области, то для каждого логического понятия будут существовать различные логические сущности, подпадающие под данное понятие (т. е. изменяется объем понятия). И эти логические сущности подлежат просмотру и систематизации для ЛПР в области естественных наук. Отметим, что чисто комбинаторная интерпретация онтологии присуща «Логико-философскому трактату» Л. Витгенштейна. Он сводит все модальности к чисто логическим модальностям.

Конечно, для традиционно мыслящих естествоиспытателей это кажется ненужной «морокой». Но без такого подхода можно увязнуть в деталях эксперимента или воспарить на крыльях фантазии, полностью оторванной от эксперимента. Конечно, можно «спрятать голову в песок», но от этого проблемы и парадоксы сами собой не решатся и дискуссии будут носить бесплодный характер. Другой исход – это «махнуть рукой» на фундаментальные проблемы и «посыпать голову пеплом», но это отказ от познаваемости мира и конец науки как таковой. Чтобы избежать этих крайностей и научиться коллективно управлять научной интуицией, целесообразно для естествоиспытателей воспользоваться типизацией онтологий.

Анализ понятия «онтология» позволил философам и логикам уточнить термин **формальная онтология**. *Формальная онтология трактуется как теория, в которой исследуются формальные структуры объектов и структуры возможных отношений между ними.* Формальная онтология формулируется не как аксиоматическая система, а как структура, в которой даются лишь интуитивные основания для ее разработки.

Еще один принципиально иной вид формальной онтологии мы находим в работах Э. Гуссерля. В этом случае *формальная онтология рассматривается как теория части и целого и их взаимоотношений*.

При этом следует подчеркнуть, что Гуссерль в своих работах не использует какой-либо формальный аппарат в современном понимании смысла этого слова. Его исследования представляют собой скорее анализ с целью выяснения интуитивных оснований и понятий для разработки систем формальной онтологии. Несмотря на их различие, обе разновидности формальной онтологии по большинству вопросов занимают сходные позиции.

Стандартная семантика обычной логики предикатов задается с помощью понятия модели, представляющей собой некоторое множество с заданной на нем системой отношений и функций.

Ученик Гуссерля Лесневский предложил свой вариант формальной онтологии, который позволил установить «мостик» между понятиями Гуссерля и определениями формальной онтологии в более рациональном ключе.

Таким образом, онтологию Лесневского можно рассматривать как некий вид систем формальной онтологии, в которой характеристика онтологических понятий предполагает не теоретико-множественные термины, но лишь термины исчисления имен. Преимущество такой точки зрения оказывается при расширении диапазона понятий онтологических объектов и отношений между ними.

Примером служит *проблема представления* и его объекта. С точки зрения традиционной проблемы чужого сознания материальный предмет, являясь объектом представления многих сознаний, обладает новым измерением своей собственной сущности. Если бы оно было просто эпистемологическим по природе, такое измерение могло бы быть истолковано в рамках гуссерлевских рассмотрений части и целого.

Когда интенциональная активность нашего сознания направлена на некоторый предмет, то лишь часть его значения может быть воспринята в акте представления и, следовательно, мы получаем лишь возможный образ подлинного предмета. В свою очередь во всех актах представлений одного и того же предмета его основной образ (как некий вид фона, как его, говоря топологическим языком, «внутренность») всегда присутствует в сознании. Будучи зависимым от акта представления, образ подлинного предмета представляет собой как бы некоторое усреднение всех возможных образов, их пересечение (непустота подобного пересечения является условием его идентификации). Отсюда его появление всегда необходимо и, так или иначе, всегда независимо от нашей воли. Следует особо отметить возможность человеческого сознания мыслить зрительными образами. Поэтому кажется естественным появление средств для визуализации таких образов (по крайней мере в рамках компьютерной метафоры).

Согласно взглядам Васюкова, для модальной интерпретации не трудно адаптировать семантику возможных миров модальной логики. Достаточно говорить об интенциональном состоянии (состоянии направленности на предметы) сознания вместо возможного мира. Это позволяет передать смысл понятия «возможного» или «необходимого» предмета как объекта представления, чье восприятие связано с интуитивным убеждением (или знанием) о его восприятии в некоторой или во всех ситуациях (интенциональных состояниях).

Итак, если принять определение формальной онтологии, то в соответствии с вышеупомянутым рассмотрением «феноменологический способ существования» мог бы быть подходящим для специальной формальной онтологии. Здесь компьютер выступает (разумеется, после диалога с ЛПР) и как генератор образов формальных онтологий, и как генератор определенных языковых структур, отражающих эти онтологии.

Возникающий здесь вопрос связан с взаимоотношениями структуры языка и онтологических допущений. Известно, что структура языка и мышления связана с допущениями о познающем. Это справедливо не только для естественных языков, но также и для искусственных, в частности, для языков логики, несмотря на то, что они более просты, что их структура более прозрачна, и, принимая их, мы заведомо абстрагируемся от ряда моментов.

Согласно мнению В. А. Смирнова, онтологические проблемы, несомненно, являются правомерными. Однако решаются они не в рамках натурфилософии и не методами, подобными естественнонаучным, а путем анализа познавательных процедур и категориальной структуры мышления. И далее: «Мы исходим из допущения, что принимаемый язык, используемые познавательные процедуры небезразличны к познаваемому; принятие того или иного языка, той или иной логики вынуждает нас сделать определенные допущения о познаваемых объектах. Одна из задач философии и состоит в том, чтобы установить связь между принимаемыми средствами выражения и рассуждения, с одной стороны, и допущениями об объектах рассуждения – с другой. И не только описать, но и четко сформулировать и обосновать. Конструирование искусственных языков и выяснение содержащихся в них онтологических допущений является хорошим средством изучения проблем онтологии». К этому можно добавить, что генерация когнитивных образов также может послужить дополнительным инструментом для изучения и формирования онтологий.

Васюков предлагает использовать термин «формальная феноменология» как имя систем, являющихся расширениями онтологии Лесневского. Это название с самого начала побуждает действовать в направлении создания компьютерных метафор с учетом вклада феноменологических идей в проводимые исследования.

Само по себе конструирование искусственных языков с эпистемологическими допущениями не является новостью для современной логики. В современных системах неклассических логик в явном виде фигурируют не только чисто онтологические допущения, но и понятия познающего субъекта, систем знания, систем норм, ценностей и оценок. Подобного рода эпистемологические допущения помогают преодолевать трудности, возникающие не только при анализе экспериментальных данных в наблюдательной космологии, но и при конструировании языков программирования, и при решении проблемы искусственного интеллекта. На пути преодоления этих трудностей родились такие дисциплины, как компьютерная феноменология, компьютерная герменевтика и компьютерная когнитивная графика. Как показано выше, развитие этих компьютерных дисциплин и наблюдательной космологии требует достаточно подробных компьютерных метафор, отражающих фундаментальные онтологии.

2. Идея компьютерных метафор для феноменологических конструкций онтологических систем Ф. Брентано, М. Хайдегера и Ж. П. Сартра.

Брентано, принимая метафизику Аристотеля, видел источник знания в непосредственном осознании наших собственных ментальных феноменов. Кроме того, он предполагал существование внешнего мира. Согласно классификации Поли, его дискриптивная психология, по сути, является онтологией ментальных структур. Если отметить его представление о существовании реального мира, то можно смело взять его онтологию для формирования компьютерных метафор при анализе экспериментальных данных в pragma-тических науках.

Используя феноменологический метод редукции, Хайдеггер вводит свою известную категорию «бытие-в-мире». Интенциональный метод предполагает не только редукцию, но и конституцию. Сознание не просто имеет в виду предмет, но придает ему смысл в зависимости от всего предшествующего ему опыта. Так, когда, скажем, ребенок, смотрит на ромашку, он еще не знает названия цветка, хотя уже отличает цветы от других растений. Ученый же назовет вам разновидность, семейство, возраст ромашки и т. д. Для ученого объект будет наделяться более богатым смыслом.

Этот тезис показывает необходимость существования в компьютерной метафоре для хайдеггеровской онтологии рекурсивных процедур и структур байесовского вывода.

В интенциональном анализе становится очевидной активность нашего сознания, придающая смыслы вещам в зависимости от опыта, а также от целевой и эмоционально-волевой установок субъекта, который конституирует предметы различными актами сознания как прекрасные или безобразные, истинные или ложные, реально существующие или воображаемые.

Этот тезис показывает необходимость существования в компьютерной метафоре для хайдеггеровской онтологии средств отображения исходной картины данных в эстетически оформленные образы [17; 25–27].

В методе редукции и конституции в действительности мы видим два взаимосвязанных процесса. Сартр использует феноменологический метод для построения своего онтологического учения, изменяя в соответствии со своим замыслом и значением ряд терми-

нов гуссерлевской философии. Гуссерль, по существу, стремится углубить трансцендентализм философии Канта. Для него главной задачей было дать описание структур чистого трансцендентального сознания. В его работах феноменологическая редукция не распространяется на это Я, которое в виде «Я мыслю» сопровождает все наши представления.

Сартр радикализирует феноменологическую редукцию и распространяет ее на любые предметности, в том числе и на это чистое Я.

Этот тезис показывает необходимость существования в компьютерной метафоре для сартровской онтологии средств отображения исходной картины данных в эмоциональный настрой лица, наблюдающего когнитивные образы.

Для Гуссерля единство сознания определяется этим «Я мыслю», сопровождающим всю нашу сознательную деятельность. Здесь определяется единство наук и мира. Единство сознания определяется его интенциональностью, направленностью на объект, трансцендентный сознанию. Источник единства находится именно в объекте.

Этот тезис, как отмечалось ранее, обеспечивается как эйдетическим, так и интенциональным характером когнитивного образа в компьютерной метафоре.

Для Сартра трансцендентальное сознание существует без субъекта, оно есть чистая безличностная активность. Сартр пишет: «Мы можем сформулировать наш тезис: трансцендентальное сознание есть безличностная активность, она определяется к существованию в каждый момент, без чего нельзя понять ничего перед ней. Итак, в каждый момент нашей сознательной жизни мы открываем творение ex nihilo [из ничего]. Но новое расположение и новое существование. Это не есть творение мира и его вещей».

Стержневой идеей Сартра является констатация антагонизма между сознанием и бытием, субъектом и объектом, свободой и необходимостью, свободой и отчуждением, а также стремление найти их синтез и примирение. Современные программные продукты типа интеллектуальных интерфейсов и интеллектуальных агентов составляют техническую основу для такого примирения. Таким методом Сартр создает свою версию феноменологической онтологии.

Источники Сартровской онтологии, кроме Гуссерля, мы находим у Декарта, Гегеля и Хайдеггера. Дуализм субстанций Декарта обнаруживается у Сартра в дуализме двух сфер бытия: **бытия-в-себе и бытия-для-себя (сознания)**. Сартр отрицает какие-либо качественные и количественные характеристики бытия-в-себе. Оно просто есть. Оно непрозрачно, неделимо, бесконечно плотно и не-проницаемо. Похожую характеристику бытия мы находим в элейской школе философии Древней Греции. В соответствии с феноменологической теорией раскрытия бытия посредством интуиции, принимающей у Шелера ценностный, эмоционально-моральный характер, Сартр утверждает, что бытие будет открываться нам через эмоции.

Однако в самом понятии бытия-в-себе, которое мы находим у Канта, где оно означало и его материалистическую посылку, и невозможность познания вещи, какой она существует сама по себе, есть проблема. Мы убеждены, что познаем вещи реального мира более или менее такими, какими они существуют сами по себе. Но о вещах вне всякой познавательной деятельности можно сказать лишь то, что они есть. Нет никакого противоречия, если мы вообразим себе мыслящих существ самого различного психофизиологического типа, пространственных размеров и временной длительности своего бытия. За исключением того, что все они должны следовать в жизни и познании законам логики, без которых невозможна разумная жизнь, качественные особенности познаваемых вещей окажутся у разных типов разные. Каждый будет правильно познавать те стороны реальности, которые соответствуют условиям его бытия. Мир же, каким он существует сам по себе, может познать только предельная, гипотетическая сущность.

Если бытие-в-себе не нуждается в чем-либо для своего существования, то бытие-для-себя, сознание, появляется только на основе бытия-в-себе и не представляет собой самостоятельной субстанции. Сартр отрицает за бытием сознания обладание каким-либо внутренним содержанием. Это чистое ничто, функция которого отрицание, «ничтожение» всего того, что не есть оно. Здесь феноменологическая онтология не является онтологией в традиционном смысле слова, т. е. учением о фундаментальных структурах мира. Она не является онтологией и в хайдеггеровском понимании как раскрытие смысла бытия вообще через бытие человека. Категорию

Хайдеггера «бытие-в-мире» Сартр переводит в понятие «человеческая реальность», упрекая Хайдеггера в том, что у него о сознании ничего не говорится. Сартр разрабатывает онтологию сознания. Сознание реально, оно существует на поверхности бытия в себе. «Сознание (в его бытийном слое) это средство не только овладения, но в известном смысле преодоления конкретных пространственно-временных форм и определений реальности, средство “обмена” времени действия на пространство образа и пространства образа на время действия. Такая обратимость дает возможность подняться над ситуацией. Рефлексивный слой сознания – это отношение к действительности». Эту сложную структуру сознания как раз и старается проанализировать французский философ.

Анализ поведения сложных систем и данных, которые они порождают, требует учета возможностей человеческого сознания. Учет этих возможностей может осуществляться с помощью интеллектуальных интерфейсов, снабженных когнитивными технологиями. Сартр утверждает, что эмоции, например, не пассивные состояния, а наделены значением; они несут в себе цель, проект. Это особенно важно в pragматических науках. Посредством эмоций сознание стремится достичь цели «магически», избегая реальности. Как и все психические состояния, они порождаются нечистой рефлексией и поэтому пребывают в самообмане, они неискренни. Такое отношение к действительности устраняется посредством очищающей рефлексии. Сартр выступает против теорий, делающих человека рабом эмоций и освобождающих его от ответственности. Это достигается за счет проектного мышления, принятого в инженерных, естественных и pragматических науках. Современные программные средства интеллектуальных интерфейсов позволяют гармонично сочетать проектное мышление и человеческую интуицию.

Сознание как свобода имеет функцию постоянного бегства от предметностей, от данностей сознания. Это свобода от чего-то, которая более всего подчеркивается Сартром. Но одновременно свобода является свободой для чего-то. Именно здесь «место» современных IT-технологий.

На языке Сартра эта мысль выражается в терминах «бытие-в-себе» и в термине «сознание». Если бытие-в-себе плотно, непроницаемо, заполнено и его всегда предстаточно, «слишком» (de trop), то сознание прозрачно, пусто; оно представляет собой недостаток,

выражаемый в желаниях, целях и проектах, которые должны быть выполнены, «заполнены».

Позитивной функцией сознания является конституирование мира со всеми его вещами, отношениями и свойствами. Бытие-в-себе не имеет никаких качеств. Время, пространство, качество и количество, отношение, необходимость, возможность и т. д. – все это конституируется ничтожением (неантанизацией) бытия-в-себе.

Рассмотрим теперь описание сознания. В нем подчеркивается существенно проективный, целеполагающий характер сознания, его противоречивая природа. Человек всегда проектирует себя в будущее таким, каким он еще не стал. Сознание не является тем, что оно есть, так как оно уже позади себя как «превзойденное», «отсталое». Прошлое – есть необходимая структура сознания, но его уже нет, оно застыло в себе. Сознание постоянно проектирует воплощение себя. Это неизменное колебание между прошлым и будущим через настоящее, действительно, образует диалектическое противоречие человеческого духа. Отсюда и такая структура сознания, как быть в самообмане, в колебании между заблуждением и истиной, отчуждением и свободой, идеалом, трансцендентностью и фактичностью, «низменным» бытием.

Этот тезис показывает необходимость существования в компьютерной метафоре для сартровской онтологии средств отображения исходной картины данных во временную последовательность когнитивных образов, реализованных как последовательность «проектов», которые доступны всем пользователям.

Подводя итоги рассмотрения всего набора компьютерных метафор, описывающих различные варианты феноменологических онтологий, хорошо видно, что компьютерные метафоры обеспечивают неограниченные возможности для лиц, принимающих решения, учесть все формы предпочтений в процессе принятия решений. Актуальность такого учета кажется очевидной в таких областях естественных наук, как космология и физика высоких энергий.

Данный подход еще раз иллюстрирует возможности феноменологии для успешной интеграции гуманитарных и точных знаний в процессе принятия решений в условиях глубокой априорной неопределенности.

Заключение. Таким образом, на основе проведенного анализа возможностей работы с когнитивными образами, которые открываются при использовании компьютерных метафор (конструируемых на основе феноменологических онтологий Брентано, Гуссерля, Хайдеггера и Сартра), можно сделать вывод о необходимости и перспективности разработок методик и интеллектуальных интерфейсов для манипуляции с когнитивными образами, порождаемыми системами когнитивной машинной графики. Такой подход послужит мощным стимулом для развития современных человеко-машинных систем, поддержки принятия решений в современном естествознании.

Литература

1. *Lemm J. C.* Bayesian field theory // The Johns Hopkins University Press 2715 North Charles Street Baltimore, Maryland 21218-4363 ISBN 0-8018-7220-0.
2. *Lemm J. C.* Inverse time-dependent quantum mechanics // Physics Letters A, 276(1-4): 19-24, 2000.
3. *Горохов В. Л., Барышев Ю. В., Гозина Я. Л.* Модифицированный алгоритм обнаружения репрезентативности данных гравитационных наблюдений: Тр. Междунар. конф. по мягким вычислениям. 17–19 июня 2004 г., (SCM – 2004), СПб., 2004.
4. *Agostini G.* Bayesian reasoning in physics // CERN 99-03. July 1999.
5. *Трухаев Р. И.* Модели принятия решений в условиях неопределенности. М.: Наука, 1981.
6. *Горохов В. Л., Муравьев И. А.* Выявление компьютерных метафор интенциональных и эйдетических объектов в когнитивных образах // Вестник ИНЖЭКОНа. 2006. Вып. 3 (12). С. 74–85. Сер. «Технические науки».
7. *Гусева Е. А., Леонов В. Е.* Проблема реализуемости высших психических функций в системах машинного интеллекта. Вестник ИНЖЭКОНа. Вып. 3 (12). 2006. С. 85–89. Сер. «Технические науки».
8. *Горохов В. Л., Витковский В. В., Иванов Л. Н.* Робастно-когнитивная технология динамической визуализации многомерных наблюдательных данных / Препринт САО РАН N 93, Ниж. Архыз, 1992.
9. *Allen R. B.* Cognitive Factors in Human Interaction with computers behavior and Information Technology. 1989. Vol. 1. № 3. P. 257–278.
10. *Gorohov V. L., Vitkovskij V. V., Ivanov L. N.* Cognitive informational technology of planning and control of ecological monitoring with further robust analysis of extreme manifestations // Proceedings First Eurasian symposium on space science and technologies Gebze, Turkey, Oct. 25–27, 1993.
11. *Горохов В. Л., Иванов Л. Н.* Пакет программ квантильной визуализации и классификации многомерных данных и его развитие для задач обработки сигналов // Актуальные проблемы развития радиотехники электроники и связи: Мат. 45-й науч.-техн. конф. 16–18 апреля 1990. Л., 1990.
12. *Bija D., Cook D., F. Swayne Interactive High-Dimensional Data Visualization // Journal of Computational and Graphical Statistics 1996. № 5(1). P. 78–99.*
13. *Koschat M., Swayne D. F.* Interactive Graphical Methods in the Analysis of Customer Panel Data, Journal of Business and Economics Statistics. 1996. № 14(1). P. 113–132.
14. *Symanzik J., Majore B., Cook D. and Cressie N.* Dynamic graphics in a GIS: a link between ARC/INFO and XGobi, Computing Science and Statistics: Proc. of the 26th Symp. on the Interface. 1994. C. 431–535.
15. *Geladi P., Esbensen K.* Regression on multivariate images: principal component regression for modeling, prediction and visual diagnostic tools // Journal of Chemometrics. 1991. Vol. 5. P. 97–111.
16. *Кулинич А. А.* Когнитивная система поддержки принятия решений «Канва» // Программные продукты и системы. 2002.
17. *Горохов В. Л., Муравьев И. А.* Компьютерные метафоры для интенциональных и эйдетических объектов в когнитивных системах: Тр. Междунар. конф. по мягким вычислениям. 17–19 июня 2006 г. (SCM–2006), СПб., 2006.
18. *Горохов В. Л., Террикорти П., Барышев Ю. В., Витковский В. В.* Синтез новых когнитивных метафор для интерактивного анализа многомерных данных мониторинга космических систем ближнего и дальнего космоса // Современные проблемы прикладной информатики: Сб. науч. тр. Междунар. науч.-практ. конф. 23–25 мая 2007 г. СПб.: СПбГТУ. 2007. С. 90–93.
19. *Горохов В. Л., Лукьянец А. А., Ротарь В. Г., Чернов А. Г.* Методы когнитивной визуализации многомерных данных для поддержки принятия решений: Тр. Междунар. конф. по мягким вычислениям. 25–27 июня 2007 г. (SCM – 2007). СПб., 2007.
20. *Горохов В. Л., Террикорти П., Барышев Ю. В., Муравьев И. П.* Компьютерные метафоры феноменологических конструкций Ф. Брентано, М. Хайдеггера, Ж. П. Сартра для систем обработки астрофизических наблюдений: Тр. Междунар. конф. по мягким вычислениям. 25–27 июня 2007, (SCM – 2007). СПб., 2007.
21. *Горохов В. Л.* Байесовский подход: последние достижения и будущее систем интеллектуальной поддержки принятия решений: Тр. Междунар. конф. по мягким вычислениям. 25–27 июня 2007 г. (SCM–2007). СПб., 2007.
22. *Горохов В. Л., Муравьев И. П.* Когнитивная машинная графика. Методы динамических проекций и робастная сегментация многомерных данных. Методология, методики и интерфейсы: Монография. СПб.: СПбГИЭУ. 2007.

23. Горохов В. Л., Лукьянец А. А., Чернов А. Г. Современные методы когнитивной визуализации многомерных данных: Монография. Томск.: Некоммерческий фонд развития региональной энергетики. 2007.
24. Vitkovskiy V. V., Gorochov V. L. New method of data mining in practical cosmology // Problems of Practical Cosmology. Proceedings International conference. SPb., 2008. P. 256–259: [Электронный ресурс]: ppc08.astro.spbu.ru/fin_program.html
25. Gorokhov V. L., Evdokimov V. A., Vitkovskiy V. V. Cognitive multidimensional data visualization in analyzing and decision _support systems // III Междунар. конф. по когнитивной науке: Тез. докл. Т. I. 20–25 июня 2008 г., М., 2008. С. 55. (The Third international conference on cognitive science. June 20–25, 2008. Moscow. Russia abstracts volume 1) М., 2008. P. 55.
26. Komarinskiy S., Vitkovskiy V., Gorohov V., Zakharevski D. The Cognitive Visualization System Astronomical Data Analysis Software and Systems (ADASS) XVII / Editors: Argyle, Robert W.; Bunclark, Peter S.; Lewis, James R. London, UK 2008.

УДК 378.001.658.011.56

К. П. Голосков, А. А. Кусов

Санкт-Петербургский государственный
инженерно-экономический университет

ИНФОРМАЦИОННАЯ БАЗА ПРОГНОЗИРОВАНИЯ КАЧЕСТВА ПРОДУКЦИИ

Большинство стран прилагают огромные усилия, чтобы повысить качество своих товаров и тем самым отстоять свой престиж и положение на мировом рынке в ожесточенной борьбе против конкурентов. Промышленные фирмы различных стран перенимают японский опыт организации производства и управления качеством.

При этом все большее значение приобретает социальный аспект качества, когда качество рассматривается в широком смысле – качество жизни, жизнедеятельности. Под этим понимается совокупность объектов качества: окружающая среда, охрана здоровья, образование и развитие личности, товары и услуги, коммуникации и др.

Особенно остро проблема качества стоит и требует своего решения в нашей стране. Эта проблема для нас застарелая, она возникла еще в условиях директивной экономики, когда все работы по

обеспечению и улучшению качества продукции планировались и контролировались сверху. Однако при этом слабо учитывались требования потребителей и качество продукции оценивалось по ее соответствуанию требованиям нормативных документов, которые чаще всего отставали от запросов потребителей. При монопольном положении и отсутствии мощного рыночного стимула качественного роста – конкуренции – производители не были заинтересованы в повышении качества продукции, в расходовании дополнительных финансовых ресурсов на эти цели. Положение с качеством продукции затем усугубилось нарастанием товарного дефицита, когда спрос все больше превышал предложение, и лишенный выбора потребитель был готов купить товар любого качества и по диктуемой цене (правда, цены были доступными).

Так как наши производители практически не выходили на внешний рынок (за небольшим исключением), то отсутствовала и внешняя конкуренция и не было необходимости сопоставлять качество наших товаров с качеством товаров других стран.

Сейчас же, когда рынок насыщен импортными товарами, проблема качества встала перед нашими товаропроизводителями в полный рост. Без ее решения наша продукция не будет иметь сбыта ни внутри страны, ни на мировом рынке.

Производственные системы – сложные объекты, включающие большое число разнородных элементов, работающих на основе разных принципов, с большим числом параметров, определяющих их техническое состояние. В качестве прогнозируемых выбирают независимые параметры, отображающие техническое состояние.

Все процессы, происходящие в каждом объекте прогнозирования, носят случайный характер вследствие флуктуаций выходных параметров, имеющих место в отдельных элементах; взаимно компенсирующего изменения большого числа внутренних параметров объекта из-за явлений старения, изнашивания, разрегулировок. Измерение прогнозируемых параметров производится обычно в условиях различных случайных помех, погрешностей, сбоев.

Таким образом, процессы изменения прогнозируемых параметров могут рассматриваться как нестационарные, случайные, с априорно неизвестными статистическими свойствами (законами

распределения, корреляционными свойствами и т. д.) и структурными характеристиками, определяемыми наличием или отсутствием обратимых или необратимых изменений, скачков, выбросов, случайных шумов собственно объектов прогнозирования, случайных шумов измерения параметров и т. д.

Такой характер поведения признаков приводит к пересечению классов технического состояния систем, что является причиной ошибок при прогнозировании. С целью сокращения числа ошибочных решений разработан метод построения разделяющей классы состояний гиперповерхности, наиболее эффективный для указанного класса задач.

Распознавание представляет собой информационный процесс, реализуемый некоторым преобразователем информации (интеллектуальным информационным каналом, системой распознавания), имеющим вход и выход. На вход системы подается информация о том, какими признаками обладают предъявляемые объекты. На выходе системы отображается информация о том, к каким классам (обобщенным образом) отнесены распознаваемые объекты.

Обучающая выборка представляет собой базу данных, содержащую описания конкретных реализаций объектов на языке признаков, дополненную информацией о принадлежности этих объектов к определенным классам распознавания.

После распознавания может быть установлена адекватность. Для объектов обучающей выборки это может быть сделано сразу, так как для них просто известно, к каким классам они относятся. Для других объектов эта информация может быть получена позже. В любом случае может быть определена фактическая средняя вероятность ошибки по всем классам распознавания, а также вероятность ошибки при отнесении распознаваемого объекта к определенному классу.

Результаты распознавания должны интерпретироваться с учетом имеющейся информации о качестве распознавания.

При этом не требуется никаких предположений о конфигурации собственных областей работоспособности (R_1 и R_2) и о характере расположения точек внутри них.

Выбор признаков (измерений), свойств, на которых основывается решение задачи прогнозирования и диагностирования техни-

ческого состояния систем, является одним из наиболее важных вопросов.

Уменьшение количества признаков снижает затраты на производство измерений и вычислений, но может привести к падению достоверности и точности прогнозирования. Но если время на обучение и принятие решения жестко ограничено, повышение размерности признакового пространства может оказаться единственным средством увеличения достоверности требуемого уровня.

Очевидно, что с практической точки зрения требования минимума общей размерности задачи распознавания и максимума достоверности оказываются противоречивыми. Уже из этого очевидно, что формирование признакового пространства является одной из важнейших задач.

Первоначальный выбор признаков формируется до начала распознавания из числа доступных измерению характеристик объекта $y_1, y_2, y_3, \dots, y_p$, отражающих его наиболее существенные для оценки технического состояния свойства. На следующем этапе из первоначального набора пытаются сформировать новый набор $x_1, x_2, x_3, \dots, x_k$, состоящий из меньшего числа переменных $k < p$.

Традиционный способ формирования новых признаков в условиях полного априорного знания основан на максимизации некоторой функции $g(y_1, y_2, \dots, y_p)$, называемой критерием, и обычно понимаемой как некоторое «расстояние» между классами в признаковом пространстве с координатами $y_1, y_2, y_3, \dots, y_p$. В других случаях критерий $g(y_p)$ выражает «диаметр», или «объем», области, занимаемой классом в признаковом пространстве. И новые признаки формируются путем минимизации критерия [2]. Оба эти варианта критериев по своей сути равнозначны.

Конкретно в качестве критерия $g(y_p)$ выбирают среднеквадратическую ошибку аппроксимации признаков $y_1, y_2, y_3, \dots, y_p$ с помощью новых признаков $x_1, x_2, x_3, \dots, x_k$, среднее межклассовое расстояние, внутриклассовый разброс наблюдений, энтропию одного класса относительно другого и т. д.

Традиционные критерии, основанные на геометрических понятиях расстояния между классами, исходят из того, что значения указанного расстояния пропорциональны достоверности распознавания.

Считают, что чем больше расстояние (различие) между классами, тем легче его обнаружить, и, следовательно, тем выше будет достоверность различия классов.

Максимизация расстояния между классами повышает «разделяющую силу признаков» [1], которая, как ожидается, обеспечит требуемую достоверность различия, особенно если само правило различия основано на том же самом критерии, что и выбор наиболее информативных параметров, как, например, в кластерном анализе [2].

Указанные критерии интуитивно убедительны, они могут быть обоснованы в определенной мере, когда достоверность можно связать со значением межклассового расстояния явной функциональной зависимостью.

Существует множество методов формирования признакового пространства, приспособленных не только к задачам различия, когда классы полностью заданы законами распределений вероятности признаков, и к задачам распознавания, в которых характеристики классов заранее не известны и получаются в процессе обучения [3].

Таким образом, различные критерии могут приводить к противоположным по смыслу рекомендациям по выбору признаков.

Причина этого заключается в отсутствии явной связи критериев, основанных на понятиях расстояний, с основными показателями качества распознавания, в частности, с главным из них – достоверностью.

Поэтому трудно бывает отдать предпочтение какому-то определенному критерию и сделать обоснованный выбор между противоречиями в рекомендациях. В этом, собственно, и заключается недостаток перечисленных методов выбора признакового пространства.

Задача оптимизации может быть сформулирована как задача определения наиболее простой для реализации группы признаков, обеспечивающей качество распознавания не хуже заданного, или же как задача максимизации показателя качества распознавания при ограничении на степень сложности реализации отыскиваемой группы признаков.

Поставим теперь задачу найти такое преобразование параметров изделий в информационные признаки, которое обеспечи-

вает наилучшее в определенном смысле разделение объектов обучающей выборки на классы работоспособности или долговечности.

Пусть r объектов x_i и $N-r$ объектов x_i обучающей выборки размером N принадлежат классам с запасом работоспособности R_1 и R_2 соответственно.

В качестве разделяющей гиперповерхности выберем поверхность вида

$$x_1 + x_2 + \dots + x_m - e = 0,$$

которая разделяет m -мерный гиперкуб с единичными ребрами.

Точное решение задачи распознавания с помощью гиперповерхности представляет собой решение задачи частично-целочисленного программирования.

$$\text{Максимизировать } \varphi = \sum_{i=1}^N \alpha_i,$$

при ограничениях

$$\begin{cases} -\sum_{k=1}^m x_{ik} + e + \Lambda \alpha_i \leq \Lambda - \lambda, & i = \overline{1, r} \\ \sum_{k=1}^m x_{ik} - e + \Lambda \alpha_i < \Lambda - \lambda, & i = \overline{r+1, N} \\ 0 \leq \alpha_i \leq 1. \end{cases}$$

Здесь, как и, прежде α_i – булевые переменные;

Λ, α – соответственно верхняя и нижняя границы для неравенств;

α_i – принимает значение 1, если x_i входит (попадает) в свой класс и 0 – в противном случае.

Сопоставим каждому k -му признаку булеву переменную μ_k . Положим $\mu_k = 1$, если x_k входит в описание объекта и $\mu_k = 0$ – в противном случае.

Потребуем минимизировать количество признаков описания объектов, обеспечивающих значение показателя качества не ниже заданного значения.

Тогда задача информативных параметров примет вид

$$W = \sum_{k=1}^m \mu_k \rightarrow \min$$

при ограничениях

$$\left\{ \begin{array}{l} - \sum_{k=1}^m x_{ik} \mu_k + e + \Lambda \alpha_i \leq \Lambda - \lambda, \quad i = \overline{1, r} \\ \sum_{k=1}^m x_{ik} \mu_k - e + \Lambda \alpha_i < \Lambda - \lambda, \quad i = \overline{r+1, N} \\ \sum_{i=1}^N \alpha_i \geq \phi_1 \\ 0 \leq \alpha_i \leq 1, \\ 0 \leq \mu_k \leq 1. \end{array} \right.$$

Очевидно, что поставленная задача поиска информативных параметров для прогнозирования технического состояния систем также является задачей частично-целочисленного линейного программирования с булевыми переменными, которая может быть решена с помощью тех же программных средств, что и задача отыскания разделяющей классы состояний гиперповерхности.

Выводы. Обеспечение качества начинается при формулировании технического задания на разработку. Уровень качества, планируемый техническим заданием, с одной стороны, должен быть достаточно высоким, чтобы удовлетворить требования потребителя, а с другой – должен соответствовать технологическому уровню совершенствующегося производства и быть экономически сбалансированным. Таким образом, при составлении технологического задания закладываются те технические и технологические параметры, которые будут определять качество изделия.

Управление качеством изделий на этапе производства является также важным звеном в единой системе управления качеством. Используя результаты анализа информации, полученные при контроле качества применяемых материалов, технологических процессов, оборудования и готовых изделий, можно управлять технологическими процессами, контролировать режимы и воздействовать на разработку или модернизацию изделий, выпускаемых в настоящее

время. Отсюда очевидна связь между системой управления качеством и системой управления технологическими процессами.

Литература

1. Голосков К. П. Прогнозирование технического состояния изделий электронной техники. СПб., ООО «ПаркКом», 2007.
2. Айвазян С. А., Бежаева З. И., Староверов О. В. Классификация многомерных наблюдений. М.: Статистика, 1974.
3. Гаскаров Д. В., Голосков К. П., Шкабардня А. В. Применение математического программирования в дискриминантном анализе для решения задачи прогнозирования // Автоматика и телемеханика. 1988. № 7. С. 174–181.

УДК 378.001.658.011.56

А. И. Дащевский, И. В. Янковский

Санкт-Петербургский государственный
инженерно-экономический университет

ПРАГМАТИЧЕСКАЯ ОЦЕНКА ПРИМЕНИМОСТИ МОДЕЛИ СММ В СОВЕРШЕНСТВОВАНИИ ОРГАНИЗАЦИОННЫХ ПРОЦЕССОВ

Для достижения устойчивых результатов в процессе развития технологии и организации управления жизненным циклом разработки программного обеспечения (ЖЦПО) часто рекомендуется методология обеспечения качества сложных программных средств СММ (Capability Maturity Model) – система и модель оценки зрелости комплекса применяемых в процессе разработки технологических процессов.

Главным понятием стандарта является зрелость организации. Незрелой считается организация, в которой процесс разработки программного обеспечения зависит только от конкретных исполнителей и менеджеров и решения зачастую просто импровизируются «на ходу». В этом случае велика вероятность превышения бюджета или заваливания сроков сдачи проекта, и потому менеджеры вынуждены заниматься только разрешением ближайших проблем.

© А. И. Дащевский, И. В. Янковский, 2009.

В то же время в зрелой организации имеются четко определенные процедуры создания программных продуктов и управления проектами. Эти процедуры по мере необходимости уточняются и совершенствуются в пилотных проектах или с помощью анализа «стоимость/прибыль». Оценки времени и стоимости выполнения работ основываются на накопленном опыте и достаточно точны. Наконец, в компании существуют стандарты на процессы разработки, тестирования и внедрения ПО, правила оформления конечного программного кода, компонент, интерфейсов и т. д. Все это составляет инфраструктуру и корпоративную культуру, поддерживающую процесс разработки программного обеспечения.

Таковы базовые посылки стандарта СММ. Можно сказать, что стандарт в целом состоит из критериев оценки зрелости организации и рецептов улучшения существующих процессов. В этом наблюдается принципиальное различие с моделью, принятой в ISO 9001, так как в ISO 9001 сформулированы только необходимые условия для достижения некоторого минимального уровня организованности процесса и не дается никаких рекомендаций по дальнейшему совершенствованию процессов.

Модель СММ основана на формализации и использовании пяти уровней зрелости технологий поддержки ЖЦПО, которые определяют потенциально возможное качество и безопасность промышленно создаваемых комплексов программ. Данные уровни зрелости характеризуются степенью формализации, адекватностью измерения и документирования процессов и продуктов ЖЦПО, широтой применения стандартов и инструментальных средств автоматизации работ, наличием и полнотой реализации функций системой обеспечения качества технологических процессов и их результатов.

Каждый уровень зрелости содержит от 0 до 7 Key Process Area (всего модель представляет 18 КРА); в свою очередь КРА имеет от 2 до 4 целей (всего 52 цели). Ключевые области процессов определяют наборы связанных работ, которые в случае их совместного выполнения позволяют достичь целей, рассматриваемых как важные для повышения устойчивости процесса разработки ПО. Каждая из КРА характеризует свой уровень зрелости.

Цели резюмируют основные действия КРА, они определяются СММ как наиболее важные моменты для повышения устойчивости

процессов до определенного уровня зрелости. Цели определяют объем, границы и назначение каждой КРА.

КРА представлены набором атрибутов:

- обязательства по выполнению (commitment to perform);
- способность к выполнению (ability to perform);
- измерения и анализ (measurement and analysis);
- проверка внедрения (verifying implementation).

Каждый атрибут содержит несколько ключевых практик, или Key Practices (всего 316 ключевых практик). Таким образом, каждая КРА описывается посредством ключевых практик, которые, будучи выполненными, помогают достичь целей этой КРА. Ключевые практики описывают инфраструктуру и работы, во многом способствующие эффективному внедрению и становлению данной КРА.

В приводимой ниже таблице представлены усредненные изменения показателей разработки программного обеспечения после внедрения модели СММ.

Эффективность инвестиций в СММ

Категория	СММ
Повышение уровня качества	4,55
Увеличение производительности	2,92
Сокращение времени жизненного цикла	2,99
Возврат инвестиций, вложенных в обеспечение и улучшение качества (ROI)	6,0:1

Несмотря на то, что СММ – набор положений, обобщающих хорошую практику разработки ПО и является стандартом де-факто в индустрии создания заказного, а также коробочного продукта в данной отрасли, модель является частной мифологией процесса эволюции производства ПО и не может претендовать на полное и всестороннее представление процесса разработки ПО.

СММ – это согласие среди отдельной группы теоретиков и практиков программирования, собравших коллекцию эффективных практик, которые сгруппированы в соответствии с простой моделью эволюции организации. Однако во многих случаях модель может сдерживать естественную динамику инженерии ПО, основан-

ную во многом на инициативном умственном труде исполнителей, производящих нематериальный продукт. Если организация следует СММ исключительно из-за зарубежных (правительственных – в случае американских фирм) контрактов, то это может легко привести ее к коллапсу (потере) потенциала конкурентоспособности компании. Именно по этой причине СММ малопопулярна среди высоко конкурентных инновационных компаний, производящих коммерческое (коробочное) ПО.

Далее перечислены не все, но самые крупные проблемы СММ с точки зрения компании (проекта), ориентированной на инновационные процессы разработки ПО или создание научноемких программных продуктов.

1. СММ не имеет формализованной теоретической базы. Она основана лишь на опыте «очень знающих специалистов». Однако наличие такой теории необходимо, несмотря на то, что создатели являются экспертами в области разработки ПО. Ведь иначе, в соответствии с таким принципом, любая модель, основанная на опыте других знающих людей, имеет такую же достоверность.

2. СММ имеет неясную эмпирическую поддержку. Модель основана на опыте крупных подрядчиков правительства и Министерства обороны США и собственном опыте создателей модели в мире мэйнфреймов. Она не учитывает успех коробочных компаний. Уровни 1, 4 и 5 не представлены с хорошей информативностью: первый – потому что он просто непрезентабелен, а другие два – так как существует мало организаций, действительно достигших этих уровней.

3. СММ чтит процесс, но игнорирует творческий потенциал людей. В СММ человеческий фактор представлен как ненадежный элемент и допускается, что определенные процессы могут чем-то помочь, чтобы сделать индивидуальное превосходство менее значимым. Идея, что процесс может помочь заурядности, является опорой СММ, т. е. люди второстепенны по отношению к процессам.

4. СММ почитает институализацию процессов ради них самих, так как СММ принципиально концентрируется на способности организации к изменению. Но способность организации к изменению является следствием выражения способности проектной команды действовать в этом направлении. Даже если необходимые процессы не утверждены формально, они могут быть очень хороши

на практике (неформально) благодаря умению членов коллектива. Другими словами, усилия по институализации ведут к раздвоению между сверхупрощенным формализованным (публичным) процессом и богатым частным процессом, который должен практиковаться неформально. Безусловно, институализация полезна, но параллельно с ней имеет смысл предложить систему для идентификации и поддержки, ключевых с точки зрения способности к инновации сотрудников организации, оставив ради них приоритет формализованных процессов на втором плане.

5. СММ содержит очень мало информации о динамиках процесса. Это делает непонятным соотношения между практиками и уровнями СММ, так как имеются скрытые допущения. Например, почему совсем нет тренинга на 1 уровне? Ведь данная практика особенно важна на этом уровне. В СММ ответ состоит в том, что на 1 уровне нет ничего (он просто определен, как не уровень 2). Скрытое допущение состоит в том, что не имеет значения, каков вектор цели развития компании, с какими проблемами сталкивается она при построении процессов и чего уже достигла на момент оценки по СММ. Просто идем по практикам по направлению к уровню 2. Иными словами, СММ не адаптируется к условиям клиентоориентированных организаций. Поэтому тренинги и иные неформальные практики уровня 1 в независимости от их эффективности могут быть случайно исключены слепым и статичным СММ. Можно сделать вывод, что большинство ключевых практик (а, может быть, и все) могут весьма пригодиться на уровне 1 в зависимости от необходимых конкретных изменений в конкретной организации. Вместо адекватного оценивания и последующего актуального моделирования динамик этих процессов СММ просто наслаждается ими.

6. СММ повторяет смешению целей с реальной миссии улучшения процессов на искусственную миссию достижения более высокого уровня зрелости. Можно называть это «уровнем зависти», и этот путь может сдержать организацию в отношении наиболее эффективного использования ее ресурсов.

Мир технологий процветает лучше всего тогда, когда процессы инновации достаточно обеспечиваются индивидуальностями разными, творческими и непокорными. Ярким примером в индустрии высоких технологий может послужить Silicon Valley.

Наиболее серьезным аргументом против СММ как эффективного предписания для процессов создания ПО является существование многих успешных компаний, которые по СММ вообще не должны существовать, быть конкурентоспособными и создавать качественное ПО. В СММ отсутствуют те разновидности процессов, которые поддерживают инновации для предприятий низших уровней зрелости. Нет упора на лидерстве в решении проблем для достижения инноваций. По существу, в СММ вообще нет инноваций, а появляются они только на уровне 5. Таким образом, многие инновационные фирмы в компьютерной индустрии работают на уровне 1 в соответствии с моделью (к примеру, Microsoft, Borland, Apple). В терминологии СММ нет разницы между этими фирмами и компаниями, рухнувшими на старте. Итак, СММ недостаточно ориентирована на инновационные процессы. Если сравнивать рекомендации известных новаторов, то:

- там, где новаторы советуют компаниям быть гибкими, СММ советует быть предсказуемыми;
- там, где новаторы предлагают снизить власть в организации, СММ выдвигает ее наверх;
- там, где новаторы предлагают постоянные конструктивные инновации, СММ относит их к хаосу на уровне 1;
- там, где новаторы исходят из необходимости следовать изучаемому опыту, СММ исходит из необходимости следовать букве правил;
- нигде раскол между этими двумя позициями не выглядит настолько очевидным, как в отношении к героизму. Авторы модели рассматривают героизм как необоснованную жертву со стороны некоторых индивидуумов, наделенных специальными талантами, как единственную причину достижения успеха компанией уровня 1, если она вообще успешна.

Итак, суть проблемы и главная причина, почему СММ опасна для любой компании (проекта), ориентированной на инновации, в том, что СММ относится подозрительно к персональным взносам, игнорируя условия, необходимые для выращивания нестандартных идей. Модель помещает их под ограничивающую структуру, продиктованную якобы промышленной необходимостью. А следствием является, что достижение уровня 2 по СММ-шкале может погасить ту инициативу, которая двигала компанию к успеху с самого начала в ее конкурентной борьбе.

Литература

1. Оценка и аттестация зрелости процессов создания и сопровождения программных средств и информационных систем (ISO/IEC TR 15504 – СММ): Пер. с англ. ЗАО «АйТи» М.: «Книга и Бизнес», 2001.
2. Анишина А. С. Страсти по качеству ПО // Открытые системы. 1998. № 6.
3. Paulk M. C. How ISO 9001 Compares With CMM // IEEE Software. 1995. January. P. 74–84.
4. Стандарты в проектах современных информационных систем: Сб. тр. IV Всероссийской практ. конф. М., 2004.

УДК 378.001.658.011.56

В. А. Евдокимов, Д. В. МинаевСанкт-Петербургский государственный
инженерно-экономический университет

ИНТЕГРАЛЬНАЯ ОЦЕНКА ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЙ НА ОСНОВЕ ИНТЕРАКТИВНОГО ВЫЯВЛЕНИЯ СУБЪЕКТИВНОГО МНЕНИЯ КОНЕЧНЫХ ПОТРЕБИТЕЛЕЙ

Отсутствие единого информационного пространства на рынке образовательных услуг затрудняет осознанный извешенный выбор конечного потребителя. Наличие огромного числа параметров образовательных учреждений, влияющих на удобство процесса обучения и, возможно, на будущую судьбу абитуриента (основного потребителя образовательных услуг рынка профессионального образования), выливается в огромные временные затраты, необходимые для анализа предложений и выбора. Предлагается алгоритм расчета интегральной оценки предложений, учитывающей не только объективные параметры качества, но и атрибуты потребительского восприятия.

Введение. Отсутствие единого информационного пространства рынка образовательных услуг затрудняет не только ориентацию населения в достоинствах и недостатках предлагаемых услуг профессионального образования, но также не позволяет эффективно

решать задачи мониторинга системы высшего образования в целом, выявления тенденций в развитии региональной системы образования (здесь и далее мы имеем в виду систему высшего профессионального образования), координации процессов формирования конкурентной образовательной среды органами муниципального, регионального и федерального управления.

Создание механизма интегральной оценки образовательных услуг, учитывающей потребительское восприятие, позволит, с одной стороны, легче ориентироваться потребителям, а с другой стороны, позволит выявить направления стратегического развития на уровне отдельных учебных заведений.

Существующие оценочные системы, в основном, используют объективную парадигму оценки, тем самым отражая обобщенное мнение группы экспертов о значимости тех или иных параметров образовательных услуг и их влиянии на общую оценку и принимая общую, не учитывающую отношение различных слоев потребителей услуг, информационную модель учреждения профессионального образования.

Необходимо разработать механизм, способный оперативно отражать объективную информацию и мнение потребителей о предложениях рынка образовательных услуг профессионального образования (РУПО), выраженные в общей интегральной оценке.

Этот подход будет реализован в открытой системе построения динамических рейтингов учреждений профессионального образования.

Цели и задачи проекта. Отмеченная выше особенность (а по сути – недостаток) существующих оценочных механизмов обуславливает постановку задачи построения такого способа интегральной оценки, который учитывал бы многокритериальное мнение потребителей РУПО и объективных параметров, характеризующих качество образовательных услуг. Важно подчеркнуть, что предлагаемая интегральная оценка должна опираться на объективную статистическую информацию о предоставляемых образовательных услугах. Мнение потребителя, его мотивация и потребности учитываются в том вкладе, который вносит каждый параметр в интегральную оценку.

В центре мониторинга системы высшего, среднего и послевузовского профессионального образования при СПбГИЭУ (ЦМПО) был проведен ряд НИР, направленных на создание методического и технологического обеспечения системы мониторинга системы профессионального образования, благодаря чему был разработан подход расчета интегральной оценки, учитывающей в явном виде субъективное мнение конечных потребителей. В ходе работ по этой оценке была создана база данных актуализированной информации об учреждениях высшего профессионального образования Санкт-Петербурга. На основе данного научного задела создается сайт динамического рейтингования вузов Санкт-Петербурга. Сайт позволяет решать ряд задач.

1. Задачи, связанные с интересами конечных потребителей предложений РУПО:

– анкетирование потребителей образовательных услуг с целью выявления их мотивов и требований к учреждениям профессионального образования:

– расчет интегральной оценки учреждений профессионального образования и выдача отчета-рейтинга на основе интегральной оценки, рассчитанной на основе информации, полученной от одного анкетируемого (индивидуальных рейтинг УПО), и оценки, рассчитанной на основе информации о потребностях укрупненных групп потребителей (групповой рейтинг УПО);

– анкетирование потребителей для составления образа конкретных образовательных учреждений с целью уточнения интегральной оценки для разных групп потребителей:

– проведение дополнительных (фоновых) исследований, направленных на выявление тенденций в изменении потребностей потребителей.

2. Задачи, связанные с интересами специалистов РУПО:

– расчет интегральных оценок УПО на основе потребностей групп потребителей РУПО;

– уточнение и поддержание актуальности информации о конкретных УПО;

– сбор экспертных мнений специалистов для уточнения механизмов расчета интегральной оценки;

Таблица 1

Элементы мотивации (атрибуты восприятия)

Элементы мотивации	Сокращенное обозначение
<i>Мотивы/выгоды</i>	
Высокооплачиваемая профессия, но без гарантий быстрого трудоустройства	Материальный достаток
Востребованная профессия, но не самая высокооплачиваемая	Надежная профессия
Сформированные дружеские и деловые связи	Дружба, связи
Реализация творческого потенциала в процессе учебы и профессиональной деятельности	Творчество
Сопричастность к бренду, престижному, модному образованию, профессии, вузу	Символический статус
Причастность к решению важных общественных проблем	Государственность
Получение формального документа об образовании	Формальный статус
Удовольствие от комфортных условий пребывания в стенах вуза	Комфорт
Особые мотивы (обязательно уточнить)	Особые мотивы
<i>Издержки и барьеры</i>	
Низкие разовые материальные издержки, связанные с поступлением	Входные издержки
Низкие регулярные материальные издержки в период обучения	Регулярные издержки
Низкие психологические издержки, связанные с поступлением	Психологические издержки
Малые временные издержки, связанные с поступлением	Временные издержки
Отсутствие формальных препятствий, ограничивающих доступность	Формальные преграды

– получение материалов для создания рекомендаций по стратегическому развитию конкретных образовательных учреждений с целью повышения качества образовательных услуг.

Развертывание сайта связано с разработкой ряда информационно-логических блоков. Обсудим их.

Механизм построения интегральной оценки. Интегральная оценка образовательного учреждения профессионального образования, как уже было сказано выше, опирается как на объективную информацию, характеризующую образовательное учреждение, так и на оценку мотивации и потребности конкретного потребителя (или усредненные потребности группы потребителей) рынка образовательных услуг. Рассмотрим подробнее процесс сбора у пользователей информации, необходимой для построения рейтинга.

В ходе исследования, проведенного в ЦМПО, были получены список черт образования, делающих его важным, и список черт идеального учебного заведения (подробнее см. [1]). В результате экспертной обработки этих данных были выявлены основные мотивы для поступления и отмеченные издержки более всего волнующие будущих абитуриентов (табл. 1), а также набор элементов образа идеального вуза (табл. 2), положенные в основу построения интегральной оценки.

Процесс построения индивидуальной интегральной оценки вузов происходит в несколько этапов.

1. Регистрация на сайте, ввод контактной информации и выявление группы, к которой относится испытуемый.

2. Ранжирование атрибутов основной мотивации для поступления в вуз.

3. Выбор из полярных значений элементов образа идеального вуза.

4. Просмотр результатов с учетом выбранного направления обучения и формы (очная, заочная, вечерняя).

5. После выполнения п.п. 2–4 испытуемый может вновь перейти к п. 2 для получения новой индивидуальной интегральной оценки.

Опишем подробнее каждый этап исследования и алгоритм формирования интегральной оценки.

1. Регистрация, контактные данные, группа. При регистрации пользователь вводит предпочтительное (уникальное) имя пользователя, пароль, почтовый ящик для создания новой учетной записи в системе. Кроме того, предлагается ответить на ряд вопросов для определения социологической группы, к которой относится пользователь. Если пользователь оставляет контактную

Таблица 2

Параметр	Инициативная характеристика									
	Исторический индекс УПО	Награды за деятельность	Руководство профессиональными объединениями	Индекс спонтанности известности	Индекс известности выпускников	Модельность профессий (текущая)	Доходность профессий (текущая)	Востребованность профессий (текущая)	Доходность профессий (будущая)	Востребованность профессий (будущая)
/наличие/ отсутствие										
Электронность (по входным условиям)	9	3	3	9	1	9	1	9	1	9
Условия оплаты (на платных формах обучения)	10	9	1	9	3	3	3	1	3	1
Входной конкурсный барьер	10	3	3	9	3	3	1	9	3	9
Интеллектуальный ценз абитуриентов	9	3	3	9	9	9	3	1	3	9
Индекс широты потребительского выбора	8	3	1	3	1	1	1	1	3	1
Уровень веб-сайта	5	1	1	1	1	1	1	1	1	1
Уровень периодического научного издания УПО	6	4	1	1	3	1	1	1	1	1
Уровень периодического научного издания	0,91	0,85	0,88	0,80	0,84	0,84	0,77	0,75	0,70	0,92
Нормированные веса атрибутов потребительского восприятия	0,21	0,53	0,50	0,57	0,91	0,42	0,33	0,33	0,83	0,03
потребителя										
Вклад каждого атрибута в интегральную оценку	0,19	0,45	0,44	0,46	0,76	0,36	0,26	0,25	0,58	0,03
Интегральная характеристика вуза с учетом мотивации потребителя	6,19									

информацию для связи офф-лайн и является представителем вуза, регулирующего органа или специалистом в области профессионального образования, ему в дальнейшем могут быть назначены права для доступа к дополнительным исследовательским возможностям, более развернутым результатам ранее проведенных исследований, доступ для внесения изменений в информацию о высших учебных заведениях с целью поддержания ее в актуальной форме.

2. Ранжирование атрибутов основной мотивации. Посредством механизма парных сравнений (рис. 1 – один шаг этапа ранжирования) строится матрица $n \times n$ элементов, в которой значение элемента с индексами (i, j) представляет собой отношение между i -м и j -м элементами мотивации потребителя (0 – если важнее j -й элемент; 1 – если элементы равнозначны для пользователя, и 2 – если важнее i -й). Нормированные суммы по строкам (или по столбцам) являются весами атрибутов основной мотивации при поступлении.

Параметр качества 1	Параметр качества 2		
	Высокооплачиваемая профессия	Надежное трудоустройство	
Главное – побольше зарабатывать (возможно, не сразу), остальное решат деньги; принцип – надо брать максимум от жизни	λ	λ	Главное – востребованная в долгосрочном плане профессия (возможно, не самая высокооплачиваемая); принцип – «тише едешь – дальше будешь»

Рис. 1. Одиночная операция процедуры опроса потребителя в методе парных сравнений

3. Выбор полярных значений элементов образа идеального вуза. После того как пользователь даст сравнительную оценку всем атрибутам восприятия, перечисленным в табл. 3, рассчитываются их веса, а пользователь переходит к составлению образа идеального вуза. Здесь пользователь должен выбрать одно из полярных значений для каждого элемента образа (рис. 2).

Теперь давайте составим ваш образ идеального вуза. Выберите один из двух вариантов ответов для всех элементов образа.

Элемент образа	
Возраст	Старый или новый
Консервативность	Консервативный или гибкий
Элитарность	Элитарный или демократичный
Величина	Крупный или камерный
Универсальность	Универсальный или специализированный
Образовательная парадигма	Теоретический или прикладной
Зависимость	Аффилированный или независимый

Рис. 2. Выбор элементов образа идеального вуза

4. Просмотр результатов с учетом выбранного направления обучения и формы (очная, заочная, вечерняя). После опроса пользователя запускается процедура расчета рейтинга, результаты которой выводятся на следующей странице сайта. Образец расчета индивидуальной интегральной оценки приведен в табл. 3.

Таблица 3

**Результаты вычисления интегральной оценки
(вузы ранжированы согласно индивидуальной интегральной оценке)**

Место	Аббревиатура	Название вуза	Оценка	Общая оценка
1	СПбГИЭУ	Санкт-Петербургский государственный инженерно-экономический университет	0,3895	0,9102
2	СПбГАСЭ	Санкт-Петербургская государственная академия сервиса и экономики	0,3164	1,0256
3	СПбГУЭФ	Санкт-Петербургский государственный университет экономики и финансов	0,2987	1,4202
4	СПбГПУ	Санкт-Петербургский государственный политехнический университет	0,2301	1,4675
5	СПбСЗАГС	Северо-Западная академия государственной службы	0,1522	0,7941
6	СПбГУВК	Санкт-Петербургский государственный университет водных коммуникаций		

Окончание табл. 3

Место	Аббревиатура	Название вуза	Оценка	Общая оценка
7	ЛГУ	Ленинградский государственный областной университет (г. Пушкин)	0,0262	1,0705
8	СПбТЭИ	Санкт-Петербургский торгово-экономический институт	0,0259	0,4343
9	СЗГЗТУ	Северо-Западный государственный заочный технический университет	0,0258	1,0402
10	СПбГУАП	Государственный университет аэрокосмического приборостроения	0,0183	1,1454

Интегральная оценка рассчитывается как свертка весов атрибутов потребительского восприятия, полученных после метода парных сравнений с весами, рассчитанными для каждого конкретного учебного заведения.

С помощью составленного образа идеального вуза и выбора интересующего направления рассчитывается второй коэффициент, включающий в себя коэффициент специализации и влияние полярных характеристик.

Соответственно, интегральная оценка вычисляется по формуле

$$R_i = K_{\text{мотив}_i} \cdot K_{\text{идеальн}_i} \cdot K_{\text{спец}_i},$$

где

$$K_{\text{мотив}_i} = \sum_{k=1}^N \|\omega_k \cdot W_{i,k}\|,$$

$$K_{\text{спец}_i} = \frac{C_{i,j}}{\sum_j C_{i,j}} + \frac{S_{i,j}}{\sum_j S_{i,j}},$$

где $C_{i,j}$ и $S_{i,j}$ – количество специальностей i -го вуза по j -му направлению и приведенное количество студентов этого вуза по этому направлению. Приведенное количество студентов считается для выбранной формы обучения и будет различаться для дневной, вечерней и заочной форм обучения. (Коэффициент соответствия образу идеального вуза представляет собой довольно громоздкое выражение и поэтому здесь не приводится.)

В табл. 3 приведен пример результатов вычисления индивидуальной интегральной оценки вузов, ранжированный по интегральной оценке список вузов с учетом выбранной специальности.

Выходы. Разработка тестового макета сайта рейтингования вузов (системы для расчета интегральных оценок ОУ с учетом мотивов и потребностей потребителя) поставила ряд вопросов и выявила следующие проблемы для дальнейшего рассмотрения и реализации в проекте.

1. Расчет значений терминальных параметров вузов является нетривиальной математической задачей, связанной с рядом серьезных методологических проблем, и требует участия эксперта, поэтому одним из ключевых направлений дальнейшего совершенствования системы является создание информационной системы для расчета терминальных параметров на основе сырых статистических данных об образовательных учреждениях.

2. Влияние мотивов потребителя на интегральную оценку, суждя по всему, непостоянно во времени, и потому актуальной представляется задача создания своеобразной обратной связи с экспертами в виде постоянного уточнения связи атрибутов основной мотивации потребителя и терминальных параметров посредством проведения дополнительных фоновых исследований.

3. Интересной является оценка потребителем результатов исследования (рангов ОУ для выбранных направлений), поэтому кроме фоновых исследований, обозначенных в п. 2, требуется собирать информацию о согласии или несогласии испытуемого с результатами исследований.

4. Образовательные учреждения также не являются статичными объектами, поэтому ставится вопрос о механизме поддержания актуальности исходных данных о ОУ для расчетов интегральных и групповых оценок.

В заключение следует отметить, что реализация проекта будет хорошим подспорьем абитуриентам в нелегком выборе своей будущей *alma mater* и даст возможность представителям образовательных учреждений в необычной и новой плоскости взглянуть на достоинства и недостатки своих учреждений.

УДК 378.001.658.011.56

А. Ю. Евстратов

Санкт-Петербургский государственный
инженерно-экономический университет

ОСНОВНЫЕ ПРИНЦИПЫ ФОРМИРОВАНИЯ СИСТЕМЫ ОЦЕНКИ СТОИМОСТИ КАДРОВОГО ПОТЕНЦИАЛА ПРЕДПРИНИМАТЕЛЬСКОЙ СТРУКТУРЫ

Система управления персоналом на коммерческом предприятии представляет собой взаимоувязанный комплекс мероприятий, направленных на обеспечение благоприятных условий для реализации интеллектуальных, профессиональных, творческих и предпринимательских способностей работников, и предполагает создание механизма воздействия на деятельность людей для достижения поставленных экономических, финансовых и инвестиционных целей. В этой системе большое значение играет та ее основная компонента, которая связана с получением стоимостной оценки как отдельного работника (например, специалиста, менеджера), так и кадрового потенциала предприятия в целом. Эту компоненту из-за ее высокой сложности будем условно именовать системой оценки стоимости кадрового потенциала предпринимательской структуры. Построение такой системы представляется весьма актуальным, поскольку на сегодняшний день остается много нерешенных теоретических и методических вопросов.

Создание эффективно функционирующей системы оценки стоимости кадрового потенциала предпринимательской структуры невозможно без предварительного формулирования состава основных принципов. Рекомендуется ряд основных принципов (от лат. *principium* – начало, основа), подлежащих обязательному учету при проектировании научно обоснованной системы оценки стоимости кадрового потенциала предпринимательской структуры. К ним, в частности, относятся следующие.

Принцип системности – стоимостная оценка отдельных сотрудников и кадрового потенциала коммерческого предприятия в целом должна рассчитываться с учетом взаимного влияния (воздействия) всех элементов инфраструктуры системы.

Принцип формализации состоит в разработке достаточно строгой системы математических расчетов, применяемых для решения задачи, связанной с получением стоимостной оценки кадрового потенциала коммерческого предприятия.

Принцип полноты заключается в необходимости учета в математической модели задачи, связанной с определением оценки стоимости кадрового потенциала предприятия, наиболее существенных факторов и ограничений.

Принцип непротиворечивости заключается в том, что включенные в экономико-математические модели задач ограничения не должны противоречить друг другу.

Принцип независимости данных проявляется в том, что используемые в модели задачи исходные данные не должны быть между собой взаимосвязаны; они должны быть независимыми; использование опосредованных данных или информации может привести к построению экономико-математической модели задачи, которая будет неадекватно отражать реальное положение дел.

Принцип компетентности предполагает привлечение к разработке системы расчетов по оценке стоимости кадрового потенциала предпринимательской структуры профессионально подготовленных специалистов в данной области научного знания.

Принцип структурированности данных заключается в том, что необходимые для реализации определенной экономико-математической модели задачи исходные данные должны быть предварительно структурированы, упорядочены и иерархически организованы.

Принцип объективности означает необходимость обеспечения независимости итоговых результатов расчетов по оценке стоимости кадрового потенциала от влияния частных факторов.

Принцип достоверности означает необходимость использования в расчетах таких необходимых исходных данных, которые характеризуются достаточно высоким уровнем точности (достоверности).

Принцип связанности заключается в обеспечении необходимой взаимосвязи (прямой и обратной) между основными элементами как внутри системы, так и между системой и внешней средой.

Принцип целостности определяет значимость каждого элемента, свойства системы в зависимости от их места и назначения внутри нее.

Принцип иерархичности означает строгий порядок подчинения составных нижестоящих элементов (подсистем, задач) вышестоящим.

Принцип прогностичности означает, что используемые в расчетах исходные данные, обычно получаемые с помощью современных методов прогнозирования, должны прояснить достаточно отдаленную перспективу деятельности коммерческого предприятия.

Принцип доступности означает, что система расчетов (основные процедуры) и критерии получения стоимостных оценок кадрового потенциала на разных уровнях управления коммерческим предприятием должны быть понятны всем заинтересованным сторонам.

Принцип актуализации означает необходимость систематического обновления исходных данных при выполнении требуемых расчетов. Это обусловлено тем, что по своей сути рассматриваемая система не статична, она нуждается в постоянном развитии (совершенствовании).

Принцип целостности означает, что при проектировании системы, предназначенной для оценки стоимости кадрового потенциала коммерческого предприятия, необходимо предусмотреть учет взаимосвязи между основными элементами системы.

Принцип прогрессивности, основной смысл которого проявляется в необходимости формирования системы, используемой для оценки кадрового потенциала любой предпринимательской структуры в соответствии с передовым зарубежным и отечественным опытом.

Принцип адаптивности, суть которого проявляется в необходимости учета специфики деятельности конкретной предпринимательской структуры, принятой к исполнению стратегии ее развития, особенностей организационной культуры, т. е. умении приспосабливаться к изменяющимся условиям макро- и микросреды.

Принцип оптимальности означает, что на каждом этапе разработки системы оценки стоимости кадрового потенциала предпринимательской структуры должно приниматься наилучшее решение из совокупности альтернативных управлеченческих решений.

Благодаря наиболее полному учету всех перечисленных выше принципов при разработке научно обоснованной системы оценки стоимости кадрового потенциала коммерческого предприятия будут созданы благоприятные условия для получения достоверных итоговых результатов расчетов.

ПРОБЛЕМНЫЕ ВОПРОСЫ ПОЛУЧЕНИЯ СТОИМОСТНОЙ ОЦЕНКИ КАДРОВОГО ПОТЕНЦИАЛА

Величина производственного потенциала любого коммерческого предприятия во многом зависит от его кадрового потенциала. Поэтому получение его достоверной стоимостной оценки представляется весьма актуальным.

Вполне доказанным всей мировой практикой является и тот факт, что инвестиции в человека представляют собой важнейшую институциональную компоненту развития не только любых рыночных структур, но и самого человека, а также современного общества в целом. Из множества инвестиций в человеческий капитал наиболее важными являются вложения в образование и здоровье. Образование не только позволяет овладеть старыми, уже накопленными человечеством знаниями, но и способствует приобретению новых знаний в процессе работы и систематического повышения уровня квалификации, обеспечивает условия для их воспроизведения в будущем.

Под человеческим капиталом обычно понимается воплощенный в человеке запас способностей, знаний, навыков, амбиций и мотиваций.

Известно, что человеческий капитал как экономическая категория включает в себя различные аспекты воплощенной в индивиде способности приносить доход себе и обществу. Однако важнейшим из них является высшее образование. Общепринятое является точка зрения, что формирование человеческого капитала происходит путем инвестиций (долгосрочных вложений капитала) в человека в виде затрат на образование, подготовку рабочей силы на предприятии, на охрану здоровья, миграцию и поиск информации о ценах и доходах.

© А. Ю. Евстратов, В. В. Царёв, 2009.

Провозглашенный много лет назад лозунг «кадры решают все» приобретает еще большую актуальность в современной динамично изменяющейся рыночной экономике.

Проблема определения стоимостной оценки кадрового потенциала предприятия особенно актуальна в ситуациях, когда, во-первых, происходит смена собственника (покупка/продажа предприятия), и, во-вторых, намечаются кардинальные кадровые перестановки персонала в функциональных отделах или департаментах.

Получение стоимостной оценки кадрового потенциала имеет большое практическое значение и в случае создания системы управления стоимостью компании (УСК). Многими видными учеными как за рубежом, так и у нас в стране считается доказанным, что показатель оценки стоимости компании является одним из главных и вместе с тем интегрированным показателем оценки конечных экономических результатов функционирования коммерческого предприятия.

Благодаря наличию методики, позволяющей с достаточно высокой точностью получать стоимостную оценку каждого отдельного работника (специалиста, менеджера), облегчаются условия для назначения справедливого месячного оклада (рыночной стоимости) при приеме его на работу, а также стимулирование его дальнейшей производственной деятельности.

Располагая оценкой потенциала отдельного работника, можно определить совокупную стоимостную оценку трудового коллектива по коммерческому предприятию в целом. При осуществлении купли/продажи предприятия эта совокупная оценка кадрового потенциала выступает как важная компонента общей его стоимости (обычно относимая к нематериальному активу).

Стоимостная оценка отдельного работника и кадрового потенциала предприятия может выступать в двух ипостасях. Во-первых, как текущая, а во-вторых, как прогнозируемая стоимостная оценка (ценность) отдельного работника и кадрового потенциала по коммерческому предприятию в целом. Наиболее сложной и вместе с тем до конца не решенной проблемой представляется получение прогнозируемой стоимостной оценки потенциала отдельного работника, специалиста, менеджера и кадрового потенциала предприятия в целом. Это обусловлено тем, что весьма сложно располагать необходимыми достоверными исходными данными относительно:

- будущих продвижений работников по служебной (карьерной) лестнице и между различными отделами (такие планы-прогнозы на российских предприятиях, как правило, не разрабатываются);
- наиболее вероятной продолжительности работы специалистов, менеджеров на данном предприятии;
- прогнозируемых уровней текучести персонала по различным годам;
- дифференцированных и разных во времени уровнях оплаты труда работников разных профессий и квалификаций;
- возможных сроков увольнения работников по различным причинам;
- величин издержек, связанных с увольнениями работников;
- динамики роста их заработной платы и других доходов;
- объемов валовой прибыли предприятия по прогнозируемым периодам;
- структуры затрат живого и прошлого труда в себестоимости годовых объемов выпуска готовой продукции;
- перспективных планов (карьерограмм) продвижения работников по служебной (карьерной) лестнице (карьерограмма – это перспективный план профессионального роста и последовательного перемещения сотрудника по соответствующим должностям, характеризующимся более высоким статусом и уровнем оплаты труда);
- объемов инвестиций, которые будут выделены на повышение квалификации, переподготовку, переобучение работников в разные периоды времени.

Все перечисленные выше исходные данные, необходимые для получения достоверной стоимостной оценки кадрового потенциала коммерческой структуры, могут носить преимущественно вероятностный характер, что требует использования достаточно сложных специальных методов расчетов (например, базирующихся на теории нечетких множеств). Оценить же надежность и достоверность перечисленных выше исходных данных пока еще не представляется возможным. Решение указанной задачи является предметом последующих научных исследований.

УДК 378.001.658.011.56

Д. С. Евсюков

Санкт-Петербургский государственный
инженерно-экономический университет

МЕХАНИЗМЫ И МЕТОДЫ ОПРЕДЕЛЕНИЯ СТРУКТУРЫ СТАТЕЙ ДОХОДОВ И РАСХОДОВ ПРИ БЮДЖЕТИРОВАНИИ ПРОЕКТОВ МАЛОЭТАЖНОГО КОТТЕДЖНОГО СТРОИТЕЛЬСТВА

В связи со сложившейся в последние годы ситуацией в области малоэтажного коттеджного строительства для совершенствования оперативного управления бюджетом необходимо классифицировать механизмы и методы определения структуры статей доходов и расходов.

Каждый проект может иметь свои статьи доходов и расходов. Поскольку бюджет проекта может рассматриваться в качестве финансового интерфейса с бюджетом портфеля проектов и компаний в целом, статьи доходов и расходов должны быть унифицированы.

Рассмотрим существующую классификацию статей расходов. Статьи доходов обычно меньше, и они все напрямую относятся к проекту.

В бухгалтерском и управлеченческом учете применяется целый ряд классификаций расходов с различных точек зрения. По отношению к проекту или портфелю проектов затраты можно разделить на:

- прямые (они же, как правило, регулируемые), относящиеся непосредственно к проекту или портфелю, которыми распоряжается руководитель проекта или центр ответственности за портфель проектов;

- косвенные (они же нерегулируемые), которые не находятся в распоряжении руководителя проекта или центра ответственности за портфель проектов, но как-то соотносятся с проектом и портфелем проектов.

Определение структуры затрат портфеля проектов и входящих в него проектов строится следующим образом.

Шаг 1. Определить прямые и косвенные расходы портфеля проектов (кроме них будут еще расходы, вообще не относящиеся к

портфелю, – например, к портфелю одной бизнес-единицы расходы другой бизнес-единицы не будут иметь никакого отношения).

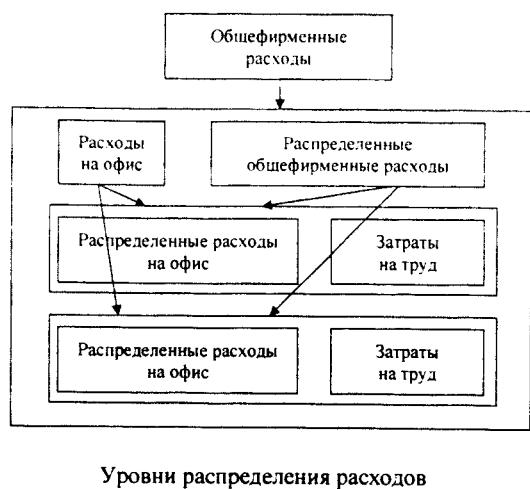
Шаг 2. Установить, какие из расходов портфеля являются прямыми расходами для проектов, а какие – косвенными.

Шаг 3. Установить правила распределения косвенных расходов на портфели проектов.

Шаг 4. Установить правила распределения косвенных расходов на проекты.

Шаг 2 осложняется тем, что при определении структуры затрат нет полного перечня проектов, входящих в портфель, – он изменяется динамически. Поэтому должны быть определены принципы того, как это делается.

Распределение косвенных расходов на портфель проектов и проекты схематично изображено на рисунке.



В бюджете проекта часто предусматривают особые статьи затрат, называемые резервами. Они могут быть выражены в человеко-часах, машино-часах, деньгах и предназначены для смягчения предусмотренных и непредусмотренных рисков. Выделение резервов дает больше самостоятельности руководителю проектов, который может принимать решения об их расходовании без пересмотра бюджета.

В некоторых проектах важен денежный поток, т. е. превышение доходов над расходами в каждом периоде. Например, могут быть установлены требования, чтобы доходы всегда превышали расходы, т. е. проект был полностью и постоянно самофинансируемым. В этом случае в бюджете проекта необходимо вычислять и денежный поток.

Иногда пытаются создавать бюджеты непосредственно на основе плана счетов, однако такое целесообразно только в небольших компаниях, да и то в редких случаях.

Ставки распределения косвенных расходов определяются на период на основе прогнозов о деятельности компании или параметров портфеля проектов. Их можно пересматривать в течение этого периода, однако это приведет к изменению всех бюджетов. Поэтому эти ставки часто фиксируют, а разницу, полученную за счет изменения базы и ставок распределения, относят на прибыль или убытки. При этом точное значение расходов по статье бюджетируется на уровне компании или портфеля, а их возмещение отражается в бюджетах проектов.

Если подразделения обладают постоянным штатом, получающим фиксированную зарплату, то в этом случае возникает аналогичная ситуация. Если сотрудники работают по проектам меньшее время, чем ожидалось при бюджетном планировании, то часть зарплаты не возмещается за счет проектов и вычитается из прибыли компании.

Проблема определения и классификации механизмов и методов определения структуры статей доходов и расходов является на сегодняшний день важной проблемой в области малоэтажного коттеджного строительства и требует исследования.

УДК 378.001.658.011.56

Э. А. Пиль

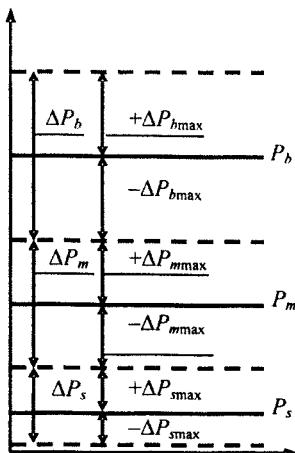
Санкт-Петербургский государственный
инженерно-экономический университет

СИЛЫ, ДЕЙСТВУЮЩИЕ НА ЭКОНОМИЧЕСКИЕ ОБОЛОЧКИ

В своих работах ряд авторов описали кризисные процессы, протекающие в экономике [1; 2]. Их основным недостатком являет-

ся то, что в них не представлен необходимый математический аппарат, позволяющий описывать процессы, происходящие в экономике, с помощью которых можно прогнозировать будущие кризисы. В работе [3] автор показал, что экономику любой страны можно представить в виде трех оболочек: малого, среднего и большого бизнеса. При воздействии внешних или внутренних сил (либо при их совместном действии) экономические оболочки деформируются и их деформацию можно свести к таким видам, как расширение и сжатие [3]. При этом под одновременным расширением (сжатием) экономических оболочек (либо при их совместном расширении и сжатии) подразумевается то, что это может происходить как пропорционально, т. е. по одному какому-то математическому закону и на одну и ту же величину, так и не пропорционально, т. е. по разным математическим законам.

Так, как силы P_V (см. рисунок), действующие на экономическую оболочку, могут различаться по своей относительной величине, введем для них следующие три градации: P_b – большая внешняя (внутренняя) сила; P_m – средняя внешняя (внутренняя) сила; P_s – малая внешняя (внутренняя) сила.



Распределение сил деформации P_V экономических оболочек

Примем значение силы P_V со знаком « $-$ » для внешних сил, которые сжимают экономическую оболочку, отчего она деформируется и ее объем уменьшается. Если же на экономическую оболочку действуют внутренние силы, то будем их считать положительными, т. е. со знаком « $+$ », так как в этом случае экономическая оболочка также деформируется, но при этом ее объем увеличивается.

Теперь дадим определение всем трем силам.

Большая внешняя (внутренняя) сила P_b – это такая сила, при воздействии которой экономическая оболочка сильно деформируется и в ней появляется, как минимум, одна трещина.

Средняя внешняя (внутренняя) сила P_m – это такая сила, при воздействии которой экономическая оболочка сильно деформируется, но при этом в ней не появляются трещины.

Малая внешняя (внутренняя) сила P_s – это такая сила, при воздействии которой экономическая оболочка деформируется незначительно.

На рисунке представлен вид распределения силы деформации P_V экономической оболочки, исходя из которого можно вывести следующие выражения

$$\begin{aligned}\Delta P_b &= +\Delta P_{b\max} + |-\Delta P_{b\max}|; \\ \Delta P_m &= +\Delta P_{m\max} + |-\Delta P_{m\max}|; \\ \Delta P_s &= +\Delta P_{s\max} + |-\Delta P_{s\max}|,\end{aligned}$$

где ΔP_i – величина силы деформации P_V экономической оболочки (i – номер деформации);

$+\Delta P_{\max}$ – максимальное отклонение величины силы деформации P_V , которая действует на экономическую оболочку в сторону увеличения;

$-\Delta P_{\max}$ – максимальное отклонение величины силы деформации P_V , которая действует на экономическую оболочку в сторону уменьшения.

Таким образом, величину силы деформации P_V экономической оболочки можно представить следующим уравнением

$$P = \Delta P_b + \Delta P_m + \Delta P_s = +\Delta P_{b\max} + |-\Delta P_{b\max}| + (+\Delta P_{m\max}) + |-\Delta P_{m\max}| + (+\Delta P_{s\max}) + |-\Delta P_{s\max}| = 100\%.$$

Здесь следует отметить, что значения ΔP_b превышают значения ΔP_m и во много раз ΔP_s (т. е. $\Delta P_b > \Delta P_m$, $\Delta P_b \gg \Delta P_s$) и при этом значения ΔP_b должны изменяться по времени намного реже, чем ΔP_m и тем более, чем ΔP_s . В противном случае экономическая система будет нестабильной и ее ожидают частые экономические потрясения в виде мировых экономических кризисов. Да и трудно себе представить, чтобы каждый месяц издавались такие законы или происходили катаклизмы, которые приводили к такому состоянию экономические оболочки.

Литература

1. Петросян В. С. Единая теория циклов, кризисов, формаций. М.: Гравитоника, 1999. (Приложение к научному журналу «Гравитоника»).
2. Туган-Барановский М. И. Избранное. Периодические промышленные кризисы. История английских кризисов. Общая теория кризисов. М.: Наука, (РОССПЭН), 1997 (Сер. «Памятники экономической мысли»).
3. Пиль Э. А. Деформация экономических оболочек при воздействии внешних и внутренних сил. Проблемы современной экономики. 2007. № 1 (21). С. 427–429.

УДК 378.001.658.011.56

Т. В. Ростовцева

Санкт-Петербургский государственный
инженерно-экономический университет

РЕШЕНИЕ ЗАДАЧИ ОПТИМИЗАЦИИ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОГО СНАБЖЕНИЯ СТРОИТЕЛЬНО-МОНТАЖНЫХ РАБОТ

В обобщенной постановке задача оптимизации материально-технического снабжения строительно-монтажных работ (СМР) выглядит следующим образом: для заданной совокупности групп наименований строительных материалов (необходимых для производства отдельной СМР) и при ограничениях на качество этих материалов требуется найти поставщика такого набора материалов, который обеспечит наименьшие затраты в денежном выражении.

© Т. В. Ростовцева, 2009.

Предлагаемое решение данной задачи заключается в построении всех наборов совместимых материалов из разных групп и выборе среди них такого набора, который обеспечивает наименьший расход материалов по каждой строительно-монтажной работе.

Основная сложность при решении данной задачи заключается в том, что при выполнении заданной СМР норма расхода конкретного материала из конкретной группы зависит от выбора материалов других групп. Эти зависимости определены в ГОСТах, СНИПах, технических условиях выполнения строительно-монтажных работ, где для каждого конкретного материала задан список других материалов, влияющих на норму расхода материала, и определено значение нормы расхода материала для каждого «влияющего» набора материалов.

Рассмотрим наиболее простой вариант решения задачи оптимизации затрат на приобретение строительных материалов, где для проведения конкретной СМР имеется такая комплектация строительных материалов, где расход материала k -й группы зависит только от расхода материала $k-1$ -й группы.

Данная задача является задачей динамического программирования и удовлетворяет принципу оптимальности Беллмана, который требует, чтобы всякий отрезок a_k, a_{k+1}, \dots, a_m оптимальной последовательности a_1, \dots, a_n ($1 \leq k \leq M \leq N$) был бы сам оптимальным (т. е. давал бы минимальное значение функции $F(a_k, \dots, a_m)$) среди всех последовательностей, совпадающих с ним в крайних компонентах и по числу компонент.

Решение задачи оптимизации затрат на приобретение строительных материалов сводится к вычислению последовательности функций

$$f_1(a_1) = c_{a1}r_{a1}, f_2(a_2) = f_1(a_1) + c_{a2}r_{a2};$$

$$f_n(a_n) = \min(f_{n-1}(a_{n-1}) + c_{an}r_{an});$$

$$a_{n-1} \in D_{n-1}, a(a_{n-1}, a_n) = 1$$

и значения $a_{n-1} \in D_{n-1}$, $a(a_{n-1}, a_n) = 1$ такого, что для него достигается наименьшее значение $f_{n-1}(a_{n-1}) + c_{an}r_{an}$.

Вычисление функций $f_n(a_n)$ производится с помощью рекурсивной процедуры.

Для решения данной задачи разработана модификация графового метода, который заключается в пересчете всех кратчайших пу-

тей из вершин k -й группы во все вершины $k+1$ -й группы и определении среди них самого кратчайшего пути. Пересчет осуществляется путем сравнения длин всех кратчайших путей из вершины k -й группы в вершину $k+1$ -й группы с текущим кратчайшим путем.

В более сложном варианте имеется такая комплектация строительных материалов, где требуется совместимость материалов нескольких групп и где расход материала k -й группы зависит не только от расхода материала $k-1$ -й группы, но и от расхода материалов других групп.

Решение данной задачи заключается в пересчете всех путей, соединяющих вершины k -й группы с вершинами $k+1$ -й группы согласно совместимости вершин, а не оптимальных на каждом шаге. Затем определяем длину пути от вершин 1-й группы до вершин последней – n -й – группы и находим среди них самый короткий.

Данное решение не удовлетворяет принципу оптимальности Беллмана, поскольку расход материала a_l зависит материалов $a_1, a_2, \dots, a_i, \dots, a_{n-1}$, и набор материалов $a_1, a_2, \dots, a, \dots, a_{n-1}$ не обязан быть оптимальным (неоптимальный набор материалов $a_1, a_2, \dots, a_i, \dots, a_{n-1}$ может обеспечить такой расход a_l , что общий расход материалов $a_1, a_2, \dots, a, \dots, a_{n-1}, a_l$ будет лучший, чем для оптимального набора).

Для расчета затрат на приобретение одного наименования строительного материала необходимо решить следующий круг задач:

- выявить бинарные отношения между материалами различных групп;
- рассчитать расход основных и вспомогательных строительных материалов;
- рассчитать общую стоимость приобретения строительного материала.

Бинарные отношения между материалами различных групп определяют совместимость строительных материалов, т. е. возможность их совместного использования для реализации отдельной СМР. Данные отношения представлены в виде матрицы из нулей и единиц, где элемент $a_{ij} = 1$, если материалы номер i и номер j , принадлежащие разным группам, совместимы, и $a_{ij} = 0$, если материалы номер i и номер j , принадлежащие разным группам, несовместимы.

Расчет расхода материала выполняется по правилам, определяющим норму расхода конкретного материала от набора материа-

лов других групп. Эти правила составляют ядро нормативно-справочной базы расхода материалов в процессе выполнения строительно-монтажных работ. Правила записываются в виде строки электронной таблицы, в которой отмечены знаком «+» ячейки, соответствующие влиятельным материалам, а в колонках с указанием зависимых материалов указаны нормы расхода их на единицу выбранного материала предпоследней группы. В том случае, если норма расхода материала не зависит от указанного, то ячейка пустая и норма расхода определяется по нормам расхода данного материала на единицу выполняемых работ.

Цена приобретения конкретного наименования строительного материала вычисляется на основе цены материала, указанной в прайс-листе производителя (поставщика) материала, удельных затрат доставки материала и его доводки, т. е. стоимости дополнительных материалов и работ, необходимых для доведения исходного материала до состояния, необходимого по техническим условиям.

Задача оптимизации затрат на приобретение материалов сводится к построению всех путей, соединяющих вершины первой и последней групп, и определению среди них пути наименьшей длины. Данную задачу предлагается решать с помощью параллельных алгоритмов теории графов.

Для реализации параллельного алгоритма построения путей графа последовательные группы материалов объединяются в блоки по n групп. При этом последняя группа k -го блока совпадает с первой группой $k+1$ -го блока. Число n определяется производительностью кластера. На каждом кластере независимо от других и параллельно с другими кластерами определяются все пути, соединяющие вершины первой и последней группы блока. Поиск путей на кластере производится в параллельном режиме. На первом элементе кластера определяются пути, выходящие из вершины V_1 , на втором элементе определяются пути, выходящие из вершины V_2 , на i -м элементе определяются пути, выходящие из вершины V_i . После построения путей на каждом блоке на k -м кластере объединяются пути k -го и $k+1$ -го блоков и получаются пути длины $2n$. Затем в параллельном режиме объединяются пути двойных блоков и т. д. В результате получаются пути вершин первой группы в вершины последней.

Для практического решения задачи необходимо иметь мультипроцессорный вычислительный комплекс, кластер, гипер-

сеть. Все эти устройства можно получить по Интернету, обратившись к услугам вычислительных фирм, которые заказывают в Интернете серверы или кластеры, распределяют по серверам или кластерам приложения пользователей и обеспечивают их выполнение, обеспечивают обмен данными в процессе выполнения приложений, записывают и сохраняют результаты решения промежуточных задач в виде распределенных баз данных или файла автономного Интернет-хранилища.

Применительно к задаче оптимального материального снабжения строительно-монтажных работ пользователь находит в Интернете исходные данные и обеспечивает ими приложения. Вычислительная фирма распределяет по кластерам исходные данные и программы нахождения путей в группе материалов, программы объединения путей двух соседних групп; обеспечивает их выполнение и обмен данными между ними; записывает результаты решения (множество путей, соединяющих элементы первой и последней групп) в виде распределенной Интернет-базы данных и обеспечивает к ней доступ пользователю.

Был проведен вычислительный эксперимент, который заключался в построении, записи и обработке путей, соединяющих 90 вершин, распределенных на 9 групп по 10 вершин в каждой группе. Пути состоят из 9 дуг, соединяющих 9 вершин из разных групп. Количество таких путей равно 10^9 . Для вычислительного эксперимента использовался вычислительный комплекс из четырех компьютеров и двадцати пяти процессорных кластеров, объединенных в локальную сеть. По сути дела, над решением задачи трудились 100 процессоров, выполняя независимо друг от друга по 10^7 логических и арифметических операций.

Вначале исходные данные были равномерно распределены по четырем компьютерам и на каждом компьютере были построены 1 000 путей с тремя вершинами. Затем на первом компьютере были построены 100 000 путей, соединяющих вершины первой и пятой групп, а на втором компьютере были построены 100 000 путей, соединяющих вершины пятой и девятой групп. Для асинхронной загрузки данных записываем на первом компьютере пути, заканчивающиеся в вершине V_i , в 10 файлов по 1 000 записей в каждом файле. На втором компьютере делаем десять копий файла путей, начинающихся в вершине V_i . Получим 100 файлов по 10 000 запи-

сей в каждом. Таким образом, и с первого, и со второго компьютера каждый из ста процессоров загружает данные из своего файла, параллельно остальным процессорам, не блокируя остальные процессы. Время загрузки данных приблизительно 10 мин.

Для построения путей, проходящих через фиксированную вершину V_i из пятой группы, используются 10 процессоров. На каждом процессоре записано 1 000 путей, заканчивающихся в вершине V_i , и 10 000 путей, начинающихся в данной вершине. Пути строятся методом соединения путей соседних блоков. Построение путей на каждом процессоре методом соединения длится 15 мин. Запись 10^7 путей (последовательностей из 100 символов) длится 25 минут. После того как пути построены и записаны, процессоры загружают пути в оперативную память и находят пути минимальной длины. Время загрузки приблизительно 20 минут. Время обработки загруженных путей приблизительно 7 минут. Таким образом, общее время решения реальной задачи оптимизации материально-технического обеспечения строительно-монтажных работ равно приблизительно двум часам.

Таким образом, предлагаемое решение проблемы оптимизации затрат материально-технического снабжения СМР может быть реализовано на практике, имеет практическое значение и соответствует современному процессу развития экономико-математических моделей.

УДК 378.001.658.011.56

С. А. Соколовская,

Е. В. Стельмашонок

Санкт-Петербургский государственный
инженерно-экономический университет

ЦЕЛИ И ОСНОВНЫЕ ФУНКЦИИ ВИРТУАЛЬНОГО ПРЕДПРИЯТИЯ

Тенденции развития современных рынков, такие как глобализация рынков, спрос на качество товара и снижение его цены, повышение важности устойчивых отношений с потребителями (индивидуальными заказчиками), а также возрастающее значение применения новых информационных и коммуникационных технологий

породили новую – виртуальную – структуру организации и управления предприятиями.

Виртуальное предприятие (ВП) – это сетевая, компьютерно-опосредованная организационная структура, состоящая из неоднородных взаимодействующих агентов, расположенных в различных местах [1] (Дж. Хоплэнд).

Основной целью ВП является формирование гибкой распределенной в пространстве системы предприятий-агентов, направленной на быстрый выпуск новой продукции, повышение ее конкурентоспособности и поставки на рынок. Предприятия-партнеры (агенты) «...разрабатывают совместный проект, находясь между собой в отношениях партнерства, кооперации, сотрудничества...» [1]. Главная цель при этом – максимальное удовлетворение требований клиента. Более того, именно требования клиента и определяют структуру и функции как самого ВП, так и его агентов, основные требования заказа и, в конечном итоге, задают основные требуемые характеристики эффективности ВП [2].

ВП строится на отборе человеческих, организационно-методических и технологических ресурсов различных предприятий путем их интеграции, приводящей к формированию гибкой, динамично-организационной структуры. Эта структура наиболее приспособлена для скорейшего выпуска новой продукции и ее оперативной поставки на рынок. В таком предприятии осуществляется интенсивное взаимодействие специалистов и подразделений различных предприятий с помощью новейших информационно-коммуникационных технологий. Это взаимодействие способствует повышению уровня кооперации и координации партнеров, а в конечном итоге конкурентоспособности производимой ими продукции.

ВП является непосредственно ориентированным на заказчика, так как его основные характеристики – быстрота выполнения заказа и полнота удовлетворения потребностей клиента. Создание ВП означает интеграцию уникального опыта, производственных возможностей и передовых технологий предприятий – партнеров вокруг некоторого проекта, который они не могут выполнить в отдельности. Упрощенно функционирование виртуального предприятия выглядит в виде схемы (рисунок).



Упрощенная схема виртуального предприятия

Можно сделать вывод, что виртуальная структура организации предприятия базируется на следующих принципах:

- отказ от целостности технологического процесса производства готовой продукции;
- партнеры по производству совместного продукта существуют до тех пор, пока их поставки соответствуют стандартам качества и уровню технологичности;
- в глобальной экономике поиск партнеров производится по всему миру;
- выгодно, чтобы предприятие имело гибкую структуру, с максимальной эффективностью используя существующие и приобретаемые ресурсы;
- в условиях быстрого развития технологий невыгодно вкладывать большие деньги в закупку оборудования, стационарных помещений, особенно если неизвестно, какой объем продукции будет выпущен;
- сокращение непроизводственных расходов, прежде всего связанных с управлением.

Таким образом, ВП – это структура, ориентированная на выпуск конкретного продукта, создаваемая на время жизненного цикла этого продукта путем объединения производственных возможностей и ресурсов различных хозяйствующих субъектов (предпри-

ятий или физических лиц) на договорных условиях в определенном объеме и на фиксированное время. Для выпуска определенного изделия, состоящего из нескольких составных частей, требуется найти агентов и возможность изготовить необходимые узлы, договориться об их поставке в заданный срок и нужное место.

Целями построения ВП являются:

- обеспечение экономически выгодного для участников сотрудничества, интеграции и координации предприятий, коллективов и специалистов, пространственно удаленных друг от друга;

- организация предприятий вокруг сквозных бизнес-процессов, поддерживающих жизненный цикл продукта, что обеспечивает возможность быстрого образования, развития, реструктурирования и безболезненного расформирования виртуальных предприятий в соответствии с потребностями рынка;

- интеграция средств, знаний и опыта различных предприятий для повышения конкурентоспособности и качества конечного продукта.

Анализ деятельности виртуальных предприятий показал, что основными характеристиками виртуальной формы организации являются:

- открытая распределенная структура системы управления;
- гибкость производственной структуры;
- приоритет горизонтальных связей с предприятиями-агентами;
- высокий уровень оснащения информационно-техническими средствами.

ВП можно охарактеризовать не только поставленными задачами, целями и функциями, но также распределением властных полномочий и ролей, способами коммуникации, правилами распределения прибыли и другими особенностями. Существует, по крайней мере, три вида виртуальных предприятий (таблица) [3].

Деятельность агентов для различных видов ВП разнообразна, в том числе и включая «...три ее важнейших ипостаси: поведение, мышление и коммуникацию...» [4]. Агентов ВП можно представить как некоторые системы организационного управления, в которых «...действуют отдельные люди или коллективы, осуществляющие направленную деятельность в процессе производства...» [4].

Виды и свойства виртуальных предприятий

Виды ВП	Описание
С централизован-ным типом управ-ления	Агенты действуют по поручению своих организаций, причем один из агентов управляет процессом: уясняет задачу, выдает задания другим агентам, обобщает ре-зультаты и принимает решение
С распределенным типом управления	Знания и ресурсы распределяются между агентами, но сохраняется общий орган командного управления, принимающий решения в конфликтных ситуациях
С децентрализован-ным типом управ-ления	Все управленческие процессы осуществляются только за счет локальных взаимодействий между агентами

Литература

1. Тарасов В. Б. Предприятия XXI века: проблемы проектирования и управления // Автоматизация проектирования. 1998. № 4.
2. Балабанов И. Т. Интерактивный бизнес. СПб.: Питер, 2001.
3. Скобелев П. О. Самоорганизация и эволюция в открытых мультиагентных системах для холонических предприятий // Искусственный интеллект в 21 веке: Тр. Междунар. конгр.: Дивноморское, 3–8 сентября 2001. Т. 1. М.: Физматлит, 2001. С. 314–338.
4. Игнатьева А. В., Максимцов М. М. Исследование систем управления. М.: ЮНИТИ-ДАНА, 2001.

УДК 62 – 50

В. И. Фомин

Санкт-Петербургский государственный
инженерно-экономический университет

СТРУКТУРНО-ТИПОЛОГИЧЕСКИЙ ПОДХОД ПРИ МОДЕЛИРОВАНИИ ЗАТРАТ ВРЕМЕНИ НА ПОВЫШЕНИЕ ДОСТОВЕРНОСТИ ПРЕОБРАЗОВАНИЯ ЭКОНОМИЧЕСКОЙ ИНФОРМАЦИИ

В современных экономических информационных системах (ЭИС) предъявляются высокие требования к достоверности преобразования

(сбора, передачи, хранения, обработки и представления) информации. В связи с этим в ЭИС реализуются различные методы контроля и коррекции ошибок в процессе преобразования данных. При проектировании ЭИС необходимо иметь возможность оценивать затраты времени на преобразование информации с учетом реализации тех или иных методов повышения достоверности. Анализ функционирования систем показывает, что эти затраты зависят от места выполнения контроля, а также от применяемой процедуры контроля. На рисунках, представленных в данной статье, схематически показаны типовые структуры организации контроля и коррекции информации в ЭИС.

Без учета реализации контроля время преобразования единицы информации (символа, реквизита, сообщения и т. д.) T_e определяется реализуемой в ЭИС процедурой преобразования информации, а также производительностью применяемых технических средств и персонала на каждом из этапов преобразования

$$T_e = \sum_{i=1}^{m_e} (T_{ei} + t_{ei}),$$

где T_{ei} , t_{ei} – время ожидания начала выполнения и время выполнения i -го преобразования единицы информации;

m_e – число последовательных этапов преобразования единицы информации.

Без учета процедуры коррекции время выполнения единичного (i -го) этапа преобразования и контроля единицы информации T_{ei} равно

$$T_{ei} = T_{ci} + t_{ei} + t_{kei}, \quad (1)$$

где t_{kei} – время контроля единицы информации на i -м этапе.

Рассмотрим случай коррекции без повторного контроля для группы из m_e последовательных этапов преобразования, охватываемых единым контролем,

$$T_e = t_{ke} + \sum_{i=1}^{m_e} (T_{ci} + t_{ei}) = t_{ke} + T_e, \quad (2)$$

где t_{ke} – время контроля единицы информации.

Значение t_{ei} в общем виде определяется из соотношений:

а) для n -го реквизита $t_{ni} = \frac{L_n}{V_{ei}}$;

б) для z -го сообщения $t_{zi} = \sum_{n=1}^{m_{pz}} t_{ni}$;

в) для партии z -х сообщений $t_{nzi} = n_{\text{парт}} t_{zi}$,

где V_{ei} – скорость преобразования на i -м этапе [симв/с];

m_{pz} – число разных реквизитов в z -м сообщении;

$n_{\text{парт}}$ – число сообщений в партии;

L_n – длина (число символов) в n -м реквизите.

Таким образом, оценки значений t_{ei} могут быть получены исходя из известных параметров производительности работы технических средств и персонала ЭИС или определены на основе контрольного хронометража соответствующих преобразований информации.

Значения T_{ei} определяются спецификой применяемой процедуры преобразования информации. Величины T_{ei} могут быть определены на основе соответствующих статистических данных или экспертной оценкой. В качестве экспертов в этом случае должны выступать работники соответствующих служб предприятия (ЭИС), имеющие практический опыт решения задач рассматриваемого класса. В том случае, если задержка T_{ei} определяется временем ожидания, обусловленным возникновением очереди на обслуживание техническим средством на i -м этапе, ее величина может быть оценена методами теории массового обслуживания.

Реализация коррекции выявленных контролем искажений может вносить дополнительные задержки, зависящие от характера применяемой процедуры. Рассмотрим оценки для этих задержек (рис. 1 и 2).

Для i -го этапа преобразования к затратам времени на сбор и контроль T_{ei} добавятся затраты на коррекцию (т. е. повторное преобразование) части единиц информации, в которых при контроле будут выявлены искажения. Значение времени сбора единицы информации на i -м этапе с учетом контроля и коррекции T_{ei}^* может быть в этом случае оценено

$$T_{ei}^* = \begin{cases} \tau_{ei} + t_{ei} + t_{kei} & \text{при отсутствии возврата} \\ \tau_{ei} + t_{ei} + t_{kei} + t'_{ei} + t''_{ei} & \text{при возврате информации,} \end{cases}$$

а среднее время выполнения i -го этапа $[T_{ei}^*]_{cp}$ равно:

$$[T_{ei}^*]_{cp} = T_{ei} + t_{ei} + t_{k,ei} + (T'_{ei} + t'_{ei})\sigma_{ei},$$

где σ_{ei} – параметры в режиме выполнения коррекции; каждый из них – коэффициент, учитывающий относительную частоту (вероятность) возврата единиц информации контролем, определяемый по формуле:

$$\sigma_{ei} = [P_{ei}(1 - K_{Ri}) + P_{k,o}(1 - P_{ei})],$$

где P_{ei} – вероятность невыявленного искажения единицы информации на i -м этапе преобразования;

K_{Ri} – коэффициент редукции, характеризующий обнаруживающую способность методов контроля на i -м этапе, в общем виде

$$K_{Ri} = \frac{P_{ei}^*}{P_{ei}},$$

где P_{ei}^* – значение P_{ei} при реализации контроля на i -м этапе;

$P_{k,o}$ – вероятность ложного срабатывания контрольного органа (схемы, программы, человека) на i -м этапе.

Случай коррекции без повторного контроля

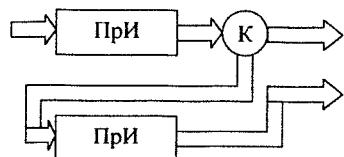
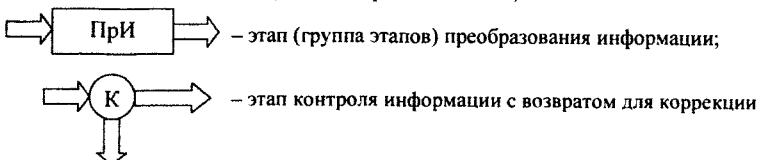


Рис. 1. Преобразование информации с контролем и коррекцией ошибок (без повторного анализа):



Случай коррекции путем повторного выполнения преобразования и контроля

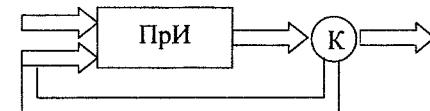


Рис. 2. Преобразование информации с контролем и коррекцией путем повторного преобразования и контроля:
обозначения см. на рис. 1.

В случае неизменности процедуры ожидания и выполнения на i -го этапа при обычном режиме сбора и при заполнении коррекции, т. е. при $T_{ei} = T_{ei}$ и $t'_{ei} = t_{ei}$, получим

$$[T_{ei}^*]_{cp} = t_{k,ei} + (T_{ei} + t_{ei})(1 + \sigma_{ei}).$$

Для обоих случаев среднее приращение времени выполнения i -го этапа (за счет реализации контроля и коррекции) $[\Delta T_{ei}]_{cp}$ составит

$$[\Delta T_{ei}]_{cp} = t_{k,ei} + (T_{ei} + t_{ei})\sigma_{ei}.$$

Если контролем охватывается группа последовательных преобразований, расчетные соотношения примут вид

$$T_{ei}^* = \begin{cases} t_{k,e} + \sum_{i=1}^{m_e} (\tau_{ei} + t_{ei}) & \text{при отсутствии возврата} \\ t_{k,e} + \sum_{i=1}^{m_e} (\tau_{ei} + t_{ei} + t'_{ei} + t''_{ei}) & \text{при возврате,} \end{cases}$$

$$[T_{ei}^*]_{cp} = t_{k,e} + \sum_{i=1}^{m_e} (\tau_{ei} + t_{ei}) + \sigma_e \sum_{i=1}^{m_e} (t'_{ei} + t''_{ei})$$

$$[\Delta T_{ei}]_{cp} = t_{k,e} + \sigma_e \sum_{i=1}^{m_e} (t'_{ei} + t''_{ei})$$

Время преобразования, контроля и коррекции единицы информации при d циклах коррекции (поскольку возможно много-

кратное, т. е. циклическое, возвращение единицы информации на преобразование и контроль) для i -го этапа $T_{e(i)}$ равно

$$T_{e(i)}^* = T_{ei} + t_{ei} + t_{kei} + d(T_{ei} + t'_{ei} + t_{kei}),$$

а среднее время завершения i -го преобразования с учетом процедуры коррекции составит

$$[T_{ei}]_{cp} = T_{ei} + t_{ei} + t_{kei} + \frac{\sigma_{ei}}{1 - \sigma_{ei}} (T_{ei} + t'_{ei} + t_{kei}), \quad (3)$$

где t'_{kei} – время выполнения контроля в режиме коррекции.

При $T_{ei} = T_e$, $t_{ei} = t_{ei}$, $t'_{kei} = t_{kei}$ и с учетом (1) получим:

$$T_{e(i)}^* = (d + 1)(T_{ei} + t_{ei} + t_{kei}) = (d + 1)T_e,$$

$$[T_{ei}]_{cp} = \frac{1}{1 - \sigma_{ei}} T_e. \quad (4)$$

Для группы из m_e этапов преобразования, охваченных одним контролем, получим:

$$\begin{aligned} T_{e(d)}^* &= t_{ke} + \sum_{i=1}^{m_e} (\tau_{ei} + t_{ei}) + d[t'_{ke} + \sum_{i=1}^{m_e} (\tau'_{ei} + t'_{ei})], \\ [T_e]_{cp} &= t_{ke} + \sum_{i=1}^{m_e} (\tau_{ei} + t_{ei}) + \frac{\sigma_{ei}}{1 - \sigma_{ei}} [t'_{ke} + \sum_{i=1}^{m_e} (\tau'_{ei} + t'_{ei})]. \end{aligned} \quad (5)$$

При $T_{ei} = T_e$, $t_{ei} = t'_{ei}$, $t'_{ke} = t_{ke}$ справедливы соотношения:

$$T_{e(d)}^* = (d + 1)[t_{ke} + \sum_{i=1}^{m_e} (\tau_{ei} + t_{ei})] = (d + 1)T_e,$$

$$[T_e]_{cp} = \frac{1}{1 - \sigma_e} [t_{ke} + \sum_{i=1}^{m_e} (\tau_{ei} + t_{ei})] = \frac{1}{1 - \sigma_e} T_e. \quad (6)$$

Если некоторый объем собираемой информации может делиться при коррекции на части (так как представляет собой партию из n_{part} единиц информации более низкого ранга), то будут справедливы следующие соотношения:

$$\begin{aligned} [T_{n(d)}^*]_{cp} &= \left\{ T_e + \frac{1 - \sigma_e^d}{1 - \sigma_e} \left[t'_{ke} + \sum_{i=1}^{m_e} (\tau'_{ei} + t'_{ei}) \right] \right\} n_{part}; \\ [T_n^*]_{cp} &= [T_e]_{cp} n_{part}, \end{aligned} \quad (7)$$

где $[T_{n(d)}^*]_{cp}$ – среднее время преобразования партии единиц информации (например, массива сообщений) с d циклами коррекции для составляющих партию единиц информации (например, сообщений);

$[T_n^*]_{cp}$ – среднее время завершения преобразования и коррекции для партии;

T_e – см. формулу (2).

Увеличение времени преобразования единицы первичной информации на i -м этапе, для группы из m_e этапов преобразования и среднее увеличение для партии из n_{part} единиц первичной информации при d циклах коррекции может быть оценено по следующим формулам:

$$\begin{aligned} \Delta T_{e(i)} &= d(T_{ei} + t'_{ei} + t_{kei}), \\ \Delta T_{e(d)} &= d[t'_{ke} + \sum_{i=1}^{m_e} (\tau'_{ei} + t'_{ei})], \\ [\Delta T_{n(d)}]_{cp} &= \frac{1 - \sigma_e^d}{1 - \sigma_e} \left[t'_{ke} + \sum_{i=1}^{m_e} (\tau'_{ei} + t'_{ei}) \right] n_{part}. \end{aligned}$$

Среднее увеличение времени завершения i -го преобразования единиц первичной информации, завершение группы из m_e преобразования для единицы информации и для партии из n_{part} единиц первичной информации может быть оценено

$$[\Delta T_e]_{cp} = \frac{\sigma_{ei}}{1 - \sigma_{ei}} (T_{ei} + t'_{ei} + t_{kei}), \quad (8)$$

$$[\Delta T_e]_{cp} = \frac{\sigma_e}{1 - \sigma_e} [t_{ke} + \sum_{i=1}^{m_e} (\tau'_{ei} + t'_{ei})]. \quad (9)$$

$$[\Delta T_n]_{cp} = [\Delta T_e]_{cp} n_{part}. \quad (10)$$

Во всех случаях (3)–(10) предполагается, что преобразование завершается при положительном результате контроля для всех единиц.

ниц первичной информации. В остальных случаях значение T_e^* ограничивается практически необходимым для получения требуемого уровня достоверности $[P_e^*]_{\text{зад}}$ числом циклов $d = d_{\text{зад}}$.

Случай последовательного выполнения группы этапов преобразования, контроля и коррекции информации при действии контроля и коррекции только в пределах своего этапа (рис. 3 и рис. 4)

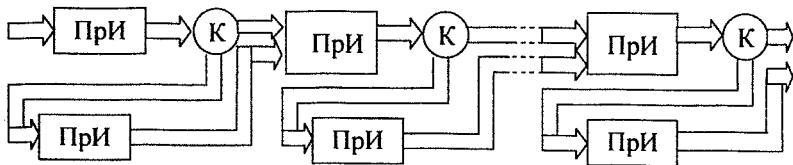


Рис. 3. Последовательное выполнение группы этапов преобразования, контроля и коррекции без повторного контроля (при выполнении контроля и коррекции только в пределах своего этапа)

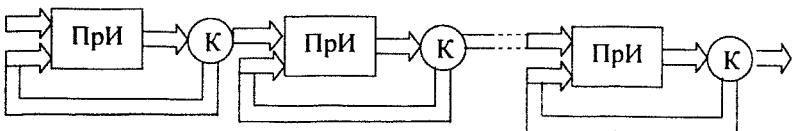


Рис. 4. Последовательное выполнение группы этапов преобразования, контроля и коррекции с повторным контролем (при выполнении контроля и коррекции только в пределах своего этапа)

Общая оценка $[T_e^*]_{\text{ср экв}}$ и $[\Delta T_e]_{\text{ср экв}}$ для подобных структур находится суммированием соответствующих оценок для i -х этапов $[T_{ei}^*]_{\text{ср}}$ и $[\Delta T_{ei}]_{\text{ср}}$, вычисляемых по формулам предыдущих вариантов (см. рис. 1 или рис. 2)

$$[T_e^*]_{\text{ср экв}} = \sum_{i=1}^{m_e} [T_{ei}^*]_{\text{ср}} \quad \text{и} \quad [\Delta T_e]_{\text{ср экв}} = \sum_{i=1}^{m_e} [\Delta T_{ei}]_{\text{ср}}.$$

Оценка этого случая может быть выведена путем последовательного рассмотрения цепочек из двух, трех, ... m_e этапов преобразования первичной информации при первом, втором, третьем ... d -м циклах (под циклом в данном случае будем понимать каждый запуск единицы информации на преобразование (рис. 5) вне зави-

симости от происхождения по всей цепочке или только по ее части). Опуская несложные, но громоздкие выкладки, приведем окончательные результаты.

Случай последовательного выполнения группы этапов преобразования и контроля информации с общей целью возврата и коррекции (рис. 5)

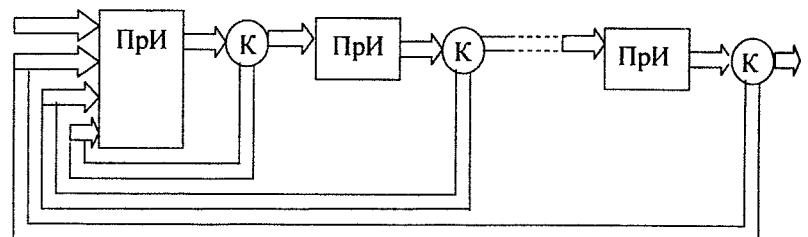


Рис. 5. Последовательное выполнение группы этапов преобразования и контроля с общей целью возврата и коррекции.

Вероятность возврата единицы информации на i -м этапе контроля в d -м цикле $P_{e(d)}^B$ может быть оценена по формуле

$$P_{e(d)}^B = (A_m)^a A_i,$$

где A_m и A_i – параметры, зависящие от числа этапов m_e и места i -го этапа в общей цепочке преобразований соответственно.

Эти параметры определяются соотношениями:

$$A_m = \sum_{i=1}^{m_e} R_i - \sum_{j < i}^{m_e} R_i R_j + \sum_{\xi < j < i}^{m_e} R_i R_j R_\xi - \dots + (-1)^{m_e-1} R_1 R_2 \dots R_{m_e}; \quad (11)$$

$$A_i = R_i - \sum_{j < i}^{i-1} R_i R_j + \sum_{\xi < j < i}^{i-1} R_i R_j R_\xi - \dots + (-1)^{i-1} R_1 R_2 \dots R_i, \quad (12)$$

где $R_i \leq [P_{e(1,i)} (1 - K_{R(1,i)} + P_{K,oi} [1 - P_{e(1,i)}])]$.

Здесь $P_{e(1,i)}$ – эквивалентная вероятность искажения единицы информации в результате ее прохождения через этапы преобразования с 1-го по i -й включительно; $K_{R(1,i)}$ – коэффициент редукции,

характеризующий способность реализуемого на i -м этапе метода повышения достоверности выявить ошибки, вносимые на этапе с i -го по i -й включительно [3].

Для упрощения оценок (11) и (12), учитывая, что $R_i < 1$, $R_j < 1$, $R_\xi < 1$, можно использовать верхние границы A'_m и A'_i :

$$A'_m = \sum_{i=1}^{m_e} R_i \geq A_m; A'_i = R_i \geq A_i.$$

Суммарное среднее время, затрачиваемое на i -е преобразование единицы первичной информации за m_e циклов $[T^*_{e(d)i}]_{cp}$, может быть оценено

$$[T^*_{e(d)i}]_{cp} \leq T'_{ei} + (\tau'_{ei} + t'_{ei} + t'_{k,ei}) \frac{1 - [A'_m]^\alpha}{1 - A'_m} A'_i. \quad (13)$$

Общие средние затраты времени за d циклов по всем этапам определяются соотношением

$$[T^*_{e(d)}]_{cp} \leq T'_{ei} + \sum_{i=1}^{m_e} (\tau'_{ei} + t'_{ei} + t'_{k,ei}) \frac{1 - [A'_m]^\alpha}{1 - A'_m} A'_i. \quad (14)$$

При малом числе m_e и d могут использоваться в (13) и (14) точные значения A_m и A_i . Значение среднего увеличения времени сбора $[\Delta T_{e(d)}]_{cp}$ определяется соотношением

$$[\Delta T_{e(d)}]_{cp} \leq \sum_{i=1}^{m_e} (\tau'_{ei} + t'_{ei} + t'_{k,ei}) \frac{1 - [A'_m]^\alpha}{1 - A'_m} A'_i.$$

Рассматривая этот вариант как сочетание случаев, представленных на рис. 2 и на рис. 3 или на рис. 4, можно расчеты для него вести по формулам, предложенным выше, но при этом в качестве T'_{ei} , T'_{e} использовать значение $[T^*_{e}]_{cp, экв}$ (см. выше).

Рассмотренные в данной работе расчетные формулы позволяют на этапе проектирования системы преобразования информации в ЭИС проводить оценку затрат времени на повышение достоверности преобразования информации и с учетом этого осуществлять

выбор наиболее рациональных вариантов обеспечения достоверности данных в процессе их преобразования в ЭИС.

Случай выполнения последовательности независимых этапов преобразования, контроля и коррекции с дополнительным общим контролем и коррекцией
(рис. 6)

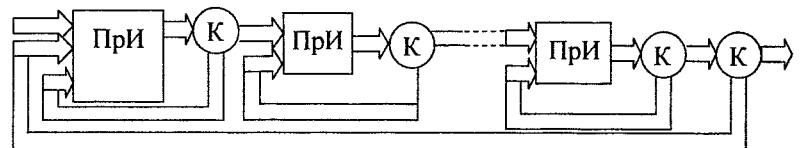


Рис. 6. Последовательное выполнение независимых этапов преобразования, контроля и коррекции с дополнительным общим контролем и коррекцией

УДК 62 – 50

М. А. Шапченко

Санкт-Петербургский государственный
инженерно-экономический университет

ИТ-СИСТЕМЫ УПРАВЛЕНИЯ НА ОСНОВЕ АУТСОРСИНГА

Развитие бизнеса, как правило, происходит двумя путями: укрупнением за счет слияния или поглощения либо тиражированием структуры бизнеса на другие территории (открытие филиалов и т. п.). Но в обоих случаях критическим моментом становится наложение единого управления всей разрастающейся структурой. Например, если до слияния на рынке существовало несколько бизнес-единиц, каждая из которых вела свои дела по-своему (осуществляла закупки, управляла бюджетом и т. п.), то после объединения необходимо определить единые стандарты, которые позволили бы идти ровным строем в заданном направлении.

Создание единого портала для всех подразделений компании, где можно было бы увидеть данные обо всей производственной цепочке, особенно актуально для управляющих компаний, имеющих дочерние структуры.

Сегодня строить управление по-старому, на основании данных, собираемых и обрабатываемых вручную, больше не представляется возможным. Поэтому структуры, которые, вероятно, раньше и не думали о внедрении на корпоративном уровне систем класса ERP (Enterprise-Resource Planning – планирование ресурсов предприятия), СЭД (система электронного документооборота), BPM (Business Process Management – системы управления бизнес-процессами), все чаще в момент реорганизации или развития разворачивают у себя такие проекты.

Без использования современных систем управления сложно не только выйти на западные рынки, но и даже публично предложить свои акции посредством IPO; ведь компании придется иметь дело с аудиторами, привыкшими к определенным нормам в управлении.

Все предприятия идут по стандартному пути: сначала оснащают бизнес техникой, потом – информационными системами. Все начинается с установки бухгалтерских систем, потом, по мере роста, когда весь производственный процесс уже невозможно отследить только бухучетом, возникает потребность в системах управления, защиты информации, развития сетевой инфраструктуры, доступа к информационным ресурсам.

Для решения целевых бизнес-задач и минимизации финансовых потерь компании занимаются расширением, обновлением ИТ-продуктов, установкой нового, более мощного программного обеспечения. Необходимый набор включает в себя системы бухгалтерского и управленческого учета, поддерживающие особенности многофилиальных структур, системы документооборота, позволяющие наладить быстрое распространение и эффективный контроль управленческих решений, системы удаленного администрирования и поддержки пользователей, системы управления ИТ-инфраструктурой. Этот список дополняют системы видеоконференций, АТС новых поколений, управляющие входящими/исходящими звонками и обеспечивающими сохранение и анализ информации о переговорах с клиентами.

Наиболее серьезными и стабильными потребителями ИТ-технологий являются государственный сектор, розничная торговля, нефтяные и энергетические компании. В этих отраслях есть деньги и высока потребность в информации, необходимой для эффективного управления.

Скорость внедрения ИТ-технологий напрямую связана с финансовыми возможностями компаний, ведь ломка сложившейся структуры управления – вещь недешевая.

Наибольший интерес к развитию своей информатизации проявляют компании из нефтедобывающей и нефтеперерабатывающей промышленности и автомобилестроения. Так, сейчас компания «СофтИнтегро» выполняет проект по построению единой системы электронного документооборота для группы «КамАЗ».

Рынок ИТ-технологий растет и, несомненно, будет продолжать наращивать объем. При этом процесс сопровождается не только количественными, но и качественными изменениями. Сегодня заказчики предпочитают целостные решения по созданию единой структуры в координации действий. Даже небольшие компании, может быть, и не имеющие пока достаточных материальных ресурсов, проявляют интерес к внедрению систем управления. Для них выходом становится модель на основе СЭД, если она имеет в качестве ядра систему автоматизации документооборота или технологического процесса (Work Flow system). СЭД – наиболее доступная по цене программа, к тому же не очень сложная в использовании.

На развитие рынка систем управления бизнесом влияет и количество компетентных ИТ-компаний. Отнюдь не любая фирма может заниматься предоставлением таких услуг. Нужно иметь не только высококвалифицированных специалистов, но и налаженный бизнес-процесс, обладать мобильностью. Функции по внедрению и поддержке ИТ-системы в принципе должны выполнять не ее специалисты, а специализированные компании на основе аутсорсинга. Только таким образом можно оптимально решить проблемы и сохранить средства.

Аутсорсинг предполагает передачу внешним подрядчикам отдельных бизнес-функций – как правило, являющихся вспомогательными или непрофильными для компании. Фактически аутсорсинг является развитием принципа разделения труда: вы передаете непрофильные, поддерживающие процессы на исполнение организации, для которой они являются профильными.

Приобретающий сегодня все большую популярность ИТ-аутсорсинг – это передача внешнему исполнителю функций по созданию и управлению ИТ-инфраструктурой торговой компании, в том числе:

- администрирование и поддержка баз данных;
- организация, администрирование и поддержка локальных сетей в офисе заказчика;
- создание, администрирование и поддержка Интернет-ресурсов;
- создание, администрирование и поддержка почтовой системы;
- обеспечение защиты информационных ресурсов компании;
- устранение сбоев в работе информационных систем;
- ремонт и обслуживание компьютеров, периферийного и электронного оборудования;
- поддержка и консультирование пользователей;
- техническое обслуживание оборудования и ИТ-инфраструктуры в офисе заказчика.

Преимущества аутсорсинга очевидны.

Необходимая составляющая затрат на обеспечение деятельности любого предприятия – это затраты не только на основной бизнес, но и на управление непрофильными процессами, которые не приносят прибыли, но жизненно необходимы для нормальной работы любой компании.

Уделять слишком большое внимание непрофильным активам, стремясь достичь в этой области высокого качества, – занятие, отнимающее слишком много времени и сил у менеджмента предприятия и требующее довольно значительных финансовых вложений. Например, информационные технологии для торговой компании не являются профильными функциями и не позволяют максимально сосредоточиться на основном бизнесе. Аутсорсинг же позволяет оптимизировать соответствующие затраты.

Компания, работающая на высококонкурентном рынке, становится более эффективной при использовании аутсорсинга не являющихся ключевыми процессов, так как внешний подрядчик благодаря своему опыту и технологиям способен обеспечить развитие и оптимизацию переданных непрофильных активов на более высоком и качественном уровне.

Кроме того, ИТ-аутсорсинг позволяет:

- сфокусировать внимание на основной деятельности компании;
- высвободить внутренние ресурсы менеджмента для достижения стратегических целей;

- упростить организационную структуру и улучшить управляемость компании в целом;
- контролировать операционные расходы, обеспечить прозрачность и управляемость расходов на ИТ-инфраструктуру;
- привлечь для выполнения работ высококвалифицированных специалистов;
- обеспечить непрерывность бизнес-процессов;
- разделить и минимизировать риски, в том числе связанные с человеческим фактором.

Литература

1. Рубцов С. В. Целевое управление в корпорациях. Управление изменениями. М., 2001.
2. [Электронный ресурс]: itocom.ru/

УДК 338.314

А. И. Ястребов

Санкт-Петербургский государственный
инженерно-экономический университет

УЧЕТ РИСКОВ, ВОЗНИКАЮЩИХ В ПРОЦЕССЕ ДЕЯТЕЛЬНОСТИ ВИРТУАЛЬНЫХ ПРЕДПРИЯТИЙ В МОДЕЛИ ОЦЕНКИ СТОИМОСТИ

На Западе давно уже стало популярным управлять стоимостью компаний для собственников, ориентируясь на ее увеличение. В конечном итоге, этим достигается рост благосостояния всех членов общества. Действительно, преимущества использования стоимости в качестве критерия принятияправленческих решений не только видны из теории, но и неоднократно подтверждены практикой. Сейчас все больше компаний начинают управлять своей стоимостью, закладывая в свои планы требование ее увеличения.

Кроме того, произошедшие за последние десятилетия изменения в мировой экономике позволяют говорить о некотором смеше-

ний приоритетов ведения бизнеса. Традиционные виды экономической деятельности переносятся в сетевую среду и приобретают некоторые новые свойства, например, меняются правила игры, степень информированности участников и др.

На сегодняшний день не выработано однозначного подхода к определению понятия «виртуальное предприятие», однако все сходятся на том, что бизнес-процессы на таких предприятиях координируются электронными средствами по таким сетям, как Интернет.

Наряду с преимуществами, присущими виртуальному бизнесу, он характеризуется также повышенным уровнем риска, вызванным:

- чрезмерной экономической зависимостью от партнеров, связанной с узкой специализацией членов сети;
- практическим отсутствием социальной и материальной поддержки своих партнеров, вызванным отказом от долгосрочного взаимодействия;
- опасностью чрезмерного усложнения, вытекающей, в частности, из разнородности членов предприятия, открытости сетей;
- утратой компетенции в областях, в которых заняты партнеры;
- утратой близости к потребителю;
- отсутствием жесткой структуры предпринимателя;
- различными целями организаций-участников.

В связи с этим одно из основных мест в ходе процесса оценки стоимости виртуального предприятия следует уделять выявлению факторов риска и оценке воздействия последних на показатели деятельности компании.

Приступая к оценке рисковой среды, в которой реализуется сетевой проект, необходимо определить основные виды риска, которые представляют наибольшую опасность. Понятие риска есть субъективное понятие, отражающее отношение субъекта к неопределенности результата.

В рамках теории финансового менеджмента принято разделение риска на две составляющие: систематический риск и несистематический риск.

1. Систематический риск обусловлен факторами, влияющими на весь рынок в целом, такими как изменения в национальной экономике, проводимые правительством реформы, изменение тенденций в мировой экономике.

2. Несистематический риск характерен для конкретной отрасли или компании; он не зависит от экономических, политических и других факторов, оказывающих систематическое влияние на развитие различных процессов в бизнес-среде.

Деятельность виртуального предприятия подвержена воздействию как систематических, так и несистематических рисков. При этом если систематические риски одинаковы для всех предприятий, то несистематические риски имеют свою специфику в рамках сетевой экономики.

В связи с многообразием несистематических рисков в сетевой экономике, которые могут оказывать воздействие на исследуемую среду, можно выделить несколько наиболее значащих для исследуемого процесса рисков и оценить их воздействие. Данный подход базируется на предположении о том, что получение информации сопряжено с финансовыми затратами. Другими словами, потребление информации, снижающей риск, можно рассматривать как инвестиционные решения, влияющие на стоимость проекта. Таким образом, оценка ограниченного набора рисков является одним из путей снижения затрат.

С точки зрения рационального поведения инвестор будет оценивать тщательнее всего тот вид риска, который он будет стараться избежать в наибольшей степени. Инвестор будет меньше уделять внимания тому виду риска, в управлении которым он имеет определенный опыт.

В качестве базового при оценке стоимости виртуальных предприятий целесообразно применять метод дисконтирования будущего денежного потока, поскольку он позволяет учитывать нематериальные активы, которые доминируют в виртуальных предприятиях. Кроме того, применение данного метода позволяет просчитать несколько вариантов развития бизнеса.

Расчеты по методу дисконтированного будущего денежного потока ведутся по формуле

$$C_n = \sum_{i=1}^n D_i r_i + C_{\text{рев}} r_{\text{рев}},$$

где C_n – стоимость бизнеса;

D_i – денежный поток в i -м периоде владения объектом собственности;

r_i – ставка дисконта по i -му периоду;

$C_{\text{рев}}$ – стоимость реверсии, т. е. выручки от продажи бизнеса за первый год постпрогнозного периода;

$r_{\text{рек}}$ – ставка рекапитализации.

Поскольку метод дисконтированных денежных потоков предполагает наличие известных прогнозных значений потока прибыли, то оценка прогнозируемого потока будет являться одним из наиболее важных этапов определения стоимости виртуального предприятия.

Прогноз будущих доходов и расходов является достаточно сложной задачей. Значительные трудности представляет прогнозирование соответствующих показателей абсолютно нового продукта, как это происходит при функционировании виртуальных предприятий. Прогноз требует учета множества различных факторов, особенно на ранних стадиях только что образованного предприятия или начатого проекта, когда отсутствуют какие-либо ретроспективные данные. При этом, в силу сложности природы неопределенности условий, в которых развивается виртуальное предприятие, можно говорить только об оценке тех или иных показателей, которые в итоге будут преобразованы в показатель оценки коммерческой выгоды от проекта – оценку величины перспективной стоимости виртуальной компании.

Чаще всего прогнозные данные представлены в виде дискретных величин, составляющих денежный поток. Так как проекты виртуальных организаций обычно представляют собой инвестиции в среднем на 5–7 лет, то прогноз значений предполагает охват всего заданного временного горизонта. При этом, если на начальных этапах величина ошибки прогноза может быть незначительной, то с течением времени она будет возрастать, что объясняется ростом неопределенности относительно будущих условий реализации проекта. Для решения данной проблемы в ходе моделирования необходимо использовать методы количественного учета рисков.

Первичной задачей оценки риска является выявление основных факторов, способных оказать положительное или отрицательное влияние на развитие проекта. По мере их выявления встает задача количественной оценки влияния данных факторов на характеристики процесса, конечный результат, эффективность и иные величины.

С данных позиций методики экспертной оценки не являются совершенными, так как не учитывают фактор неопределенности. Одним из способов решения проблемы является введение элемента стохастичности, что выражается в оценке вероятностей достижения различного уровня результатов по каждому из оцениваемых критериев. Таким образом, экспертные методы в большей степени ориентированы на формирование качественной оценки.

Неопределенность возникновения риска учитывается в статистических методах оценки. В рамках данной методики рассматривают два подхода.

1. Вычисление риска как вероятности неблагоприятного результата – это статистическая задача моделирования сложных систем. Реализация данного метода возможна при наличии соответствующих статистических данных о реализации аналогичных проектов в отрасли, сегменте рынка и т. д.

2. Анализ влияния факторов на реализацию проекта базируется на оценке распределения значений исследуемых характеристик процесса и изменения их параметров при возникновении рисковой ситуации.

Оценка непосредственного влияния факторов риска также производится и в ходе анализа чувствительности (состоит в определении связи между исходными данными расчетных моделей и значениями целевых функций), основным недостатком которого является предположение о стационарном характере неанализируемых величин.

Развитием данного метода является сценарный подход, основным достоинством которого является возможность оценить одновременное влияние нескольких параметров на конечный результат.

Среди методов количественной оценки рисков в литературных источниках выделяют также метод иерархической декомпозиции (предполагает создание иерархической модели выбора), метод аналогий (оценка риска производится путем сравнения средней величины уровня риска сопоставимых компаний), метод критических значений (заключается в нахождении условий и факторов развития фирмы, приводящих расчетную величину к критическому значению).

Следующим этапом управления риском является учет рисковых показателей в создаваемой модели оценки стоимости.

Одним из наиболее распространенных методов учета риска в модели является внесение его в виде рисковой надбавки в ставку дисконтирования. Расчет ставки, помимо включения в нее всех рисковых составляющих, требует также учета эффекта уменьшения неопределенности с течением времени. В рамках реализации данного подхода предлагается использование переменной ставки дисконтирования при оценке стоимости бизнеса.

Практика оценки бизнеса в условиях нестабильной доходности предполагает два альтернативных варианта использования данного подхода.

1. Учет рисков бизнеса осуществляется посредством применения метода сценариев, с помощью которого в меньшую сторону корректируются прогнозируемые по бизнесу денежные потоки. По оцениваемому бизнесу выделяют некоторые ключевые факторы риска в сценарном разрезе и применительно к ним пересчитывают компоненты денежных потоков.

2. Периодическое увеличение ставки дисконтирования на премию, компенсирующую риски оцениваемого бизнеса. Оценка ставки возможна с двух позиций: через метод аналогии и использование модели оценки капитальных активов.

Метод аналогий предполагает наличие ликвидного актива, количественная мера риска инвестиций в который сопоставима с мерой риска инвестирования в оцениваемый бизнес. Задача учета будущего изменения ставки сводится к прогнозированию на основе имеющегося тренда будущих доходностей актива, которые будут служить переменной ставкой дисконтирования.

Сущность метода корректировки параметров проекта состоит в страховании от возможного неблагоприятного развития событий путем введения в расчет преувеличенных затрат, уменьшения доходов по сравнению с наиболее вероятной их величиной.

К данным методам также можно отнести модели оценки эффективности проекта, базирующиеся на анализе рисковых затрат. Наиболее распространеными среди них являются:

- модель оценки эффективности проекта (учитывает возможную структуру антирисковых мероприятий);
- модель оптимизации интегральных рисковых затрат (позволяет оценить ожидаемую величину валовых затрат на предотвращение риска проекта);

– модель оптимизации интегральных внешних и внутренних рисковых затрат.

Приведенные факторные модели ориентированы на сценарный подход к оценке результатов проекта, что требует оценки вероятности наступления того или иного исхода. Вероятностные характеристики используются в моделях в качестве весовых коэффициентов при оцененных факторах. Основная трудность применения моделей состоит в оценке вероятностных характеристик. Для их расчета чаще всего используются методы экспертных оценок.

При этом метод корректировки также характеризуется рядом недостатков. При корректировке возможен учет надежных величин, что искажает результат. Кроме того, не раскрываются последствия изменений в величинах, от которых страхи инвестор.

Методы, основанные на использовании теории нечетких множеств, позволяют преодолеть недостатки вероятностного подхода, связанные с учетом неопределенности. Основные достоинства метода, базирующегося на теории нечетких множеств, заключаются в следующем:

- становится возможным сформировать достаточно полный набор сценариев протекания жизненного цикла предприятия;
- окончательное инвестиционное решение принимается не на основе двух оценок эффективности проекта (максимальной и минимальной), а по всей совокупности возможных оценок;
- ожидаемая эффективность бизнес-проекта не является однозначным показателем, а представляет собой некий интервал значений. Взвешенная полная совокупность ожиданий позволяет получить интегральную меру ожиданий отрицательных результатов в ходе реализации проекта.

Таким образом, проведенный анализ показал, что для достижения наибольшей точности при оценке стоимости виртуальных предприятий методом дисконтирования будущих денежных потоков необходимо учитывать многочисленные риски, присущие сетевому бизнесу. Для этого в ходе моделирования денежных потоков необходимо ввести раздельный учет рисков. Так, на основе методов, базирующихся на теории нечетких множеств, предлагается учитывать несистематические риски, такие как специфические риски проекта или компании, а систематический риск и риски, общие для проектов в отрасли деятельности компаний, внести в ставку дисконтирования.

Раздел 2

**ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
ЗАЩИТЫ ДАННЫХ**

УДК 378.001.658.011.56

И. Н. Васильева

Санкт-Петербургский государственный
инженерно-экономический университет

**ПРАВОВЫЕ ОСНОВЫ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
И ЗАЩИТЫ ИНФОРМАЦИИ В РОССИИ**

Обеспечение информационной безопасности отдельных граждан, предприятий, организаций, так же, как и обеспечение национальной безопасности в информационной сфере, требует законодательной поддержки на государственном уровне. К правовым мерам обеспечения информационной безопасности относится разработка специализированных нормативно-правовых актов (законов, постановлений и т. п.), а также нормативно-методических и нормативно-технических документов (в первую очередь, стандартов обеспечения безопасности).

В 1990-х гг. защита информации трактовалась, в основном, как защита конфиденциальности тех или иных сведений, что отразилось и на правовом обеспечении этой сферы. Информационную безопасность, согласно логике Закона РФ от 05.04.92 № 2446-І «О безопасности», можно понимать, как состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз. Вопросы информационной безопасности регулировались законами РФ «О безопасности», от 21.07.93 № 5485-І «О государственной тайне»; кроме того, в различных законах и кодексах перечислялось около 40 различных видов тайн. Нормативно-техническая и нормативно-мето-

дическая база защиты информации сводилась к рассмотрению проблеме утечки и защиты конфиденциальной информации от несанкционированного доступа (ГОСТ Р 50739–95, ГОСТ 50922–96, руководящие документы Гостехкомиссии по защите от несанкционированного доступа к информации) и стандартизации алгоритмов шифрования (ГОСТ 28147–89, ГОСТ Р 34.10–94, ГОСТ Р 34.11–94). Исключение составляет, пожалуй, лишь стандарт, касающийся компьютерных вирусов (ГОСТ Р 51188–98).

Нормы одних правовых актов (даже на уровне законов и кодексов) зачастую не соответствовали другим, отсутствовал единый понятийный аппарат, в ряде случаев в законах использовались понятия без четкого их определения. Например, термин «коммерческая тайна» встречался более чем в 30 законах, «служебная тайна» – в 12 законах, при этом законы, собственно регламентирующие правовые режимы коммерческой и служебной тайн, так и не были приняты. Еще большая путаница была связана с понятием конфиденциальной информации, состав которой в разных законодательных актах трактовался по-разному, так что в 1997 г. Президент Российской Федерации издал указ, утверждающий перечень сведений конфиденциального характера (№ 188 от 06.03.97).

Принятый в 1995 г. Федеральный закон от 24.02.95 № 24-ФЗ «Об информации, информатизации и защите информации», предназначенный регламентировать отношения в сфере обеспечения информационной безопасности и защиты информации, так и не привел к созданию стройной правовой системы в этой области.

Следует отметить также декларативность большинства норм, за нарушение которых не предусматривалось никакой ответственности.

В целом на тот период времени в достаточной степени урегулированными были лишь вопросы охраны государственной тайны. Не получили достойного отражения в законодательстве такие группы правоотношений, как право граждан на доступ к информации и защита информации ограниченного доступа (кроме государственной тайны): коммерческой, служебной тайн, персональных данных. Хотя права граждан на охрану личной тайны продекларированы в Конституции РФ (ст. 23, 24), а правовые режимы личной и семейной тайны закреплены в Гражданском кодексе РФ (ст. 150), вопросы охраны персональных данных так и не были урегулированы

специальным законом, принятие которого предусматривалось законом «Об информации, информатизации и защите информации».

В российских нормативно-технических документах не были отражены такие важные аспекты защиты информации, как обеспечение целостности и доступности информационных ресурсов.

Растущая роль информационных технологий, тенденции усиления государственного регулирования в информационной сфере в мировом масштабе не могли оставить в стороне и Россию, что привело к разработке нового информационного законодательства. Поворотным пунктом стало утверждение в 2000 г. «Доктрины информационной безопасности Российской Федерации» от 09.09.2000 № Пр-1895.

«Доктрина» вводит понятие информационной безопасности Российской Федерации как состояния защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства. Таким образом, «Доктрина» развивает концепцию национальной безопасности применительно к информационной сфере и служит основой для трех направлений:

- формирование государственной политики в области обеспечения информационной безопасности Российской Федерации;
- подготовка предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;
- разработка целевых программ обеспечения информационной безопасности Российской Федерации, а также развитие отечественной информационной инфраструктуры.

Еще одним импульсом стало принятие Федеральной целевой программы «Электронная Россия» (концепция использования информационных технологий в деятельности федеральных органов государственной власти), рассчитанной на 2002–2010 гг. Цель программы – повышение эффективности государственного управления на основе использования информационных технологий. К 2010 г. планируется:

- внедрить системы электронного документооборота во всех федеральных органах власти и обеспечить совместимость ведомственных информационных систем;

специальным законом, принятие которого предусматривалось законом «Об информации, информатизации и защите информации».

В российских нормативно-технических документах не были отражены такие важные аспекты защиты информации, как обеспечение целостности и доступности информационных ресурсов.

Растущая роль информационных технологий, тенденции усиления государственного регулирования в информационной сфере в мировом масштабе не могли оставить в стороне и Россию, что привело к разработке нового информационного законодательства. Поворотным пунктом стало утверждение в 2000 г. «Доктрины информационной безопасности Российской Федерации» от 09.09.2000 № Пр-1895.

«Доктрина» вводит понятие информационной безопасности Российской Федерации как состояния защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства. Таким образом, «Доктрина» развивает концепцию национальной безопасности применительно к информационной сфере и служит основой для трех направлений:

- формирование государственной политики в области обеспечения информационной безопасности Российской Федерации;
- подготовка предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;
- разработка целевых программ обеспечения информационной безопасности Российской Федерации, а также развитие отечественной информационной инфраструктуры.

Еще одним импульсом стало принятие Федеральной целевой программы «Электронная Россия» (концепция использования информационных технологий в деятельности федеральных органов государственной власти), рассчитанной на 2002–2010 гг. Цель программы – повышение эффективности государственного управления на основе использования информационных технологий. К 2010 г. планируется:

- внедрить системы электронного документооборота во всех федеральных органах власти и обеспечить совместимость ведомственных информационных систем;

– придать официальный статус (с помощью использования электронной цифровой подписи) электронным формам взаимодействия как межведомственного, так и в случае обращений граждан;

– разработать стандарты, регламентирующие порядок и процедуры сбора, хранения и безопасной обработки информации в государственных информационных системах.

В 2002 г. приняты федеральные законы «Об электронной цифровой подписи» от 10.01.02 № 1-ФЗ, «О техническом регулировании» от 27.12.02 № 184-ФЗ, в 2004 – «О коммерческой тайне» от 29.07.04 № 98-ФЗ. В 2005 г. Россияratифицировала Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 19.12.05 № 160-ФЗ.

В 2004 г. реформированы две основные структуры, традиционно отвечающие за информационную безопасность: ФАПСИ и Гостехкомиссия России. ФАПСИ переведена в состав ФСБ, а Гостехкомиссия России преобразована в Федеральную службу по техническому и экспортному контролю (ФСТЭК). В 2005–2006 гг. российское правительство плотно взялось за создание и совершенствование законодательства в сфере информационных технологий и информационной безопасности, немалую роль в этом процессе сыграл и Комитет по безопасности Государственной Думы Российской Федерации.

В июле 2006 г. был принят основополагающий в сфере информационной безопасности и защиты информации Федеральный закон от 27.07.06 № 149-ФЗ «Об информации, информационных технологиях и защите информации», пришедший на смену старым законам «Об информации, информатизации и защите информации» № 24-ФЗ от 24.02.95 и «Об участии в международном информационном обмене» № 85-ФЗ от 04.07.96. Новый закон более согласован внутренне, имеет более четкую логическую структуру, приведен в соответствие с современным развитием информационных технологий и актуальными проблемами информационной безопасности, а также отражает общие тенденции ИТ-законодательств стран Евросоюза и США. Закон регламентирует вопросы реализации права на доступ и ограничения доступа к информации, государственного регулирования в информационной сфере.

Новый закон определяет информацию как сведения (сообщения, данные) независимо от формы их представления. Информация,

в зависимости от категории доступа, подразделяется на общедоступную и ограниченного доступа (ст. 5). При этом ограничения доступа к информации может быть установлено только федеральными законами (ст. 3; 5).

Отдельное определение конфиденциальной информации не вводится, поэтому, по логике нового закона, под конфиденциальной можно понимать любую информацию, конфиденциальность которой соблюдается согласно действующему законодательству. Это фактически синоним информации ограниченного доступа, поскольку, согласно ст. 9, соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами, является обязательным.

Федеральными законами регулируется правовой режим государственной, коммерческой, служебной, различных видов профессиональной (например, банковской, адвокатской, нотариальной, врачебной, налоговой и др.) и иных видов тайн, а также персональных данных.

Закон определяет права на доступ к информации и перечень сведений, доступ к которым не может быть ограничен (ст. 7; 8).

Таким образом, определены следующие режимы доступа к информации (рис. 1).

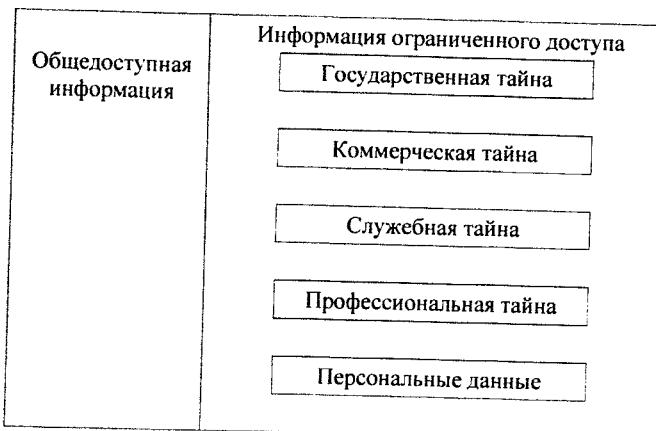


Рис. 1. Правовые режимы доступа к информации в Российской Федерации

При этом обеспечение конфиденциальности служебной и коммерческой тайн (ст. 139 ГК РФ Закона «О коммерческой тайне») возложено прежде всего на ее обладателя – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к ней. В общем случае защита информации возлагается на обладателя и оператора информационной системы – гражданина или юридическое лицо, занимающееся обработкой информации с помощью информационной системы (ст. 16).

Закон предусматривает право лиц на защиту в судебном порядке своих прав, законных интересов и компенсацию вреда, связанные с разглашением информации ограниченного доступа. Однако возмещение убытков не может быть удовлетворено в случае предъявления их лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные законодательством Российской Федерации требования о защите информации (ст. 17).

Защита информации определена в новом законе (ст. 16) более полно и не сводится только к обеспечению конфиденциальности – это принятие правовых, организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модификации, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

- соблюдение конфиденциальности информации ограниченного доступа;

- реализацию права на доступ к информации.

В случаях, установленных законодательством Российской Федерации, обладатель информации, оператор информационной системы обязаны обеспечить:

- предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

- своевременное обнаружение фактов несанкционированного доступа к информации;

- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- постоянный контроль за обеспечением уровня защищенности информации.

Закон вводит ограничение на использование программно-технических средств, предназначенных для обработки и защиты информации, содержащейся в государственных информационных системах (ст. 14; 16). Эти средства должны отвечать требованиям законодательства Российской Федерации о техническом регулировании (Закон «О техническом регулировании», Постановление Правительства РФ от 26.06.95 № 608 «О сертификации средств защиты информации», Указ Президента РФ от 12.05.04 № 611 «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена»).

Федеральными законами могут быть установлены ограничения использования средств защиты информации и осуществления отдельных видов деятельности в области защиты информации (Закон от 08.08.01 № 128-ФЗ «О лицензировании отдельных видов деятельности»), а порядок лицензирования определяется Правительством РФ (постановления Правительства РФ от 23.09.02 № 691 «Об утверждении Положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами», от 15.08.06 № 504 «О лицензировании деятельности по технической защите конфиденциальной информации», от 31.08.06 № 532 «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации»).

За стандартизацию и сертификацию в области обеспечения информационной безопасности отвечают две государственные структуры: ФСБ и ФСТЭК, полномочия которых определены указами Президента РФ от 27.01.06 № 799 и от 30.11.06. № 1321. ФСБ

отвечает за криптографические средства и безопасность конфиденциальной информации в высших органах государственной власти, ФСТЭК – за некриптографическую защиту.

Нарушение требований закона «Об информации, информационных технологиях и защите информации» влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации (ст. 17).

Наряду с существующими ранее законами «О государственной тайне», «О средствах массовой информации», законодательстве об архивном фонде РФ и архивах и уже упомянутых законах «Об информации, информационных технологиях и защите информации», «Об электронной цифровой подписи» и «О коммерческой тайне» принят ряд важных для развития информационных технологий и обеспечения информационной безопасности законодательных актов:

- Закон от 27.07.06 № 152-ФЗ «О персональных данных», вступивший в силу 26.01.07;
- новые кодексы Российской Федерации: Трудовой, Гражданский (особенно интересна ч. IV Гражданского кодекса от 18.12.06 № 230-ФЗ, вступившая в действие 01.01.08, в которой заметное место отведено использованию компьютерных технологий), Уголовный (глава 28 которого посвящена преступлениям в сфере компьютерной информации) и Административный;
- в 2007 г. Россией ратифицирована Конвенция ООН об использовании электронных сообщений в международных договорах;
- рассматривается проект Федерального закона РФ «О служебной тайне».

Таким образом, в настоящее время правовое поле в области защиты информации получило весомое дополнение.

Проблема утечек персональных данных остро стоит во всем мире. Так, по утверждениям Privacy Right Clearinghouse, Информационного центра по защите прав на конфиденциальную информацию, утечки данных из университетов, правительственные учреждений и компаний стали обыденным явлением в США, а по сведениям arstechnica.com, за последние три года от утечек, связанных со взломами или кражей физических носителей, пострадала примерно

половина населения страны; не лучше обстоит дело и в Европе – в октябре 2007 г. произошла крупнейшая утечка персональных данных в Европе, когда правительство Великобритании потеряло два диска с данными о 25 млн родителей, получающих пособия на детей. Однако нелегальный оборот информации в России стал уже «притчей во языцах», поэтому принятие закона о защите персональных данных было встречено с удовлетворением.

Принятие данных законодательных актов направлено на реализацию конституционных положений, закрепляющих право каждого на неприкосновенность частной жизни и свободу информации, а также международных обязательств Российской Федерации по ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных.

Под персональными данными понимается информация, для которой можно определить, какому физическому лицу она принадлежит: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и другая информация.

Хотя многие виды профессиональной тайны (банковская, врачебная, адвокатская, тайна нотариальных действий и т. п.) в отношении физических лиц тесно связаны с персональными данными, их правовые режимы не совпадают. Персональные данные являются тайной «первичной», а профессиональная тайна – «вторичной». Профессиональная тайна (в отношении сведений о гражданах) не является личной тайной, а призвана быть одной из гарантий защиты личной, семейной тайны, сохранности персональных данных, т. е. представляет собой особый режим информации с ограниченным доступом [4].

Согласно Закону РФ «О персональных данных» для обработки персональных данных требуется письменное согласие субъекта персональных данных за исключением случаев, предусмотренных действующим законодательством, а также, если данные используются в целях исполнения договора, предоставления услуг связи либо для защиты жизни и здоровья. Письменное согласие требуется и для публикации персональных данных в общедоступных источниках. При этом человек может отозвать согласие на обработку или публикацию своих персональных данных. Согласия и обеспечения

конфиденциальности не требуется, если персональные данные были обезличены (например, для статистических исследований).

В сферу действия Закона РФ «О персональных данных» попадают все юридические и физические лица, на попечении которых находятся приватные сведения других граждан. Новый закон требует, чтобы каждая организация, владеющая персональными данными своих сотрудников, клиентов, партнеров и т. д., обеспечила конфиденциальность этой информации. Согласно ст. 19 оператор при обработке персональных данных обязан принимать необходимые организационные [3] и технические меры, в том числе использовать шифровальные (криптографические) средства для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Вместе с тем российским законодательством, в отличие от законодательств Великобритании и США, не предусмотрено обязательное информирование о произошедших утечках персональных данных. Поэтому об утечках из российских фирм и организаций практически ничего не известно, хотя никто не сомневается в том, что они есть.

Несмотря на то что проблема защиты персональных данных в России наболела уже давно, принятие нового закона само по себе эту задачу не решает. Закон предъявляет лишь формальные требования к безопасности личной информации, за разработку необходимой нормативной и методической базы к закону отвечает Правительство Российской Федерации. Постановлением Правительства РФ от 17.11.07 № 781 утверждено «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», содержащее список мероприятий, проведение которых должно обеспечивать безопасность персональных данных при их обработке, размещении и обмене. Разработка методов и способов защиты в информационных системах возложена на ФСТЭК и ФСБ России.

Функции по контролю за соответствием Закону РФ «О персональных данных» возложены Постановлением Правительства РФ от 15.12.07 № 878 «О некоторых вопросах деятельности Федеральной службы по надзору в сфере массовых коммуникаций, связи и

охраны культурного наследия» на указанное ведомство (Россвязьохранкультуры). Это ведомство создает реестр операторов персональных данных. С 01.01.08 не вошедшие в реестр организации и лица не вправе обрабатывать персональные данные.

Понятно, что для реализации требований закона многие организации будут вынуждены модернизировать свою информационную инфраструктуру, причем, согласно опросам (InfoWatch и SecurityLab, 2007), примерно для половины опрошенных организаций эти изменения могут быть весьма значительными [2]. Существующие информационные системы обработки персональных данных должны быть приведены в соответствие с Законом РФ «О персональных данных» до 1 января 2010 г., и именно с этого времени закон должен заработать в полную силу.

Однако уже сейчас гражданин, если безопасность его персональных данных нарушена, может рассчитывать на правовую защиту. Закон «О персональных данных» предусматривает гражданскую, уголовную, административную и дисциплинарную ответственность оператора (ст. 24).

Трудовой кодекс Российской Федерации предусматривает, что лица, виновные в нарушении норм, регулирующих обработку и защиту персональных данных работника, могут быть привлечены к дисциплинарной и материальной, гражданско-правовой, административной и уголовной ответственности (ст. 90 ТК РФ). Виновнику можно привлечь к дисциплинарной или материальной ответственности в порядке, установленном ТК РФ и федеральными законами, а к гражданско-правовой, административной и уголовной ответственности – в порядке, установленном федеральными законами (ст. 90 ТК РФ).

Сотрудник, разгласивший охраняемую законом тайну (к которой относятся и персональные данные), может быть уволен (ст. 81 ТК РФ). В случае других нарушений в рамках ТК на него может быть наложено иное дисциплинарное или материальное взыскание.

Административная ответственность может наступить в случаях нарушения порядка обработки персональных данных (ст. 13.11 КоАП РФ), разглашения конфиденциальной информации (ст. 13.14 КоАП РФ), за отказ в предоставлении информации, непосредствен-

но затрагивающей права и свободы гражданина, либо за предоставление неполной или заведомо недостоверной информации (ст. 5.39 КоАП РФ).

Административная ответственность предусмотрена также за нарушение правил защиты информации, в том числе за использование несертифицированных информационных систем и средств защиты, если сертификация обязательна (ст. 13.12 КоАП РФ), и незаконную деятельность в области защиты информации (ст. 13.13 КоАП РФ).

Уголовная ответственность может наступить за злоупотребление информацией о частной жизни (ст. 137 Уголовного кодекса РФ), неправомерный отказ должностного лица в предоставлении информации либо предоставление неполной или заведомо недостоверной информации, если это причинило вред правам и законным интересам гражданина (ст. 140 УК РФ), а также за неправомерный доступ к компьютерной информации (ст. 272 УК РФ). Уголовная ответственность предусмотрена также за незаконный сбор и использование сведений, составляющих коммерческую или банковскую тайну (ст. 183 УК РФ); нарушение авторских и смежных прав (ст. 146 и 180 УК РФ); разглашение государственной тайны и утрату документов, составляющих государственную тайну (ст. 283, 284 УК РФ); разглашение некоторых других сведений (ст. 155, 310, 311, 320 УК РФ); нарушение правил эксплуатации ЭВМ, системы или сетей ЭВМ, если это причинило существенный вред (ст. 274 УК РФ); создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК РФ).

Привлечение к гражданско-правовой ответственности возможно в виде денежной компенсации за причиненный моральный вред, обязанности опровержения сведений, порочащих честь, достоинство или деловую репутацию гражданина, и т. д. (ст. 150, 151, 152 Гражданского кодекса РФ).

Интересен проект закона «Об особенностях обеспечения информационной безопасности критически важных объектов телекоммуникационной инфраструктуры», разработка которого связана с попыткой запретить использование зарубежного программного обеспечения в стратегических сферах России: телекоммуникациях,

банках, энергетике, оборонной промышленности и т. д. По оценкам некоторых экспертов, доля несертифицированного ПО в государственных информационных системах достигает сейчас 80% (в основном это общесистемное и прикладное ПО), в то время как средства защиты информации используются в основном только сертифицированные [1]. Вместе с тем для организации адекватной защиты информационной инфраструктуры необходимо, чтобы помимо собственно средств защиты все используемые компоненты (программные, аппаратные) соответствовали требованиям безопасности.

Несмотря на то что проект был отклонен и отправлен на доработку, государством осознается важность проблемы качества используемого ПО. Озабоченность данной проблемой проявляется, прежде всего, в принятии нормативно-технической и нормативно-методической документации, регламентирующей требования к информационным системам, использованию информационных технологий и средств защиты информации. Такими документами являются руководящие документы, на основе которых проводится сертификация ФСТЭК и ФСБ, и технические регламенты и стандарты ФСТЭК (ГОСТы). Согласно Закону «О техническом регулировании» соблюдение стандартов носит добровольный характер.

Вместе с тем вне зависимости от формы собственности, согласно Постановлению Правительства РФ от 15.08.06 № 504 «О лицензировании деятельности по технической защите конфиденциальной информации», для обработки и защиты конфиденциальной информации должны использоваться только сертифицированные средства. Еще более строгие требования предъявляются к защите государственной тайны.

Ведущие российские компании-потребители сегодня склонны прислушиваться к требованиям государства, в том числе и в вопросах защиты своей информации. Востребованы в России и международные стандарты безопасности (ISO 17799, 27001, 13335 и 15408). Общая либерализация рынка информационной безопасности, участие в международном информационном обмене, выход российских компаний на мировые рынки, стремление России вступить в ВТО – все это обусловило необходимость адаптации международных стандартов. Приняты национальные стандарты, являющиеся аналогами наиболее авторитетных международных

стандартов (ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью», основанный на ISO 17799-2000, ГОСТ Р ИСО/МЭК ТО 13335-2006 «Информационная технология. Методы и средства обеспечения безопасности», ГОСТ Р ИСО/МЭК 15408-2002 «Критерии оценки безопасности информационных технологий»), ожидается принятие ГОСТов, основанных на международных стандартах ISO 17799-2005 и ISO 27001-2005.

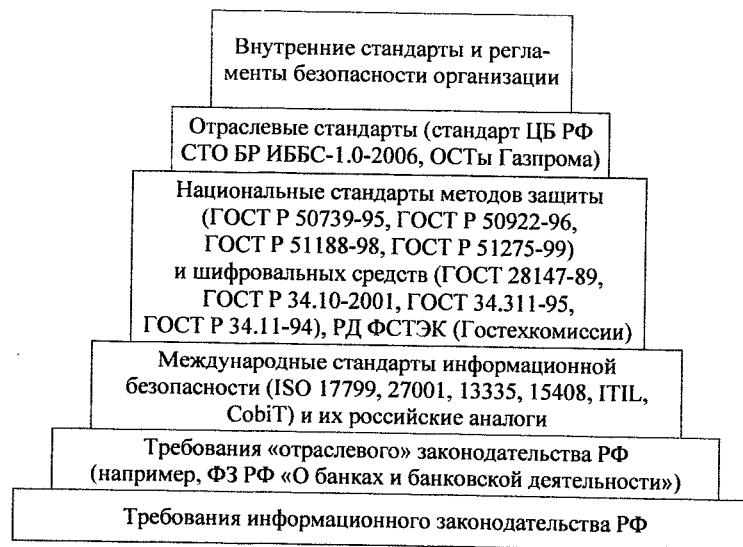
В 2002–2003 гг. были также выпущены новые руководящие документы по безопасности информационных технологий, касающиеся разработки и регистрации профилей защиты и заданий по безопасности, определяющие критерии оценки безопасности информационных технологий.

Кроме нормативных документов, регулирующих использование решений в области информационной безопасности, разрабатываются различные отраслевые стандарты. В частности, при построении информационных систем в финансовой сфере применяются стандарты Центрального Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» (СТО БР ИББС-1.0-2006), основанные на международных стандартах CobiT, ISO 17799/27001 и др.; информационные системы топливно-энергетического комплекса требуют ссылки на ОСТы Газпрома; Ассоциацией документальной электросвязи (АДЭ) готовятся рекомендации по базовому уровню информационной безопасности операторов связи и т. д.

Российские компании, заинтересованные в повышении эффективности своей работы и снижении издержек, ориентируясь на мировой опыт, разрабатывают внутренние нормативы, регламентирующие организацию информационных процессов и обеспечение их безопасности. Польза от внутренних стандартов и регламентов безопасности наиболее очевидна в крупных и территориально-распределенных организациях.

Иерархия нормативных актов, стандартов и регламентов в области информационной безопасности приведена на рис. 2.

Таким образом, в России постепенно создается единая система государственного регулирования в области обеспечения информационной безопасности и защиты информации.



Вместе с тем эффективное действие информационного законодательства в России затруднено отсутствием сложившейся правоприменительной базы, что требует преодоления медлительности российской судебной системы, а также повышения общей правовой культуры в области информационной безопасности и защиты информации.

Литература

1. Антиномов Д. Защитное ПО в России: секретно ли секретное? // Cnews: [Электронный ресурс]: www.cnews.ru, 29.11.07
2. Доля А. Закон «О персональных данных»: причины провала // CNews: [Электронный ресурс]: www.cnews.ru, 21.02.07
3. Соколова Г. А. Персональные данные работников // Кадровая служба и управление персоналом предприятия. 2007. № 7.
4. Ястребов Д. А. Соотношение банковской тайны и персональных данных // Регламентация банковских операций. Документы и комментарии. 2007. № 2.

УДК 378.001.658.011.56

Е. Б. Попов, И. А. Рогалёва

Санкт-Петербургский государственный
инженерно-экономический университет

СОСТАВЛЯЮЩИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

На сегодняшний день в Российской Федерации на рынке ПО общего назначения сложилась ситуация, когда более 90% программного обеспечения относится к так называемому проприетарному, или несвободному, программному обеспечению, основанному на закрытом исходном коде.

При этом основу этого проприетарного ПО в России (а именно операционные системы и пакеты офисных программ) составляют программные продукты американской корпорации Microsoft. В результате сложилась чудовищная ситуация сверхмонополии Microsoft, когда компьютерная инфраструктура России во многом основана на программном обеспечении этой американской корпорации. И это очень и очень опасно.

И за примерами далеко ходить не надо, сама корпорация Microsoft наглядно это всем нам продемонстрировала 24 августа 2007 г. и в последующие несколько дней, осуществив несанкционированный доступ в десятки миллионов компьютеров по всему миру, включая и Россию. Несанкционированный доступ заключался в установке на компьютеры с операционной системой Windows XP и Windows Vista и подключенных к Интернету девяти файлов. Причем в данном конкретном случае на экран монитора не выводилось обычное предупреждение с диалогом на получение разрешения пользователя для установки обновления.

Особое беспокойство вызывает тот факт, что файлы были изменены даже на компьютерах, где функция автоматического обновления в операционной системе была отключена. При этом в документации к Microsoft Windows не указано, что операционная система может обновляться, если пользователь отключил обновление. После публикации в средствах массовой информации сведений об этом факте 14 сентября корпорация Microsoft признала факт загруз-

ки исполняемых файлов для Windows XP и Windows Vista через систему автоматических обновлений Windows Update без санкции (разрешения) пользователя.

Исходя из имеющейся информации, можно утверждать, что при каждом включении компьютера с установленной операционной системой Windows XP или Windows Vista, подключенного к сети Интернет, посыпается запрос на сервер корпорации Microsoft, расположенный на территории США, извещающий о включении данного компьютера и о его готовности к обмену информацией с этим сервером. Учитывая, что на подавляющем большинстве ПК в России установлено ПО этой корпорации, можно предположить, что в связи с наличием таких возможностей американские спецслужбы имеют техническую возможность осуществлять несанкционированный доступ в любой компьютер на территории Российской Федерации, подключенный к сети Интернет, причем не только на ПК частных лиц, но и на компьютеры, установленные в органах государственной власти и управления, на предприятиях и в организациях, включая оборонные, а также в воинских частях и учреждениях.

По-видимому, 24 августа 2007 г. США произвели успешное испытание совершенно нового вида оружия, а именно – кибероружия. Была проверена возможность одновременного несанкционированного пользователями доступа в десятки миллионов персональных компьютеров. А значит, США проверили возможность несанкционированной установки в компьютеры файлов, позволяющих осуществлять дистанционное управление этими компьютерами и съем содержащейся в них информации.

Как известно, 18 сентября 2007 г. пресс-служба Пентагона сообщила, что в США заканчивается создание киберкомандования BBC США. Специальный отряд, получивший обозначение JFCCNW (Joint Functional Component Command for Network Warfare – Совместное функциональное командное подразделение для ведения сетевой войны), численностью около 25 тысяч человек располагается на базе BBC США «Барксдейл» в штате Луизиана, а главной обязанностью его персонала станут «глобальные операции в киберпространстве, интегрированные с воздушными и космическими операциями».

И сегодня в плане готовности к объявленной или готовящейся «кибервойне» мы оказались в положении, намного худшем, чем Советский Союз накануне 22 июня 1941 г.

По разным данным, сегодня в России насчитывается около 25 млн персональных компьютеров. На 99% этих компьютеров установлено ПО американской корпорации Microsoft. Поэтому мы сегодня не в состоянии защититься от кибератак со стороны США.

После 24 августа 2007 г. стало ясно, что сегодня США имеют техническую возможность несанкционированного доступа в любой компьютер, на котором установлена операционная система Windows и который подключен к Интернету. Тем самым они продемонстрировали: возможность дистанционного съема любой информации, имеющейся в таких компьютерах; возможность удаленного управления таким компьютером; возможность вывода из строя такого компьютера, по крайней мере, уничтожение как операционной системы, так и информации, имеющейся в таком компьютере.

А если еще предположить возможность наличия аппаратных закладок в компьютерных комплектующих, то возможен дистанционный вывод из строя и собственно компьютера.

Элементарно просто проводить такие кибероперации избирательно в отношении отдельных стран или регионов земного шара и даже отдельных пользователей (например, по русской раскладке клавиатуры, или по IP-адресам). Возможно выявление компьютеров, включая домашние, владельцы которых представляют интерес как для корпорации Microsoft, так и для спецслужб США.

Так, домашний компьютер генерального конструктора крупного российского оборонного КБ, занимающегося разработкой стратегического оружия, может содержать такую информацию, которая позволит США быть в курсе всех российских новейших разработок такого оружия. Или доступ в компьютеры российских разработчиков программного обеспечения. Да даже конфиденциальная официальная информация о планах по закупке программного обеспечения для российских школ может принести большую коммерческую выгоду владельцам такой информации.

А разве не представляет большой интерес для определенных структур личная информация в домашнем компьютере министра российского правительства, крупного военачальника или руководи-

теля спецслужб? И разве возможность единовременного вывода из строя всей российской компьютерной инфраструктуры, во многом основанной на программном обеспечении Microsoft, не представляет угрозу не только информационной, но и национальной безопасности нашей страны?

А ведь в свое время Бисмарк сказал: «Меня не интересуют намерения моих врагов, меня интересуют их возможности».

Что делать?

Единственное, чем мы можем противостоять существующим угрозам и вызовам в этой сфере – это ограничиться чисто организационными мероприятиями, связанными в первую очередь с запретами на подключение к Интернету компьютеров, на которых проходит обработка особой и специфической информации.

Кажется, ответ очевиден – нужны отечественная операционная система и пакет прикладных программ, позволяющие отказаться от использования ПО Microsoft, в первую очередь ОС Windows, в органах государственной власти и управления. Сюда же можно отнести государственные учреждения и организации, воинские части и оборонные предприятия, а также стратегические системы обеспечения жизнедеятельности страны (системы электро-, газо-, тепло- и водоснабжения, транспорт, связь и т. п.).

При этом речь не идет о коммерческих структурах и частном бизнесе, а также о домашних пользователях. Если можешь заплатить за программное обеспечение Microsoft и при этом твой компьютер не содержит информацию, разглашение которой может нанести ущерб информационной безопасности страны, если ты хочешь продолжать использовать это программное обеспечение, то имеешь на это полное право. Но если ты работаешь в государственной структуре или учреждении, финансируемом из бюджета, то будь добр использовать отечественный программный продукт. И только если в отечественном программном продукте нет тех программ, которые жизненно необходимы для функционирования твоего учреждения или предприятия, то в данном конкретном случае можно использовать и иностранное ПО.

Можно ли в кратчайший срок создать весь упомянутый выше отечественный пакет программного обеспечения, причем создать с нуля? К сожалению, ответ один – невозможно.

Напомним, что создание ОС Windows Vista потребовало от Microsoft шести лет напряженной работы и финансирования в размере 6 млрд. долл. И это при том, что у нее уже к этому времени имелись серьезные наработки в плане создания ОС.

Поэтому выход только один – обратиться к свободному программному обеспечению, и в первую очередь к «Линукс». Как известно, свободное ПО – программное обеспечение, в отношении которого пользователь обладает «четырьмя свободами»: запускать, изучать, распространять и улучшать программу.

За последние 15 лет компьютерным сообществом было создано огромное количество программного обеспечения, распространяемого на основе свободной лицензии. Именно поэтому, чтобы не начинать все с нуля и не изобретать велосипед, предлагается начать создание отечественной операционной системы именно на основе «Линукса».

Создать такие программные средства в России возможно в кратчайший срок, если использовать уже существующие в открытом доступе выверенные программные наработки мирового сообщества, основанные на открытом исходном тексте и распространяемые на основании свободной лицензии. Это также минимизирует финансовые затраты.

Частично эта задача уже решена, по крайней мере, в силовых структурах Российской Федерации. Как известно, за последние годы в России были разработаны и внедрены три ведомственные операционные системы на основе «Линукс».

Первая – Мобильная Система Вооруженных Сил (МСВС), основанная на базе RedHat Linux. Она сертифицирована Министерством обороны РФ и Федеральной службой по техническому и экспортному контролю. Данная операционная система не распространяется вне Минобороны и предприятий ВПК.

Вторая – операционная система «Атликс», разработана для Федеральной службы безопасности, является клоном RedHat Linux. Свободно не распространяется.

Третья – операционная система Уапух на основе RedHat Linux. Свободно не распространяется.

Кроме того, имеется пять операционных систем, разработанных в России на основе ядра Linux и распространяемых на рынке, а именно: ALT Linux, ASP Linux, Linux-Ink, Linux-online и MOPSLinux.

Разрабатываемое ПО должно состоять из двух частей – собственно ОС на основе ядра «Линукса» и пакета прикладных программ, обеспечивающих, в первую очередь, документооборот и делопроизводство в госучреждениях, а также другие основные задачи. Для этого необходима адаптация ряда программных продуктов, например, «1С» или FineReader под Linux.

Эта задача по своей сложности, трудозатратам и объемам финансирования сравнима с советским «атомным» или «ракетным» проектами.

Без современной отечественной ОС и отечественного компьютерного оборудования мы никогда не сможем вернуть нашей стране статус великой державы и решить вопросы ее информационной безопасности, совершив технологического прорыва в нашей экономике и образовании. Именно поэтому вопрос создания такой операционной системы и российского компьютерного оборудования должен быть приоритетным.

Неслучайные случайности. Одно из главных светил открытой криптографии, израильский профессор Ади Шамир (Adi Shamir) опубликовал работу без преувеличения взрывного характера. В ней показано, сколь гигантскую роль в стойкости компьютерных систем безопасности играет надежное выявление ошибок программирования, ибо даже мельчайший и почти незаметный «баг» может иметь роковые последствия. Вместе с ростом числа строк кода в программах, усложняющейся оптимизацией операций и нарастающей длиной слова в процессорах становится все более вероятным появление ошибок в конечных продуктах, запускаемых в массовое производство. Примером тому может служить случайное открытие в середине 1990-х гг. глубоко спрятавшегося «бага деления» в процессорах Pentium или совсем недавно обнаруженная ошибка умножения в программе Microsoft Excel.

Если какая-нибудь спецслужба, пишет Шамир, обнаружит (или тайно встроит) хотя бы пару таких целых чисел, произведение которых микропроцессор вычисляет некорректно, то последствия ошибки (даже в единственном бите низкого разряда) будут сокрушительными с точки зрения криптографии и защиты информации в компьютере. Потому что тогда любой ключ в любой криптов программе на основе RSA, работающей на любом из миллионов компьютеров с

этим процессором, может быть взломан с помощью специально подобранного сообщения. Кроме того, по заключению Шамира, аналогичная атака может применяться против любых криптосхем на основе дискретных логарифмов и эллиптических кривых (где вдобавок можно эксплуатировать еще и «баги деления»). Иначе говоря, мелкий баг способен радикально подрывать стойкость практически всех современных криптосхем с открытым ключом.

Почти наверняка можно утверждать, что нет никакой связи между появлением работы Шамира и одновременной публикацией эссе другого известного криптографа – Брюса Шнайера. Статья посвящена вроде бы совсем другой теме – стандартам на генераторы случайных чисел, но и здесь звучит тот же самый мотив. Генераторы случайных чисел (RNG) играют в криптографии очень важную роль: они применяются для выработки ключей шифрования, векторов инициализации и запросов аутентификации, формирования общего ключа, генерации простых чисел и т. д. Если взломан генератор случайных чисел, то в большинстве случаев можно считать взломанной и всю систему безопасности. Шнайер забил тревогу, когда увидел, что в новый спецвыпуск Национального института стандартов США (NIST Special Publication 800-90), описывающий четыре одобренных к использованию схемы RNG, включен генератор Dual_EC_DRBG, разработанный в недрах американского Агентства национальной безопасности.

Криптографы АНБ США, спору нет, слывут очень компетентными специалистами, однако генератор, предложенный этим ведомством в 2006 г., известен независимым исследователям с другой стороны – как довольно странный алгоритм, очень медленный в работе и весьма мутный по конструкции. Более того, на августовской конференции CRYPTO 2007 два аналитика (Dan Shumow и Niels Ferguson) показали, что алгоритм содержит слабость, называемую backdoor, т. е. «черный ход». Устроено это примерно так. Dual_EC_DRBG работает на основе аппарата эллиптических кривых, которые задаются определенным набором констант. АНБ не объясняет, почему были выбраны именно эти константы. Но они хотя бы известны. Однако при анализе схемы выяснилось, что эти числа связаны со вторым – секретным – набором чисел, которые действуют в качестве «скелета» схемы или мастер-ключа. И если вы знаете эти секретные чис-

ла, то всего по 32 байтам выхода можно предсказывать всю генерируемую «случайным генератором» последовательность. Проще говоря – взламывать безопасность, обеспеченную Dual_EC_DRBG, фактически на лету.

Таким образом, следует всячески избегать Dual_EC_DRBG. Однако выбор возможен далеко не всегда. Скажем, генератор случайных чисел, встроенный в ОС Windows, автоматически используется во всех приложениях системы, связанных с защитой информации. И при этом конкретные алгоритмы генерации, используемые в Microsoft для данной цели, никогда открыто не публиковались и не подвергались независимому анализу. Ныне этот пробел восполнила группа израильских криптографов из университетов Иерусалима и Хайфы (Leo Dorrendorf, Zvi Guterman, Benny Pinkas), которые провели обратную инженерную разработку критичных мест в двоичном коде Windows 2000, в частности, восстановив функцию CryptGenRandom. И обнаружили массу неприятных вещей (eprint.iacr.org/2007/419).

Прежде всего, аналитики нашли уязвимость, позволяющую организовать атаку, эффективно отыскивающую предыдущие состояния генератора, а значит, и вычислять будущие числа на выходе. Кроме того, установлено, что генератор управляет системой таким образом, который многократно усиливает значение уязвимости. А именно – функция запускается в режиме пользователя, а не в режиме ядра, что делает очень легким доступ к состояниям генератора даже без привилегий администратора. В совокупности с другими выявленными слабостями это приводит к тому, что злоумышленник, получив всего лишь одно состояние генератора (например, переполнение буфера), может вычислить 128 килобайт прошлых и будущих «случайных» чисел на выходе алгоритма (используемых, напомним, в качестве секретных криптопараметров для всех алгоритмов защиты информации в ОС, которая имеет много общего с самой распространенной на сегодня Windows XP). Никто толком не знает, как устроен генератор случайных чисел в XP, но есть веские основания полагать, что он не слишком отличается от Windows 2000.

Тайнопись. «Стеганография» занимается защитой информации, являясь, таким образом, родственницей криптографии. Однако

в этой области появились новые и, без преувеличения, революционные технологии.

От бульжника до спама. Нередко стеганографию считают частным разделом криптографии, что совершенно неверно. Криптография просто защищает данные, а задача стеганографии гораздо глубже – скрыть сам факт существования защищаемой информации. Это различие не менее принципиально, чем между бронежилетом и шапкой-невидимкой.

Можно предположить, что уже в каменном веке, задолго до появления первых шифров, люди могли договориться и особым образом поворачивать бульжник у входа в пещеру, тем самым подавая условные знаки соплеменникам. Примеры аналогичных тайных знаков каждый может вспомнить из собственного детства или прочитанных книг. Скажем, у Сергея Довлатова описано, как друзья будущего заключенного, провожая его в тюрьму и зная, что письма будут вымарываться цензурой, просили его по приезде выслать свою фотографию – если все хорошо, то обычную, а если плохо, то с сигаретой в руке. Через некоторое время им пришло фото, на котором друг был чисто выбрит, аккуратно одет и держал в руках две пачки «Беломора». Краткость – сестра таланта! Если добавить к этому цветок на окне из «Семнадцати мгновений весны» или утюги на подоконнике из анекдота о Штирлице (типичные примеры скрытого информирования), то становится очевидно, что стеганография может быть удивительно разнообразной.

Цифровой век подарил стеганографии второе дыхание. Все мы слышали о невидимых чернилах, проявляющихся на бумаге после нагревания. Казалось бы – сугубо шпионская амуниция, но сейчас любая секретарша, имеющая Word, может сделать себе такие «чернила» одним движением мыши, просто изменив цвет набранного текста. К примеру, вытряхните из мусорной корзины своей почтовой программы какое-нибудь спамерское сообщение. Как видите, абзацы в письме разделены пустой строкой. Скопируйте этот текст в Word и наберите в пустых строках между абзацами свое секретное донесение, допустим: «В Пхеньяне все спокойно». Выделите набранные слова и измените их цвет таким образом, чтобы он совпал с цветом фона (белый на белом). Ваш текст «исчезнет», а письмо приобретет вид обычного спама. Сохраните результат и отправьте письмо своим знакомым, например, в Белый дом.

Черт в табакерке. В Интернете можно найти десятки программ для компьютерной тайнописи, от больших и дорогих пакетов до маленьких бесплатных утилит. Некоторые из них используют очень причудливые алгоритмы, но всегда неизменной остается суть: для скрытой передачи сообщения нужен подходящий носитель – «контейнер», который, во-первых, безошибочно выглядит и, во-вторых, по размеру значительно больше скрытого сообщения (в перевесе на килобайты). Оба требования очевидны, и им подчиняются все программы – от Snow1, скрывающей данные в тексте с разной длинной пробелов, до файловой системы StegFS2, создающей во множестве подходящих файлов целый спрятанный раздел, который может работать как обычный диск.

Хотя «контейнерами» могут быть различные файлы – даже dll-библиотеки и XML-страницы, – чаще всего в этой роли выступают аудиофайлы или графика. Помимо того, что их легко пересыпать, не вызывая подозрений, у звука и картинок есть уникальная особенность – они позволяют прятать в себя информацию, совершенно не увеличиваясь в размерах и почти не меняясь «в лице». С помощью простейшей утилиты можно вставить 10 Кбайт текста в 100-килобайтную картинку так, что на глаз она будет неотличима от прежней, а размер не изменится ни на бит. Думаю, стоит объяснить этот фокус, поскольку его используют примерно девять стеганографических программ из десяти.

Представим простейшую черно-белую картинку, в которой каждый пиксель описывается одним байтом. Допустим, байт кодирует яркость пикселя: ноль – черный, 255 – белый, все остальное – градации серого. Если мы изменим любой байт нашего файла или, что то же самое, отдельные биты этого байта, то соответствующий ему пиксель изменит яркость. При этом окажется, что изменение разных битов влияет на яркость пикселя по-разному: первый очень сильно, второй слабее, а последний, восьмой бит может добавить байту (а значит, и пикслю) только единицу. Заметит ли нормальный человек изменение серой точки на одну (1/255) градацию серого? Конечно, нет. А значит, для нашей картинки абсолютно не важно, каковы последние биты ее байтов. И что бы мы с ними ни делали – обнуляли, переставляли, заменяли на случайные, – картинка будет казаться одинаковой. Также не будет меняться и ее размер –

ведь количество байтов мы не меняем. Таким образом, для размещения в картинке тайного сообщения достаточно превратить его в цепочку битов и записать их на место последних битов картинки.

Описанный метод очень прост, применим к аудиофайлам так же, как и к картинкам, и в разных вариантах его используют почти все программы. Однако, при всей его элегантности, этим способом нельзя спрятать слишком много: алгоритм требует, чтобы соотношение скрываемой информации и файла-контейнера было не более 1:8. Если мы попытаемся изменять не только восьмые, но и седьмые и шестые биты, то картинка сильно и подозрительно исказится. По правде говоря, даже изменение последних битов бывает заметным на больших однотонных участках. Поэтому хорошие программы делают вставки только в самые надежные участки картинки. В результате для скрытой передачи средней величины текста с короткими аудиороликами общим размером, скажем, 300 Кбайт надо использовать огромное письмо-контейнер объемом 3 Мбайт. Помимо всего прочего, если за вашей почтой наблюдают (а иначе чего вы прячетесь?), то пересылка столь больших объемов может легко привлечь внимание кого не нужно.

Тайнопись украинская. Windows-программа BMP Secrets обладает простым интерфейсом и способна незаметно скрывать в bmp-файлах информацию большого объема, размером до 65% от файла-контейнера – 65%! В то время как обычные «пряталки» делают вставки максимум в 10–12%, на сайте компании Parallel Worlds рассказывалось, что при работе программы файл-контейнер визуально не меняется, размер его остается прежним и, главное, в картинку запросто входит (а затем выходит) что угодно размером до 2/3 от ее объема. В обои рабочего стола Windows с разрешением 1024x768 и размером (в формате TrueColor) 2,3 Мбайт можно спрятать архив почти в 1,5 мегабайта – больше, чем на дискету! При этом обои визуально не изменятся.

Таким образом, можно сделать вывод: часть проблем безопасности может быть исправлена исключительно на уровне государства, например, воссоздание бездумно уничтоженной электронной промышленности, создание собственной патентно чистой ОС, можно решать уже сейчас, например, использование более безопасного Линукса, собственных систем криптографии и стеганографии.

Во всяком случае, учить пользователей уже сейчас, ибо мы живем в мире Гоббса-Дарвина, в котором пренебрежение безопасностью может обойтись очень дорого.

УДК 378.001.658.011.56

И. В. Поночевная

Санкт-Петербургский государственный
инженерно-экономический университет

КОНЦЕПЦИЯ ПОСТРОЕНИЯ УНИФИЦИРОВАННОЙ МОДЕЛИ ИЕРАРХИИ УГРОЗ

Предложено рассматривать множество иерархии угроз как множество дестабилизирующих факторов, действующих на корпоративную информационную систему предприятия.

Формирование полной системы иерархии угроз – на основе сведений об уже известных и наиболее опасных или неизвестных информационных угрозах является одним из основных направлений унифицированной модели иерархии угроз.

Таким образом, принципиальной особенностью унифицированной модели иерархии угроз (УМИУ) является требование абсолютной полноты моделирования возможных угроз для объектов корпоративной ИС (носители информации, информационный ресурс, программное обеспечение, аппаратное обеспечение и т. д.). Даже один неучтенный, невыявленный или не принятый во внимание фактор угрозы может значительно снизить эффективность средств защиты системы информационной безопасности, так как в защитных средствах по определению присутствует такая особенность, как «*уязвимые места в системе*», которая позволяет манипулировать объектами корпоративной информационной системы предприятия.

На сегодняшний день существует целый ряд различных подходов, связанных с классификацией информационных угроз.

Некоторые вопросы информационных угроз рассмотрены в указанных ниже работах.

© И. В. Поночевная, 2009.

Существенным недостатком классификации информационных угроз в работе «Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Информационная безопасность» (М.: МГФ, «Знание», ГЭИТИ, 2005. 512 с.) является отсутствие многих важных для практической реализации факторов, деления угроз на «потенциальные угрозы» и «реальные угрозы».

Реальная угроза является информационной атакой на систему со стороны нарушителей «субъекта угроз» как внутренних, так и внешних.

В классификации информационных угроз в работе О. Ю. Гаценко «Защита информации: Основы организационного управления» (СПб.: Сентябрь 2001. 228 с.) важным является разделение угроз на «внутренние» и «внешние», на «случайные» и «целенаправленные», а также «на субъект воздействия», осуществляющий эту информационную угрозу, и представлена классификация, выполненная «по типам воздействия», «характеру воздействия» и «объектам воздействия». Существенным недостатком в приведенной классификации является попытка объединить разные классификационные характеристики в единую многоуровневую схему.

Основой классификации информационных угроз в работе: [Электронный ресурс]: www.dsec.ru/products/grif/fulldese/classification//ugroza_fin.jpg является объект информационной угрозы, источник информационной угрозы, характер информационной угрозы и вид воздействия информационной угрозы. Существенным недостатком в данной классификации является то, что не учитываются цели воздействия угроз и уязвимостей системы. Это говорит о том, что данная классификация является только классификацией источников угроз.

В приведенной классификации угроз Ю. А. Щеглова «Защита компьютерной информации от несанкционированного доступа» (СПб.: Наука и техника, 2004. 384 с.) дано разделение угроз на «скрытые» и «явные». Под «явными угрозами» понимаются такие угрозы, которые «поняты и предсказуемы». Как пишет автор, «явные угрозы» связаны с некорректной реализацией и настройкой средств защиты. Приводимое разделение «явных угроз» на противоречивость реализации средств защиты и настройки средств защиты показывает фактически слабые места в защитных средствах, что указывает на уязвимости в системе, а не на информационные угрозы. В приводимой классификации «скрытые угрозы» содержат в

себе фактическое описание уязвимостей средств защиты. Кроме того, некорректная реализация средств защиты не является понятной и однозначно предсказуемой, так же, как и некорректность возможных настроек средств защиты.

Зачастую настройки средств защиты бывают настолько сложны, что даже квалифицированный специалист не сможет выявить некорректность этих настроек. Фактически данная классификация представляет собой неполную классификацию уязвимостей средств защиты.

В работе О. О. Варламова «Системный подход к созданию модели компьютерных угроз информационной безопасности» (Материалы VI Междунар. науч.-практ. конф. «Информационная безопасность». Таганрог: Изд-во ТРГУ, 2004. с. 61–65) вводится понятие «техническая компьютерная угроза». «Техническая компьютерная угроза» представляет собой угрозу добывания конфиденциальной информации с помощью программно-аппаратных средств.

Автором представлена следующая классификация «технических компьютерных угроз»:

- *семантический уровень угрозы* (обеспечивает добывание информации путем поиска, сбора и анализа конфиденциальной информации);
- *вирусный уровень угрозы* (обеспечивает добывание информации путем внедрения вредоносных антивирусных программных средств);
- *разграничительный уровень угрозы* (обеспечивает добывание информации преодолением средств разграничения доступа);
- *сетевой уровень угрозы* (обеспечивает добывание конфиденциальной информации путем анализа уязвимостей сетевых ресурсов);
- *алгоритмический уровень угрозы* (использует программно-аппаратные закладки и недекларированные возможности);
- *пользовательский уровень угрозы* (обеспечивает добывание конфиденциальной информации о пользователях системы);
- *форматный уровень угрозы* (обеспечивает добывание конфиденциальной информации путем фильтрации и декодирования форматов данных);
- *потоковый уровень угрозы* (обеспечивает добывание информации перехватом и обработкой сетевого трафика).

Данный подход к классификации угроз представляется интересным, но приведенные Варламовым угрозы частично пересека-

ются между собой и содержат фактически одинаковые элементы. Так, например, форматная угроза представляет собой часть потоковой угрозы, семантическая угроза является следствием успешной реализации других угроз из представленного списка.

Рассмотренное существующее многообразие различных классификаций угроз не дает возможности осуществить полноценное моделирование угроз.

Однако важность таких разработок очевидна, так как эта технология дает возможность дополнить классификационную характеристику наличием дестабилизирующих факторов воздействия по отношению к системе.

Открытым остается вопрос влияния не известной к настоящему времени иерархии угроз и атак, а также наличия неизвестных уязвимостей в средствах защиты, влияющих на безопасность объектов корпоративной информационной системы, и на этой основе строится унифицированная модель иерархии неучтенных дестабилизирующих факторов угроз.

УДК 378.001.658.011.56

И. В. Поночевная, Д. А. Поночевный

Санкт-Петербургский государственный
инженерно-экономический университет

ОСНОВНЫЕ ПОДХОДЫ К ПОСТРОЕНИЮ МОДЕЛИ «СУБЪЕКТА УГРОЗ»

Модель «субъекта угроз» носит причинно-следственный характер воздействий, т. е. отражает преследуемые цели, причины и мотивы действий, его финансовые возможности.

Цель нарушителя – получить максимальную прибыль за счет воздействия дестабилизирующих факторов на информационный ресурс, а также добиться повышения расходов на средства защиты системы безопасности (СБ).

Для достижения поставленной цели нарушитель должен приложить немалые усилия и затратить определенные средства, включая и технические, для воздействия на систему.

Под техническими возможностями подразумевается перечень различных технических средств, которыми может располагать злоумышленник в процессе совершения действий, направленных против системы безопасности.

С точки зрения службы безопасности, определив основные причины нарушений, предоставляется возможность оказать влияние на эти причины и скорректировать требования к системе безопасности от данного типа «субъектов угроз».

Вопросы безопасности большей частью есть вопросы человеческих отношений и человеческого поведения. При анализе нарушений информационной защиты необходимо уделять внимание субъекту (личности нарушителя). Выявление причин или мотивов, побудивших к нарушению, в дальнейшем может помочь избежать несанкционированных воздействий.

Модель может быть не одна. Целесообразно построить несколько отличающихся друг от друга моделей разных типов «субъектов угроз» для системы безопасности предприятия. У злоумышленника существует своя собственная модель нападения, и в общем случае эта модель может не совпадать с моделью защищающейся стороны. Пользователь системы также может стать нарушителем информационной безопасности.

Для построения модели нарушителя системы используется информация от служб безопасности и аналитических групп о существующих средствах доступа к конфиденциальной информации, о возможных способах перехвата данных на стадиях передачи, обработки и хранения, об обстановке в коллективе и на объекте защиты, сведения о конкурентах и ситуации на рынке, об имевших место свершившихся случаях хищения информации и т. п.

С точки зрения преследуемых целей угрозы для системы представляют *инсайдеры* (недобросовестные внутренние сотрудники), *хакеры (конкуренты)* (внешние нарушители системы), *комбинированные* (предполагаемый говор внутреннего и внешнего нарушителя) и *форс-мажорные ситуации (обстоятельства)* – пожар, природные явления, выход из строя оборудования без участия человеческого фактора.

Инсайдеры – авторизованные пользователи корпоративной ИС могут совершить неправомерные действия, которые с высокой степенью вероятности не будут раскрыты, поскольку у инсайдеров из-

начально имеется доступ к системе и они знакомы с принципами функционирования системы, включая связи между ее компонентами и информацию о наличии уязвимостей (рис. 1). У этих нарушителей системы есть возможность нанести больший ущерб по сравнению с внешними нарушителями, если они обладают неограниченными привилегиями.

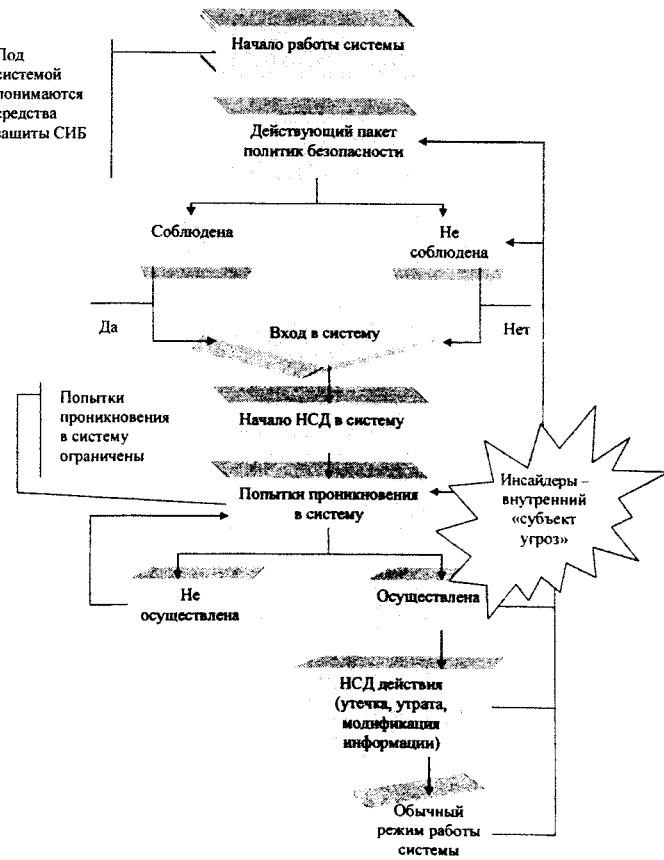


Рис. 1. Модель дестабилизирующих факторов внутреннего «субъекта угроз»

В данном контексте будем считать инсайдеров с ограниченными привилегиями и правами доступа в систему.

Такого рода нарушители являются наиболее опасными, поскольку любые применяемые средства (например, аппаратно-программные средства защиты) от них будут неэффективны.

Внешний «субъект угроз» не является легальным пользователем. Для нанесения ущерба системе безопасности внешнему нарушителю необходимо определить уязвимости в системе, что требует определенных расходов на приобретение аппаратно-программного сервиса и т. д.

Хакеры (конкуренты). Объектом атак со стороны хакеров являются не только корпоративные ИС, базы данных, но и активное сетевое оборудование, вмешательство в работу которого зачастую имеет еще более плачевые последствия.

Часто угрозе хакеров уделяется гораздо большее внимание, чем всем прочим угрозам. Действительно, воздействие хакеров на корпоративную информационную систему – достаточно распространенное явление. Кроме того, у предприятия есть возможность повлиять на внутреннего нарушителя системы административными мерами, однако нет такой возможности в отношении внешнего нарушителя, разве что в случае прямого нарушения уголовного или административного законодательства.

Вместе с тем хакеры заставляют пользователей системы чувствовать себя «уязвимыми», ведь фактически злоумышленник не определен. Наконец, предприятию неизвестны истинные цели хакера, так как взлом системы может быть произведен с целью организации утечки конфиденциальной информации, а может быть, и из «спортивного интереса».

Хакер, по определению, стремится обойти средства защиты вне зависимости от того, преследуются по закону его несанкционированные действия или нет, т. е. это постороннее лицо, не имеющее никаких легальных привилегий и прав доступа в систему (рис. 2).

Для этих дестабилизирующих факторов внешний «субъект угроз» использует слабые места в системе, т. е. ее уязвимости, для получения прав легального пользователя. Это нарушение осуществляется с помощью подбора паролей пользователей системы. Далее

«субъекты угроз» попытаются установить контроль над некоторыми компьютерами с целью их дальнейшего использования для информационной атаки на другие компьютеры в сети для повторного вторжения в систему.

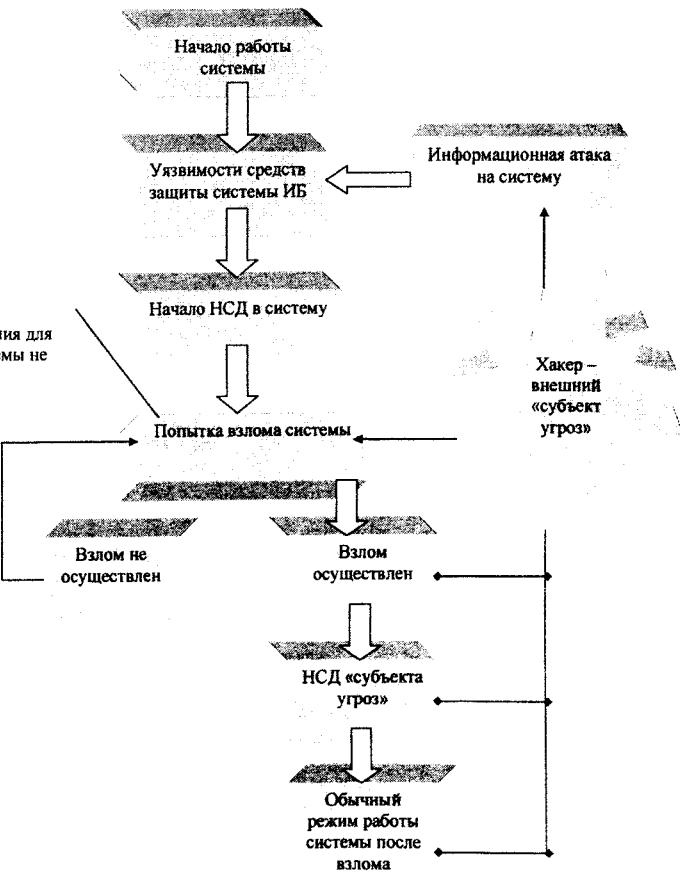


Рис. 2. Модель дестабилизирующих факторов внешнего «субъекта угроз»

Форс-мажорные ситуации – это различные бедствия (пожар, природные явления и др.), которые относятся к страховым рискам (рис. 3).



Рис. 3. Модель дестабилизирующих форс-мажорных факторов

Вышесказанное свидетельствует о том, что чем успешнее бизнес предприятия и чем оно известнее, тем выше вероятность того, что это предприятие становится желанной мишенью для «субъектов угроз» – как внутренних, так и внешних. Цель любого нарушителя системы – получить максимальную прибыль для себя, что неизбежно наносит финансовый ущерб предприятию.

Каждое из этих неучтенных уязвимостей на этапе проектирования потенциально может в дальнейшем привести к дополнительным финансовым расходам.

Для того чтобы избежать этих уязвимостей, предприятию необходимо при разработке системы информационной безопасности использовать комплекс организационных, правовых, технических, технологических и экономических составляющих.

УДК 378.001.658.011.56

И. В. Поночевная, А. М. Петрова,
Д. А. Поночевный

Санкт-Петербургский государственный
инженерно-экономический университет

КОНЦЕПЦИИ ПАКЕТА ПОЛИТИК СИСТЕМЫ БЕЗОПАСНОСТИ

Эффективность системы неосуществима без действующей политики в области безопасности. Рассматриваемая в данной работе разработка декомпозиции средств защиты заключается в реализации пакета политик, отражающих правила работы и ответственность персонала при работе с информационными ресурсами корпоративной информационной системы (КИС). В общем случае действующая политика включает в себя концепцию пакета политик для системы безопасности предприятия.

Концепция пакета политик средств защиты системы безопасности представляет собой механизм управленческих решений в совокупности правил, распоряжений, приказов, указаний. Примерами таких документов могут служить «Политика управления паролями», «Политика управления доступом к информационным ресурсам системы», «Политика обеспечения информационной безопасности при взаимодействии с глобальной сетью Internet/Intranet», т. е. пакет политик слагается в зависимости от конкретной корпоративной информационной системы и системы безопасности (рис. 1).



Рис. 1. Пакет политик безопасности системы

© И. В. Поночевная, А. М. Петрова, Д. А. Поночевный, 2009.

Этот пакет политик представляет собой систематизированное изложение основных принципов и способов для достижения требуемого уровня безопасности, который должен закладываться в архитектуру ядра системы безопасности в совокупности с поставленными целями и задачами (рис. 2).

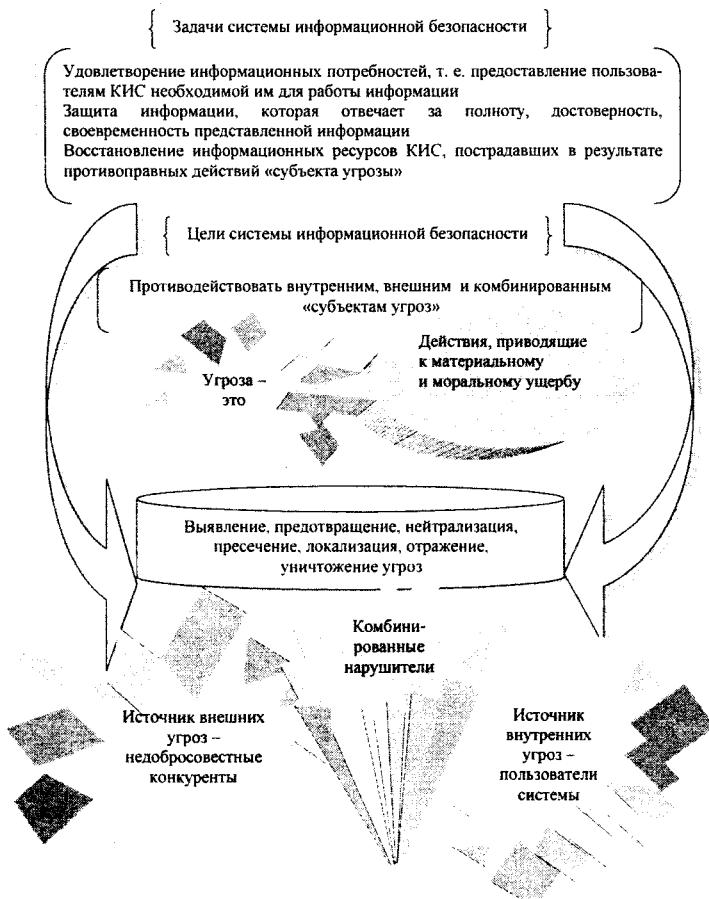


Рис. 2. Цели и задачи системы безопасности

Вышеизложенное является достаточным для получения максимального эффекта решаемых задач в области обеспечения безопасности КИС. Перечислим основные принципы обеспечения безопасности:

- **принцип целостности** – информация, на основе которой принимаются управленческие решения, должна быть достоверной и точной, защищенной от возможных дестабилизирующих факторов, непреднамеренных и злоумышленных искажений;
- **принцип доступности (готовности)** – информация и соответствующие административные службы должны быть доступны, готовы к работе всегда, когда в них возникает необходимость;
- **принцип конфиденциальности** – засекреченная информация должна быть доступна только тому, кому она предназначена.

В данном аспекте концепция пакета политик будет формироваться в терминах целостности, конфиденциальности, доступности (рис. 3).

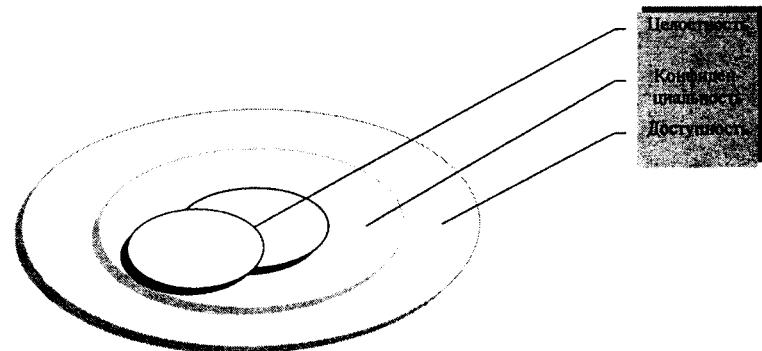


Рис. 3. Термины безопасности

Однако есть и другая сторона медали, где присутствуют такие дестабилизирующие факторы, как изменения, вскрытие, уничтожение. Эти термины противоположны терминам обеспечения безопасности (рис. 4).

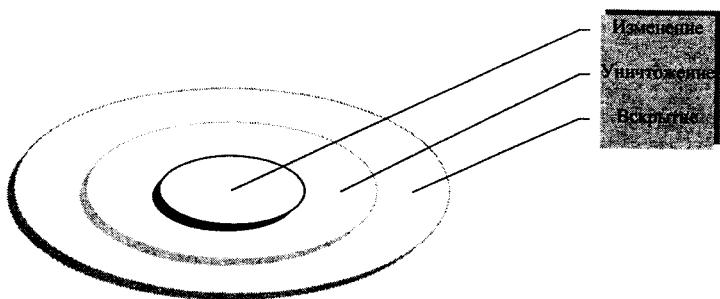


Рис. 4. Термины антибезопасности

Основные требования пакета политик будут распространяться на корпоративную информационную систему, содержащую сведения коммерческой и служебной тайны, а также персональные данные. Требования распространяются и на подразделения других предприятий (или структур), взаимодействующих с корпоративной информационной системой в качестве пользователей системы.

Можно утверждать, что адекватный уровень работоспособности корпоративной информационной системы может быть обеспечен только комплексным подходом, предполагающим разработку и реализацию системы безопасности на правовом, организационном, техническом и технологическом уровнях защиты с позиций экономической целесообразности (рис. 5).

Зарубежный и отечественный опыт в области безопасности показывает, что работоспособность корпоративной информационной системы обеспечивается комплексом этих составляющих.

Организационное направление защиты производственной деятельности предприятия строится на нормативно-правовой основе, предполагающей, что разглашение, утечка конфиденциальной информации и несанкционированный доступ или взлом системы будет невозможным или существенно затрудненным за счет проведения организационных действий.

Одним из основных компонентов организационного направления является служба информационной безопасности. Именно от профессиональной подготовки сотрудников службы информационной безопасности во многом зависит эффективность современных средств защиты.

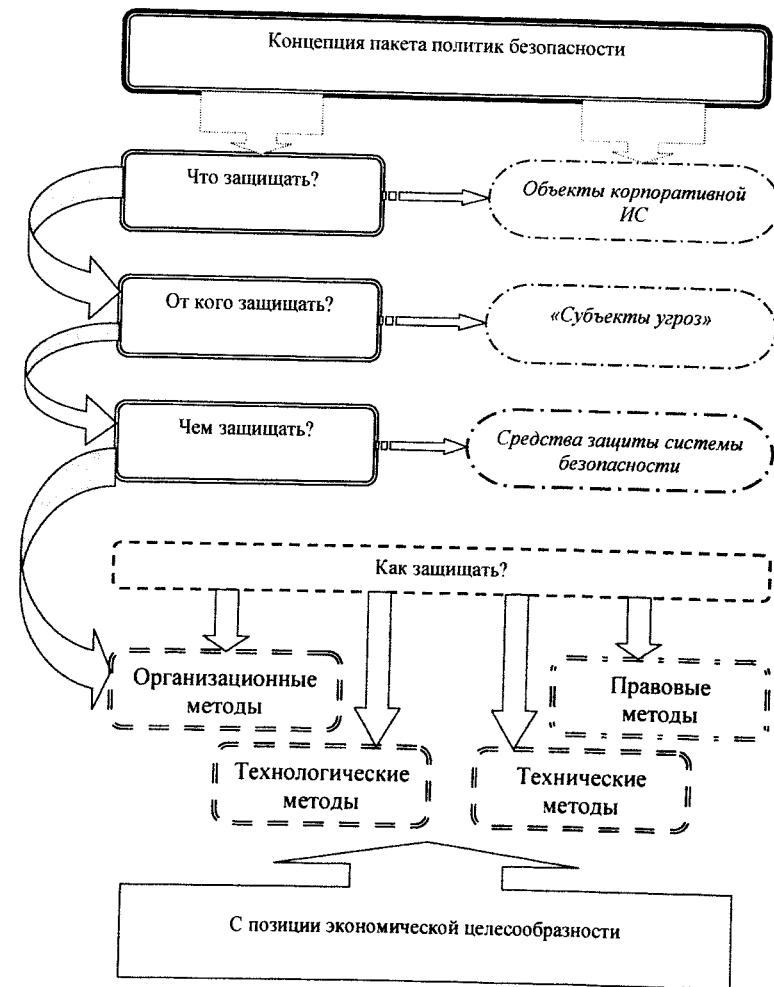


Рис. 5. Концепция пакета политик безопасности

Основная цель функционирования службы информационной безопасности, использующей комплекс средств защиты, – избежать или свести до минимума возможность нарушения, или вовремя за-

метить и устраниТЬ последствия дестабилизирующих факторов по отношению к системе.

Предполагается, что организационная составляющая пакета политик играет первостепенную роль, так как эффективность самых дорогостоящих и сложных средств защиты сводится к нулю, если пользователи системы будут игнорировать элементарные правила работы (например, будут нарушать правила предоставления доступа в систему и разрушать парольную политику системы).

Инженерно-техническое направление формируется на основе программных и аппаратных средств защиты.

Под *программными средствами защиты* следует понимать совокупность специальных программ, реализующих функции безопасности и режима функционирования системы.

К *аппаратным средствам защиты* относятся механические, оптические, лазерные, радиотехнические, биометрические и другие средства.

Выбор аппаратных и программных средств обеспечения безопасности во многом определяется разработанным пакетом политик.

Система безопасности должна быть эффективной, устойчивой к воздействиям, обеспечивать прозрачность, т. е. соответствовать требованиям международных и отечественных стандартов.

Вышесказанное свидетельствует о том, что, если система будет соответствовать стандартам, то она будет открыта для взаимодействия с любой другой системой, которая также соответствует стандартам (например, средствам криптографической защиты, средствам защиты от несанкционированного воздействия, средствам антивирусной защиты и др.). Это направление относится к *технологической составляющей пакета политик*, где предлагается сделать акцент на такое актуальное направление в комплексе системы защиты, как *стандартизацию*.

Правовое направление защиты трактуется как формирование совокупности законодательных актов, нормативно-правовых документов, положений, приказов, распоряжений, инструкций, требования которых являются обязательными в рамках деятельности предприятия.

Для поддержания пакета политик в актуальном состоянии на протяжении всего жизненного цикла системы необходимо выполнение следующих правил:

- непрерывный контроль исполнения пакета политик;
- повышение осведомленности пользователей системы в вопросах безопасности;
- обучение пользователей выполнению правил, предписываемых системой;
- регулярный пересмотр и корректировка правил безопасности.

С помощью предлагаемой концепции пакета политик можно разработать наиболее оптимальный комплекс средств защиты, а также смоделировать систему безопасности, экономически эффективную в борьбе против дестабилизирующих воздействий «субъекта угроз» на систему.

СОДЕРЖАНИЕ

Предисловие.....	3		
Раздел 1			
ТЕХНОЛОГИИ ОБРАБОТКИ ИНФОРМАЦИИ			
<i>Аминов Х. И. (СПбГИЭУ)</i> Моделирование банковской деятельности	4	<i>Евстюков Д. С. (СПбГИЭУ)</i> Механизмы и методы определения структуры статей доходов и расходов при бюджетировании проектов малоэтажного коттеджного строительства.....	83
<i>Брускова И. А., Бугорский В. Н. (СПбГИЭУ)</i> Основные этапы разработки бизнес-плана создания провайдерской фирмы.....	7	<i>Пиль Э. А. (СПбГИЭУ)</i> Силы, действующие на экономические оболочки	85
<i>Брускова И. А., Фомин В. И. (СПбГИЭУ)</i> Магистерская диссертация по направлению «Прикладная информатика»: варианты построения	21	<i>Ростовцева Т. В. (СПбГИЭУ)</i> Решение задачи оптимизации материально-технического снабжения строительно-монтажных работ.....	88
<i>Бугорский В. Н., Сергиенко А. Г. (СПбГИЭУ)</i> Особенности моделирования прогноза котировок ценных бумаг с использованием нейронных сетей	25	<i>Соколовская С. А., Стельмашонок Е. В. (СПбГИЭУ)</i> Цели и основные функции виртуального предприятия.....	93
<i>Горохов В. Л., Террикорни П., Барышев Ю. В. (СПбГИЭУ)</i> Конструирование компьютерных метафор на основе феноменологических онтологий для систем когнитивной машинной графики.....	29	<i>Фомин В. И. (СПбГИЭУ)</i> Структурно-типологический подход при моделировании затрат времени на повышение достоверности преобразования экономической информации	97
<i>Голосков К. П., Кусов А. А. (СПбГИЭУ)</i> Информационная база прогнозирования качества продукции.....	54	<i>Шапченко М. А. (СПбГИЭУ)</i> ИТ-системы управления на основе аутсорсинга	107
<i>Дашевский А. И., Янковский И. В. (СПбГИЭУ)</i> Прагматическая оценка применимости модели СММ в совершенствовании организационных процессов	61	<i>Ястребов А. И. (СПбГИЭУ)</i> Учет рисков, возникающих в процессе деятельности виртуальных предприятий в модели оценки стоимости	111
<i>Евдокимов В. А., Минаев Д. В. (СПбГИЭУ)</i> Интегральная оценка образовательных учреждений на основе интерактивного выявления субъективного мнения конечных потребителей	67		
<i>Евстратов А. Ю. (СПбГИЭУ)</i> Основные принципы формирования системы оценки стоимости кадрового потенциала предпринимательской структуры.....	77		
<i>Евстратов А. Ю., Царёв В. В. (СПбГИЭУ)</i> Проблемные вопросы получения стоимостной оценки кадрового потенциала.....	80		
Раздел 2			
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ДАННЫХ			
<i>Васильева И. Н. (СПбГИЭУ)</i> Правовые основы информационной безопасности и защиты информации в России.....	118		
<i>Попов Е. Б., Рогалёва И. А. (СПбГИЭУ)</i> Проблемы информационной безопасности.....	133		
<i>Поночевная И. В. (СПбГИЭУ)</i> Концепция построения унифицированной модели иерархии угроз.....	144		
<i>Поночевная И. В., Поночевный Д. А. (СПбГИЭУ)</i> Основные подходы к построению модели «субъекта угроз»	147		
<i>Поночевная И. В., Петрова А. М., Поночевый Д. А. (СПбГИЭУ)</i> Составляющие пакета политик системы безопасности	153		

НАУЧНОЕ ИЗДАНИЕ

**СОВРЕМЕННЫЕ
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ОБРАБОТКИ
И ЗАЩИТЫ ИНФОРМАЦИИ**

Сборник научных трудов

Редактор *Т. В. Янова*
Корректор *Е. Г. Закревская*
Компьютерная верстка *Л. А. Солдатовой*
Оформление обложки *Ю. А. Гайнутдиновой*

ИД № 00918 от 02.02.2000 г.

Подписано в печать 17.11.09. Формат 60×84¹/₁₆. Бумага типогр. № 1.
Печать цифровая. Усл.-печ. л. 9,41. Уч.-изд. л. 9,00. Изд. № 68. Тираж 200 экз. Заказ 860.

СПбГИСУ 191002, Санкт-Петербург, ул. Марата, 27.
ИзПК СПбГИСУ 191002, Санкт-Петербург, ул. Марата, 31.