

Федеральное агентство по образованию  
Государственное образовательное учреждение  
высшего профессионального образования  
«Санкт-Петербургский государственный  
инженерно-экономический университет»



Посвящается 100-летию  
Университета ИНЖЭКОН

**СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ  
ОБРАБОТКИ И ЗАЩИТЫ ИНФОРМАЦИИ**

Сборник научных трудов

**ИНЖЭКОН**



**Санкт-Петербург  
2005**

УДК 378.001.658.011.56  
ББК 32.97  
С56

*Утверждено редакционно-издательским советом СПбГИЭУ*

**Рецензенты:**

кафедра математического моделирования СПбГУИТМО (зав. кафедрой  
д-р техн. наук, проф. С. И. Росс),  
д-р техн. наук, проф. А. Н. Жуковский (СПбГУ)

**Редакционная коллегия:**

д-р физ.-мат. наук, проф. В. Л. Горохов (отв. ред., СПбГИЭУ); канд. экон.  
наук, доц. И. Г. Гниденко (зам. отв. ред., СПбГИЭУ); канд. техн. наук,  
проф. Ф. Ф. Паевов (чл. редкол., СПбГИЭУ)

*Одобрено к изданию научно-техническим советом СПбГИЭУ*

**C56 Современные информационные технологии обработки и  
защиты информации: Сб. науч. тр. / Редкол.: В. Л. Горохов (отв.  
ред.) и др. – СПб.: СПбГИЭУ, 2005. – 139 с.**

ISBN 5-88996-604-9

Рассматриваются проблемы применения информационных технологий в различных сферах (разработка алгоритмов решения задач, моделирование, прогнозирование работы сложных систем, информационная поддержка принятия экономических решений, управление информационными технологиями, вопросы компьютерного обучения и оценки качества такого обучения), а также проблемы защиты информации (анализ существующих информационных рисков, использование средств и методов криптографической защиты информации, защита информационных систем).

Сборник подготовлен на кафедре вычислительных систем и программирования и предназначен для преподавателей, аспирантов и студентов, специализирующихся в области информационных технологий и защиты информации.

ISBN 5-88996-604-9

УДК 378.001.658.011.56  
ББК 32.97

© СПбГИЭУ, 2005

## **ПРЕДИСЛОВИЕ**

Переход к информационному обществу вызвал бурное развитие технологий обработки и передачи информации во всех сферах деятельности. 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 моделирования информационных систем разработки систем искусственного интеллекта, систем поддержки принятия управленческих решений, создания компьютерных тренажеров и автоматизированных систем обучения, а также оценки его эффективности.

Во втором разделе рассматриваются основные технологии защиты данных, методы повышения достоверности информации, основные алгоритмы защиты, обеспечение безопасности информации при работе в компьютерных сетях.

Сборник предназначен для преподавателей, аспирантов, магистров, студентов, а также всех, кто интересуется проблемами применения современных технологий обработки и защиты информации.

**Редакционная коллегия**

## Раздел I

# ТЕХНОЛОГИИ ОБРАБОТКИ ИНФОРМАЦИИ

УДК 378.001

© В. Л. Бродо, Р. Р. Шарипов  
Санкт-Петербургский государственный  
инженерно-экономический университет

### ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ НА СТОЛЕ РУКОВОДИТЕЛЯ

Стабилизация экономики, снижение инфляционных сверхприбылей и спекулятивных доходов лишают возможности делать «легкие» деньги практически без риска и ведут к обострению конкуренции. Чтобы устоять в новых условиях, от бизнесменов требуется умение принимать максимально взвешенные решения и определять оптимальную финансовую стратегию. Эффективное управление крупным и средним бизнесом сегодня немыслимо без применения передовых информационных технологий – систем поддержки принятия решений (СППР).

В настоящее время в бизнесе реально следует рассчитывать лишь на использование комплексного программного обеспечения (ПО). Сегодня мы являемся свидетелями стремительного прогресса в создании подобного ПО под общим названием OLAP (On-line Analytical Processing). Предназначение новых технологий хранилищ данных и OLAP – заполнить объективно существующие разрывы познавательной деятельности.

Хранилища данных по своей сути больше идея, чем технология. Идея заключается в том, чтобы собрать в едином по крайней мере с точки зрения пользователя месте всю информацию, которая может понадобиться управляющему при принятии решения. Источниками данных для информационного хранилища служат в первую очередь данные из разрозненных транзактных информационных систем, основанных на различных реляционных СУБД, которые об-

служивают повседневную бизнес-деятельность. Следует особо подчеркнуть, что хранилище данных не предназначается для замены существующих систем, а является как бы надстройкой над ними. В хранилище данных могут быть включены сведения о клиентах, о штатном персонале, о конкурентах, о демографической ситуации, о показателях экономики и др. Источниками необходимой информации могут быть газеты, радио, телевидение, Интернет и любые др. При этом предполагается, что данные предварительно должны быть приведены к единым стандартам, очищены от противоречий, структурированы и обобщены с требуемым уровнем детализации. Прогнозируемый объем хранилищ данных оценивается в десятки терабайт. Сама идея хранилищ данных не является новой. Отличительной особенностью хранилищ являются лишь прогнозируемые объемы хранимой информации, которые позволяют надеяться получить качественно новое свойство БД – восполнить разрывы познавательной деятельности аналитика, которые состоят в ограниченности личного опыта и невозможности проводить целенаправленные эксперименты. Не без основания предполагается, что в процессе анализа показателей собственной коммерческой деятельности и деятельности конкурентов в их взаимосвязи с внутренними и внешними факторами аналитик выработает интуицию, необходимую для выдвижения гипотез, а затем сумеет проверить справедливость найденных закономерностей, но не в ходе проведения целенаправленного эксперимента, а опять же при помощи информации из хранилища, которая уже содержит результаты требуемых опытов, поставленных самой жизнью.

Программные средства OLAP – это инструмент оперативного анализа данных, содержащихся в хранилище. Главной особенностью является то, что эти средства ориентированы на использование не специалистом в области информационных технологий, не экспертом-статистиком, а профессионалом в прикладной области – менеджером кредитного отдела, менеджером бюджетного отдела, начальником, директором. Они предназначены для общения аналитика с проблемой, а не с компьютером.

Имея гибкие механизмы манипулирования данными и визуального отображения, исследователь, как правило, сначала рассматривает с разных сторон данные, которые могут быть (а могут и не быть) связаны с решаемой проблемой, не имея при этом никаких

идей, просто пытаясь заметить какие-либо особенности. Сопоставляет различные показатели бизнеса между собой, стараясь выявить скрытые взаимосвязи. Заинтересовавшись какой-либо позицией, он может рассмотреть данные более пристально, детализировав их, например, разложив на составляющие по времени, по регионам или по клиентам, или наоборот еще более обобщить представление информации, чтобы убрать отвлекающие подробности. У него, например, может зародиться гипотеза о том, что разброс роста активов в различных филиалах банка зависит от соотношения в них специалистов с техническим и гуманитарным образованием. Тогда аналитик может запросить из хранилища (а не у отдела информатизации!) и отобразить на одном графике интересующее его соотношение для тех филиалов, у которых за текущий квартал рост активов снизился по сравнению с прошлым годом более чем на 10% и для тех, у которых повысился более чем на 25%. Для этого исследователь должен иметь возможность использовать не сложный SQL-запрос, а простой выбор из предлагаемого меню. Если полученные результаты ощутимо распадутся на две соответствующие группы, то это должно стать стимулом для дальнейшей проверки выдвинутой гипотезы. Может быть полученные результаты извлекут из подсознания какие-то новые ассоциации и поиск начнет продвигаться в другом направлении. По всей видимости, сегодня мы являемся свидетелями достаточно редкого явления – широкого внедрения элементов искусственного интеллекта в практическую деятельность, да еще в такой заповедной области как бизнес. В отличие от традиционных систем искусственного интеллекта технология OLAP не пытается моделировать естественный интеллект, а усиливает его возможности мощностью современных вычислительных серверов и хранилищ данных.

Универсальность законов психологии, положенных в основу OLAP, позволяет разработчику приложений мало заботиться о характере возможных запросов данных конечным пользователем. Законы человеческого мышления мало изучены. Вместе с тем вряд ли кто-нибудь сомневается в том, что общие законы мышления существуют и действуют. Можно сколько угодно критиковать 12 признаков OLAP-систем, декларированных Коддом (Codd), но основная их часть сформировалась под влиянием каких-то, пока не познан-

ных, законов человеческого мышления. К признакам OLAP, основанным на законах психологии, следует отнести:

- разделение данных на показатели (переменные) и измерения, определяющие соответственно состояние и пространство бизнеса;
- логическое представление значений показателей в виде многомерных кубов, упорядоченных по равноправным измерениям;
- неограниченное число и количество уровней иерархических связей между значениями измерений;
- гибкое манипулирование данными. Возможность построения подмножества значений показателя по любому дискриминирующему правилу, определенному на множестве значений его измерений. Логические операции над полученными множествами;
- неограниченные возможности агрегирования заданного подмножества значений показателя;
- возможность обработки запросов в «реальном времени» в темпе процесса аналитического осмысливания данных пользователем;
- развитые средства табличного и главное графического представления данных конечному пользователю.

Важность гибкого графического представления хотелось бы подчеркнуть особо. Такие выдающиеся ученые, как Жак Адамар и Жуль Пуанкарэ, которые пытались при помощи самоанализа изучить творческий процесс математического открытия, сошлись во мнении, что мыслят при решении сложной задачи не словами, не математическими знаками, а некоторыми геометрическими образами и, когда воображаемые образы соединяются в решение, то остается только формализовать его в символном виде, чтобы донести это решение до остальных. Современная психология также утверждает, что творческое мышление – образно. Она называет его право-полушарным. Не углубляясь в психологические аспекты проблемы, приведем известный факт, что человеческий мозг способен воспринимать и анализировать информацию, которая представлена в виде геометрических образов, в объеме на несколько порядков большем, чем информацию, представленную в алфавитно-цифровом виде.

Наглядные геометрические образы, связанные с решаемой проблемой, колossalно стимулируют творческое мышление и приводят к открытиям даже в такой формальной области, как теория чисел. Один из ведущих российских специалистов в области искус-

ственного интеллекта профессор Д. Поспелов назвал системы, по-добные OLAP, новым окном в мир познания. Важность развитого графического представления информации и его влияние на интуицию исследователя подчеркивают и зарубежные специалисты.

Технология OLAP призвана повысить эффективность информационно-аналитической и управленческой деятельности руководящего персонала. Используя эти средства, можно быстрее и более обоснованно принимать оперативные и стратегические решения. Открытые при помощи OLAP закономерности реализуются затем в экономические модели, позволяющие заглянуть в будущее, которое, по словам Нейла Рейдена (Neil Raden), президента «Archer Decision Sciences Inc.», «принадлежит тому, кто сможет его предвидеть и первым к нему приблизится».

УДК 378.001

© А. Ю. Потягайло

Санкт-Петербургский государственный  
инженерно-экономический университет

## ПРОЕКТНЫЙ ПОДХОД К СОЗДАНИЮ И РАЗВИТИЮ ИНФОРМАЦИОННОЙ СРЕДЫ ТЕХНОЛОГИЧЕСКОГО ОБРАЗОВАНИЯ

Необходимость адаптации современного общества к жизни в условиях информационного взрыва активизировала внедрение научных технологий в различные сферы деятельности: науку, промышленность, сельское хозяйство, медицину, образование. В результате произошла постепенная трансформация существовавшего привычного мира вещей и понятий в мир информации и информационных технологий.

В современном информационном мире информация получила статус ключевого понятия наравне с материей и энергией, а технология как область научных знаний и процесс осознанной деятельности человека переросла в системный феномен современной действительности, оказывая системоформирующее воздействие на все сферы жизнедеятельности человека и социума в целом. Информационная революция породила новую, информационную цивилизацию,

цию, важнейшей особенностью которой является качественно новый уровень значимости образования, в особенности, технологического.

Указанные положения позволяют утверждать, что сегодня, как, может быть, никогда ранее, возрастает роль подготовки школьников и студентов по профилю технологического образования. Будущие специалисты призваны стать носителями и пропагандистами системного технологического мышления и, в целом, технологической культуры, адекватной сложному и многогранному миру. С этой точки зрения очевидной становится необходимость фундаментализации и структурной систематизации технологического образования на основе органичного сочетания естественнонаучной и технической составляющих всей совокупности технологических знаний, объединенных в стройную и логически непротиворечивую систему. При этом развитие технологического образования предполагает не только его содержательную и структурную перестройку, но и поиск новых педагогических технологий передачи целостного технологического знания.

Совокупность таких технологий и современных условий их реализации определяет информационную среду технологического образования как основу его эффективного функционирования. Учитывая указанное назначение информационной среды, можно утверждать, что она представляет собой сложную, многосвязную систему информационных объектов. Само понятие информационной среды и интуитивные методы ее создания и развития для различных уровней образования используются достаточно широко. Однако проблема ее квалифицированного, профессионального проектирования в современном информационном обществе становится все более актуальной. В связи с этим представляется весьма актуальным и перспективным применение проектного метода создания и развития информационной среды технологического образования, причем эффективная реализация такого подхода, в свою очередь, базируется на использовании современных информационных технологий управления проектами.

Научная проблема создания информационной среды технологического образования на современном этапе заключается в разрешении целого ряда противоречий и, прежде всего, между все еще существующей и довольно значительной разобщенностью информа-

мационных, кадровых и иных ресурсов в географических условиях нашей страны и важнейшей тенденцией к стандартизации технологического образования.

Концептуальная основа решения научной проблемы создания информационной среды технологического образования на современном этапе заключается в разработке методологии проектирования информационной среды в образовательной области «Технология» для школ и различных специальностей вузов как средства повышения готовности школьников профильных классов и студентов вузов к профессиональной деятельности в сфере образования, производства товаров и услуг, предпринимательства.

Указанная методология должна определять пути решения следующих основных задач, которые можно выделить в результате декомпозиции глобальной научной проблемы создания информационной среды технологического образования:

- системный анализ социального заказа современного информационного общества на подготовку специалистов по направлению технологического образования с позиций его исторической эволюции и инновационных тенденций развития российского образования;

- разработка и исследование принципов создания и структуры информационной среды как педагогического пространства для подготовки специалистов по направлению технологического образования, ее роли и места в общей системе образования на современном этапе развития науки и техники;

- создание и обоснование концепции развития информационной среды технологического образования для школ и вузов в современных условиях;

- формирование принципов автоматизации проектирования информационной среды в образовательной области «Технология» для школ и вузов на основе применения современных информационных технологий;

- создание методики проектирования информационной среды в образовательной области «Технология» для школ и вузов, а также методики оценки эффективности ее реализации при обучении школьников и студентов вузов.

Каждая из перечисленных задач – весьма масштабна и может служить предметом отдельного рассмотрения. Пути решения ряда

сформулированных задач определены в работах автора и других исследователей. Однако следует отметить, что на сегодняшний день отсутствует общая методология проектирования информационной среды технологического образования, а существующая практика разработки информационных сред опирается на интуитивные методы.

Такое положение нельзя считать удовлетворительным еще и потому, что как в школьном, так и в высшем профессиональном образовании, все более острой становится потребность в проектировании и создании информационных сред, обеспечивающих образовательный процесс на различных уровнях подготовки: от школьников старших классов до студентов, магистрантов и аспирантов. В этих условиях решение научной задачи разработки общей методологии проектирования информационной среды технологического образования является ключевым для обеспечения всего процесса успешного развития технологического образования.

Развитие последнего положения в современных условиях позволяет предложить для автоматизации проектирования информационной среды технологического образования школы и педагогического вуза современную информационную технологию Microsoft Project Professional 2003. Основной идеей такого подхода считается распространение методов управления проектами в производственной деятельности различных предприятий на предметную область технологического образования.

При этом реализуется широкий спектр возможностей Microsoft Project Professional 2003 в обеспечении календарного, ресурсного, бюджетного планирования и оптимизации проекта создания информационной среды технологического образования при любой степени детализации, адекватной целям, задачам и ресурсам различных образовательных учреждений как высшего профессионального, так и школьного профильного обучения.

Существенными преимуществами предлагаемого подхода перед используемыми ранее интуитивными методами создания информационной среды являются возможность автоматизации мониторинга и управления проектами, организации командной работы над проектами, а также работы с портфелем проектов создания информационных сред для обеспечения технологического образования любого уровня.

Таким образом, можно сделать вывод об актуальности предлагаемого направления и перспективности его практического использования для развития современного технологического образования.

УДК 378.001

© В. Л. Стельмашонок

Санкт-Петербургский государственный  
инженерно-экономический университет

## ОБЗОР МЕТОДОВ МОДЕЛИРОВАНИЯ СТРУКТУР СЛОЖНЫХ СИСТЕМ

Для моделирования структур сложных систем в настоящее время используют, как правило, графический, графо-аналитический и аналитический методы их формализации. Такое деление методов (способов) формализованного описания структур в ряде случаев достаточно условно вследствие того, что фрагменты одного метода могут содержаться в другом, дополняя, расширяя его, и т. п. Однако в общем случае использование любого метода формализации структур основано на следующих положениях:

- система функционирует во времени, взаимодействует с внешней средой, и в каждый момент времени может находиться в определенном состоянии;
- система является относительно обособленной, так как способна принимать, обрабатывать и выдавать информацию;
- система способна к реконфигурации своих структур в строго определенных границах по результатам оценки своего состояния;
- структуры системы отражают строение внутреннего взаимодействия некоторой совокупности элементов.

В настоящее время выбор того или иного метода формализации во многом зависит от типа описываемой структуры. Так, например, для описания организационных структур наиболее часто используется графический метод, при котором вершинам графа ставятся в соответствие элементы системы, а структурные связи отображают их соподчиненность. Графический метод применяется также при описании некоторых информационных структур. Если систему представить как множество элементов, объединенных прямыми и обратными связями, которые имеют некоторый коэф-

фициент передачи информации (задержки, трансформации, объема и т. п.), то данную совокупность можно формализовать графом Мейзона (рис. 1). Указанный график позволяет непосредственно рассчитывать обобщенные коэффициенты передач между любой парой его вершин.

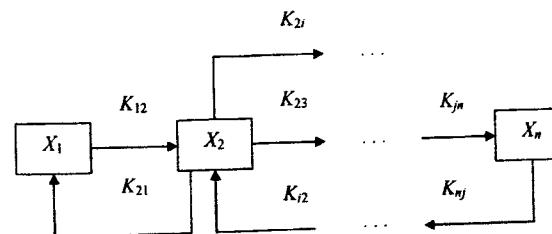


Рис. 1. Фрагмент графа Мейзона:

$X_i$  – элемент системы;  $K_{ij}$  – коэффициент передачи из  $i$ -го элемента в  $j$ -й

Если при изучении информационных структур необходимо учитывать возможности самих элементов, то график Мейзона нетрудно трансформировать в график Коутса, который показан на рис. 2.

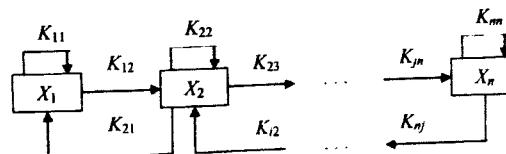


Рис. 2. Фрагмент графа Коутса

Однако применение рассмотренных графов ограничено, вследствие весьма узкого спектра решаемых задач и невозможности использования этих графов для описания большинства других структур системы.

К графоаналитическим методам формализации алгоритмических структур относится широко применяемый метод структурных схем и передаточных функций. Элементы такой структуры рассматриваются как динамические звенья, которые выступают в роли операторов преобразования информации, циркулирующей в системе (рис. 3).

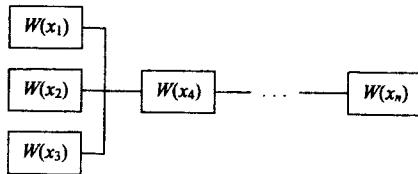


Рис. 3. Динамическая схема системы:  
 $W(x_i)$  – передаточная функция  $i$ -го элемента

Существуют определенные правила преобразования таких структурных схем. Поскольку структурные схемы являются графическим изображением дифференциальных уравнений движения потоков информации в системе, поскольку их преобразования адекватно отображают преобразования этих уравнений. Следует отметить, что преобразование структурных схем практически оказывается чрезвычайно сложной и трудоемкой процедурой. При большой же размерности системы (большом количестве элементов) данный метод оказывается непригодным из-за резкого увеличения громоздкости выкладок. Кроме того, метод структурных схем и передаточных функций направлен на изучение динамических свойств системы и никак не учитывает внутреннее строение и организацию ее элементов.

В настоящее время все большее применение для исследования структур параллельных и последовательно-параллельных процессов, протекающих в системах, находят сети Петри. Сеть Петри – это набор  $\langle P, T, I, O, M \rangle$ , где  $P = \{p_1, p_2, \dots, p_n\}$  – конечное множество позиций;  $T = \{t_1, t_2, \dots, t_m\}$  – конечное множество переходов;  $I$  – входная функция (отображение множества переходов в комплексы позиций);  $O$  – выходная функция;  $M$  – маркировка сети, отображающая множество позиций в множество неотрицательных чисел  $N$ .

Сеть Петри может быть представлена как двудольный ориентированный мультиграф, возможно, нагруженный информацией о фишках и переходах (понимая под фишкой объект сети, использующийся для определения ее выполнения). Сети Петри применяются, как правило, для описания и моделирования систем, центральную часть которых составляют ЭВМ. Основная ценность сетей заключается в способности формализовать и анализировать некоторые свойства процессов в структурах системы. К таким свойствам

относятся: безопасность, ограниченность, сохранение, активность, достижимость, покрываемость.

Несмотря на то, что с помощью сетей Петри можно моделировать большой класс систем, существуют объекты, которые нельзя адекватно описать сетью Петри. Кроме того, сеть Петри предполагает наличие определенной структуры системы, которая составляет материальную основу протекающих в ней процессов. Следовательно, сеть Петри (по определению) не в состоянии учсть особенности внутреннего строения (организации) системы.

Для формализации морфологических структур (структур, в которых элементы представляют собой реальные физические объекты, – части системы) в настоящее время все чаще используются аналитические методы их описания. К этим методам относятся: метод структурных матриц, метод структурных чисел, метод структурных функций, а также методы, основанные на алгебре логик.

Содержание метода структурных матриц составляет математический аппарат преобразования передаточных функций элементов системы на основе их матричного описания, который в значительной степени упрощает вычисления по сравнению с методом структурных схем и передаточных функций. Однако методами, которые в наибольшей степени затрагивают вопросы внутренней организации системы и обладают достаточной общностью, являются методы структурных чисел и функций. Первый из них рассматривает структуру как некоторое абстрактное число, имеющее определенные свойства, обусловленные системой взаимоотношений в структуре. При этом сама структура описана в строгих топологических терминах. Изменение взаимоотношений в структуре влечет изменение свойств структурного числа, которое используется для оптимизации организации данных взаимоотношений. Главная задача второго метода – метода структурных функций – состоит в построении функции, аргументом которой является структура, представленная некоторым комбинаторным оператором. Указанная функция отображает множество структур, полученное комбинаторикой, в множество значений, определяющих качество комбинаторной схемы, что выражает, по сути дела, косвенную оценку организации элементов системы.

Метод, который наиболее полно позволяет описать внутреннее строение и организацию системы, обладает абсолютной общностью (пригоден для формализации любого типа структур) и имеет хоро-

шо разработанный математический аппарат – топологический метод формализованного описания структур. Пуанкаре так определял содержание Analysis situs (геометрии положения, как тогда называли топологию): «Analysis situs есть наука, которая позволяет нам узнавать качественные свойства геометрических фигур не только в обычном пространстве, но также и в пространстве больше трех измерений. Analysis situs в трех измерениях является для нас познанием почти интуитивным; напротив, Analysis situs в более чем трех измерениях представляет громадные трудности, и чтобы начать пытаться их преодолевать, нужно быть очень убежденным в крайней важности этой науки. Если эта важность не всем понятна, то это потому, что об этом недостаточно размышляли». Качественные свойства геометрических фигур уже тогда было принято называть топологическими. Анализ топологических (внутренних) свойств объекта был направлен на характеристику частей и их положений в целом (объекте) относительно других частей и их положений, описание взаимосвязи этих частей, оценку целостности и силы их связности.

Было замечено, что если геометрической фигуре поставить в соответствие граф, то последний должен обладать такими же топологическими свойствами, что и сама фигура независимо от того, в скольких измерениях она описана. Иными словами, любая структура системы, описанная в топологических терминах и обладающая топологическими свойствами, может быть при определенных условиях представлена графом, который раскрывает сущность организации структуры и, следовательно, некоторого аспекта строения системы. Поэтому топологический метод как самостоятельный метод исследования синтезирует в себе указанные выше методы формализации структур, так как он является наиболее общим по отношению к теории множеств, графов, матриц и т. д.

В данном методе фундаментальным понятием является понятие собственно топологии, которое, будучи абсолютно абстрактным, позволяет описать строение связного множества элементов любой природы с точки зрения внутреннего устройства этого множества. Имея такое формализованное описание (топологическую структуру), представляется возможным выделить и оценить важнейшие топологические свойства структуры, проявления которых в своей совокупности и обуславливают качество организации и взаимодействия элементов данного множества.

Таким образом, учитывая вышеизложенное, методом, который обладает наибольшими потенциальными возможностями для формализованного описания и анализа структур системы, а также имеет хорошо разработанный математический аппарат, является топологический метод исследования. Применение этого метода в графоаналитическом моделировании структур и будет рассматриваться в дальнейшем.

УДК 378.001

© С. А. Путилов

Санкт-Петербургский государственный  
инженерно-экономический университет

## ТЕХНОЛОГИЯ ПАРАМЕТРИЧЕСКИ-ОРИЕНТИРОВАННОГО ПРОГРАММИРОВАНИЯ

Рассмотрим конфигурирование типовой информационной системы параметрически-ориентированного проектирования на примере «1С:Предприятие 8.0».

Все составляющие системы программ «1С:Предприятие 8.0» можно разделить на технологическую платформу и конфигурации. Технологическая платформа представляет собой набор различных программных компонентов, настроенных на особенности управления конкретным предприятием и используемых для автоматизации экономической деятельности и не зависящих от конкретного законодательства и методологии учета. Конфигурации являются, собственно, прикладными решениями.

Система «1С:Предприятие 8.0» состоит из трех ключевых составляющих (рис. 1):

- приложение 1С:Предприятие – программная среда, в которой функционирует макропрограмма, называемая «конфигурацией». Она предназначена для трансляции и запуска минимально необходимого набора программных компонентов;
- конфигурация – макропрограмма, определяющая функциональность решаемых пользователем задач, в том числе и настройку интерфейса;
- конфигуратор – основная среда разработки конфигурации (пользовательской программы).



Рис. 1. Схема составляющих программы «1С:Предприятие 8.0»

Особенностью системы программ «1С:Предприятие 8.0» является возможность изменения конфигурации самим пользователем или организациями, специализирующимися на внедрении и поддержке программных продуктов 1С. Эта возможность позволяет обеспечить необходимое соответствие автоматизированной системы особенностям учета в конкретной организации.

Технологическая платформа «1С:Предприятие 8.0» содержит средство разработки, с помощью которого создаются новые или меняются существующие прикладные решения. Это средство разработки называется «конфигуратор». Конфигуратор представляет собой специальный режим запуска системы «1С:Предприятие 8.0» и может быть вызван прямо из окна запуска «1С:Предприятие» (рис. 2).

Так как конфигуратор включен в стандартную поставку системы «1С:Предприятие 8.0», то пользователь может самостоятельно или с помощью сторонних специалистов разработать или модифицировать прикладное решение.

Окно конфигурации позволяет:

- создавать новые объекты конфигурации;
- редактировать существующие объекты конфигурации;
- удалять объекты конфигурации с контролем наличия ссылок на удаляемый объект;
- располагать объекты конфигурации в требуемом порядке в пределах «своей» группы;

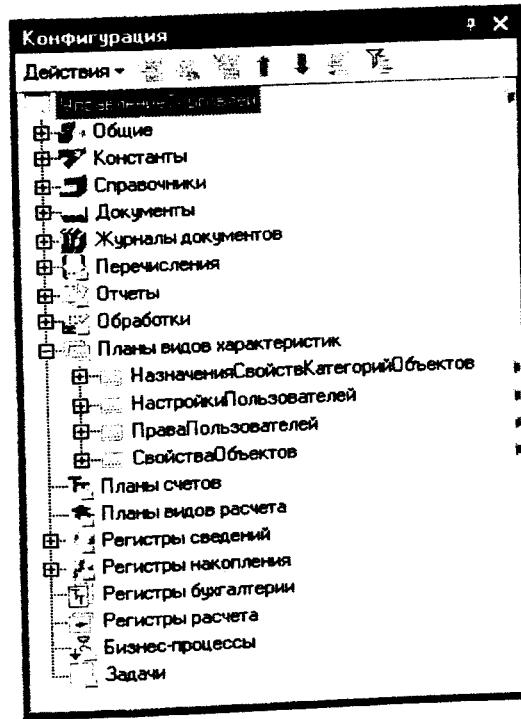


Рис. 2. Окно конфигурации «1С:Предприятие 8.0»

- находить в «дереве» объект, данные которого в данный момент редактируются (в окне редактирования объекта, в редакторе формы, макета, модуля);
- сортировать объекты конфигурации, подчиненные одному объекту конфигурации, по имени, синониму или комментарию;
- искать ссылки на данный объект конфигурации в других объектах конфигурации;
- искать ссылки на другие объекты конфигурации в данном объекте конфигурации;
- отбирать объекты конфигурации по принадлежности к каким-либо подсистемам, определенным в конфигурации;
- запускать конструкторы, связанные с объектом конфигурации.

Структура конфигурации создается с помощью визуальных средств при использовании различных конструкторов. Разработчик прикладного решения сосредотачивается на реализации бизнес-логики и интерфейса, при этом основную долю технологических задач выполняет система. Даже начинающий разработчик может освоить систему и быстро начать создавать свои собственные конфигурации или модифицировать существующие.

Конфигуратор предоставляет разработчику все необходимые инструменты для визуального описания структуры прикладного решения, создания форм диалогов и выходных документов, механизмов работы пользователей с данными (интерфейсов) и прав доступа различных групп пользователей к информации. Кроме того, конфигуратор позволяет создавать и настраивать взаимодействие различных элементов прикладного решения друг с другом и писать модули на встроенным объектно-ориентированном языке для обработки различных событий и реализации специфических алгоритмов взаимодействия, обработки входных и выходных данных.

Любое прикладное решение в «1С:Предприятие 8.0» имеет в своей основе набор проблемно-ориентированных объектов, поддерживаемых на уровне технологической платформы. Задача разработчика заключается в том, чтобы собрать из таких объектов, как из конструктора, необходимую структуру прикладного решения и затем описать специфические алгоритмы функционирования и взаимодействия этих объектов, отличающиеся от их типового поведения.

Состав объектов, поддерживаемых технологической платформой, является результатом анализа предметных областей использования «1С:Предприятие 8.0», выделения и классификации используемых в этих областях бизнес-сущностей. В результате этого анализа разработчик может оперировать такими объектами, как справочники, документы, регистры сведений и т. п.

Чтобы стандартизировать и упростить процесс разработки и модификации прикладных решений, разработчику предоставляется графический интерфейс, с помощью которого он имеет возможность описать состав объектов, используемых в конкретном прикладном решении.

На основании этого описания технологическая платформа создаст в базе данных соответствующие информационные структуры и определенным образом будет работать с данными, хранящимися в этих структурах. Разработчику нет необходимости заботиться о том, в каких таблицах, например, должны размещаться данные, как они будут модифицироваться или предоставляться пользователю. Все эти действия платформа будет выполнять автоматически исходя из типового поведения используемых объектов.

Таким образом, разработчик оперирует метаданными – «данными о данных», или объектами конфигурации. Добавляя в структуру прикладного решения очередной объект, разработчик добавляет описание того, как будут размещаться соответствующие данные и как они будут взаимодействовать с другими данными, хранящимися в информационной базе.

Рассмотрим некоторые возможности настроек основных объектов конфигурации.

1. Справочники позволяют хранить в информационной базе данные, имеющие одинаковую структуру и списочный характер. Это может быть, например, список сотрудников, перечень товаров, список поставщиков или покупателей. Каждый элемент справочника характеризуется кодом и наименованием. На этапе конфигурирования можно настроить вид справочника, способ отображения информации и т. п.

2. Документы позволяют хранить в прикладном решении информацию о совершенных хозяйственных операциях или о событиях, произошедших в «жизни» предприятия вообще. Это могут быть, например, приходные накладные, приказы о приеме на работу, счета, платежные поручения и т. д. На этапе конфигурирования можно описать алгоритмы проведения документа, его заполнение, набор реквизитов и т. п.

3. Планы счетов предназначены для построения модели, реализующей систему двойной записи бухгалтерского учета. Реализуют многоуровневые планы счетов с фиксированной или переменной разрядностью кодов, многоуровневый и многомерный аналитический учет, учет по нескольким планам счетов, учет по нескольким организациям, опциональное ведение количественного, суммового и валютного учета по отдельным разрезам аналитики и т. д.

4. Регистры сведений позволяют хранить в прикладном решении произвольные данные по нескольким измерениям. Например, в регистре сведений можно хранить курсы валют в разрезе валют, или цены предприятия в разрезе номенклатуры и типа цен. Информация в регистре сведений хранится в виде записей, каждая из которых содержит значения измерений и соответствующие им значения ресурсов. Измерения регистра описывают разрезы, в которых хранится информация, а ресурсы регистра непосредственно содержат хранимую информацию.

Рассмотрим пример настройки учета основных средств и расчета амортизации. Первоначальная поставка имеет ряд свойств, позволяющих сразу приступить к задаче. Пользователь может:

- вести учет основных средств, находящихся в эксплуатации;
- вести учет основных средств, находящихся на консервации;
- осуществлять постановку на учет любого количества одинаковых основных средств;
- оформлять перевод основных средств в категорию МБП;
- регистрировать ввод основных средств в эксплуатацию/вывод их из эксплуатации при списании/реализации, передачу в ремонт, модернизацию или реконструкцию;
- проводить переоценку по индивидуальным коэффициентам или по единому коэффициенту для всех основных средств;
- проводить дооценку основных средств, связанную с дополнительными расходами и т. п.

Конфигурация позволяет рассчитывать амортизацию с учетом различных факторов: амортизуемой стоимости, срока полезного использования, объема продукции или работ, пробега (для автотранспорта), поправочного коэффициента. В настройке могут быть выбраны следующие способы начисления амортизации:

- линейный способ;
- способ уменьшающего остатка;
- способ списания стоимости пропорционально объему продукции;
- способ использования единых норм амортизации из классификатора;
- способ списания стоимости по сумме чисел лет срока полезного использования.

УДК 378.001

© С. А. Соколовская

Санкт-Петербургский государственный  
инженерно-экономический университет

## ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ГЕНЕРАТОРА ОТЧЕТОВ CRYSTAL REPORTS

Одной из главных задач корпоративных информационных систем является оперативное представление информации, необходимой для принятия решений. Современные системы управления базами данных позволяют хранить структурированные данные, а не направлены на оптимизацию произвольной выборки и представления данных. Вследствие этого информация, хранящаяся в корпоративных информационных системах, как правило, используется неэффективно. Главной проблемой становится не хранение информации, а предоставление ее конечному пользователю в виде отчета в нужном контексте.

Специфика аналитических отчетов, предназначенных для облегчения процесса принятия решений, состоит в их изменчивости, поскольку в реальной жизни требования бизнеса изменяются чуть ли не каждый день. Генератор отчетов Crystal Reports позволяет:

- оперативно создавать сложные отчеты презентационного качества на основе имеющейся в базах данных или электронных таблицах информации;
- разрабатывать Windows-приложения, способные создавать такие отчеты;
- публиковать отчеты в Web для распространения их в масштабе компании и даже за ее пределами.

Crystal Reports имеет большое число экспертов (специальных средств для создания отчета в интерактивном режиме), позволяющих даже неподготовленному пользователю создать отчет в короткие сроки. Помимо традиционных иерархических отчетов, Crystal Reports позволяет создавать матричные отчеты (Cross-tab) и OLAP-отчеты, а также отчеты, включающие различные типы графиков и географические карты. Использование гиперссылок позволяет связать объекты отчета, включая текст, графику, поля БД и формулы с Web-сайтами, e-mail адресами и другими отчетами Crystal Reports.

Возможно распространение отчетов по электронной почте, экспорт в форматы HTML, PDF, RTF и другие, компиляция в exe-файлы.

Crystal Reports обеспечивает широкие возможности использования разнообразных источников данных, облегчая доступ к источникам корпоративной информации и удовлетворяя информационные запросы конечных пользователей. Если необходим доступ к базам данных, файлам, журналам, системным приложениям (CRM, ERP и т. д.) или программным элементам, всегда можно использовать Crystal Reports.

Crystal Reports предлагает высокий уровень гибкости и контроля над методами представления и форматирования данных.

*Визуальный проектировщик отчетов.* При быстром интерактивном проектировании отчетов используется интуитивно понятный интерфейс перетаскивания (drag-and-drop) и объектно-ориентированные проводники.

*Эксперты и мастера.* Возможности экспертов и мастеров используются для упрощения стандартных задач создания отчетов, таких, как связь с источниками данных, выбор, группировка, сортировка и окончательная обработка информации.

*Поддержка всех типов отчетов* – позволяет создавать практически любые требуемые отчеты, используя возможность включения матричных отчетов, условных операторов, специальную сортировку групп (Top N/Bottom N), итоговые значения и иерархическую детализацию данных, формы, адреса электронной почты, OLAP и подотчеты.

*Составление диаграмм и схем* – дает возможность улучшить внешний вид создаваемых отчетов, используя графические элементы из большого списка доступных таблиц и диаграмм различных типов (включая панели инструментов, в том числе объемные; секторные/торOIDальные, линейные, круговые диаграммы и диаграммы Ганта; шкалы, диаграммы двумерного разброса, линейные таблицы, таблицы плотности растровых точек и другие); показывая различные варианты визуального представления данных.

*Многократно используемые объекты отчетов* – позволяют ускорить процесс проектирования отчетов благодаря сохранению их ключевых элементов, включая тексты, команды SQL, растровые изображения и функции пользователя (формулы) в централизованно управляемой библиотеке (поставляемой в составе Crystal Enterprise). Таким образом, достигается совместное повторное использование и централизованное обновление взаимосвязанных отчетов.

*Настраиваемые шаблоны.* Сокращается время форматирования отдельных отчетов. Можно разрабатывать и применять на-

страиваемые шаблоны в соответствии с собственными требованиями к форматированию и логике, включая операции доступа к данным, для гарантированной согласованности между создаваемыми отчетами. Можно также использовать существующие отчеты в качестве шаблонов.

*Мощный язык формул.* Можно использовать содержащийся в Crystal Reports богатый язык формул с более чем 160строенными и определяемыми пользователем функциями и операторами для исчерпывающего контроля над форматированием отчетов, сложной логикой обработки и отбора данных. Благодаря стеку вызовов упрощается отладка ошибок, возникающих на уровне данных. Также в программу включены экстрактор формул и среда работы с формулами (Formula Workshop).

*Настраиваемые функции.* Устраняется избыточность при создании формул. Бизнес-логику можно извлечь из формул, создав настраиваемые функции, которые затем использовать в различных отчетах.

*Несимметричное создание отчетов.* Обеспечивается возможность настраиваемого просмотра таблиц OLAP. Благодаря асимметричному созданию отчетов можно скрыть отдельные измерения данных так, чтобы конечный пользователь получал только наиболее важную и ценную для него информацию.

*Дополнительные модули для Access и Excel.* Используется интуитивно понятный мастер для упрощения добавления в отчеты информации из Microsoft Access или Excel.

УДК 378.001

© Г. М. Чернокнижный

Санкт-Петербургский государственный  
инженерно-экономический университет

© А. Г. Коробейников, Е. Г. Чернокнижная

Санкт-Петербургский государственный университет  
информационных технологий механики и оптики

## МАТЕМАТИЧЕСКАЯ ТЕОРИЯ КАТЕГОРИЙ ПРИ ПРОЕКТИРОВАНИИ САПР

Прогрессирующий интерес к использованию теории многосвязных систем в больших и сложных системах порождает постанов-

ку новых задач, решение которых необходимо для успешного преодоления разнообразных трудностей вычислительного характера.

Исходя из системного подхода, необходимо введение пространства состояний предметной области САПР как класса всех возможных конечных множеств ситуаций, в которых могут находиться объекты предметной области. После этого в нем (в пространстве) можно рассматривать последовательности состояний или траекторий, совокупность общих свойств которых и будем понимать под семантикой предметной области.

Воплощение в математическую теорию категорий диалектического принципа, согласно которому математические объекты рассматриваются в связях с другими (вместо того, чтобы определять свойства объекта через его элементы), позволяет применить категорный подход к представлению системы знаний в САПР. Индивидуальные объекты могут быть представителями разных сообществ-категорий, и это дает разные точки зрения на каждый данный объект. Таким образом, можно сказать, что представление знаний – категорный подход. Предполагается, что знание можно представить в виде набора областей, системы отображений и отношений, но с меньшими требованиями к полноте представляемой информации. В категорном подходе к представлению знаний предполагается, что представляемые знания проектируемого объекта структурированы в виде системных понятий, с которыми связывают определение и знания, вытекающие из определения.

Теория категорий предоставляет математические средства для отражения семантики и логики понятий [1; 2]. Для представления отдельного понятия строится алгебраический объект (категория), который потенциально отражает полное знание о предмете, вытекающее из определения этого понятия, а также конечная аппроксимация категории, в которой отражаются уже имеющиеся знания о представляемом понятии, реально отражаемые в системе представлений.

По определению математическая категория  $K$  состоит из двух непересекающихся классов – класса объектов  $\text{Ob}K$  и класса морфизмов  $\text{Mor}K$ . Морфизмы называют еще стрелками. Причем:

– для любой пары объектов  $\{(A, B) : A, B \in \text{Ob}K\}$  задано семейство отображений  $\text{Mor}K(A, B)$ , называемых семейством морфизмов из  $A$  в  $B$ . Вместо  $u \in \text{Mor}K(A, B)$  будем писать  $u: A \rightarrow B$ .

– для любой тройки объектов  $\{(A, B, C) : A, B, C \in \text{Ob}K\}$  задано отображение:

$\mu: \text{Mor}K(A, B) \times \text{Mor}K(B, C) \rightarrow \text{Mor}K(A, C)$  – (образ  $\mu(u, v)$ ) пары  $(u, v)$ , где семейство  $u \in \text{Mor}K(A, B)$ ,  $v \in \text{Mor}K(B, C)$  будем обозначать  $vu$  и называть композицией морфизмов.

Семейство морфизмов  $\text{Mor}K(A, B)$  и композиция морфизмов удовлетворяют следующим аксиомам:

α) композиция ассоциативна: для каждой тройки морфизмов  $u: A \rightarrow B$ ,  $v: B \rightarrow C$ ,  $w: C \rightarrow D$  справедливо равенство  $w(vu) = (wv)u$ ;

β) для любого объекта  $A \in \text{Ob}K$  существует морфизм  $1_A: A \rightarrow A$ , который будем называть тождественным морфизмом или единицей  $A$ .

γ) если пары  $(A, B)$ ,  $(A', B')$  различны, то  $\text{Mor}K(A, B) \cap \text{Mor}K(A', B') = \emptyset$ .

Например, пусть  $\Omega$  – некоторый набор символов операций, возможно многоарных. Тогда все  $\Omega$ -алгебры вместе с их гомоморфизмами составляют категорию.

Каждой категории  $K$  однозначно сопоставляется двойственная (дуальная) категория  $K^*$ , которая строится следующим образом.

1. Объекты категории  $K^*$  те же, что и у категории  $K$ , т. е.  $\text{Ob}K = \text{Ob}K^*$ .

2. Семейство морфизмов  $\text{Mor}K^*(A, B)$  по определению принимается  $\text{Mor}K(B, A)$ .

3. Композиция  $\text{Mor}K^*(A, B) \times \text{Mor}K^*(B, C) \rightarrow \text{Mor}K^*(A, C)$  определяется так:

если  $u \in \text{Mor}K^*(A, B)$  и  $v \in \text{Mor}K^*(B, C)$ , то  $vu = uv$

Категория  $K$  называется малой, если  $\text{Ob}K$  образуют множество. В силу аксиом α, β, γ это определение эквивалентно утверждению, что и морфизмы категории образуют множество. Для методов, предназначенных для реализации на ЭВМ, используются только малые категории. Всякую малую категорию  $K$  можно рассматривать как многоосновную алгебру с множеством сортов  $S = \text{Ob}K \times \text{Ob}K$  и множеством операций  $\Omega$ , состоящих из нульварных операций  $1_A$ ,  $A \in \text{Ob}K$  и бинарных операций умножения морфизмов:

$\varpi((A, B)(B, C), (A, C)) : \text{Mor}K(A, B) \times \text{Mor}K(B, C) \rightarrow \text{Mor}K(A, C)$ .

Произведение объектов в категории  $K$  определяется следующим образом: объект  $P$  называется произведением объектов  $A$  и  $B$  в категории  $K$ , если существуют такие морфизмы  $p_A: P \rightarrow A$  и  $p_B: P \rightarrow B$ , то для каждой пары морфизмов  $f: X \rightarrow A$ ,  $g: X \rightarrow B$  существует единственный морфизм  $h: X \rightarrow P$ , удовлетворяющий равенствам  $h p_A = f$ ,  $h p_B = g$ . Объект  $P$  обозначается  $A \times B$ , морфизмы  $p_A$  и  $p_B$  называются проекциями произведения. Морфизм  $h$  также обозначают кортежем  $\langle f, g \rangle$ , так как из определения произведения немедленно следует, что  $\text{Mor}K(X, P)$  изоморфно  $\text{Mor}K(X, A) \times \text{Mor}K(X, B)$  для любого объекта  $X \in \text{Ob}K$ .

По аналогии с определением произведения двух объектов можно определить произведение любого семейства объектов. В частности, если в категории  $K$  существуют произведения любых пар объектов, то в  $K$  существуют произведения произвольных  $n$  объектов,  $n \geq 1$ .

В дальнейшем для разработки автоматизированных методов проектирования понадобится понятие декартового произведения категорий. Оно определяется следующим образом.

Пусть  $\{K_i\}_{i \in I}$  – семейство категорий,  $I$  – множество индексов. Объекты категории  $\prod_{i \in I} K_i$  – всевозможные семейства объектов  $\{X_i\}$ , где  $X_i \in K_i$  – объект категории  $K_i$ ;

$$\text{Mor} \prod_{i \in I} K_i (X_i, Y_i) = \prod_{i \in I} \text{Mor} K_i (X_i, Y_i).$$

Если  $\{u_i\}_{i \in I} \in \text{Mor} \prod_{i \in I} K_i (X_i, Y_i)$  и  $\{v_i\}_{i \in I} \in \text{Mor} \prod_{i \in I} K_i (Y_i, Z_i)$ , то

$$\{v_i u_i\}_{i \in I} \in \text{Mor} \prod_{i \in I} K_i (X_i, Z_i).$$

Будем говорить, что категория  $K$  есть категория с конечными производствами, если всякое конечное семейство объектов из  $K$  обладает хотя бы одним произведением. Если же вообще всякое семейство объектов из  $K$  обладает хотя бы одним произведением, то будем говорить, что  $K$  есть категория с произведениями.

Для отображения одних категорий в другие в математической теории категорий используется понятие функторов. Определим одноместный и многоместные функторы.

Одноместным ковариантным функтором из категории  $K$  в категорию  $\lambda$  называется пара отображений  $\rho = (\text{Ob}K \rightarrow \text{Ob}\lambda, \text{Mor}K \rightarrow \text{Mor}\lambda)$  или  $\rho: K \rightarrow \lambda$ , удовлетворяющая следующим условиям:

$$1) \rho(1_A) = 1_{\rho(A)}$$
 для любого объекта  $A \in \text{Ob}K$ ;

$$2) \rho(fg) = \rho(f) \rho(g)$$
 для любых морфизмов  $f: A \rightarrow B$ ,  $g: B \rightarrow C$  категории  $K$ .

Функтор из категории  $K^*$  в категорию  $\lambda$  ( $\rho: K^* \rightarrow \lambda$ ) называется одноместным контравариантным функтором или просто контравариантным функтором из категории  $K^*$  в категорию  $\lambda$ . Для таких функторов условие 1 остается без изменений, а условие 2 заменяется на:

$$2') \rho(fg) = \rho(g) \rho(f)$$
 для любых морфизмов  $f: A \rightarrow B$ ,  $g: B \rightarrow C$  категории  $K$ .

Функторы, определенные на декартовых произведениях категорий, будем называть многоместными. Многоместные функторы могут быть ковариантными по одним аргументам и контравариантными по другим. Поэтому вариантность должна специально оговариваться.

При задании конечномерной аппроксимации множество образующих категорий  $K$  задается перечислением некоторых областей  $K_1, \dots, K_n$  и преобразований  $f_1, \dots, f_k$ , которые входят в определение определяемого категорией  $K$  понятия. Затем, базируясь на заданном в конкретной алгебре наборе операций и отношений, строятся выражения (термы) для задания области в категории  $K$ . Например,  $(K_1 + K_2) \times K_3$  и т. д. Аналогично определяется выражение (терм) для задания преобразования в категории  $K$ . Кроме того, на множестве термов, задающих области и преобразования в категории  $K$ , индуктивно строятся отношения эквивалентности:  $=_0$  – равенство термов областей и  $=_p$  – равенство термов преобразований. Это наименьшие рефлексивные, симметричные и транзитивные бинарные отношения, включающие некоторое конечное множество пар выражений, которые называются определяющими соотношениями категории  $K$ , а также пар выражений из равенств, входящих в определение категориальных операций.

Итак, для представления знаний в категорионном подходе используется алгебра с развитым набором операций теории категорий. Такая алгебра имеет достаточно изученную структуру топоса [3], а также структуру рефлексивной категории. Таким образом, имею-

щиеся средства при проектировании САПР позволяют отражать знания не только о внешних объектах, но и о самих средствах представления знаний.

### Литература

1. Коробейников А. Г. Применение математической теории категорий в разработке методов представления знаний // Тезисы докладов XXX научно-технической конференции профессорско-преподавательского состава СПб ГУИТМО «Автоматизация проектирования, технология элементов и узлов компьютерных систем», 25–28 января 1999. СПб., 1999. С. 91.
2. Category theory and computer science: 6<sup>th</sup> international conference; proceeding/ CTCS'95, Cambridge, United Kingdom, August 1995, David Pitt ... (ed). Berlin; Heideberg; New York: Springer, 1995. (Lecture notes in computer science, Vol. 953).
3. Джонстон П. Т. Теория топосов: Пер. с англ. / Под ред. Ю. И. Манина. М.: Наука, 1986.

УДК 378.001

© В. В. Пономарев

ЗАО «Транзас», Санкт-Петербург

© И. Г. Гниденко, В. В. Пономарев  
Санкт-Петербургский государственный  
инженерно-экономический университет

## РАЗРАБОТКА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ОЦЕНКИ ПОДГОТОВКИ ОБУЧАЕМОГО ПРИ ИСПОЛЬЗОВАНИИ КОМПЬЮТЕРНОГО ТРЕНАЖЕРА

Повсеместное распространение компьютерных тренажеров, предназначенных для обучения персонала по различным направлениям деятельности, остро ставит вопрос об эффективности такого обучения и качестве подготовки обучаемых. Данная статья посвящена вопросу организации недорогого и эффективного автоматизированного тренинга по технологии оценки, которая может быть использована для подготовки персонала при помощи навигационных компьютерных тренажеров. Предлагаемая система поможет удовлетворить требования различных программ подготовки.

Тренировочный процесс включает в себя использование автоматического тренажера Competence Assessment Systems (Надежные

системы оценки) – «CAS». Эти системы обладают целым рядом преимуществ по сравнению с традиционными методами:

- объективностью в оценке знаний;
- высокой эффективностью оценки;
- широкими возможностями ведения учета и статистики по ходу обучения;
- предельной ясностью в постановке задачи;
- возможностями применения дистанционного (Интернет) обучения.

И сами CAS, и библиотеки контрольных заданий к ним сейчас изобилуют на рынке программных продуктов. Однако эти продукты, как правило, предоставляют главным образом теоретические знания и располагают лишь некоторыми практическими функциями, что создает определенные трудности в адаптации к характерным чертам конкретного тренировочного курса.

Отличительной чертой оценивания правильности действий обучаемого на тренажере является то, что предмет оценивания во многом зависит от условий проведения тренинга, таких как время и пространство. Поэтому формальные результаты оценивания формируются под влиянием таких внешних факторов, как место проведения, время суток, взаимное расположение частей тренажера, равно как и целей тренинга и уровня квалификации обучения. Разумеется, вышеупомянутая зависимость слишком сложна (если не неопределенна), и это создает определенные трудности в нахождении решения для конкретного пользователя. Кроме того, в зависимости от конкретного направления обучения, количество оценочных критериев может существенно меняться.

Возможны следующие сферы применения CAS в навигационных тренажерах:

- комплектация курса упражнениями в помощь обучаемому;
- объективная оценка выполнения упражнений;
- отслеживание динамики изменений профессиональной квалификации пользователя;
- учет эффективности процедуры обучения;
- дистанционная и Интернет-сертификация;
- дистанционное обучение.

Рассматриваемая система включает в себя три основных компонента:

- редактор правил работы с тренажером;
- модуль оценки упражнений (шкала градации);
- отчет о результатах тренинга.

*Редактор правил* – это приложение к редактору упражнений, который позволяет центру обучения (инструктору) совершенствовать или редактировать упражнение при помощи изменения правил оценивания. Редактор предназначен для создания, корректировки и хранения «Автоматизированного сценария контроля знаний обучаемых», т. е. ряда правил для оценки упражнений, выполненных на навигационном тренажере. «Автоматизированный сценарий контроля знаний обучаемых» разрабатывается вместе со сценарием упражнений и хранится в файле упражнений. При разработке условий выполнения упражнения инструктор задает правило оценивания, принимая во внимание конкретные особенности данного компьютерного тренажера.

Разработанное инструктором правило оценивания включает в себя:

- текстовое описание правила;
- рекомендации для обучаемого;
- параметры оценивания прохождения маршрута;
- развернутое пояснение правила оценивания;
- количество нарушений установленного правила;
- стоимость допущенных ошибок.

Инструктор формулирует развернутое логическое объяснение условий нарушения правила. Логические выражения, обозначающие эти условия, включают в себя параметры прохождения маршрута и заданные инструктором константы. В операциях, осуществляемых для вычисления значений выражений, используются стандартные логические операторы («и», «или», «равно», «не равно», «больше или равно» и т. д.).

Второй и третий компоненты включаются в любую систему обучения независимо от ее конфигурации и активизируются вместе с упражнением, снабженным правилами оценивания.

Оценивание строится на проверке правильности выполнения упражнения в соответствии с рядом выбранных критериев. Эта проверка по критериям состоит в сопоставлении «оценочных парамет-

ров» упражнения со значениями, ранее установленными инструктором. В продолжение проверки любая найденная ошибка (расхождение параметров) регистрируется, и штрафные очки считаются как функция от величины расхождения и от стоимости вопроса

$$\text{Очк} = f(\text{ош}, \text{стоим}).$$

Полная сумма штрафных очков в диапазоне заданий начисляется как сумма штрафных очков в любой момент времени за каждый «оценочный параметр»

$$\text{Сум} = \sum_{i=1}^n \sum_{j=0}^{l_i} \text{очк}.$$

Проверка по критериям может быть промежуточной (производится до завершения цикла упражнений на данную тему) или итоговой (производится по завершении выполнения цикла). Во время выполнения заданий информация об ошибках и рекомендации инструктора могут высвечиваться на дисплее пользователя и (или) вверху центрального экрана, если он содержит соответствующий параметр в конфигурации тренажера. Подведение итогов по выполненному заданию происходит при помощи автоматического сравнения суммарного штрафного балла с «проходным баллом», заранее установленным инструктором для данного сценария подготовки.

*Модуль оценивания выполнения упражнений* создан для отслеживания выполнения заданий автоматизированного сценария оценивания в рамках занятий на тренажерах. Результаты проверки высвечиваются на *Шкале градации*, размещенной на экране инструктора, которую при желании может увидеть обучаемый. Полученные параметры оценивания по данному критерию автоматически сверяются с заранее установленными значениями, и суммарный балл вычисляется как 100% минус сумма штрафных очков

$$\text{Оценка} = 100\% - \text{Штраф}.$$

Правильность выполнения упражнения также может быть проверена путем просмотра компьютерного журнала упражнения. Отчеты о прохождении курса подготовки хранятся в MS Excel-совместимом формате, что позволяет применять множество подходов к подведению различной статистики.

Темпы роста квалификации обучаемого обычно оцениваются посредством сравнения результатов выполнения им одного и того же упражнения в различные периоды подготовки. При сравнении используется стандартная оценочная процедура, но лишь с тем исключением, что, вместо установленных инструктором значений, используются параметры оценивания самого обучаемого за предыдущие тестирования.

Иногда при оценивании уровня подготовки обучаемого используется принцип сравнения результатов обучаемого с «идеальными» (результаты, полученные самим инструктором).

Рассмотренная система позволяет центру подготовки развивать и распространять программы обучения и сценарии автоматической оценки для использования различными организациями, нуждающимися в компьютерных тренажерах или для интерактивного обучения.

Гибкость системы поиска подходящего сценария, большое количество критериев оценки и возможность использования задаваемых пользователем переменных алгебры-логики в задании правил оценивания позволяет использовать систему для разработки самых различных сценариев работы компьютерных тренажеров.

УДК 378.001

© И. В. Поночевная

Санкт-Петербургский государственный  
инженерно-экономический университет

## ИСПОЛЬЗОВАНИЕ УНИФИЦИРОВАННОГО ЯЗЫКА МОДЕЛИРОВАНИЯ В СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ

В последнее время наблюдается большой интерес ко всем аспектам, связанным с моделированием систем. На сегодняшний день моделирование широко используется в информационных технологиях управления проектированием систем, сложность, масштабы и функциональность которых постоянно возрастают.

Наибольшее распространение для этих целей получил унифицированный язык моделирования Unified Modeling Language (UML).

Этот язык позволяет одновременно с анализом создавать документацию для проектирования систем, чтобы воплощать ее в рабочоспособный код на любом из языков объектно-ориентированного

программирования, таких как C++, VB, JAVA, CORBA, ORACLE, POWER builder, Forte, Smalltalk, а также осуществлять генерацию базы данных на большинстве существующих SQL-серверов.

Унифицированный язык моделирования включает в себя определенную систему условных обозначений – «нотацию», предназначенных для выражения идей и решений, выполненных на этапе объектно-ориентированного анализа и проектирования.

Модели системы позволяют наладить плодотворное взаимодействие между заказчиком, пользователем и командой разработчиков. Модели обеспечивают ясность представления выбранных решений, которые позволяют понять разрабатываемую систему во всей ее полноте.

Сложность разрабатываемых систем на сегодняшний день продолжает увеличиваться, и поэтому возрастает актуальность использования таких методов моделирования. Этот язык включает:

- элементы модели – фундаментальные концепции моделирования и их семантику;
- нотацию – визуальное представление элементов моделирования;
- принципы использования – правила применения элементов в рамках построения тех или иных типов моделей.

Унифицированный язык моделирования предоставляет выразительные средства для проектирования моделей.

При построении визуальных моделей можно решить сразу несколько типичных проблем, так как эта технология моделирования позволяет работать со сложными системами и проектами. Моделирование системы существенно облегчает достижение такой цели, как повышение качества моделируемого продукта.

При моделировании на UML используются восемь видов диаграмм, каждая из которых может содержать элементы определенного типа. Типы допустимых элементов и отношений между ними зависят от вида диаграммы.

Каждая диаграмма позволяет рассматривать систему под различным углом. Например, пользователи при помощи данных диаграмм могут оценить основные положения и разобраться в том, кто за что отвечает.

*Диаграммы вариантов использования.* Эти диаграммы описывают функциональность системы, которая будет видна пользователям. Каждая функциональность изображается в виде «прецедентов

использования» (use case). Прецедент – это типичное взаимодействие пользователя с системой, которое при этом:

- описывает видимую пользователем функцию;
- может представлять различные уровни детализации;
- обеспечивает достижение конкретной цели, важной для пользователя.

Прецедент рисуется как овал, связанный с типичными пользователями, называемыми актерами (actors). Актеры используют систему (или используются системой) в данном precedente. Актер, представляющий человека-пользователя, характеризуется ролью в данном precedente. На диаграмме изображается только один актер, однако реальных пользователей, выступающих в данной роли по отношению к системе, может быть много.

Список всех precedenteов фактически определяет функциональные требования, с помощью которых может быть сформулировано техническое задание. Эта диаграмма является графическим представлением взаимодействия пользователя и компьютерной системы, в нашем случае – компьютерной модели.

**Диаграммы классов** (class diagrams). Эти диаграммы описывают статическую структуру классов. Также они могут описывать «словарь предметной области» на концептуальном уровне.

На детальном уровне (уровне спецификаций и уровне реализаций) диаграммы определяют структуру программных классов. Они используются для генерации каркасного программного кода на данном языке программирования, поддерживающем UML.

**Диаграммы поведения** (behavior diagrams). Используются для описания динамики – поведения объектов в системе, которые подразделяются на:

- диаграммы состояний (statechart diagrams);
- диаграммы активностей (activity diagrams);
- диаграммы взаимодействия (interaction diagrams), состоящие из:
  - диаграмм последовательности (sequence diagrams);
  - диаграмм взаимодействий (collaboration diagrams).

Широкий набор средств и методов позволяет выделить те стороны поведения объектов, которые наилучшим образом отражают их свойства. Последовательность и взаимные связи диаграмм отражают интерактивные процессы, так как мы видим не только объекты и классы, но и сообщения, которыми они обмениваются.

Таким образом, с помощью системы можно моделировать ситуации, применяя обычную в таких случаях технологию «что, если».

Диаграммы состояния используются для описания динамических объектов, часто отправляющих и принимающих сообщения.

С помощью разработанной модели поведения устанавливаются зависимости между классами, производится разделение системы на модули и выделение классов, реализуемых в данных модулях, чтобы можно было эффективно организовать разработку системы.

Наконец, диаграммы реализации (implementation diagrams) состоят из компонентных диаграмм (component diagrams) и диаграмм развертывания (deployment diagrams).

Диаграммы компонентов и развертывания предназначены для физического представления системы (в том числе исполняемых модулей, библиотек, интерфейсов).

Из всего сказанного можно сделать следующий вывод: особенность языка моделирования состоит в том, что он оптимизирован для применения при разработке системы, это позволяет максимально ускорить разработку и заметно улучшить качество системы.

Такие модели, разработанные в UML, значительно упрощают процесс кодирования и направляют усилия программистов непосредственно на реализацию системы. Данный язык упрощает процесс проектирования, снижает его стоимость и повышает эффективность.

Унифицированный язык моделирования имеет большие перспективы работы в научных разработках.

УДК 378.001

© Е. В. Стельмашонок

Санкт-Петербургский государственный  
инженерно-экономический университет

## ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА КАК ОСНОВА ПОДДЕРЖКИ И ЗАЩИТЫ КОРПОРАТИВНЫХ БИЗНЕС-ПРОЦЕССОВ

Эффективная деятельность промышленной корпорации в современных условиях невозможна без создания единой бизнес-системы на основе бизнес-процессов, без разработки концепции форм

мирования широкого спектра управленческих решений по управлению бизнес-объектами и бизнес-процессами посредством бизнес-функций, объединяющих все виды ресурсов: материальные, финансовые, человеческие, интеллектуальную собственность, инфраструктурные активы.

Успешное функционирование бизнес-системы промышленной корпорации весьма затруднительно без такой компоненты, как информационная инфраструктура, основной задачей которой является защита информационных активов и поддержание в рабочем состоянии нематериальных активов корпорации.

Многими авторами [1; 4; 7] признается, что инфраструктура является обязательным компонентом любой целостной экономической системы, что инфраструктура в обычном ее понимании не создает самостоятельного продукта в материально-вещественной форме, она лишь обеспечивает определенные условия для его производства, что не совсем верно для информационных ресурсов предприятий.

Согласно предлагаемой новой методологии, выделяется информационная инфраструктура, обеспечивающая информационными ресурсами все уровни управления корпорацией (рисунок).



Понятие информационной инфраструктуры в трактовке различных специалистов отличается.

Наиболее подходящим можно считать определение, данное в [5]: под корпоративной информационной инфраструктурой понимается совокупность программно-технических средств и организационно-административных мероприятий, обеспечивающих в совокупности безопасную обработку данных и информационное обеспечение бизнес-процессов внутри корпорации, а также адекватные возможности по обмену информацией с внешними организациями, – которое необходимо дополнить следующим: так как на сегодняшний день информационная инфраструктура обладает большим и разнообразным набором компонент, имеющих различные формы как материальные, так и нематериальные: оборудование, аппаратное и программное обеспечение, средства связи, запоминающие устройства, информационный контент, Web-сайты, электронную почту сотрудников корпорации, клиентские базы данных и др., то в состав информационной инфраструктуры корпорации входят информационные системы и сети, научно-техническое обеспечение, технические библиотеки (таблица).

**Рекомендуемая информационная инфраструктура  
промышленной корпорации**

Компоненты	Необходимые элементы
1. Материальные Оборудование и аппаратное обеспечение	Кабельная система Сетевое оборудование Серверное аппаратное обеспечение Дополнительное оборудование (принтеры, факсы, устройства авторизации) Клиентские рабочие места
2. Нематериальные 2.1. Программное обеспечение	Системное программное обеспечение (операционные системы, средства защиты информации, драйверы устройств) Стандартное прикладное обеспечение (средства обработки электронных таблиц, работы с текстами, электронной почтой, файлами) Сетевые службы (серверы DNS, DHCP, пакетной защиты, авторизация, доступа в Интернет, серверы приложений – СУБД и т. д., почтовые сервисы) Прикладное программное обеспечение (сопровождение корпоративных информационных систем)

## Окончание

Компоненты	Необходимые элементы
2.2. Типовые инструменты и методики	Инструкции по настройке серверного и клиентского программного места Регламент проведения работ
2.3. Службы технического сопровождения	Центр диспетчеризации и контроля качества Библиотеки
2.4. Информационный контент	Содержимое Web-сайтов корпорации Любая информация о корпорации, в том числе рекламного характера на любых носителях

Согласно новой методологии информационная инфраструктура следует двум положениям (гипотезам в новой теории).

1. На этапе создания и практического формирования информационного продукта (услуг) информационная инфраструктура предоставляет все необходимое для построения эффективной бизнес-системы и реализации целей и задач всей бизнес-системы корпорации, что позволяет контролировать этот процесс, управлять им и реализовывать в намеченные сроки, обеспечивая ее безопасность.

2. Правильно спроектированная информационная инфраструктура должна обеспечить надежное функционирование и взаимодействие всех входящих в бизнес-систему бизнес-процессов и бизнес-объектов посредством бизнес-функций таким образом, чтобы представить полный комплекс ресурсов, механизмов и инструментов управления корпорацией в виде самонастраивающейся системы как информационного сопровождения, модификаций и развития всех ее бизнес-процессов на протяжении всего жизненного цикла корпораций, который может составить не один десяток лет.

Необходимость комплектования такой инфраструктурой современных промышленных корпораций обусловлена жесткими требованиями рыночной конкуренции, заставляющими промышленные корпорации оценивать и внедрять новые подходы к оценке информационных активов промышленной корпорации как объектов нематериальных активов.

Под поддержкой и защитой всей бизнес-системы промышленной корпорации будем понимать прежде всего поддержку и защиту всех бизнес-процессов за счет инфраструктурной составляющей бизнес-системы. В частности, за счет информационной составляю-

щей возможно преодоление инфраструктурной и информационной разобщенности подразделений промышленной корпорации. Инвестиции в развитие инфраструктуры корпоративных бизнес-процессов являются скорее венчурными, так как могут приносить свердоходы за счет повышения эффективности работы и ускорения бизнес-процессов, а также за счет повышения рыночной стоимости компании относительно нематериальной части ее активов (НМА): информационных в инфраструктурной составляющей нематериальных активов [2], [3].

Так как оценка таких бизнес-процессов как особых активов корпорации имеет свою специфику [4], [6], традиционные показатели эффективности здесь неприменимы. Например, информационные системы класса Enterprise Content Management управления корпоративными бизнес-процессами могут помочь промышленным корпорациям в разработке единой информационной среды как единого информационного контента корпорации, которая объединила бы все ресурсы корпорации и все бизнес-процессы в единую бизнес-систему.

Несомненно, стоит выделить следующие принципы разработки информационной инфраструктуры:

- интегрированность;
- управление неисправностями;
- масштабируемость;
- поддержание инфраструктуры в рабочем состоянии;
- необходимость использования интеллектуальных систем управления, так как на сегодняшний день эти системы могут отвечать поставленной задаче.

Так как в сегодняшних условиях выбор той или иной стратегии разработки информационной инфраструктуры промышленной корпорации является одним из необходимых условий успешного развития и процветания бизнеса, то возможная реструктуризация инфраструктуры промышленной корпорации в России может быть обусловлена:

- изменением качественного содержания инфраструктурных бизнес-процессов за счет отслеживания (мониторинга) факторов морального старения аппаратной и программной части информационных активов;
- переходом от традиционных принципов управления к управлению бизнес-процессами в единой бизнес-системе промышленной корпорации;

- переоценкой и реструктуризацией активов промышленной корпорации в случаях купли-продажи всех (или части) ее активов;
- увеличением активов корпорации за счет возможного создания, выявления НМА, либо приобретения за плату.

### Литература

- Балукова В. А. Методология корпоративного подхода к реструктуризации промышленных предприятий в условиях российской экономики. СПб.: СПбГИЭУ, 2002.*
- Еникеева Л. А., Стельмашонок Е. В. Методологические подходы к оценке информационных активов как инфраструктурной составляющей нематериальных активов // Актуальные проблемы экономики и новые технологии преподавания (Смирновские чтения): Материалы IV Международной научно-практической конференции, 15–16 марта 2005 г. Т. 2. СПб., 2005. С. 181–183.*
- Еникеева Л. А., Стельмашонок Е. В. Инфраструктурная составляющая нематериальных активов как объект оценки и защиты // Экономика и промышленная политика России: Труды III Международной научно-практической конференции, 14–19 июня 2004 г. СПб., 2004. С. 525–528.*
- Ойхман Е. Г., Попов Э. В. Рейнжиниринг бизнеса: реинжиниринг организационной и информационной технологии. М.: Финансы и статистика, 1997.*
- Орлов С. Фундамент информационной инфраструктуры // LAN. 2003. № 1.*
- Тельнов Ю. Ф. Рейнжиниринг бизнес-процессов. М.: МЭСИ, 1999.*
- Федько В. П., Федько Н. Г. Инфраструктура товарного рынка. Ростов н/Д: Феникс, 2000.*

УДК 378.001

© Д. А. Говорунов

Санкт-Петербургский государственный  
инженерно-экономический университет

### ПРОГНОЗИРОВАНИЕ СПРОСА НА МЕДИЦИНСКИЕ УСЛУГИ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ МЕТОДА SSA (SINGULAR SPECTRUM ANALYSIS)

Серьезные преобразования в отрасли здравоохранения, начавшиеся в нашей стране в конце 1980-х гг., привели к серьезным изменениям в деятельности медицинских учреждений. Изменения за-

тронули, в частности, экономический статус медицинского учреждения, который сблизился со статусом предприятий, действующих в условиях рынка.

До упомянутых преобразований проводимый в этой области экономический анализ был ориентирован в основном на задачи административного контроля в условиях затратных методов управления государственными медицинскими учреждениями.

С появлением платных услуг и услуг добровольного медицинского страхования (ДМС) приобрели значение новые задачи экономического анализа деятельности медицинского учреждения, среди которых можно отметить:

- вопросы ценообразования на платные услуги и услуги ДМС;
- планирование и оптимизация расходов ресурсов;
- вопросы, связанные с организацией профилактических мероприятий и исследованием рынка медицинских услуг.

Для всех вышеперечисленных задач крайне важной является информация о предстоящем уровне спроса на предоставляемые медицинские услуги.

К особенностям временных рядов спроса на медицинские услуги относятся:

- сложная структура временного ряда (сложный тренд, периодические колебания, наличие структурных сдвигов);
- короткий временной период (следствие реформирования системы финансирования отрасли здравоохранения);
- изменчивый характер временных рядов спроса для различных услуг, что исключает возможность использования какой-либо параметрической модели.

Метод анализа временных рядов SSA (Singular Spectrum Analysis – сингулярный спектральный анализ), называемый также метод «гусеница», был предложен в 60–70-е гг. сразу в ряде научных центров (в нашей стране – в частности, в Санкт-Петербургском государственном университете) [1], [3], [5].

Метод SSA в последние годы достаточно широко применяется в климатологии, геофизике, гидрологии, астрономии, физике, химии. Использованию данного метода посвящено много литературы [1], [2], [4]. Следует, однако, отметить, что в сфере экономики (и особенно при исследовании экономических аспектов здравоохранения) данному методу уделяется значительно меньше внимания.

В то же время метод SSA может быть весьма эффективен при изучении экономических (медицинско-экономических) рядов с их сложной структурой и большим количеством определяющих факторов.

Метод SSA обладает большим количеством достоинств по сравнению с другими методами применительно к описываемой задаче:

- является непараметрическим методом, что позволяет находить и исследовать заранее неизвестные закономерности (периодики), при этом не возникает необходимости в поиске факторов, влияющих на развитие изучаемого процесса (соответственно, и нет риска неправильного их определения), что является большим преимуществом при изучении сложных и изменчивых систем;

- позволяет находить и анализировать периодики с изменяющейся амплитудой, что очень важно при исследовании экономических рядов в здравоохранении, так как амплитуды сезонных колебаний спроса на платные медицинские услуги зависят от его объема, т. е. от состояния рынка;

- позволяет получать интерпретируемые результаты на коротких временных рядах, что актуально при изучении платных медицинских услуг в государственных медицинских учреждениях: длина приемлемого для статистического анализа временного ряда составляет от 1 до 3-х лет (на данный момент);

- позволяет фильтровать временной ряд (выделять сигнал и шум); так, если имеется необходимость в анализе составляющих ряда (тRENда или периодических колебаний), можно воспользоваться уникальной особенностью метода SSA отфильтровывать ненужные компоненты, а затем интерпретировать или анализировать полученный результат любыми другими статистическими методами.

Существует несколько модификаций метода SSA:

- MSSA – Multidimensional Singular Spectrum Analysis, модификация для построения моделей с использованием нескольких временных рядов и учетом взаимной корреляции;

- CSSA – Complex Singular Spectrum Analysis, модификация для исследования двух временных рядов, где в сингулярном разложении участвуют комплексные числа, которые получаются на основе исследуемых рядов.

Эти модификации открывают широкие возможности для анализа медико-экономических рядов.

Метод SSA можно кратко описать следующим образом: временной ряд представляется в виде последовательности векторов, состоящих из отрезков временного ряда выбранной длины (получается многомерная выборка, называемая траекторной матрицей). Далее, используя анализ главных компонент, получают сингулярное разложение траекторной матрицы. На основе этого разложения можно судить о структуре временного ряда, а также получать различные его реконструкции (модели). Базовый алгоритм метода SSA состоит из четырех этапов. Пусть имеется временной ряд длины  $N$ :  $F = (f_0, \dots, f_{N-1})$ ,  $N > 2$ .

*Этап 1. Разворотка одномерного ряда в многомерный (вложение).* Выбирается целый параметр – длина окна  $L$ ,  $1 < L < N$ . Строится траекторная матрица (рис. 1).

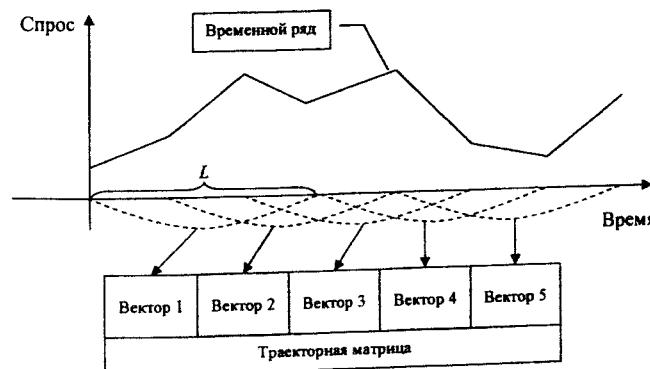


Рис. 1. Порядок построения траекторной матрицы

Столбцами траекторной матрицы являются вектора (скользящие отрезки ряда длины  $L$ ):  $X_i = (f_{i-1}, \dots, f_{i+L-2})^T$ ,  $1 \leq i \leq K$ . Количество векторов равно  $K = N - L + 1$ .

*Этап 2. Сингулярное разложение.* На данном этапе производится процедура сингулярного разложения (SVD – Singular Value Decomposition) полученной траекторной матрицы. Траекторная матрица представляется в следующем виде:

$$X = X_1 + \dots + X_d,$$

где  $X_i = \sqrt{\lambda_i} U_i V_i^T$ ,  $i = 1, \dots, d$ ;  $d = \max \{i : \lambda_i > 0\}$ ;

$\lambda_1, \dots, \lambda_L$  – собственные числа матрицы  $S = XX^T$ ;

$U_1, \dots, U_L$  – ортонормированная система собственных векторов матрицы  $S$ , соответствующая собственным числам;

$V_i = X^T U_i / \sqrt{\lambda_i}$  – главные компоненты; набор  $\sqrt{\lambda_i}, U_i, V_i$  называется  $i$ -й собственной тройкой сингулярного разложения.

**Этап 3. Восстановление (группировка).** На этом этапе отбираются собственные тройки для этапа восстановления. Как правило, эта операция требует участия специалиста. Существуют различные алгоритмы для автоматического определения собственных троек, однако они могут применяться только тогда, когда известна информация о постоянных компонентах изучаемых временных рядов и цели исследования достаточно узко конкретизированы. Таким образом, временной ряд представляется в виде:  $X = X_{I_1} + \dots + X_{I_m}$ , где  $I_1, \dots, I_m$  – группы собственных троек.

**Этап 4. Восстановление (диагональное усреднение).** На последнем этапе каждая матрица сгруппированного разложения  $Y[L \cdot K]$  (с элементами  $y_{ij}$ ) переводится в ряд  $g_0, \dots, g_{N-1}$  по формуле

$$g_k = \begin{cases} \frac{1}{k+1} \sum_{m=1}^{k+1} y_{m,k-m+2}^* & \text{для } 0 \leq k < L^* - 1, \\ \frac{1}{L^*} \sum_{m=1}^{L^*} y_{m,k-m+2}^* & \text{для } L^* - 1 \leq k < K^*, \\ \frac{1}{N-k} \sum_{m=k-K^*+2}^{N-K^*+1} y_{m,k-m+2}^* & \text{для } K^* \leq k < N, \end{cases}$$

где  $1 \leq i \leq L$ ,  $1 \leq j \leq K$ ,  $L^* = \min(L, K)$ ,  $K^* = \max(L, K)$ .

В результате получаем исходный ряд, разложенный в сумму  $m$  рядов:  $f_n = \sum_{k=1}^m \tilde{f}_n^{(k)}$ .

Подробное теоретическое обоснование метода дано в работах [1]–[3].

**Алгоритм SSA-прогнозирования.** Существуют две разновидности прогноза: рекуррентный и векторный. Для наших целей вполне достаточно будет использовать базовый метод – рекуррентное прогнозирование. Опишем алгоритм рекуррентного SSA-прогнозирования.

Задача состоит в определении членов ряда

$$G_{N+M} = (g_0, \dots, g_{N+M-1})$$

по формуле:

$$g_i = \begin{cases} \tilde{f}_i & \text{для } i = 0, \dots, N-1, \\ \sum_{j=1}^{L-1} a_j g_{i-j} & \text{для } i = N, \dots, N+M-1, \end{cases}$$

где  $M$  – число точек прогноза,

$$R = (a_{L-1}, \dots, a_1)^T,$$

$$R = \frac{1}{1-\nu^2} \sum_{i=1}^r \pi_i U_i^\nabla,$$

$$\nu^2 = \pi_1^2 + \dots + \pi_r^2,$$

где  $\pi_i$  – последняя компонента вектора  $U_i$  ( $i = 1, \dots, r$ );

$U^\nabla$  – вектор, состоящий из первых  $L-1$  компонент вектора  $U^\nabla$  ( $U^\nabla \in R^{L-1}$ ).

**Анализ временного ряда методом SSA.** Рассмотрим применение метода SSA на примере реальных данных об оказании платных медицинских услуг, любезно предоставленных администрацией одной из крупных больниц города Санкт-Петербурга.

На рис. 2 изображен исходный временной ряд, отражающий спрос на платную медицинскую услугу за период с 01.01.01 по 01.01.04, временное разрешение ряда составляет один месяц. Для удобства отображения месяцы последовательно пронумерованы.

Анализ временного ряда рассматриваемой услуги показал наличие сезонных периодик, а также позволил выделить тренд.

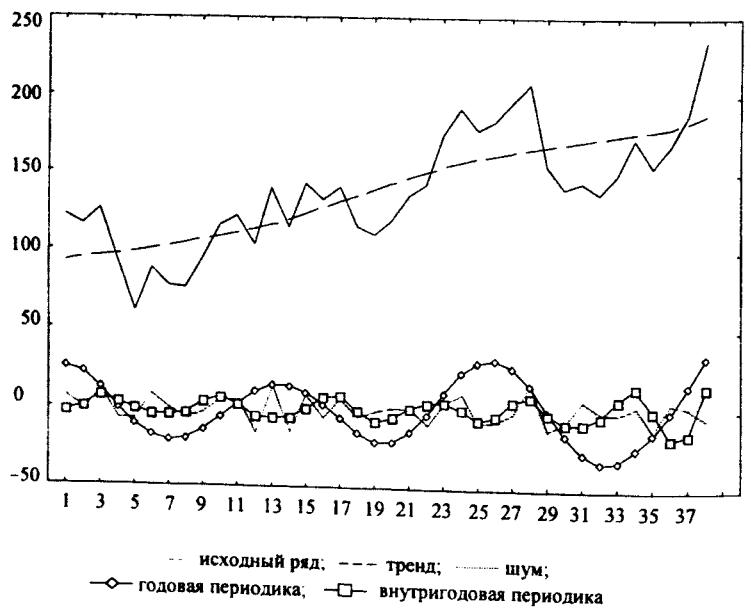


Рис. 2. Исходный ряд и компоненты, полученные с помощью метода SSA

На основе выделенных периодик (годовая и внутригодовая периодики) и тренда строим SSA-модель ряда (рис. 3).

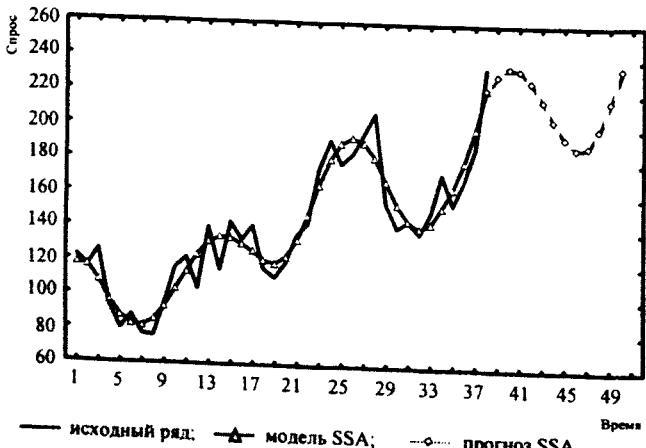


Рис. 3. Исходный ряд, SSA-модель ряда и SSA-прогноз

С помощью алгоритма SSA прогнозирования строим прогноз на год (12 месяцев) вперед (рис. 3).

Оценим эффективность прогноза (рис. 4):

- удалим небольшую часть исходного ряда;
- построим прогноз укороченного исходного ряда;
- сравним реальные и прогнозируемые значения.



Рис. 4. Оценка эффективности прогноза

Среднее абсолютное расхождение реальных данных и прогноза составляет 27 обращений. Среднеквадратическая ошибка прогноза – 33,29.

Таким образом, получен достаточно правдоподобный прогноз исследуемого процесса, при использовании короткого временного ряда. В процессе прогнозирования не был проведен анализ каких-либо факторов, которые могли оказывать влияние на исследуемый процесс. Метод SSA может успешно применяться для прогнозирования спроса на медицинские услуги.

#### Литература

1. Главные компоненты временных рядов: метод «Гусеница» / Под ред. Д. Л. Данилова, А. А. Жиглянского. СПб.: Пресском, 1997.

2. Golyandina N., Nekrutkin V., Zhitljavsky A. Analysis of Time Series Structure: SSA and Related Techniques. London: Chapman & Hall/CRC, 2001.
3. Голяндина Н. Э. Метод «Гусеница»-SSA: анализ временных рядов: Учеб. пособие. СПб.: СПбГУ, 2004.
4. Pascal Yiou, Didier Sornette, Michael Ghil. Data-Adaptive Wavelets and Multi-Scale SSA, Institute of Geophysics and Planetary Physics University of California Los Angeles at Los Angeles.
5. Golyandina N., Nekrutkin V., Solntsev V. «Caterpillar» – SSA Technique for Analysis of Time Series in Economics, Saint-Petersburg State University, Mathematical Department: <http://vega.math.spbu.ru>

УДК 338.24

© А. И. Дащевский, А. С. Обухов

Санкт-Петербургский государственный  
инженерно-экономический университет

## СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В ЭКОНОМИЧЕСКИХ ЗАДАЧАХ

В настоящее время все большую актуальность приобретает разработка систем поддержки принятия решений, все больше и больше специалистов имеют непосредственное отношение к их изучению и развитию, создаются новые информационные продукты данного назначения.

Среди особенностей информационной технологии систем поддержки принятия решений в отличие от традиционных технологий выделяются следующие, которые надо учитывать при создании таких систем.

Информация, необходимая для принятия решений, – это не просто факты, которые надо выдавать человеку, принимающему решения, а факты, интерпретированные по цели деятельности этого человека, т. е. один и тот же факт, разный для людей, имеющих разную целевую деятельность, интерпретируется по-разному. Поэтому в рассматриваемой системе все факты должны интерпретироваться по сферам деятельности. Этот момент учитывается, начиная с предпроектной стадии создания системы, где в дополнение к обычным работам необходимо предусмотреть создание соответствующих классификаторов. На следующих стадиях, при разработке баз данных и знаний, все хранимые факты связываются в цепочки по сферам дея-

тельности и обслуживают операции по принятию решений. Самы же базы в экономических системах строятся преимущественно по фреймовому принципу.

При создании такого рода систем должен быть учтен ряд принципов, которые сами по себе могут быть противоречивыми:

- принципы IBM. Машина должна работать, а человек думать (машина думать не может, а думать и принимать решения может только человек), т. е. система данного рода относится к классу информационно-советующих;

- принцип полноты информационного пространства. Совокупность правил, поддерживающих выработку решения, должна быть доведена до прагматического завершения (пусть даже частичного по сравнению с конечной целью). Отсутствие некоторой необходимой части правила может привести к тому, что сама цепочка потеряет прагматическую ценность;

- принцип децентрализации информационного источника. В экономических системах поддержки решения по экономическим задачам он особенно важен, так как практически всегда объективное решение должно базироваться на информации, поступающей из различных источников;

- принцип интеграции информационного пространства. В нашем случае разрабатываемая задача по поддержке принятия решений фактически всегда встраивается во включающую систему (оболочку) и становится ее элементом;

- принцип Шоу. Применительно к экономическим системам это означает, что пользователь может обладать минимальной технологической квалификацией, хотя тематическая (предметная квалификация) у него должна быть высока. Система должна быть такой, чтобы с ней мог работать пользователь любого уровня, и тогда любой (даже абсолютно неопытный) пользователь захочет ею пользоваться;

- принцип иерархической «бюрократичности». Каскадное уменьшение потока информации, который должен доставляться человеку для принятия решения;

- принцип объектно-ориентированного моделирования при построении картины предметной области;

- принцип динамической структуры. Система должна предполагать учет внешних факторов. Применительно к экономической

области такие факторы могут постоянно изменяться, пополняться новыми. Соответственно, экономико-математические модели, применяемые в таких системах, должны включать динамические элементы;

– принцип компонентной сборки прикладных режимов.

Эти принципы должны в такого рода системе работать совместно. Поскольку они могут быть противоречивы, надо вспомнить старый закон сложных систем. Любая сложная система способна работать оптимально и тогда, когда не оптимально работает каждый из ее элементов. Этот принцип, к сожалению, очень часто забывается. Надо искать компромисс между каждым из этих принципов. С тем, чтобы он работал более или менее нормально, с одной стороны, а с другой стороны, не мешал работе других.

При удачном совмещении всех этих принципов в рамках одной системы специалистами уже создавались соответствующие технологии обработки информации, программы и лингвистические продукты, которые поддерживают эти технологии. Каждая система поддержки решения – это уникальный продукт, который ориентирован на конкретную целевую деятельность. Опыт разработчиков показывает, что два предприятия, одинаковые по направленности своей деятельности, требуют разные системы поддержки для каждого из них. Собственно говоря, цели у каждого предприятия свои, и под эти цели должна создаваться определенная система. Это означает, что создание типовых систем поддержки решения довольно проблематично.

Многие системы поддержки принятия решений разрабатываются так, что человек, который работает с этой системой, не обязан знать об ЭВМ вообще ничего, он должен просто нажимать на кнопки, главное – это умение работать с информацией, т. е. ему предстоит пользоваться очень хорошей графической подсказкой о ситуациях, которые складываются в точках, на которые ему надо обратить внимание в процессе своей работы. Тогда он может достать соответствующую информацию, относящуюся к этой ситуации. И уже принимать соответствующее решение, как реагировать на сложившуюся ситуацию. Далее, если пользователь получает позитивное развитие ситуации, – это значит, что ему не надо вмешиваться. Если негативную ситуацию, то это значит, что нарастают негативные моменты, на которые ему надо обратить внимание и принимать соответ-

ствующее решение. Сейчас в системах поддержки принятия решений уже реализуются методы, с помощью которых можно заложить в систему возможные действия, и на фоне негативно сложившейся ситуации человек сможет увидеть, возможно ли переломить ситуацию.

При моделировании ситуации системой предлагается, как правило, несколько вариантов, а лицо ответственное за принятие решения должно выбрать из них наиболее оптимальные по его мнению. Такая человеко-машичная система заставляет машину предлагать варианты (машина не должна принимать решения), а человек уже сам должен принимать решение. Норберт Винер, отец кибернетики, в одной из бесед с журналистами на вопрос, что будет, если машина будет изобретательнее человека, еще пятьдесят лет назад ответил: «Если машина изобретательнее человека, это уже катастрофа». Он никогда даже не допускал такой мысли, которую впоследствии стали допускать его, казалось бы, последователи, что увлечение этой работой с информацией приведет человека к идеи создания действительно думающей, даже чувствующей машины, как нам сейчас обещает новый прорыв в компьютерных технологиях.

В настоящее время чем мощнее бизнес, тем чаще приходится сталкиваться с ситуациями предпринимательского риска. Работа на российском рынке в условиях политической и экономической нестабильности серьезно увеличивает набор угроз, а соответственно и рисков в предпринимательской деятельности. Предпринимателю приходится больше внимания уделять планированию и контролю на предприятии, и зачастую он не способен обойтись без специального инструментария поддержки принятия решений по бюджетированию. Опыт показывает, что даже жизненно важные для бизнесмена решения в подавляющем большинстве случаев приходится принимать в условиях дефицита времени и необходимой информации.

Известно, что принятие решения в сфере бизнеса может основываться, например, либо на минимизации потерь, либо на максимизации прибыли. При этом выбор той или иной стратегии принятия решения должен опираться на объективную информацию, прогнозные оценки и аналитические выводы. Если потери при возможном неблагоприятном развитии событий больше ожидаемой прибыли при выигрыше ситуации, то риск не обоснован. Тем не менее многие российские предприниматели необоснованно рисуют (иногда даже не осознавая наличия риска), ставя на карту не только все

свое дело, но и средства кредиторов, разбивая свою и чужие судьбы. Известно, что средства, затрачиваемые на минимизацию риска, не должны превышать ожидаемой прибыли. Если эти условия не выполняются, то не надо бороться за безопасность бизнеса, им просто не следует заниматься в данных условиях.

Таким образом, можно говорить не только об огромном вкладе технологического прорыва последних лет в компьютерных технологиях, обеспечивающих работу систем поддержки принятия решений, но и о необходимости развития систем поддержки принятия решений и внедрении их в различные отрасли народного хозяйства, в том числе для решений экономических задач различных масштабов.

УДК 338.24

© В. Л. Горохов

Санкт-Петербургский государственный  
инженерно-экономический университет

© И. В. Вдовенко

Санкт-Петербургский государственный  
электротехнический университет

## РАЗРАБОТКА УСТОЙЧИВЫХ НЕПАРАМЕТРИЧЕСКИХ АЛГОРИТМОВ И ПРОГРАММНЫХ СРЕДСТВ ДЛЯ ПРОВЕРКИ ОДНОРОДНОСТИ ДАННЫХ ПРИ КОНТРОЛЕ ПРОЦЕССОВ ОБРАЩЕНИЯ С ТБО

Экономическое развитие, как известно, приводит к росту производства и потребления, что в свою очередь вызывает рост образования отходов. К настоящему времени отсутствует реальный учет образования отходов, их состава и маршрутов их размещения для Европы в целом, включая Россию. Систематический сбор данных по учету отходов проводится недавно, и его количественные результаты обычно совпадают с нормативами, заданными в законодательных актах, указах, постановлениях и правилах обращения с отходами. Статистика по странам, касающаяся систем образования и сбора отходов, часто не сопоставима из-за несовпадения дефиниций, систем классификации и целей. В целом мониторинг состояния окружающей среды показывает серьезные нарушения природопользования и значительное загрязнение территорий в мегаполисах и

охраняемых природных зонах. Во многом это результат практики неправильного управления процессами обращения с отходами.

В настоящее время проблема удаления твердых бытовых отходов не осознается широкой общественностью как одна из ключевых среди всех проблем прикладной экологии [1]. Сейчас на Северо-Западе очень остро стоит вопрос утилизации твердых бытовых отходов. Существующая сегодня в нашем городе система учета и контроля за сбором и размещением твердых бытовых отходов не позволяет полностью регулировать процесс движения потоков ТБО и исключить их размещение на несанкционированных свалках. В большей степени данная система отработана для жилого муниципального фонда, но и там она слабо контролирует движение потоков ТБО, образующихся в нежилом фонде. Практически отсутствует необходимый контроль за размещением отходов мелких и средних коммерческих структур [2].

Учет количества образующихся отходов и контроль за их перемещением и обезвреживанием в Санкт-Петербурге не централизован на основе современных сетевых технологий, а существующие программные системы носят локальный ведомственный характер и не содержат алгоритмических средств интеллектуальной поддержки административных решений в области обращения с отходами. Таким образом, программно-алгоритмическое обеспечение в области обращения с отходами оставляет желать лучшего, а в Ленинградской области практически отсутствует. Между тем, не наладив эффективный контроль, невозможно уберечь природную среду и население от вредного воздействия отходов.

Для эффективного оперативного контроля за движением отходов в регионе необходимо иметь справочно-информационную систему по отходам и интеллектуальную систему поддержки принятия решений по обращению с отходами, общую для Санкт-Петербурга и Ленинградской области.

Банк данных системы должен содержать в себе несколько баз данных, в том числе:

- базу данных, характеризующих территории региона с точки зрения их геологических и гидрологических условий с выделением мест, пригодных для размещения отходов;
- базу данных об источниках отходов, их составе, опасности и количестве, об условиях их вывоза, об объектах, занятых их переработкой ( заводы, полигоны, свалки и т. д.);

- базу данных о существующих в мире и об используемых в России методах и технологиях переработки отходов различных видов;
- базу данных по экономическим аспектам обращения с отходами;
- базу данных по действующим федеральным и региональным правовым и нормативным документам.

В справочно-информационную систему должны оперативно стекаться сведения о движении отходов и иная информация, необходимая для принятия как стратегических, так и оперативных решений. В системе должно использоваться соответствующее программное обеспечение. Такая система позволит организовать учет и контроль движения отходов с момента их образования и до конечного цикла переработки и утилизации, что предотвратит или по крайней мере снизит попадание отходов на несанкционированные места захоронения [3].

Примерная однородность потребления товаров многими людьми является причиной однородности состава твердых бытовых отходов. Учитывая глобальные процессы распространения продуктов и одинаковость потребностей людских масс, по изменению однородности распределения, можно решать актуальные задачи.

В комплекс критериев, определяющих подходы к реализации различных этапов санитарной очистки от ТБО, входят качественные показатели, характеризующие твердые бытовые отходы: морфологический и фракционный состав, содержание органического вещества, влаги, химических компонентов, а также критерии эпидемического неблагополучия.

ТБО по морфологическому признаку подразделяются на компоненты: бумагу, картон; пищевые отходы; дерево; металл (черный и цветной); текстиль; кости; стекло; кожу, резину; камни; полимерные материалы; прочие (неклассифицируемые фракции); отсев менее 15 мм.

Фракционный состав ТБО (процентное содержание массы компонентов, проходящих через сита с ячейками различного размера) оказывает влияние как на технологию и организацию сбора и транспорта, так и на параметры оборудования мусороперерабатывающих заводов.

Работа по определению морфологического и фракционного состава ТБО проводится по методике, разработанной и утвержденной

НИИ АКХ им. К. Д. Памфилова [4]. Решения по определению состава ТБО должны приниматься на основе тщательного анализа имеющейся информации, быть обоснованными и доказуемыми в рамках программных систем поддержки управленческих решений.

Для решения задач, связанных с анализом данных при наличии случайных воздействий, математиками был выработан арсенал методов робастной и непараметрической статистики. Широкому внедрению методов устойчивого анализа данных немало способствовало появление специализированных программных систем. Статистические программные пакеты сделали методы анализа данных более доступными и наглядными: теперь уже не требуется вручную выполнять трудоемкие расчеты по сложным формулам, строить таблицы и графики – всю эту черновую работу взял на себя компьютер, а человеку осталась главным образом творческая работа: постановка задач, выбор методов их решения и интерпретация результатов.

Результатом появления мощных и удобных пакетов для анализа данных на компьютерах стало резкое расширение и изменение круга потребителей методов анализа данных. Если раньше эти методы рассматривались главным образом как инструмент научных исследований, то сейчас основными потребителями статистических пакетов стали уже не научные, а коммерческие и производственные организации.

Во многих технологических процессах необходимо систематически контролировать состояние процесса, чтобы вовремя вмешаться при отклонениях его от нормального режима и предотвратить тем самым потери от выпуска некачественной продукции. Для этого используются статистические методы контроля качества [5].

Предлагается в системе обращения с ТБО использовать теорию качества, т. е. статистические методы обеспечения качества продукции, которые нашли широкое применение в промышленности [6]. Твердые бытовые отходы – это тоже в конечном счете продукт, только продукт жизнедеятельности человека, за которым необходим контроль. Контроль может быть основан на измерениях состава и количественных характеристиках ТБО. Таким образом, возникает необходимость разработки статистических методов обнаружения и контроля за процессом обращения с ТБО, используя различные свойства параметров распределений данных, полученных при натурных измерениях и мониторинге состава ТБО.

Предлагаемая концепция развития программных средств контроля качества обращения с ТБО относится к сфере переработки городских ТБО на заводах по механизированной переработке бытовых отходов (МПБО), здесь активно используется информационное и программное обеспечение для биотехнических методов охраны окружающей среды. В системе обращения с ТБО проводятся исследования фракционного и морфологического составов ТБО по сезонам года. Известно, что морфологический и фракционный составы ТБО в течение года приблизительно одинаковы. Потеря ТБО на несанкционированных свалках при транспортировке, изменение потребления продуктов людьми в различные периоды приводит к нарушению состава ТБО, что влияет на распределение данных по массе, полученных при определении фракционного и морфологического составов ТБО [7]. Резкое изменение морфологического и фракционного составов приводит к тому, что отдельные фрагменты выборки данных принадлежат к разным распределениям. Поэтому использование статистических решающих правил, обеспечивающих проверку на однородность в выборках данных по составу ТБО, позволит обеспечить выявление этого факта неоднородности, который выступает как индикатор нарушений состава ТБО и, следовательно, нарушений процесса обращения с ТБО. Таким образом можно пойти к решению задачи автоматизированного программного контроля качества окружающей среды в сфере обращения с ТБО.

Трудностью, возникающей на пути применения количественных решающих правил для оценивания качества среды, является необходимость обеспечения достоверности и надежности получаемых оценок и решающих правил. Причина возможной недостоверности и ненадежности стандартных решающих правил в том, что они конструируются под конкретную статистическую, достаточно узкую модель данных (например, нормальность выборки). В реальной практике наблюдаются серьезные отклонения от этих моделей, что приводит к ненадежности применения параметрических решающих правил и оценок. Таким образом, незнание или отклонение модели данных способствует ложным оценкам и выводам. Эта трудность преодолевается с помощью методов непараметрической статистики, которые обеспечивают стабильную работу решающих правил в условиях, когда тип распределения неизвестен и может меняться.

Кроме того, непараметрические решающие правила, используемые здесь, включают в свои структуры оценки качества среды (статистики) и пороговые уровни, которые задаются исходя из принципов приемлемой опасности. Назначение порогового уровня делается из практических и экологических соображений, обеспечивающих безопасность населения или экологических систем.

Таким образом, концепция информационных систем управления отходами предполагает набор количественных характеристик качества среды – морфология и фракционность. По этим характеристикам на основании статистических решающих правил проверки однородности принимается решение о состоянии процесса обращения с ТБО. Эти решающие правила и соответствующие решения, полученные в программной системе поддержки управлеченческих решений служат основой для формирования административных норм. Такие оценки и решающие правила должны схватывать все основные свойства и характеристики сложного социального и физико-химического процесса обращения с ТБО и поэтому получили название интегральных оценок и решающих правил.

Именно на базе таких оценок и решающих правил появляется возможность разрабатывать современные программные системы поддержки экологических решений.

Предлагается проверять гипотезу об однородности данных по массе фракционного и морфологического составов ТБО с помощью непараметрического (свободного от распределения решающего правила (критерия) однородности двух выборок (Колмогорова–Смирнова)). Для повышения устойчивости работы правила в условиях наличия случайно цензурированных данных (верхних пределов), предлагается использовать в структуре критерия модифицируемые соответствующим образом (модификация Пето–Прентиса) эмпирические функции распределения.

С точки зрения экологии это правило хорошо выявляет любые изменения в процессе обращения с отходами, т. е. является интегральным экологическим критерием.

Проверка гипотезы о статистической однородности основывается на непараметрических критериях, которые в общем случае могут быть записаны как

$$\begin{cases} f(X_i) > C_\alpha(H_0) \\ f(X_i) \leq C_\alpha(H_1) \end{cases},$$

где  $f(X_i)$  – функция преобразования (статистика);  
 $C_\alpha$  – порог критерия;

$\alpha$  – ошибка первого рода (вероятность ложной тревоги), которая задается пользователем из практических соображений. На данном этапе последовательно используются несколько функций преобразования:

Колмогорова–Смирнова

$$f(X_i, Y_i) = \sqrt{\frac{mn}{m+n}} \sup_t |F_{n,x}^*(t) - F_{m,y}^*(t)|,$$

где  $m$  и  $n$  объемы выборок по  $X$  и  $Y$  соответственно;  
 $F_{n,x}^*(t), F_{m,y}^*(t)$  – эмпирические функции распределения, обеспечивающие обработку данных с учетом верхних пределов.

Для успешной адаптации данной процедуры в технологический цикл контроля ТБО предлагается также усовершенствовать таблицу для записи морфологического состава путем внесения промежуточных результатов по морфологии отдельных фракций, чтобы выяснить, какой именно тип отходов изменился по объему.

Методика контроля за обращением с ТБО предполагает необходимость проводить периодический контроль состава ТБО, а данные по морфологическому и фракционному составам ТБО предполагается заносить в данные таблицы, заполняя таким образом базу данных. После этого следует проводить контроль однородности состава ТБО по предложенному критерию для обнаружения нарушений в составе ТБО. Контроль однородности следует проводить на мусороперерабатывающих заводах, так как все оборудование рассчитано на однородный постоянный состав мусора. При проектировании заводов механизированной переработки твердых бытовых отходов целесообразно использовать в первую очередь отечественное серийно выпускаемое промышленностью оборудование, надежность которого проверена в условиях многолетней эксплуатации на действующих в стране заводах, и которое может успешно перерабатывать образующийся состав мусора.

При разработке принципиальной технологической схемы заводов МПБО необходимо учитывать особенности работы как технологической схемы, так и отдельных элементов оборудования. Первая (основная, с точки зрения обезвреживания ТБО) стадия процесса аэробного биотермического компостирования ТБО на современных заводах МПБО осуществляется в горизонтальных вращающихся барабанах. Биотермическое разложение органического вещества происходит в результате жизнедеятельности сапроптических аэробных микроорганизмов, способных выделять при биохимических реакциях обмена веществ определенное количество тепла. Требующаяся для биотермического процесса микрофлора имеется в необходимых количествах в ТБО. Вторая стадия – в штабелях на площадке дозревания.

На основе предложенного критерия разработана и предлагается к использованию программа компонента системы контроля окружающей среды в сфере обращения с ТБО на заводах МПБО на основе модернизированного правила проверки гипотезы об однородности данных фракционного и морфологического составов ТБО – это программное инструментальное средство обработки данных по составу ТБО («алгоритм Колмогорова–Смирнова»), полученных по методике НИИ АКХ им. К. Д. Памфилова. Программная компонента написана с использованием языка C++ и библиотеки шаблонов STL. В программной компоненте применяются встроенные контейнеры библиотеки для автоматизации некоторых операций, в частности, сортировки и автоматического выделения памяти. Рассмотрим детально, как функционирует программа.

В процессе работы создаются два объекта-контейнера. Multi-set-контейнер – это обозначение математического одномерного пространства, в котором хранятся элементы, отсортированные по определенному признаку. Пространство безразмерно. Доступ к элементам осуществляется с помощью специальных переменных – так называемых итераторов. Vector-контейнер – аналог одномерного массива, который содержит элементы определенного типа. Этот контейнер также безразмерен.

Заключительной фазой работы программной компоненты является нахождение в таблицах Колмогорова–Смирнова значения  $\alpha$  и сравнения величины  $J_3$  с табличным значением. Таблица организована в виде структуры [8]:

X  
Alpha  
X  
Alpha  
...  
...

Особенностью этого пакета является использование модернизированного алгоритма, а также более удобное задание порогового уровня. Как известно, проверка однородности данных осуществляется во многих программных пакетах. Но в этих пакетах решение при использовании правила Колмогорова–Смирнова выносится на основе достигаемого уровня значимости, вычисляемого программой (концепция Фишера). Программная компонента «алгоритм Колмогорова–Смирнова» обеспечивает реализуемое на практике количественное описание результата работы – уровень значимости, задаваемый пользователем в рамках концепции Неймана–Пирсона.

#### Литература

1. Юлдышев Ю. Н. Отходы: не зарывать, а перерабатывать // Экология и жизнь. 2003. № 1(30). С. 52–54.
2. Багдасаров Р. С., Нечистяк Т. А. Проблемы и реальность управления московскими ТБО // Чистый город. 2002. № 2. С. 2.
3. Единая политика обращения с отходами в Санкт-Петербурге и Ленинградской области / Под ред. С. Г. Инге-Вечтомова, Ю. И. Скорика. СПб.: НИИ Химии СПбГУ, 2000.
4. Новиков М. Г. и др. Отчет о научно-технической продукции. Определение фракционного и морфологического состава ТБО Санкт-Петербурга и Ленинградской области и балласта / М. Г. Новиков, А. С. Гурьев, В. Л. Горюхов, Н. В. Оттас. СПб., 2001.
5. Миттаг Х.-Й., Ринне Х. Статистические методы обеспечения качества. М.: Машиностроение, 1995.
6. Твердые бытовые отходы (сбор, транспорт и обезвреживание): Справочник / В. Г. Систер, А. Н. Мирный, Л. С. Скворцов и др. М., 2001.
7. Тюрин Ю. Н., Макаров А. А. Анализ данных на компьютере / Под ред. В. Э. Фигурнова. М.: ИНФРА-М, Финансы и статистика, 1995.
8. Березин Б. И., Березин С. Б. Начальный курс С и С++. М.: ДИАЛОГ-МИФИ, 2001.

УДК 378.001

© О. П. Ильина, Г. А. Мамаева

Санкт-Петербургский государственный  
инженерно-экономический университет

## УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ ТЕХНОЛОГИЯМИ

Для динамичного развития экономики необходимы эффективные информационные технологии (ИТ) управления, комплексная информатизация сферы принятия управленческих решений. В последнее время возникло самостоятельное направление менеджмента – система управления ИТ (IT Governance), определяемое как «структура взаимоотношений и процессов выбора вектора развития предприятия и его контроля, направленных на увеличение стоимости при сбалансированном риске в сфере информационных технологий»<sup>1</sup>. По инициативе ассоциации Information Systems Audit and Control Association (ISACA) и фонда Information Systems Audit and Control Foundation (ISACF) в 1998 г. создан IT Governance Institute, назначение которого – разработка методологии использования и аудита ИТ. Основополагающими принципами IT Governance являются.

1. Ответственность (accountability) за каждое действие или решение, связанное с ИТ.
2. Прозрачность (transparency) объектов контроля ИТ, принятых решений и действий.
3. Представление (disclosure) важной информации для всех заинтересованных лиц, охваченных ИТ.
4. Независимость (independence) решений от интересов отдельных групп.
5. Ясность ожиданий (clear expectations) результатов внедрения ИТ.

Целями IT Governance являются: приведение ИТ в соответствие с реальными потребностями и условиями деятельности предприятия, внедрение новых, улучшение существующих ИТ, эффективное использование ИТ-ресурсов, управление ИТ-рискаами. Участники IT Governance – руководители предприятия, которые могут

<sup>1</sup> COBIT 3<sup>rd</sup> Edition, Released by the COBIT Steering Committee and the IT Governance Institute, July 2000.

определить цели нововведений и оценить конечные результаты, ограничить финансирование ИТ<sup>1</sup>, а также ИТ-менеджеры.

Для реализации IT Governance применяется методология COBIT (Control Objectives for Information and Related Technologies) – управление задачами информационных и смежных технологий, оформленная как стандарт, а сам управленческий цикл включает:

- 1) рассмотрение системы ценностей для предприятия;
- 2) согласование стратегических целей бизнеса и возможностей ИТ;

- 3) собственно реализацию ИТ;
- 4) мониторинг и управление рисками ИТ;
- 5) оценку и анализ эффективности ИТ.

COBIT объединяет ряд руководств, моделей анализа, инструментов оценки ИТ, которые могут применяться на протяжении жизненного цикла ИТ, на различных уровнях или в разных сферах управления:

- резюме для руководителя – описание стандарта COBIT, ориентированное на топ-менеджеров организации для принятия ими решения о применимости стандарта в конкретной организации;
- концептуальное ядро – содержит задачи управления высокого уровня;
- детальные задачи управления;
- руководство по менеджменту;
- руководство по ИТ-аудиту;
- модели зрелости;
- критические факторы успеха;
- ключевые показатели цели;
- ключевые показатели эффективности.

Переход к IT Governance требует определения информационных критериев, ИТ-ресурсов, ИТ-процессов. К ИТ может быть применен «процессный подход», согласно которому выделяют **ключевые показатели цели** – КПЦ (оценка степени достижения цели); **ключевые показатели эффективности** – КПЭ (оценка средств, применяемых для достижения целей). Условиями достижения поставленных целей ИТ являются **критические факторы успеха** – КФУ.

<sup>1</sup> Согласно статистике, компании США в среднем тратят 5,5% своего оборота на ИТ (средние данные по отраслям варьируются от 3,8 до 7,4%).

Взаимосвязь составляющих процессного подхода к ИТ показана на рис. 1.



Рис. 1. Взаимосвязь составляющих процессного подхода к ИТ

Для эффективного управления ИТ выделяют иерархию объектов (рис. 2).

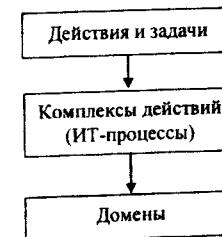


Рис. 2. Иерархия объектов эффективного управления ИТ

Задачей управления ИТ является формулировка желаемого результата или целей, которые должны быть достигнуты за счет реализации механизмов управления в рамках конкретного действия или ИТ-процесса. Действия и задачи выделяют так, чтобы можно было получить измеримый результат эффективности управления. ИТ-процессы включают набор действий и задач, нацеленных на достижение поставленных бизнес-целей. Домены связаны с группировкой ИТ-процессов в соответствии с ответственностью в организационной структуре предприятия. Согласно COBIT в качестве доменов рассматриваются.

## 1. Планирование и организация ИТ.

2. Проектирование и внедрение ИТ.
3. Эксплуатация и сопровождение ИТ.
4. Мониторинг ИТ.

Внутри доменов определены 33 высокоуровневые цели контроля за ИТ-средой.

#### *Планирование и организация ИТ.*

1. Определить стратегический план ИТ.
2. Определить информационную архитектуру.
3. Определить технологическое направление.
4. Определить организацию и взаимоотношения ИТ.
5. Управлять инвестициями в ИТ.
6. Согласованно управлять целями и задачами.
7. Управлять персоналом.
8. Обеспечить согласование с внешними требованиями.
9. Оценить риски.
10. Управлять проектами.
11. Управлять качеством.

#### *Проектирование и внедрение ИТ.*

1. Определить решения по автоматизации.
2. Приобрести и поддерживать прикладное программное обеспечение.

3. Приобрести и поддерживать технологическую инфраструктуру.
4. Разработать и поддерживать процедуры.
5. Установить и аккредитовать системы.
6. Управлять изменениями.

#### *Эксплуатация и сопровождение ИТ.*

1. Определять уровни обслуживания и управлять ими.
2. Управлять услугами сторонних организаций.
3. Управлять производительностью и наращиваемостью.
4. Обеспечивать непрерывность услуг.
5. Обеспечивать безопасность системы.
6. Определить и распределить затраты.
7. Обучать пользователей.
8. Помогать пользователям и консультировать их.
9. Управлять конфигурацией.
10. Управлять деньгами.
11. Управлять оборудованием.
12. Управлять операциями.

#### *Мониторинг ИТ.*

1. Проводить мониторинг процессов.
2. Оценивать адекватность внутреннего контроля.
3. Получать независимые гарантии.
4. Обеспечивать независимый аудит.

В качестве критериев успеха ИТ применяются показатели:  
– эффективности (effectiveness) применения ИТ в бизнес-процессе;

- производительности (efficiency) объекта управления ИТ;
- конфиденциальности (confidentiality);
- целостности (integrity);
- доступности (availability) информации ИТ;
- правомочности использования (compliance);
- надежности (reliability) ИТ и др.

Механизмы управления ИТ выбираются с учетом требований бизнес-целей и включают в себя:

- политики (доступа, защиты, выполнения процедур обработки и т. п.);
- организационные структуры;
- процедуры;
- регламенты.

Для реализации ИТ используются ИТ-ресурсы, которые можно разделить на: *данные* (все виды используемых источников данных), *приложения* (автоматизированные и ручные процедуры обработки данных), *технические и программные средства* (техническое и программное обеспечение), *персонал*. Для управления ИТ-ресурсами применяются адекватные механизмы управления.

Руководство предприятия реализует более эффективные стратегии управления ИТ; устанавливает контроль над использованием информационных ресурсов и соответствующими процессами; осуществляет мониторинг; дает сравнительную оценку достижения бизнес-целей; оценивает производительность в рамках каждого ИТ-процесса.

СОБИТ вводит понятие *модели зрелости организации* (Maturity Model), с помощью которой можно дать оценку текущему состоянию ИТ-процессов (сравнить с лучшими примерами в данной отрасли и найти возможности их совершенствования). Определяются шесть уровней зрелости системы управления ИТ:

*Уровень 0 – полное отсутствие системы ИТ;  
Уровень 1 – осознание необходимости комплексного подхода к ИТ;  
Уровень 2 – повторяющиеся процессы следуют некоторым схемам;  
Уровень 3 – определенные процессы описаны и доведены до сведения всех участников;  
Уровень 4 – управляемые процессы измеряются и управляются;  
Уровень 5 – оптимизация ИТ.*

УДК 378.001

© Г. А. Мамаева

Санкт-Петербургский государственный  
инженерно-экономический университет

## СТРАТЕГИИ РАЗВИТИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Внедрение информационных технологий (ИТ) в корпоративную систему управления связано с серьезными рисками и значительными инвестициями. Но роль ИТ постоянно возрастает, и более того, начинает сильно влиять на маркетинг, закупки и все остальные стороны деятельности предприятия. При этом информационное обеспечение организации должно соответствовать уровню развития управлеченческих процессов и корпоративной стратегии. Поэтому при внедрении информационных технологий необходим взвешенный подход, в соответствии с которым следует определить приоритеты в решении управлеченческих задач, выработать стратегию развития информационных технологий и после этого приступить к последовательной ее реализации.

ИТ-стратегия – это программа развития информационных систем и технологий в соответствии со стратегией развития предприятия, текущими и будущими потребностями бизнеса.

О необходимости разработки или актуализации ИТ-стратегии свидетельствуют следующие проблемы: неудовлетворенность текущим состоянием информатизации предприятия; недостаточная эффективность отдачи от ИТ; отсутствие понимания, в каких направлениях развивать имеющиеся информационные системы, какие

проекты выбрать в качестве приоритетных, стоит ли вкладываться в очередные новые технологии, и если да, то когда. Решить эти проблемы можно при помощи четко составленной ИТ-стратегии.

Однако основная проблема большинства ИТ-проектов заключается в отсутствии у руководства четкой ИТ-стратегии, прежде всего, ясного понимания целей проекта. Причиной является незнание всех потенциальных эффектов автоматизации своего предприятия и способа их достижения. Следствием неверной ИТ-стратегии становится прежде всего несоответствие вложенных ресурсов и полученного эффекта от внедрения новой технологии, а также невнимание руководства к структурным проблемам ИТ-предприятия.

Кроме того, в отсутствие ясной стратегии, связывающей затраты на ИС и результаты бизнеса, финансовые службы склонны относить затраты на ИС к накладным расходам и минимизировать их всеми доступными способами.

В общем случае в ИТ-стратегию могут быть включены следующие составляющие:

- информационные системы: прикладное программное обеспечение типа «делопроизводство», «бухучет» и др., ради чего используются компьютеры. Иногда, например, в рамках методологии ITIL (Information Technologies Infrastructure Library – библиотека передового опыта в области управления ИТ) говорят об ИТ-сервисах;
- ИТ-инфраструктура: компьютеры, телекоммуникации, системное программное обеспечение;
- ИТ-служба и управление ею: цели и задачи службы, организационная структура, методы управления персоналом и др.

На большинстве предприятий, к сожалению, очень часто начинают строить ИТ-стратегию с определения и внедрения технической инфраструктуры. Это может привести к автоматизации плохо организованных или устаревших процессов и только усугубит бизнес-проблемы и приведет к резкому увеличению операционных затрат.

Прежде чем браться за создание ИТ-инфраструктуры компаний, необходимо осуществить перемены, направленные на укрепление организационной дисциплины внутри этой компании и особенно ее бизнес-процессов. В результате стандартизации и упрощения существующих бизнес-процессов еще до начала ИТ-проекта удается получить реальную и быструю отдачу от инвестиций.

По сравнению со стоимостью технических и программных средств затраты на разработку и актуализацию ИТ-стратегии вряд ли превысят несколько процентов ИТ-бюджета. Между тем проблемы, связанные с отсутствием стратегии или ее плохой проработкой, наверняка могут вылиться в гораздо большие деньги. Кроме того, безупречная с точки зрения формальностей ИТ-стратегия вряд ли приведет к чему-то хорошему на предприятии, где не определена стратегия бизнеса.

*Методика построения ИТ-стратегии.* На начальном этапе формирования ИТ-стратегии необходимо понять бизнес-стратегию компании, которая включает в себя набор бизнес-задач предприятия в отношении отдельных рынков, категорий продуктов, клиентов, географического распределения филиалов, а также основные финансовые показатели деятельности компании. Руководители информационных служб должны принимать активное участие в формировании бизнес-стратегии компании.

Второй этап – построение операционной модели, которая описывает процесс взаимоотношений бизнес-подразделений в ходе решения задач, определенных в бизнес-стратегии.

Третий этап – построение модели данных, на которые опираются ключевые бизнес-процессы, составляющие операционную модель.

Четвертый этап – определение и внедрение технической инфраструктуры.

ИТ-стратегия дает компании следующие преимущества: обеспечивает интегрированный подход к автоматизации всех контуров управления предприятием («Финансы/Управление», «Производство», «Торговля», «Маркетинг» и т. д.) и позволяет избежать типичных ошибок «блоскунной автоматизации», особенно в быстрорастущих организациях.

ИТ-стратегия позволяет:

- оптимизировать затраты на реализацию ИТ-задач;
- сократить риски при внедрении ИТ-систем;
- организовать адекватную информационную поддержку текущих бизнес-процессов;
- обеспечить развитие ИТ-систем по мере роста бизнеса.

Процессы построения ИТ-стратегии в компаниях разных отраслей одни и те же независимо от отрасли. Однако содержание стратегий может значительно различаться. Причина тому – разли-

чия бизнес-задач. Именно это сказывается на рыночных характеристиках той или иной компании.

Основная цель бизнес-стратегии – повышение рыночной стоимости компании или валового дохода. Это достигается разными способами – поглощениями, географической экспанссией, предложением новых услуг и продуктов, снижением цен, улучшением сервиса и т. п. ИТ-стратегия будет строиться в зависимости от способа достижения бизнес-целей и может потребовать применения одного или нескольких следующих методов: реинжиниринга ключевых бизнес-процессов, построения процессов и систем доступа к ключевой информации об операционной деятельности компании, внедрения передовых технологий и приложений, оптимизации существующей ИТ-инфраструктуры и т. п.

Свои особенности, связанные с масштабом бизнеса, имеет автоматизация крупных предприятий. Чтобы не потерпеть неудачу, необходимо тщательно учитывать целый комплекс взаимосвязанных факторов.

На крупных предприятиях, в силу специфики, приходится использовать разнородные программные продукты. Современные интегрированные информационные системы ERP-класса, хотя и охватывают большинство функциональных областей деятельности предприятия, но обычно не покрывают все потребности в автоматизации, которые на крупном предприятии очень обширны.

Существуют два пути построения информационной системы крупного предприятия. Первый – выбрать полнофункциональную интегрированную ERP-систему в качестве ядра и развивать ее своими силами или силами сторонних организаций. Второй подход – выбрать решения, лучшие в своей области, и интегрировать их в единую информационную систему. Возможен и комбинированный подход. В первом случае риски лежат в области квалификации постановщиков задач и программистов, во втором – в сложности интеграции разнородных систем.

Стратегия автоматизации крупных предприятий требует особого внимания. Во-первых, последовательность автоматизации должна быть такой, чтобы не требовалось кардинально менять то, что уже сделано на предыдущих этапах автоматизации. Во-вторых, последовательность автоматизации должна быть тесно связана с ее эффективностью. А значит, в первую очередь должны быть автоматизированы те области деятельности предприятия, в которых при-

менение информационных технологий принесет наибольший эффект для бизнеса компаний.

Что касается требований к ИТ-подразделению крупной компании, которое решает целый комплекс сложных, взаимосвязанных задач, то здесь особенно целесообразной будет организация функционирования ИТ-подразделения на основе процессного подхода в соответствии со стандартами Cobit, ITIL и др.

Если ИТ-стратегия построена правильно, она дает ответ на целый ряд ключевых вопросов, связанных, прежде всего, с популярной концепцией стоимости бизнеса:

- какова польза и ценность информационных технологий для бизнеса предприятия;
- где именно и как на предприятии ИТ могут быть использованы наилучшим образом, принося наивысшую отдачу;
- каков должен быть уровень вложений в ИТ.

Кроме того, грамотно выстроенная ИТ-стратегия непосредственно способствует росту стоимости бизнеса путем:

- оптимизации производительности и полезности основных ИТ-работ;
- поддержки функционирования и преобразования цепочки создания прибавочной стоимости данного предприятия;
- опробования новых технологий, новых способов ведения бизнеса, продуктов и услуг.

Одним словом, правильная ИТ-стратегия помогает достигать поставленных целей гораздо более эффективно и открывает возможность удовлетворения как сегодняшних, так и будущих требований.

УДК 378.001

© Ж. Г. Салимьянова

Санкт-Петербургский государственный  
инженерно-экономический университет

## ФОРМИРОВАНИЕ УМЕНИЙ ИСПОЛЬЗОВАНИЯ СРЕДСТВ КОМПЬЮТЕРНОЙ ГРАФИКИ У СТУДЕНТОВ

В настоящее время в связи с внедрением в образовательную практику университетов инновационных информационных технологий появилась реальная возможность обучать студентов компью-

терной графике и использованию средств коммуникаций для творческого самовыражения.

В силу расширения влияния средств массовой информации компьютерная графика должна быть частью непрерывного компьютерного образования, когда на всем периоде обучения изучение и использование вычислительной техники являются одним из важных дидактических условий успешного и устойчивого формирования алгоритмико-компьютерных знаний у будущих специалистов.

Сегодня можно утверждать, что наряду с профессиональным медиаобразованием, необходимо говорить и об общем медиаобразовании, цели которого должны быть ориентированы на приобретение студентами знаний о коммуникациях и средствах массовой информации, которым не придается профессиональная направленность.

Значительная роль, широкие возможности и разнообразие применений компьютерной графики в создании визуального ряда средств массовой коммуникации актуализируют изучение данного курса. Свойство компьютерной графики быть многозначной, необычной, способность скрывать некие смыслы за иносказательной формой, имеет большую дидактическую ценность.

Компьютерная графика сегодня – наиболее мощное средство творческого создания визуального ряда средств массовой коммуникации и мощный инструмент визуального мышления.

Курс компьютерной графики приобщает студентов к современной визуальной медиакультуре, восприятию информации, подаваемой с экрана, творчеству средствами компьютерной графики в целях овладения «механикой» создания и интерпретации масс-медиа, развитию коммуникативных способностей, готовит к жизни в новых информационных условиях.

Особое значение в процессе изучения данного курса придается практическому освоению использования средств компьютерной графики в создании корпоративного стиля, в рекламном бизнесе, в средствах массовой информации, использованию графических программ в бизнесе, в области дизайна, Интернете, телевидении.

Не будет преувеличением сказать, что во всех профессиональных областях много точек приложения графических программ.

Эффективность обучения достигается расширением возможностей обратной связи индивидуальной работы.

Курс компьютерной графики может быть построен «вертикально» или «горизонтально». Вертикальное построение ведет от технологии и эстетики традиционного рисунка, живописи и традиционной анимации к компьютерной анимации. Горизонтальное построение курса представляет компьютерную анимацию как одно из средств новых медиа-технологий, выявляет роль компьютерных компонент в структуре медиа-продуктов.

Обучение состоит из двух частей.

1. Изучение теории, задач компьютерной графики, областей ее применения.

2. Практическое освоение ее программного инструментария, принципов построения изображений.

Это означает, что система практических заданий и технология практического обучения должны стимулировать студентов не только осваивать богатый инструментарий, но и генерировать художественные задачи, требующие творческого исследования этого инструментария. Практические занятия дают пищу теоретическому анализу.

Таким образом, с учетом дидактических возможностей и специфики компьютерной графики общие цели изучения графических программ конкретизируются следующим образом:

- выработка ориентации в современной культуре масс-медиа;
- творчество средствами компьютерной графики в целях овладения механикой создания и интерпретации;
- развитие коммуникативных способностей студентов.

УДК 621.322

© Т. Н. Нестерук

Санкт-Петербургский государственный  
инженерно-экономический университет

## СПЕЦИФИКА МОДЕЛИРОВАНИЯ ИНТЕЛЛЕКТУАЛЬНОГО КОРПОРАТИВНОГО САЙТА

Рассмотрим вопросы моделирования адаптивных процессов на корпоративном сайте (КС) с целью анализа эффективности применения механизмов рекламы (МР), их размещения в иерархии страниц КС, направленного на выявление интересов посетителей сайта, соответствующую коррекцию информационной составляющей рек-

ламных материалов, повышение достоверности экономического анализа положения хозяйствующего субъекта на рынке.

Понятие «информационно-коммуникационные технологии» (ИКТ) ассоциируется с прогрессом, передовым уровнем развития науки и техники, экономической и финансовой сферы, организационных и управляющих структур. Наряду с ИКТ неотъемлемым атрибутом современности является реклама. Выводы проведенных исследований подтверждают существенное влияние рекламы на процессы жизнедеятельности человеческого общества.

Наряду с информационными технологиями неотъемлемым атрибутом современности является *реклама*, присутствующая во всех сферах общественной, политической, экономической, социальной и других видов деятельности. Многоликий феномен рекламы исследуется учеными со всевозможных сторон, в том числе с философской, социальной, экономической, этической. Выводы проведенных исследований зачастую противоречивы, но бесспорным остается один факт – существенное влияние рекламы на процессы, протекающие во всех сферах жизнедеятельности человеческого общества.

Повсеместное распространение и доступность ИКТ ставит перед специалистами в области рекламы актуальные задачи проведения эффективного Интернет-маркетинга [1] и оптимизации информационного содержания сайтов хозяйствующих субъектов, занимающихся коммерцией в Интернете [2]. Оптимизация информации, размещенной на КС, осуществляется с использованием интеллектуальных механизмов нейронных сетей (НС), систем нечеткой логики (НЛ), семантического web. Формирование семантического ядра, вокруг которого организуется сайт, основных элементов HTML-разметки сайта, регулярная коррекция информационного содержимого сайта – необходимые этапы проведения оптимизации КС [2].

Основная цель, преследуемая созданием КС, заключается в пробуждении интереса у потенциальных потребителей товаров и услуг, производимых субъектом рыночных отношений, а также формировании у потребителей в процессе посещения сайта желаемого для корпорации спектра потребностей.

Актуальным представляется исследование влияния МР в информационной архитектуре КС на повышение эффективности бизнес-процессов. Динамичная коррекция используемого набора МР,

оптимизация информационного наполнения иерархии вложенных страниц приводят к необходимости адаптации информационной архитектуры КС в соответствии с интересами посетителей сайта.

Реализация свойства адаптивности информационной структуры сайта, учитывающего интересы посетителей КС, невозможна без использования инструментальных средств интеллектуального анализа динамики пользовательского интереса. В связи с этим задача анализа и коррекции информационного содержания КС с применением интеллектуальных средств НС, НЛ является актуальной.

При решении экономических задач, для которых характерно наличие неполной и недостаточно достоверной информации, хорошо зарекомендовали себя системы интеллектуального анализа данных. НС и НЛ являются инструментом интеллектуального поиска и извлечения знаний, так как обладают способностью выявления значимых признаков и закономерностей в исходных данных [4]; [5]. Гибридные (нейронечеткие) системы интеллектуального анализа позволяют оптимизировать затраты на разработку, модификацию и эксплуатацию КС субъекта рыночных отношений.

Для автоматизации процесса адаптации механизмов рекламы под интересы посетителей КС необходимо выбрать математический аппарат, разработать комплекс показателей и интерактивные инструментальные средства, входящие в состав модели адаптивного КС. Для субъекта рыночных отношений представляется целесообразной разработка адаптивных средств моделирования бизнес-процессов, системы показателей эффективности размещения рекламных материалов на иерархии страниц сайта и методик смены информационного содержания рекламных материалов КС исходя из результатов интеллектуального анализа коммерческой деятельности хозяйствующего субъекта и интересов посетителей сайта.

Модель адаптивного КС [3] представляют в виде иерархии страниц, содержащих набор МР, информационных и рекламных материалов, размещение которых на сайте выполняется в соответствии с целевой функцией (рейтингом сайта). Рейтинг КС рассчитывается исходя из экспертных оценок, корректируемых в процессе работы сайта на основе анализа информационных полей нейронных и нейронечетких сетей (ННС), входящих в состав адаптивного КС.

На нижних уровнях иерархии модели КС решают задачу классификации интересов по совокупности признаков посещения сайта,

носящих неполный и недостоверный характер. НС нижних уровней, исходя из опыта экспертов реализуют систему нечетких правил, которая описывает процесс логического вывода, используя нечеткие посылки в виде векторов признаков посещения сайта.

На верхних уровнях иерархии для страниц сайта используют результаты классификации интересов (посылок) для формирования заключений-соответствий «интересы-МР». Решается задача классификации МР по вектору признаков посещения сайта. НС и ННС после обучения отражают достоверность удовлетворения интересов, входящих в отдельное правило, соответствующим МР.

Адаптивные свойства сайта реализуются через способность НС к классификации и кластеризации объектов анализа. Нечеткий логический вывод позволяет использовать опыт экспертов в виде системы нечетких правил логического вывода для предварительного обучения ННС – способность информационного поля НС к накоплению знаний в процессе обучения и возможность наследования опыта путем переноса информационных полей в модификацию КС.

Отображение системы нечетких правил логического вывода в структуре ННС и их изучение на множестве интересов посетителей сайта позволяют устраниТЬ противоречивость системы нечетких правил и проанализировать процесс логического вывода для коррекции системы нечетких правил средств анализа КС. Механизм нечеткого логического вывода может быть использован при решении задачи классификации входных векторов (интересов) посредством нейронечеткого классификатора [4].

Модель адаптивного КС сопровождается разработкой системы показателей и методики оценки эффективности МР в иерархии страниц сайта, интерактивных программных средств и методики их применения для визуализации результатов расчетов с целью последующего анализа специалистами и оптимизации размещения МР и информационных материалов на иерархии страниц КС.

Система показателей для оценки эффективности МР в иерархии страниц сайта, учитывающая достоверность активации МР и прибыль от удовлетворения интересов посетителей КС может быть построена аналогично оценочным показателям информационных ресурсов и безопасности иерархических систем [5]. При оптимизации размещения МР на сайте используют экспертные оценки для

сопоставления интересов посетителей сайта с прибылью от их удовлетворения и местом размещения MP на страницах КС.

Результаты экспертных оценок и последующего обучения ННС представляют матрицей  $A$  достоверности «страницы–MP»

$$A_{mn} = \begin{pmatrix} a_{11} & a_{12} & a_{1j} & a_{1n} \\ a_{21} & a_{22} & a_{2j} & a_{2n} \\ a_{i1} & a_{i2} & a_{ij} & a_{in} \\ a_{m1} & a_{m2} & a_{mj} & a_{mn} \end{pmatrix},$$

где  $i = 1, \dots, m$  – число MP,  $j = 1, \dots, n$  – число страниц КС.

Активность страницы КС по удовлетворению интересов посетителей сайта определяется строкой интегральных показателей, представленных, например, строкой показателей значимости, сформированной из модулей векторов активности страниц КС

$$x_j = \sqrt{\sum_{i=1}^n a_{ij}^2}, \quad j = 1, \dots, n.$$

Если каждый столбец матрицы рассматривать в качестве вектора активности отдельного MP, то элементам столбца интегральных показателей значимости MP можно поставить в соответствие длину вектора активности одноименного MP на странице КС

$$x_i = \sqrt{\sum_{j=1}^n a_{ij}^2}, \quad i = 1, \dots, m.$$

Методика оценки эффективности сайта использует модель адаптивного КС, систему показателей для оценки эффективности MP для минимизации соотношения «затраты/эффективность» КС.

1. Исходные данные – экспертные оценки представляют в матричной форме. Для страниц сайта оценивают достоверность удовлетворения интересов посетителей сайта механизмами рекламы и формируют матрицы  $B$  достоверности «MP–интересы»

$$B_{mp} = \begin{pmatrix} b_{11} & b_{12} & b_{1p} \\ b_{21} & b_{22} & b_{2p} \\ b_{m1} & b_{m2} & b_{mp} \end{pmatrix},$$

где  $i = 1, \dots, m$  – число MP;

$j = 1, \dots, p$  – число интересов посетителей сайта, и матрицы  $C$  достоверности «интересы–страницы»

$$C_{pn} = \begin{pmatrix} c_{11} & c_{12} & c_{1n} \\ c_{21} & c_{22} & c_{2n} \\ \vdots & \vdots & \vdots \\ c_{p1} & c_{p2} & c_{pn} \end{pmatrix},$$

где  $i = 1, \dots, p$  – число интересов посетителей сайта;

$j = 1, \dots, n$  – число страниц КС. Для страниц сайта оценивается уровень прибыли и формируются матрицы  $D$  «страницы–интересы»

$$D_{np} = \begin{pmatrix} d_{11} & d_{12} & d_{1p} \\ d_{21} & d_{22} & d_{2p} \\ \vdots & \vdots & \vdots \\ d_{n1} & d_{n2} & d_{np} \end{pmatrix},$$

где  $i = 1, \dots, n$  – число страниц КС;

$j = 1, \dots, p$  – число интересов посетителей сайта, и матрицы  $E$  «интересы–MP» (здесь  $i = 1, \dots, p$  – число интересов посетителей сайта,  $j = 1, \dots, m$  – число MP)

$$E_{pm} = \begin{pmatrix} e_{11} & e_{12} & e_{1m} \\ e_{21} & e_{22} & e_{2m} \\ \vdots & \vdots & \vdots \\ e_{p1} & e_{p2} & e_{pm} \end{pmatrix}.$$

2. Для страниц КС экспертные оценки через правила логического вывода отображают в структуре ННС. В процессе адаптации ННС на обучающей выборке из подмножества интересов производится автоматическая коррекция системы нечетких правил, а также показателей прибыли и достоверности удовлетворения интересов посетителей сайта соответствующей страницей или MP-сайта.

3. Интегральные оценки эффективности получают умножением матриц достоверности  $B$  «MP–интересы» и  $C$  «интересы–страницы» для формирования матрицы  $A$  достоверности активации известных MP для удовлетворения интересов посетителей сайта – матрицу «MP–страницы». Аналогично, умножением матриц прибыли  $D$  и  $E$  формируют матрицу прибыли  $F$  «страницы–MP», отразив

жающую распределение потенциальной прибыли от реализации интересов посетителей сайта по МР и страницам КС

$$A_{mn} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix},$$

где  $i = 1, \dots, m$  – число МР;

$j = 1, \dots, n$  – число страниц КС,

$$F_{nm} = \begin{pmatrix} f_{11} & f_{12} & \cdots & f_{1m} \\ f_{21} & f_{22} & \cdots & f_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ f_{n1} & f_{n2} & \cdots & f_{nm} \end{pmatrix},$$

где  $i = 1, \dots, n$  – число страниц КС;

$j = 1, \dots, m$  – число МР.

Интегральные показатели значимости характеризуют активность использования отдельного МР либо страницы сайта, а также позволяют оценить прибыль в разрезе МР и страниц КС.

4. Операции над матрицами  $A$  и  $F$  позволяют обобщить в диагональных элементах итоговой матрицы как показатель достоверности активации МР, так и прибыли от их реализации. Умножением матриц  $A$  и  $F$  получают квадратную матрицу  $H$  достоверности потенциальной прибыли «МР–МР»

$$H_{mm} = \begin{pmatrix} h_{11} & h_{12} & \cdots & h_{1m} \\ h_{21} & h_{22} & \cdots & h_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ h_{m1} & h_{m2} & \cdots & h_{mm} \end{pmatrix},$$

где  $i = j = 1, \dots, m$  – число МР, а умножением матриц  $F$  и  $A$  – матрицу  $K$  достоверности потенциальной прибыли «страницы–страницы»

$$K_{nn} = \begin{pmatrix} k_{11} & k_{12} & \cdots & k_{1n} \\ k_{21} & k_{22} & \cdots & k_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ k_{n1} & k_{n2} & \cdots & k_{nn} \end{pmatrix},$$

где  $i = j = 1, \dots, n$  – число страниц корпоративного сайта.

Для матрицы  $H$  обобщающий показатель – модуль вектора из диагональных элементов  $p_i = h_{ii}$ ,  $i = j = 1, \dots, m$ , матрицы – вектор достоверности распределения прибыли по механизмам рекламы  $P_{1xm} = (p_1, p_2, \dots, p_m)$ , а для матрицы  $K$  – вектор из диагональных элементов  $s_i = k_{ii}$ ,  $i = j = 1, \dots, n$ , – вектор достоверности распределения прибыли по страницам КС  $S_{1xn} = (s_1, s_2, \dots, s_n)$ .

5. В качестве интегральных оценок эффективности рекламы на сайте в разрезе МР можно использовать рейтинговый показатель  $R_M$  – модуль вектора  $P_{1xm}$ , а в разрезе страниц КС – рейтинговый показатель  $R_S$  – модуль вектора  $S_{1xn}$

$$R_M = |P_{1xm}| = \sqrt{\sum_{i=1}^m p_i^2}, \quad i = 1, \dots, m,$$

$$R_S = |S_{1xn}| = \sqrt{\sum_{i=1}^n s_i^2}, \quad i = 1, \dots, n.$$

Использование интегральных показателей в модели адаптивного КС позволяет отслеживать динамику использования МР для удовлетворения интересов посетителей сайта за счет фиксации временного ряда из векторов  $P_{1xm}$  и  $S_{1xn}$  в моменты расширения классификаций (кластеризации) и активации МР.

Инструментальные средства «Сайт» – интерактивная программная среда, которая реализует систему показателей эффективности использования МР, которая в составе модели адаптивного КС используется для осуществления эволюционных механизмов развития и адаптации к изменению интересов посетителей сайта, а также определения путем моделирования изменения интересов посетителей сайта положения МР, включение которых в архитектуру сайта будет способствовать росту прибыли хозяйствующего субъекта. Рис. 1 иллюстрирует результаты расчета потенциальной прибыли хозяйствующего субъекта, а рис. 2 – распределение рейтинговых показателей по используемым МР и страницам КС.

Программные средства используют для анализа последствий изменения интересов посетителей и моделирования влияния местоположения механизмов рекламы в иерархии страниц сайта на достижение заданного уровня прибыли хозяйствующего субъекта.

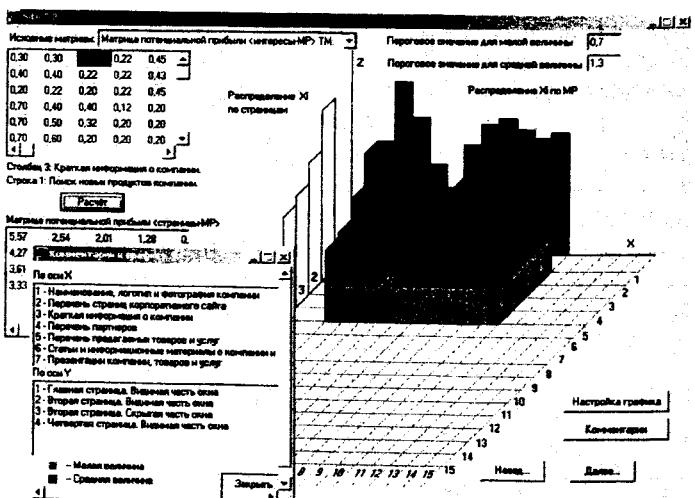


Рис. 1. Окно расчета потенциальной прибыли хозяйствующего субъекта при заданной архитектуре корпоративного сайта

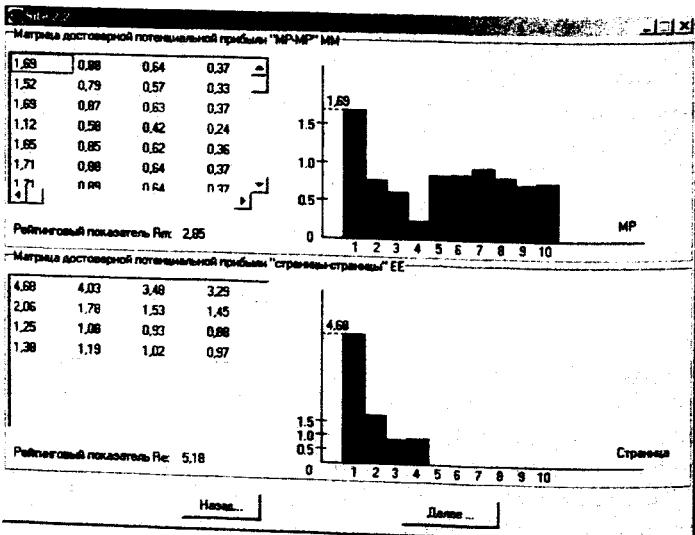


Рис. 2. Окно расчета рейтинговых показателей при заданной архитектуре корпоративного сайта

В результате моделирования динамики интересов посетителей сайта, целенаправленного или эволюционного изменения экспертизных оценок определяются механизмы рекламы, активация которых экономически оправдана.

### Литература

- Белов В. «Сарафанное радио» Интернета // PC WEEK/RE. 2004. № 25. С. 22, 31.
- Коберский Ю. Оптимизация сайта: проблема выбора // PC WEEK/RE. 2004. № 25. С. 23, 30.
- Неструк Г. Ф., Осовецкий Л. Г., Неструк Ф. Г. Адаптивная модель нейросетевых систем информационной безопасности // Перспективные информационные технологии и интеллектуальные системы. 2003. № 3.
- Гимаров В. А. Нейронечеткий идентификатор // Нейрокомпьютеры: разработка и применение. 2003. № 2.
- Неструк Ф. Г. и др. Разработка комплекса показателей для оценки информационных ресурсов и безопасности иерархических систем // IX Санкт-Петербургская междунар. конф. «Региональная информатика – 2004»: Тез. докл. СПб., 2004. С. 146.

## Раздел II

# ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ДАННЫХ

УДК 50.37.23

© И. В. Поночевная

Санкт-Петербургский государственный  
инженерно-экономический университет

### ТЕНДЕНЦИИ РАЗВИТИЯ СОВРЕМЕННЫХ ЗАЩИТНЫХ ТЕХНОЛОГИЙ

В настоящее время защитные технологии по уровню развития не опережают информационные технологии, а всего лишь следуют за ними. Например, можно ли представить себе межсетевой экран в системе, состоящей из несвязанных между собой персональных компьютеров.

Ни одна технологическая новинка не требует обязательной разработки адекватной защиты, так как подобные работы ведутся только в случае их финансовой целесообразности. Отсюда следует, что любая серьезная защитная технология появляется только в ответ на какую-либо технологическую новинку.

Следует также отметить, что на развитие защитных технологий влияет деятельность хакеров или кракеров. И это понятно, поскольку даже для самой востребованной технологии не будут разрабатываться защитные меры, пока эта технология не подвергнется атакам со стороны нарушителей.

Например, технология беспроводных сетей в свое время не обладала серьезной защитой, а так как действия нарушителей показали всю уязвимость беспроводных сетей, то сразу стали появляться механизмы ее защиты от них.

В зависимости от вида работы применяются различные защитные технологии. Так, на выбор защитной технологии важное влия-

ние оказывает размер того объединения персональных компьютеров, которое принято называть компьютерной сетью, так как масштаб компьютерной сети диктует и свои правила игры. Для одного персонального компьютера, подключенного к глобальной сети Интернет, не нужны системы контроля утечки конфиденциальной информации, а сетям крупных и средних масштабов, например предприятия или фирмы, без таких средств защиты вообще не обойтись.

Все сказанное позволяет сделать вывод, что выбор защитных технологий зависит от таких факторов, как известность и распространенность, а также от вида хакерских атак и от масштаба компьютерной сети.

На сегодняшний день распространены следующие технологии защиты.

**Антивирусная защита.** Сегодня в вирусных хит-парадах лидируют такие классы вредоносных программ, как троянцы и черви, которые распространяются не от файла к файлу, а от компьютера к компьютеру, нанося ущерб, который измеряется десятками миллиардов долларов.

**Межсетевые экраны.** В связи с масштабным развитием компьютерных сетей возникла задача их защиты от нападения хакеров. Она была решена с помощью межсетевых экранов. Эта технология активно развивается и в настоящее время. Яркими представителями среди российских разработок таких средств являются «Эльвис+» («Застава»), «Инфосистемы Джет» («Ангара» и «Z-2»).

**Авторизация и разграничение доступа.** По статистике, 51–83% всех компьютерных инцидентов на предприятиях происходят по вине их собственных сотрудников, где никакие межсетевые экраны не помогут.

Поэтому возникла необходимость в системах авторизации и разграничения доступа. Эти системы определяют, кому, к какому ресурсу и в какое время можно получить доступ.

Эти системы базируются на классических моделях разграничения доступа (Кларка–Вильсона), разработанных в 70–80 гг.

Одним из основных направлений данной системы является аутентификация, которая позволяет сопоставить вводимые пользователем пароль и имя с информацией, хранящейся в базе системы за-

щиты. При совпадении вводимых данных разрешается доступ к соответствующим ресурсам (информации).

*Системы обнаружения и предотвращения атак.* Несмотря на наличие межсетевых экранов антивирусной защиты, некоторые атаки все равно проникают сквозь защитные преграды. Эти атаки получили название гибридных (например, My Doom, Code Red, Nimda, SQL Slammer, Blaster).

Для защиты от этих эпидемий предназначена технология обнаружения и предотвращения атак. История этой технологии началась в 1980 г., когда Джеймс Андерсон предложил использовать для обнаружения несанкционированных атак журнал регистрации событий.

Со временем ситуация несколько изменилась, так как нужно было не только обнаруживать атаки, но и блокировать их до того момента, как они достигнут своей цели.

Далее появились персональные системы, защищающие рабочие станции и мобильные компьютеры, что привело к слиянию персональных межсетевых экранов, систем обнаружения атак и антивирусов, и это стало почти идеальным решением для защиты компьютера.

*Сканеры безопасности.* Сканеры безопасности предназначены для устранения дыр, используемых атаками, т. е. надо обнаружить все уязвимости и устраниить их до того, как их обнаружат злоумышленники.

Этой цели служат сканеры безопасности (их также называют системами анализа защищенности), работающие как на уровне сети, так и на уровне отдельного узла. Первым сканером, ищущим дыры в ОС Unix, стал Cops, разработанный Юджином Спаффордом в 1991 г., а первым сетевым сканером – Internet Scanner, созданный Кристофером Клаусом в 1993 г.

В настоящее время происходит постепенная интеграция систем обнаружения атак и сканеров безопасности, что позволяет практически полностью исключить из процесса обнаружения и блокирования атаки со стороны нарушителя.

Эта интеграция заключается в следующем – сканер, обнаруживший дыру, дает команду сенсору обнаружения атак на отслеживание соответствующей атаки, и наоборот, сканер, обнаруживший атаку, дает команду на сканирование атакуемого узла.

Ярким представителем среди российских разработок этих средств является Positive Technologies, которая выпустила первый российский сканер безопасности – Xspider.

Другие защитные технологии, хотя и очень перспективные, но пока что мало распространенные в корпоративных сетях – системы корреляции событий безопасности, системы единого управления разнородными средствами защиты, PKI (Public Key Infrastructure – инфраструктура открытых сетей).

Данные технологии востребованы только в случае эффективного применения и межсетевых экранов, и антивирусов, и систем разграничения доступа. Лишь единицы из тысяч российских компаний дорошли до использования технологий корреляции событий безопасности, единого управления разнородными средствами защиты, PKI.

Таким образом, можно сделать вывод, что по уровню зрелости самые передовые защитные технологии на сегодняшний момент – это межсетевые экраны, антивирусы.

Развивающиеся защитные технологии – это контроль доступа, обнаружение и предотвращение атак.

УДК 50.37.23

© О. Д. Мердина

Санкт-Петербургский государственный  
инженерно-экономический университет

## ПОДХОД К АНАЛИЗУ ЗАЩИЩЕННОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

С появлением и развитием открытых компьютерных сетей количество уязвимостей сетевых операционных систем и прикладных программ и возможных атак на них постоянно растет. Уязвимыми являются все информационные объекты:

- сама сеть, т. е. сетевые протоколы (TCP/IP, IPX/SPX, NetBIOS/SMB) и устройства (маршрутизаторы, коммутаторы), образующие сеть;
- операционные системы (Windows NT, Unix, Netware);
- базы данных (Oracle, Sybase, MS SQL Server) и приложения (SAP, почтовые и Web-сервера и т. д.).

Причинами невозможности своевременного устранения причин и последствий нарушения информационной безопасности являются:

- отсутствие у организаций достаточного времени и средств для решения проблем, которых они не могут физически видеть и касаться;
- отсутствие поддержки у руководства для принятия решения, которое напрямую не увеличивает эффективность работы организации или не приносит существенной прибыли;
- особенности совершения преступлений в киберпространстве.

Можно выделить следующие основные подходы к созданию систем информационной безопасности<sup>1</sup>:

на основе частичного решения проблемы:

Безопасность = Традиционные средства защиты;

создание надежной системы сетевой безопасности:

Безопасность = Политика безопасности +  
+ Традиционные средства защиты + Анализ риска + Реализация контрмер;

на основе использования модели адаптивного управления безопасностью

Безопасность = Анализ риска + Политика безопасности +  
+ Традиционные средства защиты + Реализация контрмер +  
+ Аудит + Мониторинг + Реагирование.

Снижение проблем в информационной безопасности требует адаптивного, высокочувствительного к изменениям, работающего в реальном режиме времени механизма. Адаптивная безопасность – именно такой подход, который позволяет контролировать, обнаруживать и реагировать в реальном режиме времени на риски безопасности, используя правильно спроектированные и хорошо управляемые процессы и средства.

Yankee Group в июне 1998 г. опубликовала отчет, в котором адаптивная безопасность описывается как процесс, содержащий:

- технологию анализа защищенности или поиска уязвимостей;
- технологию обнаружения атак;

<sup>1</sup> Лукацкий А. В. Адаптивная безопасность сети // Компьютер-Пресс. 1999. № 8.

- адаптивный компонент, который включает в себя и расширяет две первые технологии;
- управляющий компонент.

Анализ защищенности – это поиск уязвимых мест в сети. Технологии анализа защищенности исследуют сеть и ищут «слабые» места в ней, обобщают эти сведения и печатают по ним отчет. Если система, реализующая эту технологию, содержит и адаптивный компонент, то вместо «ручного» устранения найденной уязвимости оно будет осуществляться автоматически. К проблемам, идентифицируемым технологией анализа защищенности, относятся:

- «люки» в системах (back door) и программы типа «троянский конь»;
- слабые пароли;
- восприимчивость к проникновению из незащищенных систем и атакам типа «отказ в обслуживании»;
- отсутствие необходимых обновлений (patch, hotfix) операционных систем;
- неправильную настройку межсетевых экранов, Web-серверов и баз данных.

Технологии анализа защищенности являются действенным методом, позволяющим реализовать политику сетевой безопасности прежде, чем осуществляется попытка ее нарушения снаружи или изнутри организации.

Обнаружение атак является процессом оценки подозрительных действий, которые происходят в корпоративной сети. Обнаружение атак реализуется посредством анализа или журналов регистрации операционной системы и приложения, или сетевого трафика в реальном времени. Компоненты обнаружения атак, размещенные на узлах или сегментах сети, оценивают различные действия, в том числе и использующие известные уязвимости.

Адаптивный компонент отвечает за модификацию процесса анализа защищенности, предоставляя ему самую последнюю информацию о новых уязвимостях. Он также модифицирует компонент обнаружения атак, дополняя его последней информацией об атаках. Пример адаптивного компонента – механизм обновления баз данных антивирусных программ для обнаружения новых вирусов.

Управляющий компонент должен быть способен к генерации отчетов и анализу тенденций, связанных с усилиями формирования системы защиты организации.

Адаптация данных может заключаться в различных формах реагирования, которые могут включать:

- посылку уведомлений системам сетевого управления по протоколу SNMP, по электронной почте или на пейджер администратору;
- автоматическое завершение сессии с атакующим узлом или пользователем, реконфигурация межсетевых экранов или иных сетевых устройств (например, маршрутизаторов);
- выработку рекомендаций администратору, позволяющих своевременно устранить обнаруженные уязвимости в сетях, приложениях или иных компонентах информационной системы организации.

Использование модели адаптивной безопасности сети позволяет контролировать практически все угрозы и своевременно реагировать на них высокоеффективным способом, способствующим не только устраниению уязвимостей, которые могут привести к реализации угрозы, но и проанализировать условия, приводящие к появлению уязвимостей. Эта модель также позволяет уменьшить злоупотребления в сети, повысить осведомленность пользователей, администраторов и руководство компаний о событиях безопасности в сети.

Средства анализа защищенности, называемые сканерами безопасности, предназначены для автоматизации процесса поиска уязвимостей. Использование этих средств поможет определить уязвимости на узлах корпоративной сети и устраниить их до тех пор, пока ими воспользуются злоумышленники.

Функционировать такие средства могут на сетевом уровне, уровне операционной системы (ОС) и уровне приложения. Наибольшее распространение получили средства анализа защищенности сетевых сервисов и протоколов. Связано это, в первую очередь, с универсальностью используемых протоколов. Изученность и повсеместное использование таких протоколов, как IP, TCP, HTTP, FTP, SMTP и других, позволяют с высокой степенью эффективности проверять защищенность информационной системы, работающей в сетевом окружении. Вторыми по распространенности оказались средства анализа защищенности операционных систем. Связано это также с универсальностью и распространенностью некоторых операционных систем (например, UNIX и Windows NT). Однако из-за того, что каждый производитель вносит в операционную

систему свои изменения (ярким примером является множество разновидностей ОС UNIX), средства анализа защищенности ОС анализируют в первую очередь параметры, характерные для всего семейства одной ОС. И лишь для некоторых систем анализируются специфичные для нее параметры. Средства анализа защищенности приложений на сегодняшний день не так много, как хотелось бы. Такие средства пока существуют только для широко распространенных прикладных систем, типа Web-браузеры (Netscape Navigator, Microsoft Internet Explorer), СУБД (Microsoft SQL Server, Oracle) и т. п.

Применяя средства анализа защищенности, можно быстро определить все узлы корпоративной сети, доступные в момент проведения тестирования, выявить все используемые в ней сервисы и протоколы, их настройки и возможности для несанкционированного воздействия (как изнутри корпоративной сети, так и снаружи). По результатам сканирования эти средства вырабатывают рекомендации и пошаговые меры, позволяющие устранить выявленные недостатки.

Для крупных организаций, сети которых насчитывают десятки компьютеров, функционирующих под управлением различных операционных систем, на первое место выступает задача управления всем многообразием защитных механизмов в этих ОС. Поэтому администраторам служб автоматизации и безопасности требуются специализированные средства, позволяющие следить за всем многообразием программного и аппаратного обеспечения в организации, за постоянной текучестью кадров, за постоянно расширяющимся списком уязвимостей.

Существуют два подхода к решению этой проблемы.

Первый заключается в интеграции механизмов управления средствами защиты в средства сетевого или системного управления. По такому пути пошли компании Hewlett Packard, Computer Associates, PLATINUM Technology, Tivoli Systems. Системы управления этих компаний поддерживают традиционные действия и услуги: управление учетными записями пользователей, управление ресурсами и событиями, производительность, маршрутизацию и т. д. Однако у данных средств своя область применения – они ориентированы в первую очередь на управление сетью или информационными системами.

Второй подход заключается в использовании средств, предназначенных только для решения одной задачи – управление безопасностью. Например, Open Security Manager (OSM) от Check Point Software Technologies позволяет централизованно управлять корпоративной политикой безопасности и инсталлировать ее на сетевые устройства по всей компании. Продукт OSM является одной из основных компонент технологии OPSEC (Open Platform for Secure Enterprise Connectivity), разработанной компанией Check Point, он создает интерфейс для управления устройствами сетевой безопасности различных производителей (например, Cisco, Bay, 3Com).

Сегодня администратору безопасности уже недостаточно иметь средства управления учетными записями и ресурсами, ему необходим механизм прослеживания тенденций и прогнозирования событий в области безопасности. Несмотря на то, что такие механизмы существуют в системах сетевого и системного мониторинга, в области безопасности они пока не нашли широкого распространения.

УДК 50.37.23

© Д. В. Тихонов, Е. В. Стельмашонок

Санкт-Петербургский государственный  
инженерно-экономический университет

## ИСПОЛЬЗОВАНИЕ ОБЪЕКТНО-ОРИЕНТИРОВАННОГО ПОДХОДА ПРИ РЕШЕНИИ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Современный уровень развития компьютерных и информационных технологий характеризуется возрастающей сложностью не только отдельных физических и программных компонентов, но и лежащих в основе этих технологий концепций и идей. Поэтому построение современных информационных систем основано на использовании объектно-ориентированного подхода, чего нельзя утверждать, если речь идет о системах информационной безопасности. Объектно-ориентированный подход является основой современной технологии программирования, испытанной методом борьбы со сложностью систем. Так как системы информационной безо-

пасности являются сложными системами, то целесообразно распространить объектно-ориентированный подход и на них<sup>1</sup>.

Рассмотрим возможность применения такого распространенного CASE-средства, как унифицированный язык моделирования UML (Unified Modeling Language) для решения одной из задач информационной безопасности – проектирование системы шифрования данных.

Язык UML предназначен для описания, визуализации и документирования объектно-ориентированных систем и бизнес-процессов с ориентацией на их последующую реализацию в виде программного обеспечения. Наиболее востребованным UML оказывается при проектировании больших и сложных систем.

Применение UML заключается в построении диаграмм, каждая из которых уточняет и расширяет ранее построенные диаграммы. Визуальное моделирование можно представить как некоторый процесс спуска от наиболее общей и концептуальной модели к физической программной модели. Чаще всего выделяют диаграммы:

- вариантов использования;
- классов;
- состояний;
- последовательности;
- деятельности;
- кооперации и др.

Рассмотрим применение диаграммы вариантов использования и диаграммы классов на примере моделирования системы шифрования данных на основе метода укладки ранца.

Процесс зашифрования начинается с генерации сверхвзрастающей последовательности (текущий элемент больше суммы всех предыдущих), являющейся закрытым ключом. Затем на его основе генерируется открытый ключ, используемый для зашифрования. Генерация ключей осуществляется в соответствии с формулами:

$$c_i = \sum_{j=1}^{i-1} c_j + d,$$

$$o_i = c_i \cdot M \bmod N,$$

<sup>1</sup> Галатенко В. А. Основы информационной безопасности. М.: ИНТУИТ.РУ «Интернет-университет информационных технологий», 2003.

где  $c_i$  – элемент закрытого ключа;  
 $o_i$  – элемент открытого ключа  $d$ ;  
 $M, N$  – коэффициенты;  
 $i \in [1; 8]$ .

Зашифровка идет следующим образом:

- получаем ASCII код шифруемого символа;
- переводим его в двоичное число;
- получаем так называемый «ранец», вычисляемый по формуле:

$$S = \sum_{i=1}^8 g_i \cdot o_i,$$

где  $g_i$  – цифра полученного двоичного числа.

Процесс построения программы начинается с построения диаграммы вариантов использования, которая описывает функциональное назначение системы или то, что система будет делать в процессе своего функционирования. Данная диаграмма является исходным концептуальным представлением или концептуальной моделью системы в процессе ее проектирования и разработки. Разработка диаграммы преследует следующие цели:

- определить общие границы и контекст моделируемой предметной области на начальных этапах проектирования системы;
- сформулировать общие требования к функциональному поведению проектируемой системы;
- разработать исходную концептуальную модель системы для ее последующей детализации в форме физических и логических моделей;
- подготовить исходную документацию для взаимодействия разработчиков с ее заказчиками и пользователями.

Проектируемая система представляется в виде множества сущностей и актеров, взаимодействующих с системой с помощью так называемых вариантов использования. При этом актером называется любая сущность, взаимодействующая с системой извне. Вариант использования служит для описания сервисов, которые система предоставляет актеру. Другими словами, каждый вариант использования определяет некоторый набор действий, совершаемых системой при диалоге с актерами. Между компонентами диаграммы могут быть различные отношения. Остановимся на двух:

– отношения ассоциации – показывают семантические особенности взаимодействия актера и варианта использования;

– отношения обобщения – вариант использования  $A$  может быть обобщен до варианта использования  $B$ .

Проанализировав задачу, мы получим диаграмму вариантов использования, представленную на рис. 1.

Как видно из рис. 1, в диаграмме присутствует основной вариант использования «Зашифровать данные», который включает три других варианта использования: «Сгенерировать ключ», «Выдать ключ пользователю», «Наложить ключ на данные». С главным вариантом использования ассоциированы два актера «Шифратор» и «Данные». Отношение обобщения показывает, что существует два наследуемых актера «Программа шифрования данных» и «Файлы» соответственно.

Char ID: CryptUseCaseDiagram  
 Char Name: CryptSystemUseCaseDiagram  
 Char Type: UML Use Case Diagram

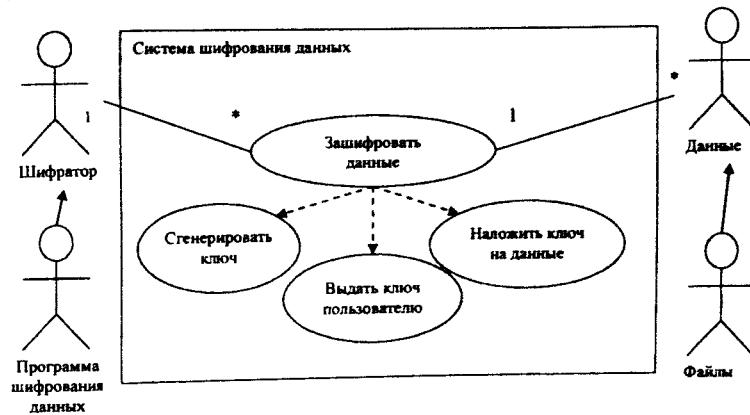


Рис. 1. Диаграмма вариантов использования

Диаграмма классов служит для представления статической структуры модели системы в терминологии классов объектно-ориентированного программирования. Она может отражать, в частности,

различные взаимосвязи между сущностями предметной области, такими как объекты и подсистемы, а также описывает их внутреннюю структуру и типы отношений. Диаграмма классов представляет собой некоторый граф, вершинами которого являются классы, связанные различными типами структурных отношений.

Класс в языке UML служит для обозначения множества объектов, которые обладают одинаковой структурой, поведением и отношением с объектами из других классов. Класс обязательно должен содержать имя, а также может содержать перечень атрибутов и операций. Между классами существуют следующие отношения:

- отношение зависимости;
- отношение ассоциации;
- отношение обобщения;
- отношение реализации.

Построение данной диаграммы имеет большое значение для программистов, поскольку на основе данной диаграммы можно генерировать программный код на нужном языке программирования, что будет продемонстрировано далее. Удобство этих диаграмм заключается в наглядности построения системы. Программисту куда легче писать код в уже созданной иерархии классов, нежели разрабатывать ее самостоятельно. Особенно все преимущества такого подхода проявляются в проектировании сложных систем с большим количеством классов и сложной иерархией отношений между ними. К таким системам, несомненно, относятся системы информационной безопасности ввиду их повышенной сложности.

Учитывая все вышесказанное, можно построить для нашей системы диаграмму классов, как показано на рис. 2.

В данной диаграмме представлены три класса. В верхней области указано имя класса. В средней – перечень атрибутов, а в нижней – перечень операций. Знакок «+» перед именем класса или операцией означает квантор видимости – Public. А «–» означает – Private. Пунктирная стрелочка показывает отношение зависимости. В нашем случае источником зависимости выступает класс Crypt, а клиентами зависимости классы KeyGen и DataCrypt.

После построения диаграммы классов генерируется программный код (например, на языке Visual Basic, Visual C++). После генерации кода программисту остается только произвести наполнение функций кодом, в результате чего мы получим готовый программный продукт.

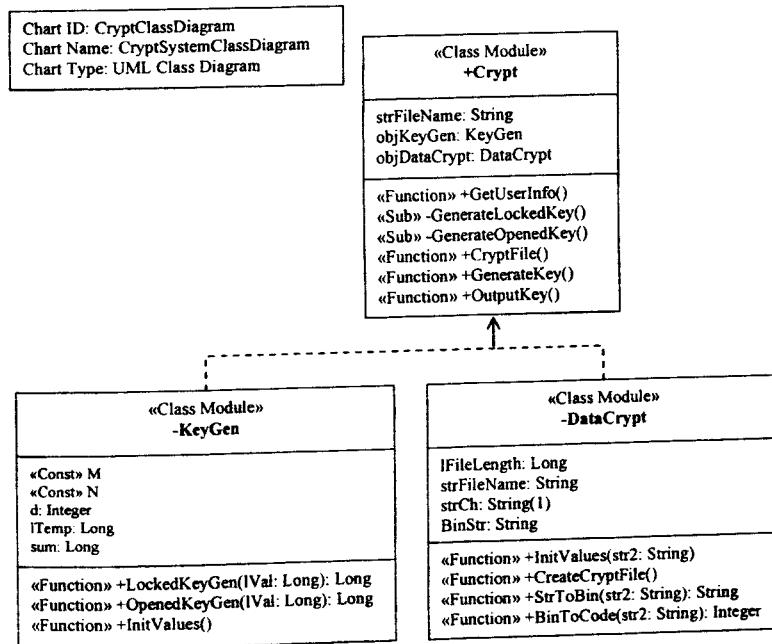


Рис. 2. Диаграмма классов

УДК 50.37.23

© И. В. Поночевная

Санкт-Петербургский государственный  
инженерно-экономический университет

## ТЕСТИРОВАНИЕ КАК ПРОЦЕСС СОВРЕМЕННОЙ ИНФОРМАЦИОННОЙ ТЕХНОЛОГИИ ПРИ РАЗРАБОТКЕ СИСТЕМЫ ЗАЩИТЫ

На сегодняшний день тестирование – это один из самых важных этапов работы и проверки качества разработанной системы защиты. Так сложилось, что о качестве системы в большинстве случаев создает представление только его эксплуатация, а тестирование –

это один из важнейших этапов проверки на предмет обнаружения ошибок в системе.

Для оценки качества системы применяется целый комплекс мер, так как заказчик вправе требовать от разработчика гарантий ее работы. Для проведения тестирования необходим объект тестирования – в данном случае система и эталон, с которым этот объект сравнивается. Так как тестирование системы проводится на соответствие заранее определенным требованиям – по функциональности, производительности и безопасности, то можно сделать вывод, что объект тестирования – сложный процесс, и необходим системный подход к его организации и проведению:

- тестирование частей системы (модулей, компонентов) с целью проверки правильности реализации алгоритмов, что выполняется разработчиками;
- функциональное тестирование подсистем в целом с целью проверки степени выполнения функциональных требований, которое рекомендуется проводить независимой группой;
- нагрузочное тестирование (в том числе стрессовое) для выявления характеристик функционирования системы при изменении нагрузки (интенсивности обращений к нему, наполнения базы данных).

Система – это сложный объект, который меняется по составу и проверяемым свойствам на разных стадиях своей разработки. Важно понимать, что если разработчик и заказчик не сформулировали свои требования к системе еще до начала ее разработки, то ее нельзя будет проверить, поскольку объект есть, а эталона нет. А это говорит о том, что одно из главных правил для разработчика системы – это работа с заказчиком, так как обе стороны будут лучше понимать, что происходит при создании системы в каждый конкретный момент и быстрее находить совместные решения.

Таким образом, требования к системе следует определять в самом начале разработки с заказчиком, так как у заказчика и разработчика должна быть возможность сравнить текущее функционирование системы с ее эталонным (ожидаемым) поведением.

Для этого рекомендуется использовать план тестирования, разработанный в соответствии с требованиями Международного стандарта IEEE 829-1983 (Standard for Software Test Documentation).

Если не забывать, что тестирование – это процесс обнаружения ошибок, то стоит потребовать от разработчика, чтобы он систематически силами специальных независимых групп проводил так называемые «структурные просмотры» проектных материалов и аудит исходных кодов программ.

В этом случае заказчик может быть уверен, что качество разрабатываемой системы контролируется и обеспечивается в ходе разработки.

Желательно, чтобы на этапах сборки, комплексной отладки и опытной эксплуатации разработчик фиксировал интенсивность обнаружения ошибок, тогда по характеру изменения этой интенсивности можно будет судить об изменении качества системы. Также необходимо проведение комплекса испытаний системы на соответствие требованиям технического задания или других нормативных документов, на возможность эффективно работать с системой на основе использования программной документации. Именно на это направлены так называемая модель технологической зрелости СММ (Capability Maturity Model) и стандарт ISO 15504.

Также для проверки системы надо применять разные стратегии, позволяющие добиваться максимального результата при существующих ограничениях на ресурсы тестирования, при этом тестирования позволяет заранее определить, что нужно подготовить для проведения тестирования.

План тестирования определяется Международным стандартом IEEE 829-1983. В нем должны быть предусмотрены как минимум три раздела:

- что будет тестироваться (тестовые требования, тестовые варианты);
- какими методами и насколько подробно будет тестироваться система;

– план-график работ и требуемые ресурсы (персонал, техника).

Дополнительно описываются критерии удачного и неудачного завершения тестов, критерии окончания тестирования, риски, не-предвиденные ситуации и т. д. Следовательно, тестированием важно заниматься не только постоянно, но и систематично, поскольку тестирование системы дает гарантию эффективной работы системы, а также ее работоспособности для конечного пользователя.

## КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ФИРМЫ «АНКАД»

Фирма «Анкад» известна на отечественном рынке как разработчик аппаратно-программных криптографических средств защиты информации под торговыми марками КРИПТОН/Crypton. Наряду с производством и поставкой устройств серии «КРИПТОН», «Анкад» предлагает готовые решения: от программ абонентского и архивного шифрования и электронной подписи до аппаратно-программных систем защиты отдельных рабочих мест и систем в целом.

В состав средств криптографической защиты информации фирмы «Анкад» включены:

- устройства криптографической защиты данных;
- устройства серии «КРИПТОН», интерфейсы, программные эмуляторы;
- программные средства защиты информации;
- программы серии Crypton для:
  - защиты данных на жестком диске компьютера методом прозрачного и архивного шифрования данных;
  - защиты информации при организации электронного документооборота методом ЭЦП, абонентского шифрования, комплексной защиты(шифрование + ЭЦП + специализированное архивирование);
  - системы защиты информации от несанкционированного доступа (НСД);
  - программно-аппаратные системы ограничения доступа к компьютеру и его ресурсам. Области применения:
    - ограничение доступа к ПК (рабочей станции);
    - полная защита ресурсов ПК;
    - средства защиты сетей;
    - продукты для построения корпоративных виртуальных частных сетей (VPN).

*Устройства серии «КРИПТОН» и программные эмуляторы.*  
Устройства криптографической защиты данных (УКЗД) семейства «КРИПТОН» фирмы «Анкад» аттестованы в ФАПСИ, широко применяются в разнообразных защищенных системах и сетях передачи данных и имеют сертификаты соответствия ФАПСИ самостоительно и в составе целого ряда АРМ абонентских пунктов при организации шифровальной связи I класса для защиты информации, содержащей сведения, составляющие государственную тайну. В устройствах реализуется российский алгоритм шифрования ГОСТ 28147-89.

В настоящее время «Анкад» предлагает следующие устройства криптографической защиты информации (УКЗД) серии «КРИПТОН»:

- КРИПТОН-4 (имеет сертификат ФАПСИ от 20.08.96 № СФ/024-0126);
  - КРИПТОН-4К/8;
  - КРИПТОН-4К/16 (имеет сертификаты ФАПСИ от 30.06.99 № СФ/120-0278, -0279, -0280);
  - КРИПТОН-4/PCI.

Ведется разработка УКЗД следующего поколения с увеличенным быстродействием (для шины PCI) и развитием дополнительных пользовательских возможностей:

- КРИПТОН-7/PCI;
- КРИПТОН-8/PCI.

Перечисленные УКЗД серии «КРИПТОН» обладают следующими общими функциональными свойствами:

- наличие загружаемого до операционной системы мастер-ключа (главного ключа), что исключает его перехват;
- выполнение криптографических функций внутри платы, что исключает их подмену или искажение;
- наличие аппаратного датчика случайных чисел;
- достаточно высокая скорость шифрования от 200 Кбайт/с (КРИПТОН-4) до 1Мбайт/с (КРИПТОН-4К/16).

Средства серии «КРИПТОН» независимо от операционной среды обеспечивают защиту ключей шифрования и электронной цифровой подписи (ЭЦП) и неизменность алгоритма шифрования и ЭЦП. Все ключи, используемые в системе, могут шифроваться на мастер-ключе и храниться на внешнем носителе в зашифрованном виде. Они расшифровываются только внутри платы. В качестве

ключевых носителей используются дискеты, микропроцессорные электронные карточки (смарт-карты).

Для систем защиты информации от несанкционированного доступа разработана специальная плата (выполняющая при необходимости программное шифрование по ГОСТ 28147-89, аппаратную генерацию случайных чисел, загрузку ключей с дискеты и электронной карточки): «КРИПТОН-НСД».

Для встраивания в конечные системы пользователя УКЗД имеют два возможных уровня интерфейса: драйвера под операционные системы Windows 95, 98 и NT 4.0, Unix (Solaris x.86).

**УКЗД «КРИПТОН».** Как драйвера, так и Библиотеки Crypton API поставляются фирмой «Анкад» в качестве прикладного программного обеспечения для средств КРИПТОН/Crypton. Кроме того, большинство программ фирмы «АНКАД», работающих с УКЗД «КРИПТОН», предоставляют интерфейс командной строки.

Программные эмуляторы функций шифрования УКЗД серии «КРИПТОН» в DOS, Windows'95/NT 4.0 позволяют осуществлять криптографическую защиту информации по алгоритму ГОСТ 28147-89, совместимы с УКЗД серии «КРИПТОН» и используют общее программное обеспечение:

- CryptonLITE для DOS, которое поставляется фирмой «Анкад» в составе комплекса программ CryptonLITE (для MS-DOS или отдельно);
- Crypton Emulator для Windows'95/NT 4.0 поставляется фирмой «Анкад» в составе комплекса программ CryptonLITE (для Windows'95(98)/NT 4.0 или отдельно).

Драйвер-эмулатор Crypton Emulator позволяет заменить драйвер УКЗД «КРИПТОН» без изменения при этом программ, использующих программный интерфейс Crypton API.

Использование эмуляторов рекомендуется в случаях, когда конструктивные особенности компьютера не позволяют использовать аппаратные УКЗД серии «КРИПТОН» (например, в notebook).

### Программные средства защиты информации

**Защита данных, хранящихся на жестком диске.** Используется метод прозрачного шифрования данных. Приложение обеспечивает защиту информации от угроз изъятия жесткого диска с конфиденциальными данными из ПК, несанкционированного доступа к ПК-

серверу и копирования данных, кражи ПК или notebook. Дополнительным удобством является «невидимое» для пользователя автоматическое зашифрование и расшифрование файлов заданной области жесткого диска (выделяемой в логический диск) без изменения привычного порядка работы с этими файлами.

#### Решения:

- для MS-DOS: система «КРИПТОН-ВЕТО» (программа Crypton Access). Комплекс программ Crypton Access является основным компонентом программно-аппаратной системы защиты информации от несанкционированного доступа «КРИПТОН-ВЕТО», обеспечивая разграничение доступа к информации и ее «прозрачное» шифрование;

- для Windows: КРИПТОН®Сигма для Windows'95(98)/NT 4.0. Программа прозрачного шифрования диска использует в работе УКЗД серии «КРИПТОН» или его программный эмулятор Crypton Emulator.

**Система защиты конфиденциальной информации.** Secret Disk Pro обеспечивает прозрачное шифрование логических дисков. Защита данных производится с помощью криптографического алгоритма ГОСТ 28147-89, реализованного в криптомульте Crypton методом архивного шифрования данных.

Приложение обеспечивает защиту информации, находящейся на жестком диске ПК и не предназначено для обмена в какой-либо компьютерной сети, от несанкционированного доступа и копирования. Шифрование на уровне файлов производится под непосредственным управлением пользователя.

#### Решения:

- для MS-DOS

Crypton Tools: программа шифрования и генерации ключей, поставляется фирмой «Анкад» в качестве прикладного программного обеспечения для средств КРИПТОН/Crypton;

Crypton Soft: программа шифрования, электронной цифровой подписи и работы с ключами, используется в работе УКЗД «КРИПТОН» или программный эмулятор CryptonLITE;

- для Windows:

CryptonLITE.КРИПТОН®Шифрование для Windows'95(98)/NT 4.0: пакет предназначен для защиты электронных документов (файлов) от несанкционированного доступа путем их шифрования.

рования. Пакет поставляется фирмой «АНКАД» в качестве прикладного программного обеспечения для средств КРИПТОН/Crypton.

Кроме того, фирма «Анкад» занимается разработкой аппаратно-программных криптографических средств защиты информации:

- для организации электронного документооборота;
- защиты сетей;
- для построения виртуальных частных сетей – ВЧС (или VPN – Virtual Privat Network).

УДК 50.37.23

© М. М. Мгебришвили

Санкт-Петербургский государственный  
инженерно-экономический университет

## МЕТОД ОСТАТОЧНОГО КОДИРОВАНИЯ КАК МЕТОД КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Защита информации может решаться разными методами, но наибольшей надежностью и эффективностью обладают системы и средства, построенные на базе криптографических методов. В случае использования иных методов большую сложность составляет доказательство достаточности реализованных мер и обоснование надежности системы защиты от несанкционированного доступа.

Необходимо иметь в виду, что подлежащие защите сведения могут быть получены «противником» не только за счет проникновения в ЭВМ, которые с достаточной степенью надежности могут быть предотвращены, но и за счет побочных электромагнитных излучений и наводок на цепи питания и заземления ЭВМ, а также проникновения в каналы связи. Все без исключения электронные устройства, блоки и узлы ЭВМ в той или иной мере излучают побочные сигналы, причем они могут быть достаточно мощными и распространяться на расстояния от нескольких метров до нескольких километров. Наибольшую опасность представляет получение «противником» информации о ключах. Восстановив ключ, можно предпринять успешные действия по завладению зашифрованными данными, которые, как правило, обергаются менее серьезно, чем

соответствующая открытая информация. С этой точки зрения выгодно отличаются именно аппаратные и программно-аппаратные средства защиты от несанкционированного доступа, для которых побочные сигналы о ключевой информации существенно ниже, чем для чисто программных реализаций.

Одним из методов криптографической защиты информации является применение непозиционной системы остаточных классов (СОК), которая нашла воплощение во многих оригинальных разработках.

Преимущества непозиционной системы остаточных классов успешно проявились как в цифровых, так и в аналоговых вычислительных машинах. Необходимо отметить, что эта система применяется как для кодирования и защиты информации, так и в вычислениях с большими числами.

В основе непозиционной системы счисления в остаточных классах (СОК) лежит понятие сравнимости чисел по модулю  $m$ . Произвольное число  $N$  можно представить в виде:

$$N = n \cdot m + \alpha, \text{ т. е. } N \equiv \alpha \pmod{m},$$

где  $n$  – число, показывающее, сколько раз  $m$  укладывается в числе  $N$ , а  $\alpha$  – остаток, причем  $0 \leq \alpha \leq m - 1$ .

Точность вычислений связана с модулем  $m$  величиной  $1/m$ . Для высокоточных вычислений количество представимых в системе чисел должно быть увеличено, т. е. необходимо брать несколько модулей  $m$ , произведение которых определяет суммарный числовой диапазон и точность вычислений  $1/M$ .

Тогда число  $N$  из диапазона  $0 - (M - 1)$  представляется совокупностью остатков  $\{\alpha\}$  по совокупности модулей  $\{m\}$ , причем все модули должны быть взаимно простыми числами.

При выполнении операций сложения и умножения, называемых модульными операциями, полностью отсутствуют взаимосвязи между модульными каналами. Поэтому проблема переносов, свойственная позиционному представлению информации, в этой системе отсутствует.

Кроме того, системы остаточных классов позволяют получить безошибочные вычисления, которые основаны на представлении чисел в виде остатков их деления на заданные простые числа – мономы системы и выполнении целочисленных арифметических опе-

раций над ними. Окончательный результат вычислений в системе остаточных классов преобразуется в позиционную систему счисления (ПСС) и представляется в виде пары чисел – числителя и знаменателя несократимой дроби Фарея. Преимуществом безошибочных вычислений в системе остаточных классов является возможность параллельной обработки чисел по нескольким модулям. Это обеспечивает значительное увеличение быстродействия по сравнению с последовательной обработкой.

УДК 50.37.23

© И. С. Авдонин

Санкт-Петербургский государственный  
инженерно-экономический университет

## ЗНАКОМСТВО С КРИПТОПРОВАЙДЕРАМИ

Функции CryptoAPI обеспечивают прикладным программам доступ к криптографическим возможностям Windows. Однако они являются лишь «передаточным звеном» в сложной цепи обработки информации. Основную работу выполняют скрытые от глаз программиста функции, входящие в специализированные программные (или программно-аппаратные) модули – провайдеры (поставщики) криптографических услуг (CSP – Cryptographic Service Providers), или криптопровайдеры.

Программная часть криптопровайдера представляет собой dll-файл, подписанный Microsoft; периодически Windows проверяет цифровую подпись, что исключает возможность подмены криптопровайдера.

Криптопровайдеры отличаются друг от друга:

– составом функций (например, некоторые криптопровайдеры не выполняют шифрование данных, ограничиваясь созданием и проверкой цифровых подписей);

– требованиями к оборудованию (специализированные криптопровайдеры могут требовать устройства для работы со смарт-картами для выполнения аутентификации пользователя);

– алгоритмами, осуществляющими базовые действия (создание ключей, хеширование и пр.).

По составу функций и обеспечивающих их алгоритмов криптопровайдеры подразделяются на типы. Например, любой CSP типа PROV\_RSA\_FULL поддерживает как шифрование, так и цифровые подписи, использует для обмена ключами и создания подписей алгоритм RSA, для шифрования – алгоритмы RC2 и RC4, а для хеширования – MD5 и SHA.

В зависимости от версии операционной системы состав установленных криптопровайдеров может существенно изменяться. Однако на любом компьютере с Windows можно найти Microsoft Base Cryptographic Provider, относящийся к типу PROV\_RSA\_FULL. Именно с этим провайдером по умолчанию будут взаимодействовать все программы.

Использование криптографических возможностей Windows напоминает работу программы с графическим устройством. Криптопровайдер подобен графическому драйверу: он может обеспечивать взаимодействие программного обеспечения с оборудованием (устройство чтения смарт-карт, аппаратные датчики случайных чисел и пр.). Для вывода информации на графическое устройство приложение не должно непосредственно обращаться к драйверу – вместо этого нужно получить у системы контекст устройства, посредством которого и осуществляются все операции. Это позволяет прикладному программисту использовать графическое устройство, ничего не зная о его аппаратной реализации. Точно так же для использования криптографических функций приложение обращается к криптопровайдеру не напрямую, а через CryptoAPI. При этом вначале необходимо запросить у системы контекст криптопровайдера.

Выясним, какие же криптопровайдеры установлены в системе. Для этого понадобятся четыре функции CryptoAPI:

– CryptEnumProviders (*i*, резерв, флаги, тип, имя, длина\_имени) – возвращает имя и тип *i*-го по порядку криптопровайдера в системе (нумерация начинается с нуля);

– CryptAcquireContext (проводер, контейнер, имя, тип, флаги) – выполняет подключение к криптопровайдеру с заданным типом и именем и возвращает его дескриптор (контекст). При подключении будем передавать функции флага CRYPT\_VERIFYCONTEXT, служащего для получения контекста без подключения к контейнеру ключей;

– CryptGetProvParam (проводер, параметр, данные, размер\_данных, флаги) – возвращает значение указанного параметра про-

вайдера, например, версии (второй параметр при вызове функции – PP\_VERSION), типа реализации (программный, аппаратный, смешанный – PP\_IMPTYPE), поддерживаемых алгоритмов (PP\_ENUMALGS). Список поддерживаемых алгоритмов при помощи этой функции может быть получен следующим образом: при одном вызове функции возвращается информация об одном алгоритме; при первом вызове функции следует передать значение флага CRYPT\_FIRST, а при последующих флаг должен быть равен 0;

– CryptReleaseContext (провайдер, флаги) – освобождает дескриптор криптопровайдера.

Каждая из этих функций, как и большинство других функций CryptoAPI, возвращает значение типа Boolean, определенного в языке C, которое в языке Visual Basic приводится к типу Boolean с помощью функций Cbool. Полученное значение типа Boolean можно проанализировать, чтобы определить, успешно ли выполнена операция открытия контекста CSP.

*Шифрование с использованием паролей.* После ознакомления со структурой CryptoAPI можно воспользоваться ею в практических целях. Самым ожидаемым действием криптографической подсистемы является шифрование файлов, чтобы лишь пользователь, знающий определенный пароль, мог получить к ним доступ.

Для шифрования данных в CryptoAPI применяются симметричные алгоритмы. Симметричность означает, что для шифрования и расшифровки данных используется один и тот же ключ, известный как шифрующей, так и расшифровывающей стороне. При этом плохо выбранный ключ шифрования может дать противнику возможность взломать шифр. Поэтому одной из функций криптографической подсистемы должна быть генерация «хороших» ключей либо случайным образом, либо на основании некоторой информации, предоставляемой пользователем, например пароля.

В случае создания ключа на основании пароля должно выполняться следующее обязательное условие: при многократном повторении процедуры генерации ключа на одном и том же пароле должны получаться идентичные ключи. Ключ шифрования имеет, как правило, строго определенную длину, определяемую используемым алгоритмом, а длина пароля может быть произвольной. Даже интуитивно понятно, что для однозначной генерации ключей нужно

привести разнообразные пароли к некоторой единой форме. Это достигается с помощью хеширования.

Хешированием (от англ. hash – разрезать, крошить, перемешивать) называется преобразование строки произвольной длины в битовую последовательность фиксированной длины (хеш-значение, или просто хеш) с обеспечением следующих условий:

- по хеш-значению невозможно восстановить исходное сообщение;
- практически невозможно найти еще один текст, дающий такой же хеш, как и заранее заданное сообщение;
- практически невозможно найти два различных текста, дающих одинаковые хеш-значения (такие ситуации называют коллизиями).

При соблюдении приведенных условий хеш-значение служит компактным цифровым отпечатком (дайджестом) сообщения. Существует множество алгоритмов хеширования. CryptoAPI поддерживает, например, алгоритмы MD5 (MD – Message Digest) и SHA (Secure Hash Algorithm).

Чтобы создать ключ шифрования на основании пароля, необходимо вначале получить хеш этого пароля. Для этого следует создать с помощью CryptoAPI хеш-объект, воспользовавшись функцией CryptCreateHash (provайдер, ID\_алгоритма, ключ, флаги, хеш), которой нужно передать дескриптор криптопровайдера (полученный с помощью CryptAcquireContext) и идентификатор алгоритма хеширования (остальные параметры могут быть нулями). В результате получим дескриптор хеш-объекта. Этот объект можно представить себе как черный ящик, который принимает любые данные и «перемалывает» их, сохраняя внутри себя лишь хеш-значение. Поставить данные на вход хеш-объекта позволяет функция CryptHashData (дескриптор, данные, размер\_данных, флаги).

Непосредственно создание ключа выполняет функция CryptDeriveKey (provайдер, ID\_алгоритма, хеш-объект, флаги, ключ), которая принимает хеш-объект в качестве исходных данных и строит подходящий ключ для алгоритма шифрования, заданного своим ID. Результатом будет дескриптор ключа, который можно использовать для шифрования.

Следует обратить внимание, что при работе с CryptoAPI мы все время имеем дело не с самими объектами или их адресами, а с

дескрипторами – целыми числами, характеризующими положение объекта во внутренних таблицах криптопровайдера. Сами таблицы располагаются в защищенной области памяти, так что программы «шпионы» не могут получить к ним доступ.

Алгоритмы шифрования, поддерживаемые CryptoAPI, можно разделить на блочные и поточные: первые обрабатывают данные относительно большими по размеру блоками (например, 64, 128 битов или более), а вторые – побитно (теоретически, на практике же – побайтно). Если размер данных, подлежащих шифрованию, не кратен размеру блока, то последний, неполный блок данных, будет дополнен необходимым количеством случайных битов, в результате чего размер зашифрованной информации может несколько увеличиться. Разумеется, при использовании поточных шифров размер данных при шифровании остается неизменным.

Шифрование выполняется функцией CryptEncrypt (ключ, хеш, финал, флаги, данные, рамер\_данных, размер\_буфера):

- через параметр *ключ* передается дескриптор ключа шифрования;
- параметр *хеш* используется, если одновременно с шифрованием нужно вычислить хеш-значение шифруемого текста;
- параметр *финал* равен true, если шифруемый блок текста – последний или единственный (шифрование можно осуществлять частями, вызывая функцию CryptEncrypt несколько раз);
- значение *флага* должно быть нулевым;
- параметр *данные* представляет собой адрес буфера, в котором при вызове функции находится исходный текст, а по завершению работы функции – зашифрованный;
- следующий параметр, соответственно, описывает размер входных/выходных данных;
- последний параметр задает размер буфера – если в результате шифрования зашифрованный текст не уместится в буфере, возникнет ошибка.

Для расшифровки данных используется функция CryptDecrypt (ключ, хеш, финал, флаги, данные, рамер\_данных), отличающаяся от шифрующей функции только тем, что размер буфера указывать не следует: поскольку размер данных при расшифровке может только уменьшиться, отведенного под них буфера наверняка будет достаточно.

УДК 50.37.23

© А. М. Петрова, И. В. Поночевная

Санкт-Петербургский государственный  
инженерно-экономический университет

## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ГЛОБАЛЬНОЙ КОМПЬЮТЕРНОЙ СЕТИ ИНТЕРНЕТ С ТОЧКИ ЗРЕНИЯ ЭТИКИ И МОРАЛИ

Проблема информационной безопасности на сегодняшний день все чаще преподносится как инженерно-техническая дисциплина. Самые совершенные научные разработки – это защита информации от несанкционированного использования, криптографическая защита и многое другое. Подобная информационная защита не имеет ничего общего с защитой общества от общественно опасных вариантов, разрушающих основы личности, культуры и духовности. Прогресс информационных технологий в получении и распространении информации и знаний вызывает потребность в создании концепции безопасности информационного общества. Появление глобальной компьютерной среды Интернет с ее анархичной структурой усложнило проблемы цензуры.

Интернет представляет собой глобальное объединение компьютерных сетей и информационных ресурсов, принадлежащих множеству различных пользователей, предприятий и фирм. Это объединение является децентрализованным и единого свода правил и законов для пользования среды Интернет не установлено. Существуют, однако, общепринятые нормы работы в Интернете, направленные на то, чтобы деятельность каждого пользователя сети не мешала работе других пользователей. Фундаментальное положение этих норм таково: правила использования любых ресурсов Интернета (от почтового ящика до канала связи) определяют владельцы ресурсов.

Владелец любого информационного или технического ресурса сети может установить для этого ресурса собственные правила его использования. Правила использования ресурсов, либо ссылка на них публикуются владельцами или администраторами этих ресурсов. Как и любое другое средство массовой коммуникации, Интернет порождает множество этических проблем, однако этика здесь несколько отличается от общепринятой.

Желательно придерживаться следующих правил и норм:

- чересчур долго и часто не играть в компьютерные игры, требующие больших ресурсов Сети;
- злобно и агрессивно не относиться к другим пользователям и не совершать другие антиобщественные деяния;
- не создавать общедоступные файлы непристойного содержания;
- намеренно нельзя наносить ущерб или вмешиваться в действия других пользователей.

Российские Интернет-пользователи в целом достаточно высокообразованные люди – доля пользователей с незаконченным высшим и высшим образованием составляет более 78%. Тенденции последних лет свидетельствуют о росте числа домашних пользователей Интернета. Сегодня среди российской аудитории доля тех, кто выходит в Сеть из дома, составляет более 80%, в то же время практически 70% респондентов используют Интернет еще и на работе.

Общая проблема информационной безопасности состоит в анонимности, которую обеспечивает Сеть. Эта анонимность провоцирует активность жуликов и любителей безнаказанно сделать гадость – непрошенная почтовая реклама «спам». Материальный ущерб от «спама» в США, например, оценивается в 8 млрд долл. в год. Существуют компьютерные преступления, связанные с несанкционированным доступом к информации и разрушением конфиденциальных данных, а также преступления, связанные, главным образом, с «выражением мнения»: показом насилия, расовой дискриминацией, порнографией. Поскольку среда Интернета – всемирное средство для передачи текстов, изображений и звуков, она идеально подходит для совершения таких правонарушений. Первые преступления уже достаточно хорошо известны. Разработана юридическая база для борьбы с ними, изложенная в уголовном законодательстве.

Интернет несет много потенциально вредной и незаконной информации, которая может быть использована как средство осуществления незаконной деятельности. Эти нарушения и злоупотребления, связанные с сетью, неукоснительно требуют мер защиты по следующим направлениям:

- национальная безопасность (изготовление взрывчатых устройств, террористическая деятельность и т. д.);

– охрана несовершеннолетних (оскорбительные формы маркетинга, производство наркотиков, насилие и порнография);

– защита человеческого достоинства (расовая дискриминация и расистские оскорблении);

– сохранение тайн личной жизни (несанкционированный доступ к персональным данным, электронные оскорблении) и репутации («навешивание ярлыков», незаконная сравнительная реклама);

– обеспечение прав сохранности интеллектуальной собственности (несанкционированное распространение защищенных авторским правом работ; например, программного обеспечения, музыки и т. п.).

Необходимо выделить основные проблемные и правовые области, связанные с Интернет-доступом, Интернет-технологиями и поддержкой Интернет-ресурсов, с которыми сталкиваются пользователи.

**Защита данных.** Как известно, Интернет – открытая система, где электронные сообщения могут легко быть перехвачены, Web-ресурсы – прочитаны и переписаны и т. д. Выходом является шифровка, создание и совершенствование криптографии, которая позволяет надежно защищать информацию. Однако в некоторых странах у государства есть право раскрытия любых шифров по «необходимости» или в «интересах национальной безопасности». Сегодня в ряде стран, в частности, в Великобритании широко обсуждаются вопросы о правах личности и легитимности подобных государственных действий.

**Интернет-коммерция.** На сегодняшний день это уже достаточно распространенное явление затрагивает и библиотеки: Интернет-подписка, Интернет-книжные магазины и др. В связи с этим возникают проблемы онлайновых платежей, к которым ни технически, ни юридически многие библиотеки не готовы. Читатели уже требуют права использовать свои кредитные карточки, например, для оплаты полнотекстовых копий или услуг по электронной доставке документов, а правовой механизм финансового взаимодействия читателей и библиотек все еще не продуман.

**Возможная дискредитация.** Опубликованные в Интернете издания могут содержать неверные, клеветнические или оскорбительные высказывания. Требуется внести ясность: кто именно из цепочки взаимодействующих субъектов Интернета является автором,

кто – издателем, а кто – распространителем информации. Очевидно, что клевета или оскорблении, а также различные формы дискредитации, попадая в Интернет, могут многократно тиражироваться.

Например, один из известных случаев, связанных с Интернет-дискредитацией произошел с одной английской фирмой, которая через электронную почту объявила о якобы имевшей место финансовой нестабильности другой фирмы. Суд взыскал 450 тыс. фунтов стерлингов с этой фирмы. В Великобритании подобные дела часто являются предметом судебного разбирательства.

*Зашита персональных сведений.* При работе в Интернете может произойти разглашение нежелательных персональных сведений, а также нарушение тайны личной переписки и другие проблемы, связанные, в том числе, и с этикой. Многие владельцы Интернета загружают информацию без учета того, что не все сведения можно свободно всем предоставлять. Так, по сведениям прессы, недавно союз американских врачей и дантистов возбудил судебный процесс против медицинского совета штата Калифорния, который опубликовал перечень адресов лечащих врачей на Web-сайте без согласия многих врачей. Многие администраторы компаний в США устанавливают специальные пакеты просмотра определенных фраз и словосочетаний из электронных почт своих сотрудников, несмотря на то, что неприкосновенность частной жизни, гарантированная американской конституцией, предупреждает о недопустимости подобных действий в отношении своих граждан.

*Проблемы интеллектуальной собственности.* После открытия Интернета появились притязания на право собственности информационных сведений и информационных массивов. В основном две главные компоненты в сфере интеллектуальной собственности вызывают много вопросов – авторское право и торговая марка (товарный знак).

*Авторское право.* Имеется ряд проблем, связанных с применением обычного авторского права в Интернете. Обычно автор текста или композитор обладают эксклюзивными правами на выдачу разрешения на воспроизведение или распространение объекта своего интеллектуального творчества. Для печатной продукции эти права в большинстве случаев передаются издателю на условиях, указанных в соглашении о публикации. Свои особые права имеют соответствующие исполнители и распространители.

На сегодняшний день вопрос свободы доступа к глобальной сети Интернет довольно сложен с этической точки зрения и требует очень тщательного подхода. В настоящее время идет активное обсуждение проблем доступности Сети. Большинство из рассмотренных выше проблем пока не имеют однозначного правового решения и в большей степени относятся к сфере этики. Очевидна назревшая необходимость создания особой сферы этики – этики киберпространства, своеобразной виртуальной деонтологии.

Таким образом, в использовании информационных ресурсов Интернет-технологии идут вперед и это значительно облегчает поиск и сбор информации по необходимой теме. В то же время имеют место очевидные недостатки, которые со временем будут исправлены. К таким недостаткам относится засоренность сети бесполезной и, зачастую, вредной и даже опасной информацией. Отсутствие единой программы, систематизирующей информацию и доступ к ней, также является значительным препятствием.

УДК 50.37.23

© М. Ю. Ермина, Е. В. Стельмашонок

Санкт-Петербургский государственный  
инженерно-экономический университет

## АНАЛИЗ ИНФОРМАЦИОННЫХ РИСКОВ В СИСТЕМЕ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Одной из главных задач современного предприятия является обеспечение информационной безопасности. Угрозу могут представлять не только технические сбои, несогласованность данных в различных учетных системах, но также неограниченный доступ сотрудников к информации.

Устойчивое развитие промышленной корпорации предполагает существенное увеличение объемов информации в составе информационного контента, что в результате неизбежно связано с увеличением различных информационных рисков, однако это не приводит к уменьшению интенсивности общения с деловыми партнерами.

При оценке информационных активов промышленной корпорации, т. е. тех ценностей, которые корпорация считает целесообразными

разным защищать, следует учитывать все компоненты в составе единой бизнес-системы корпорации, все ее материальные и нематериальные активы.

Сегодня не вызывает сомнений необходимость вложений в обеспечение информационной безопасности современного крупного бизнеса.

Основной же проблемой остается оценка необходимого уровня вложений в информационную безопасность для обеспечения максимальной эффективности инвестиций в данную сферу.

Управление информационными рисками подразумевает:

1. Выбор объектов защиты.
2. Выбор методологии оценки рисков.
3. Идентификацию активов.
4. Анализ угроз и их последствий.
5. Оценку рисков.
6. Выбор защитных мер.
7. Реализацию и проверку средств и методов защиты.
8. Оценку остаточного риска.

Основная проблема в сфере информационных рисков – их объективная идентификация и оценка, выбор адекватных средств контроля, мер защиты. Это должно осуществляться с позиций обеспечения эффективности и рентабельности экономической деятельности предприятия.

Определенной проблемой становится совместимость нового инструментария управления рисками со сложившейся операционной и аппаратно-программной структурой, с традициями промышленной корпорации.

Степень риска устанавливается по одному из признанных международных методов, определяющему соответствие информационной системы стандарту ISO 17799 (BS 7799).

В соответствии с существующими методиками управление информационными рисками промышленной корпорации (методики международных стандартов ISO 15408, ISO 17799 (BS7799), BSI; а также национальных стандартов NIST 80030, SAC, COSO, SAS 55/78) предполагает следующее:

– определение основных целей и задач защиты информационных активов корпорации;

– создание эффективной системы оценки и управления информационными рисками;

– расчет совокупности детализированных не только качественных, но и количественных оценок рисков, адекватных заявленным целям стратегии развития промышленной корпорации;

– применение специального инструментария оценивания и управления рисками.

Современные методики и технологии управления информационными рисками позволяют оценить существующий уровень остаточных информационных рисков в отечественных промышленных корпорациях. Это особенно важно в тех случаях, когда к информационной системе промышленной корпорации предъявляются повышенные требования в области защиты информации и непрерывности бизнеса.

Цель оценки риска состоит в том, чтобы определить риск утечки информации из корпоративной сети предприятия. Процесс оценки риска проводится в два этапа. На первом этапе определяют границы сети для анализа и детальную конфигурацию корпоративной сети, т. е. определяется модель компьютерной сети предприятия. На втором этапе проводится анализ риска. Анализ риска разбивается на идентификацию ценностей, угроз и уязвимых мест, оценку вероятностей и измерение риска. Показатели ресурсов, значимости угроз и уязвимостей, эффективности средств защиты могут быть определены как количественными методами, например, при определении стоимостных характеристик, так и качественными, например, учитывающими штатные или чрезвычайно опасные воздействия внешней среды.

Преимущества и недостатки количественных, качественных методик управления рисками приведены в таблице.

Качественные и количественные методики управления рисками

Методики	Преимущества	Недостатки
Качественные	Отсутствие необходимости присваивания денежной стоимости активу Отсутствие необходимости количественного вычисления частоты появления угроз, точного размера ущерба, соответствия эффективности мер угрозам	Субъективность подхода к оценке Отсутствие возможности установления количественного соответствия угроз затратам

Окончание

Методики	Преимущества	Недостатки
Количественные	<p>Возможность моделирования оценки информационных активов с позиции безопасности корпорации</p> <p>Классифицирование и оценивание информационных активов</p> <p>Возможность ранжирования угроз и уязвимостей на основе количественных оценок</p> <p>Возможность оценки меры контроля рисков и выбора инструментальных средств</p> <p>Возможность количественной оценки эффективности и/или стоимости различных вариантов защиты</p>	<p>Непроработанность и сложность в использовании менеджментом корпорации расчетных составляющих параметров моделей</p>

В настоящее время известно множество табличных методов оценки информационных рисков компаний. Они рекомендованы международными стандартами информационной безопасности, главным образом ISO 17799 (BS 7799). Существенно, что в этих рекомендуемых методах количественные показатели существующих или предлагаемых физических ресурсов компании оцениваются с точки зрения стоимости их замены или восстановления работоспособности ресурса. А существующие или предполагаемые программные ресурсы оцениваются так же, как и физические, т. е. с помощью определения затрат на их приобретение или восстановление.

Наибольшее распространение среди методик оценки рисков получила методика «матрицы рисков». Это достаточно простая методика анализа рисков. В процессе оценки экспертами определяются вероятность возникновения каждого риска и размер связанных с ним потерь (стоимость риска). Причем оценивание производится по шкале с тремя градациями: «высокая», «средняя», «низкая». На базе оценок для отдельных рисков выставляется оценка системе в целом (в виде клетки в такой же матрице), а сами риски ранжируются. Данная методика позволяет быстро и корректно произвести оценку. Но, к сожалению, дать интерпретацию полученных результатов не всегда возможно.

Кроме того, в данной области разработан механизм получения оценок рисков на основе нечеткой логики, который позволяет заме-

нить приближенные табличные методы грубой оценки рисков современным математическим методом, адекватным рассматриваемой задаче.

Механизм оценивания рисков на основе нечеткой логики по существу является экспертной системой, в которой базу знаний составляют правила, отражающие логику взаимосвязи входных величин и риска. В простейшем случае – это «табличная» логика, в общем случае – более сложная логика, отражающая реальные взаимосвязи, которые могут быть formalизованы с помощью продукционных правил вида «если ..., то».

Кроме того, механизм нечеткой логики требует формирования оценок ключевых параметров и представления их в виде нечетких переменных. При этом необходимо учитывать множество источников информации и качество самой информации. В общем случае это достаточно сложная задача. Однако в каждом конкретном случае могут быть найдены и формально обоснованы ее решения.

Можно выделить следующие подходы разработчиков программных средств анализа рисков к решению поставленной задачи:

- получение оценок рисков только на качественном уровне;
- вывод количественных оценок рисков на базе качественных, полученных от экспертов;
- получение точных количественных оценок для каждого из рисков;
- получение оценок механизмом нечеткой логики.

УДК 50.37.23

© А. Г. Коробейников

Санкт-Петербургский государственный университет  
информационных технологий механики и оптики

© Г. М. Чернокнижный

Санкт-Петербургский государственный  
инженерно-экономический университет

## ИСПОЛЬЗОВАНИЕ КРИПТОСИСТЕМ НА БАЗЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Криптостойкость таких широко известных криптосистем с открытым ключом, как RSA, или Эль-Гамала [1], базируется на том, что задачи факторизации больших целых чисел и логарифмирования

ния в конечном поле являются достаточно сложными с вычислительной точки зрения. Однако конечные поля являются не единственными алгебраическими структурами, в которых может быть поставлена задача вычисления дискретного логарифма. В 1985 году Коблиц и Миллер (причем независимо друг от друга) предложили использовать для построения криптосистем алгебраические структуры, определенные на множестве точек эллиптической кривой (ЭК). Рассмотрим определение ЭК над полями Галуа [2].

Пусть  $p > 3$  – простое число,  $a, b \in GF(p)$  такие, что  $4a^2 + 27b^2 \neq 0$ . Эллиптической кривой  $E$  над полем  $GF(p)$  называется множество решений  $(x, y)$  уравнения

$$y^2 = x^3 + ax + b \text{ Mod}(p) \quad (1)$$

над полем  $GF(p)$  вместе с дополнительной точкой  $\infty$ , называемой точкой в бесконечности.

Представление ЭК в виде уравнения (1) носит название *эллиптической кривой в форме Вейерштрасса*.

Для точек на кривой вводится бинарная операция сложения, которая играет ту же роль, что и операция умножения в криптосистемах RSA и Эль-Гамала:

$$1. \infty + \infty = \infty.$$

$$2. \text{ Для любых } (x, y) \in E, (x, y) + \infty = (x, y).$$

$$3. \text{ Для любых } (x, y) \in E, (x, y) + (x, -y) = \infty.$$

$$4. \text{ Для любых } (x_1, y_1) \in E, (x_2, y_2) \in E, x_1 \neq x_2, (x_1, y_1) + (x_2, y_2) = (x_3, y_3), \text{ где } x_3 = \lambda^2 - x_1 - x_2, y_3 = \lambda(x_1 - x_3) - y_1, \lambda = \frac{y_2 - y_1}{x_2 - x_1}.$$

$$5. \text{ Для любых } (x_1, y_1) \in E \text{ и } y_1 \neq 0, (x_1, y_1) + (x_1, y_1) = (x_3, y_3), \text{ где } x_3 = \lambda^2 - 2x_1, y_3 = \lambda(x_1 - x_3) - y_1, \lambda = \frac{(3x_1^2 + a)}{2y_1}.$$

Множество точек на кривой  $E$ , с заданной таким образом бинарной операцией, образует абелеву группу.

Пользуясь операцией сложения точек на кривой, можно естественным образом ввести операцию умножения точки  $P \in E$  на произвольное целое число  $k$ :

$$kP = P + P + \dots + P,$$

где операция выполняется  $k$  раз.

Построим теперь одностороннюю функцию, на базе которой будем строить криптосистему.

Пусть  $E$  – ЭК, точка  $P \in E$ . Возьмем  $k \in Z$ , причем  $k < NE$ . В качестве прямой функции выберем произведение  $kP$ . Для его вычисления по оптимальному алгоритму требуется не более  $2\log_2 k$  операций сложения. Обратную задачу определим так: по заданным ЭК, точке  $P \in E$  и произведению  $kP$  найти  $k$ . В настоящее время такая задача за полиномиальное время не разрешима.

Далее рассмотрим криптографический протокол, аналогичный протоколу Диффи-Хелмана [1].

Для установления секретной связи два пользователя  $A$  и  $B$  выбирают ЭК  $E$  и точку  $P$  на ней. Затем  $A$  и  $B$  генерируют независимо друг от друга по секретному числу  $\alpha$  и  $\beta$ . Затем пользователь  $A$  вычисляет произведение  $\alpha P$  и пересыпает его  $B$ , а пользователь  $B$  вычисляет  $\beta P$  и пересыпает его  $A$ . При этом параметры кривой, координаты точки на ней, значения произведений являются открытыми и могут передаваться по незащищенным каналам связи. Далее пользователь  $A$  умножает присланное значение  $\beta P$  на  $\alpha$ , получив после этого  $\alpha\beta P$ , пользователь  $B$  умножает присланное значение  $\alpha P$  на  $\beta$ , получая такой же результат –  $\alpha\beta P$ . Таким образом, оба пользователя получили общее секретное значение (координаты точки  $\alpha\beta P$  на ЭК), которое они могут использовать для получения секретного ключа шифрования. Необходимо отметить, что криptoаналитику для восстановления ключа потребуется решить сложную с вычислительной точки зрения математическую задачу восстановления  $\alpha$  и  $\beta$  по известным  $E$ ,  $P$ ,  $\alpha P$  и  $\beta P$ .

Пример. Пусть абоненты  $A$  и  $B$  решили провести передачу сообщений, используя криптосистему на базе ЭК. Для этого они выбрали ЭК

$$\begin{aligned} E : y^2 &= x^3 + 31\ 575x + 22\ 833 \text{ Mod}(33\ 613), \\ (4 \cdot 31\ 575 \cdot 31\ 575 + 27 \cdot 22\ 833 \cdot 22\ 833) \text{ Mod}(33\ 613) &= \\ = 521\ 345\ 889 \text{ Mod}(33\ 613) &= 4 \cdot 19\ 045 + 27 \cdot 8\ 259 \text{ Mod}(33\ 613) = \\ = 8\ 954 + 21\ 315 \text{ Mod}(33\ 613) &= 30\ 269 \text{ Mod}(33\ 613) \neq 0 \end{aligned}$$

и точку  $P(20\ 607, 10\ 567)$  на ней. Затем  $A$  генерирует секретное число  $\alpha = 27\ 846$ . Пользователь  $B$  генерирует секретное число  $\beta = 18\ 535$ .

Затем пользователь  $A$  вычисляет произведение  $\alpha P = (24\ 387, 3\ 717)$  и пересыпает его  $B$ , а пользователь  $B$  вычисляет  $\beta P = (13\ 692, 25\ 053)$  и пересыпает его  $A$ . Далее пользователь  $A$  умножает присланное значение  $\beta P$  на  $\alpha$ , получив после этого  $\alpha\beta P = (11\ 867, 32\ 791)$ . Пользователь  $B$  умножает присланное значение  $\alpha P$  на  $\beta$ , получая такой же результат –  $\alpha\beta P = (11\ 867, 32\ 791)$ . Таким образом, оба пользователя получили общее секретное значение (координаты точки  $\alpha\beta P$  на ЭК), которое они могут в дальнейшем использовать в качестве общего секретного ключа.

Переход на «эллиптическую» криптографию позволяет сохранить приемлемую длину ключа при резком (на порядки) увеличении стойкости крипtosистем. Появление «эллиптической» криптографии и было обусловлено именно этой причиной.

#### Литература

1. Чмора А. Л. Современная прикладная криптография. 2-е изд. М.: Гелиос, АРВ, 2002.
2. Ван Дер Варден Б. Л. Алгебра: Пер. с нем. 2-е изд. М.: Наука, 1979.

УДК 50.37.23

© В. И. Фомин

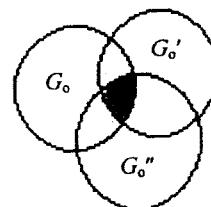
Санкт-Петербургский государственный  
инженерно-экономический университет

### ОПРЕДЕЛЕНИЕ ЭФФЕКТА ОТ СОВМЕСТНОГО ПРИМЕНЕНИЯ МЕТОДОВ ПОВЫШЕНИЯ ДОСТОВЕРНОСТИ ИНФОРМАЦИИ

При проектировании экономических информационных систем (ЭИС) необходимо обеспечить достоверность информации при выполнении различных этапов ее преобразования (ввод с клавиатуры, считывание с различных видов технических носителей, хранение, передача по каналам связи, обработка, представление результатов пользователю и т. п.). Эта задача решается путем использования различных методов контроля ошибок (помехозащищенное кодирование, использование контрольных сумм, дублирование операций со сравнением результатов, визуальный контроль данных, проверка

допустимого диапазона при вводе некоторых данных и т. д.), а также за счет использования методов, не связанных с контролем (выбор вводимых значений из заранее подготовленного списка, стимулирование безошибочной работы персонала и т. п.). В процессе проектирования ЭИС необходимо иметь возможность оценивать эффект от применения отдельного метода или группы различных методов повышения достоверности на разных этапах преобразования информации.

Наибольшее внимание в литературе уделяется оценке эффективности методов контроля и исправления ошибок. Для оценки эффективности контроля чаще всего используют интегральную характеристику «вероятность пропуска методом ошибок»  $P_{\text{проп}}$  или «вероятность обнаружения методом ошибок»  $P_{\text{обн}} = 1 - P_{\text{проп}}$ . Однако такая обобщенная оценка не позволяет определять эффект от совместного применения нескольких методов контроля и не позволяет с тех же позиций учитывать влияние методов повышения достоверности, не связанных с контролем. Каждый метод обнаруживает лишь определенный набор типов ошибок, а каждый этап преобразования информации характеризуется своим специфическим набором типов ошибок и частотой их возникновения. В связи с этим обобщенная оценка  $P_{\text{проп}}$  (или  $P_{\text{обн}}$ ) справедлива обычно только для одной пары «метод контроля–этап преобразования» и не может использоваться для других случаев. При совместном применении группы методов выявляемые этими методами типы ошибок могут частично различаться, а частично перекрываться (совпадать):



Графическая интерпретация применения двух различных методов для обнаружения некоторого класса ошибок  $G_o$ :

$G_o$  – некоторый класс типов ошибок, возникающих в процессе преобразования информации;  
 $G'_o, G''_o$  – типы ошибок, выявленные двумя разными методами контроля

По изложенной выше причине обобщенная оценка  $P_{\text{проп}}$  (или  $P_{\text{обн}}$ ) не позволяет однозначно оценивать эффект от совместной реализации нескольких методов обнаружения ошибок.

Различные варианты реализации контроля (человеком-оператором, с помощью электронного устройства, по программе и т. п.) существенно различаются по своей надежности, что может приводить к изменениям эффективности одного и того же метода в зависимости от его конкретной реализации. Помимо методов контроля ошибок, в ЭИС используются также разнообразные мероприятия по снижению числа возникающих искажений. Как уже было отмечено, обычно применяемые характеристики  $P_{\text{обн}}$  не позволяют с единых позиций оценивать эффект от совместного применения различных методов контроля и мероприятий по снижению числа ошибок, не связанных с контролем, с учетом их взаимного влияния, надежности и структуры реализации. В качестве такой оценки могут быть предложены коэффициенты редукции  $K_R$ , определяемые в соответствии с различными уровнями оценки достоверности следующими соотношениями:

$$K_{R_c} = \frac{P^*}{P}; K_{R_n} = \frac{P_n^*}{P_n}; K_{R_z} = \frac{P_z^*}{P_z}, \quad (1)$$

где  $K_{R_c}$ ,  $K_{R_n}$ ,  $K_{R_z}$  – коэффициент редукции при применении контроля преобразования символа, реквизита (числа, слова)  $n$ -го типа и сообщения  $z$ -го типа;

$P$ ,  $P_n$ ,  $P_z$  – вероятность получения искаженного символа, реквизита, сообщения;

$P^*$ ,  $P_n^*$ ,  $P_z^*$  – то же при применении контроля.

Исходя из известной статистики искажений и сведений о способности метода выявлять ошибки разных классов (типов),  $K_R$  могут быть оценены в общем виде аналитически:

$$K_R = \sum_{s=1}^{S_{\text{общ}}} q_s (1 - P_{\text{обн}_s}) = 1 - \sum_{s=1}^{S_{\text{общ}}} q_s P_{\text{обн}_s}, \quad (2)$$

где  $S_{\text{общ}}$  – общее число типов ошибок;

$q_s$  – относительная частота появления ошибок класса  $s$ , причем выполняется нормирование  $\sum_{s=1}^{S_{\text{общ}}} q_s = 1$ ;

$P_{\text{обн}_s}$  – вероятность обнаружения ошибок класса  $s$ .

Значение  $P_{\text{обн}_s}$  зависит от вероятности  $P_{ms}$  выявления ошибок класса  $s$ , определяемой используемой процедурой контроля (методом), причем  $0 \leq P_{ms} \leq 1$ , а также от условной вероятности  $Q_{k,o}$  обнаружения ошибки контрольным органом (схемой, человеком, программой):  $P_{\text{обн}_s} = P_{ms} \cdot Q_{k,o}$ . Величины  $P_{ms}$  неизменны для конкретной процедуры контроля (метода). Значения  $Q_{k,o}$  должны определяться для каждого варианта реализации.

Таким образом, с учетом изложенного

$$K_R = 1 - Q_{k,o} \sum_{s=1}^{S_{\text{общ}}} q_s P_{ms}.$$

Во многих практических случаях можно пренебречь ненадежностью реализации контроля.

Тогда справедливо

$$\tilde{K}_R = 1 - \sum_{s=1}^{S_{\text{общ}}} q_s P_{ms} \leq K_R.$$

Для оценки  $K_R$  может быть использована упрощенная формула

$$K'_R = 1 - Q_{k,o} \sum_{s=1}^{S_{\text{общ}}} q_s k_{\text{обн}_s} \leq K_R, \quad (3)$$

где  $k_{\text{обн}_s} = 1$  при обнаружении методом ошибок класса  $s$  или  $k_{\text{обн}_s} = 0$  – в противном случае.

Точность оценки (3) определяется характером дробления ошибок на классы  $s$ .

Использование  $K_R$  позволяет оценивать обнаруживающую способность контроля для группы этапов преобразования информации по характеристикам отдельных этапов. Для символов искажения на разных этапах, как показывают экспериментальные исследования, могут считаться независимыми и несовместимыми. На основе определения (1) и формулы вероятности независимых несовместных событий можно записать

$$K_{R_{cl}} = \frac{P^*}{P} = \frac{\sum_{i=1}^m P_i K_{Rci}}{\sum_{i=1}^m P_i} = \sum_{i=1}^m v_i K_{Rci},$$

где  $K_{Rc1}$  – значение  $K_R$  для символов при контроле одним методом группы этапов преобразования информации;

$m$  – число этапов преобразования;

$P_i$  – вероятность искажения символа на  $i$ -м этапе;

$K_{Rci}$  – значение  $K_{Rc}$  при действии метода контроля на  $i$ -м этапе преобразования;

$v_i$  – весовой коэффициент для  $i$ -го этапа.

$$v_i = \frac{P_i}{\sum_{i=1}^m P_i}, \text{ причем } \sum_{i=1}^m v_i = 1. \quad (4)$$

С учетом формулы (2) получим

$$K_{Rc1} = 1 - Q_{k,o} \sum_{i=1}^m v_i \sum_{s=1}^{S_{\text{общ}}} q_{si} P_{ms},$$

где  $q_{si}$  – относительная частота возникновения ошибок класса  $s$  на  $i$ -м этапе преобразования.

Для преобразований реквизита искажения на разных этапах могут считаться независимыми и совместными (что подтверждается известными экспериментальными данными). Следовательно, оценка  $K_{Rn1}$  (по аналогии с  $K_{Rc1}$ ) будет иметь вид

$$K_{Rn1} = \frac{P_n^*}{P_n} = \frac{\left[ \begin{array}{c} m \\ 1 - \prod_{i=1}^m (1 - P_{ni} K_{Rni}) \end{array} \right]}{\left[ \begin{array}{c} m \\ 1 - \prod_{i=1}^m (1 - P_{ni}) \end{array} \right]}, \quad (5)$$

где  $P_{ni}$  – вероятность искажения реквизита  $n$ -го вида на  $i$ -м этапе;

$K_{Rni}$  – значение  $K_R$  для реквизита  $n$ -го вида при действии контроля на  $i$ -м этапе. Однако расчет по формуле (5) при  $m > 2$  не всегда удобен. Для приближенной оценки  $K_{Rn1}$  сверху и снизу могут быть использованы соотношения

$$\sum_{i=1}^m v_{ni} K_{Rni} \leq K_{Rn1} \leq \sum_{i=1}^m v_{ni}^* K_{Rni},$$

где

$$v_{ni} = \frac{P_{ni}}{\sum_{i=1}^m P_{ni}}, \text{ причем } \sum_{i=1}^m v_{ni} = 1, \quad (6)$$

$$v_{ni}^* = \frac{P_{ni}}{\left[ 1 - \prod_{i=1}^m (1 - P_{ni}) \right]}, \text{ причем } \sum_{i=1}^m v_{ni}^* \geq 1. \quad (7)$$

Аналогичным образом может быть найдена оценка  $K_{Rz}$  для сообщения по известным значениям  $K_{Rn}$  для реквизитов, входящих в его состав:

$$\sum_{n=1}^{N_z} v_{zn} \cdot K_{Rn} \leq K_{Rz} \leq \sum_{n=1}^{N_z} v_{zn}^* \cdot K_{Rn},$$

где  $N_z$  – общее число реквизитов в  $z$ -м типе преобразования;

$v_{zn}$ ,  $v_{zn}^*$  – весовые коэффициенты для  $n$ -х реквизитов, которые определяются по формулам, аналогичным (6) и (7), где вместо  $P_{ni}$ ,  $m$  и  $P_n$  используются  $P_n$ ,  $N_z$  и  $P_z$ .

Использование  $K_R$  позволяет также оценивать совместное действие группы методов. В общем виде величина коэффициента редукции при действии группы методов на одном этапе преобразования информации

$$K_{R2} = 1 - \sum_{s=1}^{S_{\text{общ}}} q_s P_{\text{общ}}^s,$$

где  $P_{\text{общ}}^s$  – значение  $P_{\text{общ}}$  для группы методов.

Выявление ошибок класса  $s$  одновременно несколькими методами чаще всего не приводит к улучшению суммарной вероятности обнаружения ошибок по сравнению с лучшим из используемых методов (за исключением случая выявления разными методами различных видов ошибок в пределах общего класса  $s$ ). Поэтому  $P_{\text{общ}}^s$  можно оценить:

$$P_{\text{общ}}^s \geq \max_{1 \leq j \leq R_m} [P_{mj} Q_{k,oj}], \quad (8)$$

где  $R_m$  – общее число методов в группе;  
 $P_{mj}$ ,  $Q_{k,oj}$  – значения  $P_{mj}$  и  $Q_{k,oj}$  для  $j$ -го метода контроля.

Для приближенной оценки

$$K'_{R2} = \sum_{s=1}^{S_{\text{общ}}} \left[ q_s \prod_{j=1}^{R_s} (1 - k_{\text{обн},j}) Q_{k,o,j} \right].$$

Возможна также совместная оценка  $K_{R3}$  эффекта от применения группы методов контроля для группы этапов преобразования. В общем виде

$$K_{R3} \geq 1 - \sum_{i=1}^m \left[ v_i \sum_{s=1}^{S_{\text{общ}}} q_{si} P_{\text{общ}}^{\Sigma} \right],$$

где  $v_i$  определяется по формулам, аналогичным (4) или (7), а  $P_{\text{общ}}^{\Sigma}$  – из соотношения (8).

Для методов, не связанных с выполнением контроля при известном распределении снижения числа разных видов искажений, значение  $K_R$  может быть оценено по формуле

$$K_R = 1 - \sum_{s=1}^{S_{\text{общ}}} q_s k_{us},$$

где  $k_{us}$  – коэффициент исключения ошибок вида  $s$ , причем  $0 \leq k_{us} \leq 1$  (при  $k_{us} = 1$  полное исключение ошибок вида  $s$ , при  $k_{us} = 0$  данное мероприятие не затрагивает ошибки вида  $s$ ). При совместном действии методов контроля и мероприятий, не связанных с контролем, суммарное значение  $K_{R\Sigma}$  может быть оценено так

$$K_{R\Sigma} = 1 - \sum_{s=1}^{S_{\text{общ}}} q_s k_{us} - \sum_{s=1}^{S_{\text{общ}}} q_s P_{\text{общ}} + \sum_{s=1}^{S_{\text{общ}}} q_s k_{us} P_{\text{общ}}.$$

При отсутствии данных о распределении  $k_{us}$  действие методов повышения достоверности может оцениваться недифференцированно по (1).

Рассмотренный подход позволяет в процессе проектирования осуществлять оценку обнаруживающей способности отдельных методов контроля и их комплексов для различных этапов и групп этапов преобразования информации, а также учитывать с единых позиций влияние на достоверность информации мероприятий, не связанных с выполнением контроля.

УДК 681.3

© М. В. Харинов

Санкт-Петербургский государственный  
инженерно-экономический университет

## СТЕГАНОГРАФИЯ НА ОСНОВЕ МОДЕЛИ ВИРТУАЛЬНОЙ ВИДЕОПАМЯТИ

Последние 5 лет характеризовались повышенным вниманием к проблеме сокрытия и обнаружения сообщений в изображениях и аудиосигналах. Судя по открытым источникам, возможности стеганографии (сокрытия и передачи в составе сигналов относительно больших объемов произвольных данных – сообщений) пока недостаточно исследованы даже на уровне постановки задачи. В известных приемах сокрытия сообщений в изображениях обычно недостаточно полно описывается информация исходного сигнала (контейнера), которая сохраняется после встраивания данных сообщения. В методах адаптивной стеганографии, в которых координаты кодов встроенного сообщения зависят от содержания контейнера, вычисление координат по стего-изображению (контейнеру со встроенным сообщением) оказывается затруднительным. Поэтому при извлечении сообщения обычно учитывается «ключ», который кодирует способ размещения встроенных данных независимо от контейнера [1].

В предлагаемой модели виртуальной видеопамяти информация изображения раскладывается на инвариантную и переменную компоненты. Встраивание сообщения описывается модификацией переменной компоненты информации, не влияющей на вычисление инвариантной компоненты. Размещение кодов сообщения по координатам и яркостным диапазонам определяется инвариантной компонентой информации и вычисляется при извлечении сообщения без использования ключа [1]. Многоканальная суперпозиция кодов сообщения в различных яркостных диапазонах обеспечивает повышение объема сообщения.

*Модель виртуальной памяти.* Виртуальная память приписывается изображению формально, но используется для записи и считывания произвольных кодов сообщений подобно реальной компьютерной памяти. Виртуальная память состоит из запоминающих элементов, которые вводятся посредством обобщения понятия битов, используемых для хранения информации в компьютере.

Если отвлечься от строения ячейки памяти компьютера, то биты, в которых хранятся значения яркости пикселов (элементарных клеточных полей) изображения, можно описать посредством вложенных диапазонов шкалы яркости, по величине кратных степени  $\langle 2 \rangle$ . Разряды виртуальной памяти определяются последовательностью вложенных диапазонов шкалы яркости, которые вычисляются в алгоритме [2] итеративного разделения гистограммы яркости на части приблизительно равной площади. Итеративное разбиение яркостной шкалы продолжается до тех пор, пока не окажется, что каждый диапазон содержит единственную яркость, которая сопоставляется последовательности стягивающихся к ней диапазонов и на каждой итерации принадлежит одному из них. Алгоритм разбиения шкалы яркости таков, что варьирование яркости каждого пикселя изображения внутри своего диапазона, хотя и влияет на гистограмму яркости, но не влияет на вычисление текущего разбиения яркостной шкалы, а также на вычисление предыдущих ее разбиений на диапазоны яркости. При этом пиксели могут модифицироваться по яркости независимо друг от друга.

Предполагается, что ячейки виртуальной памяти сопоставляются пикселям изображения и состоят из последовательных запоминающих элементов. Значение очередного элемента ячейки виртуальной памяти, в зависимости от номера итерации разбиения яркостной шкалы, определяется положением яркости пикселя относительно центра рассматриваемого диапазона яркости. При этом очередному элементу ячейки виртуальной памяти приписывается положительное, отрицательное, либо нулевое значение знака разности яркости пикселя и центральной яркости рассматриваемого диапазона. Тем самым определяется считывание троичных единиц информации, которые согласно Н. П. Брусенцову называются тритами [3]. Триты, вычисленные для данного разбиения шкалы яркости, составляют каналы виртуальной памяти и считаются упорядоченными по уменьшению вложенных диапазонов яркости. Старший трит каждой ячейки виртуальной памяти вычисляется по общему диапазону яркости изображения, а младшие триты – по вложенным диапазонам.

Запись сообщения в триты виртуальной памяти связывается с отражением яркостного значения пикселя относительно центра соответствующего диапазона и выполняется последовательно от

старших тритов – к младшим. Яркостное значение, оказавшееся в центре диапазона, очевидно, при отражении не меняется. Поэтому триты с нулевыми значениями при записи сообщения не подлежат модификации и считаются неактивными. К неактивным относят также триты, изменение которых влечет модификацию предшествующих тритов.

Для алгоритма  $R$  чтения сообщения из изображения и встраивание  $P_h$  сообщения  $h$  (от hidden) описывается соотношениями

$$\begin{aligned} h &= RP_h u \\ P_h : P_h^2 u &= P_h u, \\ u &= P_{Ru} u \end{aligned}$$

где  $n$  – номер итерации;

$P_h u$  – стего-изображение.

Здесь имеется в виду, что извлечение встроенного сообщения  $h$  достигается в алгоритме  $R$  чтения сообщения, повторная запись сообщения не влияет на стего-изображение (преобразование  $P_h$  идемпотентно), а также, что любое изображение сохраняется при обратном встраивании извлеченного из него сообщения.

Выписанные формулы описывают класс обсуждаемых алгоритмов.

Компоненты цветового изображения при вычислении виртуальной памяти рассматриваются независимо друг от друга. Избыточность изображения выражается повторениями тритов по координатам, каналам виртуальной памяти и цветам. Искажение кодов сообщения в процессе передачи изображения компенсируется их простым суммированием с последующим вычислением знака полученной суммы. Для учета случая равновесного распределения альтернативных значений битов сообщения, в качестве запоминающих элементов виртуальной памяти необходимо использовать именно триты, а не биты.

Таким образом, триты, по сравнению с битами, позволяют проще отобразить результаты вычисления виртуальной памяти и деформализовать избыточность видеинформации. Особенности единиц представления информации в виртуальной памяти по сравнению с исходным представлением в компьютерной памяти отражены (для байтовых изображений) в таблице.

## Единицы представления и запоминания видеинформации

Атрибуты	Единицы	
	Биты	Триты
Порядковый номер	0, 1, 2, ..., 7	0, 1, 2, ..., $Ch$
Состояние	0, 1	$\pm 1,0$
Статус	$RW$	$R, RW$

Примечания:

$Ch$  – число каналов виртуальной памяти,

$R$  и  $RW$  – обозначения неактивных и активных разрядов.

**Метод многоканальной адаптивной стеганографии.** Практическим обоснованием модели виртуальной памяти служит ее применение в стеганографии, которая в настоящее время обычно подразделяется на собственно стеганографию (скрытие в произвольном контейнере сообщения, неизвестного на приемном конце), встраивание заранее известных водяных знаков, криптографическое кодирование координатного размещения информации сообщения и т. д. Модель виртуальной памяти позволяет представить для различных условий применения стеганографии единое решение и описать его в терминах обратимой записи сообщения в троичные ячейки, упорядоченные по координатам, каналам и цветовым компонентам. При этом рабочесть, устойчивость сообщения к искажениям (например, к JPEG-сжатию) обеспечивается за счет избыточного кодирования сообщения с повторениями и использования старших разрядов виртуальной памяти. Инвариантность сообщения относительно упаковки, растяжения, эквидистантной нормировки и других стандартных преобразований стего-изображения по яркости достигается благодаря замещению изображения представлением, которое не зависит от указанных преобразований. Незаметность встраивания сообщения, помимо использования младших разрядов виртуальной памяти, обеспечивается записью сообщения на повышенной частоте несущего сигнала.

Встраивание сообщения по нескольким яркостным каналам повышает его объем, который достигает 20–30% от объема контейнера, что в 2–3 раза больше объема встраивания, достигаемого известными методами [1]. При фиксированном числе каналов, помимо исходного контейнера для скрытия сообщения, может использоваться искусственно добавленный шум. В методе многоканальной

адаптивной стеганографии сообщение встраивается в каналы, число которых зависит от контейнера. С изменением контейнера распределение кодов сообщения по координатам, каналам и цветам меняется, причем сообщение при этом играет роль одного из криптографических ключей.

Метод многоканальной адаптивной стеганографии иллюстрируется рисунком. Встраиваемые данные представляют собой суперпозицию рисунков цифр в последовательных битовых плоскостях компьютерного представления, образуемых битами одинаковых разрядов. Содержимое битовых плоскостей сообщения записывается в каналы виртуальной памяти с повторением по цветам и периодическим повторением по координатам. На стего-изображении рисованные цифры, встроенные в старшие каналы, затирают цифры, встроенные в младшие каналы (рисунок).



Метод многоканальной адаптивной стеганографии

На рисунке верхний ряд: контейнер в виде полноцветного 24-битового изображения (слева) и стего-изображение (справа). Следующий ряд: структурное и числовое представления виртуальной памяти (слева и справа, соответственно). Внизу – сообщение в виде последовательности цифр.

Структурное представление виртуальной памяти задает разделение тритов на активные и неактивные. При этом установленные биты ячеек структурного представления для каждого пикселя изображения задают активные триты виртуальной памяти. Оба представления виртуальной памяти вычислены для исходного контейнера. В компонентах встроенного сообщения серые пиксели обозначают биты сообщения, которые не помещаются в виртуальную память и вычисляются как биты с неопределенным значением. Для наглядности встраивание выполнено без специальных приемов скрытия сообщения.

Как показывают эксперименты, модель виртуальной памяти позволяет встраивать сообщения с улучшением качества, повышением емкости контейнера и уменьшением числа градаций для сжатия и упрощения автоматической обработки, а также реализовать другие технологии двойного применения. Методом многоканальной адаптивной стеганографии можно встраивать сообщения не только в полутоновые (серые и цветовые), но и в бинарные картины, а также в аудиосигналы. При этом оказывается возможным без принципиального изменения конструкции передающих устройств встраивать в аудиосигналы видеосопровождение. В существующих базах изображений и аудиосигналов без изменения стандартного формата хранения файлов можно использовать встроенные «подрисуночные подписи», полезные для оптимизации поиска системными средствами и средствами сети Интернет. При банковских расчетах для защиты от подделки можно неявно визировать электронные копии документов в виртуальной памяти. Многоканальная адаптивная стеганография обеспечивает самостоятельную защиту криптографических ключей, а также позволяет решить ряд других задач информационной безопасности.

Таким образом, для эффективной защиты информации очевидна необходимость создания собственной элементной базы, возможно, с применением многозначной логики. При этом может оаться полезным опыт эксплуатации, созданной почти полвека на-

зад троичной ЭВМ «Сетунь», которая благодаря минимальному числу базовых команд превосходила современные компьютеры по простоте программирования [3]. Дальнейшему развитию аппаратной реализации троичной логики препятствовало соображение, что в теории информации ее количество измеряется в битах, а не тритах.

В предложенной модели виртуальной памяти использование тритов обосновывается решением задач представления и запоминания видеинформации. Количественная оценка использует конструктивную интерпретацию понятия информации [4] и строится в соответствии с комбинаторным подходом А. Н. Колмогорова [5]. Достигаемые при этом простота и наглядность модели позволяют надеяться на ее дальнейшее внедрение, если не в аппаратной, то в программной реализации.

#### Литература

1. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. М.: Солон-Пресс, 2002.
2. Прэйтт У. Цифровая обработка изображений. Т. 1–2. М.: Мир, 1982.
3. Брусенцов Н. П. Вычислительная машина «Сетунь» Московского государственного университета // Новые разработки в области вычислительной математики и вычислительной техники. Киев, 1960. С. 226–234.
4. Харинов М. В., Горохов В. Л. Оценка количества информации сегментированного изображения как виртуального носителя цифровых данных // Известия вузов России. Радиоэлектроника. Вып. 4. СПб., 2004. С. 16–24.
5. Колмогоров А. Н. Три подхода к определению понятия «Количество информации» // Проблемы передачи информации. 1965. Вып. 1. Т. 1. С. 3–8.

БИБЛИОТЕКА  
СПб ГИЭУ

6165

## СОДЕРЖАНИЕ

Предисловие .....	3
-------------------	---

### Раздел I ТЕХНОЛОГИИ ОБРАБОТКИ ИНФОРМАЦИИ

<i>Бройдо В. Л., Шарипов Р. Р. (СПбГИЭУ)</i> Искусственный интеллект на столе руководителя .....	4
<i>Потягайло А. Ю. (СПбГИЭУ)</i> Проектный подход к созданию и развитию информационной среды технологического образования .....	8
<i>Стельмашонок В. Л. (СПбГИЭУ)</i> Обзор методов моделирования структур сложных систем .....	12
<i>Путилов С. А. (СПбГИЭУ)</i> Технология параметрически-ориентированного программирования.....	17
<i>Соколовская С. А. (СПбГИЭУ)</i> Возможности использования генератора отчетов Crystal Reports	23
<i>Чернокнижный Г. М. (СПбГИЭУ), Коробейников А. Г., Чернокнижная Е. Г. (СПбГУИТМО)</i> Математическая теория категорий при проектировании САПР ...	25
<i>Пономарев В. В. (ЗАО «Транзас»), Гниденко И. Г., Пономарев В. В. (СПбГИЭУ)</i> Разработка автоматизированной системы оценки подготовки обучаемого при использовании компьютерного тренажера .....	30
<i>Поночевная И. В. (СПбГИЭУ)</i> Использование унифицированного языка моделирования в современных информационных технологиях .....	34
<i>Стельмашонок Е. В. (СПбГИЭУ)</i> Информационная инфраструктура как основа поддержки и защиты корпоративных бизнес-процессов .....	37
<i>Говорунов Д. А. (СПбГИЭУ)</i> Прогнозирование спроса на медицинские услуги на основе использования метода SSA (Singular Spectrum Analysis).....	42

<i>Дашевский А. И., Обухов А. С. (СПбГИЭУ)</i> Системы поддержки принятия решений в экономических задачах .....	50
<i>Горохов В. Л. (СПбГИЭУ), Вдовенко И. В. (СПбГЭТУ)</i> Разработка устойчивых непараметрических алгоритмов и программных средств для проверки однородности данных при контроле процессов обращения с ТБО .....	54
<i>Ильина О. П., Мамаева Г. А. (СПбГИЭУ)</i> Управление информационными технологиями .....	63
<i>Мамаева Г. А. (СПбГИЭУ)</i> Стратегии развития информационных технологий .....	68
<i>Салимьянова Ж. Г. (СПбГИЭУ)</i> Формирование умений использования средств компьютерной графики у студентов .....	72
<i>Нестерук Т. Н. (СПбГИЭУ)</i> Специфика моделирования интеллектуального корпоративного сайта .....	74

### Раздел II ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ДАННЫХ'

<i>Поночевная И. В. (СПбГИЭУ)</i> Тенденции развития современных защитных технологий .....	84
<i>Мердина О. Д. (СПбГИЭУ)</i> Подход к анализу защищенности компьютерных систем .....	87
<i>Тихонов Д. В., Стельмашонок Е. В. (СПбГИЭУ)</i> Использование объектно-ориентированного подхода при решении задач информационной безопасности .....	92
<i>Поночевная И. В. (СПбГИЭУ)</i> Тестирование как процесс современной информационной технологии при разработке системы защиты .....	97
<i>Шапченко М. А. (СПбГИЭУ)</i> Криптографические средства защиты информации фирмы «Анкад» .....	100

**НАУЧНОЕ ИЗДАНИЕ**

<i>Мгебришвили М. М. (СПбГИЭУ)</i>	
Метод остаточного кодирования как метод криптографической защиты информации.....	104
<i>Авдонин И. С. (СПбГИЭУ)</i>	
Знакомство с криптовайдерами .....	106
<i>Петрова А. М., Поночевная И. В. (СПбГИЭУ)</i>	
Информационная безопасность в глобальной компьютерной сети INTERNET с точки зрения этики и морали.....	111
<i>Ермина М. Ю., Стельмашонок Е. В. (СПбГИЭУ)</i>	
Анализ информационных рисков в системе корпоративной информационной безопасности.....	115
<i>Коробейников А. Г. (СПбГУИТМО), Чернокнижный Г. М. (СПбГИЭУ)</i>	
Использование криптосистем на базе эллиптических кривых.....	119
<i>Фомин В. И. (СПбГИЭУ)</i>	
Определение эффекта от совместного применения методов повышения достоверности информации.....	122
<i>Харинов М. В. (СПбГИЭУ)</i>	
Стеганография на основе модели виртуальной видеопамяти .....	129

**СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ  
ОБРАБОТКИ И ЗАЩИТЫ ИНФОРМАЦИИ**

Сборник научных трудов

Редактор *П. А. Тимачева*  
Корректор *Е. Г. Закревская*  
Компьютерная верстка *О. Д. Мамоновой*

---

ИД № 00918 от 02.02.2000 г.  
Подписано в печать 14.02.06. Формат 60×84<sup>1</sup>/16. Бумага типогр. № 1.  
Печать цифровая. Усл.-печ. л. 8,0. Уч.-изд. л. 8,5. Изд. № 99. Тираж 150 экз. Заказ 107.

СПбГИЭУ, 191002, Санкт-Петербург, ул. Марата, 27.  
ИзПК СПбГИЭУ, 191002, Санкт-Петербург, ул. Марата, 31.