R_a - радиус частицы;

H - характерный линейный размер;

F - сила адгезионного взаимодействия.

Как видно из (13), критерий диспергирования зависит от $p_{ух}$ и для технического углерода, из которого состоит, в основном, диспергируящаяся фаза при приготовлении резиновой смеси, $p_{ух}$ составляет примерно 0,02 МПа [4].

Таким образом, исходя из вышесказанного, представляется возможным вести процесс смешения, обеспечивая требуемое значение $p_{r\theta}$.

ЛИТЕРАТУРА

1. Кафаров В.В., Дорохов И.П., Арутюнов С.Ю. Системный анализ процессов химической технологии. - М.: Наука, 1985.
2. Торнер Р.В. Основные процессы переработки полимеров. - М.: Химия, 1972.
3. Торнер Р.В. Теоретические основы переработки полимеров. - М.: Химия, 1977.
4. Вострокнутов Е.Г. и др. Переработка каучуков и резиновых смесей. - М. Химия, 1980.
5. А.с. 1407814.

УДК 681.32.001

Е.А. Бартош, аспирант

НАПРАВЛЕНИЕ ИСПОЛЬЗОВАНИЯ ОБЪЕКТНО-ОРИЕНТИРОВАННОГО АНАЛИЗА ДЛЯ СОЗДАНИЯ ОБУЧАЮЩИХ ПРОГРАММ

The article considers questions of use of object-oriented analysis method for creation of training systems with elements of artificial intelligence. In particular the attention is devoted to a problem of creation of ecological system models for use in the training purposes and opportunity of use of the object-oriented analysis method for construction of such models.

1.Постановка задачи

Проблеме разработки обучающих систем (ОбС) с элементами искусственного интеллекта (ИИ) уже уделялось много внимания и с теоретической, и с практической стороны (см.,например,[1]). По некоторым данным [2], применение экспертных систем (ЭС) при профессиональной подготовке позволяет сократить затраты на индивидуальную работу с обучаемым в 8-12 раз без потери качества обучения.

Процесс обучения с помощью ЭС носит исследовательский или даже игровой оттенок. Обучающие системы с элементами игры уже зарекомендовали себя в педагогической практике [3]. Существует класс программного обеспечения, называемый «деловые игры», которые широко применяются при подготовке экономистов [4]. ЭС - модель изучаемой предметной области (ПрО). Она функционирует по законам ПрО, формализованным с некоторой степенью точности. В работу этой модели можно вмешаться, изменить или добавить некоторые факты и даже правила и таким образом комбинировать условия для получения некоторого желаемого результата. Задав исходное состояние системы объектов ПрО, можно получить представление об их взаимном влиянии, а также понаблюдать за развитием этой ситуации во времени.

При применении ЭС в обучении достаточно актуальна задача использования мультимедиа-технологий. Во-первых, это позволяет визуализировать и озвучивать динамические процессы ПрО, что существенно повышает привлекательность системы и в конечном счете качество обучения. Во-вторых, предоставить контекстно-зависимую оперативную информацию, которая может быть удобно организована в виде системы гипертекстовых ссылок. Имеется в виду, что информация необходима не в контексте программной оболочки ЭС, а в контексте модели, с которой обучаемый работает.

Важное значение имеет изучаемая ПрО. В данной статье мы ориентируемся на сложные и плохо формализуемые ПрО с большим количеством взаимодействующих объектов различной природы и характера поведения. Такими ПрО являются, в частности, социально-экономические, экологические процессы. Построение ЭС для данных ПрО имеет самостоятельную практическую ценность. Детальное и точное моделирование в этой области требует высоких затрат труда и квалификации, вычислительной мощности уровня суперкомпьютеров, сложного и дорогого программного обеспечения. При разработке ЭС для обучающих целей возможны существенные упрощения моделей.

После анализа вышеизложенных тезисов встает вопрос об инструментальных средствах (ИС) для разработки ЭС для обучающих целей. С учетом современных тенденций и технологий эти ИС должны обеспечивать следующее: 1.Удобные средства для построения моделей ПрО (оболочек ЭС) с использованием визуальных средств моделирования (CASE-технологии). Модель описывает структуру объектов ПрО, их взаимосвязи и правила поведения (во времени). Наполнив такую оболочку конкретными фактами (объектами), получим реальную ЭС. 2.Возможность построения и модификации модели пользователем-непрограммистом.

3.Возможность использования мультимедиа-технологий при построении моделей и их наполнении.

В настоящее время на рынке программного обеспечения нет ИС для создания ЭС, которые бы отвечали вышеизложенным требованиям.

2.Инструментальные средства создания ЭС

В 80-е годы были созданы сотни ИС для построения ЭС. Все они основаны на специальных языковых средствах (у каждой ИС обычно был свой язык) для описания модели ПрО [2]. Использование этих средств не требовало знания технических аспектов программирования и приближало процесс описания модели к описанию на естественном языке. Задача описания ПрО на языке ЭС определила новую специальность - инженер по знаниям. Но каждое ИС имеет свои ограничения и, следовательно, некоторую свою область применения, а один даже высококвалифицированный инженер по знаниям не мог владеть более чем 3-4-мя ИС.

В начале 90-х годов средства разработки общего назначения достигли такого уровня, что их использование при создании тех же ЭС стало более эффективным и по скорости разработки, и по качеству, чем использование ИС специального назначения.

Причины:

- переход на объектно-ориентированную (ОО) технологию разработки;
- широкое применение визуальных средств разработки (CASE-технология).

Необходимо отметить, что ОО технология привлекла внимание специалистов в области ЭС сразу после ее возникновения в начале 80-х годов и задолго до ее широкого распространения. Язык SmallTalk, первый язык, в котором реализована наиболее строгая парадигма объектно-ориентированного программирования (ООП), рассматривался как одно из ИС общего назначения для создания ЭС. Этому способствует сама парадигма ООП, которая вынуждает разработчика создавать структуру программы в соответствии со структурой ПрО. К концу 80-х годов технология ООП распространилась достаточно широко и появились методы ОО анализа (ООА) и ОО проектирования, на которых и базируются разрабатываемые нами ИС. В качестве базовой выбрана методология, изложенная в [5]. Эта методология:

- определяет процесс формализации ПрО как последовательный и итерационный процесс, т.е. дает в руки инженера по знаниям готовый инструмент для анализа ПрО;
- использует в качестве базового инструмента диаграммы, а не языковые средства, что обеспечивает возможность для реализации CASE-подхода при моделировании;

– обеспечивает построение модели ПрО с такой степенью детализации, что эта модель может рассматриваться как оболочка ЭС и может быть интерпретирована с помощью машинного интерпретатора. Заполнив эту оболочку фактами, можно смоделировать некоторую ситуацию в реальном или относительном времени.

3. Элементы методологии объектно-ориентированного анализа

Моделирование в ООА состоит из 2-х основных этапов (достаточных для построения оболочки ЭС): 1.Информационное моделирование - описание структуры объектов ПрО и их взаимосвязей. Фактически это задача проектирования реляционной структуры ПрО [6]. Существует уже достаточно много программных продуктов для автоматизации этого процесса, например ERWin/ERX компании Logic Works [7,8]. Реляционная модель - достаточно мощный инструмент для статического моделирования. Принцип реляционного моделирования положен в основу ЭС ИНДУС [9]. 2.Моделирование состояний - описание правил поведения объектов и их взаимного влияния во времени. На этом этапе строятся диаграммы переходов состояний (ДПС) объектов. ДПС - событийно управляемая модель. Поведение объекта задается с помощью переходов из состояния в состояние. С каждым состоянием связано некоторые действие, которое выполняется в момент перехода в данное состояние. Инициаторы изменения состояний объекта - события. События служат главным механизмом связи ДПС различных объектов и передачи данных.

Достаточно высокая степень структуризации и детализации предметной области в модели ООА открывает широкие возможности для применения мультимедиа-технологий (построение гипертекстовой системы на основе информационной модели, закрепление звуковых и анимационных эффектов за состояниями объектов на ДПС и моментами перехода между состояниями).

Однако высокая степень структуризации также является недостатком метода с точки зрения процесса моделирования. Работа с реляционными моделями всегда считалась достаточно сложной и требующей высокой квалификации. Данные недостатки частично можно устранить за счет применения CASE-технологии моделирования, шаблонов и типовых моделей.

4.Использование метода ООА для моделирования

Разрабатываемые нами ИС предназначены для создания ситуационных моделей экологических систем. ИС должны предоставлять инструмент для создания топологического ситуационного плана экологической системы (лес, река, атмосфера, населенные пункты, предприятие, очистные сооружения и т.п.) и описания свойств (атрибутов) и взаимосвязей данных объектов. Созданная таким образом модель предназначена для

обучения методике проведения экологической экспертизы предприятия. Не претендуя на точность полученных с помощью модели результатов, система должна давать практические навыки освоения экологической экспертизы. В контексте модели должна быть доступна необходимая методическая и юридическая информация. При работе с данными моделями обучаемый должен иметь возможность с некоторой степенью свободы менять размещение объектов на плане, изменять параметры объектов окружающей среды (загрязненность, климатические параметры, требования по предельно допустимым концентрациям загрязняющих веществ и т.п.), параметры предприятия (объем производства, параметры материалов и оборудования и т.п.), использовать природоохранные меры (добавлять на план очистные сооружения и т.п.), таким образом добиваясь требуемых характеристик предприятия и окружающей среды.

Для создания таких ситуационных моделей ИС должны обеспечить графические средства построения ситуационного плана и средства для описания информационных свойств и взаимосвязей объектов, динамики их поведения, то есть нарисованный план нужно «оживить». В качестве средства «оживления», то есть собственно моделирования, предполагается использовать метод ООА.

Метод ООА частично поддерживает стандарты моделирования, поддерживаемые основными институтами стандартов (ANSI, IEEE, ISO). В частности, процедура информационного моделирования соответствует спецификации ISO IDEF1X [7]. При реализации наших ИС также планируется поддержка спецификации IDEF1X. Это позволит импортировать в нашу систему информационные модели, созданные с помощью других систем, поддерживающих IDEF1X (ERWin/ERX, Design/IDEF и др.).

Но информационная модель, ориентированная на реляционную структуру, имеет очень высокий потенциал моделирования конечных процессов (без применения моделирования состояний).

Можно выделить два типа моделей - статические и динамические. Статические модели отражают структуру и взаимосвязи ПрО и могут быть полностью описаны в рамках информационной модели IDEF1X. Но для удобства моделирования предполагается реализовать некоторые расширения спецификации IDEF1X.

Одно из таких расширений - зависимые атрибуты (ЗА). ЗА (в отличие от основных атрибутов (ОА)) не хранят никаких значений. Их значение - выражение, состоящее из ОА и базовых операций и функций преобразования ОА, включая агрегатные функции, аналогичные агрегатным функциям языка SQL. И ОА, и ЗА несут смысловую нагрузку. Определив ЗА, его можно использовать при определении других ЗА наравне с ОА.

Таким образом можно несколько скрыть сложность структуры данных и выстраивать очень сложные иерархии атрибутов.

Второе расширение спецификации IDEF1X предполагается ввести для реализации некоторых ограниченных функций динамического моделирования. Динамическое моделирование - моделирование поведения системы объектов во времени. Диаграммы переходов состояний представляют собой мощное средство для создания таких моделей. Но в некоторых случаях для отражения поведения во времени применение непосредственно динамического моделирования не обязательно. Псевдо-динамическое моделирование (назовем его так) возможно и в рамках информационной модели. Для этого планируется ввести специальные типы атрибутов. Например, атрибут может зависеть в каждый момент относительного (системного) времени (заданного с определенной дискретностью) от датчика случайных чисел, либо значение может определяться функцией, зависящей от относительного времени. Для данных атрибутов необходимо сохранять значения во всех точках дискретизации относительного времени. При моделировании социально-экономических или экологических процессов такой подход даже более предпочтителен, чем ДПС.

ЛИТЕРАТУРА

1. Железко Б.А., Морозевич А.Н. Методология проектирования информационно-аналитических систем принятия решений и ее использование в подготовке специалистов //Тез. докладов II Международной конференции «Новые информационные технологии в образовании» - Минск, 1996. - Т.2. С.84-89
2. Искусственный интеллект. Справочник в 3 кн. Книга 1 под ред. Попова Э.В. - М: Радио и связь, 1990.
3. Хатхоху М.Н., Валькман Ю.Р. Методы и средства разработки игровых программных комплексов для компьютерных технологий обучения в школе //Программные продукты и системы: научно-пр. и пром.-рекл. приложение к журналу «Проблемы теории и практики управления», 1996. - №1. - С.23-28
4. Быков А.В., Веселько С.Е., Лавников А.М. Деловая игра «Дельта» как гибкая тренинговая система для подготовки специалистов экономического профиля //Тез. докладов II Международной конференции «Новые информационные технологии в образовании». - Минск, 1996. - Т.2.- С.226-231.
5. Шлеер С., Меллор С. Объектно-ориентированный анализ: моделирование мира в состояниях. - Киев: Диалектика, 1993.
6. Змитрович А.Н. Базы данных. - Мн.:Университетское, 1991.
7. ERwin. Methods Guide. - Logic Works, Inc, 1994.

8. Орлов С. Программное обеспечение CASE. - КомпьютерУик, №19. - 1996. - С.29-32.
9. Виньков М.М. ИНДУС - система приобретения знаний, основанная на индуктивном выводе //III конф. по искусственному интеллекту. - Тверь, 1992. - С.183-184.

УДК 681.325.6

П.П. Урбанович, профессор;
Н.В. Пацей, аспирант

КОНЦЕПЦИЯ СОЗДАНИЯ ВЗАИМОДОПОЛНЯЕМЫХ АЛГОРИТМОВ ОБЕСПЕЧЕНИЯ НАДЕЖНОСТИ И ЦЕЛОСТНОСТИ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

In the network techology the problem of data transmission is the main problem. This article contains the authors classifications and analyses of methods and algorithms for reliable and secret information transmission. Some elements of creating new cryptography algorithms, supplemented with error-correcting encryption are given.

Защита отдельных сообщений в подсистеме связи использует функции защиты от несанкционированного просмотра содержимого сообщения и случайных или преднамеренных модификаций, т.е. функции, гарантирующие секретность и правильность сообщения. В основном эти функции используются раздельно. Однако во многих случаях при передаче данных требуется гарантировать и конфиденциальность, и целостность, поэтому целесообразным был бы интегрированный способ реализации этих функций.

Существует ряд обоснованных теоретически и реализованных на практике криптостойких алгоритмов, обеспечивающих безопасность передачи данных, и методов, удовлетворяющих требованию надёжности и целостности информации.

Авторами данной статьи рассмотрены и оценены наиболее известные криптометоды и алгоритмы (рис.1) с точки зрения возможности практического применения при интегрированном подходе, проведена их классификация. Алгоритмы должны иметь высокую криптостойкость, вычислительную эффективность и простую реализацию. На сегодняшний день высокоэффективные системы с открытым ключом пока не найдены. Почти повсеместно принято ограничение использования асимметричных криптосистем только для управления ключами и для цифровой подписи.

Постоянное увеличение скорости каналов и объемов шифруемой информации, а также введение дополнительной избыточности, вводимой при помехоустойчивом кодировании,и увеличение объема шифротекста