

Секция 16

«НАУЧНО-МЕТОДИЧЕСКИЕ ПРОБЛЕМЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»

Содержание

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ПРОЦЕССА СПРОСА И ПРЕДЛОЖЕНИЯ НА РЫНКЕ ОБРАЗОВАТЕЛЬНЫХ УСЛУГ НА ОСНОВЕ МОДЕЛИ ЛОРЕНЦА	
Акманова Ю.А.	3044
О СФЕРИЧЕСКИХ КОДАХ И МЕТОДАХ ИХ ПОСТРОЕНИЯ	
Белов С.В.	3050
РАЗРАБОТКА ИНФОРМАЦИОННОГО ПОРТАЛА ДЛЯ ДОСТУПА ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ ОРЕНБУРГСКОЙ ОБЛАСТИ К МЕТОДИЧЕСКИМ ИНФОРМАЦИОННЫМ РЕСУРСАМ И ПРОГРАММНЫМ ПРОДУКТАМ	
Болодурина И.П., Лабузов В.А., Шухман А.Е., Полежаев П.Н., Ушаков Ю.А., Легашев Л.В.	3054
МЕТОДОЛОГИЧЕСКИЕ ПОДХОДЫ РАЗВИТИЯ КОМПЕТЕНЦИЙ УЧИТЕЛЯ КВАЛИФИЦИРОВАННО НАБИРАТЬ МАТЕМАТИЧЕСКИЙ ТЕКСТ	
Бугрова О.В.	3065
КАТЕГОРИРОВАНИЕ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ ДЛЯ ВЫБОРА СРЕДСТВ ФИЗИЧЕСКОЙ ЗАЩИТЫ	
Бурькова Е.В.	3073
АНАЛИЗ ПОДХОДОВ К АУДИТУ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ	
Бурькова Е.В., Хрыкина Н.А.	3077
ТИПЫ МОДЕЛЕЙ И ПРИНЦИПЫ МОДЕЛИРОВАНИЯ В ПРЕПОДАВАНИИ ГРАФИЧЕСКИХ ДИСЦИПЛИН	
Ваншина Е.А., Ваншин В.В.	3082
ПОДГОТОВКА В ОБЛАСТИ КОМПЬЮТЕРНОГО МОДЕЛИРОВАНИЯ СТУДЕНТОВ ПРОФЕССИОНАЛЬНОГО ОБУЧЕНИЯ	
Вергасова О.М.	3087
О СИММЕТРИЧНЫХ ШИФРАХ НА ОСНОВЕ УПРАВЛЯЕМЫХ ОПЕРАЦИЙ	
Винокуров Д.В.	3092
ИССЛЕДОВАНИЕ МЕТОДОВ ПОВЫШЕНИЯ ДОСТОВЕРНОСТИ ДЕКОДИРОВАННЫХ ДАННЫХ В ЗАБОЙНЫХ ТЕЛЕМЕТРИЧЕСКИХ СИСТЕМАХ С ГИДРАВЛИЧЕСКИМ КАНАЛОМ СВЯЗИ	
Влацкая И.В., Голубенко И.В.	3096
МЕТОДИЧЕСКИЕ АСПЕКТЫ ФОРМИРОВАНИЯ УЧЕБНО- ПОЗНАВАТЕЛЬНОЙ КОМПЕТЕНЦИИ НА УРОКАХ МАТЕМАТИКИ	
Газизова В.В.	3101

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБУЧЕНИИ НА СОВРЕМЕННОМ ЭТАПЕ	
Колобов А. Н.	3110
КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ.	
Курушин А. А.	3114
ИСПОЛЬЗОВАНИЕ МУЛЬТИМЕДИЙНЫХ НАГЛЯДНЫХ ПОСОБИЙ ПРИ ОБУЧЕНИИ МАТЕМАТИКЕ СТУДЕНТОВ ВУЗОВ	
Максименко Н.В.	3119
МОДЕЛЬ АДАПТИВНОГО ТЕСТИРОВАНИЯ КАК СПОСОБ РЕАЛИЗАЦИИ ИНДИВИДУАЛЬНОГО ПОДХОДА	
Маслова О.В.	3122
ИНТЕЛЛЕКТУАЛЬНАЯ ПРОГРАММНАЯ СИСТЕМА УПРАВЛЕНИЯ РИСКАМИ ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ	
Наточая Е.Н., Моргунова А.Т.	3131
ОБЗОР МЕТОДОВ ОТЫСКАНИЯ ГАМИЛЬТОНОВЫХ ЦИКЛОВ В ГРАФЕ	
Носов В.В., Орлов М.С.	3137
ОБ ОДНОМ ОПИСАНИИ РАДИКАЛА ДЖЕКОБСОНА ДЛЯ АЛГЕБР ЛИ	
Носов В.В., Павленко А.Н., Пихтилькова О.А.	3142
МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ. КРАТКИЙ ИСТОРИЧЕСКИЙ ОБЗОР	
Острая О.В.	3146
О ЦЕЛЕСООБРАЗНОСТИ ИСПОЛЬЗОВАНИЯ ЛЕКЦИОННЫХ ЗАНЯТИЙ ПРОПЕДЕВТИЧЕСКОГО ХАРАКТЕРА С ПРИМЕНЕНИЕМ МУЛЬТИМЕДИЙНЫХ ТЕХНОЛОГИЙ ПРИ ИЗУЧЕНИИ МАТЕМАТИЧЕСКИХ ДИСЦИПЛИН ЕСТЕСТВЕННОНАУЧНЫХ НАПРАВЛЕНИЙ	
Павленко А.Н., Пихтилькова О.А.	3151
ОБ ИЗЛОЖЕНИИ ТЕМЫ «ОПРЕДЕЛЕННЫЙ ИНТЕГРАЛ И ЕГО ПРИЛОЖЕНИЯ» В ПРОПЕДЕВТИЧЕСКОМ КУРСЕ ПО ВЫСШЕЙ МАТЕМАТИКЕ ДЛЯ ЕСТЕСТВЕННОНАУЧНЫХ НАПРАВЛЕНИЙ	
Павленко А.Н., Пихтилькова О.А.	3156
ПОДХОДЫ К ПОВЫШЕНИЮ КАЧЕСТВА ОБСЛУЖИВАНИЯ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИЛОЖЕНИЙ И СЕРВИСОВ МУЛЬТИОБЛАЧНЫХ ПЛАТФОРМ НА БАЗЕ ТЕХНОЛОГИЙ VNF И SDN	
Парфёнов Д.И., Болодурина И.П.	3162

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СУЩЕСТВУЮЩИХ СИСТЕМ УПРАВЛЕНИЯ РЕСУРСАМИ НА БАЗЕ ОБЛАЧНЫХ ТЕХНОЛОГИЙ	
Парфёнов Д.И., Шардаков В.М., Дедюрин В.В.	3166
К ВОПРОСУ О ПОВЫШЕНИИ КАЧЕСТВА ЗНАНИЙ ОБУЧАЮЩИХСЯ ПРИ ПРОВЕДЕНИИ ТЕКУЩЕГО КОНТРОЛЯ	
Пастухов Д.И.	3170
О РАЗЛИЧНЫХ РАДИКАЛАХ АЛГЕБР ЛИ	
Пихтильков С.А., Благовисная А.Н., Павленко А.Н.	3174
РЕШЕНИЕ ЗАДАЧ ПЛАНИРОВАНИЯ ВИРТУАЛЬНЫХ МАШИН И СБОРА СТАТИСТИКИ О РАБОТЕ ОБЛАЧНЫХ ПРИЛОЖЕНИЙ	
Полежаев П.Н.	3178
СОЗДАНИЕ ЭФФЕКТИВНЫХ АЛГОРИТМОВ ФУНКЦИОНИРОВАНИЯ ОБЛАЧНЫХ СИСТЕМ	
Полежаев П.Н.	3185
СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЭМУЛЯТОРОВ КОМПЬЮТЕРНЫХ СЕТЕЙ	
Порохненко Ю.С., Полежаев П.Н.	3194
СТРУКТУРА И МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСТАНЦИОННОГО КУРСА ПО МАТЕМАТИКЕ ДЛЯ ШКОЛЬНИКОВ И АБИТУРИЕНТОВ	
Руцкова И.Г.	3200
ПРИМЕНЕНИЕ ПРИКЛАДНЫХ ПРОГРАММ УЧЕБНОГО НАЗНАЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНЦИЙ БУДУЩЕГО БАКАЛАВРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	
Рычкова А.А., Гайфулина Д.А., Хакимова Э.Р.	3207
ОСОБЕННОСТИ ПОДГОТОВКИ БАКАЛАВРОВ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ	
Сидоров А.В.	3212
О ПРИМЕНЕНИИ ТЕОРИИ ВЫЧЕТОВ ПРИ РЕШЕНИИ ДИАФАНТОВЫХ УРАВНЕНИЙ	
Сикорская Г.А., Косилов Е.А.	3215
СИСТЕМАТИЗАЦИЯ КАК СРЕДСТВО ПОВЫШЕНИЯ КАЧЕСТВА МАТЕМАТИЧЕСКОЙ ПОДГОТОВКИ СТУДЕНТА	
Смирнова Е.Н., Томина И.П.	3220
ПРОБЛЕМЫ РАЗРАБОТКИ МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ ФГОС 4-ГО ПОКОЛЕНИЯ	
Сурина Е.Е.	3223
ПОПУЛЯРИЗАЦИЯ МАТЕМАТИЧЕСКИХ ЗНАНИЙ И МАТЕМАТИЧЕСКОГО ОБРАЗОВАНИЯ В ПРОЦЕССЕ ОБУЧЕНИЯ ИСТОРИИ РОССИИ	
Уткина Т.И., Игнатьева Е.С.	3231

РЕАЛИЗАЦИЯ СИМУЛЯТОРА ИНФРАСТРУКТУРЫ ДЛЯ
МНОГОАДРЕСНОЙ ШИРОКОПОЛОСНОЙ ПЕРЕДАЧИ
МУЛЬТИМЕДИЙНОГО ТРАФИКА НА БАЗЕ ПРОГРАММНО-
КОНФИГУРИРУЕМЫХ СЕТЕЙ

Ушаков Ю.А., Полежаев П.Н., Шухман А.Е., Бахарева Н.Ф.3234

«САЙТ КОНФЕРЕНЦИИ» КАК ИНФОРМАЦИОННАЯ ПЛОЩАДКА ДЛЯ
ПЕДАГОГИЧЕСКОГО СООБЩЕСТВА

Янгичер О.С., Усманов Р.И.3242

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ПРОЦЕССА СПРОСА И ПРЕДЛОЖЕНИЯ НА РЫНКЕ ОБРАЗОВАТЕЛЬНЫХ УСЛУГ НА ОСНОВЕ МОДЕЛИ ЛОРЕНЦА

Акманова Ю.А.

Оренбургский государственный университет, г. Оренбург

Одной из перспективных и быстро развивающихся областей применения математического моделирования является динамика инновационных процессов.

Большой интерес представляет исследование математических моделей инновационных процессов в научно-образовательных областях. Современные проблемы повышения качества образования, увеличения объемов услуг, реорганизации деятельности управления вузом с целью превращения вуза в коммерческо-финансово-научно-образовательную структуру, а также многие другие стоят на повестке дня в перестройке научно-образовательных процессов не только в России, но и во всем мире.

В данной работе представлено математическое моделирование процесса спроса и предложения на рынке образовательных услуг.

Рассмотрены теоретические основы применения трехпараметрической модели Лоренца для указанной модели.

Модель Лоренца обладает рядом преимуществ:

1) с математической точки зрения схема Лоренца – наиболее простая схема описания самоорганизующейся системы;

2) в модельных уравнениях системы Лоренца явно присутствуют слагаемые, соответствующие положительной и отрицательной обратным связям, являющимися необходимым атрибутом научно-образовательных систем;

3) эта модель является воплощением синергетического подхода, так как в ней определяются параметры порядка, позволяющие описать сложное поведение моделируемой системы достаточно простым образом (минимальным числом уравнений), а также управляющие параметры, при изменении которых существенно меняется макроскопическое поведение системы.

Объектом исследования модели является образовательное учреждение, состоящее из большого числа взаимодействующих подсистем и процессов. Она имеет следующие характеристики.

Роль параметра порядка системы D характеризует функция спроса $D = f_1(x_1, \dots, x_n; \{Q_1, \dots, Q_p\})$ на выпускников вуза, где D – объем спроса со стороны внешних потребителей (работодатели, предприятия и т.д.), $x_1, \dots, x_n$ – пространственные координаты, $\{Q_1, \dots, Q_p\}$ – агрегированные компоненты вектора качества выпускников $\overline{Q}_t$. При $D = 0$ вуз функционирует не эффективно, при $D > 0$ – эффективно.

Роль второго параметра S , описывающего образовательную деятельность вуза, описывает производственная функция $S = f_2(M, N)$, где S – объем продукта образовательной системы, M – модель концепции образования (управления качеством), N – потенциал вуза (ресурсы, персонал, мощности и т.д.). При этом $M = f_3[D(x_1, \dots, x_n; \{Q_1, \dots, Q_p\}), \{q_1, \dots, q_p\}]$, где $\{q_1, \dots, q_p\}$ – компоненты вектора качества учебного процесса $\vec{q}(\tau)$.

Третий параметр модели – это управляющий параметр U , который связан с качеством подготовки выпускников вуза, изменения которого приводит к самоорганизации системы, $U = |\overline{Q}(t)| / |\overline{Q}^*(t)|$.

Для пространственно однородной системы уравнения модели имеют вид (1):

$$\begin{cases} \frac{dD}{dt} = -a_1 D + a_2 S \\ \frac{dS}{dt} = -b_1 S + b_2 DU \\ \frac{dU}{dt} = -c_1 (U - U_e) - c_2 SD \end{cases} \quad (1).$$

Все величины, находящиеся в модели (1), характеризуют поведение системы как целого, т.е. представляют значения, усредненные по объему системы (ансамблю всех подсистем и процессов).

Основой синергетического подхода является то обстоятельство, что положительная обратная связь переменных $D(t)$, $U(t)$ с переменной $S(t)$, зависящими от времени, приводит к самоорганизации системы.

Вид динамической системы (1) совпадает с уравнениями Лоренца, записанными в перенормированных переменных. Запись уравнений Лоренца в форме (1) обусловлена выделением в явном виде параметра U_e , отражающего связь системы с внешней средой и влияющего на самоорганизацию. Этот параметр задает образовательной системе определенные критерии качества учебного процесса.

Особые точки системы (1) имеют вид:

$$1) (D^*, S^*, U^*) = (0, 0, U_e);$$

$$2) (D^*, S^*, U^*) = \left(\sqrt{\frac{c_1 a_2}{c_2 a_1}} (U_e - U_c), \frac{a_1}{a_2} \sqrt{\frac{c_1 a_2}{c_2 a_1}} (U_e - U_c), U_e \right), \quad \text{где}$$

$$U_e > U_c = \frac{a_1 b_1}{a_2 b_2} > 0.$$

Характеристическое уравнение для динамической системы (1) имеет виде:

$$|A - \lambda I| = \begin{vmatrix} -a_1 - \lambda & a_2 & 0 \\ b_2 U^* & -b_1 - \lambda & b_2 D^* \\ -c_2 S^* & -c_2 D^* & -c_1 - \lambda \end{vmatrix} \quad (2)$$

Для первой особой точки уравнение (2) имеет вид:

$$|A - \lambda I| = \begin{vmatrix} -a_1 - \lambda & a_2 & 0 \\ b_2 U^* & -b_1 - \lambda & 0 \\ 0 & 0 & -c_1 - \lambda \end{vmatrix} = 0 \quad (3)$$

$$(-c_1 - \lambda)[(-b_1 - \lambda)(-a_1 - \lambda) - a_2 b_2 U_e] = 0 \quad (4)$$

$$(-c_1 - \lambda)[\lambda^2 + (a_1 + b_1)\lambda + (U_c - U_e)a_2 b_2] = 0 \quad (5)$$

Из уравнения (5) получим:

$$\lambda_1 = -c_1 < 0, \lambda_{2,3} = -\left(\frac{a_1 + b_1}{2}\right) \pm \sqrt{\frac{(a_1 + b_1)^2}{4} - a_2 b_2 (U_c - U_e)}$$

Если $U_c > U_e$, $\frac{(a_1 + b_1)^2}{4} \geq a_2 b_2 (U_c - U_e)$, то $\lambda_2 < 0, \lambda_3 < 0$, и переходим к устойчивому узлу (при $U_c = U_e$ имеем $\lambda_2 < 0, \lambda_3 < 0$).

Если $U_c > U_e$, $\frac{(a_1 + b_1)^2}{4} < a_2 b_2 (U_c - U_e)$, то $\lambda_{1,2}$ имеют комплексно-сопряженный вид с отрицательной действительной частью, и приходим к устойчивому фокусу.

Если $U_c < U_e$, то $\lambda_2 > 0, \lambda_3 < 0$, и приходим к седлу.

Для второй особой точки уравнение (2) примет вид:

$$|A - \lambda I| = \begin{vmatrix} -a_1 - \lambda & a_2 & 0 \\ b_2 U_e & -b_1 - \lambda & b_2 \bar{A} \\ -\frac{a_1 c_2}{a_2} \bar{A} & -c_2 \bar{A} & -c_1 - \lambda \end{vmatrix} = 0 \quad (6)$$

$$(-a_1 - \lambda) \begin{vmatrix} -b_1 - \lambda & b_2 \bar{A} \\ -c_2 \bar{A} & -c_1 - \lambda \end{vmatrix} - a_2 \begin{vmatrix} b_2 U_e & b_2 \bar{A} \\ \frac{a_1 c_2}{a_2} \bar{A} & -c_1 - \lambda \end{vmatrix} = 0 \quad (7)$$

$$\begin{aligned} & -\lambda^3 - (a_1 + b_1 + c_1)\lambda^2 - (a_1 b_1 + a_1 c_1 + b_1 c_1 - b_2 c_2 \bar{A}^2 + a_2 b_2 U_c) \lambda - \\ & - 2a_1 b_2 c_2 \bar{A}^2 - a_1 b_1 c_1 + a_2 b_2 c_1 U_c = 0 \end{aligned} \quad (8)$$

где $\bar{A} = \sqrt{\frac{c_1 a_2}{c_2 a_1} (U_e - U_c)}$

Окончательный вид уравнения (8):

$$\begin{aligned} & \lambda^3 + (a_1 + b_1 + c_1)\lambda^2 + \left[2a_1 b_1 + a_1 c_1 + b_1 c_1 - \frac{c_1 c_2 b_2}{a_1} (U_e - U_c) \right] \lambda + \\ & + 2b_1 a_2 c_1 (U_e - U_c) = 0 \end{aligned} \quad (9)$$

Применим к уравнению (9) условия Рауса-Гурвица.

Согласно этим условиям, для того, чтобы все корни произвольного кубического уравнения

$$a_0 \lambda^3 + a_1 \lambda^2 + a_2 \lambda + a_3 = 0 \quad (10)$$

с действительными коэффициентами имели отрицательные действительные части, необходимо и достаточно, чтобы все главные диагональные миноры матрицы Гурвица для уравнения (9)

$$G = \begin{pmatrix} a_1 & a_3 & 0 \\ a_0 & a_2 & 0 \\ 0 & a_1 & a_3 \end{pmatrix} \quad (11)$$

были положительны:

$$\begin{vmatrix} a_2 & 0 \\ a_1 & a_3 \end{vmatrix} = a_2 a_3 > 0, \begin{vmatrix} a_1 & 0 \\ 0 & a_3 \end{vmatrix} = a_1 a_3 > 0, \begin{vmatrix} a_1 & a_3 \\ a_0 & a_2 \end{vmatrix} = a_1 a_2 - a_0 a_3 > 0 \quad (12)$$

Получим следующие условия на устойчивость второй особой точки:

$$\begin{cases} 2a_1b_1 + a_1c_1 + b_1c_1 - \frac{c_1c_2b_2}{a_1}(U_e - U_c) > 0 \\ (a_1 + b_1 + c_1)\left(2a_1b_1 + a_1c_1 + b_1c_1\right) - \frac{c_1b_2}{a_1}(U_e - U_c)(a_1c_2 + b_1c_2 + c_1c_2 - 2a_1a_2) > 0 \end{cases} \quad (13)$$

Рассмотри два частных случая.

$$1) a_1 = b_1 = c_1 = a_2 = b_2 = c_2 = 1 \Rightarrow U_c = 1$$

В этом случае система неравенств (9) приводится к виду: $1 < U_e < \frac{17}{5}$

$$2) a_1 = b_1 = a_2 = b_2 = 1, c_1 = c_2 = c$$

В этом случае система неравенств (9) приводится к виду:

$$\begin{cases} c^3(U_e - 1) - 2c^2(2 - U_e) + 2c(U_e - 4) - 4 < 0 \\ 0 < c < \frac{1 + \sqrt{1 + 2(U_e - 1)}}{U_e - 1} \end{cases} \quad (14)$$

Рассмотрим первое неравенство системы (14) на границах второго неравенства.

При $c = 0$ оно удовлетворяется. Подставляя первую границу второго неравенства системы (10) в первое неравенство, получим:

$$\begin{aligned} & \left(\frac{1 + \sqrt{1 + 2(U_e - 1)}}{U_e - 1} \right)^3 (U_e - 1) - 2 \left(\frac{1 + \sqrt{1 + 2(U_e - 1)}}{U_e - 1} \right)^2 (2 - U_e) + \\ & + 2 \left(\frac{1 + \sqrt{1 + 2(U_e - 1)}}{U_e - 1} \right) (U_e - 4) - 4 < 0 \end{aligned} \quad (15)$$

В случае, когда U_e стремится к единице, левая часть неравенства (15) стремится к минус бесконечности, а при возрастании U_e она быстро возрастает. Таким образом, в интервале $1 < U_e < 2$ существует некоторое пороговое значение параметра U_e , разделяющее области устойчивости и неустойчивости второй особой точки во втором частном случае. Например, если взять значение

$U_e = \frac{3}{2}$, то неравенство (15) примет заведомо выполняющийся вид $(1 + \sqrt{2})(-10 - 4\sqrt{2}) - 4 < 0$. Таким образом, в этом случае вторая особая точка является устойчивым узлом.

Таким образом, рассмотренная модель может быть использована для моделирования процесса спроса и предложения на рынке образовательных услуг.

В данной работе рассматривается трехпараметрическая модель Лоренца и на ее основе – условия и принципы функционирования вузов как самоорганизующихся систем, также оцениваются параметры эффективного развития образовательных систем с устойчивым спросом на выпускников и абитуриентов.

Дальнейшее изучение данной модели даст возможность применить другие схемы для ее улучшения, что позволит получить некоторые новые качественные результаты по количеству особых точек и их устойчивости.

Список литературы

1 Билаль Н.С., Математическое моделирование инновационных процессов на основе автономных динамических систем: дисс. ... канд. физ.-мат. наук: 05.13.18 / Н.С. Билаль – Белгород, 2012. – 181 с.

2 Вестник УГАТУ / М.Б. Гузаиров, И.Б. Герасимова, Модель накопления потенциала в образовательных системах. – 2006 - №2(15) – с. 115-119

3 Малинецкий, Г.Г., Математическое моделирование системы образования / Г.Г.Малинецкий, С.А.Кащенко, А.Б.Потапов // Синергетика и методы науки. СПб.: Наука – 1998 – 439 с.

4 Общероссийский математический портал [www.mathnet.ru]. – Буланичев В.А., Серков Л.А., Самоорганизация экономических систем с детерминированным хаосом – 2007 – С. 116-126.

О СФЕРИЧЕСКИХ КОДАХ И МЕТОДАХ ИХ ПОСТРОЕНИЯ

Белов С.В.

Оренбургский государственный университет, г. Оренбург

Пусть S^{n-1} означает сферу радиуса 1 с центром в начале координат евклидова пространства R^n . Конечное число точек $X \subset S^{n-1}$ будем называть сферическим кодом с параметрами n, ρ, M (и обозначим $X : (n, \rho, M)$). Размерность n – это размерность пространства над R , натянутого на точки X . Параметр ρ обозначает квадрат минимального евклидова расстояния между точками X .

$$\rho = \rho(X) = \min\{\rho(x, y) : x \neq y, x, y \in X\}, \quad (1)$$

$$\text{где } \rho(x, y) = \sum_{i=1}^n (x_i - y_i)^2, x = (x_1, \dots, x_n), y = (y_1, \dots, y_n).$$

Параметр M обозначает мощность кода, или просто число кодовых точек $M = |X|$.

Сферические коды связаны с проблемой упаковки шаров, имеющей приложения в различных областях, таких как теория чисел, алгебры Ли, численное вычисление интегралов, геометрия, физика, цифровая связь, проектирование антенн, статистический анализ, химия, биологии.

Особую роль играют практические и теоретические приложения к задачам цифровой связи. В частности, сферические коды находят свое применение в проектировании сигналов по каналу с шумом. В связи с этим актуальным является вопрос построения сферических кодов.

В литературе рассматриваются различные методы построения сферических кодов. Ещё в 1971 году в работе [1] Лич и Слоэн привели примеры построения сферических кодов на основе двоичных блоковых кодов. В фундаментальной работе Дж. Конвея и Н. Слоэна, посвященной различным аспектам проблемы упаковки шаров, также рассматриваются вопросы получения сферических кодов. Существует ряд работ, посвященных конструкциям кодов. Так, в работе [2] представлены конструкции, позволяющие улучшить нижние оценки мощности сферических кодов с $\rho < 1$ для размерностей $n \leq 64$. Статья [3] содержит описание конструкции для сферических кодов конечной размерности n , основанной на двух семействах двоичных кодов: кодах постоянного веса и обычных блоковых кодах.

Анализ публикаций, посвященных алгоритмам построения сферических кодов, позволяет выделить некоторые группы методов, основанных на общих принципах и идеях их построения. Первую группу объединяет общая идея, основанная на перестановках.

Перестановочная модуляция – один из старых методов построения сферических кодов. Метод очень прост и имеет два варианта выполнения. Возьмем произвольный вектор $x_0 = (x_{01}, x_{02}, \dots, x_{0N})$ с вещественными значениями и единичной нормой и построим все возможные перестановки этого вектора. Множество векторов, построенных таким образом, является сферическим кодом. Такая конструкция известна как перестановочная модуляция первого типа. Если в дополнение также допускаются все возможные изменения знаков, то такая конструкция называется перестановочной модуляцией второго типа. Оба типа производят коды со свойствами, которые легко описываются, легко исследуются и легко реализуются а, главное, для них декодирование методом максимального правдоподобия выполняется при помощи простого алгоритма. Следует отметить, что эффективность данных кодов быстро ухудшается с ростом размерности. Для размерностей больше 6 хорошие коды не производятся. Исключением являются симплекс и биортогональные коды, которые всегда строятся как частные случаи.

К следующей группе можно отнести коды, которые получаются из объединения двух и более кодов. Иногда таким образом можно построить хорошие коды даже из кодов, которые по отдельности не очень хороши. Чтобы оценить параметры сферического кода, построенного как объединение двух или более известных кодов, необходима подходящая оценка минимального расстояния между составляющими кодами.

Ещё одна группа методов имеет название «расширение кодов». Применение алгоритмов, основанных на идее расширения, позволяет довольно часто получать хорошие коды. Его также иногда называют «расширенное объединение».

Пусть $Y = \{y_1, y_2, \dots, y_m\}$ будет сферическим кодом с размерностью n_2 . Предположим, что для каждого кодового слова $y_i \in Y$ мы имеем сферические коды X_i , каждый из которых имеет размерность n_1 . Расширение Y кода с добавлением кода $X_i, i = 1, 2, \dots, m$ это следующий код

$$Z = \bigcup_{i=1}^m (X_i \sin \theta_i, y_i \cos \theta_i), \quad (2)$$

где θ_i – параметры, которые должны быть оптимизированы. Термин «расширение» обусловлен тем, что это простая модификация объединения. Можно рассматривать код Y как средство увеличения расстояния между подкодами путем добавления идентификационного окончания для каждого подкода. Разумеется, у такого увеличения расстояния есть и обратная сторона, размерность результирующего кода увеличивается с n_1 до $n_1 + n_2$ и энергия кодов X_i должна быть уменьшена, с неизбежным следствием в виде уменьшения соответствующего минимального расстояния. Тем не менее, этот метод производит хорошие коды.

Частным случаем сферического кода является равновесный код. Равновесными принято называть коды, каждая комбинация которых содержит одно и то же число r отличных от нуля символов. Простейшие из них, так называемые двоичные биортогональные коды, имеют вид

$$x_1, x_2, \dots, x_m, x_1 + 1, x_2 + 1, \dots, x_m + 1 \quad (3)$$

(к каждой комбинации безызбыточного кода дописывается комбинация, отличающаяся от нее точно в m позициях). Видно, что любая комбинация содержит точно m единиц, а $d = 2$. В биортогональных кодах обнаруживаются все ошибки, кроме ошибок, приводящих одновременно к трансформации одинакового числа нулей и единиц.

Максимальное число m -значных комбинаций веса r равно

$$M_r = (b-1)rC_m^r. \quad (4)$$

Такие множества также представляют собой равновесные коды. В бинарном случае $b=2$ их комбинации отличаются не менее чем в двух позициях, а для $b \geq 3$ кодовое расстояние равно 1.

Равновесный код применяется при передаче данных внутри устройств машины и по каналам связи. Особенностью равновесного кода является то, что в нем каждая информационная комбинация содержит фиксированное число единиц и нулей. Отличаются комбинации только позициями единиц.

Этот код получается путем добавления пятого разряда к тетраде, изображающей десятичную цифру. Код имеет высокую корректирующую способность при обнаружении асимметричных ошибок, т.е. когда происходит инверсия только единиц или только нулей. Ошибка не сможет быть обнаружена, если количество переходов нулей в единицу будет равно количеству переходов единиц в нули. Другими словами, признаком ошибки здесь является изменение количества единиц в комбинации. Избыточность равновесного кода «2 из 5» выше, чем у обычного двоично-десятичного кода. Добавление пятого разряда увеличивает число возможных комбинаций ($2^5 = 32$), однако для изображения цифр используется только 10, которые выбираются так, чтобы минимальное кодовое расстояние было равно 2. Поскольку для отображения информации используется меньше половины всех возможных комбинаций, корректирующая способность рассматриваемого кода выше, чем у обычного кода с проверкой на четность. Код «2 из 5» обнаруживает одиночные и групповые асимметричные ошибки. В некоторых машинах были попытки применить равновесный код «2 из 7». Однако резкое увеличение избыточности не повышает корректирующую способность этого кода, так как его минимальное кодовое расстояние остается тем же, т. е. равным 2. В то же время увеличение количества знаков в коде приводит к увеличению вероятности появления не обнаруживаемых симметричных ошибок.

Список литературы

1. Leech John, Sloane N.J.A. Sphere Packings and Error-Correcting Codes // *Canadian J. Mathematics*. 1971. V. 23. N4 . P. 718-745 .
2. Зиновьев В. А., Эриксон Т. Новые упаковки на евклидовой сфере для конечных размерностей // *Проблемы передачи информации*. – 1992. – Т. 28. – №. 2. – С. 47-53.
3. Додунеков С. М., Зиновьев В. А., Эриксон Т. Каскадный метод построения сферических кодов в n -размерном евклидовом пространстве // *Проблемы передачи информации*. – 1991. – Т. 27. – №. 4. – С. 34-38.
4. Зиновьев В. А., Эриксон Т. Новые нижние оценки на контактное число для небольших размерностей // *Проблемы передачи информации*. – 1999. – Т. 35. – №. 4. – С. 3-11.
5. Конвей Дж. Слоэн Н.. Упаковки шаров, решетки и группы. – Мир, 1990.
6. Юдин Н. Арифметический минимум квадратичной формы и сферические коды. – 1998.
7. Бородин Л. Ф. Введение в теорию помехоустойчивого кодирования. – 1968.

РАЗРАБОТКА ИНФОРМАЦИОННОГО ПОРТАЛА ДЛЯ ДОСТУПА ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ ОРЕНБУРГСКОЙ ОБЛАСТИ К МЕТОДИЧЕСКИМ ИНФОРМАЦИОННЫМ РЕСУРСАМ И ПРОГРАММНЫМ ПРОДУКТАМ

**Болодурина И.П., Лабузов В.А., Шухман А.Е., Полежаев П.Н.,
Ушаков Ю.А., Легашев Л.В.**

Оренбургский государственный университет, г. Оренбург

В современных сложных экономических условиях из-за серьезного повышения цен на компьютерную технику, лицензионные программные продукты и недостаточного финансирования остро встает проблема использования в школах устаревших конфигураций компьютеров и неподдерживаемых версий программных продуктов.

В августе-сентябре 2016 г. в общеобразовательных организациях Оренбургской области проведен мониторинг с целью исследовать реальный уровень использования программных продуктов в общеобразовательных организациях, определить используемые в настоящее время аппаратные и программные конфигурации компьютеров учителей и школьников.

В тестировании приняло участие 722 общеобразовательные организации из всех районов и городов Оренбургской области. Суммарное количество компьютеров, реально используемых учениками, по собранным данным составило 8820 шт. Количество компьютерных классов составило 826. В большинстве школ имеется один компьютерный класс, в 99 – два класса, в 13 школах – три класса и в одной школе (ЗАО Комаровский) – 4 компьютерных класса. Среднее количество компьютеров в компьютерном классе – 9.

Анализ применяемых операционных систем показал, что более 80% компьютеров работают под управлением различных версий Windows. При этом ОС Linux используется редко, причем, чем лучше конфигурация компьютера, тем реже применяется ОС Linux. Опыт использования программного обеспечения под Linux в обучении показывает, что основные проблемы связаны не с функционалом программ, а с недостаточно высокой квалификацией учителей и, особенно, системных администраторов. Широкое использование Linux возможно только при централизованном администрировании компьютерной техники.

Диаграммы на рис. 1 показывают процент использования различных версий Windows на компьютерах в худшей и лучшей конфигурациях.

Анализ результатов показывает, что устаревшие операционные системы Windows 2000 и Windows XP в настоящее время используются в 353 школах на компьютерах учеников и 426 школах на компьютерах учителей. Если учесть, что наиболее популярной системой в школах является Windows 7, для которой не выпускаются критические обновления с 2015 года, то можно сделать вывод, что устаревшие операционные системы в том или ином виде применяются в

89% школ, а новейшая Windows 10 – только в 15% образовательных организаций и то на новых компьютерах.

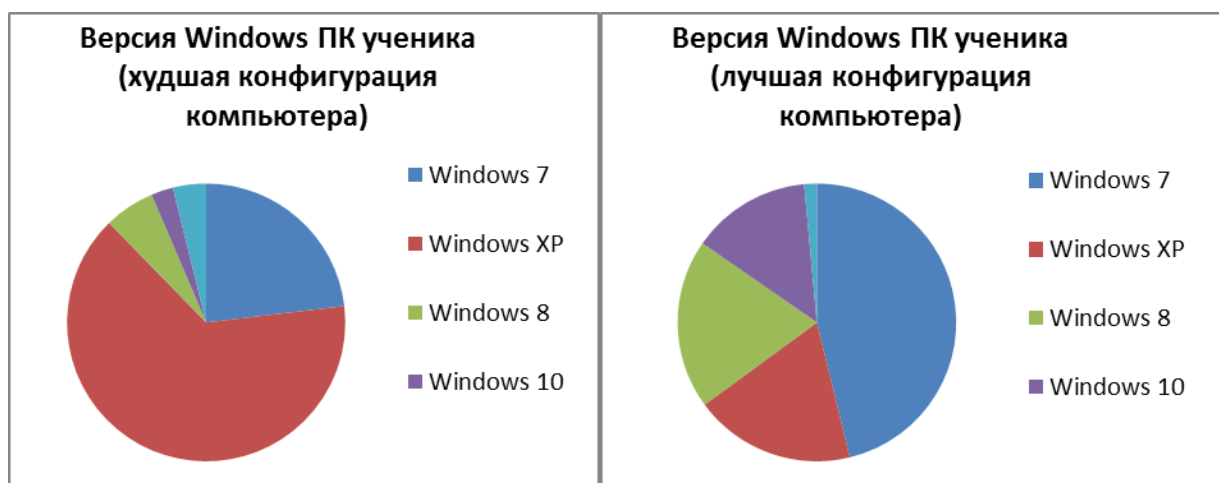


Рисунок 1 – Использование различных версий ОС Windows

Использование устаревших версий Windows опасно тем, что на них не выпускаются критические обновления, что может привести к заражению вредоносными программами. Кроме того, многое современное ПО не работает на этих версиях, например, Microsoft Office 2016, который предоставляется школам со значительной скидкой.

Основная причина использования устаревших версий Windows – устаревшие конфигурации компьютеров, поскольку достаточно долгое время переход на Windows 10 для владельцев предыдущих версий был бесплатным.

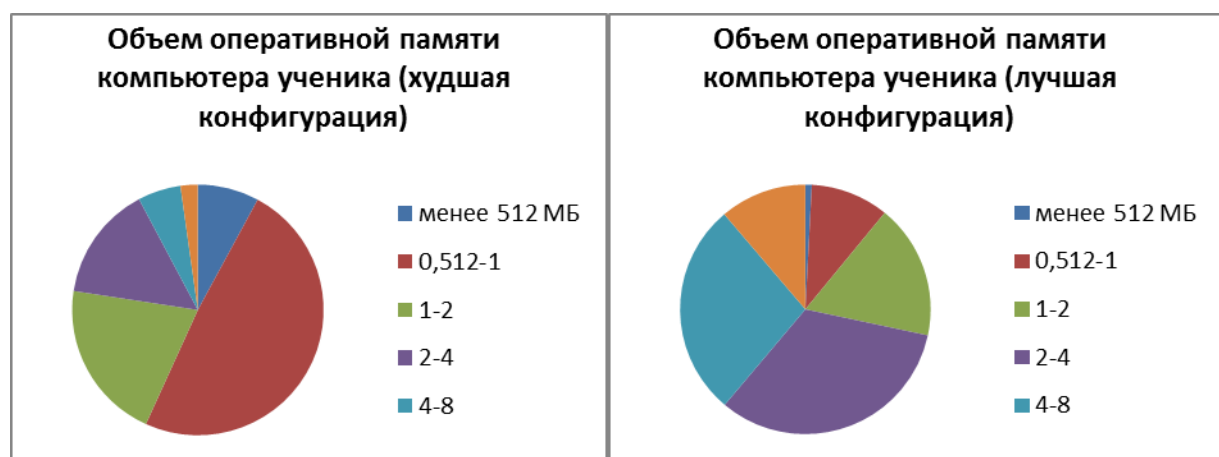


Рисунок 2 – Объем оперативной памяти

Диаграммы на рис. 2 показывают объем оперативной памяти на компьютерах в худшей и лучшей конфигурациях. К сожалению, в 6 школах еще используются компьютеры с 128 Мб ОЗУ, 26 школах – с 256 Мб ОЗУ, 351 школе – с 512 Мб ОЗУ. Объем памяти менее 1 Гб ОЗУ абсолютно неприемлем в настоящее время, потому что не позволяет использовать современные программы и информационные ресурсы. Только в 41 школе минимальная

конфигурация компьютеров имеет 3 Гб ОЗУ и более, что приемлемо для нормальной работы.

Анализ использования офисных пакетов показывает, что в большинстве школ используются устаревшие версии Microsoft Office (2003 и 2007), что связано с использованием устаревших версий Windows. Однако параллельно в 32% школ применяются бесплатные офисные пакеты OpenOffice и LibreOffice.

Проведенный анализ использования графических пакетов показывает, что в основном в школах используются бесплатные пакеты GIMP и Paint.NET. Это связано с высокой стоимостью платных продуктов от Corel и Adobe. В то же время 108 школ используют Corel Draw и 143 школы – редакторы Adobe Photoshop или Illustrator. Отметим, что для образовательных учреждений одна бессрочная лицензия CorelDRAW Graphics Suite X8 Classroom License (16 компьютеров) стоит около 30 тыс. рублей, одна годовая лицензия Adobe Photoshop на 1 компьютер стоит около 10 тыс. рублей. Таким образом, расходы на обновление используемых графических пакетов в Оренбургской области в год могут составлять до 15 млн. рублей, при том, что большинство школ не имеют возможности их закупать.

Таким образом, большинство школ до сих пор использует устаревшие компьютеры, версии операционных систем и офисных пакетов. Это сильно ограничивает возможности применения современных программных продуктов.

Решением проблемы может стать использование облачных технологий, предполагающих виртуализацию и перенос вычислительных ресурсов в центры обработки данных поставщиков облачных услуг. Облачная система может работать на основе механизма DaaS (Desktop as a Service, рабочий стол в качестве сервиса), направленного на предоставление каждому учащемуся виртуальной машины и виртуального окружения (виртуального рабочего стола) со всем необходимым для обучения установленным программным обеспечением. Доступ к виртуальному окружению осуществляется учащимися удаленно с использованием компьютеров образовательных организаций (которые могут иметь устаревшую конфигурацию) или мобильных устройств (ноутбуков, планшетных компьютеров, смартфонов).

Для сокращения издержек наиболее выгодно организовать совместное использование всеми образовательными организациями региона типовых программных конфигураций, включающих лицензии на платные продукты. При этом виртуальные ресурсы для запуска конфигураций также проще арендовать у отечественных облачных провайдеров, таких как «OneCloud», «Selectel».

Для размещения ресурсов в облаке в виде сервера Windows с удаленным доступом существуют две стратегии: размещение большого числа маломощных серверов, по одному на пользователя, либо размещение меньшего количества серверов мощных конфигураций для одновременной работы многих пользователей.

Для изучения экономически эффективной стратегии были проведены испытания комфортного количества ОЗУ и ядер для работы нескольких пользователей в офисном режиме (работа с офисным пакетом) и в высокопроизводительном режиме (работа со средами программирования и средствами моделирования). Выявлено, что стратегия размещения нескольких пользователей на одном сервере выгодней с экономической точки зрения. С учетом того, что типовое количество рабочих столов на один виртуальный класс составляет 10-12, исходя из проведенного исследования, наиболее оптимальным с точки зрения затрат является создание одного виртуального сервера на виртуальный класс.

Проведенные исследования стали основой для создания ресурсного центра коллективного доступа (РЦКД) – информационного портала www.56bit.ru для доступа образовательных организаций Оренбургской области к методическим информационным ресурсам и программным продуктам. Архитектура разработанного портала приведена на рисунке 3.

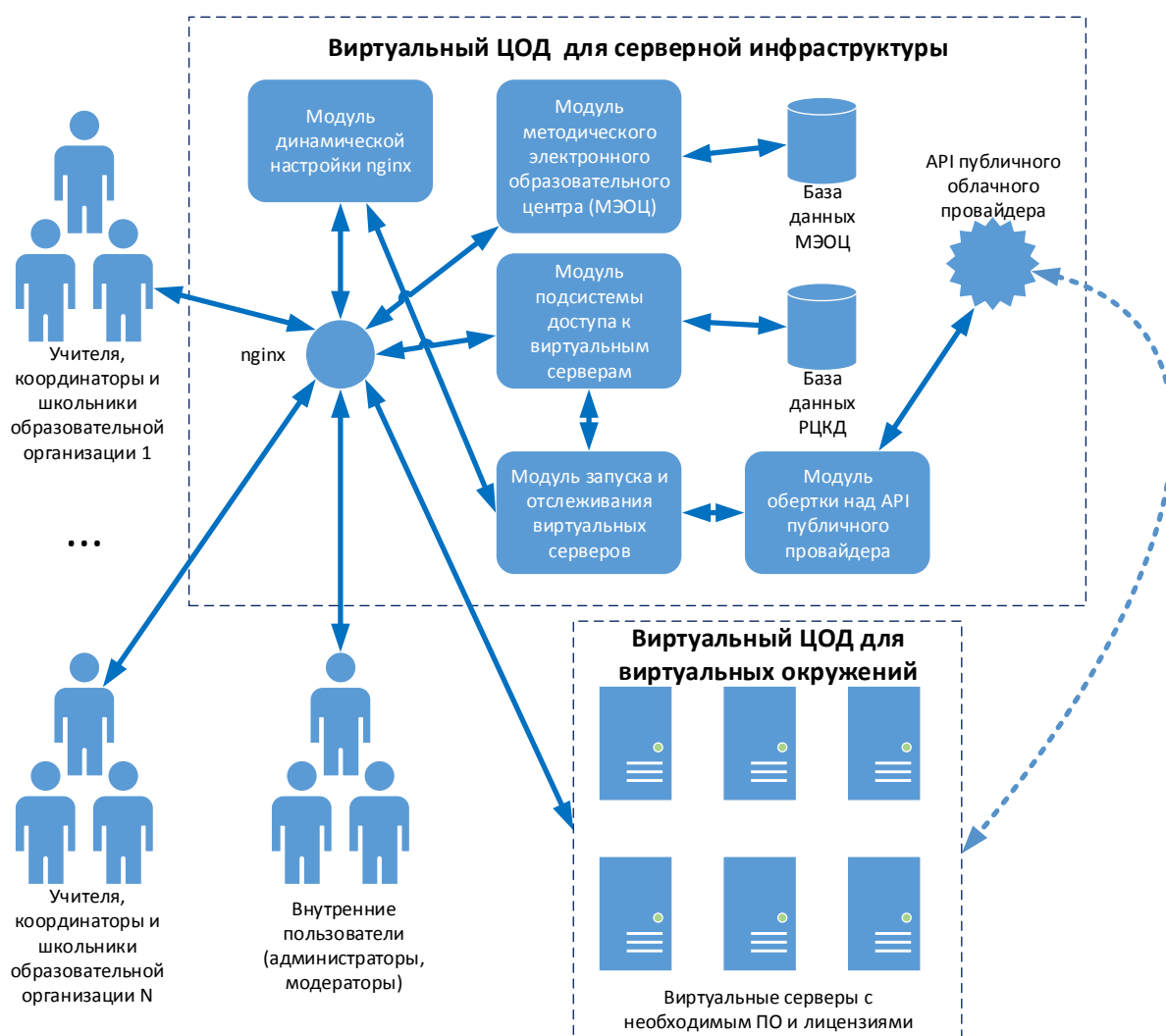


Рисунок 3 – Архитектура информационного портала www.56bit.ru

Вся система может быть развернута с использованием минимум двух виртуальных ЦОД:

а) Виртуальный ЦОД для сетевой инфраструктуры – содержит основные инфраструктурные компоненты регионального центра коллективного доступа.

б) Виртуальный ЦОД для виртуальных окружений – используется для запуска виртуальных серверов (виртуальных машин) с виртуальными окружениями для работы учителей и школьников. Подобное разделение позволяет эффективно изолировать инфраструктурные ресурсы от виртуальных окружений. Дополнительным преимуществом является отдельный биллинг, что позволяет отделить расходы на инфраструктуру от расходов на работу виртуальных окружений.

Основными инфраструктурными компонентами, изображенными на рисунке 3, являются:

а) Модуль динамической настройки nginx – осуществляет настройку доступа пользователей через nginx к виртуальным окружениям, методическому электронному образовательному центру или к подсистеме доступа к виртуальным серверам.

б) Модуль методического электронного образовательного центра (МЭОЦ) – предоставляет Web-интерфейс для доступа и размещения учебно-методических материалов, необходимых учителям для проведения занятий.

в) Модуль подсистемы доступа к виртуальным серверам – предоставляет Web-интерфейс для задания расписания занятий, формирования сведений об образовательной организации и получения доступа к виртуальным окружениям по расписанию или по требованию.

г) Модуль запуска и отслеживания виртуальных серверов – использует обертку над API публичного облачного провайдера для запуска и остановки виртуальных серверов, предоставляющих необходимые виртуальные окружения для проведения занятий.

д) Модуль обертки над API публичного облачного провайдера – единственный провайдеро-зависимый модуль системы, представляющий собой прослойку между API провайдера и модулем запуска и отслеживания виртуальных серверов. В случае смены провайдера должен переписываться только данный модуль.

е) База данных МЭОЦ – база данных, содержащая учебно-методические материалы, информацию об их авторстве, названия предметов, классы, темы и разделы.

ж) База данных РЦКД – база данных, содержащая все остальные сведения ресурсного центра коллективного доступа, включая сведения об образовательных организациях, пользователях, координаторах, учителях, расписании и т.п.

Основными пользователями портала выступают представители образовательных организаций – учителя, координаторы и школьники, а также внутренние пользователи – администраторы и модераторы.

Основными пользователями являются:

а) Ученик – пользователь по умолчанию, не имеющий учетной записи в системе. Может работать с методическими материалами, включая их просмотр, поиск и скачивание. Он также может получать доступ в созданные учителем виртуальные окружения.

б) Учитель – зарегистрированный пользователь системы, наследуется от ученика (может делать все, что и ученик). Также учитель может входить в систему и выходить из нее, просматривать расписание и работать с занятиями по требованию (создавать и отменять их). Учитель является представителем одной или нескольких образовательных организаций.

в) Координатор – зарегистрированный пользователь системы, наследуется от ученика. Координатор может входить в систему и выходить из нее, формировать расписание занятий (шаблон расписания и расписание на текущую неделю), работать с учителями (приглашать учителей, удалять и редактировать записи о них), работать с классами учеников (создавать, изменять и удалять классы), работать с расписанием звонков (создавать, изменять и удалять), редактировать описание образовательной организации. Координатор может курировать одну или несколько образовательных организаций.

г) Модератор – зарегистрированный пользователь системы, являющийся потомком ученика. Доступные действия для модератора: входить в систему и выходить из нее, формировать структуру предмета, публиковать, удалять и изменять методические материалы. Под формированием структуры предмета подразумевается работа с темами (создание, изменение и удаление), работа с разделами внутри тем (создание, изменение и удаление).

д) Администратор – зарегистрированный пользователь системы, имеющий максимальные права. Наследуется от ученика, также может входить в систему и выходить из нее, управлять пользователями (создавать в системе учетные записи координаторов и модераторов, изменять и удалять их, назначать координаторам школы, а модераторам – права доступа к предметам и классам), работать с образовательными организациями (создавать и удалять их, редактировать описание).

В рамках проекта по заказу Министерства образования Оренбургской области создана подсистема совместного доступа к виртуальным урокам, включающим учебные, текстовые и видеоматериалы, которая носит название Методического электронного образовательного центра (МЭОЦ) (схема доступа к portalу представлена на рисунке 4). Особенности портала:

- Доступ к материалам для проведения уроков по всем предметам для всех классов.
- Наглядная визуализация учебных материалов – видео, графика, инфографика, схемы, текст, презентация.
- Простота работы – получение материалов в три клика, умный поиск.

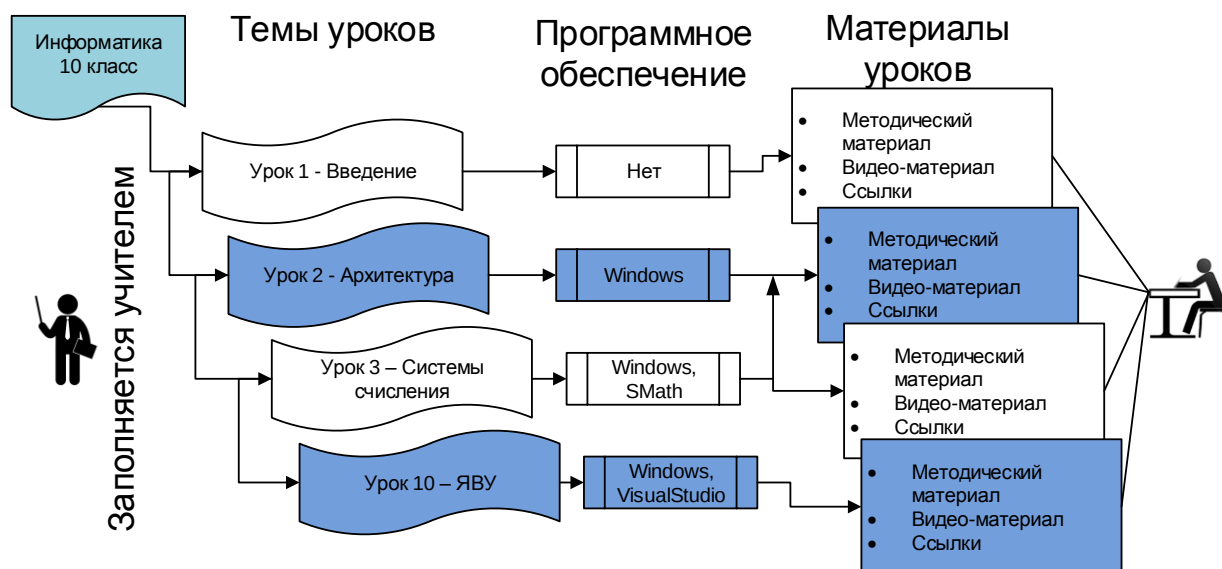


Рисунок 4 – Схема доступа к ресурсам МЭОЦ

Вся методическая информация, представленная на портале, распределяется по учебным предметам для каждого года обучения. Внутри каждого предмета для заданного года обучения с первого по одиннадцатый класс формируются разделы, каждый из которых разбивается на темы (рисунок 5).

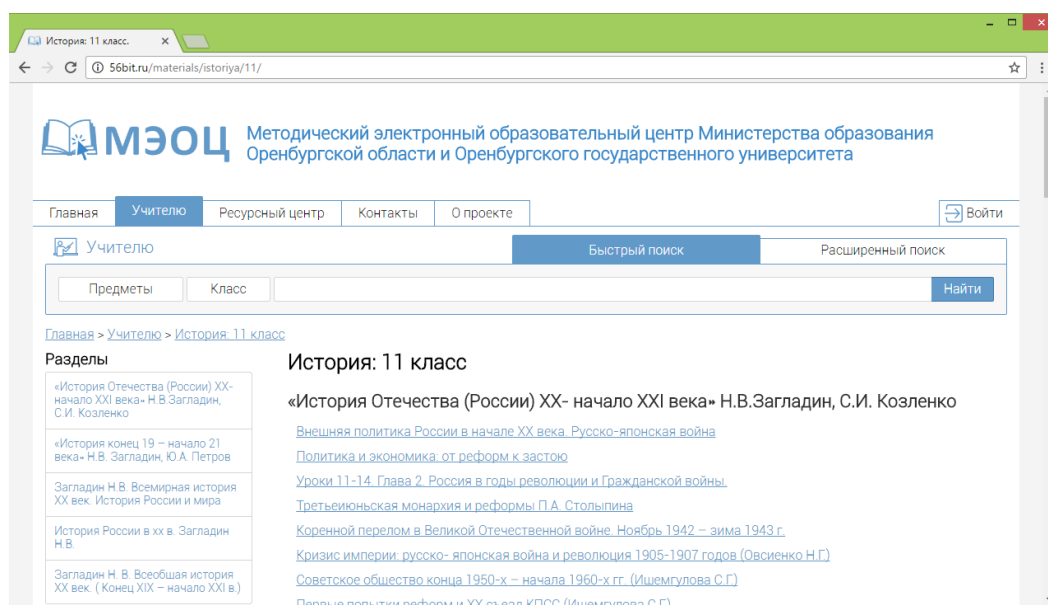


Рисунок 5 – Списки разделов и тем

Раздел обычно представляет собой главу учебника, в имени раздела указываются фамилии авторов учебника. Каждая тема обычно соответствует одному уроку в соответствии с типовым поурочным планированием. Внутри

каждой темы доступен определенный набор методических материалов, классифицированных по типу: текст, презентация, видео, вопросы, задания и другие материалы (рисунок 6).

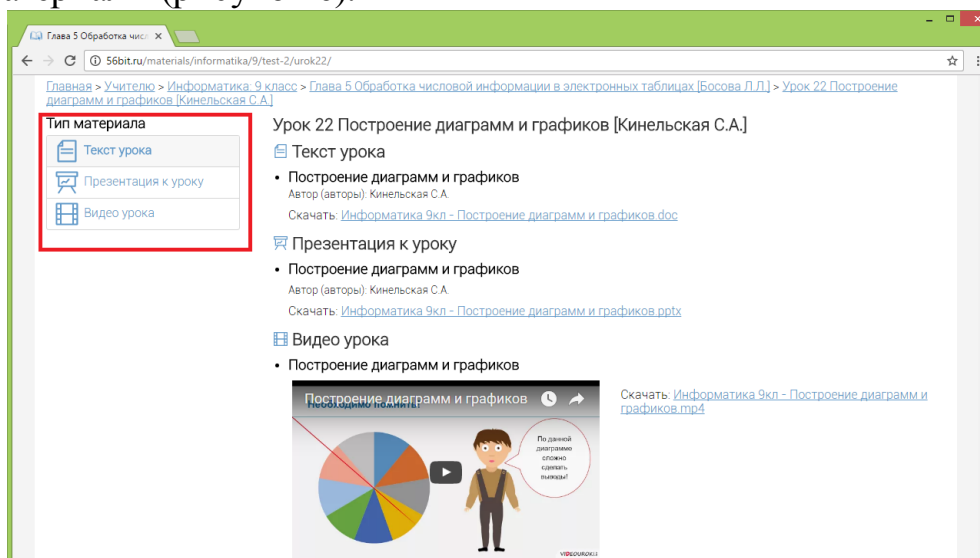


Рисунок 6 – Тема урока и методические материалы

Поиск на портале реализован как по названию, так и по полному тексту материалов. Поддерживается технология умного поиска, сразу после ввода слова выводится список тем, материалы которых содержат заданное слово. Ввод следующих слов уточняет поиск. Поддерживается технология ранжирования, которая выдвигает вперед наиболее релевантные результаты. Для удобства пользователей портал запоминает несколько последних просмотренных тем, так что к ним всегда можно быстро вернуться.

Для доступа к образовательным программным продуктам портал поддерживает два способа проведения занятий:

а) По требованию – когда учитель отправляет заявку на проведение занятия (за 10-15 минут до его начала), указывая желаемый дисковый образ с необходимым ПО, количество пользователей (включая учителя) и продолжительность занятия.

б) По расписанию – координатор образовательной организации составляет шаблон расписания, в котором описываются занятия (рисунок 7). В начале каждой недели шаблон расписания переводится в расписание текущей недели, которое при необходимости может быть изменено или уточнено координатором.

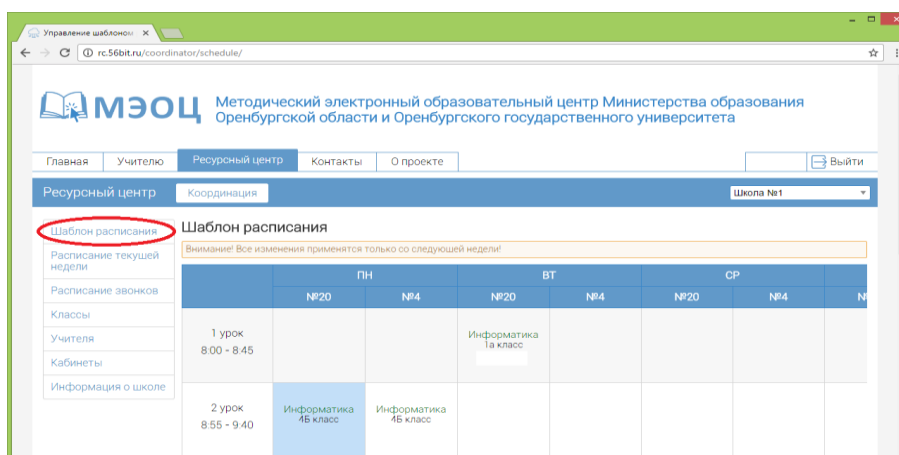


Рисунок 7 – Шаблон расписания

Для проведения каждого типа занятия заранее до начала занятия создается и запускается виртуальная машина. Для ее создания используется указанный дисковый образ с необходимым ПО, а тип виртуальной машины (количество ядер, размер оперативной и дисковой памяти) выбирается исходя из требований к ПО. После запуска виртуальной машины ученики через учителя получают код доступа и могут через браузер, пройдя авторизацию по коду, работать со своими отдельными виртуальными окружениями (рисунок 8).

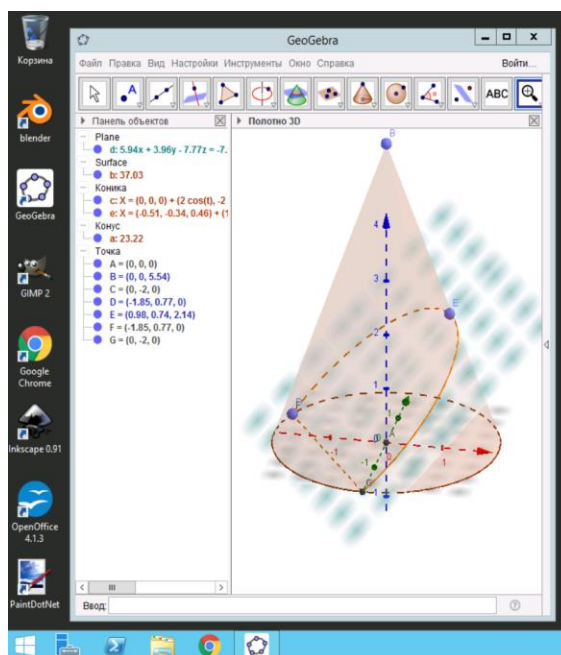


Рисунок 8 – Виртуальный рабочий стол ученика

В рамках проекта разработаны эффективные интеллектуальные алгоритмы планирования уроков виртуальных классов на основе имитации отжига и генетических алгоритмов [1-4]. Данные алгоритмы позволяют:

- составлять расписание работы виртуальных классов с учетом времени начала и окончания отдельных уроков в образовательных организациях и

пожеланий преподавателей, ведущих предметы с использованием данных классов;

- учитывать лицензионные ограничения на ПО, одновременно используемое при проведении уроков в нескольких виртуальных классах различных образовательных организаций;

- для каждого урока оптимально подбирать конфигурации виртуальных машин под рекомендуемые требования ПО, используемого на данном уроке согласно плану (при этом минимизируются расходы на оплату услуг облачных провайдеров);

- для реализации составленного расписания резервировать использование вычислительных ресурсов с указанием ПО, необходимого для урока.

Разработана технология защиты информации в РЦКД, включающая защиту инфраструктуры от внешних воздействий и защиту пользователей от нежелательного контента. Технология подразумевает установку и настройку межсетевого экрана и систем мониторинга на все узлы, установку антивируса на Windows системы, установку прокси-сервера с фильтрами для доступа в Интернет с узлов, настройку DNS на безопасный фильтрованный DNS Yandex, применение политик ограниченного использования программ, периодическое восстановление всех Windows узлов из образов, установление защищенного соединения между пользователем и компонентами РЦКД, использование разовых кодов для предоставления доступа к виртуальным окружениям.

Для тестовой эксплуатации портала проведено размещение методических материалов для 9-11 классов по 6 школьным предметам: информатике, обществознанию, истории, геометрии, алгебре, физике. На портале размещено 1103 урока, которые включают 1301 текстовый документ, 513 презентаций, 100 заданий, 24 видеоролика, 49 других материалов. Для тестовой эксплуатации подсистемы виртуальных классов в систему были добавлены координаторы 9 школ г. Оренбурга и Оренбургской области. Всего в процессе тестирования РЦКД было создано 29 занятий по требованию, 62 урока в постоянном расписании.

Проведены экспериментальные исследования эффективности, сбалансированности и производительности сервисов портала, которые позволяют сделать выводы о работоспособности системы, а также высокой эффективности системы кеширования и балансировки нагрузки. В целом, тестовая эксплуатация системы показала ее соответствие выдвинутым функциональным и нефункциональным требованиям, что позволяет считать разработку завершенной и перейти к эксплуатации системы.

Таким образом, разработанный портал полностью соответствует требованиям Министерства образования Оренбургской области и обеспечивает экономию средств за счет совместного использования лицензий на ПО, возможности использования устаревших компьютеров, упрощения обслуживания компьютеров, оплаты только фактически используемых ресурсов. Внедрение портала будет способствовать повышению качества

образования за счет использования в учебном процессе современных постоянно обновляемых программных продуктов и лучших методических материалов.

Исследования выполнены при финансовой поддержке Министерства образования Оренбургской области (грант № 37 от 30 июня 2016 г.), РФФИ (проекты № 16-07-01004, 16-47-560335), Президента Российской Федерации, стипендии для молодых ученых и аспирантов (СП-2179.2015.5).

Список литературы

1. Polezhaev P.N., Shukhman A.E., Bolodurina I.P., Ushakov Yu.A., Legashev L.V. Request Generation and Intelligent Scheduling for Cloud Educational Resource Datacenter // 2016 IEEE 8th International Conference on Intelligent Systems. – PP. 747-752.
2. Шухман А.Е., Болодурина И.П., Полежаев П.Н., Ушаков Ю.А., Легашев Л.В. Создание регионального центра коллективного доступа к образовательным программным продуктам на базе облачных технологий // Современные информационные технологии и ИТ-образование. Т. 12 (№ 3), часть 2, 2016. – С. 83-90.
3. Легашев Л.В., Болодурина И.П., Полежаев П.Н. Имитационная модель облачного ресурсного центра // Интеллект. Инновации. Инвестиции–2016–№ 2–С. 113-116.
4. Полежаев П.Н., Легашев Л.В., Шухман А.Е., Ушаков Ю.А. Алгоритмы планирования вычислений и поддержки принятия решений для облачных ресурсных центров // «Проблемы техники и технологий телекоммуникаций» ПТнТТ-2016. Материалы XVII Международной научно-технической конференции (г. Самара, 22-24 ноября 2016 г.). – Казань: ООО «16ПРИНТ», 2016. – С. 115-116.

МЕТОДОЛОГИЧЕСКИЕ ПОДХОДЫ РАЗВИТИЯ КОМПЕТЕНЦИЙ УЧИТЕЛЯ КВАЛИФИЦИРОВАННО НАБИРАТЬ МАТЕМАТИЧЕСКИЙ ТЕКСТ

Бугрова О.В.

Орский гуманитарно-технологический институт (филиал) ФГБОУ ВО
«Оренбургский государственный университет», г. Орск

В раннее проведенном исследовании была определена актуальность темы «Развитие компетенций учителя квалифицированно набирать математический текст» [1], был выявлен компонентный состав компетенций учителя квалифицированно набирать математический текст [2], [3], [4], [5].

В следующем этапе исследования определим методологические подходы развития компетенций учителя квалифицированно набирать математический текст согласно документа "ИКТ-компетентность учителей. Рекомендации ЮНЕСКО" (далее Рекомендации ЮНЕСКО) [4, с. 175].

ИКТ-компетентность учителей согласно Рекомендациям ЮНЕСКО представляется в виде матрицы компетенций, одним измерением которой являются три подхода к информатизации образовательного процесса школы, а вторым - шесть аспектов профессиональной компетентности учителя [6, с. 5]. Структура ИКТ-компетентности учителей представлена в таблице 1.

Таблица 1 - Структура ИКТ-компетентности учителей.

Шесть модулей в каждом из трех подходов	Применение ИКТ	Освоение знаний	Производство знаний
Понимание роли ИКТ в образовании	Знакомство с образовательной политикой	Понимание образовательной политики	Инициация инноваций
Учебная программа и оценивание	Базовые знания	Применение знаний	Умения жителя общества знаний
Педагогические практики	Использование ИКТ	Решение комплексных задач	Способность к самообразованию
Технические и программные средства ИКТ	Базовые инструменты	Сложные инструменты	Распространяющиеся технологии
Организация и управление образовательным процессом	Традиционные формы учебной работы	Группы сотрудничества	Обучающаяся организация
Профессиональное развитие	Компьютерная грамотность	Помощь и наставничество	Учитель как мастер

Первый методологический подход "Применение ИКТ" требует от учителей тех компетенций, которые ориентированы на оказание помощи в использовании ИКТ в учебной деятельности. Второй методологический подход

"Освоение знаний" требует от учителей наличие таких компетенций, которые ориентированы на глубокое освоение содержания учебных предметов учащимися и применение полученных знаний. Третий методологический подход "Производство знаний" ориентирован на наличие тех компетенций у учителей, которые направлены на оказание помощи учащимся в научно-исследовательской деятельности, в ходе которой ученики становятся участниками получения «новых знаний».

Для определения какой из трех подходов к информатизации образовательного процесса школы является наиболее целесообразным и с целью уточнения компонентного состава компетенций учителя квалифицированно набирать математический текст, а также для определения готовности учителями квалифицированно набирать математический текст был проведен второй этап констатирующего эксперимента с 38 учителями - слушателями курсов повышения квалификации по дополнительным профессиональным образовательным программам повышения квалификации и переподготовки на базе Орского гуманитарно-технологического института (филиала) федерального государственного бюджетного образовательного учреждения высшего образования «Оренбургский государственный университет». Мнения участников анкетирования учитывались также анонимно, как и в первом этапе констатирующего эксперимента для использования в обобщенном виде исключительно в исследовательских целях [2], [3].

Слушателям программы был предложен комплекс вопросов, состоящий из двух частей. Первая часть - это анкета с открытыми вопросами, предполагающая заполнение в письменном виде. Вторая часть - задания, предполагающие выполнение с помощью компьютера. Комплекс вопросов был разработан в соответствии с Рекомендациями ЮНЕСКО.

Анализ ответов на вопросы из I части показал, что учителя понимают, что такое ИКТ-компетентность педагога, но в профессиональной деятельности ИКТ-компетентность педагогов проявляется слабо: в использовании средств ИКТ некоторыми учителями используются видео-уроки, средства сети Интернет, интерактивные разработки, дистанционная работа. В индивидуальной работе с учениками используется тестирование с помощью компьютера в дистанционной форме, в групповой работе - интерактивная доска. Из компьютерных программных средств употребляются только текстовый редактор MS Word, табличный процессор MS Excel и приложение для показа презентаций MS PowerPoint. Учебные мероприятия по математике не проводятся в компьютерных классах. На изучение возможностей компьютерных математических программных средств (в большей части ответов) не хватает времени.

По ответам на вопросы, касающихся квалифицированного набора математического текста, можно сделать следующие выводы: узкое понимание определения "математический текст" и понятия "квалифицированно набирать

математический текст", ограниченное знание и применение математических компьютерных программных средств.

Анализ выполненных заданий из II части показал слабое пользовательское владение компьютерными программными средствами. Учителя работали только в одной программе приложения MS Office – MS Word (набор математического текста с помощью конструктора формул, конструктора при работе с диаграммами и функциями, средств рисования). При наборе математического текста также было выявлено незнание обозначений математических терминов.

Всё это говорит о необходимости разработки дополнительной профессиональной образовательной программы повышения квалификации, ориентированной на развитие компетенций учителя квалифицированно набирать математический текст в рамках подходов к информатизации образовательного процесса школы "Применение ИКТ" (для учителей, имеющих базовые навыки работы с компьютером) и "Освоение знаний" (для учителей, использующих ИКТ в своей профессиональной деятельности и желающих использовать их более эффективнее), поскольку данные подходы являются наиболее целесообразными (основываясь на слабом пользовательском владении учителями средствами ИКТ и применении некоторыми учителями в своей профессиональной деятельности информационных технологий, согласно проведенного комплекса вопросов с учителями).

Данные второго этапа констатирующего эксперимента и структура ИКТ-компетентности учителей согласно Рекомендациям ЮНЕСКО позволили выявить систему компетенций учителя квалифицированно набирать математический текст. Данная система компетенций представлена в таблице 2 для методологических подходов "Применение ИКТ" и "Освоение знаний".

Таблица 2 – Компонентный состав компетенций учителя квалифицированно набирать математический текст

Компетенции учителя квалифицированно набирать математический текст	№	Методологические подходы	Компетенции	Содержание компетенции
	1	Применение ИКТ, Освоение знаний	Компетенция учителя знакомиться и понимать образовательную политику в процессе развития компетенций учителя квалифицированно набирать математический текст	Мотивом к развитию данной компетенции будем считать желание учителей быть хорошими и ответственными работниками, поддерживать образовательную политику государства. А для этого необходимы открытость и готовность воспринимать новые идеи. Выполнение поставленных задач по реализации долгосрочных целей и задач социально-экономического развития Российской Федерации невозможно без высокого уровня математической науки, математического образования и математической грамотности всего населения. Концепция развития математического образования в Российской Федерации обозначает основные проблемы развития математического

			образования, одной из которых является проблема кадрового характера. В Российской Федерации не хватает учителей и преподавателей образовательных организаций высшего образования, которые могут качественно преподавать математику, учитывая, развивая и формируя учебные и жизненные интересы различных групп обучающихся. Система дополнительного профессионального образования преподавателей недостаточно эффективна и зачастую просто формальна в части совершенствования математического образования. Все это нашло отражение в профессиональном стандарте "Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель)" (далее - профессиональный стандарт "Педагог"). Согласно ему одним из необходимых умений для осуществления педагогической деятельности является умение квалифицированно набирать математический текст [7].
2	Применение ИКТ, Освоение знаний	Компетенция учителя включать в образовательный процесс соответствующие средства ИКТ для квалифицированного набора математического текста и оценивания образовательных результатов	Данная компетенция включает в себя поиск соответствующего инструментального программного обеспечения для квалифицированного набора математического текста, освоение этого программного обеспечения учителями, включение средств ИКТ в образовательный процесс, прогнозирование ожидаемых результатов применения программного обеспечения. При оценивании образовательных результатов учащимся предъявляются результаты учебной работы с помощью средств ИКТ с квалифицированно набранным математическим текстом (например, автоматизированный подсчет результатов, сбор и анализ данных, быстрая демонстрация полной информации).

	3	Применение ИКТ, Освоение знаний	Компетенция учителя целесообразно включать средства соответствующих ИКТ в образовательный процесс для квалифицированного набора математического текста и оценивания образовательных результатов	Рассматриваемая компетенция включает в себя знание преимуществ и недостатков использования ИКТ при традиционных методах учебной работы (в работе на уроке индивидуально или в группе, в домашней работе, в краткосрочных и длительных проектах, при работе с цифровыми учебными материалами). Для целесообразного включения средств ИКТ в образовательный процесс при квалифицированном наборе математического текста необходимо точно определять цели обучения, рассматривать весь спектр цифровых инструментов, оценивать эффективность их использования, спонтанно использовать средства ИКТ ("здесь и сейчас"). При оценивании образовательных результатов учащимся предъявляются результаты учебной работы с помощью средств ИКТ с квалифицированно набранным математическим текстом (например, автоматизированный подсчет результатов, сбор и анализ данных, быстрая демонстрация полной информации).
	4	Применение ИКТ	Компетенция учителя владеть базовыми приемами работы с техническими и программными средствами для квалифицированного набора математического текста (для учителей, имеющих базовые навыки работы с компьютером)	Для рассматриваемой компетенции определим следующие задачи: овладение базовыми приемами работы с ИКТ для квалифицированного набора математического текста, оценка эффективности использования технических средств и устройств для достижения поставленных целей; оценка необходимости использования Интернета для проведения занятий; изучение имеющегося программного обеспечения, которое помогает достичь запланированных результатов.
		Освоение знаний	Компетенция учителя работать с ИКТ в своей профессиональной деятельности для достижения более	Для рассматриваемой компетенции определим следующие задачи: овладение приемами работы с ИКТ для достижения более эффективных результатов при наборе квалифицированного математического текста, оценка эффективности использования технических средств и устройств для достижения поставленных целей; оценка необходимости использования Интернета для проведения занятий; изучение имеющегося программного обеспечения, которое помогает

		эффективных результатов, используя квалифицированный набор математического текста (для учителей, владеющих навыками работы с ИКТ)	достичь запланированных результатов, применение ИКТ для сотрудничества и общения.
5	Применение ИКТ	Компетенция учителя организовать работу с учащимися, используя квалифицированный набор математического текста	Данная компетенция предполагает разработку учебных занятий, которые можно проводить в компьютерном классе, используя квалифицированный набор математического текста; организацию индивидуальной, групповой и фронтальной работы учащихся с использованием средств ИКТ; отличие подходящих и неподходящих организационных условий для использования различных средств ИКТ.
	Освоение знаний	Компетенция учителя организовать работу с учащимися, группами сотрудничества, применяя квалифицированный набор математического текста	Данная компетенция предполагает разработку учебных занятий, которые можно проводить в компьютерном классе, используя квалифицированный набор математического текста; организацию индивидуальной, групповой и фронтальной работы учащихся с использованием средств ИКТ; отличие подходящих и неподходящих организационных условий для использования различных средств ИКТ; а также организовывать работу с преподавателями из других образовательных учреждений (группы сотрудничества, применяя квалифицированный набор математического текста)
6	Применение ИКТ	Компетенция учителя совершенствовать навыки работы с ИКТ и изучать новые ИКТ для квалифицированного набора математического текста	В рамках данной компетенции можно определить: как квалифицированный набор математического текста с помощью средств ИКТ может повысить производительность труда учителя; какую роль квалифицированный набор математического текста с помощью средств ИКТ сыграет в профессиональном развитии педагога. Рассматриваемая компетенция предполагает расширение знаний в области методики преподавания по своему предмету; использование средств ИКТ, способствующих профессиональному развитию и навыкам работы для квалифицированного набора математического текста

		Освоение знаний	Компетенция учителя совершенствовать работу с ИКТ и изучать новые ИКТ для квалифицированного набора математического текста	В рамках данной компетенции можно определить: как квалифицированный набор математического текста с помощью средств ИКТ может повысить производительность труда учителя; какую роль квалифицированный набор математического текста с помощью средств ИКТ сыграет в профессиональном развитии педагога. Рассматриваемая компетенция предполагает применение ИКТ для работы с коллегами по всему миру; дистанционное и виртуальное обучение; изучение учебных материалов; расширение знаний в области методики преподавания по своему предмету; использование средств ИКТ, способствующих профессиональному развитию и совершенствованию работы для квалифицированного набора математического текста.
--	--	------------------------	--	--

Выделенная система компетенций в проведенном теоретико-эмпирическом исследовании требует уточнения на практике и анализа выделенных компетенций в совокупности.

Список литературы:

1. Бугрова, О.В. Развитие умений учителя квалифицированно набирать математический текст в условиях дополнительного профессионального образования: перспективы/ О.В. Бугрова, Т.И. Уткина // Евразийский Союз Ученых. – 2015. - № 6(15). – С. 69-70.
2. Бугрова, О.В. Структура компетенций учителя относительно грамотного набора математического текста. / О.В. Бугрова // Университетский комплекс как региональный центр образования, науки и культуры [Электронный ресурс] : материалы Всерос. науч.-метод. конф., Оренбург 3-5 февр. 2016 г. / Оренбург. гос. ун-т. – Электрон. дан. – Оренбург : ОГУ, 2016. – 1 электрон. опт. диск (CD-ROM). – ISBN 978-5-7410-1385-4.
3. Бугрова, О.В. О грамотности учителей относительно набора математического текста. / О.В. Бугрова // Материалы МНПК «Интеграционные процессы в науке в современных условиях». – Прага, Чехия: Издательство «Мир науки», 2016. - с. 10-15.
4. Бугрова, О.В. Об уточнении структуры и содержания компетенций учителя квалифицированно набирать математический текст. / О.В. Бугрова // Материалы XXXV Международного научного семинара преподавателей математики и информатики университетов и педагогических вузов «Стандартизация математического образования: проблемы внедрения и оценка эффективности». – Ульяновск: УлГПУ, 2016. - с. 172-179.

5. Бугрова, О.В. О единице развития компетенций учителя квалифицированно набирать математический текст. / О.В. Бугрова // Материалы III Международной научной конференции, 17 – 19 ноября 2016 г. «Актуальные проблемы обучения математике и информатике в школе и вузе в свете идей Л.С. Выготского». - Под ред. М.В. Егуповой, Л.И. Боженковой – ФГБОУ ВО «Московский педагогический государственный университет» (МПГУ), Издатель Захаров С.И. («СерНа»), 2016 . – с. 143-148. - ISBN 978-5-905849-50-3.

6. Структура ИКТ-компетентности учителей. Рекомендации ЮНЕСКО. [Электронный ресурс] / UNESCO, 2011. - 115 с. - Режим доступа: <http://iite.unesco.org/pics/publications/ru/files/3214694.pdf> (дата обращения: 09.12.2016).

7. Профессиональный стандарт "Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования)(воспитатель, учитель)" [Электронный ресурс], утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 18 октября 2013 г. № 544н, 2013. – 24 с. - Режим доступа: <http://fgosvo.ru/uploadfiles/profstandart/01.001.pdf> (дата обращения: 09.12.2016).

КАТЕГОРИРОВАНИЕ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ ДЛЯ ВЫБОРА СРЕДСТВ ФИЗИЧЕСКОЙ ЗАЩИТЫ

Бурькова Е.В.

Оренбургский государственный университет, г. Оренбург

Организация физической защиты объектов информатизации в современных условиях роста угроз терроризма, несанкционированного доступа к ценным ресурсам, их кражи или нанесения повреждений, является важной задачей. При этом системы физической защиты объектов нуждаются в проведении периодической оценки эффективности их функционирования и последующей модернизации. Обоснованность требований к применяемым средствам физической защиты при их выборе позволит оптимизировать систему физической защиты, преодолеть избыточность или недостаточность с учетом анализа угроз безопасности, значимости объекта и ценности защищаемых ресурсов.

Для обеспечения корректности технических требований при проектировании систем физической защиты необходимо провести категорирование защищаемого объекта. Существующие требования нормативных документов в основном сосредоточены на защите потенциально опасных объектов: топливно-энергетического, оборонно-промышленного и транспортного комплекса Российской Федерации. Между тем, все более обостряется необходимость осуществления физической защиты объектов, находящихся за рамками этого перечня.

Понятия «категория и защищенность охраняемого объекта» введены ГОСТ Р 50776-95 (МЭК 60839-1-4:1989) «Системы тревожной сигнализации». Категория охраняемого объекта - это комплексная оценка состояния объекта, учитывающая его экономическую или иную (например, культурную) значимость в зависимости от характера и концентрации сосредоточенных ценностей, последствий от возможных преступных посягательств на них, сложности обеспечения требуемой надежности охраны.

Цель категорирования на современном этапе была сформулирована как «создание системы категорирования, предполагающей дифференциацию требований к системе антитеррористической и противокриминальной защиты объектов, обеспечивающей минимально необходимые и достаточные уровни безопасности объектов в соответствии с их категориями потенциальной опасности, с учетом критериев оценки возможного ущерба интересам личности, общества и государства, который может быть нанесен преступными действиями в случае невыполнения требований, предъявляемых к системе защиты объекта» [3].

Критерии, которые должны быть учтены при категорировании объектов, проанализированы в источниках [1,2,3,5] включают такие важные характеристики, как потенциальная опасность, значимость объектов по

функционально-отраслевым признакам, вид и величина ущерб от аварий чрезвычайных ситуаций, численность персонала, материальные активы, наличие пожаро- и взрывоопасных веществ и другие. Все критерии можно разделить на три группы: качественные, количественные и критерии значимости по функционально-отраслевым признакам. Классификация критериев категорирования объектов представлена на рисунке 1.



Рисунок 1 – Классификация критериев категорирования объектов

Качественные критерии подразумевают классификацию объектов на три группы: особо важные, важные и простые. Особо важные, повышенной опасности и жизнеобеспечения, противоправные действия на которых могут привести к крупному ущербу государству, экологии или владельцу имущества (группа А). Важные объекты (группа Б), хищения на которых могут привести к ущербу в размере свыше 500 МРОТ. Простые объекты, последствия от реализации угроз на которых средний материальный или финансовый ущерб, информационный ущерб коммерческого или служебного рода, нарушение комфортности личной жизни или служебной деятельности. Руководящий документ РД 78.36.003-2002 устанавливает такую классификацию и предъявляет требования по организации физической защиты объектов, также

приводятся основные типы извещателей, обеспечивающих защиту от криминальных воздействий.

Количественные критерии позволяют вычислить размеры возможного ущерба в виде людских потерь, территориальных и материальных потерь и их стоимостное выражение.

Критерии по функционально-отраслевым признакам определяют такие виды потерь как: политические, людские, финансовые, экономические, экологические и культурные.

При проектировании зданий и сооружений различного функционального назначения в первую очередь учитываются требования технической укреплённости и пожарной безопасности на основе требований СП 12.13130.2009 «Определение категорий помещений, зданий и наружных установок по взрывопожарной и пожарной опасности». В зависимости от категории объекта устанавливаются требования к мероприятиям и средствам физической защиты, для этого используются следующие документы: Р 78.36.007-99. «Выбор и применение средств охранно-пожарной сигнализации и средств технической укреплённости для оборудования объектов. Рекомендации»; РД 78.36.003-2002 «Инженерно-техническая укреплённость. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств»; СП 132.13330.2011 «Обеспечение антитеррористической защищённости зданий и сооружений. Общие требования проектирования. Свод правил», нормативные документы по категориям и защищённости объектов от краж и другие руководящие документы.

Основные методики категорирования объектов проанализированы в статье [5]: методика категорирования опасных производственных объектов ФГУП НТЦ «Промышленная безопасность», методика общегосударственного категорирования объектов «НПП «ИСТА-Системс». В последней методике для оценок уровня потерь применяются экспертные методы и формируется интегральный показатель потерь. Данная методика позволяет использовать результаты категорирования устанавливая значения эффективности проектируемой системы физической защиты.

Уровень эффективности функционирования системы физической защиты зависит от категории объекта, и основными результатами категорирования является оценка соответствия характеристик системы физической защиты требованиям, предъявляемым к категории этого объекта. Категорирование защищаемых объектов проводится для формирования количественных и качественных требований к системе физической защиты, так как на основании установленной категории объекта можно сформулировать такие требования:

- количество рубежей охраны, количество охраняемых зон;
- вид ограждения территории;
- оборудование КПП;
- наличие СКУД;
- виды защиты окон, виды замков;
- наличие видеонаблюдения;
- наличие автоматического пожаротушения;
- наличие средств индивидуальной защиты.

Для реализации выбора физических средств защиты основным критерием является вид, размеры и стоимостное выражение возможного ущерба. Рост затрат на систему физической защиты с превышением оптимального значения приводит к повышению суммарных затрат, и повышение надежности системы физической защиты становится неоправданно на практике. При формировании структуры СФЗ объекта кроме его категории необходимо также учитывать возможности потенциальных нарушителей, причем не только посторонних лиц, но и уволенных или работающих сотрудников [4]. В современной реальности мы имеем дело с технически грамотными нарушителями, которые основательно оснащены различными техническими средствами, имеют различную степень осведомленности об объекте и степень подготовленности. Построение модели нарушителя и модели угроз является обязательным этапом при проектировании СФЗ объекта.

В настоящее время для определения оптимального состава системы физической защиты используют имитационное моделирование функционирования СФЗ, в результате которого получают оценку эффективности предложенной конфигурации СФЗ. Имитационная модель включает объект, систему угроз и систему защиты, состоящую из подсистем обнаружения, задержки и нейтрализации угроз. Моделирование проводится на основе использования математических методов процесса анализа и оптимального проектирования систем физической защиты.

Таким образом, проведение тщательного анализа категории защищаемого объекта по количественным и качественным критериям, опираясь на нормативно-правовые документы; формирование интегрального показателя категорирования и использование имитационного моделирования функционирования СФЗ являются важными этапами при выборе средств физической защиты в процессе проектирования СФЗ объектов информатизации.

Список литературы

1 Бочков, А. Категорирование критически важных объектов по уязвимости к возможным противоправным действиям. Экспертный подход. /А.Бочков // *Безопасность. Достоверность. Информация.* - № 1, -2009.- С.22-24.
Вишняков, С. М. Системы комплексной безопасности, категории и уровни защищенности стационарных объектов.//*Системы безопасности.* - №1. - 2004. – С.26-32.

2 Зайцев, А. Категорирование объектов. / А. Зайцев // *Алгоритм безопасности.* - №6. – 2006 . - С.7-9.

3 Коновалов, В.А. Категорирование объектов. Ключевой фактор обеспечения эффективности систем комплексной безопасности. / В.А. Коновалов, Д.В. Севрюков, Р.С. Хасянов. [Электронный ресурс].– Режим доступа: http://www.secuteck.ru/articles2/kompleks_sys_sec/kategorirovanie_obiektov.

4 Панин, О. Категорирование объектов для создания эффективных систем физической защиты./ О.Панин // *Безопасность. Достоверность. Информация.* - № 70. – 2007. - С. 20-24.

АНАЛИЗ ПОДХОДОВ К АУДИТУ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Бурькова Е.В., Хрыкина Н.А.

Оренбургский государственный университет, г. Оренбург

Защита персональных данных на современном этапе развития информационного общества приобретает все большую значимость. Это связано с проникновением информационных технологий во все сферы нашей жизни, человек становится частью интернет-пространства, он окружен интеллектуальными мобильными устройствами, повсеместным видеонаблюдением; в организациях и фирмах практически все процессы обработки персональных данных автоматизированы. Возможности для сбора, хранения и обработки информации расширяются и становятся доступными для широкого круга лиц [5]. В этих условиях становится целесообразным осуществление регулярного аудита защищенности персональных данных, обрабатываемых в информационных системах. Аудит защищенности ИСПДн направлен на обеспечение прав и свобод человека и гражданина при обработке его персональных данных, общественных и государственных интересов, соблюдения законных интересов лиц, использующих персональные данные в своей деятельности, укрепления правовой защищенности и безопасности личности граждан Российской Федерации.

Аудит защищенности проводится с целью установления степени выполнения требований по обеспечению состояния защищенности ИСПДн. Результаты аудита могут указывать на соответствие или несоответствие критериям аудита или указывать на принятие мероприятий по модернизации системы защиты ПДн организации. Суть аудита сводится к оценке защищенности ИСПДн.

Согласно ГОСТ Р ИСО 19011-2012 «Руководящие указания к аудиту систем менеджмента», процедура оценки защищенности проводится как в «ручном» режиме так и в автоматизированном с привлечением специальных программных комплексов оценки защищенности и рисков, реализующих различные методики.

При проведении анализа литературы по этой теме были выделены следующие подходы к аудиту защищенности ИСПДн: формальный, классификационный, категоризованный, количественные оценки рисков, качественные оценки защищенности, комплексные оценки защищенности ИС. Наиболее распространены количественный и качественный подходы к аудиту защищенности информационных систем.

На основе анализа источников [1,2,4] была построена классификация подходов к аудиту защищенности ИС, представленная на рисунке 1.



Рисунок 1 – Классификация подходов к аудиту защищенности ИСПДн

В количественном подходе для описания риска используется двухмерная характеристика: степень риска и цена риска. Степень риска количественно характеризует вероятность негативных результатов принятого решения. Цена риска дает количественную характеристику вероятных потерь.

Количественная оценка рисков применяется в ситуациях, когда исследуемые угрозы и связанные с ними риски можно сопоставить с конечными количественными значениями ущерба, выраженным в деньгах, процентах, времени, человеко-ресурсах.

Подход количественной оценки защищенности информационных систем включает в себя:

- экспертные оценки информационной безопасности, в основе которых лежит понятие профиля защиты стандарта ISO/IEC 15408. ГОСТ Р ИСО/МЭК 15408 определяет «Общие критерии», которые предназначены для использования в качестве основы при оценке характеристик безопасности средств и систем информационных технологий;
- построение модели нарушителя и модели угроз для предприятия;

- алгоритм распределения функций безопасности с учетом всех видов информационных потоков, находящихся в оцениваемой ИС (защита от внешних воздействий (со стороны Интернета), защита от внутренних атак);
- графовый метод оценки защищенности;
- анкетирование субъектов отношений, которые служат для уяснения направленности деятельности предприятия, предполагаемых приоритетов целей безопасности, задач, решаемых ИС и эксплуатации ИС. [4]

Сущность графового метода оценки защищенности состоит в построении оценки защищенности объектов на основе характеристик защитных механизмов (ЗМ) для этого объекта и определении достаточности системы ЗИ.

Объект исследования представляется в виде графа, вершинами которого являются «модули защиты» и защищаемые объекты, а связи – это возможные пути продвижения нарушителя. Модуль защиты – это некоторый конечный результат разложения системы защиты, который можно представить в виде элемента задержки. Таким образом, получившийся граф позволяет проследить возможные пути продвижения «нарушителя» к защищаемому объекту. Вершина графа, характеризующая «модуль защиты», обладает временем задержки, имеет выходы (ребра графа). Вероятность всех выходящих из одной вершины ребер равна единице.

Количественная оценка цены риска может определяться абсолютным или относительным уровнем потерь. В абсолютном выражении риск может определяться величиной возможных потерь в физическом (натурально-вещественном) или стоимостном (денежном) выражении. В относительном выражении риск определяется как отношение величины возможных потерь к некоторой базе, например, капиталу, суммарным издержкам или прибыли.

При качественном подходе не используются количественные или стоимостные выражения для объекта оценки. Вместо этого объекту оценки присваивается показатель, проранжированный по трехбалльной, пятибалльной или десятибалльной шкале (низкий, средний, высокий). Для сбора данных при качественной оценке рисков применяются опросы целевых групп, личные встречи. Качественный подход к аудиту защищенности ИСПДн реализован в программе оценки рисков «Гриф». [3]

Подход качественной оценки систем анализа защищенности ИС организации включает:

- сбор и изучение исходных данных по ИС;
- оценку рисков, связанных с осуществлением угроз безопасности в отношении средств предприятия;
- анализ политики безопасности предприятия и организационно-распорядительной документации по обеспечению ИБ
- оценка организационно-распорядительной документации соответствия требованиям существующих нормативных документов;
- тестирование систем ИБ включает в себя проверку эффективности механизмов защиты и поиск уязвимостей. [2]

Анализ рисков начинается с формализации системы приоритетов организации в области ИБ. Для оценки ценности ресурсов необходимо выбирать подходящую систему критериев. Критерии должны позволять описать потенциальный ущерб, связанный с нарушением конфиденциальности, целостности, доступности. Анализ рисков информационной безопасности качественным методом должен проводиться с привлечением сотрудников, имеющих опыт и компетенции в той области, в которой рассматриваются угрозы.

Тестирование системы защиты проводится для проверки эффективности используемых в ней защитных механизмов, их устойчивости к атакам, а также с целью поиска уязвимостей. Традиционно используются два основных метода тестирования: по методу «черного ящика» и по методу «белого ящика». Тестирование по методу «черного ящика» предполагает отсутствие у тестирующей стороны каких-либо специальных знаний о конфигурации и внутренней структуре объекта испытаний. Против объекта испытаний реализуются все известные типы атак.

Метод «белого ящика» предполагает составление программы тестирования на основании знаний о структуре и конфигурации объекта испытаний. В ходе тестирования проверяется наличие и работоспособность механизмов безопасности, соответствие состава и конфигурации системы защиты требованиям безопасности и существующим рискам. Выводы о наличии уязвимостей делаются на основании анализа конфигурации используемых средств защиты и системного программного обеспечения, а затем проверяются на практике.

Количественная оценка позволяет определить числовое выражение вероятности возникновения рисков и их влияние на проект.

Нами был проведен сравнительный анализ подходов, результат которого представлен в таблице 1. Каждый из подходов имеет свои преимущества и недостатки, сложность и особенности реализации, а также форму представления показателя общей защищенности систем.

Таблица 1 – Сравнительная характеристика подходов к аудиту защищенности

Наименование подхода	Преимущества	Недостатки
Качественная оценка систем ИБ	Простота применения. Применимость для прогнозирования практически любых ситуаций. Выявление качественного соответствия или несоответствия системы ИБ определенным требованиям, проверка	Не применяется в условиях неполной информации. Практическая реализация данного подхода является затруднительной.
Количественный подход к аудиту защищенности	Показывает характеристики существующих механизмов защиты на исследуемой ИС, определяет достаточность системы защиты информации. Степень риска количественно характеризует вероятность негативных	Отсутствуют гарантии, что полученные в результате опроса экспертов данные достоверны. Существуют трудности в проведении

	результатов принятого решения. Цена риска дает количественную характеристику вероятных потерь.	опроса экспертов и обработке полученных результатов
--	--	---

Таким образом, в результате проведенной работы была дана характеристика подходов к аудиту защищенности, проанализированы подходы к аудиту защищенности. Количественный подход к аудиту защищенности более выгоден в применении, ввиду практичности и преимуществ, превосходящих в количестве положительные характеристики качественной оценки. Аудит ИСПДн является эффективным инструментом для получения данных о текущем уровне защищенности от угроз информационной безопасности и позволяет повысить уровень защищенности ИСПДн.

Список литературы

1. Бурькова, Е.В. Задача оценки защищенности информационных систем персональных данных / Е.В. Бурькова // Вестник Чувашского университет. – Чебоксары, 2016. - № 1. – С. 112-118. ISSN: 1810-1909
2. Методика оценки рисков информационной безопасности [Электронный ресурс]: Контур – Электрон. журн. – Москва, 2015. – Режим доступа: <https://kontur.ru/articles/1691> (дата обращения: 11.12.2016).
3. Современные методы и средства анализа и управление рисками информационных систем компаний [Электронный ресурс]: Безопасность как искусство – Электрон. журн. – Москва, 2015. – Режим доступа: https://dsec.ru/ipm-research-center/article/modern_methods_and_means_for_analysis_and_risk_management_of_information_systems_of_companies/ (дата обращения: 05.12.2016).
4. Кондаков С.Е. К вопросу о количественной оценке защищенности информации от несанкционированного доступа в информационных системах [Электронный ресурс] / Кондаков С.Е. // Труды Международного симпозиума «Надежность и качество» – Электрон. дан. – Пенза, 2015. – С. 83-85.
5. Отчет о деятельности Уполномоченного органа по защите прав субъектов персональных данных за 2015 год [Электронный ресурс]: Роскомнадзор – Электрон. дан. – Москва, 2015. – Режим доступа: http://rkn.gov.ru/docs/Otchet_ZPD_rus2015.pdf (дата обращения: 12.12.2016).

ТИПЫ МОДЕЛЕЙ И ПРИНЦИПЫ МОДЕЛИРОВАНИЯ В ПРЕПОДАВАНИИ ГРАФИЧЕСКИХ ДИСЦИПЛИН

Ваншина Е.А., Ваншин В.В.

ФГБОУ ВО «Оренбургский государственный университет»,
г. Оренбург

В математическом обеспечении промышленных систем автоматизированного проектирования (САПР) активно применяются методы моделирования с целью создания геометрических моделей проектируемых объектов. Средства реализации автоматизации конструкторско-технологической документации предоставляет компьютерная графика, предметом изучения которой является создание, хранение и обработка **моделей** и их изображений с помощью компьютера, а задачами – представление изображения в компьютерной графике; подготовка изображения к визуализации; создание изображения; осуществление действий с изображением.

Большинство современных программ относятся к системам интерактивной компьютерной графики, в которых пользователь может управлять характеристиками объектов, компьютерная система способна создавать графику и вести диалог с пользователем.

Сегодня существует насущная потребность в компетентных специалистах, способных к анализу и синтезу пространственных форм и отношений, способных при разработке оборудования, технологических линий конструировать автоматизированными методами геометрические объекты с заданными параметрами, что задает определенные требования к подготовке студентов технического профиля при изучении дисциплин графического цикла.

В научной и специальной литературе наблюдается большое количество различных трактовок термина «модель». Известно, что к основным **типам математических моделей** геометрических объектов в САПР относятся каркасные, полигональные и объемные.

С помощью каркасной модели (конструктивные элементы – ребро и точка) описывают технические объекты, у которых аппроксимирующие поверхности – плоскости. Эти модели используют для представления геометрических объектов на плоскости; получаемые изображения неоднозначны. С помощью каркасных моделей нет возможности автоматизировать процессы удаления невидимых линий и получения сечений.

Полигональные модели позволяют описывать сложные криволинейные грани технических объектов. При построении этих моделей предполагается, что объект ограничен контурами, являющимися результатом пересечения или касания поверхностей. Вершины объекта могут быть заданы пересечением трех поверхностей или множеством точек, удовлетворяющих геометрическим требованиям, в соответствии с которыми определяется контур.

При создании полигональной модели поверхность аппроксимируют многогранником (его грани – это простейшие плоские многоугольники), квадриками и криволинейными поверхностями с возможностью проведения сложных расчетов и работу с моделью в интерактивном режиме (например, поверхности Кунса, Безье).

Преимущество аппроксимации сложных поверхностей плоскими гранями – это простота математических методов при работе с такими моделями. К одному из недостатков метода относится сохранение формы и размеров объекта, что зависит от количества граней аппроксимирующего многогранника. Чем больше число граней, тем выше уровень информации, необходимой для получения внутримашинного представления, и больше соответствующий ему объем памяти.

Объемные модели (конструктивные элементы – точка, контурный элемент, поверхность) позволяют представлять сложные технические объекты с большой степенью точности. При синтезе такой модели конструктивные элементы образуют узлы сетевой структуры. С помощью такой модели можно разделить точки на внутренние и внешние по отношению к реальному объекту.

При геометрическом моделировании высокого уровня, как считают ученые И. Гардан, М. Люка, необходимо выполнять следующие требования: правильность модели; возможность конструирования сложного объекта полностью; возможность вычисления инженерно-геометрических характеристик.

Применение основных типов математических моделей геометрических объектов при моделировании сложных тел, ограниченных криволинейными поверхностями, значительно упрощает решение большинства инженерно-геометрических задач автоматизированного конструирования и технологической подготовки производства.

Важным элементом любого прикладного исследования или инженерной разработки является **моделирование**. К компьютерному геометрическому моделированию, тесно связанному с компьютерной графикой, относят методы и алгоритмы внутреннего представления и преобразования геометрических моделей на компьютере.

Компьютерные геометрические модели в САПР подразделяют на 2D-модели (плоские, двумерные) и 3D-модели (объемные, трехмерные).

Плоское компьютерное геометрическое моделирование применяется в 2D-подсистемах САПР, подсистемах инженерной графики, для разработки конструкторско-технологической документации. В этих подсистемах применяют векторные геометрические модели, при построении которых используют способы построения по заданным отношениям и с использованием преобразований.

Построение с использованием отношений – это задание пользователем сначала создаваемого примитива, затем списка отношений и примитивов, к которым заданы отношения.

Построение с использованием преобразований заключается в последовательном выполнении действий: задание преобразуемого объекта, затем преобразование, далее преобразование аналитическими расчетами и операциями с векторной математической моделью.

Объемное компьютерное геометрическое моделирование подразделяется на: каркасное (объемное тело – это набор вершин и ребер), поверхностное (объемное тело описано набором ограничивающих его поверхностей, точек, линий) и твердотельное моделирование (создание сплошного объемного тела сложной геометрической формы из множества более простых объемных элементов с помощью булевых операций).

Выделяют основные инженерные задачи компьютерного моделирования трехмерных тел. Это построение компьютерной модели уже существующего изделия или его материальной модели; синтез формы ранее не существовавшего проектируемого изделия.

Современные САПР используют все виды геометрических моделей и могут создавать модели, состоящие из разных типов элементов. При геометрическом моделировании изделий применяется ограниченное количество базовых элементов – объектов, примитивов. Это двумерные объекты: точки, прямые, отрезки прямых, окружности и их дуги, различные плоские кривые и контуры; поверхности: плоскости, поверхности, представленные семейство образующих, поверхности движения, криволинейные поверхности; объемные примитивы: параллелепипеды, призмы, пирамиды, конусы, произвольные многогранники.

Построение трехмерной твердотельной модели заключается в последовательном многократном выполнении операций объединения, вычитания и пересечения над простыми объемными элементами.

Объемные элементы, из которых состоит трехмерная модель в системе КОМПАС-3D, образуют в ней грани (гладкая часть поверхности детали, которая может состоять из нескольких граней), ребра (прямая или кривая, разделяющая две смежные грани) и вершины (точка на конце ребра). В модели могут находиться и дополнительные элементы (символ начала координат, плоскости и оси).

Для создания объемных элементов используется перемещение (операция) плоских фигур (эскизов) в пространстве. Эскиз располагается на одной из стандартных плоскостей проекций, на плоской грани созданного ранее элемента или на вспомогательной плоскости, строится средствами модуля плоского черчения и состоит из одного (различных графических объектов: отрезка, дуги, сплайна, прямоугольника) или нескольких контуров (совокупности последовательно соединенных графических объектов).

Система КОМПАС-3D (ЗАО АСКОН) располагает базовыми операциями для построения объемных элементов: операцией выдавливания – выдавливанием эскиза перпендикулярно его плоскости; операцией вращения – вращением эскиза тела вращения, состоящего из контура со стилем основной

линии и оси вращения в виде отрезка со стилем осевой линии, вокруг оси, лежащей в его плоскости, при условии расположения контура с одной стороны от оси вращения; кинематической операцией – перемещением эскиза вдоль направляющей; операцией по сечениям – построением объемного элемента по нескольким эскизам. Существуют аналогичные базовые операции, вычитающие материал из модели, при ее построении. Операция имеет дополнительные возможности, позволяющие изменять или дополнять правила создания объемного элемента. Процесс построения объемной модели состоит в многократном добавлении (бобышки, выступы, ребра) или вычитании (отверстия, проточки, канавки, пазы) дополнительных ее объемов.

Таким образом, использование типов моделей объектов на основе принципов моделирования при построении автоматизированными методами геометрических объектов с заданными характеристиками в преподавании графических дисциплин позволяет визуализировать объект, создать его образ, использовать цвет для решения поставленных перед студентами инженерно-графических задач. Умение анализировать плоские чертежи, расчленить объекты сложных геометрических форм на простые составляющие тела позволяет легко переходить от 3D-моделей (объемных чертежей) к их 2D-моделям (плоским ассоциативным чертежам), что значительно упрощает процесс редактирования чертежей.

Разработка и создание дидактических материалов на основе 3D- и 2D-моделирования с использованием современных средств, методов и алгоритмов компьютерной графики в системе КОМПАС-3D, их применение в преподавании графических дисциплин, включение их в состав учебно-методических комплексов по инженерной и компьютерной графике позволяет оптимизировать учебный процесс по дисциплинам графического цикла.

Список литературы

1. Ванишина, Е. А. Проблемы компьютеризации преподавания графических дисциплин / Е. А. Ванишина // Вестник Оренбургского государственного университета. – 2009. – №2. – С.143. – ISSN 1814-6457.
2. Ванишина, Е. А. Общие принципы твердотельного моделирования деталей / Е. А. Ванишина // Интеграция науки и образования как условие повышения качества подготовки специалистов: материалы всероссийской научно-практической конференции. – Оренбург: ИПК ГОУ ОГУ, 2008. – С.34-37. – CD-R [электронный ресурс]. – ISBN 978-5-7410-0738-9
3. Ванишина, Е. А. Создание трехмерных моделей сборок в системе КОМПАС / Е. А. Ванишина // Наука и образование: фундаментальные основы, технологии, инновации. Материалы международной научной конференции. – Оренбург: ГОУ ОГУ, 2010. – 5 с. – CD-R [электронный ресурс]. – ISBN 978-5-7410-1062-4.
4. Ванишина, Е. А. Объемное моделирование в преподавании графо-геометрических дисциплин в вузе / Е.А. Ванишина // Университетский комплекс

как региональный центр образования, науки и культуры. Материалы всероссийской научно-методической конференции (с международным участием). – Оренбург: ООО ИПК «Университет», 2013. – С.1803-1807. – CD-R [электронный ресурс]. Регистр. св-во ФГУП НТЦ «Информрегистр» №30008 от 22.04.2013 г., издание зарегистрировано 22.04.2012 г., номер гос. регистр. 0321300710. – ISBN 978-5-4417-0161-7

5. Ванишина, Е. А. 3D-моделирование сборок изделий в САПР / Е. А. Ванишина // Технические науки – от теории к практике: материалы XXI международной заочной научно-практической конференции. – Новосибирск: Изд. «СибАК», 2013. – С.7-11. – ISBN 978-5-4379-0285-1.

6. Ванишина, Е.А. Построение 3D- и 2D-моделей деталей и сборки изделия для развития профессиональных компетенций студентов технических направлений / Е. А. Ванишина, В. В. Ванишин // Научный альманах. – 2015. – №9. – С.684-687. – Тамбов: ООО «Консалтинговая компания Юком», 2015. – ISSN 2411-7609.

7. Черепашков, А.А., Носов, Н.В. Компьютерные технологии, моделирование и автоматизированные системы в машиностроении: учебник для студентов высших учебных заведений / А. А. Черепашков, Н. В. Носов. – Волгоград: Издательский Дом «Ин-Фолио», 2009. – 640 с.

ПОДГОТОВКА В ОБЛАСТИ КОМПЬЮТЕРНОГО МОДЕЛИРОВАНИЯ СТУДЕНТОВ ПРОФЕССИОНАЛЬНОГО ОБУЧЕНИЯ

Вергасова О.М.

**Бузулукский гуманитарно-технологический институт (филиал) ОГУ,
г. Бузулук**

Подготовка в области информатики занимает важную функцию в профессиональном образовании. Дисциплины связанные с информатикой и информационными технологиями стали частью естественнонаучного и общепрофессионального блоков подготовки студентов, обучающихся по различным направлениям. Особое место, занимает курс «Компьютерное моделирование», ориентированный на практическую сторону профессионального образования, использование технических и программных средств, в деятельности будущего специалиста.

Первые компьютерные модели были связаны с физическими процессами и явлениями, где с помощью моделирования решались задачи гидравлики, теплообмена, механики твердого тела, а также задачи моделирования электрических цепей. Моделирование представляло собой решение сложных нелинейных задач математической физики с помощью итерационных схем, было оно, математическим моделированием. Успехи математического моделирования в физике способствовали распространению его на задачи химии, электроэнергетики, биологии и некоторые другие дисциплины, причем схемы моделирования не слишком отличались друг от друга. Подобный вид моделирования весьма широко распространен и в настоящее время. Более того, за время развития методов моделирования на ЭВМ при решении задач фундаментальных дисциплин и смежных предметных областей накоплены целые библиотеки подпрограмм и функций, облегчающих применение и расширяющих возможности моделирования.

Из-за большого выбора программных средств, используемых для моделирования, возникает вопрос какое средство наиболее достаточно и просто в использовании. При моделировании студентами электронных устройств, удобно использовать программную среду Multisim группы Electronics Workbench. В ее библиотеке более 16000 электронных компонентов, сопровождаемых аналитическими моделями, используемые при быстром моделировании. В данной программной среде есть контрольно-измерительные приборы, внешний вид которых и характеристики совпадают с настоящими приборами. Профессиональная и образовательная среда схемотехнического проектирования Multisim является удобным инструментом для демонстрации и визуализации явлений и процессов, происходящих в электрических устройствах. Для лучшего понимания функционирования электрических схем и контроля технологическими процессами производства используется

визуализация в виде осциллографа, графиков характеристик, показаний виртуальных приборов. Примеры заданий решаемых в среде схемотехнического проектирования Multisim представлены ниже.

Задание 1: измерить индуктивность катушки и ёмкость конденсатора косвенным методом по результатам прямых измерений напряжения, тока и мощности RL - или RC -ветви и косвенного измерения угла сдвига фаз φ_k .

Для решения задачи собрать в программной среде Multisim 10 схему цепи представленную на рисунке 1.

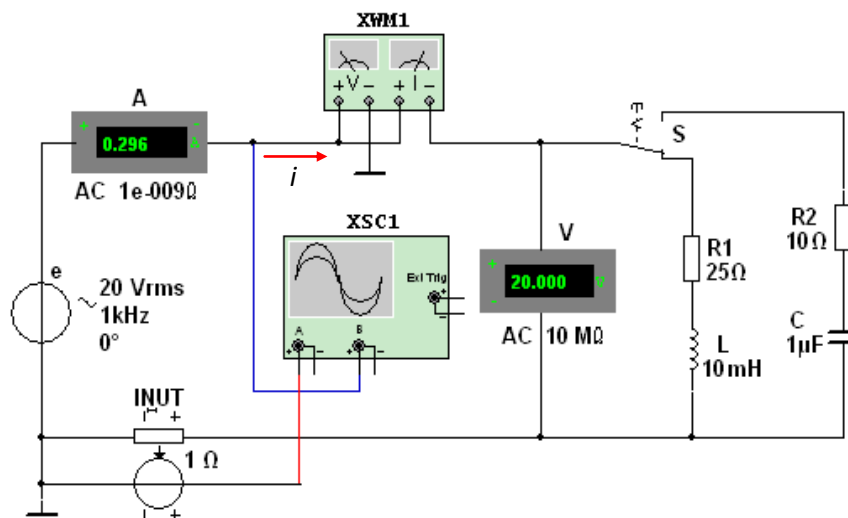


Рисунок 1 – схема электрической цепи

Задание 2: собрать схему цепи постоянного тока на рабочем поле программной среды Multisim 10 как на рисунке 2, и установить параметры элементов: $J = 2$ A, $E_1 = 10$ Ом, $E_5 = \text{int}(\sqrt{N} + 10)$ В, $R_1 = \text{int}(\sqrt{N} + 1)$ Ом, $R_2 = 2$ Ом, $R_3 = 3$ Ом, $R_4 = 4$ Ом, $R_5 = 5$ Ом, $R_6 = 6$ Ом, где N – номер индивидуального варианта, режим **DC** работы измерительных приборов, внутренние сопротивления $R_A = 1$ нОм и $R_V = 10$ МОм амперметров и вольтметров. При этом выбрать полярность включения амперметров и вольтметров, совпадающей с принятыми при расчёте схемы направлениями токов ветвей.

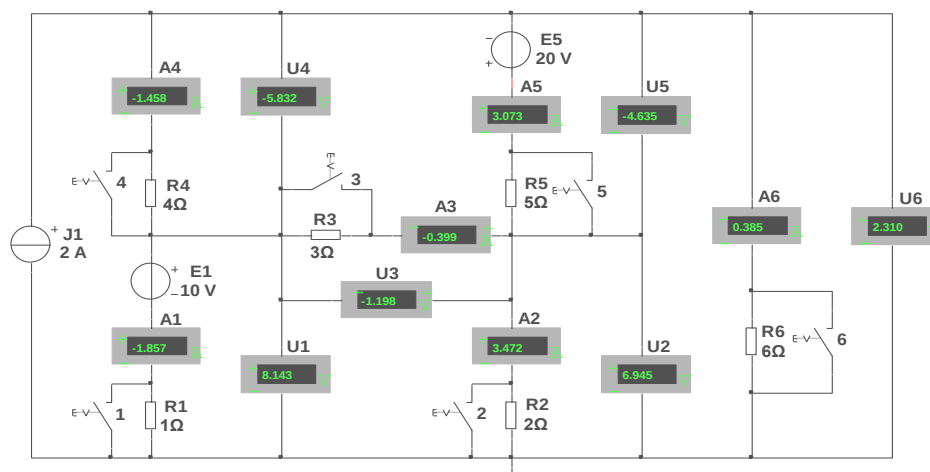


Рисунок 2 – схема электрической цепи

Запустить программу Multisim 10 и занести в таблицу значение тока $I_{кэ}$ заданной ветви схемы, которое не должно отличаться от расчётного значения $I_{кр}$ более, чем на 3...4 %.

Другим программным продуктом, реализующим концепции компьютерного моделирования и вычислительного эксперимента, является пакет программ для математических и инженерных расчетов Mathcad, разработанный фирмой Mathsoft Engineering & Education, Inc. Этот программный продукт используется для решения сложных инженерных или научных задач студентами и преподавателями естественнонаучных и технических дисциплин, таких как «Вычислительная математика», «Основы теории управления», «Методы оптимизации», «Теория принятия решений», а также «Моделирование систем» и «Компьютерное моделирование». Пакет Mathcad способствует быстрому росту профессиональной квалификации тех его пользователей, которые обладают хотя бы небольшими аналитическими способностями. Преимущество этого пакета, перед другими, в удобном для восприятия, интуитивно ясном представлении материала. При помощи пакета Mathcad решаются задачи линейного программирования. Решение данной задачи включает в себя следующие этапы: изучение теоретического материала; построение математической модели; исследование модели с помощью Mathcad; подготовка письменного отчета; защита лабораторной работы. Пример задачи линейного программирования приведен ниже.

Пример: Для изготовления изделий А, В используется токарное, сварочное и фрезерное оборудование. Затраты времени на обработку одного изделия для каждого из оборудования указаны в таблице1. В ней же указан общий фонд рабочего времени каждого из типов используемого оборудования, а также прибыль от реализации одного изделия каждого вида.

Таблица 1

Название оборудования	Затраты времени на обработку изделия		Общий фонд рабочего времени
	А	В	
Фрезерное	3	1	75
Токарное	1	1	30
Сварочное	1	4	84
Прибыль	3	4	

Требуется определить, сколько изделий и какого вида следует изготовить предприятию, чтобы прибыль была максимальной.

Для осуществления математических расчётов и моделирования, наиболее широко распространен другой вид программы такой, как электронные таблицы, в частности Microsoft Excel, входящий в стандартный офис фирмы Microsoft.

Данные программы являются многофункциональными и в то же время простыми для изучения. С помощью этой программы можно решать задачи исследовательского характера, требующие большого количества вычислений. Электронные таблицы позволяют работать с данными разных типов, с возможностью использования формул в таблицах выполняются точные расчеты, автоматически без ручных технологий. Специальное программирование в электронных таблицах позволяет решать ряд сложных задач.

Microsoft Excel позволяет использовать формулы для того, чтобы организовывать связи между данными в ячейках, при изменении значения данных в ячейке выполняется автоматический перерасчет формул, следовательно обновляется вся таблица и данные в ней. Основные функции электронных таблиц заключаются в следующем:

- автоматизация всех итоговых вычислений;
- производить однотипные расчёты над большими наборами данных;
- решение задач с помощью подбора значений;
- обработка результатов компьютерного эксперимента;
- табулирование функций и формул;
- создание табличных документов;
- выполнять поиск оптимальных значений для выбранных параметров;
- построение графиков и диаграмм для визуализации табличных данных.

При изучении курса «Компьютерное моделирование» моделирование физических процессов в электронных таблицах Microsoft Excel, наиболее доступно и понятно, так как знакомство с Microsoft Excel начинается со школьного курса информатики. Лабораторная работа «Моделирование равномерного движения тела» имеет шаблон, созданный в Microsoft Excel, где студенты вносят исходные данные, формулы для расчёта, определяют шаг изменения времени для подинтервалов, а затем строят график зависимости координаты равномерно движущегося тела от времени. Результат выполнения лабораторной работы в формате Microsoft Excel представлен на рисунке 3.

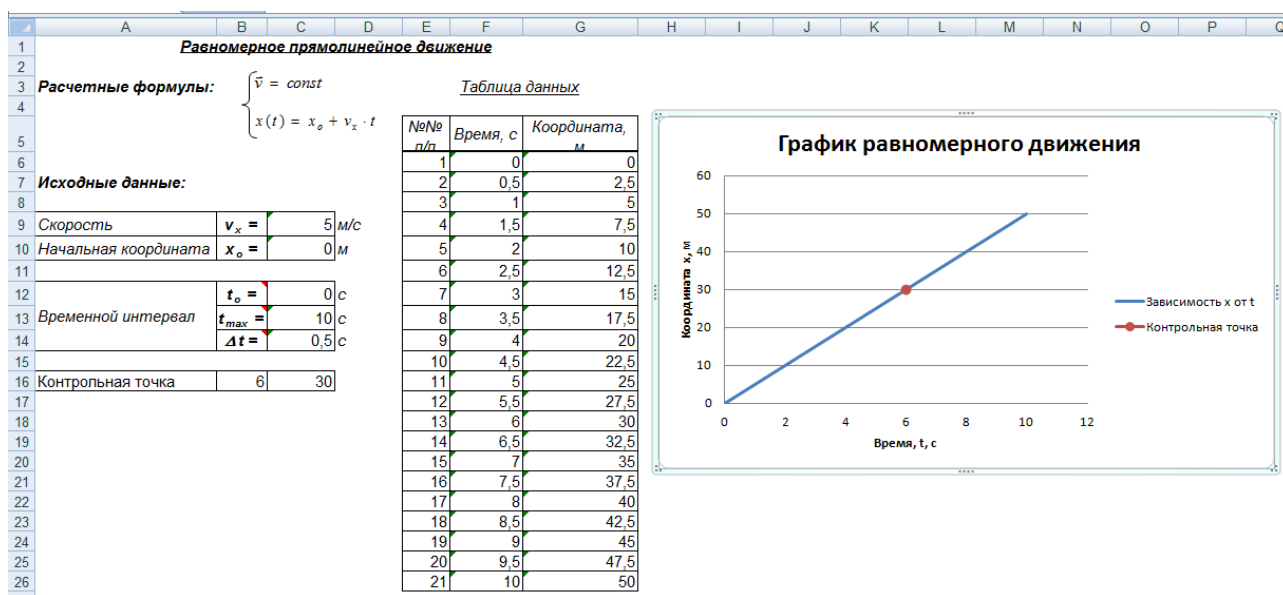


Рисунок 3 – моделирование физических процессов

Хотелось бы отметить, что рассмотренные программные средства, используемые для изучения студентами компьютерного моделирования и проведения вычислительного эксперимента будут использоваться в качестве инструментов при решении профессиональных задач. Рассмотренные подходы в подготовке студентов области компьютерного моделирования будут способствовать умению выбора и использования средств, адекватных поставленной задачи, а так же осознание необходимости и потребности использования полученных знаний в своей профессиональной деятельности.

Список литературы

1. Афонин, В.В. Моделирование систем: учеб. пособие / В.В. Афонин, С.А. Федоскин. – М.: БИНОМ, Лаборатория знаний, 2010. – 231 с. – ISBN 978-5-9963-0352-6
2. Харнитер, М.Е. Multisim 7. Современная система компьютерного моделирования и анализа схем электронных устройств [Электронный ресурс]. / М.Е. Харнитер. – М.: ДМК Пресс, 2010. – 501 с. – ISBN 5-9706-0026-1. – Режим доступа: <http://www.biblioclub.ru/book/85054/>
3. Паничев, В.В. Компьютерное моделирование: учеб. пособие [Электронный ресурс]. / Н.А. Соловьев, В.В. Паничев. – Оренбург: ГОУ ОГУ, 2008. – 115 с. – Режим доступа: <http://rucont.ru/efd/193272>
4. Информатика и образование: журн. / учредитель: Российская академия образования. – 1986 -.– М.: Образование и Информатика, 2016, № 1–10. – ISSN 0234-0453
5. Современная электроника / А. Майстренко [и др.]. – Режим доступа: http://www.soel.ru/about/for_authors.aspx

О СИММЕТРИЧНЫХ ШИФРАХ НА ОСНОВЕ УПРАВЛЯЕМЫХ ОПЕРАЦИЙ

Винокуров Д.В.

Оренбургский государственный университет, г. Оренбург

Современные симметричные программно-ориентированные и аппаратно-ориентированные шифры используют алгоритмы преобразования данных с предвычислениями, которые вносят существенные ограничения по быстродействию и зачастую требуют значительных вычислительных затрат. В связи с этим в настоящее время существуют различные алгоритмы, в которых реализуются управляемые операции. Данная проблема нашла отражение в работах Молдовяна А. А., Молдовян Н.А., Гуц Н.Д., Нгуен Минь, Шниперова А.Н. и других.

Под управляемой операцией понимается множество некоторых более простых операций, выбираемых в зависимости от значения некоторого управляющего кода. Например, управляющая подстановочная операция (УПО) представляет собой две простые алгебраические операции над двоичными векторами: побитовое сложение по модулю 2 и сложение по модулю 2^n [1].

Различают средства аппаратной и программной реализации рассматриваемых шифров. Целью данной работы является поиск и рассмотрение основных скоростных шифров, созданных на основе управляемых операций и зарегистрированных на территории РФ.

SPECTR-H64 является блочным шифром и обрабатывает информацию с 32-разрядной шиной обмена данных [2].

Схема блочного шифрования имеет следующий вид:

$$Y = F(X, Q^{(e)}), \quad (1)$$

где $Q^{(e)} = H(K, e)$ является расширенным ключом – функцией от 256-битного секретного ключа K и режима шифрования e , который принимает значение 0 и 1 (шифрование и расшифровка соответственно). Шифрование проходит в 12 раундов. X является исходным блоком двоичных данных (открытым текстом) в режиме шифрования, а в режиме расшифровки – преобразованным блоком двоичных данных (шифртекстом). В режиме шифрования результирующее значение Y является шифртекстом, а в режиме расшифровки – открытым текстом.

Секретный ключ K является объединением восьми 32-разрядных подключей и имеет следующий вид:

$$K = K_1 \| K_2 \| \dots \| K_8 \in GF(2)^{32}. \quad (2)$$

Стоит отметить, что $Q^{(e)}$ является последовательностью семидесяти четырех 32-разрядных двоичных векторов, каждый из которых является одним из восьми секретных подключей K_i .

SPECTR-128 является блочным шифром и обрабатывает информацию с 32-разрядной шиной обмена данных.

Секретный ключ в данной случае будет являться объединением четырех 64-разрядных подключей и иметь следующий вид:

$$K = K_1 \| K_2 \| K_3 \| K_4 \in GF(2)^{64}. \quad (3)$$

$Q^{(e)}$ в данном шифре является последовательностью пятидесяти 64-разрядных двоичных векторов, каждый из которых является одним из четырех секретных подключей K_i .

SIKS-128 является одним из итеративных блочных шифров и использует схемы патента РФ № 2140714 в качестве базовой схемы одного раунда [1]. Главным отличием SIKS-128 от SPECTR-128 является использование двух идентичных нелинейных векторных булевых функций вместо блока управляемых перестановок и нелинейной векторной булевой функции.

Секретный ключ также является объединением четырех 64-разрядных подключей и иметь следующий вид:

$$K = K_1 \| K_2 \| K_3 \| K_4 \in GF(2)^{64}. \quad (4)$$

Расширенный ключ $Q^{(e)}$ представляет собой последовательность пятидесяти двух 64-разрядных двоичных векторов, каждый из которых является одним из четырех секретных подключей K_i .

Рассмотрим команду DDP32, которая является 32-разрядной перестановкой и ориентирована для применения в криптографических приложениях. Входными параметрами такой команды являются: 32-разрядный преобразуемый бинарный вектор X , 32-разрядный управляющий вектор U и одноразрядный управляющий вектор e , принимающий значения 0 (прямая перестановка) и 1 (обратная перестановка). В результате выполнения данной команды получается перестановка 32-разрядного бинарного вектора

$$X : Y = P_{32/32}(X, U, e). \quad (5)$$

Команду DDP32 можно использовать для создания скоростных программных хэш-функций.

Программный шифр SPECTR-SZ использует команду управляемых перестановок DDP32. Он ориентирован на использование в компьютерах с 32-разрядным процессором и является блочнопоточным шифром. При

шифровании и расшифровке первый и последний раунды реализуют схему поточного шифра, а остальные реализуют схему блочного шифра. SPECTR-SZ реализуется в виде модуля инициализации и резидентного модуля, который обслуживает запросы других программ на шифрование и расшифровку данных. Шифрование происходит в 6 раундов, 1 и 6 из которых являются полными, а 2-4 – сокращенными. Сокращенные раунды позволяют обеспечить реализацию сильного лавинного эффекта.

Расширенный ключ шифрования Q представляет собой последовательность из 2051 байта:

$$Q = \{q_0, q_1, q_2, \dots, q_{2049}, q_{2050}\} \quad (6)$$

Секретный ключ в данном случае имеет вид

$$K = (k_0, k_1, k_2, \dots, k_s), \quad (7)$$

где $8 \leq s \leq 2050$.

COBRA-F64a и COBRA-F64b являются блочными шифрами с малым размером входного блока данных, что позволяет строить на их основе микропрограммы. Данные шифры используют команду DDP32. Общая схема шифрования может быть задана следующей формулой:

$$Y = F^{(e)}(X, Q^{(e)}), \quad (8)$$

где $Q^{(e)} = H(K, e)$ расширенный ключ, который является функцией от 128-разрядного секретного ключа K и режима шифрования e ($F^{(0)}$ – шифрование, $F^{(1)}$ – расшифровка). В режиме шифрования X является исходным блоком двоичных данных, т.е. открытым текстом, а в режиме расшифровки – преобразованным блоком двоичных данных (шифртекстом). В режиме шифрования Y является шифртекстом, а в режиме расшифровки – открытым текстом. Заметим, что $X, Y \in GF(2)^{32}$. В алгоритмах COBRA-F64a и COBRA-F64b используются два 32-разрядных подключа, а именно

$$Q^{(e)} = (Q_j^{(1,e)}, Q_j^{(2,e)}). \quad (9)$$

Секретный ключ K представлен в виде объединения 32-разрядных слов:

$$K = K_0 \| K_1 \| \dots \| K_n \in GF(2)^{32}. \quad (10)$$

В программных шифрах DDP-S64 и DDP-S128 также используется полууниверсальная схема шифрования, представленная в формуле 8, однако,

ключ K имеет 256-разрядность. Функция шифрования проходит в 3 этапа: начально преобразование, r раундов преобразования с использованием установленной алгоритмом процедуры, заключительное преобразование. Для DDP-S64 значение r принимается равным 10, а для DDP-S128 – 12. Оба шифра являются стойким к дифференциальному криптоанализу.

Шифр CryptoStar был разработан на основе аппаратно-ориентированного алгоритма COBRA-H6 и является стойким к линейному и дифференциальному аналитическим анализам. В рассматриваемом шифре используется новый криптографический примитив – переключаемая операция. Смеха шифрования и расшифровки, рассчитанная на 14 раундов, имеет вид:

$$Y = T^{(0)}(X, K), \quad (11)$$

$$X = T^{(1)}(Y, K) \quad (12)$$

где X – открытый текст, Y – шифртекст, K – секретный ключ, $T^{(e)}$ – функция для преобразования блока данных, $e = 0$ (шифрование) или $e = 1$ (расшифровка). Кроме того, $X, Y \in \{0,1\}^{256}$ $K \in \{0,1\}^{512}$ [3]. Секретный ключ рассматривается как объединение четырех подключей (формула 13), а на их основе формируется раундовый ключ $Q_j^{(e)}$.

$$K = (K_1, K_2, K_3, K_4) \quad (13)$$

Рассмотренные нами шифры несут практическую пользу для их применения. Таким образом, актуальной задачей в области компьютерных методов защиты информации является разработка и реализация скоростных шифров, которые сохраняют высокую скорость шифрования, являются криптостойкими и содержат в себе управляемые операций.

Список литературы

- 1 Молдовян А. А., Молдовян Н. А., Гуц Н.Д., Изотов Б. В. Криптография: скоростные шифры. [Текст] / А. А. Молдовян. – СПб.: БХВ-Петербург, 2002. – 496 с.
- 2 Гуц Н. Д., Изотов Б. В., Молдовян Н. А. Скоростной алгоритм шифрования SPECTR-H64 // Безопасность информационных технологий. – 2000. – № 4. – С. 37-50.
- 3 Шниперов, А. Н. Высокоскоростная симметричная криптосистема на основе управляемых операций CryptoStar / А. Н. Шниперов // Современные информационные технологии в науке, образовании и практике: сб. науч. тр. – Оренбург: ИПК ГОУ ОГУ, 2007. – С. 154-156.

ИССЛЕДОВАНИЕ МЕТОДОВ ПОВЫШЕНИЯ ДОСТОВЕРНОСТИ ДЕКОДИРОВАННЫХ ДАННЫХ В ЗАБОЙНЫХ ТЕЛЕМЕТРИЧЕСКИХ СИСТЕМАХ С ГИДРАВЛИЧЕСКИМ КАНАЛОМ СВЯЗИ

Влацкая И.В., Голубенко И.В.

Оренбургский государственный университет, г. Оренбург

Для продуктивного прироста сырья углеводородов все чаще использую наклонно-направленное и горизонтальное бурение с использованием современных телесистем. Телеметрическая система (ТС) с гидравлическим каналом связи в процессе бурения работает в условиях повышенных вибраций. Она регистрирует информацию о параметрах бурения, считывая с датчиков, установленных в ней, и осуществляет передачу полученной информации в реальном времени на наземную станцию. Своевременное получение достоверной информации с датчиков в сложных геологических условиях обеспечивает высококачественную проводку горизонтальных скважин. Сокращение времени на технологические замеры возможно только при получении достоверных данных за минимальное время и при повышенной частоте, при условии искажения сигнала, полученного по гидравлического каналу связи, из-за помех от бурового оборудования [1]. Решение этой проблемы возможно с использованием системы декодирования данных.

Многие методы цифровой обработки сигнала и декодирования не позволяют добиться необходимой помехозащищенности. Поэтому задача о получении системы повышающей достоверность декодирования данных, с возможностью восстановления сигнала, искаженного локальной помехой является актуальной до сегодняшнего дня. Использование математических методов позволяет преодолеть трудности, которые обусловлены присутствием помех.

Реализация данных ресурсоемких алгоритмов в режиме реального времени, стала возможным благодаря современным вычислительным устройствам, среди разнообразия устройств, предпочтение было отдано процессорам фирмы Intel и FPGA фирмы Xilinx [7], [6]. Целью данной работы является разработка универсальной системы, позволяющей повысить надежность приема данных в коде «Манчестер» с глубинных блоков телеметрических систем (ТС) [4]. Под универсальностью подразумевается возможность использовать систему предприятием НИП независимо от требуемой скорости передачи данных из скважины.

В разрабатываемой системе предполагается реализовать метод декодирования сигнала.

Принимаемый с канала связи сигнал оцифровывается с частотой 64 отсчета на период данных кода «Манчестер». Таким образом, все основные операции производились с векторами размером 64 элемента. Приняв код, оцифрованный на выходе канала связи, система выделяет четыре формы

сигнала, характеризующие единицы и нули цифрового сигнала, передаваемого источником информации - две формы сигнала для цифровой единицы и две формы для нуля. Форма реальных сигналов, изображенных на рисунке 1, существенно отличаются между собой, а также от формы идеального, что обусловлено влиянием помех на сигнал.

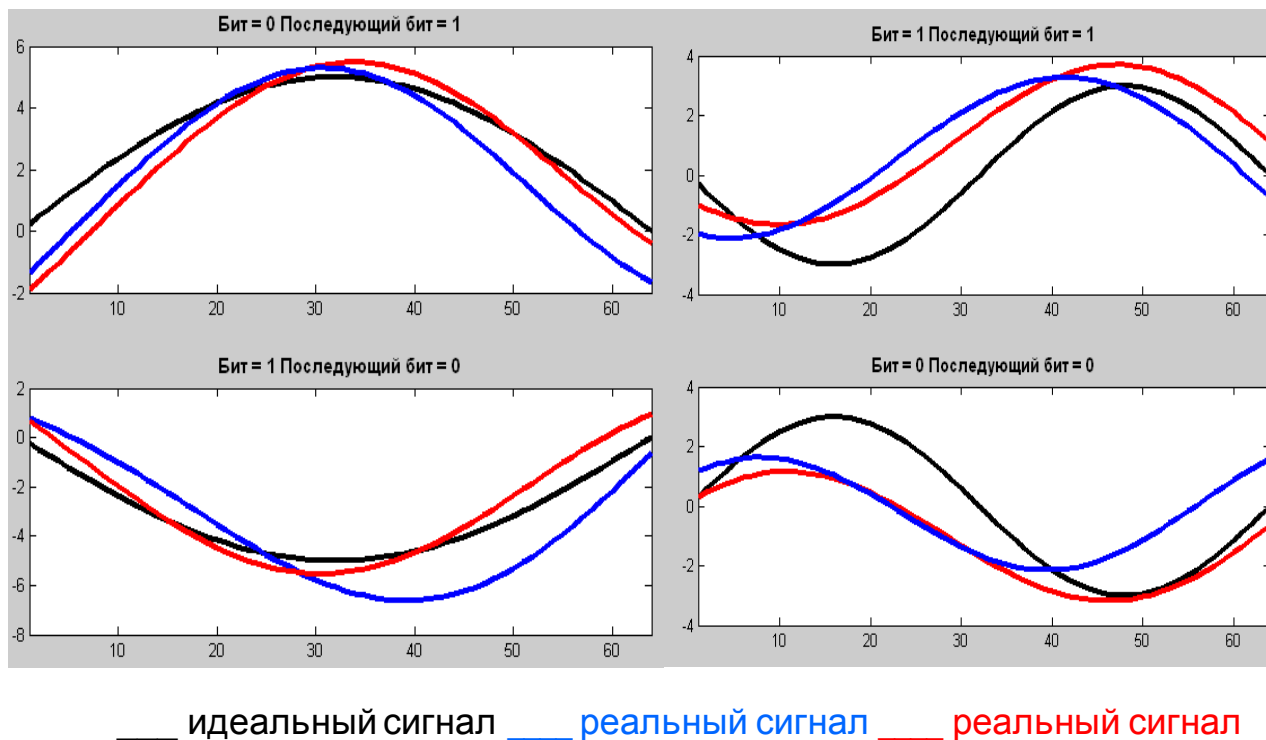


Рисунок 1 - Форма классов используемых в системе распознавания.

Четыре формы реального сигнала система принимает за четыре класса (вектора) данных. Далее, в процессе приёма информации, система классифицирует каждый вектор из потока данных, поступающих на её вход.

Для выполнения операции классификации в разрабатываемой системе реализуются методы распознавания образов и классификации, основанные на использовании нечеткой логики, нейронных сетей и скрытых марковских моделей. При этом учитываются особенности каждого из трёх обслуживаемых видов канала связи. Например, скорость передачи данных в гидравлическом канале от 0.5 бит/с, а современные требования к кабельному каналу - скорость не менее сотен килобит в секунду.

Таким образом, согласно описанному выше методу, разрабатываемая система должна выполнять следующую последовательность действий:

1. В момент запуска, ТС передает заранее известную последовательность данных, которая используется для получения центра классов (кластеризации данных). Отменить данный этап и использовать идеальные центры классов, приходится в случае, если необходимо декодировать данные с ТС, которую

изначально не планировалось использовать с разрабатываемой системой. Надежность декодирования в этом случае снижается, до тех пор, пока параллельно с классификацией не будет произведена кластеризация случайных данных, т.е. получены реальные центры классов, что повысит надежность декодирования. Основное назначение данного этапа - получить четыре класса, которые максимально похожи на реальные данные, поступающие на вход регистратора. Если данные искажены помехой, то это отражается на форме классов, что позволяет минимизировать влияние помехи. Данный этап является обучающим, позволяющий настроить систему под текущие внешние параметры. Например, отпадает необходимость указывать тип и длину геофизического кабеля перед началом геофизического исследования скважины.

2. Каждый бит данных несущих телеметрическую информацию подвергается классификации. Вычислив степень принадлежности данных к каждому классу, делается вывод о принадлежности к конкретному классу, что позволяет определить единица или ноль переданы в данные момент (рисунок 2).

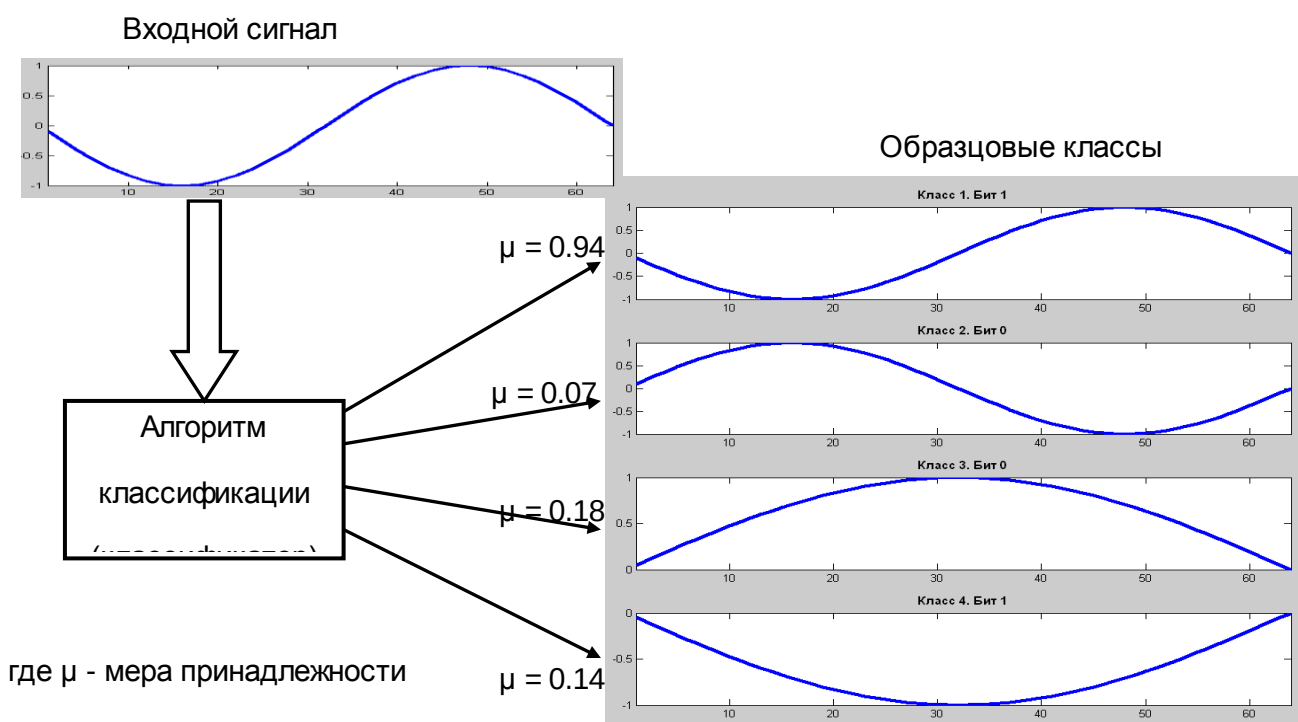


Рисунок 2 - Принцип работы классификатора

С целью повышения достоверности данных при идентификации предлагается использование нечеткой кластеризации на основе метода нечетких c -средних [2].

В начальный момент запуска ТС выдает фиксированную последовательность данных (формирование центров классов: 0 и 1), из которых формируется матрица нечеткого разбиения, удовлетворяющая условиям [3], [5]:

$$\sum_{k=1}^c \mu_{ki} = 1, \quad k = \overline{1, M};$$

$$0 < \sum_{k=1}^M \mu_{ki} < M, \quad i = \overline{1, c},$$

где c – количество кластеров, $c \in \{2, 3, \dots, M-1\}$.
Рассчитываем центры классов:

$$V_i = \frac{\sum_{k=1}^M (\mu_{ik})^m X_k}{\sum_{k=1}^M (\mu_{ik})^m}, \quad i = \overline{1, c}$$

В качестве меры близости между объектами из X (данные полученные с прибора) и центрами классов используем евклидову норму:

$$D_{ik} = \sqrt{\|X_k - V_i\|^2}, \quad k = \overline{1, M}, \quad i = \overline{1, c}$$

Элементы матрицы пересчитываем исходя из условий:

$$\text{если } D_{ik} > 0, \text{ то } \mu_{ki} = \frac{1}{\left(D_{ik} \sum_{j=1}^c \frac{1}{D_{jk}^2} \right)^{\frac{1}{m-1}}};$$

$$\text{если } D_{ik} = 0, \text{ то } \mu_{ki} = \begin{cases} 1, & \text{если } i = j \\ 0, & \text{если } i \neq j \end{cases},$$

где m – экспоненциальный вес ($m=2$).

Данный алгоритм выполняем до тех пор, пока минимальная абсолютная разность между значениями функций принадлежности на двух последовательных итерациях или норма разности матриц нечеткого разбиения не станет меньше некоторого априори заданного значения ($\varepsilon = 10^{-5}$).

Следует учесть, что при высоком уровне помех полностью помеху отфильтровать невозможно. Следовательно, данные лежащие в центре классов искажены помехой, что не мешает корректной классификации, в силу того,

что текущие данные соотносятся не с идеальными классами, а с классами, полученными во время обучения, так же искаженными помехой.

Список литературы

1. *Рязанов В.И. Направленное бурение глубоких скважин. – Т.: Изд. ТПУ, 1999. – 84с.: ил.*
2. *Влацкая И.В., Голубенко И.В., Голубенко Д.В. Автоматизированная система распознавания и классификации декодированных данных с глубинных блоков телеметрических систем. // Перспективы развития информационных технологий: сборник материалов IV Международной научно-практической конференции / Под общ. ред. С.С. Чернова. - Новосибирск: Издательство НГТУ, 2011. - 273с.*
3. *Леоненков А.В. Нечеткое моделирование в среде MATLAB и fuzzy TECH. – СПб.: БХВ – Петербург, 2005г. – 736 с.: ил.*
4. *Mark S. Wight, Method and Apparatus for decoding manchester encoded data. United States Patent, Patent Number: 5163067.*
5. *Штовба С.Д. Проектирование нечетких систем средствами MATLAB. – М.: Горячая линия – Телеком, 2007. – 288 с.: ил.*
6. *Getting Started with the Avnet Nano-ITX / Spartan-6 FPGA Development Kit, Version 1.0, 6/7/2011. Avnet Inc.*
7. *Spartan-6 Family Overview, DS160 (v2.0) October 25, 2011. Xilinx Inc.*

МЕТОДИЧЕСКИЕ АСПЕКТЫ ФОРМИРОВАНИЯ УЧЕБНО-ПОЗНАВАТЕЛЬНОЙ КОМПЕТЕНЦИИ НА УРОКАХ МАТЕМАТИКИ

Газизова В.В.

МБОУ «Первомайская СОШ Оренбургского района», г. Оренбург

Выпускнику современной школы, чтобы быть успешным в учебе и в работе, необходимо быть творческим, самостоятельным, ответственным, коммуникативным человеком. Ему должна быть присуща потребность к познанию нового.

Так каким же должен быть современный урок, на котором учитель развивал бы все перечисленные умения и был бы не простым «механическим» носителем «объективного знания», а высококомпетентным вдохновителем, чтобы он успешно мотивировал учащихся на проявление инициативы и самостоятельности?

Все самое важное для ученика совершается на уроке, поэтому, обратимся еще раз к известной цитате В.А. Сухомлинского: "Урок – это зеркало общей и педагогической культуры учителя, мерило его интеллектуального богатства, показатель его кругозора, эрудиции".

Как же организовать деятельность учащихся на уроке, чтобы каждый мог бы реализовать свои способности? Как развивать и поддерживать огонёк познавательного интереса?

Познавательный интерес, как и всякая черта личности, развивается и формируется в конкретной, живой деятельности, и, прежде всего, в учении. Китайская мудрость гласит: «Я слышу – я забываю, я вижу – я запоминаю, я делаю – я усваиваю». Исследования показывают, что память человека хранит 25% услышанного материала, 33% увиденного, 50% увиденного и услышанного, и 75 % материала, если ученик вовлечён в активные действия в процессе обучения. Формирование познавательного интереса происходит по двум основным каналам: с одной стороны, само содержание имеет в себе эту возможность, а с другой – определенная организация познавательной деятельности.

Первое, что является предметом познавательного интереса для школьников – это новые знания о мире. Удивление - сильный стимул познания!

Но познавательный интерес к учебному материалу не может поддерживаться все время только яркими фактами. Ведь далеко не все в учебном материале может быть для учащихся интересно. И тогда выступает еще один, не менее важный второй источник познавательного интереса – сам процесс деятельности.

Какие же методы помогают мне привнести в процесс обучения положительный заряд?

Наиболее эффективны и вдохновляющи такие направления:

1) игровые методики;

- 2) подчёркивание практической значимости;
- 3) создание проблемных, соревновательных ситуаций;
- 4) использование исторических сведений;
- 5) развитие творческих способностей;
- 6) учебные исследования;
- 7) метод парадоксов и др.
- 8) приобщение к мудрости великих людей.

Рассмотрим их подробнее.

1. Игровые моменты.

Игры ставят ученика в условия поиска, пробуждают интерес к победе, а отсюда – стремление быть быстрым, собранным, ловким, находчивым, уметь четко выполнять задания, соблюдать правила. В играх, особенно в коллективных, хорошо формируются и нравственные качества личности (а значит, развивается общекультурная компетенция).

Пример: игра «Угадай формулу».

Функция задана формулой $y = x + 4$

Найдите значение функции при $x = 0, 6, -3, 1$.

Приглашаю к доске ученика, даю ему карточку, на которой написано

$U = x + 4$, а на доске заготовлена таблица.

Ученик из класса называет какое-нибудь значение x . Ученик у доски вписывает это число в таблицу и, поставив его в формулу, находит и вписывает в таблицу соответствующее ему значение y . Затем другой ученик из класса называет другое значение x и ученик у доски проделывает те же операции. Задача класса – “угадать” формулу, записанную на карточке. Выигрывает тот ученик, который первый назовет формулу.

У каждого урока есть свой имидж. И если временные рамки не позволяют от души поиграть, то можно придумать к уроку девиз. Это очень оживляет урок. Например, на первом слайде презентации к уроку, может быть такой «мотиватор»: (рис.1)

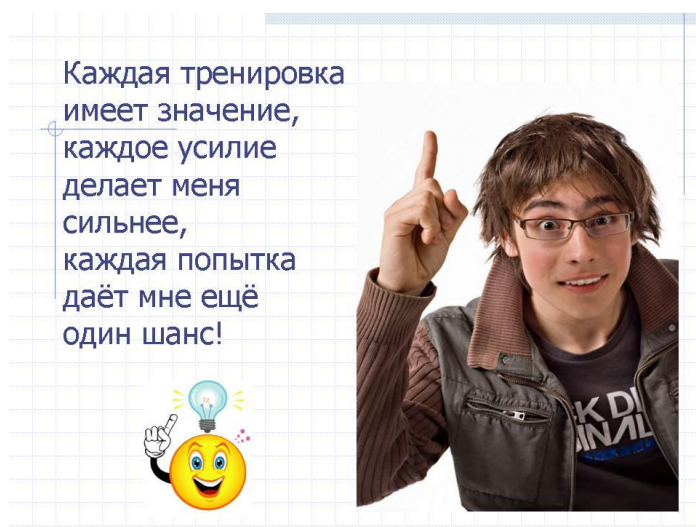


Рис.1

2. Подчёркивание практической значимости.

Опыт работы показывает, что учебная мотивация эффективно создаётся, если начинать урок с примеров практического использования знаний, которые предстоит изучить на данном уроке. Причём, примеры эти должны быть конкретными, современными, актуальными. Только через теснейшую связь с практической жизнью можно пробудить желание ученика изучить теоретический материал. Задача учителя – привлечь внимание и озадачить: как это устроено? как это работает? почему так происходит?

Пример: перед изучением темы «Свойства графика функции» полезно рассмотреть несколько графиков. Ребята отгадывают, какой из них является кардиограммой сердца. А учитель прокомментирует, что врач, считывая свойства этого графика, делает выводы о работе сердца. Другой график показывает осциллограф, улавливая удары о земную поверхность, и специалист, считывая свойства такого графика, делает выводы о наличии там полезных ископаемых. (рис.2)



Рис.2

Итак, мы видим, как важно разбираться в свойствах графика. Запишем тему сегодняшнего урока: «Свойства графика функции».

3. Создание проблемных ситуаций.

Проблемный способ изложения новой темы - мощный рычаг воспитания трудолюбия, желания и умения хорошо учиться.

Приведу примеры, как создать поисковую ситуацию, чтобы проблема опиралась на личный опыт ребенка.

На уроке геометрии при подготовке к изучению темы “Сумма внутренних углов треугольника” предлагаю решить задачи:

Один из углов треугольника содержит 36° , а другой – на 18° больше третьего. Найти величину второго угла.

В равнобедренном треугольнике, угол при основании на 18° больше угла при вершине. Найти величину каждого угла треугольника.

Пытаясь самостоятельно достигнуть поставленной практической цели, учащиеся приходят к выводу, что для решения этих задач не хватает данных. Если бы было известно, чему равна сумма величин внутренних углов каждого

из заданных треугольников и вообще любого треугольника, то задачи были бы разрешимы. Теперь каждому ясна цель поиска.

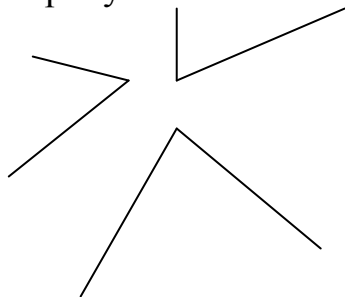
Также возникает поисковая ситуация, если мы даём ученикам шанс самостоятельно сформулировать некоторое определение, а не сообщаем его в готовом виде.

Например, изучаем треугольник в 7 классе.

Ученики сами дают определение. Они очень стараются. Ещё бы, что такое треугольник – все знают!

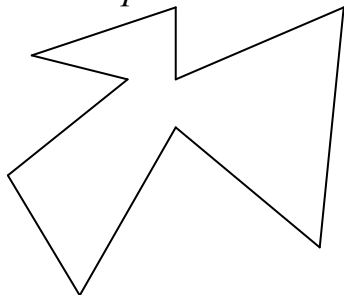
Ответ первый: - это когда есть три угла...

Я рисую:



В общем, что сказали – то и нарисовала.

Ответ второй: Уточняют: «Чтобы они соединялись». Я соединяю:



Получилось ещё страшнее.

Ответ третий:

-Лучше вершины сначала нарисовать.

-Хорошо, а их сколько?

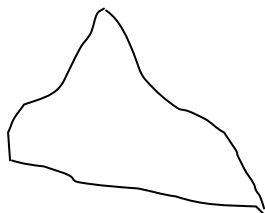
-Три.

Моя картинка: . . .

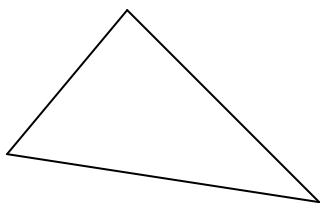
Ответ четвёртый: - Так треугольник не получится. Надо взять три точки, не лежащие на одной прямой. И соединить их.

Я соединяю.

.



Ответ пятый: Соединить отрезками.



Наконец-то материализовалось то, о чём хотели сказать.

Умения грамотно выражать свои мысли, давать лаконичные, однозначные, точные определения не свалится с потолка. Это придёт с опытом, если мы будем побуждать учащихся к сравнению, сопоставлению фактов.

4. Использование исторических экскурсов.

История математики обладает не только познавательным, но и воспитательным потенциалом. Практика работы показывает, что именно при помощи истории науки, можно формировать у учеников представления о математике как части общечеловеческой культуры. История науки дает возможность показать, что математика, как наука о пространственных формах и количественных отношениях реального мира возникла и развивается в связи с практической деятельностью человека.

5. Развитие творческих способностей учащихся.

Для этого полезно придумывать аналогичную и обратную задачу.

Например, при изучении темы по алгебре в 7 классе «Решение задач с помощью систем линейных уравнений», нужно решить такую задачу:

На турбазе имеются палатки и домики. Всего их 20. В каждом домике живут 4 человека, а в каждой палатке 2 человека. Сколько на турбазе палаток, если там отдыхают 60 человек?

Прежде чем решать эту задачу, можно устно рассмотреть решение обратной задачи:

На турбазе 10 палаток и 10 домиков. В каждом домике живут 4 человека, а в каждой палатке 2 человека. Сколько человек отдыхают на турбазе?

Ученики составят выражение к решению этой задачи: $4 \cdot 10 + 2 \cdot 10 = 60$, и это им поможет понять идею составления уравнения $4 \cdot x + 2 \cdot y = 60$ в первой задаче, когда палатки и домики будут обозначены за x и y .

Теперь придумаем аналогичную задачу, например:

У причала 20 лодок, часть из которых двухместные, а часть – четырёхместные. Всего в эти лодки может поместиться 60 человек. Сколько у причала двухместных лодок?

Такая практика решения обратной и аналогичной задачи, помогает ребятам более глубоко осознавать внутренние связи между величинами, понять принципы решения задач алгебраическим способом.

Большой интерес также вызывают такие задания, как, составить кроссворд, нарисовать свой рисунок и записать координаты точек для собственного рисунка.

6. Учебные исследования.

Именно учебные исследования дают возможность научиться самостоятельно познать новое в результате наблюдения, анализа, выдвижения гипотезы, ее проверки и формулировки вывода и поэтому делают процесс изучения математики интересным и увлекательным.

Исследовательская деятельность – это принципиально новый подход к организации школьного обучения. Учёба строится не на запоминании отобранной учителем информации, а на самостоятельном поиске и развитии интересов ребёнка.

Привлечение учащихся к выполнению исследовательских работ имеет глубокий воспитательный характер. Школа не в состоянии обеспечить ученика знаниями на всю жизнь, но она может вооружить его методами и навыками познания, особенно, через создание ситуации самостоятельной творческой активности.

Ничто не заменит ребёнку радость, вдохновение от собственного творчества, от чувства победы над своими узкими представлениями о скучности и однообразности учебного процесса.

Мои ученики продолжают исследования уже на более сложные темы не из школьной программы, например такие, как «Математическая разгадка оптических иллюзий», «Загадка чисел Фибоначчи», «Узоры, фракталы и их искусный мастер», «Золотое сечение вокруг нас». Некоторые из них стали Всероссийскими и областными лауреатами.

7. Метод парадоксов.

Целесообразно применять задачи с недостающими, избыточными, противоречивыми данными, с заведомо допущенными ошибками. Подать ошибку можно по разному, но наиболее продуктивный способ – «софистический» или «парадоксальный». Так как для лучшего запоминания ошибку нужно не только осознать, но и «пережить», т.е. сопроводить положительной эмоцией.

.Пример: софизм $65=64$

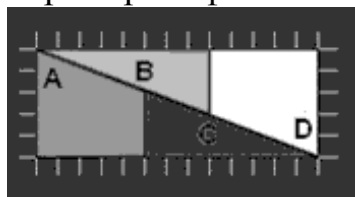


Рис.3

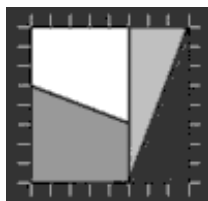


Рис.4

На рисунке 3 имеем на клетчатой бумаге нарисованный прямоугольник размерами 5×13 , т.е. площадью 65.

На рисунке 4 имеем квадрат $8 \times 8 = 64$.

Обе фигуры разрезаны на попарно равные части.

Отсюда, их площади равны; следовательно, $65 = 64$.

Разгадка заключается в том, что только при выполнении очень точного чертежа можно обнаружить, что точки А, В, С и D не лежат на одной прямой, а образуют параллелограмм, площадь которого и равна этой «лишней» единице.

Метод парадоксов заставляет кропотливо перепроверять факты, очевидные на первый взгляд, привлекает к философскому осмыслению конкретных решений.

8. Приобщение к мудрости великих людей.

Вместе с учениками мы собираем высказывания о математике и научном познании мира. Ребята узнают новые для них имена, постигают глубокие мысли, облечённые в ёмкие, лаконичные фразы, например:

"Числа управляют миром", - говорили пифагорейцы. Но числа дают возможность человеку управлять миром, и в этом нас убеждает весь ход развития науки и техники наших дней. (А. Дородницын)

Геометрия полна приключений, потому что за каждой задачей скрывается приключение мысли. Решить задачу - это значит пережить приключение. (В. Произволов)

В математике есть своя красота, как в живописи и поэзии. (Н.Е. Жуковский)

Если вы хотите научиться плавать, то смело входите в воду, а если хотите научиться решать задачи, то решайте их. (Д.Пойа)

Чтобы переварить знания, надо поглощать их с аппетитом. (А. Франц)

Предмет математики столь серьезен, что не следует упускать ни одной возможности сделать его более занимательным. (Б. Паскаль)

Периодически некоторые афоризмы мы печатаем крупным шрифтом и помещаем в кабинете математики там, где они чаще всего попадают в поле зрения. Несколько раз перечитывая, ученики лучше запоминают мудрые строки и краткие сведения об их авторах, что приобщает их к опыту духовного восхождения человечества. В лице великих мыслителей мы имеем надёжных союзников в обучении математике.

Таким образом, оснащение задач жизненным материалом, включение игровых и деловых ситуаций, поощрений, соревнований, различных форм сотрудничества, позволяет нам сформировать учебно-познавательную компетенцию.

Интересно, что учитель за свою жизнь даёт более 25000 уроков!

А ученик за 10 лет посещает более 10000 уроков!

Какой огромный резерв таится в каждом уроке, в каждой «клеточке» педагогического процесса!

Если все наши уроки будут яркими и впечатляющими – это банк знаний, компетенций, навыков на всю жизнь!

Поэтому, так важно учителю постоянно совершенствоваться, и «расти», тогда и его ученики будут успешными и востребованными в современном обществе! Как важно, чтобы зрячим было и его сердце, - главный педагогический инструмент учителя! Действительно, порой надо дирижировать, оставаясь за кадром, и вдохновлять, оставаясь в тени. Одно лишь слово, сказанное вовремя, или даже пауза... может стать точкой отсчёта, стартом ракеты в формировании учебно-познавательных компетенций!

И как бы мы не увлеклись передачей знаний, стремлением к результату, даже под «давлением» серьезных требований ЕГЭ, нам всегда надо помнить: каждый ребёнок приходит в этот мир не только и не столько для того, чтобы его учили, а для того, чтобы быть счастливым и созидательным!!!

Вот с этих позиций и взглянем на каждого: перед нами не двоечник-троечник, а человек, личность, пока еще с нераскрытыми возможностями, с несформированными навыками самообучения, с неразвитым компетентностным подходом.

Перефразируя высказывание Зака Зиглара «Не бывает ленивых людей; бывают либо больные, либо невдохновленные» получаем применительно к школьному обучению - «не бывает ленивых учеников...». Вдохновлять на обучение – насущная задача и показатель высококомпетентного подхода учителя.

Таким образом, в рамках компетентностного подхода, образование и обучение становится комплексным, многофакторным. Учащимся передаются не только знания и навыки, ведется также психологическая подготовка, формируются нужные установки, развиваются определенные личностные качества, нарабатываются конкретные алгоритмы эффективной познавательной деятельности.

Поэтому, приобретенные учениками компетенции – это не просто знания и умения, это владение такими формами поведения и индивидуальными характеристиками, которые необходимы для успешной деятельности на любом поприще. За этим, конечно, стоят и знания, и умения, но не только они. Не менее важное значение имеют: вдохновение, личностные черты, установки, ценности, убеждения, эмоции, способность ладить с друзьями и самооценка.

Список литературы

1. *Внеурочная деятельность*, Н.А.Криволапова. Издательство Москва «Просвещение», 2012 год

2. Журнал «Математика в школе», № 9, 2004 год, «Влияние индивидуальных особенностей математического мышления на процесс решения задач».

3. Журнал «Математика для школьников», №1, 2013 год, «Математические и игры головоломки».

4. *Задания развивающего характера по математике*, Т.А.Лавиненко. Пособие для учителя. Саратов, ОАО «Издательство»Лицей», 2003год.

5. *Занимательные дидактические материалы по математике*, выпуск 2 В.В.Трошин, Москва «Глобус», 2008 год.

6.Кульневич С.В. *Совсем необычный урок*, издательство «Учитель», Воронеж, 2001.

7. Матюшкин А. М. «Проблемные ситуации в мышлении и обучении». М., 2003

8. *Нестандартные задачи по математике для детей и родителей*, Г.Г. Левитас; Москва ИЛЕКСА, 2009 год
9. Пономарёв Я. А. «Психология творческого мышления» М., 2002 г.
10. Пойя Д. «Математическое открытие». М., 2003г.
11. В.А.Сухомлинский «Процесс овладения знаниями и умственное развитие». Изб. пед. соч. – М.,: 1980, т.2.
12. Щуркова Н.Е., *Игровые методики*, Педагогическое общество России, Москва 2008г.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБУЧЕНИИ НА СОВРЕМЕННОМ ЭТАПЕ

Колобов А. Н.

**ФГБОУ ВО Оренбургский государственный университет,
г. Оренбург**

Для получения информации о состоянии процесса, объекта или явления (информационного продукта) нового качества, применяется процесс использующий совокупность методов и средств сбора, передачи и обработки данных (первичной информации), который и называется информационными технологиями.

Цель информационных технологий – производство информации для ее анализа человеком и принятии на его основе решения по выполнению какого-либо действия. Для формирования людей изобретательных, инициативных, умеющих самостоятельно принимать решения, специалистов уровня необходимого в современном мире необходимо сочетание традиционные формы обучения с информационными технологиями, что даст совершенно новое качество обучения. Применение информационных технологий выведет процесс обучения на более высокий уровень, позволит облегчить этот процесс и даст широкие возможности в образовании [1].

В последние десятилетия к числу крупномасштабных инноваций, пришедших в российскую школу, относится компьютеризация школьного образования.

Выделим основные из направлений внедрения и использования компьютерной техники в процессе обучения:

- в качестве средства обучения повышающего эффективность и совершенствующего процесс преподавания;
- в качестве объектов изучения на примерах рассмотрения различных современных средств информационных технологий и самого компьютера;
- в качестве средств автоматизации процессов тестирования, контроля, психодиагностики и коррекции.

Одной из ведущих проблем научно-методической сферы, на современном этапе становится разработка методологии проектирования в сфере современных учебных (информационных) технологий, которые можно легко применить в школьном образовании. Программное обеспечение при этом должно пересекаться с действующим учебным планом и быть связанным с учебным планом школы. Поэтому важна задача качественного отбора материала и содержания по отдельным предметам, с целью создания эффективных компьютерных программ, в которых и будет заключена практическая реализация компьютерных технологий в школе.

Справочники и базы данных учебного назначения, электронные лекции, электронные учебники, сборники задач и примеров, тестирующие и

контролирующие компьютерные программы, для поддержки различных видов занятий компьютерные иллюстрации, вот неполный список программных средств, используемый в обучении на современном этапе.

В наше время существует необходимость вывода системы образования на качественно новый уровень, отвечающий потребностям и перспективам развития промышленности, различных производств и общества в целом. Среди основных проблем, влияющих на качество подготовки специалистов, можно выделить проблему организации учебной деятельности, поэтому развитие новых форм дистанционного образования необходимо усовершенствовать с помощью новейших компьютерных технологий, что позволит повысить уровень знаний специалистов, не прибегая к методам обучения, связанным с отрывом от их непосредственной работы.

В процессе подготовки специалистов высокого уровня следует стремиться переложить максимальную нагрузку в процессе обучения на самого обучаемого, а педагогу дать новую роль – роль направляющего консультанта, более опытного коллегу, реализующего в полной мере индивидуальное обучение. Рассмотрим дистанционное образование, в котором возможны следующие формы обучения:

- Независимое обучение – при этом используется только личный компьютер обучаемого или организации, за счет которой проводится обучение. Основное при обучении по этой форме заключается в том, что 70-80% контрольных испытаний проводятся без личного контакта студента с преподавателем. При этом необходима идентификация обучаемого в ходе проведения контрольных испытаний, что требует дополнительных затрат университета на выполнение данной процедуры.

- Частичное независимое обучение – данное обучение так же проводится с использованием личной компьютерной техники обучаемого или компьютера организации, за счет которой проводится обучение. Но при этом сдача всех контрольных испытаний проходит в одном из региональных представительств вуза. Сотрудники представительства проводят идентификацию обучаемого в момент проведения контрольных испытаний.

- Обучение проводится на базе регионального представительства университета с использованием его компьютерной техники и технологий. При этом на всех этапах образовательного процесса предусматривается использование компьютерной техники вуза или представительства. Все контрольные испытания проводятся в присутствии преподавателя. Так же преподаватель проводит идентификацию обучаемого в момент проведения контрольных испытаний.

Перед разработчиками образовательных программ по дистанционному обучению стоит непростая задача изложения материала в доступной, логически построенной форме, содержащей рубежи контроля по освоенному материалу. При разработке электронных учебников использование новых информационных технологий позволяет расширить наглядную составляющую

изучаемого материала. Сделать материал более насыщенным, интересным, имеющим различные ссылки и вкладки на различные источники и информационные данные, что освобождает обучающихся от самостоятельного поиска информации имеющей многозначное значение, так как преподаватель указывает именно то, что необходимо изучить.

Структура электронных учебных пособий должна представлять собой взаимосвязь логически завершенных блоков текстового и графического материала. Названия отдельных блоков, отображенные в содержании, позволят студенту быстро ориентироваться в тексте и самостоятельно составить план работы как совокупность отдельных модулей, а наличие рисунков даст возможность хорошо представить ожидаемый результат.

При разработке тестового материала необходимо руководствоваться определенными принципами. Это принцип соответствия содержания теста предполагаемым целям тестирования и включения в тест таких элементов из учебных программ, которые являются наиболее важными, раскрывающими суть данной дисциплины, а не нацеленные на фрагментарные знание по ней. В разработке таких тестов помогает взаимосвязь содержания и формы.

Существует несколько вариантов тестов: первые, в которых, отвечая на вопрос необходимо сделать выбор из ответов да или нет. Вторые, когда из предложенных ответов на вопрос необходимо выбрать единственно верный и третьи, когда необходимо выбрать несколько правильных вариантов подходящих к ответу на заданный вопрос [2].

Каждый преподаватель сам определяет варианты тестовых заданий и процентное соотношение необходимых правильных ответов при их выполнении на различных уровнях рубежного контроля.

В заключении хочется еще раз подчеркнуть положительные стороны организации дистанционного обучения с помощью информационных технологий:

- Применение компьютерных учебников или компьютерных лекций позволяет многократно обратиться к материалам лекций, чего нет при традиционном обучении.

- Обучаемый обучается в ему свойственном темпе, не быстро и не медленно.

- Время и место обучения никак не регламентировано. Мотивация обучения формируется преподавателем с помощью большого числа мультимедийных учебных материалов.

- Тестирование проводится на компьютерах в любое удобное для обучаемого время, тем самым снимая личностный момент при оценке уровня знаний.

- Большое количество вопросов при тестировании позволяет охватить всю тематику дисциплины, что не достигается при традиционном зачете или экзамене.

Разрабатывать курсы, изучаемые дистанционно более трудоемкая задача,

по сравнению с созданием нового учебного пособия или учебника, в данном случае требуется детальная проработка действий педагога и учащихся в новой предметно-информационной среде. От структуры построения и подачи учебного материала во многом зависит успешность дистанционного обучения. Перед разработчиками стоит не только проблема отбора компактного, но емкого материала, необходимо найти баланс между традиционными методами преподавания и возможностями компьютерных технологий.

В современном обществе возникает потребность создания совершенно новых форм, методов и средств обучения, с применением и использованием компьютерных технологий, которые позволили бы большему числу людей получать необходимые знания и повышать свою квалификацию. Поэтому процесс разработки и внедрения компьютерных технологий в образование не потеряет своей актуальности и будет способствовать формированию единого образовательного пространства, ведь процесс обучения безграничен и многогранен.

Список литературы

1. Колобов, А.Н. Информационные технологии и образование [Электронный ресурс] / А.Н. Колобов // «Университетский комплекс как региональный центр образования, науки и культуры»: материалы Всероссийской научно-методической конференции. – Оренбург: ООО ИПК «Университет», 2014. – С.3031-3036.

2. Колобов, А.Н. Компьютерные технологии и высшее образование [Электронный ресурс] / А.Н. Колобов // «Университетский комплекс как региональный центр образования, науки и культуры»: материалы Всероссийской научно-методической конференции (с международным участием) – Оренбург: Оренбургский государственный университет, 2016. – С.2499-2501.

КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ.

Курушин А.А.

Оренбургский государственный университет, г. Оренбург

В работе показана роль, которую занимает гомоморфное шифрование в облачных вычислениях, а также плюсы и минусы применения данного способа шифрования. В рамках практической части была реализована криптосистема Пэ́йе и RSA и сравнены скорости шифрования данных и скорости операций гомоморфных свойств.

Использование облачных вычислений дает много преимуществ, но для обработки данных в публичных «облаках» в общем случае необходимо работать с открытыми данными. Но для работы с конфиденциальными данными необходима аппаратура или хотя бы организационные меры по хранению ключей. К провайдерам облачных вычислений такие требования представить не представляется возможным. Это по определению несет в себе риски, так как мы не можем повлиять никоим образом на то, как это происходит на третьей стороне. Было бы гораздо безопаснее передавать данные в зашифрованном виде с тем, чтобы операции, которые производятся над этими данными, никоим образом не распространяло информацию об этих данных.

В 1978 году авторами известного алгоритма с открытым ключом RSA Майклом Дертусосом, Рональдом Риверстом и Леонардом Адлеманом было сформировано понятие гомоморфного шифрования. В их работе они описали концепцию гомоморфного шифрования, а также задались вопросами возможно ли такое шифрование в принципе и для каких алгебраических систем такой гомоморфизм существует. Их попытки потерпели неудачу, и было решено, что эта идея не является реализуемой. Под формальным определением гомоморфного шифрования понимается криптографический примитив, представляющий собой функцию шифрования, удовлетворяющую дополнительному требованию гомоморфности относительно каких-либо алгебраических операций над открытым текстом.

Гомоморфное шифрование как криптографический примитив представляет интерес как с прикладной, так и с чисто математической точек зрения. Несмотря на многолетние исследования в этой области, основные проблемы остаются нерешенными.

В литературе по теоретической криптографии под гомоморфным шифрованием понимается криптографический примитив, представляющий собой функцию шифрования, удовлетворяющую дополнительному требованию гомоморфности относительно каких-либо алгебраических операций над открытыми текстами.

Пусть $E(k,m)$ — функция шифрования, где m — открытый текст, k — ключ шифрования. Заметим, что для данных фиксированных k и m криптограмма $E(k,m)$ может быть, вообще говоря, случайной величиной. В таких случаях говорят о вероятностном шифровании. Функция E гомоморфна относительно операции or над открытыми текстами, если существует эффективный алгоритм M , который получив на вход любую пару криптограмм вида $E(k,m_1)$, $E(k,m_2)$, выдает криптограмму s такую, что при дешифровании s будет получен открытый текст $m_1 \text{ or } m_2$.

Гомоморфное шифрование как криптографический примитив может найти широкое применение в криптографии и, в более широком смысле, в разработке математических методов защиты информации. Здесь прежде всего следует выделить такую, интересную с прикладной точки зрения, задачу как вычисления над зашифрованными данными. Конфиденциальные данные хранятся в зашифрованном виде. Для выполнения вычислений над ними данные можно расшифровать, произвести необходимые операции, и затем результаты вновь зашифровать. Но для этого требуются защищенная аппаратура и, уж по крайней мере, организационные меры по хранению секретных ключей. Вычисления над зашифрованными данными, если они возможны, помогают избежать всех этих проблем.

Гомоморфные системы шифрования.

1. Система RSA.

Криптосистема RSA является одной из самых известных и популярных криптосистем. Она является гомоморфной относительно операции умножения открытых текстов.

Пусть

N — составной модуль,

e — открытая экспонента

$E((N,e),m) = m^e \bmod N$ — функция шифрования

Для любых двух m_1 и m_2

$$E(k,m_1) \times E(k,m_2) = m_1^e m_2^e \bmod N = E(k,m_1 \times m_2)$$

2. Криптосистема Эль Гамала.

В криптосистеме Эль Гамала в циклической группе G , если открытый ключ является (G, q, g, h) , где $h = g^x$ и x закрытый ключ функция шифрования выглядит следующим образом для сообщения m

$$E(m) = (g^r, m \times h^r)$$

Где $r \in \{0, \dots, q-1\}$

Свойство гомоморфности выглядит следующим образом:

$$\begin{aligned} E(m_1) \cdot E(m_2) &= (g^{r_1}, m_1 \cdot h^{r_1}) (g^{r_2}, m_2 \cdot h^{r_2}) = (g^{r_1+r_2}, (m_1 \cdot m_2) h^{r_1+r_2}) \\ &= E(m_1, m_2) \end{aligned}$$

Таким образом, криптосистема Эль Гамала является гомоморфной относительно операции умножения.

3. Криптосистема Пэе.

Пусть p и q – два простых числа

$$n = pq$$

$\lambda = \text{НОК}(p - 1, q - 1)$. Выберем случайное число g из $Z_{n^2}^*$ и вычислим

$$\mu = (L(g^\lambda \bmod n^2))^{-1} \bmod n, \text{ где } L(u) = (u - 1)/u$$

Открытым ключом служит пара $k = (n, g)$, а закрытым ключом – пара (λ, μ)

4. Модель Бракерски-Гентри-Вайкунтанатан.

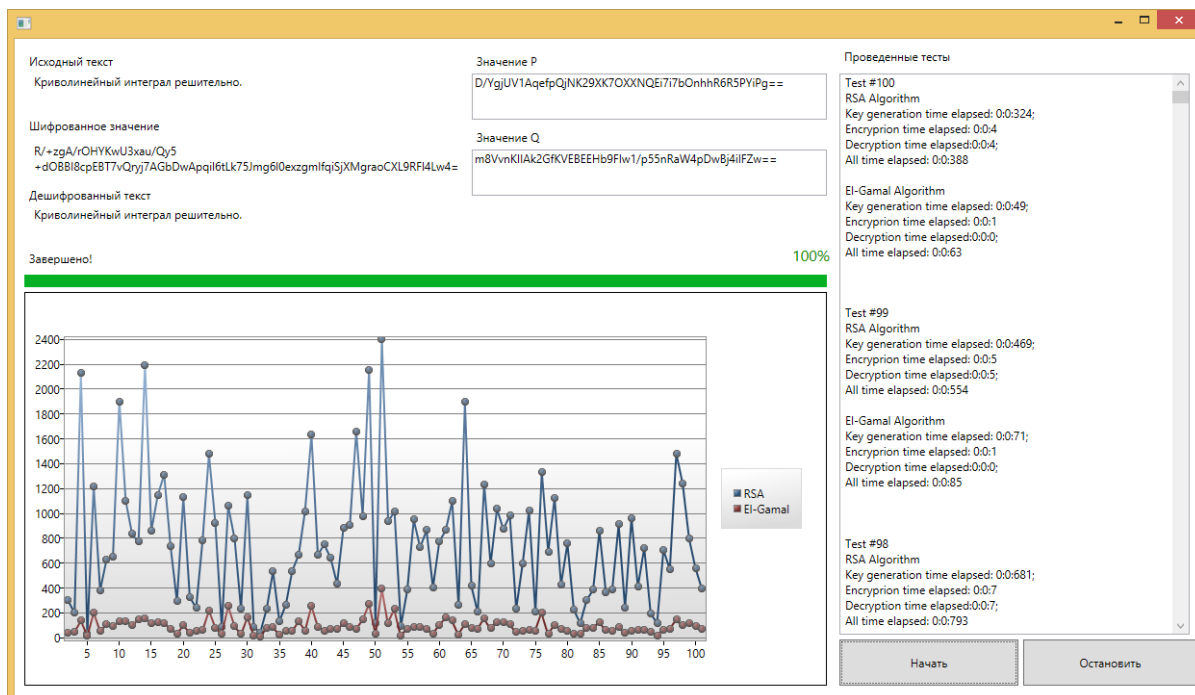
25 июня 2009 года аспирант Стэнфордского университета и стажер IBM Крейг Гентри предложил модель полностью гомоморфного шифрования, которая позволяла проводить глубокую обработку данных без их расшифровки. В алгоритме Гентри выполняются свойства гомоморфности относительно как умножения, так и сложения. Тем самым данную модель можно использовать в облачных вычислениях без ограничений. Передавая данные в облака, то есть в недоверенную зону, можно не задумываться об их конфиденциальности. Однако модель Гентри оказалась слишком непрактичной. С увеличением количества операций производимых над зашифрованным текстом сложность и размер шифр текста увеличивается с невероятной скоростью. И не смотря на то, что за последние несколько лет были произведены множество улучшений данной модели, она все еще остается скорее теоретической моделью, которая не применима на практике.

Описание практической части.

В рамках данной работы были протестированы криптосистема Пэе и RSA и сравнены скорости шифрования данных и скорости операций гомоморфных свойств. Реализации были написаны на языке C#. Для каждой криптосистемы были реализованы выделены отдельные классы, которые содержали следующие функции:

1. Генерация ключей (KeyGeneration)
2. Шифрование (Encrypt)
3. Дешифрование (Decrypt)

В ходе эксперимента были получены следующие результаты:



Криптосистема	Генерация ключа	Шифрование	Расшифрование
RSA	0:0:212 мс	0:0:5 мс	0:0:4 мс
Эль Гамала	0:0:143 мс	0:0:2 мс	0:0:1 мс

Характеристики компьютера, на котором проводились замеры:

- Процессор: Intel Core i5 2.6Ghz
- ОЗУ: 4Гб
- Жесткий диск: WDC - WD3200LPVT
- ОС: Windows 8.1 x64

Заключение.

В ходе работы рассмотрено гомоморфное шифрование, как наиболее перспективное направление в области защиты информации при использовании облачных вычислений. Проведены эксперименты производительности криптосистем RSA и Пэе обладающих одним гомоморфным свойством. В ходе экспериментов выяснилось, что на данный момент криптосистема Гентри на практике не применима. В то же время, криптосистемы RSA и Пэе могут использоваться в очень узконаправленных приложениях.

Список литературы

1. NIST Определение облачных вычислений
2. Ronald L. Rivest, Len Adleman, Michael L. Dertouzos On data banks and privacy homomorphisms (1978)
3. Ronald L. Rivest Voting, Homomorphic Encryption
4. Craig Gentry; Shai Halevi. "A Working Implementation of Fully Homomorphic Encryption" pdf
5. SattvaQ Homomorphic encryption

6. B. Barak *Fully Homomorphic Encryption*

7. Вик Уинклер *Облачные вычисления: Вопросы безопасности в виртуальных облаках.*

8. Cisco *Безопасная сегментация в унифицированной архитектуре центров обработки данных Cisco* 9. Ronald L. Krutz, Russel Dean Vines, *Cloud Security: Comprehensive Guide to Secure Cloud Computing*, Wiley Publishing, 2011
27

10. Н.П. Варновский, А.В. Шокуров *Гомоморфное шифрование*

11. K. Lauter, M. Naehrig, V. Vaikuntanathan

ИСПОЛЬЗОВАНИЕ МУЛЬТИМЕДИЙНЫХ НАГЛЯДНЫХ ПОСОБИЙ ПРИ ОБУЧЕНИИ МАТЕМАТИКЕ СТУДЕНТОВ ВУЗОВ

Максименко Н.В.

Оренбургский государственный университет, г. Оренбург

Модернизация современного высшего образования предполагает не только освоение обучающимися определенного ФГОС объема знаний, умений и навыков, но и развитие личности студента, его познавательных и креативных способностей. Использование прогрессивных образовательных технологий при этом является важнейшим условием результативности обучения. В основных образовательных программах акцент делается на компетентностном подходе, формировании положительной мотивации обучения и интереса к учебной деятельности. Актуален по-прежнему лозунг: “Студент – не сосуд, который нужно заполнить знаниями, а факел, который нужно зажечь”.

Все вышесказанное в полной мере относится к высшему математическому образованию. При изучении дисциплины “Математика” в высшей школе должны использоваться современные образовательные технологии, выбор которых целесообразно осуществлять в зависимости от предметного содержания, целей учебного занятия, уровня подготовленности студентов, возможности удовлетворения их образовательных запросов.

Следует особо отметить интерактивные технологии. Интерактивные технологии позволяют процесс изучения математики организовать так, чтобы формировать собственное мышление студента, активизировать его познавательную деятельность. Кроме того, данные технологии осуществляются в условиях постоянного, активного взаимодействия всех участников образовательного процесса и направлены на развитие творческих способностей студентов.

При преподавании дисциплины “Математика” задача преподавателя состоит в том, чтобы обеспечить связь обучения с жизнью, с практической деятельностью, учитывая при этом возрастные и психологические особенности студентов.

Дело в том, что традиционная система преподавания в вузах имеет такие недостатки, как низкий уровень познавательной активности обучающихся, механическое усвоение знаний, что приводит к несформированности умения находить выход из затруднительной ситуации при решении задач. Когда преподаватель объясняет новый материал по математике, предлагая его в готовом виде, то это не гарантирует полноценного понимания информации большинством студентов и способности применять ее на практике. Традиционное обучение основывается на психических процессах восприятия и памяти. Обучающиеся, получая готовую информацию от преподавателя, усваивают ее, запоминают, а потом воспроизводят (если запомнил). Но студенты с кратковременной памятью не способны запомнить большой объем математической информации и переходят в разряд “слабоуспевающих”. “Сильными” могут быть только студенты с хорошей памятью.

Проанализировав недостатки обучения по традиционной схеме, можно прийти к выводу о необходимости внедрения таких форм и методов обучения при преподавании математики, которые способствуют повышению мыслительной активности обучающихся в процессе самостоятельной учебной деятельности, т.е. когда репродуктивную деятельность сменяет продуктивная.

Уход от традиционных форм проведения учебного занятия позволил бы устранить однообразие и монотонность образовательного процесса, создать условия для рациональной смены видов деятельности студентов, реализовать основные принципы здоровьесбережения [1].

Добиться прочного знания курса математики можно лишь при условии, когда обучающийся практически на каждом шагу убеждается, что знание математических понятий с успехом применимо к решению многочисленных и разнообразных задач, возникающих в повседневной жизни. И проще показать эти задачи, используя мультимедийные наглядные пособия.

Один из путей решения этой проблемы – создание мультимедийных наглядных пособий, которые на современном этапе развития информационных технологий являются одним из самых эффективных методов представления и изучения любого материала. Мультимедийные наглядные пособия позволяют подойти к процессу обучения творчески, разнообразить способы подачи материала, сочетать различные организационные формы проведения занятий в целях получения высокого результата при минимальных затратах времени на обучение.

По способу использования их можно разделить на две группы - мультимедийные наглядные пособия для сопровождения лекции и для индивидуальной работы над проектом.

Первая группа пособий органично вписывается в структуру занятия, сопровождая рассказ преподавателя. Возможность вставлять любые объекты (картинки, графики, таблицы и др.) в мультимедийное наглядное пособие особенно привлекательна при изучении сложных тем, когда необходимо показать модели или ход процесса. К тому же при представлении материала в таблицах, графиках и тезисах включаются механизмы не только слуховой, но зрительной и ассоциативной памяти. Однако следует помнить, что использование мультимедийных наглядных пособий, как и любое использование компьютерных технологий, должно быть оправдано. То есть нужно давать возможность продемонстрировать тот материал, который станет понятнее именно в данной реализации, именно с использованием технических средств компьютера. В любом случае при первичном применении мультимедийных наглядных пособий даже самая простая реализация способна заинтересовать студентов.

Вторая группа пособий является одной из ведущих форм личностно ориентированного обучения. Такой метод активного обучения стимулирует творческий потенциал обучающегося, учит работать с информацией, выбирать главное, систематизировать, анализировать, выбирать наиболее удачный способ представления материала. Каждый студент наглядно демонстрирует свои знания, умения, навыки, может реализовать себя.

В качестве примера можно рассмотреть систему занятий по теме “Функция одной переменной”. Выбор данной темы не случаен.

Функция является одним из основных понятий математики, в частности математического анализа, так как математические модели реальных ситуаций, изучаемые на протяжении всего курса математики, напрямую связаны с функциями. Таким образом, формирование функциональной грамотности у студентов является одной из основных задач преподавателя математики.

Для правильного формирования у обучающихся представления как о самом понятии функции, так и о методологической сущности этого понятия полезно рассматривать кусочные функции, т.е. функции, заданные различными формулами на различных промежутках области определения. Во многих случаях именно кусочные функции являются математическими моделями реальных ситуаций. Процесс построения таких функций становится более понятным, а самое главное, более наглядным и быстрым, если весь этот процесс представить в среде PowerPoint. На занятиях по данной теме можно использовать презентации “Построение графиков кусочных функций”, “Исследование функций на монотонность”, “Основные свойства функции”, “Взаимно обратные функции”. Для проверки знаний и умений студентов по пройденному материалу можно составить графические тесты в среде PowerPoint. Такая реализация контроля знаний дает возможность получения быстрой обратной связи о знаниях и умениях студентов, помогает скорректировать дальнейшую работу по устранению ошибок и недопонимания темы.

Использование мультимедийных наглядных пособий на занятиях по математике помогает:

- повысить степень наглядности;
- экономить время на занятиях;
- усваивать эффективнее учебный материал;
- получить быструю обратную связь;
- активизировать познавательную деятельность студентов;
- создать эмоциональное отношение к учебной информации;
- отвечать научным и культурным интересам и запросам студентов;
- реализовать принципы индивидуализации и дифференциации учебного процесса [2].

Список литературы

1. Бурсова, А.П., Крутова, Л.Н. Интерактивные технологии в преподавании микробиологии в медицинском колледже [Текст] / А.П. Бурсова // Среднее профессиональное образование. – 2016. – № 6. – С. 108-115.
2. Бочонина, М.Б. Использование мультимедийных наглядных пособий при обучении математике студентов СПО [Текст] / М.Б. Бочонина // Среднее профессиональное образование. – 2016. – № 11. – С. 107-111.

МОДЕЛЬ АДАПТИВНОГО ТЕСТИРОВАНИЯ КАК СПОСОБ РЕАЛИЗАЦИИ ИНДИВИДУАЛЬНОГО ПОДХОДА

Маслова О.В.
Сиб ГАУ, г. Красноярск

В настоящее время в образовательном процессе все более актуальными становятся такие способы обучения, которые максимально приближены к внутренним потребностям обучаемых, к их привычному способу взаимодействия с окружающим миром. Студенты современного вуза обладают хорошей подготовкой в области компьютерной грамотности, поэтому следует учитывать этот факт в условиях все возрастающей компьютеризации большинства сфер человеческой деятельности, распространения информационных и телекоммуникационных технологий. Использование таких технологий и различных технических средств в обучении позволяет повысить его интенсификацию, оптимизацию и реструктурирование для значительной экономии и более рационального использования учебного времени. При этом меняется и сам процесс обучения: он становится более разнообразным, живым, ярким; повышается мотивация и вырастает заинтересованность обучаемых в изучении предмета уже по причине того, что современное поколение студентов знакомится с компьютером и компьютерными технологиями достаточно рано. Поэтому актуальной задачей является разработка учебно-методических материалов, планирование проведения занятий и организация учебной и внеучебной деятельности обучаемых с учетом этой «особенной» характеристики сегодняшнего студента.

В современной практике преподавания такая компьютерная технология как тестирование, проводимая с определенной периодичностью и выполняющая как обучающую, так и контролирующую функцию, является одной из наиболее часто применяемых. Но, к сожалению, этот метод имеет существенный недостаток – потеря индивидуального подхода к каждому обучаемому, когда преподаватель не имеет возможности объективно оценить степень усвоения проверяемого материала каждым студентом [3].

Модели адаптивного тестирования, в которых сложность заданий меняется в зависимости от правильности ответов испытуемого, являются прогрессивными и наиболее интересными для исследования, они, частично, могут содействовать устранению этой проблемы.

В данной статье приведена модель адаптивного тестирования, использующая аппарат IRT (Item Response Theory, в русской литературе известная как математическая теория педагогических измерений) [4, 5]. Данная модель может помочь разработчикам систем тестирования и преподавателям, активно использующим технологии тестирования в обучении [6].

Для оценки трудности заданий и уровня знаний испытуемых используется аппарат IRT, в частности, однопараметрическая модель Раша

(Rasch Measurement Model) [7, 8]. Модель ИРТ имеет ряд преимуществ перед классической теорией тестов [9]. Во-первых, модель использует количественные методы оценки знаний испытуемых и трудности заданий. Во-вторых, модель является линейной, что позволяет использовать аппарат математической статистики для анализа результатов. В-третьих, оценка трудности заданий не зависит от выборки испытуемых, равно как оценка уровня подготовки испытуемых не зависит от выборки тестовых заданий. В-четвертых, существует возможность получить оценку уровня знаний испытуемых на выборке тестовых заданий, а не на полном множестве, что позволяет использовать ИРТ в адаптивном тестировании.

Основными переменными однопараметрической модели Раша являются уровень знаний испытуемого Θ и трудность задания β . Аргументом функции успеха испытуемого при ответе на задание теста является разность $\Theta - \beta$. Функция, связывающая успех испытуемого с уровнем его подготовленности и трудностью задания, в соответствии с моделью Раша, имеет следующий вид:

$$P(\Theta | \beta) = P(\beta | \Theta) = \frac{e^{(\Theta - \beta)}}{1 + e^{(\Theta - \beta)}} \quad (1)$$

На рисунке 1 слева представлен вид функции $P(\Theta)$ при значениях трудности задания β : -2, 0 и 2, а справа – вид функции $P(\beta)$ при соответствующих значениях β [10].

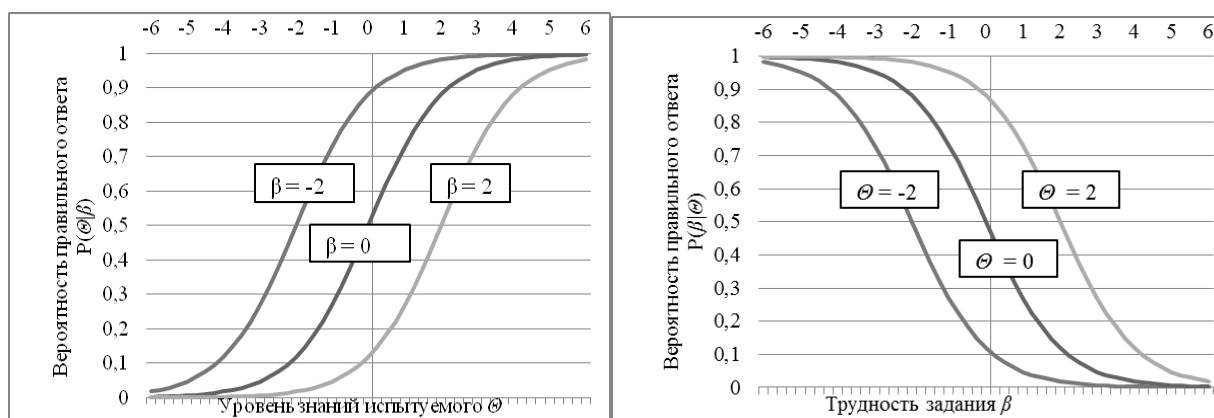


Рис. 1. Характеристические кривые заданий (*Item Characteristic Curve*) и характеристические кривые испытуемых (*Person Characteristic Curve*)

Чем выше уровень знаний испытуемого Θ , тем выше вероятность успеха в том или ином задании. В точках $\Theta = \beta$ вероятность правильного ответа равна 0,5. То есть, если трудность задания равна уровню знаний испытуемого, то он с равной вероятностью может справиться или не справиться с этим заданием [11].

На рисунке 2 представлен вид функции $P(\beta)$. Чем выше уровень знаний испытуемого, тем выше вероятность правильного ответа на задание.

Далее рассмотрим алгоритм получения значений Θ и β [12]. Пусть Q – индивидуальный балл испытуемого (количество правильных ответов), M –

общее количество ответов, данных испытуемым, R – количество правильных ответов данных группой испытуемых на задание теста, N – общее количество ответов, данных на задание теста. Тогда начальные значения уровня знаний испытуемых и уровня трудности заданий вычисляются по следующим формулам:

$$\Theta_0 = \ln \frac{Q}{M - Q} \quad (2)$$

$$\beta_0 = \ln \frac{R}{N - R} \quad (3)$$

Затем значения Θ_0 и β_0 переводятся в единую интервальную шкалу стандартных оценок. Для этого необходимо вычислить среднее и несмещенную оценку дисперсии по множествам Θ_0 и β_0 . Пусть V – несмещенная оценка дисперсии по множеству Θ_0 , а U – несмещенная оценка дисперсии по множеству β_0 . $\bar{\beta}$ и $\bar{\Theta}$ – математическое ожидание соответственно Θ и β поправочные коэффициенты определяем по следующим формулам [13]:

$$C_Q = \sqrt{\frac{1 + U/2,89}{1 - UV/8,35}} \quad (4)$$

$$C_\beta = \sqrt{\frac{1 + V/2,89}{1 - UV/8,35}} \quad (5)$$

Θ и β в единой интервальной шкале вычисляются по следующим формулам:

$$\Theta = \bar{\beta} + C_Q * \Theta_0 \quad (6)$$

$$\beta = \bar{\Theta} + C_\beta * \beta_0 \quad (7)$$

Рассмотрим пример вычисления параметров Θ и β для группы испытуемых из восьми человек ($N = 8$) по результатам ответа на 10 заданий теста ($M = 10$). Исходная матрица ответов представлена в бинарном виде (таблица 1), т.е. 1 соответствует успешному выполнению задания испытуемым, 0 – неуспешному.

Таблица 1 – Матрица вычислений значений Θ и β

№ Фамилия	1	2	3	4	5	6	7	8	9	10	Q	Θ_0	Θ
1. Воробьев	1	1	0	0	1	0	0	0	1	1	5	0	0,051

2. Голубев	0	0	1	0	1	1	0	0	0	1	4	- 0,405	-0,387
3. Гусев	0	1	1	0	1	1	1	0	0	1	6	0,405	0,489
4. Журавлев	1	0	1	1	0	0	0	0	1	0	4	- 0,405	-0,387
5. Куликов	1	1	0	1	0	1	1	1	0	0	6	0,405	0,489
6. Лебедев	1	0	0	1	0	0	0	1	1	0	4	- 0,405	-0,387
7. Орлов	1	0	0	0	1	1	0	0	0	1	4	- 0,405	-0,387
8. Соколов	1	0	1	1	1	1	1	0	1	1	8	1,386	1,548
R	6	3	4	4	5	5	3	2	4	5			
β_0	1,099	-0,511	0	0	0,511	0,511	-0,511	-1,099	0	0,511			
β	1,258	-0,479	0,072	0,072	0,623	0,623	-0,479	-1,114	0,072	0,623			

Можно выделить ряд утверждений о значениях Θ и β :

- при $\Theta > \beta$ вероятность того, что испытуемый справится с текущим заданием выше $\frac{1}{2}$ (чем больше разница между Θ и β , тем вероятность ближе к 1);
- при $\Theta < \beta$ вероятность того, что испытуемый справится с текущим заданием ниже $\frac{1}{2}$ (чем больше разница между Θ и β , тем вероятность ближе к 0);
- при $\Theta = \beta$ вероятность того, что испытуемый справится с текущим заданием равна 0,5.

Для применения однопараметрической модели Раша при адаптивном тестировании необходимо произвести начальное обучение системы. Для этого выбирается группа испытуемых с разным уровнем знаний в исследуемой области, предположительно 10 человек, для достижения достаточного уровня дифференцирования тестовых заданий по трудности ($M=10$). Рассмотрим основные этапы процедуры начального обучения системы.

1. Выбирается шкала оценки знаний испытуемого. Так как модель тестирования разрабатывается для проверки знаний студента по иностранному языку, то рекомендуется пятибалльная шкала оценки (неудовлетворительно, удовлетворительно, хорошо, отлично). Таким образом, получаем 4 группы заданий теста по уровню трудности.

2. После выбора шкалы оценки составляется база вопросов по исследуемой области, и испытуемым предлагается пройти тест. По результатам прохождения вычисляется оценка трудности каждого задания β_j .

3. Рекомендуется произвести корректировку базы вопросов, а именно:

– исключить задания, с которыми не справился ни один испытуемый, и задания, с которыми справились все испытуемые (эти задания несут мало информации об уровне знаний испытуемых в исследуемой области);

– при достаточно сильном отклонении среднего значения уровня трудности заданий $\bar{\beta}$ от 0 необходимо добавить вопросы в базы, при $\bar{\beta} \gg 0$ необходимо добавить «трудные» вопросы, а при $\bar{\beta} \ll 0$ «легкие» вопросы, при $\bar{\beta}$ близком к 0 набор тестовых заданий считается сбалансированным.

4. Затем, используя полученную оценку трудности заданий теста β , необходимо разделить задания на 4 группы сложности. При этом деление производится одним из двух способов:

– интервал делится на 4 равных подинтервала;

– интервал делится таким образом, чтобы в каждой группе оказалось равное количество вопросов.

Каждая группа сложности характеризуется минимальным и максимальным значением трудности задания в пределах данной группы.

Если используется первый способ деления, желательно, чтобы в каждой группе было достаточное количество вопросов для оценки знаний испытуемых.

Рассмотрим теперь алгоритм тестирования, который предлагается испытуемым. Введем обозначения: X – количество выданных заданий; Y – количество правильных ответов, данных испытуемым; Θ – текущий уровень подготовки испытуемого; i – номер текущего шага; R – оценка испытуемого (неудовлетворительно, удовлетворительно, хорошо или отлично); G – группа сложности, g – вопрос теста. Также для описания алгоритма необходимо ввести понятие критического количества вопросов $X_{\text{крит}}$ – количество вопросов для группы сложности, на которое испытуемый должен ответить (без изменения группы сложности), чтобы выставить ему оценку R . Значение $X_{\text{крит}}$ зависит от общего числа вопросов в базе и в каждой группе сложности и от времени тестирования; на начальном этапе определяется преподавателем. Во избежание постоянных смен уровней сложности при чередовании верных и ошибочных ответах тестируемого введём переменную η – коэффициент верных ответов для сохранения уровня сложности (изменяется от 0 до 1), также определяется преподавателем. Рекомендуется на начальном этапе использовать значение $\eta = 1/3$.

Исходные данные алгоритма: $i = 0$; $\Theta_0 = \bar{\Theta}$; $Y_0 = 0$; $X_0 = 0$. Исходная группа сложности $G_0 = G(\Theta_0)$ – множество вопросов, входящих в группу сложности, содержащую значение Θ_0 .

Процедура оценки уровня подготовки испытуемых (рисунок 2):

1. Выбирается задание из текущей группы сложности вопросов $g_i \in G_i$ и предлагается для ответа испытуемому.

2. При успешном ответе испытуемого, увеличивается количество правильных ответов.

3. Увеличивается количество выданных заданий, выданное задание исключается из набора заданий для данного испытуемого.

4. Вычисляется новый уровень подготовки испытуемого Θ_i по модели Раша ранее описанным способом.

5. Вычисляется группа сложности в зависимости от значения Θ_i . Принадлежность Θ_i к группе сложности определяется путем сравнения значения Θ_i с максимальным и минимальным значениями трудности заданий для каждой группы сложности. Если $\Theta_i \geq \beta_{\min}(G_k)$ и $\Theta_i < \beta_{\max}(G_k)$, то $G_i = G_k$ (k – индекс перебора по всем группам сложности, k изменяется от 1 до 4).

6. Если группа сложности изменилась, количество выданных заданий превышает η -ую часть от $X_{\text{крит}}$ и новая группа сложности больше максимальной (оценка 5) или меньше минимальной (оценка 2), то выставляется оценка в соответствии с группой сложности на предыдущем шаге (5 или 2).

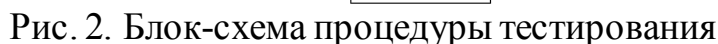
7. Если группа сложности изменилась, количество выданных заданий превышает η -ую часть от $X_{\text{крит}}$ и новая группа сложности не больше максимальной (оценка 5) и не меньше минимальной (оценка 2), то количество выданных вопросов и правильных ответов обнуляется и происходит возврат к шагу 1.

8. Если группа сложности изменилась, а количество выданных заданий не превышает η -ую часть от $X_{\text{крит}}$, то группа сложности возвращается к предыдущему значению (изменения не принимаются).

9. Если группа сложности не изменилась, не превышено количество критических вопросов и текущая группа сложности содержит еще хотя бы 1 вопрос, то происходит возврат к шагу 1.

10. Если группа сложности не изменилась, но при этом превышено количество критических вопросов или все вопросы текущей группы сложности уже были выданы испытуемому ранее, то выставляется оценка в соответствии с текущей группой сложности.

После ответа испытуемым на текущий вопрос результаты должны сохраняться в базе для вычисления Θ_i .



После корректировки значений β необходимо произвести расчет среднего уровня подготовки испытуемых заново. Затем заново формируются группы сложности. Возможно, что некоторые задания изменят группу сложности. Также существует возможность добавления в базу новых вопросов, желательно небольшими группами. В противном случае необходимо будет выполнить процедуру переобучения системы для балансировки уровня сложности заданий. При единичных добавлениях новым добавляемым вопросам присваивается средний уровень трудности.

3128

зависимости от данных ответов. При этом если ответы испытуемого нестабильны, то число заданных вопросов в пределах одного уровня сложности будет выше среднего, что позволит получить более точное представление об уровне его подготовленности.

Данная модель может помочь создателям систем тестирования и преподавателям, активно использующим технологии тестирования в обучении, усовершенствовать и повысить эффективность проведения тестового контроля знаний [14, 15].

Список литературы

1. Девтерова З.Р., Новые информационные технологии в преподавании иностранного языка в ВУЗе // Вестник Адыгейского государственного университета, № 4, 2006. С.157-159.
2. Шерматов Ш.М., Гафорова М.С., Использование компьютерных технологий и методов обучения в преподавании гуманитарных дисциплин // Вестник ТГУПБП, № 3 (51), 2012. С.262-267.
3. Маслова О.В., Медведева Т.Е., Пятков А.Г., Трудности использования online-тестирования как формы контроля знаний // сборник «Тенденции, наработки, инновации, практика в науке», Гданьск, 2014. – С.124-128.
4. Аванесов В.С. Item Response Theory: Основные понятия и положения // Педагогические измерения. № 2, 2007. – С. 3-28.
5. Авенсов В.С., Основные понятия и положения математической теории измерений (Item Response Theory) // Педагогические измерения [электронный ресурс]. URL: <http://testolog.narod.ru/Theory60.html> (01.09.14).
6. Использование модели Раша в пересчете баллов ЕГЭ // Сайт по менеджменту [электронный ресурс]. URL: <http://baguzin.ru/wp/?p=3370> (27.08.14).
7. Ким В.С. Тестирование учебных достижений // монография. – Уссурийск: Издательство УГПИ, 2007. – 214 с.
8. What is Rasch Analysis // Official site of Rasch analysis method [электронный ресурс]. URL: <http://www.rasch-analysis.com/rasch-analysis.htm> (27.08.14).
9. Nordin A.R., Ahmad Z.K, Lei M.T., Examining Quality of Mathemtics Test Items Using Rasch Model: Preminarily Analysis // International Conference on Education & Educational Psychology (ICEEPSY 2012), vol. 69, 2012. – С.2205-2214.
10. Malcolm J.R., Estimating Item Characteristic Curves // Applied psychological measurement vol. 3. № 3, 1979. – С.371-385.
11. Dodeen, H. (2004). The relationship between item parameters and item fit // Journal of Educational Measurement, vol. 41. – С.261-270.
12. B. N. Wright and G. N. Masters, Rating Scale Analysis: Rasch Measurement, MESA Press, Chicago, Ill, USA, 1982. – 206 с.

13. Чельщикова М.Б. *Теория и практика конструирования педагогических тестов // учебное пособие.* – М.: Логос, 2002. – 432 с.
14. Wagner-Menghin M., Preusche I., Schmidts M., *The Effects of Reusing Written Test Items: A Study Using the Rasch Model // International Scholarly Research Notices*, vol. 2013, 2013. – С.7-14.
15. Lukman N., Ibrahim N., Utaberta N., Hassanpour B., *Rasch Modeling Analysis in Assessing Student's Ability and Questions Reliability in Architecture Environmental Science Examination // Journal of Applied Sciences Research*, vol. 8(3), 2012. – С.1797-1801.

ИНТЕЛЛЕКТУАЛЬНАЯ ПРОГРАММНАЯ СИСТЕМА УПРАВЛЕНИЯ РИСКАМИ ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Наточая Е.Н., Моргунова А.Т.

Оренбургский государственный университет, г. Оренбург

Неопределенность образовательной деятельности является одним из факторов формирования компетенций обучающихся (Абрамова И.Г., Баташов М.В., Белоусова С.А., Зубок Ю.А., Кокорева О.Г., Костюков Т.П., Лысенко И.А., Никитина Н.Ш., Орёл А.Е., Щеглов П.Е., Чупров В.И.). Соответственно качественная подготовка кадров в сфере информационных технологий невозможна без грамотного управления образовательными рисками на строго научной основе.

Трудоемкость процесса управления образовательными рисками обуславливает необходимость его автоматизации. К настоящему времени существует несколько сотен систем, реализующих функции управления рисками. К наиболее функциональным программным продуктам по управлению рисками на российском рынке относятся: @RiskProfessionalforProject, Dekker TRAKKER, Enterpriseproject, IntelligentPlanner, Mesa/VistaRiskManager, RiskTrack, OpenPlan. В результате проведенного обзора существующих аналогов не было выявлено ни одного программного продукта, позволяющего в полной мере реализовать задачи управления рисками подготовки кадров в области информационных технологий, что послужило основанием разработки собственного программного средства.

Процесс управление рисками включает в себя следующие этапы:

- 1 Планирование управления рисками.
- 2 Идентификация выявленных рисков.
- 3 Анализ рисков.
- 4 Реагирование на риски.
- 5 Мониторинг и контроль рисков.

Входные данные для задачи управления рисками подготовки кадров в области информационных технологий не всегда можно формализовать, поэтому целесообразно применить интеллектуальные методы, основанные на нечеткой логике и продукционно-фреймовой модели представления знаний.

Метод нечеткого логического вывода включает следующие этапы:

- 1 Формирование базы правил и соответствующих функций принадлежности.
- 2 Фаззификация входных переменных на основе кусочно-линейной функции принадлежности трапеции.
- 3 Агрегирование подусловий в нечетких правилах продукций на основе операции максимума.

В качестве инструментальных средств разработки приложения и базы данных выбраны Visual Studio 2010 и СУБД SQ Lite в.3.2.

Основными функциями разработанной интеллектуальной программной системы являются: авторизация пользователя, создание базы знаний, редактирование структуры интеллектуальной модели и лингвистических переменных, работа с правилами вывода, оценка образовательных рисков, формирование отчетов по рискам.

Корректность работы программной системы проверена с помощью пакета прикладных математических программ системы MatLAB – FuzzyLogicToolBox и с помощью системы ESWin.

На рисунке 2 приведен контрольный пример оценки образовательных рисков на основе нечеткого логического вывода.

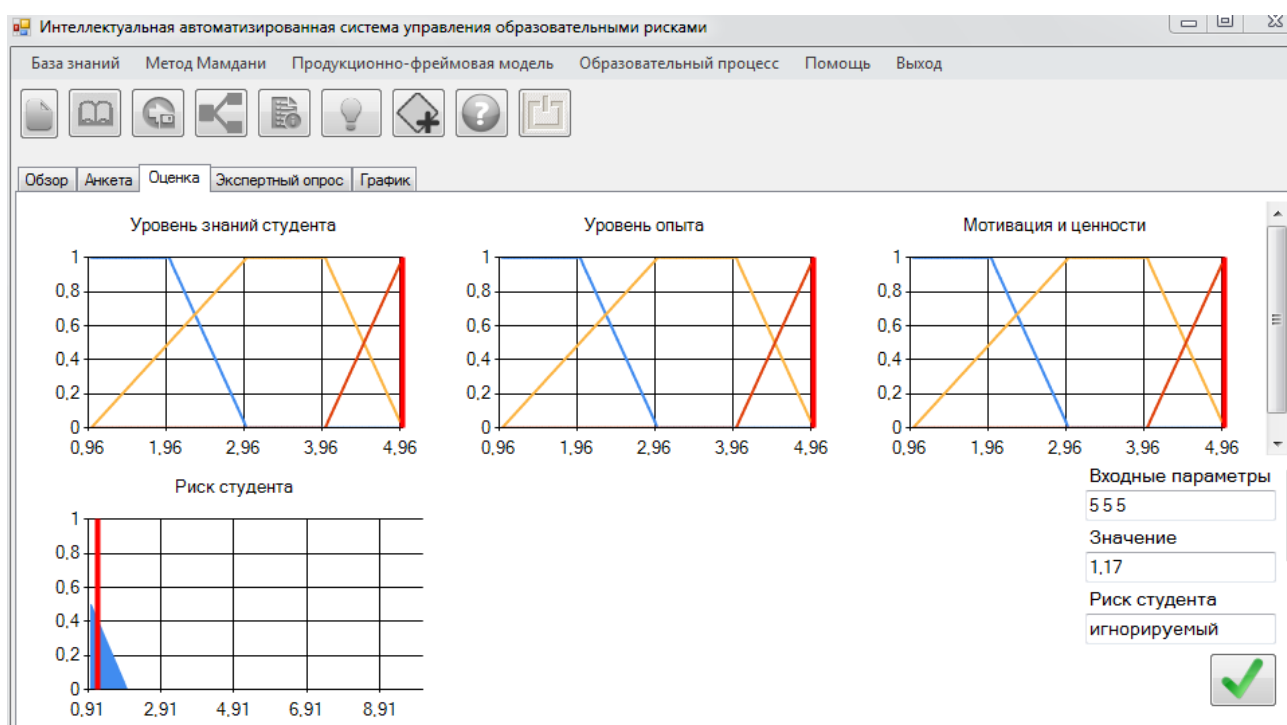


Рисунок 2 - Реализация метода нечеткой логики в программной системе

В контрольном примере введены следующие значения лингвистических переменных:

- уровень знаний студентов – 5 баллов;
- уровень практического опыта студентов – 5 баллов;
- уровень мотивационно-ценностного отношения студентов к сфере информационных технологий – 5 баллов.

В результате расчета в программной системе риск студента по 10-балльной шкале равен 1,17, что соответствует игнорируемую риску.

Контрольный пример тестирования продукционно-фреймовой модели в программной системе показан на рисунке 3.

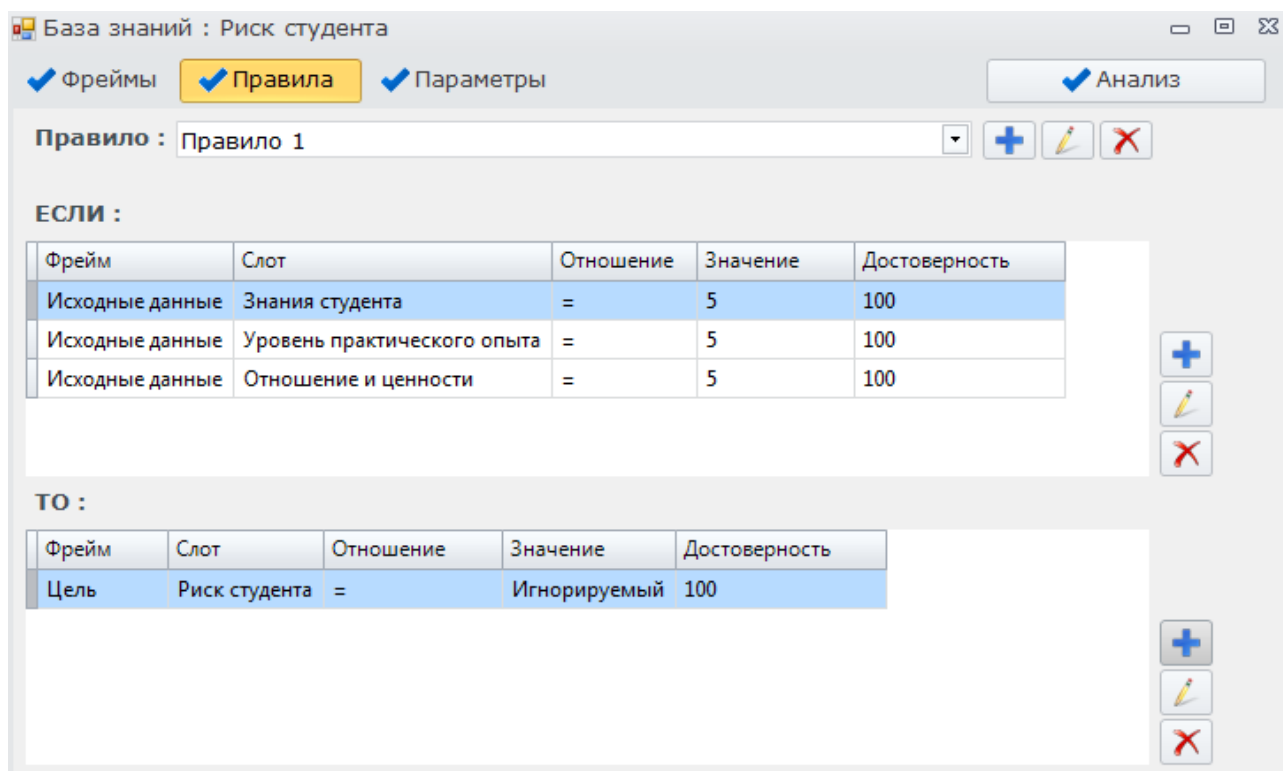


Рисунок 3 – Реализация продукционно-фреймовой модели в программной системе

Таким образом, все рассмотренные методы для данного набора входных данных оценили риск студента как игнорируемый.

Внедрение интеллектуальной программной системы управления рисками подготовки кадров в области информационных технологий проводилось в течение двух лет на базе кафедры программного обеспечения вычислительной техники и автоматизированных систем Оренбургского государственного университета. Экспериментальная и контрольная группы исследования образованы из студентов третьего курса направления «Информатика и вычислительная техника» и «Программная инженерия» в составе 14 человек каждая.

Цель опытно-экспериментальной работы состояла в проверке эффективности внедрения программной системы в образовательный процесс Оренбургского государственного университета.

В качестве критерия эффективности опытно-экспериментальной работы определено оптимальное соотношение развития профессиональных и общекультурных компетенций студентов.

В критериальный комплекс по показателю «профессиональные компетенции» включены такие признаки, как профессиональные знания, умения, навыки и отношение студентов к сфере информационных технологий.

По показателю «общекультурные компетенции» признаками выступили следующие функции студента: аксиологические, морально-нравственные и управленческо-организаторские.

Соотношение уровней развития профессиональных и общекультурных компетенций студентов определяет эффективность управляющих воздействий в образовательном процессе.

Для оценки эффективности эксперимента мы оценивали степень тесноты связи между двумя показателями - «профессиональные компетенции» и «общекультурные компетенции» студентов с помощью коэффициент взаимной сопряженности А.А. Чупрунова (С) и К. Пирсона (Р) [4].

Значения данных коэффициентов в ходе проведения эксперимента приведены в таблице 2.

Таблица 2 - Значения коэффициентов сопряженности

	Экспериментальная группа		Контрольная группа	
	«до»	«после»	«до»	«после»
Коэффициент сопряженности	P=0,517 C=0,427	P=0,741 C=0,779	P=0,519 C=0,429	P=0,503 C=0,411
Вид связи	слабая	сильная	слабая	слабая

Данные таблицы свидетельствуют о том, что после проведения эксперимента связь между уровнями развития профессиональных и общекультурных компетенций студентов в экспериментальной группе значительно усилилась. А в контрольной группе, она не только не усилилась, но и несколько уменьшилась.

В силу того, что проведенная нами опытно-экспериментальная работа позволила добиться сильной связи между показателями «профессиональные компетенции» и «общекультурные компетенции» студентов, можно сделать заключение о высокой эффективности управляющих воздействий в образовательном процессе.

Для определения итогового количества сдвигов в экспериментальной и контрольной группе мы использовали универсальный критерий Фишера. Согласно этому критерию доказано, что доля положительных сдвигов в экспериментальной группе больше, чем в контрольной при уровне значимости различий процентных долей $p \leq 0,01$.

Таким образом, теоретическая значимость проведенного исследования заключается в разработке методики оценки образовательных рисков с элементами искусственного интеллекта. Практическая значимость исследования состоит в разработке интеллектуальной программной системы управления рисками подготовки кадров в области информационных технологий, позволяющей повысить оперативность и объективность принимаемых управленческих решений.

Список литературы

1. Ишакова, Е.Н. Программная реализация управления образовательными рисками на основе нечеткого логического вывода / Ишакова Е.Н., Зубкова Т.М. // Наука и образование: фундаментальные основы, технологии, инновации: материалы Международной научной конференции, посвященной 60-летию Оренбургского государственного университета. – Оренбург: ООО ИПК «Университет», 2015. – С. 217-221.
2. Зубкова, Т.М. Программная система оценки рисков в сфере высшего образования с использованием продукционно-фреймовой модели // Т.М. Зубкова, Е.Н. Ишакова, А.С. Медведев // Вестник ОГУ. - 2014. - №1. - С. 183 - 188.
3. Экспертная система оценки рисков на основе продукционно-фреймовой модели. Свидетельство об официальной регистрации программы для ЭВМ № 2013660215 Российская Федерация / Е.Н. Ишакова, А.С. Медведев; РОСПАТЕНТ, Реестр программ для ЭВМ. - № 2013660215; заявл. 02.09.2013; зарегистр. 28.10.2013.
4. Климова, Т.Е. Методы корреляционного анализа в педагогике: учебное пособие / Т.Е. Климова. – Магнитогорск, МаГУ, 2000. – 96 с.

ОБЗОР МЕТОДОВ ОТЫСКАНИЯ ГАМИЛЬТОНОВЫХ ЦИКЛОВ В ГРАФЕ

Носов В.В., Орлов М.С.

Оренбургский государственный университет, г. Оренбург

Первая работа по теории графов, принадлежавшая известному швейцарскому математику Л. Эйлеру, появилась в 1736 г. Вначале теория графов казалась довольно незначительным разделом математики, так как она имела дело в основном с математическими развлечениями и головоломками.

В последние годы особую важность приобрели разделы математики, которые имеют отношение к развитию цифровых устройств, цифровой связи и цифровых вычислительных машин. Базой для преподавания этих дисциплин наряду с классическими методами анализа непрерывных физических моделей стали алгебраические, логические и комбинаторные методы исследования различных моделей дискретной математики.

В настоящее время, с развитием научно-технического прогресса, изучение теории графов обрело актуальность в связи с применением при разработке эффективных алгоритмов оптимизации тех или иных процессов.

Название «гамильтонов цикл» произошло от задачи «Кругосветное путешествие» предложенной ирландским математиком Вильямом Гамильтоном в 1859 году. Нужно было, выйдя из исходной вершины графа, обойти все его вершины и вернуться в исходную точку. Граф представлял собой укладку додекаэдра, каждой из 20 вершин графа было приписано название крупного города мира.

Если граф имеет простой цикл, содержащий все вершины графа по одному разу, то такой цикл называется гамильтоновым циклом, а граф называется гамильтоновым графом. Граф, который содержит простой путь, проходящий через каждую его вершину, называется полугамильтоновым. Это определение можно распространить на ориентированные графы, если путь считать ориентированным.

Гамильтонов цикл не обязательно содержит все ребра графа. Ясно, что гамильтоновым может быть только связный граф и, что всякий гамильтонов граф является полугамильтоновым. Заметим, что гамильтонов цикл существует далеко не в каждом графе.

Любой граф G можно превратить в гамильтонов граф, добавив достаточное количество вершин. Для этого, например, достаточно к вершинам $v_1, \dots, v_r$ графа G добавить вершины $u_1, \dots, u_r$ и множество ребер $\{(v_i, u_i)\} \{(u_i, v_{i+1})\}$.

Степенью вершины v называется число ребер $d(v)$, инцидентных ей, при этом петля учитывается дважды. В случае ориентированного графа различают степень $do(v)$ по выходящим дугам и $di(v)$ – по входящим.

Рассмотрим методы отыскания гамильтоновых циклов в графе.

Алгебраические методы определения гамильтоновых циклов не могут

быть применены с более чем несколькими десятками вершин, так как они требуют слишком большого времени работы и большой памяти компьютера. Однако неявный метод перебора имеет для большинства типов графов очень небольшой показатель роста времени вычислений в зависимости от числа вершин. Он может быть использован для нахождения гамильтоновых циклов в очень больших графах. Этот метод включает в себя построение всех простых цепей с помощью последовательного перемножения матриц. «Внутреннее произведение вершин» цепи $x_1, x_2, \dots, x_{k-1}, x_k$ определяется как выражение вида $x_2 \cdot x_3 \cdot \dots \cdot x_{k-1}$, не содержащее две концевые вершины x_1 и x_k . «Модифицированная матрица смежности» $B = [\beta(i, j)]$ – это $(n \times n)$ – матрица, в которой $\beta(i, j) = x_j$, если существует дуга из x_i в x_j и нуль в противном случае. Предположим, что есть матрица

$$PL = [pL(i, j)],$$

где $pL(i, j)$ – сумма внутренних произведений всех простых цепей длины $L (L \geq 1)$ между вершинами x_i и x_j для $x_i \neq x_j$. Положим $pL(i, i) = 0$ для всех i . Обычное алгебраическое произведение матриц определяется как

$$B \cdot PL = P'L + l = [p'L + l(s, t)],$$

т.е. $p'L + l(s, t)$ является суммой внутренних произведений всех цепей из x_s в x_t длины $l + 1$. Так как все цепи из x_k в x_t , представленные внутренними произведениями из $pL(k, t)$, являются простыми, то среди цепей

$$p'l + l(s, t) = \sum_k \beta(s, k) \cdot pl(k, t),$$

получающихся из указанного выражения, не являются простыми лишь те, внутренние произведения которых в $pL(k, t)$ содержат вершину x_s . Таким образом, если из $p'L + l(s, t)$ исключить все слагаемые, содержащие x_s , то получим $pL + l(s, t)$. Матрица $PL + l = [pL + l(s, t)]$, все диагональные элементы которой равны 0, является тогда матрицей всех простых цепей длины $L + 1$.

Вычисляя затем $B \cdot PL + 1$, находим $PL + 2$ и т.д., пока не будет построена матрица P_{n-1} , дающая все гамильтоновы цепи (имеющие длину $n - 1$) между всеми парами вершин. Гамильтоновы циклы получаются тогда сразу из цепей в P_{n-1} и тех дуг из G , которые соединяют начальную и конечную вершины каждой цепи. С другой стороны, гамильтоновы циклы даются членами внутреннего произведения вершин, стоящими в любой диагональной ячейке матрицы $B \cdot P_{n-1}$ (все диагональные элементы этой матрицы одинаковые).

Очевидно, что в качестве начального значения матрицы P следует взять матрицу смежности A графа, положив все ее диагональные элементы равными нулю.

Недостатки этого метода совершенно очевидны. В процессе умножения матриц каждый элемент матрицы PL будет состоять из большего числа членов вплоть до некоторого критического значения L , после которого число членов снова начнет уменьшаться. Это происходит вследствие того, что для малых значений L и для графов, обычно встречающихся на практике, число цепей

длины $L+1$, как правило, больше, чем число цепей длины L , а для больших значений L имеет место обратная картина. Кроме того, так как длина каждого члена внутреннего произведения вершин увеличивается на единицу, когда L увеличивается на единицу, то объем памяти, необходимый для хранения матрицы PL , растет очень быстро вплоть до максимума при некотором критическом значении L , после которого этот объем снова начинает уменьшаться.

Небольшая модификация вышеприведенного метода позволяет во много раз уменьшить необходимый объем памяти и время вычислений. Так как нас интересуют только гамильтоновы циклы и, как было отмечено выше, они могут быть получены из членов внутреннего произведения любой диагональной ячейки матрицы $B \cdot P_{n-1}$, то необходимо знать только элемент $p_{n-1}(1,1)$. При этом на каждом этапе не обязательно вычислять и хранить всю матрицу PL , достаточно лишь найти первый столбец PL . Эта модификация уменьшает необходимый объем памяти и время вычислений в n раз. Однако даже при использовании этой модификации программа для ЭВМ, написанная на языке $PL/1$, который позволяет строчную обработку литер и переменное распределение памяти, не была способна найти все гамильтоновы циклы в неориентированных графах с более чем примерно 20 вершинами и средним значением степени вершины, большим 4.

В противоположность алгебраическим методам метод перебора имеет дело с одной цепью, непрерывно продлеваемой вплоть до момента, когда либо получается гамильтонов цикл, либо становится ясно, что эта цепь не может привести к гамильтонову циклу. Тогда цепь модифицируется некоторым систематическим способом (который гарантирует, что, в конце концов, будут исчерпаны все возможности), после чего продолжается поиск гамильтонова цикла. В этом способе для поиска требуется очень небольшой объем памяти и за один раз находится один гамильтонов цикл.

Следующая схема перебора, использующая обычную технику возвращения, была первоначально предложена Робертсом и Флоресом. Начинают с построения $(k \times n)$ -матрицы $M = [m_{ij}]$, где элемент m_{ij} есть i -я вершина, для которой в графе $G(X, \Gamma)$ существует дуга (x_j, x_q) . Вершины x_q во множестве $\Gamma(x_j)$ можно упорядочить произвольно, образовав элементы j -го столбца матрицы M . Число строк k матрицы M будет равно наибольшей полустепени исхода вершины.

Метод состоит в следующем. Некоторая начальная вершина (скажем, x_l) выбирается в качестве отправной и образует первый элемент множества S , которое каждый раз будет хранить уже найденные вершины строящейся цепи. К S добавляется первая вершина (например, вершина a) в столбце x_l . Затем к множеству S добавляется первая возможная вершина (например, вершина b) в столбце a , потом добавляется к S первая возможная вершина (например, вершина c) в столбце b и т.д. Под «возможной» вершиной понимается вершина, еще не принадлежащая S . Существуют две причины,

препятствующие включению некоторой вершины на шаге r во множество $S = \{x_l, a, b, c, \dots, x_{r-1}, x_r\}$:

1) В столбце x_r нет возможной вершины.

2) Цепь, определяемая последовательностью вершин в S , имеет длину $n-1$, т.е. является гамильтоновой цепью.

В случае 2) возможны следующие случаи:

а) В графе G существует дуга (x_r, x_l) , и поэтому найден гамильтонов цикл.

б) Дуга (x_r, x_l) не существует и не может быть получен никакой гамильтонов цикл.

В случаях (1) и (2б) следует прибегнуть к возвращению, в то время как в случае (2а) можно прекратить поиск и напечатать результат (если требуется найти только один гамильтонов цикл), или (если нужны все такие циклы) произвести печать и прибегнуть к возвращению.

Возвращение состоит в удалении последней включенной вершины x_r из S , после чего остается множество $S = \{x_l, a, b, c, \dots, x_{r-1}\}$, и добавлении к S первой возможной вершины, следующей за x_r , в столбце x_{r-1} матрицы M . Если не существует никакой возможной вершины, делается следующий шаг возвращения и т.д.

Поиск заканчивается в том случае, когда множество S состоит только из вершины x_l и не существует никакой возможной вершины, которую можно добавить к S , так что шаг возвращения делает множество S пустым. Гамильтоновы циклы, найденные к этому моменту, являются тогда всеми гамильтоновыми циклами, существующими в графе.

Рассмотрим улучшение основного переборного метода Робертса и Флореса. Допустим, что на некотором этапе поиска построенная цепь задается множеством $S = \{x_1, x_2, \dots, x_r\}$ и что следующей вершиной, которую предполагается добавить к S , является $x^* \in S$. Рассмотрим теперь две следующие ситуации, в которых вершина является изолированной в подграфе, остающемся после удаления из $G(X, \Gamma)$ всех вершин, образующих построенную до этого цепь.

а) Если существует такая вершина $x \in X \setminus S$, что $x \in \Gamma(x_r)$ и $\Gamma - l(x) \subseteq S$, то, добавляя к S любую вершину x^* , отличную от x , мы не сможем в последующем достигнуть вершины x ни из какой конечной вершины построенной цепи, и, значит, эта цепь не сможет привести нас к построению гамильтонова цикла. Таким образом, в этом случае x является единственной вершиной, которую можно добавить к S для продолжения цепи.

б) Если существует такая вершина $x \in X \setminus S$, что $x \in \Gamma - l(x_l)$ и $\Gamma(x) \subset S \cup \{x^*\}$ для некоторой другой вершины x^* , то x^* не может быть добавлена к S , так как тогда в остающемся подграфе не может существовать никакой цепи между x и x_l . Цепь, определяемая множеством $S \cup \{x^*\}$, не может поэтому привести к гамильтонову циклу, а в качестве кандидата на добавление

к множеству S следует рассмотреть другую вершину, отличную от x^* .

Проверка условий (a) и (b) будет, конечно, замедлять итеративную процедуру, и для небольших графов (менее чем с 20 вершинами) не получается никакого улучшения первоначального алгоритма Робертса и Флореса. Но для больших графов эта проверка приводит к заметному сокращению необходимого времени вычислений, уменьшая его обычно в 2 или более раз.

Таким образом, из рассмотренных методов отыскания гамильтоновых циклов в графе наиболее эффективным является улучшенный метод перебора Робертса и Флореса.

Список литературы

1. Харари Ф. Теория графов / Пер.с англ. и предисл. В. П. Козырева. Под ред. Г. П. Гаврилова. Изд. 2-е. – М.: Едиториал УРСС, 2003. 296 с.
2. Мельников О.И. Теория графов в занимательных задачах. Изд.3, испр. и доп. 2009. 232 с.
3. Дистель Р. Теория графов Пер. с англ. - Новосибирск: Издательство института математики, 2002. 336 с.
4. Кирсанов М. Н. Графы в Maple. М.: Физматлит, 2007. 168 с.

ОБ ОДНОМ ОПИСАНИИ РАДИКАЛА ДЖЕКОБСОНА ДЛЯ АЛГЕБР ЛИ

Носов В.В., Павленко А.Н., Пихтилькова О.А.
Оренбургский государственный университет, г. Оренбург

В работе рассматривается вопрос гомологического описания радикала Джекобсона для алгебр Ли. Предлагается считать радикалом Джекобсона алгебры Ли L пересечение аннуляторов всех неприводимых PI -представлений алгебры Ли L и саму алгебру L если их нет.

На Международной алгебраической конференции, посвященной 100-летию со дня рождения А. Г. Куроша (Москва, МГУ им. М. В. Ломоносова, 2008) Борис Исаакович Плоткин поставил вопрос о гомологическом описании радикала Джекобсона для алгебр Ли.

Следующее определение радикала Джекобсона было дано Е. Маршаллом: назовем радикалом Джекобсона $J(L)$ алгебры Ли L пересечение максимальных идеалов и саму алгебру L , если их нет [**Ошибка! Источник ссылки не найден.**].

Отметим, что для конечномерной алгебры Ли над полем характеристики нуль нильпотентный радикал совпадает с радикалом Джекобсона [**Ошибка! Источник ссылки не найден.**].

Для бесконечномерных алгебр Ли свойства радикала Джекобсона исследовал F. Kubo [**Ошибка! Источник ссылки не найден.**].

В 1963 г. В. Н. Латышев ввел новый класс алгебр Ли [**Ошибка! Источник ссылки не найден.**], которые он назвал специальными по аналогии с йордановыми алгебрами.

Скажем, что алгебра Ли L специальная или SPI -алгебра Ли, если существует ассоциативная PI -алгебра A такая, что L вложена в $A^{(-)}$ как алгебра Ли, где $A^{(-)}$ – алгебра Ли, заданная на A с помощью операции коммутирования $[x, y] = xy - yx$.

Известно, что существует специальная алгебра Ли, локально нильпотентный радикал которой строго содержится в радикале Джекобсона [**Ошибка! Источник ссылки не найден.**, пример 1].

Обозначим через $Irr(L)$ пересечение аннуляторов неприводимых модулей над алгеброй Ли L и саму алгебру L если их нет.

Пусть M неприводимый L -модуль. Обозначим через $A(M)$ ассоциативную алгебру, порожденную элементами алгебры L в алгебре $End(M)$.

Назовем PI -представлением алгебры Ли L представление алгебры L в алгебре эндоморфизмов $End(M)^{(-)}$ модуля M над алгеброй L , для которого ассоциированная алгебра представления $A(L)$ является PI -алгеброй.

Обозначим через $IrrPI(L)$ пересечение аннуляторов всех неприводимых PI -представлений алгебры Ли L и саму алгебру L если их нет.

Ю. А. Бахтурин использовал пересечение аннуляторов конечномерных неприводимых представлений для доказательства теоремы Леви-Мальцева для конечномерных алгебр Ли [Ошибка! Источник ссылки не найден.]. Известно, что для конечномерных алгебр Ли пересечение аннуляторов конечномерных представлений совпадает с нильпотентным радикалом [Ошибка! Источник ссылки не найден.] и, следовательно, с радикалом Джекобсона для поля нулевой характеристики [Ошибка! Источник ссылки не найден.].

Обозначим через $IrrFin(L)$ пересечение аннуляторов всех неприводимых конечномерных модулей над алгеброй Ли L и саму алгебру L если их нет.

Л. А. Симонян рассмотрел пары $L \subseteq A^{(-)}$, где L – алгебра Ли над полем F характеристики нуль, A – локально конечная ассоциативная алгебра [Ошибка! Источник ссылки не найден.]. Он ввел обозначение $J_A(L) = L \cap J(A)$.

В [Ошибка! Источник ссылки не найден.] было доказано:

1. Всякий идеал алгебры Ли L , состоящий из нильпотентных в A элементов, лежит в $J_A(L)$;

2. Если R – локально разрешимый идеал L , то $[R, L] \subseteq J_A(L)$.

Докажем следующие утверждения.

Теорема 1. Пусть L – произвольная алгебра Ли. Тогда

$$Irr(L) = L \cap J(U(L)),$$

где $U(L)$ – универсальная обертывающая алгебра.

Доказательство. Пусть M – произвольный неприводимый $U(L)$ -модуль. Тогда M также является неприводимым L -модулем.

Имеет место включение $Irr(L)$ содержится в аннуляторе $U(L)$ модуля M .

Так как радикал Джекобсона $J(U(L))$ ассоциативной алгебры $U(L)$ совпадает с пересечением аннуляторов всех неприводимых $U(L)$ -модулей, получим $Irr(L) \subseteq J(U(L))$.

Пусть $x \in L \cap J(U(L))$, M – произвольный неприводимый L -модуль, $A(L)$ – ассоциированная с представлением L ассоциативная алгебра и $\alpha: L \rightarrow A(L)^{(-)}$ – гомоморфизм алгебр Ли, задающий L -модуль M .

Тогда существует его продолжение $\bar{\alpha}: U(L) \rightarrow A(L)$ где $\bar{\alpha}$ – гомоморфизм ассоциативных алгебр и $\bar{\alpha}(l) = \alpha(l)$ для всех $l \in L$.

Следовательно, M также является $U(L)$ -модулем.

Модуль M неприводим над $U(L)$ тогда и только тогда, когда неприводимым является L -модуль M .

Следовательно, x содержится в аннуляторе модуля M и $x \in Irr(L)$.

Включение $J(U(L)) \subseteq Irr(L)$ завершает доказательство теоремы.

Пример 1. Пусть $L = \{\alpha x + \beta y | \alpha, \beta \in F\}$ – двумерная абелева алгебра Ли над полем F .

Ее универсальная обертывающая алгебра $U(L)$ изоморфна кольцу многочленов $F[x, y]$ от коммутирующих переменных x и y .

Как известно, $J(F[x, y]) = 0$. Следовательно, $Irr(L) = 0$.

Этот пример не противоречит нашим представлениям о радикалах конечномерных алгебр Ли. Нильпотентный радикал $N(L)$ алгебры Ли L также равен нулю.

Пример 2. Дадим новую интерпретацию следующего известного примера.

Пусть F – поле характеристики нуль, $F[x]$ – кольцо многочленов.

Зададим для произвольного $f(x) \in F[x]$ три отображения:

$$a(f(x)) = f'(x), b(f(x)) = x \cdot f(x), e(f(x)) = f(x).$$

Легко проверить, что тождественное отображение e коммутирует с a и b , $[a, b] = e$.

Мы получили представление трехмерной разрешимой алгебры Ли

$$L = \{\alpha x + \beta y + \gamma z \mid \alpha, \beta, \gamma \in F\}$$

в алгебре эндоморфизмов $End(F[x])$.

Легко проверить, что векторное пространство $F[x]$ является неприводимым L -модулем. Следовательно, $Irr(L) = 0$.

Алгебра $U(L)$ соответствует градуированная алгебра, которая является алгеброй многочленов от трех коммутирующих переменных [6].

Согласно теореме Размыслова-Кемера-Брауна радикал Джекобсона конечнопорожденной PI -алгебры нильпотентен [Ошибка! Источник ссылки не найден.], [Ошибка! Источник ссылки не найден.]. Из первичности $U(L)$ следует, что $J(U(L)) = 0$.

Пусть M – точный неприводимый L -модуль задающий PI -представление алгебры L .

Тогда M -неприводимый $U(L)$ -модуль, алгебра $A(L)$ является гомоморфным образом алгебры $U(L)$ и, следовательно, удовлетворяет тождеству разрешимости степени 2, что невозможно. Согласно теореме Познера [Ошибка! Источник ссылки не найден.], алгебра $A(L)$ изоморфна алгебре матриц D_2 порядка n над телом D .

Следовательно, $IrrPI(L) = N(L) = \{\alpha e \mid \alpha \in F\}$.

Алгебра Ли L является разрешимой степени 2. Получим, $P(L) = L$ (первичный радикал совпадает с разрешимым для конечномерных алгебр [Ошибка! Источник ссылки не найден.]).

Используя рассуждения аналогичные рассуждениям из примера 2, можно доказать следующую теорему.

Теорема 2. Пусть L – конечномерная алгебра Ли над полем F характеристики нуль. Тогда $IrrPI(L) = N(L)$, где $N(L)$ – нильпотентный радикал алгебры Ли L .

Теорема 3. Пусть основное поле имеет нулевую характеристику. Тогда следующие включения в общем случае строгие: $Irr(L) \subset IrrPI(L) \subset IrrFin(L)$.

Доказательство. Строгость первого включения следует из примера 2.

Докажем строгость второго включения.

Пусть $F \subseteq K$ – расширение поля F , которое не является конечномерным. Таким, например, будет поле рациональных функций с коэффициентами из F . Алгебра $sl_2 K$ является простой алгеброй Ли над K . Несложно проверить, что $sl_2 K$ является простым кольцом Ли и, следовательно, простой алгеброй Ли над F .

Алгебра $sl_2 K$ имеет точное PI –представление над двумерным арифметическим векторным пространством K^2 . Следовательно, $IrrPI(sl_2 K) = 0$.

В силу бесконечномерности над полем F и простоты алгебра $sl_2 K$ не может иметь конечномерных неприводимых представлений над F .

Следовательно, $IrrFin(sl_2 K) = sl_2 K$.

Предлагаем считать радикалом Джекобсона алгебры Ли L пересечение аннуляторов всех неприводимых PI –представлений алгебры Ли L и саму алгебру L если их нет. Из теоремы 2 и результата Маршалла следует, что $IrrPI(L) = J(L)$ для конечномерных алгебр Ли над полем характеристики нуль.

Список литературы

1. Marshall E. I. The Frattini subalgebras of a Lie algebra. J. London Math. Soc. 1967. V. 42. P. 416-422.
2. Kubo F. Infinite-dimensional Lie algebras with null Jacobson radical // Bull. Kyushu Inst. Technol. Math. Nat. Sci. 1991. V. 38. P. 23-30.
3. Латышев В. Н. Об алгебрах Ли с тождественными соотношениями // Сиб. мат. журнал. 1963. Т. 4. N 4. С. 821-829.
4. Пихтильков С. А. О локально нильпотентном радикале специальных алгебр Ли // Фундаментальная и прикладная математика. 2002. Т. 8. Вып. 3. С. 769-782.
5. Бахтурин Ю. А. Тождества в алгебрах Ли. М.: Наука, 1985.
6. Бурбаки Н. Группы и алгебры Ли (главы I-III). М.: Мир, 1976.
7. Симонян Л. А. О радикале Джекобсона алгебры Ли // Латвийский математический ежегодник. 1993. Вып. 34. С. 230-234.
8. Кемер А. Р. Тождества Капелли и нильпотентность радикала конечно порожденной PI -алгебры // ДАН СССР. 1980. Т. 255. N 4. С. 793-797.
9. Braun A. The nilpotency of the radical in a finitely generated PI -ring // J of Algebra. 1984. V. 89. N 2. P. 375-396.
10. Бейдар К. И., Пихтильков С. А. Первичный радикал специальных алгебр Ли // Фундаментальная и прикладная математика. 2000. Т. 6. Вып. 3. С. 643-648.
11. Херстейн И. Некоммутативные кольца. М.: Мир, 1972.

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ. КРАТКИЙ ИСТОРИЧЕСКИЙ ОБЗОР

Острая О.В.

ГОУ ВО «Оренбургский государственный университет», г. Оренбург

Слово «Модель» происходит от латинского *modulus* – «мера, аналог, образец». Оно означает систему, исследование которой может дать информацию о какой-либо другой, более сложной системе. Моделирование, то есть построение моделей, применяется для того, чтобы получить некоторое упрощённое представление о реальном устройстве или природном явлении, о процессе, изучающемся в природе или технике. Моделирование как метод познания, так или иначе, интуитивно или осознанно, применялось человечеством еще на заре его развития. Например, на стенах древних храмов предков южно-американских индейцев исследователями обнаружены своеобразные графические модели мироздания. Учение о моделировании возникло в средние века. Выдающаяся роль в создании этого учения принадлежит гению эпохи Возрождения Леонардо да Винчи (1452-1519). Гениальный русский полководец А.В. Суворов (1730—1800) перед атакой крепости Измаил тренировал солдат на модели измаильской крепостной стены, построенной специально в тылу.

Знаменитый русский механик-самоучка И.П. Кулибин (1735-1818) создал модель одноарочного деревянного моста через Неву, а также ряд металлических моделей мостов. Они были полностью технически обоснованы и получили высокую оценку Л. Эйлера и Д. Бернулли. К сожалению, ни один из этих мостов не был построен.

Широко известны работы Н.Н. Моисеева по моделированию систем управления. В частности, для проверки одного нового метода математического моделирования была создана математическая модель Синопского сражения – последнего сражения эпохи парусного флота. 18 (30) ноября 1853 г. в сражении у мыса Синоп русская эскадра под командованием адмирала П.С. Нахимова (1802-1855) разгромила главные силы турецкого флота. Моделирование с помощью вычислительной машины подтвердило, что Нахимов действовал безошибочно. Он так верно расставил корабли русской эскадры и нанес первый удар, что единственным спасением турок могло стать отступление. Они не отступили и были разгромлены.

Сложность и громоздкость технических объектов, которые могут изучаться методами моделирования, практически неограниченны. Во второй половине XX века работа всех крупных сооружений опробовалась на моделях. Имеются в виду модели плотин, каналов, крупнейших электростанций (Братской, Красноярской ГЭС), систем дальних электропередач, образцов военных систем и др.

Под *математическими моделями* понимаются основные закономерности и связи, присущие изучаемому явлению и представленные с помощью формул или уравнений, наборов правил или соглашений, выраженных в математической форме. В современной науке математические модели являются одним из основных инструментов познания человеком явлений окружающего мира. Они использовались для описания изучаемых явлений в математике, механике, физике и других точных науках еще на ранних этапах развития разных областей естествознания и техники. Например, законы Ньютона полностью описывают движение планет вокруг Солнца. Используя основные законы механики, относительно нетрудно составить уравнения, описывающие движение космического аппарата, например, от Земли к Луне. Однако далеко не всегда возможно получить решение этих уравнений в виде простых выражений. Для расчета траекторий космических аппаратов служат компьютеры.

Применение компьютеров в математическом моделировании изменило само понятие «решить задачу». Ранее исследователь обходился созданием математической модели. Если априори полагалось, что эта модель адекватно описывает изучаемое явление, и удавалось доказать, что решение поставленной задачи в принципе существует, то этого было достаточно. Как правило, не существует простых формул, описывающих поведение модели. Тогда единственный путь решения задачи – свести его к вычислениям, к применению численных методов решения задач. В этом случае необходим конкретный алгоритм, указывающий последовательность вычислительных и логических операций, которые должны быть произведены для получения численного решения.

С алгоритмами связана вся история математики. Еще древнегреческим ученым были известны алгоритмы решения различных вычислительных задач, например, алгоритм вычисления числа "пи" с высокой точностью. Само слово "алгоритм" произошло от имени средневекового восточного ученого Аль-Хорезми (ок. 783-ок. 850), который впервые изложил порядок действий при решении алгебраических уравнений первой и второй степеней. Именно набор инструкций, описывающих порядок действий, выполняемых при решении той или иной задачи, мы называем алгоритмом.

В XVII в. И. Ньютон предложил эффективный численный метод решения алгебраических уравнений, а Л. Эйлер в XVIII в. – численный метод решения обыкновенных дифференциальных уравнений. Как известно, модифицированные методы И. Ньютона и Л. Эйлера и в наше время занимают почетное место в арсенале вычислительной математики. Ее предметом является выбор расчетной области и расчетных точек, в которых вычисляются характеристики моделируемого объекта, и правильная замена исходной математической модели ее аналогом, пригодным для расчета, т. е. некоторой дискретной моделью. Поскольку модели должны представлять изучаемые явления в необходимой полноте, понятно, что они становятся весьма

сложными. В математические модели входят величины, подлежащие определению и зависящие от большого числа переменных и постоянных параметров.

Аппарат классической математической физики приспособлен для работы с линейными моделями. В этом случае сумма (суперпозиция) частных решений дифференциального уравнения также является его решением. Значит, отыскав частное решение уравнения для линейной модели, можно с помощью принципа суперпозиции получить и общее решение. На этом пути в традиционной математической физике были получены замечательные результаты. Однако она становится бессильной, если встречается с нелинейными моделями. Принцип суперпозиции здесь неприменим, и алгоритмов для построения общего решения не существует. Поэтому для нелинейных моделей получено немного окончательных теоретических результатов, в то время как модели реальных процессов, происходящих в природе и технике, оказываются именно нелинейными.

Методология математического моделирования кратко выражена триадой "модель – алгоритм – программа", сформулированной основоположником отечественного математического моделирования академиком А.А. Самарским (1919-2008). Школой А.А. Самарского была разработана технологии «вычислительного эксперимента», предназначенная для изучения явлений окружающего мира, когда натурный эксперимент оказывается слишком дорогим и сложным.

Во многих важных областях исследований натурный эксперимент и вовсе невозможен, так как он либо запрещен (например, при изучении здоровья человека), либо слишком опасен (например, при изучении экологических явлений), либо просто неосуществим (например, при изучении астрофизических явлений).

Математическое моделирование с помощью компьютеров применяется не только для решения фундаментальных научных проблем, но и для разработки технологических процессов в промышленности – создание «вычислительных технологий». Для случаев, когда технологические процессы описываются с помощью хорошо известных математических моделей, для расчета которых уже есть эффективные вычислительные алгоритмы, разработаны пакеты прикладных программ, технология вычислительного эксперимента позволяет создавать новые программы и совершенствовать средства общения человека с компьютером.

Для исследования нелинейных процессов в микромире были разработаны соответствующие численные методы с применением компьютеров и компьютерных сетей (сетевых grid-технологий), ориентированные на решение задач физики элементарных частиц. Алгоритмы квантово-механических расчетов совершенствуются так же быстро, как и алгоритмы, применяющиеся в других областях вычислительной математики.

Биология остается преимущественно экспериментальной и описательной наукой, история математического моделирования биологических процессов насчитывает немногим более 20 лет, однако мы уже можем выделить немало биологических проблем, для решения которых определяющей методологией стал вычислительный эксперимент.

Математическое моделирование и вычислительный эксперимент стали ведущими методологиями для изучения глобальных моделей процессов и явлений на Земле, например климата Земли. Проведение работ такого рода стимулировалось деятельностью Римского клуба, – международной общественной организации, которая объединяет представителей мировой политической, финансовой, культурной и научной элиты. Основной задачей этой организации является привлечение внимания мировой общественности к важнейшим проблемам человечества.

Первая глобальная модель была опубликована в 1971 г. американским специалистом по теории управления Д. Форрестером. Компьютерные игры, проведенные этим ученым с глобальной моделью, показали, что в середине XXI века человечество ждет кризис, к причинам которого относятся истощение природных ресурсов, падение численности населения и производства продуктов, усиливающееся загрязнение окружающей среды.

Другим примером глобального моделирования является моделирование «ядерной зимы», выполненное в ВЦ АН СССР В.В. Александровым и Г.Л. Стенчиковым под руководством академика Н.Н. Моисеева. Полученные ими результаты дали человечеству, в том числе политикам, неопровержимые аргументы против ядерной войны, даже так называемой «ограниченной ядерной войны».

История методологии математического моделирования убеждает: она может и должна быть интеллектуальным ядром информационных технологий, всего процесса информатизации общества.

Технические, экологические, экономические и иные системы, изучаемые современной наукой, уже не поддаются полноценному исследованию обычными теоретическими методами. Прямой натурный эксперимент над ними часто слишком долг, дорог, опасен, или попросту невозможен. Цена ошибок и просчетов недопустимо высока. Поэтому математическое моделирование является неизбежной составляющей научно-технического прогресса.

Список литературы

1. Амосов, П.В. Математическое моделирование загрязнения подземных вод от потенциального объекта изоляции радиационно опасных материалов / П.В. Амосов, А.В. Наумов, Н.В. Новожилова // *Экологические системы и приборы*, 2008. – № 3. – С. 43-46.

2. Боголюбов, А.Н. Советская школа механики машин / А.Н. Боголюбов; *Акад. наук СССР. – М.: Наука, 1975. – 176 с.*

3. Голубева, Н.В. Математическое моделирование систем и процессов [Электронный ресурс] / Голубева Н.В. – Лань, 2013. – 192 с. – Режим доступа: http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=4862.

4. История и методология естественных наук / под ред. И.Г. Башмаковой, И.А. Тюлина; Моск. гос. ун-т им. М. В. Ломоносова, Секция истории и методологии естествознания Ученого совета по естественным наукам. – М.: Изд-во Моск. ун-та, 1971. – 240 с.

5. Самарский, А.А. Математическое моделирование. Идеи. Методы. Примеры / А.А. Самарский, А.П. Михайлов. – М.: Физматлит, 2005. – 316 с.

О ЦЕЛЕСООБРАЗНОСТИ ИСПОЛЬЗОВАНИЯ ЛЕКЦИОННЫХ ЗАНЯТИЙ ПРОПЕДЕВТИЧЕСКОГО ХАРАКТЕРА С ПРИМЕНЕНИЕМ МУЛЬТИМЕДИЙНЫХ ТЕХНОЛОГИЙ ПРИ ИЗУЧЕНИИ МАТЕМАТИЧЕСКИХ ДИСЦИПЛИН ЕСТЕСТВЕННОНАУЧНЫХ НАПРАВЛЕНИЙ

Павленко А.Н., Пихтилькова О.А.

Оренбургский государственный университет, г. Оренбург

Как правило, изучение каждого раздела математической дисциплины в вузе происходит следующим образом:

- 1) введение некоторого нового математического понятия (понятий);
- 2) доказательство ряда его (их) свойств;
- 3) рассмотрение приложений, важность практической применимости которых часто для студентов является сомнительной.

Очевидно, что такой подход к обучению весьма абстрактного и часто громоздкого материала не способствует высокой мотивации к его изучению.

Рассмотрение в начале каждого раздела типичных задач, приводящих к целесообразности введения нового математического понятия, не решает полностью данную проблему. Например, изучение дифференциального исчисления для функции одной переменной начинается с рассмотрения двух задач [1], приводящих к понятию производной: задаче о нахождении уравнения касательной к графику функции и задаче о нахождении мгновенной скорости материальной точки. В данном случае у студентов все равно возникают вопросы о возможности практического применения теперь уже самих этих задач: «А само уравнение касательной нам зачем?» и «Зачем так сложно находить скорость, если можно просто посмотреть на спидометр?».

Для усиления мотивации студентов к изучению математических дисциплин и, как следствие, повышению эффективности обучения, представляется целесообразным проводить параллельное изучение математических понятий и их свойств, с их приложениями и историческими сведениями об их появлении и развитии. Таким образом, должна возрасти роль межпредметных связей математики, физики (и других естественных наук) и истории математики [2].

Вернувшись к задачам о введении понятия производной можно заметить, что вывод уравнения касательной можно рассматривать вместе с методом касательных (метод Ньютона) приближенного решения алгебраических уравнений [3]. Кроме того, ввести понятие производной можно, рассматривая практически ориентированные задачи на максимум и минимум [4] и некоторые задачи, сводящиеся к дифференциальным уравнениям [5].

Для повышения эффективности учебного процесса предлагается новый подход к изучению разделов математики. Первоначально предполагается рассмотреть основные идеи раздела, как он связан с остальной математикой и другими науками, и очертить круг его практических приложений. Задачей данного предварительного изучения раздела состоит в том, чтобы студенты

восприняли «общую картину» материала, понять для чего он нужен, пока не перегружая свое внимание на данном этапе излишними частностями, которые, как правило, трудновоспринимаемы и резко снижают мотивацию к изучению математики.

Отсюда следует, что обучение разделу математики целесообразно проводить дважды.

1. Первый этап – пропедевтический (одно лекционное занятие с демонстрацией учебного фильма или презентации). В ходе данного занятия рассматриваются основные идеи математического раздела.

2. Второй этап представляет собой традиционное изложение материала.

При организации пропедевтической лекции (примеры подобных занятий в [6-10] и в приведенной там литературе) целесообразно придерживаться следующей структуры:

1) перечисление разделов математики и других дисциплин (для их самостоятельного повторения), на которые опирается данный материал;

2) исторические сведения о данном разделе;

3) основные понятия и идеи нового материала;

4) обзор приложений.

Следует отметить, что для наилучшего восприятия смысла математического раздела, пункты 2-4 целесообразнее изучать не последовательно, а одновременно.

Учитывая экспериментальный характер естественнонаучных дисциплин, на пропедевтических занятиях целесообразно использование эксперимента и при рассмотрении математических утверждений. Особенно это относится к тем теоремам, которые имеют сложные и громоздкие доказательства.

В качестве примера можно рассмотреть в разделе «Нормальное распределение» дисциплины «Теория вероятностей и математическая статистика» экспериментальное обоснование [11, 12] в среде компьютерного математического пакета MathCAD [13] центральной предельной теоремы для одинаково распределенных слагаемых. Данная теорема является одной из наиболее важных теорем всей дисциплины.

Теорема [14]. Если $X_1, X_2, \dots, X_n$ - независимые случайные величины, имеющие один и тот же закон распределения с конечными математическим ожиданием m и дисперсией σ^2 , то при неограниченном увеличении n закон распределения суммы

$$Y_n = \sum_{k=1}^n X_k$$

неограниченно приближается к нормальному.

Для случая, когда величины $X_1, X_2, \dots, X_n$ распределены по показательному закону [14] (рисунок 1) интуитивно ясно, что и их сумма Y_n должна быть распределена по показательному закону. Однако, численное нахождение закона распределения в среде пакета MathCAD (см. рисунок 2) показывает, что центральная предельная теорема верна и в данном случае.

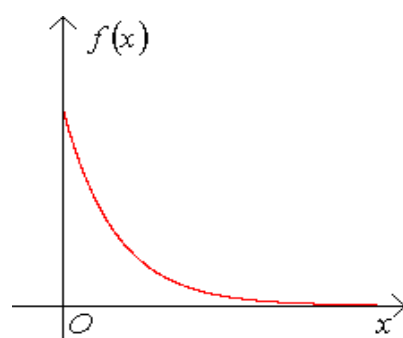


Рисунок 1

$i := 1..50000$

$n1 := 1$

$n2 := 2$

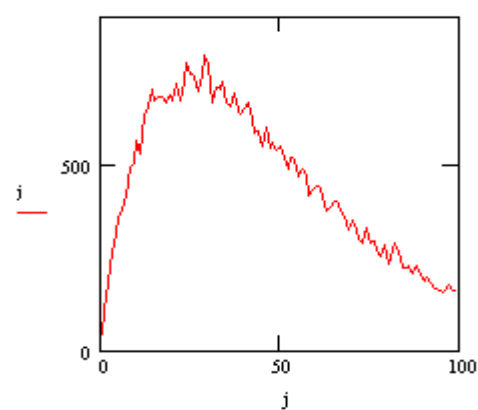
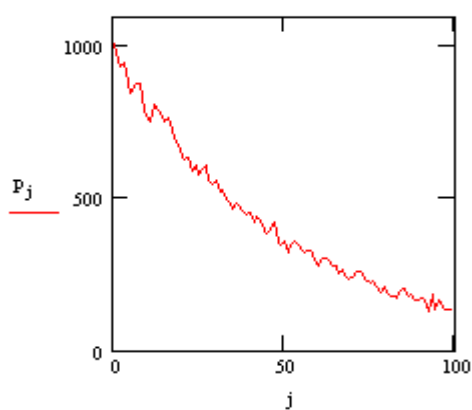
$x_i := \text{mean}(\text{rexp}(n1, 2))$

$y_i := \text{mean}(\text{rexp}(n2, 2))$

$j := 0..100$ $\text{int}_j := \frac{j}{100}$

$P := \text{hist}(\text{int}, x)$

$Q := \text{hist}(\text{int}, y)$



$n3 := 5$

$n4 := 80$

$z_i := \text{mean}(\text{rexp}(n3, 2))$

$t_i := \text{mean}(\text{rexp}(n4, 2))$

$R := \text{hist}(\text{int}, z)$

$S := \text{hist}(\text{int}, t)$

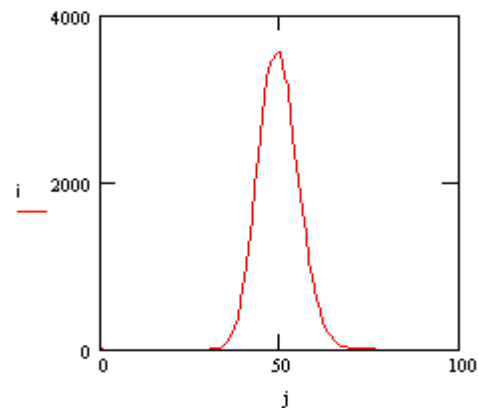
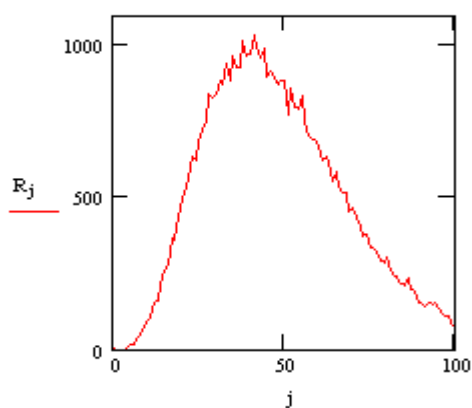


Рисунок 2

Список литературы

1. Фихтенгольц, Г.М. Курс дифференциального и интегрального исчисления / Г. М. Фихтенгольц. – М.: Физматлит, 2007. Т. 1. - 2007. - 680 с.: ил. - Алф. указ.: с. 671-679. - ISBN 978-5-9221-0436-4.
2. Арнольд, В.И. О преподавании математики / В.И. Арнольд // УМН. – 1998 - том 53, выпуск 1(319). – С. 229–234.
3. Пирумов, У.Г. Численные методы: учеб. пособие для студ. вузов / У.Г. Пирумов. – М.: Дрофа, 2004. – 224 с.: ил. - ISBN 5-7107-8777-9.
4. Павленко, А.Н. О введении понятия производной в курсе математического анализа (математики) экономических направлений [Электронный ресурс] / А.Н. Павленко, О.А. Пихтилькова // Университетский комплекс как региональный центр образования, науки и культуры: материалы Всерос. науч.-метод. конф. (с междунар. участием), 4-6 февр. 2013 г., Оренбург / Оренбург. гос. ун-т. – Электрон. дан. – Оренбург, 2013. – С. 1268–1271.
5. Битнер, Г.Г. Обыкновенные дифференциальные уравнения: учебное пособие / Г.Г. Битнер. – Ростов н/Д: Феникс, 2012. – 205 с. - ISBN 987-5-222-19438-6.
6. Чаплыгин, С.А. Пропедевтический курс механики / С.А. Чаплыгин. – изд. 2-е. – М.: Госиздат, 1923. – 242 с.
7. Сазонов, В.Н. Пропедевтический курс математического анализа: конспект лекций / В.Н. Сазонов. – М.: Моск. станкоинструм. ин-т., 1989. - 52 с. : ил.
8. Кузнецова, В.А. О целесообразности вводного пропедевтического курса в университете / В.А. Кузнецова // Вестн. Тамбовского гос. ун-та. – 2003. - № 3, том: 8. – С. 406.
9. Светлова, Н.И. Школьная математика и подготовка студентов специальности «Математические методы в экономике» / Н.И. Светлова // Вестн. Нижегородского ун-та им. Лобачевского. – 2011. – № 3(3). – С. 106–109.
10. Темникова И.С. Восстановление школьных и пропедевтика вузовских математических знаний с помощью компьютерных средств обучения: материалы Международной научно-практической конференции “Информационные технологии в образовании и фундаментальных науках (ИТО-Поволжье-2007)”, Казань 18-21 июня 2007 г. / ТГГПУ, Казань.
11. Павленко, А.Н. О целесообразности использования математического пакета «MathCAD» в преподавании теории вероятностей / А.Н. Павленко // Интеграция науки и практики в профессиональном развитии педагога: материалы Всерос. науч.-практ. конф. / Оренбург. гос. ун-т. – Оренбург: ОГУ, 2010, С. 757-760.
12. Павленко, А.Н. К вопросу об организации вводного курса "Математическая обработка экспериментальных данных" / А.Н. Павленко,

О.А. Пихтилькова, А.Г. Четверикова // *Вестн. Оренбург. гос. ун-та.* - 2015. - № 7. - С. 120-124.

13. Охорзин, В. А. *Прикладная математика в системе MATHCAD: учеб. пособие для вузов* / В. А. Охорзин. - 3-е изд., стер. - СПб.: Лань, 2009. - 349 с. : ил.. - Прил.: с. 332-340. - Библиогр.: с. 341-342. - ISBN 978-5-8114-0814-6.

14. Вентцель, Е. С. *Теория вероятностей: учеб. для вузов* / Е. С. Вентцель. - 10-е изд., стер. - М.: Академия, 2005. - 576 с. - (Высшее образование) - ISBN 5-7695-2311-5.

ОБ ИЗЛОЖЕНИИ ТЕМЫ «ОПРЕДЕЛЕННЫЙ ИНТЕГРАЛ И ЕГО ПРИЛОЖЕНИЯ» В ПРОПЕДЕВТИЧЕСКОМ КУРСЕ ПО ВЫСШЕЙ МАТЕМАТИКЕ ДЛЯ ЕСТЕСТВЕННОНАУЧНЫХ НАПРАВЛЕНИЙ

Павленко А.Н., Пихтилькова О.А.

Оренбургский государственный университет, г. Оренбург

В курсе физики, изучаемом студентами естественнонаучных направлений высших учебных заведений, понятие определенного интеграла начинает применяться уже в начале первого семестра первого курса. Однако, в программах дисциплин «Математический анализ» и «Математика» изучение интегрального исчисления для функций одной переменной предусматривается обычно не ранее второго семестра, а теме «Интеграл» в средних учебных заведениях, как правило, уделяется явно недостаточное внимание в силу отсутствия заданий по данному материалу в контрольно-измерительных материалах ЕГЭ по математике [1].

Таким образом, возникает необходимость в организации в течение первого семестра (первых двух семестров) пропедевтического курса по элементарной и высшей математике (примеры подобных курсов в [2-6] и в приведенной там литературе) в котором будут изучаться (повторяться) темы, необходимые для изучения естественнонаучных дисциплин или миникурсов внутри самих этих дисциплин.

Ниже предлагается новый подход к повторению и изучению темы «Определенный интеграл» основополагающими особенностями которого являются:

- 1) повторение понятия интеграла и рассмотрение его физических приложений не последовательно, а одновременно;
- 2) введение понятия определенного интеграла с помощью определения, максимально удобного для физических приложений;
- 3) не рассмотрение на данном этапе некоторых вспомогательных понятий, свойств определенного интеграла и методов его вычисления, за исключением формулы Ньютона-Лейбница.

Как известно [7], значения довольно большого числа физических величин численно равны площадям под графиками некоторых функций. Рассмотрим следующие примеры:

- 1) пройденный материальной точкой путь S численно равен площади под графиком (рисунок 1) зависимости скорости от времени $v = v(t)$;
- 2) работа идеального газа A численно равна площади под графиком (рисунок 2) зависимости давления газа от его объема $P = P(V)$.

Отсюда следует, что на пропедевтическом этапе изучения понятия определенного интеграла целесообразно ввести данное понятие как величину площади под графиком непрерывной неотрицательной функции. Такой подход

не только является наглядным и доступным, но и отличается естественностью и непосредственной связью с физическими приложениями.

Следует отметить, что рассмотрение темы «Определенный интеграл» по схеме, довольно сильно отличающейся от общепринятой, встречается даже в полных курсах высшей математики. В качестве примера можно указать известный учебник по высшей математике для студентов естественных (геологического, географического, биологического и др.) факультетов университетов [8].

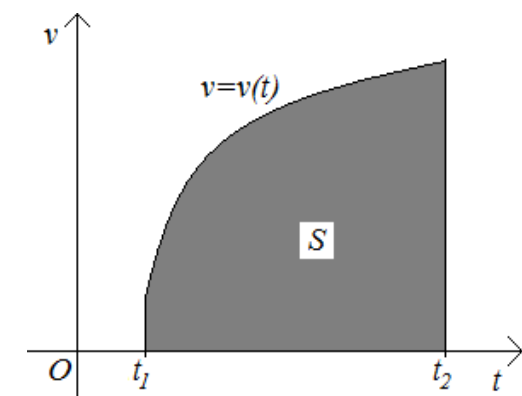


Рисунок 1

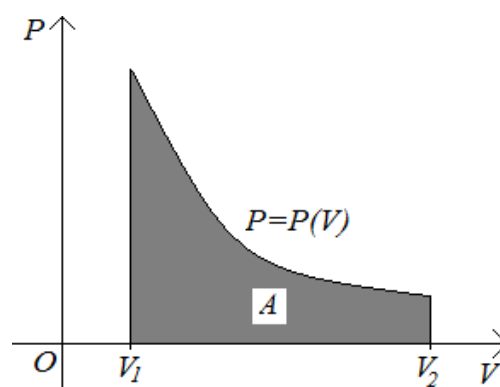


Рисунок 2

Определение. Пусть функция $y = f(x)$ непрерывна и неотрицательна на отрезке $[a; b]$ ($a < b$). Определенным интегралом $\int_a^b f(x)dx$ назовем число, равное площади (рисунок 3) под графиком функции $y = f(x)$ при $x \in [a; b]$.

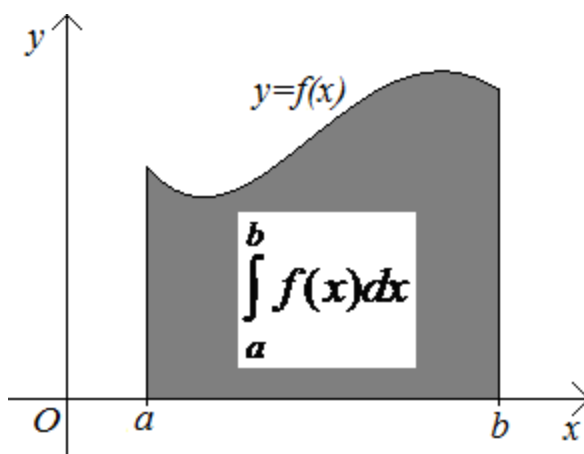


Рисунок 3

Представляется целесообразным не рассматривать свойства определенного интеграла на данном этапе, так как их использование может быть заменено учетом в решении физического смысла рассматриваемой задачи, а также, как правило, хорошо усвоенными по школьному курсу математики свойствами производной.

Учитывая важность формулы Ньютона-Лейбница, ее следует привести с обоснованием даже в пропедевтическом курсе. При этом удобен вывод на основе использования понятия определенного интеграла с переменным верхним пределом. В силу применения несколько нестандартных обозначений, ниже приводится данный вывод полностью.

Определение. Если мы будем менять значение b , то и значение определенного интеграла будет меняться (рисунок 4), таким образом можно рассмотреть функцию $F(b) = \int_a^b f(x)dx$, которую будем называть определенным интегралом с переменным верхним пределом.

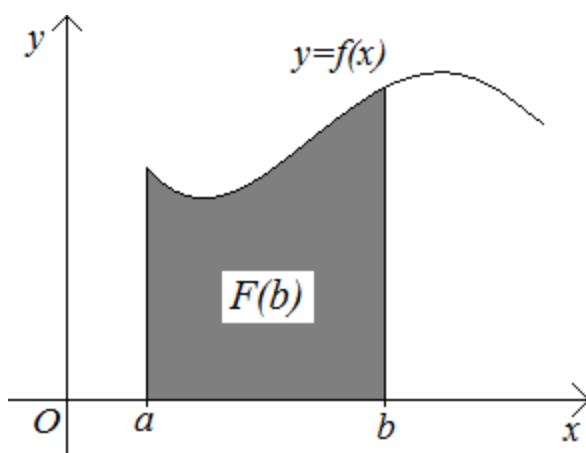


Рисунок 4

Определенный интеграл с переменным верхним пределом является первообразной для подинтегральной функции. Действительно, используя определение производной, получим:

$$F'(b) = \lim_{\Delta b \rightarrow 0} \frac{F(b + \Delta b) - F(b)}{\Delta b} = \lim_{\Delta b \rightarrow 0} \frac{\Delta F(b)}{\Delta b}.$$

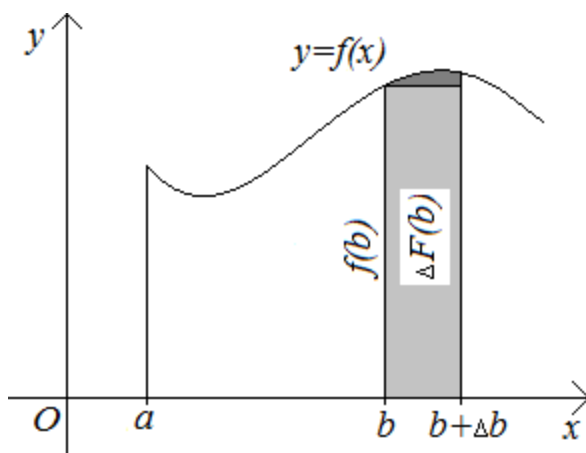


Рисунок 5

Из рисунка 5 имеем приближенное равенство

$$\Delta F(b) \approx f(b) \cdot \Delta b.$$

Тогда будем иметь:

$$F'(b) = \lim_{\Delta b \rightarrow 0} \frac{f(b)\Delta b}{\Delta b} = \lim_{\Delta b \rightarrow 0} f(b) = f(b).$$

Любую первообразную для данной функции $f(b)$ мы сможем записать в виде

$$F(b) = \int_a^b f(x)dx + C.$$

Очевидно, что

$$F(a) = \int_a^a f(x)dx + C = 0 + C = C.$$

Вычтя из предпоследнего равенства последнее равенство, получим формулу Ньютона-Лейбница

$$\int_a^b f(x)dx = F(b) - F(a).$$

Задача. Найти работу идеального газа при изотермическом процессе.

Решение. Как известно, работа идеального газа численно равна площади под графиком зависимости давления газа от его объема (рисунок 2). Тогда получим:

$$A = \int_{V_1}^{V_2} P(V)dV.$$

Используя уравнение Менделеева-Клапейрона [7]

$$PV = \frac{m}{M}RT,$$

получим

$$P = \frac{mRT}{M} \cdot \frac{1}{V}.$$

Так как при изотермическом процессе температура T является константой, то тогда множитель $\frac{mRT}{M}$ будет постоянной величиной.

$$A = \int_{V_1}^{V_2} \frac{mRT}{M} \cdot \frac{1}{V} dV.$$

Используем формулу Ньютона-Лейбница. С помощью таблицы первообразных (или даже таблицы производных) получаем, что первообразной функции $\frac{1}{V}$ является функция $\ln V$. Так как из физического смысла задачи следует, что всегда $V > 0$, то брать величину объема по модулю нет необходимости. Тогда будем иметь:

$$A = \left(\frac{mRT}{M} \cdot \ln V \right) \Big|_{V_1}^{V_2} = \frac{mRT}{M} \cdot \ln V_2 - \frac{mRT}{M} \cdot \ln V_1 = \frac{mRT}{M} \cdot (\ln V_2 - \ln V_1) = \frac{mRT}{M} \cdot \ln \frac{V_2}{V_1}.$$

Ответ: $A = \frac{mRT}{M} \cdot \ln \frac{V_2}{V_1}.$

При нахождении первообразных целесообразно использовать подробные таблицы неопределенных интегралов [9,10].

Список литературы

1. <http://www.fipi.ru/ege-i-gve-11/demoversii-specifikacii-kodifikatory>
2. Чаплыгин, С.А. Пропедевтический курс механики / С.А. Чаплыгин. – изд. 2-е. – М.: Госиздат, 1923. – 242 с.
3. Сазонов, В.Н. Пропедевтический курс математического анализа: конспект лекций / В.Н. Сазонов. – М.: Моск. станкоинструм. ин-т., 1989. – 52 с. : ил.
4. Кузнецова, В.А. О целесообразности вводного пропедевтического курса в университете / В.А. Кузнецова // Вестн. Тамбовского гос. ун-та. – 2003. – № 3, том: 8. – С. 406.
5. Светлова, Н.И. Школьная математика и подготовка студентов специальности «Математические методы в экономике» / Н.И. Светлова // Вестн. Нижегородского ун-та им. Лобачевского. – 2011. – № 3(3). – С. 106–109.
6. Темникова И.С. Восстановление школьных и пропедевтика вузовских математических знаний с помощью компьютерных средств обучения: материалы Международной научно-практической конференции

“Информационные технологии в образовании и фундаментальных науках (ИТО-Поволжье-2007)”, Казань 18-21 июня 2007 г. / ТГГПУ, Казань.

7. Детлаф, А.А. Курс физики: Учеб. пособие для студ. вузов / А.А. Детлаф, Б.М. Яворский. – 5-е изд., стер. – М.: Издательский центр «Академия», 2005. – 720 с. – ISBN 5-7695-2312-3.

8. Демидович, Б.П. Краткий курс высшей математики: учеб. пособие для вузов / Б.П. Демидович, В.А. Кудрявцев. — М.: ООО «Издательство Астрель»; ООО «Издательство АСТ», 2001. — 656 с.: ил. - ISBN 5-17-004601-4.

9. Бермант, А.Ф. Краткий курс математического анализа: учеб. для вузов / А.Ф. Бермант, И.Г. Араманович. - 11-е изд., стер. - СПб. : Лань, 2005. - 736 с. - (Учебники для вузов. Специальная литература). - Библиогр.: с. 736. - ISBN 5-8114-0499-9.

10. Двайт, Г.Б. Таблицы интегралов и другие математические формулы. / Г. Б. Двайт. - СПб.: АО ВНИИГ им. Б. В. Веденеева, 1995. - 176 с

ПОДХОДЫ К ПОВЫШЕНИЮ КАЧЕСТВА ОБСЛУЖИВАНИЯ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИЛОЖЕНИЙ И СЕРВИСОВ МУЛЬТИОБЛАЧНЫХ ПЛАТФОРМ НА БАЗЕ ТЕХНОЛОГИЙ VNF И SDN

Парфёнов Д.И., Болодурина И.П.

Оренбургский государственный университет, г. Оренбург

В настоящее время крупные коммерческие и государственные организаций, в том числе промышленные предприятия (в областях электроэнергетики, машиностроения, добычи и переработки полезных ископаемых, систем жизнеобеспечения и т.п.) переносят свою информационную инфраструктуру из физических центров обработки данных (ЦОД) в виртуальные. Такая оптимизация позволяет существенно экономить средства для организаций, а так же развивать рынок предоставления услуг в сфере аренды центров обработки данных [1-2].

На сегодняшний день не так много компаний способных предоставлять услугу виртуального ЦОД (Virtual Data center as a service, VDCaaS) своим клиентам. Такое положение связано с тем, что требования клиентов к услуге VDCaaS существенно отличается от предоставления услуг IaaS (инфраструктура, как услуга) и даже DCaaS (ЦОД, как услуга). Множество требований касается вопросов безопасности функционирования систем. Так, например, в виртуальном ЦОД предприятия размещают критически важные сервисы и приложения, от которых напрямую зависит их экономическая безопасность при осуществлении обработки финансовых потоков или безопасность людей [3-4]. Такие объекты инфраструктуры в первую очередь становятся целью кибератак.

Другой проблемой предоставления услуг виртуального ЦОД является задача построения комплексной виртуальной инфраструктуры на базе существующих физических сетевых и вычислительных ресурсов с предоставлением полноценного доступа клиента к управлению всеми функциональными возможностями реального ЦОД. Критической точкой любой инфраструктуры физического ЦОД с течением времени становится разнородность используемого оборудования. Лидеры мирового рынка сетевого оборудования компании Cisco Systems, Huawei, Juniper, HP и др. навязывают использование собственных средств мониторинга и управления сетевыми устройствами и протоколами, что не позволяет гибко и оперативно подстраивать инфраструктуру под текущие задачи клиента. Кроме того высокая стоимость такого оборудования, несмотря на гарантию надежности, накладывает существенные ограничения на масштабируемость и резервирование, закладываемые в физическую инфраструктуру ЦОД. Это в дальнейшем может приводить к долговременным простоям, связанным с

заменой, вышедших из строя объектов, или модернизацией узлов для расширения функциональных возможностей [5-6].

Как отмечалось ранее, одним из требований клиентов, предъявляемых к предоставлению услуги виртуального ЦОД, является доступ к полноценным средствам управления сетевой инфраструктурой, включая различные сервисы сетевой безопасности и обеспечения качества обслуживания. Использование традиционных подходов к организации сетевой инфраструктуры не позволяет это реализовать для множества клиентов в пределах одного ЦОД без построения выделенной физической сети, что приводит к существенным бюджетным ограничениям [7]. В последнее время для решения данной проблемы применяется технология программно-конфигурируемых сетей (Software-Defined Networks, SDN), которая позволяет отделить (абстрагировать) уровень управления сетью (control plane) от нижележащего уровня пересылки пакетов (data plane) за счет передачи функций управления (маршрутизаторами, коммутаторами и т.д.) в приложения, работающие на выделенных вычислительных узлах (контроллерах). Планирование сети и управление трафиком при этом происходит программным путем. Для приложений верхнего уровня предоставляются интерфейсы прикладного программирования API. Таким образом, ввод новых услуг на сети ускоряется и облегчается.

На практике подход, применяемый в программно-конфигурируемых сетях, позволяет повысить эффективность, безопасность и надежность передачи данных за счет гибкого реконфигурирования маршрутов и настройки политик доступа к ресурсам на уровне потоков данных. Кроме того технология программно-конфигурируемых сетей позволяет пользователям создавать новые сервисы и загружать их в сетевое оборудование. Однако клиентам виртуальных ЦОД требуется не только традиционные сетевые функции управления трафиком, но и специализированные программные или аппаратные решения, обеспечивающие высокую производительность для конкретных задач, например анализ и фильтрация сетевых пакетов (Deep packet inspection, DPI), межсетевой экран (Firewall) и другие. В традиционных сетях для таких целей применяют специализированные устройства, отвечающие должному классу по производительности и функционалу. В концепции услуги виртуальных ЦОД, доступ к управлению физическими устройствами может быть ограничен, и они чаще всего обеспечивают внешний периметр безопасности инфраструктуры ЦОД.

Для решения этой проблемы разработана технология виртуализации функций сетевых элементов телекоммуникационной сети (Network Functions Virtualization, NFV), позволяющая использовать программные модули, работающие на стандартных вычислительных узлах и виртуальных машинах (VM) вместо специализированных устройств. Эти программные модули могут взаимодействовать между собой для предоставления услуг связи, чем ранее занимались аппаратные платформы. Технологии SDN и NFV являются независимыми компонентами инфраструктуры виртуального ЦОД,

дополняющие друг друга. Однако в рамках концепции обеспечения безопасности и качества обслуживания для приложений и сервисов мультиоблачных платформ требуется комплексный подход, обеспечивающий полноценное управление всей сетевой инфраструктурой виртуального ЦОД.

В рамках исследования предложено решение в котором все задачи связанные с управлением ресурсами виртуального ЦОД будут подвергаться проактивному прогнозированию и работать автоматизировано, основываясь на принципах самоорганизации в части размещения объектов виртуальной инфраструктуры, на физических узлах и устройствах, а так же в части распределения потоков данных для обеспечения надежности мультиоблачной платформы.

Достигнуть поставленной цели возможно путем разработки эффективных алгоритмических и программных решений, а так же построения моделей обеспечения безопасности и качества обслуживания для приложений и сервисов мультиоблачной платформы, расположенной на базе инфраструктуры виртуального ЦОД.

Определим эффективность управления объектами инфраструктуры для обеспечения безопасности и качества обслуживания, как способность распределять и балансировать нагрузку между устройствами, максимизируя при этом количество обрабатываемых запросов и минимизируя возможность отказа в обслуживании при возникновении целенаправленных или непреднамеренных действий третьих лиц, направленных на выведение из строя отдельных компонентов или всей мультиоблачной платформы в целом.

Использование концепции мультиоблачных платформ позволяет одновременно размещать в пределах одного виртуального ЦОД частные, публичные и гибридные облачные системы с поддержкой контейнеризации сервисов и приложений на базе Docker, работающие под управлением различных оркестраторов OpenStack, OpenNebula, CloudStack и др. В основе подхода программно-конфигурируемых сетей лежит возможность динамически управлять пересылкой данных в сети с помощью открытого протокола OpenFlow. Все сетевые коммутаторы, поддерживающие OpenFlow, объединяются под управлением контроллера OpenFlow, который обеспечивает приложениям доступ к управлению сетью. Каждый коммутатор OpenFlow имеет таблицу потоков, содержащую правила обработки пакетов. Каждое правило включает две части – признаки заголовков пакетов и набор действий. При поступлении в коммутатор нового пакета, происходит сопоставление его заголовков с признаками правил в таблице. В случае совпадения выполняются все действия из соответствующего набора. Если подходящее правило в таблице отсутствует, то пакет передается контроллеру OpenFlow. Контроллер принимает решение о дальнейших действиях над пакетом, которое реализуется в виде команды передачи пакета на определенный порт коммутатора и/или в установке для пакета нового правила в таблицу данного и, возможно, других

коммутаторов. Признаки заголовков позволяют управлять пакетами на уровнях L1–L3 модели OSI.

Таки образом за счет применения виртуализации сетевых компонентов и внедрения эффективных алгоритмов управления виртуальными ресурсами возможно повышение производительности их работы на 30-40% по сравнению с аналогичными компонентами традиционной инфраструктуры телекоммуникационных сетей. Так же это позволит сократить время простоя на модернизацию сетевых и вычислительных узлов, а также снизит на 50-60% затраты на закупку нового дорогостоящего оборудования, поддерживающего ранее недоступный функционал, для возможности предоставления новых сервисов и услуг для клиентов в короткие сроки.

Работа выполнена при поддержке РФФИ (научные проекты 16-37-60086 мол_а_дк и 16-07-01004), Президента Российской Федерации, грант для государственной поддержки молодых российских ученых – кандидатов наук (МК-1624.2017.9).

Список литературы

1. Болодурина И.П., Парфёнов Д.И. Алгоритмы комплексной оптимизации потребления вычислительных ресурсов в облачной системе дистанционного обучения [Текст] / И.П. Болодурина, Д.И. Парфёнов // Вестник Оренбургского государственного университета. – 2013. - № 9. – С. 177-184.
2. Болодурина И.П., Парфёнов Д.И. Управление потоками данных в высоконагруженных информационных системах, построенных на базе облачных вычислений [Текст] / И.П. Болодурина, Д.И. Парфёнов // Системы управления и информационные технологии. – 2015. - № 1.1. – С. 111-118.
3. Bocchi E., Drago I., Mellia M. Personal Cloud Storage Benchmarks and Comparison // IEEE Transactions on Cloud Computing. 2015. Vol. 99. – IEEE, 2015. – pp. 1-14
4. Bolodurina I., Parfenov D., Shukhman A. Approach to the effective controlling cloud computing resources in data centers for providing multimedia services //Control and Communications (SIBCON), 2015 International Siberian Conference on. – IEEE, 2015. – pp. 1-6.
5. Charuenporn P., Intakosum S. Qos-Security Metrics Based on ITIL and COBIT Standard for Measurement Web Services //J. UCS. – 2012. – Vol. 18. – No. 6. – pp. 775-797, available at: [www. http://jucs.org/jucs_18_6/](http://jucs.org/jucs_18_6/)
6. Rajiv R., Benatallah B., Schahram D., Michael P. Cloud Resource Orchestration Programming: Overview, Issues, and Directions // IEEE Internet Computing. 2015. Vol. 19, Issue: 5. – pp. 46-56.
7. Thiago A. L., Genez L. F., Bittencourt E., Madeira R. M. Workflow scheduling for SaaS / PaaS cloud providers considering two SLA levels // Network Operations and Management Symposium (NOMS).– IEEE, 2012. – pp. 906-912.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СУЩЕСТВУЮЩИХ СИСТЕМ УПРАВЛЕНИЯ РЕСУРСАМИ НА БАЗЕ ОБЛАЧНЫХ ТЕХНОЛОГИЙ

**Парфёнов Д.И., Шардаков В.М., Дедюрин В.В.
Оренбургский государственный университет, г. Оренбург**

В настоящее время крупные облачные решения строятся на базе тысяч серверов, размещенных в центрах обработки данных (ЦОД). Это позволяет обеспечивать ресурсами десятки тысяч приложений, которые одновременно используют миллионы пользователей [1-3]. Облачные технологии являются удобным инструментом для предприятий, которым слишком дорого содержать собственные ERP, CRM или другие серверы, требующие приобретения и настройки дополнительного оборудования. Рассмотрим наиболее прогрессивные прикладные задачи для которых применяются облачные технологии.

Одной из задач является планирование ресурсов (Enterprise Resource Planning – ERP) – организационная стратегия интеграции производства и операций, управления трудовыми ресурсами, финансового менеджмента и управления активами, ориентированная на непрерывную балансировку и оптимизацию ресурсов предприятия посредством специализированного интегрированного пакета прикладного программного обеспечения, обеспечивающего общую модель данных и процессов для всех сфер деятельности предприятия.

Другой задачей является система управления взаимоотношениями с клиентами CRM (Customer Relationship Management), то есть прикладное программное обеспечение, предназначенное для автоматизации стратегий взаимодействия с заказчиками (клиентами), в частности, для повышения уровня продаж, оптимизации маркетинга и улучшения обслуживания клиентов путем сохранения информации о клиентах и истории взаимоотношений с ними, установления и улучшения бизнес-процедур и последующего анализа результатов.

Популярность использования облачных технологии объясняется тем, что они позволяют экономить как на обслуживании, так и на инфраструктуре. Аппаратное обеспечение может быть сильно упрощено при обработке данных и хранении информации в удаленных центрах данных. Все эти проблемы почти полностью перекладываются на провайдера услуг.

К тому же такой подход позволяет стандартизировать ПО, даже если на компьютерах предприятия установлены разные операционные системы (Windows, Linux, MacOS и т.п.). Облачные технологии облегчают обеспечение доступа к данным компании как для клиентов, так и для собственных сотрудников, находящихся вне офиса, но имеющих возможность подключиться через Интернет.

Как правило, системы CRM/ERP реализуются по модели SaaS (Software as a Service) – программное обеспечение как услуга. Это позволяет масштабировать приложение без участия пользователя. Однако перед пользователями остается проблема выбора требуемого программного обеспечения для эффективной работы.

Как правило, все системы планирования отталкиваются от концепции just in time (JIT- точно в срок). На основе данной концепции работают ряд систем планирования ресурсов.

Система OPT («Optimized Production Technology» – оптимизированная производственная технология) – спроектирована израильскими и американскими специалистами. Она относится к классу микрологистических систем, внедряющих процессы снабжения и производства. Данная система разработана на основе современных информационно-компьютерных технологий в начале 1980-х годов. Отличительной особенностью работы такой системы является выявление в производственном процессе так называемых «узких» мест производства.

В системе OPT реализовано автоматизированное оперативно-производственное планирование и диспетчеризация. Расчет расписания выполняется на различные интервалы времени. Решаются также задачи контроля выполнения операции и поиска альтернативных ресурсов, выдачи рекомендаций по полноценным заменам в случае отсутствия необходимых материальных ресурсов. Расписание распределения ресурсов формируется из базы данных OPT и технологических карт.

Эффект от использования систем на основе OPT заключается в уменьшении издержек, сокращении времени цикла выполнения базовых операций, повышении производительности системы планирования.

Концепция эффективной реакции на запросы – ECR (efficient consumer response) так же является системой, основанной на концепции JIT. Философия JIT заставляет поставщиков менять методы работы, чтобы обеспечивать более быстрые поставки, более высокое качество, меньшие партии и полную надежность. Для того, чтобы удовлетворить все эти требования поставщикам самим нужно взять на вооружение JIT методы. Это гарантирует, что вся логистическая цепь будет работать согласованно на основе одних и тех же целей и принципов. Концепция эффективной реакции на запросы потребителей предполагает расширение зоны JIT на весь цикл операций [5].

Система «Kanban» – используется для оперативного управления ресурсами, которое способно к быстрой перенастройке. Отличительной особенностью данной системы является то, что все этапы (процессы) снабжаются материальными ресурсами только в том количестве и к такому сроку, которые необходимы для выполнения полученного заказа. Для передачи такой информации используются специальные карточки «Kanban» (в переводе с японского kanban – карточка) двух типов: отбора и задачи. В карточке отбора указывается вид и количество ресурсов, которые должны поступить с

предыдущего участка производственной цепи. В карточке заказа вид и количество изделий, которое должно быть выпущено на предшествующем производственном участке. Таким образом, эти карточки несут информацию о количестве расходуемых материальных ресурсов и производимой продукции. Другими словами «Kanban» – это метод управления ресурсами в среде ИТ, который использует для управления задачами [6-7].

Данная система используется как система ежедневных указателей и формирования инструкций, которые эффективно реализуют ИТ концепцию. Важную роль играет график, так как он позволяет наиболее точно определить запросы к ресурсам на будущие периоды. Но конкретные инструкции для каждого процесса составляются на поток запросов (workflow). Далее благодаря системе «Kanban» они поднимаются «вверх» по этапам процесса обработки [3].

В рамках исследования нами проеден сравнительный анализ существующих систем планирования ресурсов. Результаты сравнительного анализа сведены в таблицу 1.

Таблица 1 – Сравнение существующих систем планирования ресурсов

Возможности	JIRA	Asana	Kanboard	OpenProject	KanbanTool
Диаграмма Ганта	×	✓	✓	✓	×
Отчеты	×	✓	✓	✓	✓
Приоритеты	✓	×	✓	×	×
Уведомления	✓	✓	✓	×	✓
Вложения файлов к задачам	✓	✓	✓	×	✓
Отслеживание прогресса в процентах	×	✓	✓	×	×
Число пользователей на бесплатном тарифе	15	10	неограничено	неограничено	2
Дэшборд	✓	✓	×	×	×
Развертывание	облако, сервер	облако, сервер	облако, сервер	сервер	облако
Доступные языки	English	English	English, Русский	Русский	English

Анализ данной таблицы показывает, что наиболее адекватными системами систем планирования ресурсов являются Asana и Kanboard. Однако, Asana не локализована, Kanboard же поддерживает приоритеты и локализацию

на русский язык, поэтому она и была выбрана для использования совместно с инструментами виртуализации для размещения в качестве SaaS сервиса.

Работа выполнена при поддержке РФФИ (научные проекты 16-37-60086 мол_а_дк и 16-07-01004), Президента Российской Федерации, грант для государственной поддержки молодых российских ученых – кандидатов наук (МК-1624.2017.9).

Список литературы

1. Болодурина, И.П. Исследование методов размещения и организации распределенного доступа к данным облачного хранилища системы дистанционного обучения / И.П. Болодурина, Д.И. Парфёнов // Труды международной научной конференции Параллельные вычислительные технологии 2013 (ПаВТ'2013), 2013. – С. 301-307.

2. Болодурина, И.П. Моделирование распределения ресурсов и динамической балансировки нагрузки в информационной системе дистанционной поддержки образовательного процесса / И.П. Болодурина, Д.И. Парфёнов // Труды шестой международной конференции параллельные вычисления и задачи управления PACO'2012, 2012. – С. 173-182.

3. Bocchi E., Drago I., Mellia M. Personal Cloud Storage Benchmarks and Comparison // IEEE Transactions on Cloud Computing. 2015. Vol. 99. – IEEE, 2015. – pp. 1-14.

4. Bolodurina I., Parfenov D., Shukhman A. Approach to the effective controlling cloud computing resources in data centers for providing multimedia services // Control and Communications (SIBCON), 2015 International Siberian Conference on. – IEEE, 2015. – pp. 1-6.

5. Charuenporn P., Intakosum S. Qos-Security Metrics Based on ITIL and COBIT Standard for Measurement Web Services // J. UCS. – 2012. – Vol. 18. – No. 6. – pp. 775-797, available at: [www. http://jucs.org/jucs_18_6/](http://jucs.org/jucs_18_6/)

6. Rajiv R., Benatallah B., Schahram D., Michael P. Cloud Resource Orchestration Programming: Overview, Issues, and Directions // IEEE Internet Computing. 2015. Vol. 19, Issue: 5. – pp. 46-56.

7. Thiago A. L., Genez L. F., Bittencourt E., Madeira R. M. Workflow scheduling for SaaS / PaaS cloud providers considering two SLA levels // Network Operations and Management Symposium (NOMS).– IEEE, 2012. – pp. 906-912.

К ВОПРОСУ О ПОВЫШЕНИИ КАЧЕСТВА ЗНАНИЙ ОБУЧАЮЩИХСЯ ПРИ ПРОВЕДЕНИИ ТЕКУЩЕГО КОНТРОЛЯ

**Пастухов Д.И.
ФГБОУ ВО «Оренбургский государственный университет»,
г. Оренбург**

В вузе сложились такие формы текущего контроля успеваемости обучающихся по математическим дисциплинам, как:

- 1) коллоквиумы;
- 2) самостоятельные работы, как на занятиях, так и «домашние»;
- 3) проверка наличия выполненных домашних заданий, получаемых обучающимися после каждого практического занятия;
- 4) контрольные работы;
- 5) потемная сдача.

Как показывает опыт, они действительно позволяют контролировать процесс усвоения знаний и приобретения умений обучающимися, обеспечивая его непрерывность. Вопрос в том, чтобы, используя (реализуя) их, повышать качество знаний и умений.

Одним из важных достижений педагогики, как науки, является открытие дидактических функций контроля знаний, умений и навыков. Процесс формирования и овладения знаниями, умениями и навыками становится эффективным, если используются гармонично все дидактические функции контроля: контролирующая, обучающая, ориентирующая и воспитательная.

С реализацией обучающей, ориентирующей и воспитательной функций сам контроль, из метода, фиксирующего определенный уровень знаний, умений и навыков, превращается в живой метод формирования настойчивости и целеустремленности, умения овладеть знаниями, систематизировать их, оценивать ответственно результат учебного труда, то есть, «сухой» контроль превращается в метод создания личности с качественным уровнем знаний и умений.

Дидактические функции органически сочетаются при использовании «мягкого рейтинга» для проведения коллоквиума. Идея «мягкого рейтинга» состоит в том, что преподаватель предлагает обучающемуся дать версию своего ответа на поставленный вопрос и оценивать степень точности, обоснованности ответа, без оглашения оценки. Этот же вопрос преподаватель ставит перед всей аудиторией и просит остальных обучающихся высказать свои гипотезы по содержанию ответа на него. Свои гипотезы или версии высказывают несколько обучающихся. Затем преподаватель сам формулирует правильный ответ. Так происходит с каждым вопросом (заданием).

Чтобы процесс был неустойчивым весь материал, выносимый на обсуждение, разбивается на 304 блока по 8-10 вопросов в каждом блоке. Чтобы блок был засчитан, надо ответить, примерно, на 5 вопросов. После первого

блока оглашаются результаты аттестации, и объявляется двадцатиминутный перерыв, во время которого все готовятся ко второму блоку. После рассмотрения второго блока также оглашаются результаты, и вновь наступает двадцатиминутный перерыв. Затем рассматривается третий блок.

После рассмотрения третьего блока, вначале оглашаются результаты аттестации по нему, а затем – результаты по всему обсуждению. Полученные положительные оценки выставляются в качестве итогов коллоквиума. Объявляется двадцатиминутный перерыв, во время которого идет подготовка к первому блоку тех обучающихся, которые его не сдали. Далее процесс повторяется.

В зависимости от сложности рассматриваемого материала, его объема и выделенного времени на подготовку, «мягкий рейтинг» можно повторить и в третий раз. Кстати, время, затрачиваемое на проведение коллоквиума с применением «мягкого рейтинга», не превышает времени на проведение его по классической схеме, ибо, по классической схеме оно расходуется на подготовку, а затем на «выжидательно-вытягивающую» беседу и т.д.

Краткое изложение схемы применения «мягкого рейтинга» уже позволяет увидеть то, что обучающийся участвует в познавательной деятельности, и какие педагогические и психологические основы образовательного процесса реализуются в непрерывной связи обучающегося с коллективом (аудиторией). В аудитории находится весь коллектив, поэтому начинает работать чувство собственного достоинства любого обучающегося. Все превосходства вне коллектива уходят на задний план. Остаются только знания, умение мыслить при обработке полученной информации. Рассматриваемые ответы отличаются, вроде бы, ненамного, но, как высказать правильно версию своего ответа, где истина, и как в этот момент не хватает знаний – становится очевидным. Обучающемуся хочется выглядеть среди коллег по группе, как минимум, не глупее их, как максимум – умнее. Если раньше обучающийся проходил все контрольные мероприятия как-то незаметно, то сейчас это происходит в присутствии тех людей, среди которых он, возможно, считается лидером, его непосредственных товарищей.

После прохождения «мягкого рейтинга» с положительным или отрицательным результатом, отношение обучающегося к своему обучению в вузе изменяется в сторону проявления познавательной способности и повышения уровня качества знаний. Речь и его ответы становятся осознанными и логически выдержанными. А, самое главное, он не боится огласки своих знаний и своего поведения, так как оно стало более общественно значимым.

Действительно, хорошо успевающим обучающимся надоедает помогать обучающемуся, который хочет без усилий понять изучаемую тему или ознакомиться с ее содержанием. Потому что, кроме нудного и неоцениваемого объяснения, они, лично для себя, ничего не имеют. При этом возникает мотивированная потребность в повышении познавательной способности. При участии в «мягком рейтинге» ответы становятся публичными, а, значит,

повышается не только авторитет знаний обучающегося, а также признается его метод работы, его стремление к серьезной повседневной работе, к овладению профессией.

Опыт применения «мягкого рейтинга», наблюдения за дальнейшей работой выпускников, прошедших неоднократно оценку своих знаний через участие в «мягком рейтинге», показывает положительное влияние его на поведение человека в целом. Он становится человеком стремления, человеком, умеющим защищать и отстаивать свою позицию, свою работу и свое дело. Результаты тестового контроля значительно повышаются, если обучающиеся предварительно участвовали в «мягком рейтинге».

При проверке наличия выполненных домашних заданий обучающемуся обязательно задаются вопросы по каждому из них. Ответы на эти вопросы дают возможность установить самостоятельность выполнения заданий, уровень понимания применяемых методов решения и степень овладения теоретическими положениями. Если ответы отрицательны, то обучающемуся надо еще раз «защитить» свои домашние задания.

Так как домашние задания выполнены, то их «незащищенность» на допуск к экзамену не влияет. Но она может проявиться при ответах на экзамене.

Самостоятельные работы на практических занятиях небольшие и по времени (10-15 минут) и по объему: (2-3 примера или 2-3 задачи). Они проводятся в конце практического занятия и служат показателем усвоения обучающимися методов решения, применения практических положений и эффективности уровня всего занятия. Оценки по самостоятельным работам преподаватель выставляет к себе в журнал, но они повторно, в случае неудовлетворительной оценки, не переписываются. Если практическое занятие проведено без самостоятельной работы, то можно сказать, что оно не полностью достигло цели.

Контрольная работа – это очень ответственная часть работы обучающегося и преподавателя. Поэтому существенную роль играет подготовка к ней. Подготовка к контрольной работе проводится под руководством преподавателя, а самостоятельная часть ее остается для обучающегося и заключается в тщательном анализе всех самостоятельных работ. Для обучающихся, имеющих по самостоятельным работам, неудовлетворительные оценки, в случае положительного выполнения контрольной работы, они тоже засчитываются положительно оцененными. Контрольная работа – это проявление чистой контролирующей функции контроля. Для обучающихся, выполнивших контрольную работу на «отлично» и «хорошо» не нужно искать возможности действия других функций. Но обучающиеся, получившие неудовлетворительную оценку, этот контроль не прошли, так как допустили ряд ошибок, которые они осознали, поняли причину их появления при разборе с преподавателем работ, где были допущены эти ошибки. Поэтому, при повторном выполнении контрольной работы, им не надо

давать все задания этой работы, а только те, где они допустили ошибки. Качество знаний обучающегося улучшится и станет либо удовлетворительным, либо хорошим. Этого не будет, в случае повторного выполнения всей контрольной работы. Воспитательный характер контроля пропадает, что снижает стремление к положительным знаниям. К этому процессу подключаются, исключительно по желанию, обучающиеся, получившие удовлетворительные оценки.

Выработке у обучающихся стремления самостоятельно освоить теоретические вопросы изучаемой темы способствует так называемая «потемная сдача».

Суть «потемной сдачи» состоит в том, что изучаемый материал семестра делится на несколько тем (блоков), раскрывающих определенные вопросы. При прохождении темы (блока) обучающийся может предложить свои знания по данной теме для оценки, с тем, чтобы потом она учитывалась преподавателем при его общей аттестации за семестр. Оценка ставится за анализ теоретических положений темы (два вопроса), решение качественных и количественных задач. Многолетняя работа по проведению «потемной сдачи» позволила составить комплексные задания в нескольких вариантах по каждой теме.

«Потемная сдача» сняла проблемы низкой активности обучающихся на практических занятиях, повысила качественный уровень знаний теоретических положений.

На экзамене остаются только контролирующая и воспитательная функции, а обучающая уже отсутствует. Поэтому этот контроль не может повысить качество знаний. Он его только фиксирует.

Список литературы

1. Костенко И.П. Преподавание математики: смена парадигмы? / И.П. Костенко // *Высшее образование в России*. – 2001. - № 4. – С. 159-160.
2. Пидкасистый П.И. Психолого-педагогический словарь преподавателя высшей школы / П.И. Пидкасистый, Л.И. Фридман, М.Г. Гарунов. – Москва: Педагогическое общество России, 1999. – 354 с.
3. Текущее состояние самостоятельной работы студентов и ее методического обеспечения // *«Университет» ОГУ*, № 44(1098). – 2011.

О РАЗЛИЧНЫХ РАДИКАЛАХ АЛГЕБР ЛИ

Пихтильков С.А., Благовисная А.Н., Павленко А.Н.
Оренбургский государственный университет, г. Оренбург

В работах, посвященных структурной теории алгебр Ли, встречаются различные определения понятия радикала. Это обусловлено исследованием алгебр Ли многими авторами с разных точек зрения.

Наиболее разработана теория конечномерных алгебр Ли, начало которой в конце XIX века положили работы Софуса Ли, Картана, Энгеля, Киллинга. Тогда же появляется понятие радикала для конечномерных алгебр Ли, описанное в трудах Киллинга. Согласно современному пониманию объектов структурной теории алгебр Ли, радикал по Киллингу – это наибольший разрешимый идеал в алгебре Ли.

Существуют многочисленные публикации, в которых исследуются вопросы построения структурной теории алгебр Ли с помощью различных радикалов, как для конечномерных, так и для бесконечномерных случаев. К одному из таких радикалов относится радикал Джекобсона.

По аналогии с определением радикала Джекобсона для кольца можно ввести понятие радикала для алгебр Ли. В этом случае радикалом Джекобсона $J(L)$ алгебры Ли L называется пересечение максимальных идеалов или сама алгебра L , если их нет [1]. Такой подход к определению радикала позволяет достаточно плодотворно изучить структуру и свойства конечномерных алгебр Ли.

В бесконечномерном случае изучение радикала Джекобсона проводились Н. Камийя, Е. Маршаллом [2]. В дальнейшем исследование Ф. Кубо [3] показало, что результаты, представленные в работах данных авторов, для бесконечномерных алгебр Ли в общем случае не являются верными.

Другой подход к определению радикала Джекобсона алгебры Ли предложен в статье [4]. В работе показано, что для конечномерных алгебр Ли над полем характеристики нуль $\text{IrrPI}(L) = J(L)$, где $\text{IrrPI}(L)$ – пересечение аннуляторов всех неприводимых PI -представлений алгебры Ли или сама алгебра L , если их нет. Следовательно, авторы предлагают считать радикалом Джекобсона алгебры Ли L пересечение аннуляторов всех неприводимых PI -представлений алгебры Ли и саму алгебру L , если их нет.

Хорошо развитая теория конечномерных алгебр Ли способствует возникновению идей, побуждающих применять аналогичные конструкции, методы и средства изучения в случае бесконечномерных алгебр Ли. Однако данный подход не всегда оказывается результативным. Так, например, перенесение определения радикала по Киллингу на бесконечномерный случай невозможно в силу того факта, что в бесконечномерных алгебрах Ли сумма всех разрешимых идеалов не всегда будет разрешимым идеалом. Поэтому возникает понятие локально разрешимого идеала как естественного обобщения

понятия разрешимого идеала. Однако отрицательное решение проблемы Амайо-Стьюарта В. Н. Латышевым, А. В. Михалёвым и С. А. Пихтильниковым [5] привело к пониманию того, что для всех алгебр Ли нельзя построить теорию локально разрешимого радикала.

Представление единого для всех классов алгебр Ли радикала было предложено В.А. Парфеновым в 1971 году. Согласно Парфенову [6], радикал алгебры Ли – наибольший слабо разрешимый идеал алгебры Ли. В.А. Парфенов показал, что сумма слабо разрешимых идеалов алгебры Ли является слабо разрешимым идеалом. Кроме того, класс всех слабо разрешимых алгебр Ли является радикальным в универсальном классе всех алгебр Ли. Дальнейшее исследование подхода Парфенова показало, что в общем случае для всех бесконечномерных алгебр Ли не удастся получить аналоги теорем, справедливых в случае алгебр Ли конечных размерностей.

Понятие слабо разрешимого радикала позволяет ввести определение другого вида радикала для алгебр Ли – верхнего слабо разрешимого радикала. Покажем, как это сделано в монографии [5].

Для этого введем обозначение $T(L)$ слабо разрешимого радикала алгебры Ли L . Как и в случае ассоциативных алгебр, наибольший слабо разрешимый идеал $T(L)$ алгебры Ли L называется верхним слабо разрешимым радикалом.

Также можно ввести и понятие нижнего слабо разрешимого радикала алгебры Ли L по аналогии с построением нижнего ниль-радикала в ассоциативных алгебрах.

Пусть $\rho(L)$ – сумма разрешимых идеалов алгебры Ли L .

Идеал $\rho(L)$ является локально разрешимым в силу того, что сумма двух разрешимых идеалов алгебры Ли является разрешимым идеалом.

Используя трансфинитную индукцию, определим для каждого порядкового числа α идеал $\rho(\alpha)$ следующим образом.

1. $\rho(0) = 0$.

2. Предположим, что $\rho(\alpha)$ определено для всех $\alpha < \beta$. Тогда определим $\rho(\beta)$ следующим образом.

а) если $\beta = \gamma + 1$ не является предельным порядковым числом, то $\rho(\beta)$ это такой идеал алгебры L , что $\rho(\beta) / \rho(\gamma) = \rho(L / \rho(\gamma))$.

б) Если β – предельное порядковое число, то

$$\rho(\beta) = \bigcup_{\gamma < \beta} \rho(\gamma).$$

Расширение локально разрешимой алгебры Ли с помощью локально разрешимой алгебры может не быть локально разрешимым [7], но оно будет слабо разрешимым [5].

Из соображений мощности $\rho(\beta) = \rho(\beta + 1)$ для некоторого β . Назовем $\rho(\beta)$ нижним слабо разрешимым радикалом алгебры Ли L .

Существует подход к изучению алгебр Ли, предполагающий введение первичного радикала. Первичный радикал алгебры Ли можно определить как пересечение всех первичных идеалов алгебры Ли или саму алгебру Ли, если первичных идеалов нет [8].

Для отдельных классов алгебр Ли существуют и другие способы определения первичного радикала. Например, для специальной алгебры Ли L первичным радикалом можно назвать локально разрешимый радикал [9]. Кроме того, при изучении различных видов алгебр Ли возникают и разновидности первичного радикала. Так, в работе [10] упоминается l -первичный радикал решеточно упорядоченных алгебр Ли.

Первичный радикал алгебр Ли разных типов активно исследуется в последние десятилетия. В относительно недавно появившихся работах рассматривается первичный радикал специальных алгебр Ли [5, 9], специальных супералгебр Ли [11], артиновых алгебр Ли [8], алгебр Ли, удовлетворяющих дополнительным условиям [12].

Классическая теория конечномерных алгебр Ли позволяет определить локально нильпотентный, а также родственные ему радикалы для алгебр Ли.

Нильпотентным радикалом $N(L)$ для конечномерной алгебры Ли L называется пересечение ядер её неприводимых конечномерных представлений [5].

Локально нильпотентный радикал $N(L)$ определен для обобщенно специальной алгебры Ли L над полем F как пересечение наибольших идеалов локальной нильпотентности всех PI -представлений алгебры Ли L над полем F [5].

В работах по исследованиям проблемы гомологического описания радикала Джекобсона для алгебр Ли [4, 5, 13] авторы вводят следующую серию определений.

Неприводимо представленным радикалом алгебры Ли называется пересечение аннуляторов неприводимых модулей над алгеброй Ли L и сама алгебра L , если их нет.

Пересечение аннуляторов всех неприводимых PI -представлений алгебры Ли L и сама алгебра L , если их нет, называется PI -неприводимо представленным радикалом алгебры Ли.

Конечно неприводимо представленным радикалом алгебры Ли называется пересечение аннуляторов всех неприводимых конечномерных модулей над алгеброй Ли L и сама алгебра L , если их нет.

При исследовании радикалов алгебр Ли интересен вопрос о том, как соотносятся между собой изучаемые радикалы. Возможно ли совпадение, включение радикалов, и при каких условиях. Анализ различных публикаций, посвященных радикалам алгебр Ли, позволяет сделать вывод, что такие ситуации возможны при определенных ограничениях на алгебры Ли.

Таким образом, не существует единого подхода к определению радикала бесконечномерных алгебр Ли. Изучение радикалов бесконечномерных алгебр Ли происходит при условии наложения на них дополнительных ограничений или условий. Такими условиями могут быть артиновость, нетеровость, полиномиальные тождества и другие.

Список литературы

- 1 Джекобсон, Н. Алгебры Ли / Н. Джекобсон. – М.: Мир, 1964. – 356 с.
- 2 Kamiya, N. On the Jacobson radicals of infinite-dimensional Lie algebras / N. Kamiya // Hiroshima Math. J. – 1979. – V. 9. – P. 37-40.
- 3 Kubo, F. Infinite-dimensional Lie algebras with null Jacobson radical / F. Kubo // Bull. Kyushu Inst. Technol. Math. Nat. Sci. – 1991. – V. 38. – P. 23-30.
- 4 Кучеров, А. А. О гомологическом описании радикала Джекобсона для алгебр Ли / А. А. Кучеров, С. А. Пихтильков, О. А. Пихтилькова // Чебышевский сборник. – 2010. – Т. 10. – Вып. 2. – С. 71-76.
- 5 Пихтильков, С. А. Структурная теория специальных алгебр Ли / С. А. Пихтильков. – Оренбург, ОГУ, 2013. – 171 с.
- 6 Парфенов, В. А. О слабо разрешимом радикале алгебр Ли / В. А. Парфенов // Сиб. мат. журнал. – 1971. – Т. 12. – № 1. – С. 171-176.
- 7 Amayo, R. Infinite dimensional Lie algebras / R. Amayo, I Stewart. – Leyden: Noordhoof, 1974.
- 8 Мещерина, Е. В. О проблеме А. В. Михалева для алгебр Ли / Е. В. Мещерина, С. А. Пихтильков, О. А. Пихтилькова // Известия Саратовского университета. Новая серия. Серия Математика. Механика. Информатика. – 2013. – Т. 13. – С. 84-89.
- 9 Бейдар, К. И. Первичный радикал специальных алгебр Ли / К. И. Бейдар, С. А. Пихтильков // Фундаментальная и прикладная математика. – 2000. – Т. 6. – Вып. 3. – С. 643-648.
- 10 Кочетова, Ю. В. Первичный радикал решеточно К-упорядоченных алгебр / Ю. В. Кочетова, Е. Е. Ширинова // Фундаментальная и прикладная математика. – 2013. – Т. 18, № 1. – С. 85-158.
- 11 Балаба, И. Н. Первичный радикал специальных супералгебр Ли / И. Н. Балаба, С. А. Пихтильков // Фундаментальная и прикладная математика. – 2003. – Т. 9. – Вып. 1. – С. 51-60.
- 12 Поляков, В. М. О локально нильпотентных артиновых алгебрах Ли / С. А. Пихтильков, В. М. Поляков // Чебышевский сборник. – 2005. – Т. 6. – Вып. 1. – С. 163-169.
- 13 Кучеров, А. А. О почти локально разрешимых алгебрах Ли с нулевым радикалом Джекобсона и локально нильпотентном радикале для алгебр Ли / А. А. Кучеров // Вестник Оренбургского государственного университета. – 2013. – № 1. – С. 121-125.

РЕШЕНИЕ ЗАДАЧ ПЛАНИРОВАНИЯ ВИРТУАЛЬНЫХ МАШИН И СБОРА СТАТИСТИКИ О РАБОТЕ ОБЛАЧНЫХ ПРИЛОЖЕНИЙ

Полежаев П.Н.

Оренбургский государственный университет, г. Оренбург

В настоящее время облачные вычисления получили широкое распространение во всех областях жизни человека. Сейчас публичные и приватные облачные системы используются различными организациями для размещения собственных ИТ-инфраструктур, бизнес-приложений, коммуникационных сервисов.

При использовании приватных облачных систем компании получают возможность консолидировать вычислительные и сетевые ресурсы собственного центра обработки данных (ЦОД) и эффективно управлять ими. Достоинства – гибкость и простота развертывания облачных сервисов и приложений, высокая надежность работы, эффективное использование ресурсов за счет виртуализации.

В случае публичных облачных систем компании получают дополнительные преимущества. В первую очередь – это экономия финансовых средств за счет отсутствия необходимости содержать собственный парк серверов, их обслуживать, амортизировать. Также отсутствует необходимость нанимать высокооплачиваемых специалистов для их настройки и эксплуатации. Использование публичных облачных систем позволяет оплачивать фактически используемые облачные ресурсы (время работы виртуальных машин, сетевой трафик, фактически хранящиеся данные и т.п.), это дает значительную гибкость в управлении ИТ-инфраструктурой. В частности, можно масштабировать работу собственных сервисов и приложений в зависимости от ежедневного, еженедельного, ежемесячного или годового цикла работы с ними сотрудников и клиентов компании, увеличивать их масштаб в случае прогнозируемых или непредвиденных пиков работы с ними. Как правило заказ сервисов и их масштабирование осуществляется через портал самообслуживания публичного облачного провайдера, либо это может осуществляться автоматически через предоставляемый API.

Если рассматривать сторону владельца облачной системы – провайдера (в случае публичного облака) или самой компании (в случае приватного облака), то очень важно эффективно использовать имеющиеся ресурсы – вычислительные ресурсы и память серверов, программные лицензии, каналы связи.

В рамках данной работы рассматриваются проблемы эффективного планирования виртуальных машин для облачных систем, а также построения коммуникационных схем сервисов на основе статистики их взаимодействия.

Каждый программный сервис (приложение) облачной системы может быть представлен в виде динамического взвешенного ориентированного графа:

$$G(t) = (V, E, d(e, t), w(v)),$$

где V – множество вершин, представляющих собой компоненты сервиса; E – максимальное полное множество дуг (сетевых соединений), допустимых между вершинами V ; $d(e, t)$ – функция, определяющая количество передаваемых данных по дуге $e \in E$ в момент времени $t \geq 0$; $w(v)$ – характеристики вершины $v \in V$.

Если $d(e, t) = 0$, то дуга e отсутствует в момент времени t .

Множество компонентов представляет собой следующее объединение:

$$V = P \cup Q \cup D \cup S,$$

где P – набор запущенных программ (процессов), Q – множество используемых очередей, D – множество хранилищ данных, S – множество точек взаимодействия со стандартными сервисами облачной системы (например, сервис СУБД, Hadoop, Machine Learning, входными шлюзами/балансировщиками нагрузки (для запросов из Интернет)).

Построения коммуникационных схем сервисов на основе статистики их взаимодействия заключается в выявлении вершин V и в задании функции $d(e, t)$. Сами вершины выявлять, как правило, не требуется, т.к. у программных сервисов имеется конфигурационный файл, который их описывает. Это может быть конфигурационный файл облачной системы или файл с описанием контейнеров (при использовании микросервисной контейнерной архитектуры), например, `docker-compose.yml` для Docker.

Для построения функции $d(e, t)$ может быть использовано два подхода:

а) сбор информации о коммуникациях с помощью счетчиков OpenFlow [1–3];

б) получение сведений о коммуникациях с помощью перехвата всех коммуникационных вызовов в сетевом API (библиотека передачи сообщений облачной системы, сетевые сокеты и т.п.).

Подход а) работает в программно-конфигурируемых сетях и является более универсальным по сравнению с б), т.к. последний предполагает реализацию для всех возможных коммуникационных библиотек промежуточного интерфейса API, содержащего вызовы, которые оборачивают оригинальные вызовы и дополнительно сохраняют информацию о передаваемых потоках данных.

Протокол OpenFlow поддерживает счетчик “Received Bytes” категории “Per Flow Entry” (количество байт, переданных данным потоком), который используется разработанным алгоритмом построения коммуникационных схем сервисов на основе статистики их взаимодействия.

Для реализации первого подхода контроллер должен регулярно запрашивать информацию по счетчикам у всех коммутаторов OpenFlow (см.

алгоритм 1). В данном алгоритме используется обозначение $Rb(l, t)$ – количество байт переданных по маршруту l с начала его существования до момента времени t . Данная величина вычисляется на основе значениях счетчиков производительности $Rb(Switch_j, t)$ во всех коммутаторах OpenFlow $Switch_j$, через которые проходит маршрут l , согласно формуле:

$$Rb(l, t) = \frac{1}{k(l)} \sum_{Switch_j \in l} Rb(Switch_j, t),$$

где $k(l)$ – количество коммутаторов OpenFlow в маршруте l .

Фактически $Rb(l, t)$ вычисляется, как среднее арифметическое значение счетчиков со всех коммутаторов вдоль маршрута. Это необходимо для решения проблемы временного рассогласования получаемых значений счетчиков с разных коммутаторов OpenFlow и с наличием пакетов потоков, перемещающихся вдоль маршрута.

Алгоритм 1 – Алгоритм построения коммуникационных схем сервисов на основе статистики их взаимодействия с использованием счетчиков OpenFlow

Шаг 1. Получить граф топологии облачной системы, включая физические узлы, виртуальные машины и контейнеры.

Шаг 2. По таймеру раз в ΔT_{stat} секунд выполнять следующие действия:

Шаг 2.1. Получить список запущенных облачных приложений $Apps(t) = \{G_i(t)\}_i$ облачного ЦОД.

Шаг 2.2. Получить список текущих маршрутов L_{Routes} передачи данных, проложенных алгоритмом маршрутизации. Для каждого нового маршрута $l \in L_{Routes}$ положить в t_{prev}^l текущее время.

Шаг 2.1. Для каждого маршрута $l \in L_{Routes}$:

Шаг 2.1.1. Определить приложение $G_i(t)$ и дугу e , к которым относится данный маршрут l .

Шаг 2.1.2. Взять текущее время t_{cur}^l .

Шаг 2.1.3. Присвоить $d(e, t) := \frac{Rb(l, t_{cur}^l) - Rb(l, t_{prev}^l)}{t_{cur}^l - t_{prev}^l}$ для всех $t \in [t_{prev}^l, t_{cur}^l]$.

Шаг 2.1.4. $t_{prev}^l := t_{cur}^l$.

Алгоритм 1 реализуется в виде модуля для контроллера OpenFlow.

Формализуем задачу планирования виртуальных машин с учетом топологии системы и коммуникационных схем сервисов, запускаемых внутри виртуальных машин.

Возможны два случая:

а) Запуск группы виртуальных машин для назначения компонентов запускаемого облачного сервиса (приложения).

б) Запуск одиночной виртуальной машины для размещения компоненты (микросервиса) облачного приложения. Потребность в решении подобной задачи возникает при необходимости увеличить количество экземпляров микросервиса, например, при его ручном или автоматическом масштабировании.

Рассмотрим первый случай. Коммуникационная схема облачного приложения $G(t)$ может быть задана явно пользователем или получена с помощью алгоритма построения коммуникационных схем сервисов на основе статистики их взаимодействия. В случае отсутствия информации о схеме и невозможности ее получить в ситуации, когда облачное приложение запускается первый раз в облачной системе, будем считать, что коммуникационный паттерн $G(t)$ соответствует полному графу, причем $d(e, t) = \bar{B} = \text{const}$ – т.е. для любой дуги в любой момент времени количество передаваемых данных равно средней скорости передачи данных $\bar{B}$, вычисленной по всем ранее запущенным в облачной системе приложениям.

Решение данной задачи сводится к задаче назначения облачного сервиса на новые виртуальные машины $VMs^*(t)$, которые могут быть запущены с использованием остаточных ресурсов физических серверов. Формируется список подобных потенциальных виртуальных машин, затем осуществляется на них назначение с помощью алгоритма, описанного в статье Полежаева П.Н. «Создание эффективных алгоритмов функционирования облачных систем», опубликованной в материалах данной конференции.

Второй случай. Пусть v' – новый экземпляр микросервиса. Обозначим новый граф облачного приложения в виде:

$$G'(t) = (V', E').$$

$$\text{Здесь } V' = V \cup \{v'\}, E' = E \cup \bigcup_{u \in V} \{(u, v')\} \cup \bigcup_{u \in V} \{(v', u)\}.$$

Пусть $\text{Type}(v)$ – тип вершины v (процесс, очередь, хранилище). Обозначим в качестве $M(v, G) = \{u \in V \mid \text{Type}(v) = \text{Type}(u)\}$.

Для добавленных дуг задаются значения весовой функции d по формулам:

$$d((u, v'), t) = \frac{1}{|M(v', G)|} \sum_{v \in M(v', G)} d((u, v), t),$$

$$d((v', u), t) = \frac{1}{|M(v', G)|} \sum_{v \in M(v', G)} d((v, u), t).$$

Данные формулы позволяют новым дугам, соединяющим старую вершину $u \in V$ и новую вершину v' , приписать для каждого момента времени t средние значения скорости передачи данных, вычисленные по аналогичным дугам, соединяющим вершину $u \in V$ и старые вершины того же типа. В процессе работы данные веса могут уточняться за счет детального сбора статистики.

Пусть $\varphi_{G,VM} = \text{Append}(\varphi_G, VM) = (VM_1, \dots, VM_{n(G)}, VM)$, где φ_G – определяет построенное назначение компонентов-микросервисов облачного приложения на виртуальные машин.

Опишем разработанный жадный алгоритм выбора виртуальной машины для запуска нового экземпляра микросервиса v' (см. алгоритм2).

Алгоритм 2 – Алгоритм выбора виртуальной машины для запуска нового экземпляра микросервиса

Шаг 1. По облачному приложению $G(t)$ построить $G'(t)$, уточнить значения весовой функции d .

Шаг 2. Сформировать список виртуальных машин $VMs'(t)$, существующих в ЦОД на момент времени t и удовлетворяющих ресурсным требованиям v' .

Шаг 3. Сформировать список новых виртуальных машин $VMs'^*(t)$, которые построены на основе свободных на момент времени t ресурсов серверов и удовлетворяют ресурсным требованиям v' .

Шаг 4. Используя алгоритм проактивной маршрутизации вычислить:

$$VM_{opt} = \arg \max_{VM \in VMs'(t) \cup VMs'^*(t)} \{ \alpha I_{comp}(\varphi_{G,VM}) + (1 - \alpha) I_{comm}(\varphi_{G,VM}) \},$$

где $\alpha \in [0,1]$ – весовой коэффициент, I_{comp} – оценка эффективности использования вычислительных ресурсов, на которые назначены микросервисы приложения, I_{comm} – оценка использования сети в результате назначения всех дуг $e \in E$ на маршруты передачи данных в облачном ЦОД.

Шаг 5. Если $VM_{opt} \in VMs'^*(t)$, то запустить виртуальную машину VM_{opt} .

Шаг 6. Присвоить $\varphi_{G'} := \varphi_{G,VM_{opt}}$. Назначить v' на VM_{opt} .

Шаг 7. Проложить маршруты передачи данных, соответствующие VM_{opt} .

С целью экспериментального оценивания разработанных алгоритмов был создан симулятор облачной системы и программно-конфигурируемой сети. В его основе лежит разработанная имитационная модель [4].

Экспериментальное исследование алгоритма построения коммуникационных схем сервисов на основе статистики их взаимодействие запланировано на следующий этап исследования, когда будет использоваться реальный облачный ЦОД. На данном этапе с помощью симулятора подтверждена его работоспособность и корректность работы.

Исследование предложенного алгоритма планирования виртуальных машин с учетом топологии системы и коммуникационных схем сервисов проводилось в сравнении со стандартным алгоритмом планирования match-making системы OpenNebula [5], основанном на фильтрации и ранжировании серверов. Следует заметить, что он не учитывает топологию системы и

коммуникационные схемы сервисов. Это сказалось на полученных результатах (см. рисунок 1).

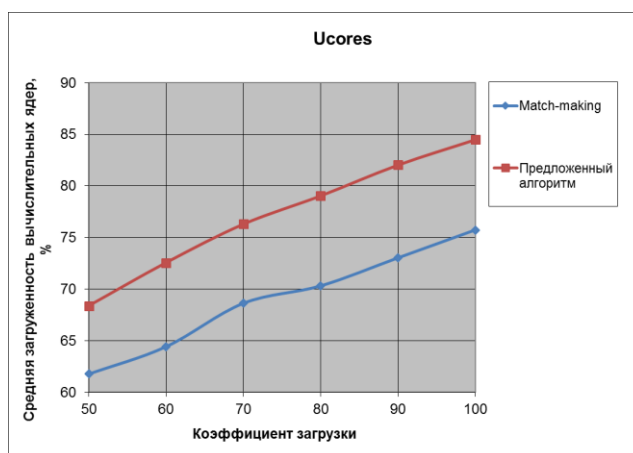


Рисунок 1 – Графики зависимости загрузки вычислительных ядер облачной системы от коэффициента загрузки для алгоритмов планирования виртуальных машин

Для предложенного алгоритма планирования в качестве алгоритма назначения использовался разработанный генетический алгоритм в сочетании с созданным алгоритмом проактивной маршрутизации, а для алгоритма match-making применялся принцип назначения Best Fit в сочетании с реактивным алгоритмом маршрутизации OSPF – характерное сочетание для обычных облачных систем.

Рисунок 1 показывает преимущество предложенного алгоритма в сравнении со стандартными решениями на 6-9 % в зависимости от коэффициента загрузки.

В рамках данной статьи были описаны созданные решения – алгоритмы планирования виртуальных машин с учетом топологии системы и коммуникационных схем сервисов, запускаемых внутри виртуальных машин, а также алгоритм построения коммуникационных схем сервисов на основе статистики их взаимодействия. Оба алгоритма были исследованы с помощью симулятора облачной системы и программно-конфигурируемой сети.

Исследования проведены при финансовой поддержке РФФИ и Правительства Оренбургской области (проект № 16-47-560335), Президента Российской Федерации, стипендии для молодых ученых и аспирантов (СП-2179.2015.5).

Список литературы

1. OpenFlow - Open Networking Foundation [Электронный ресурс] // Open Networking Foundation. – Электрон. дан. – 2016. Режим доступа: <https://www.opennetworking.org/sdn-resources/openflow>. Загл. с экрана. - (Дата обращения: 25.11.2016).
2. Полежаев П.Н. Изучение возможностей контроллера Ryu и оценка

эффективности программно-конфигурируемой сети / П.Н. Полежаев, В.И. Чернов, С.Ю. Шиховцов // Прикладные информационные системы: третья Всероссийская НПК (г. Ульяновск, 30 мая – 12 июня 2016 г.): сборник научных трудов / под ред. Е. Н. Эгова. – Ульяновск : УлГТУ, 2016. – С. 151-158.

3. Чернов В.И. Сравнительный анализ существующих контроллеров для программно-конфигурируемых сетей / В.И. Чернов, С.Ю. Шиховцов, П.Н. Полежаев // Университетский комплекс как региональный центр образования, науки и культуры [Электронный ресурс]: материалы Всероссийской научно-методической конференции; Оренбург. гос. ун-т. - Электрон. дан. - Оренбург: ОГУ, 2016. – С. 2524-2529.

4. Легашев Л.В. Имитационная модель облачного ресурсного центра / Л.В. Легашев, И.П. Болодурина, П.Н. Полежаев // Интеллект. Инновации. Инвестиции. – 2016. – №2. – С. 113-116.

5. Scheduler – OpenNebula 5.0.2 documentation [Электронный ресурс] // OpenNebula Project (OpenNebula.org). – Электрон. дан. – 2016. Режим доступа: http://docs.opennebula.org/5.0/operation/host_cluster_management/scheduler.html. Загл. с экрана. - (Дата обращения: 25.11.2016).

СОЗДАНИЕ ЭФФЕКТИВНЫХ АЛГОРИТМОВ ФУНКЦИОНИРОВАНИЯ ОБЛАЧНЫХ СИСТЕМ

Полежаев П.Н.

Оренбургский государственный университет, г. Оренбург

В рамках настоящего исследования рассматриваются проблемы эффективного назначения облачных сервисов (приложений) на виртуальные машины и маршрутизации потоков данных между ними с использованием программно-конфигурируемых сетей.

Каждый программный сервис (приложение) облачной системы может быть представлен в виде динамического взвешенного ориентированного графа:

$$G(t) = (V, E, d(e, t), w(v)),$$

где V – множество вершин, представляющих собой компоненты сервиса; E – максимальное полное множество дуг (сетевых соединений), допустимых между вершинами V ; $d(e, t)$ – функция, определяющая количество передаваемых данных по дуге $e \in E$ в момент времени $t \geq 0$; $w(v)$ – характеристики вершины $v \in V$.

Множество компонентов представляет собой следующее объединение:

$$V = P \cup Q \cup D \cup S,$$

где P – набор запущенных программ (процессов), Q – множество используемых очередей, D – множество хранилищ данных, S – множество точек взаимодействия со стандартными сервисами облачной системы.

Задача назначения облачного приложения на виртуальные машины может быть формализована следующим образом.

Будем считать, что каждое облачное приложение $G(t)$ имеет микросервисную архитектуру, основанную на контейнерах [1]. Микросервис $v \in V \setminus S$ запускается в отдельном контейнере $c(v)$. Вершины $v \in S$ не участвуют в задаче назначения, т.к. по сути они являются точками подключения (привязки) к другим облачным приложениям или к стандартным сервисам облачной системы. Однако для подобных вершин важна коммуникационная составляющая.

Пронумеруем все вершины, содержащие микросервисы, следующим образом:

$$V \setminus S = \{v_1, v_2, \dots, v_{n(G)}\},$$

где $n(G) = |V \setminus S|$ – количество микросервисов.

Пусть $VMs(t)$ – существующие в ЦОД виртуальные машины на момент времени t , которые готовы принимать для назначения контейнеры, $VMs^*(t)$ – максимальные по конфигурации виртуальные машины, которые могут быть запущены на оставшихся ресурсах физических серверов на момент времени t (по одной на каждый сервер).

Каждый контейнер $c(v)$ с микросервисом облачного приложения должен быть развернут внутри одной из запущенных виртуальных машин $VM \in VMs(t)$ облачного ЦОД или в новой виртуальной машине $VM^* \in VMs^*(t)$, которая будет запущена на одном из физических серверов $Server^* \in Servers$ (используя все свободные ресурсы).

С целью формализации соответствия микросервис-контейнер-виртуальная машина введем следующий вектор:

$$\varphi_G = (VM_1, VM_2, VM_3, \dots, VM_{n(G)}),$$

где $\varphi_G(v_i) = VM_i \in VMs(t) \cup VMs^*(t)$ – виртуальная машина, на которую назначен контейнер $c(v_i)$, содержащий микросервис v_i .

Для оценки эффективности φ_G может быть построена следующая функция, значение которой должно быть оптимизировано:

$$I(\varphi_G) = \alpha I_{comp}(\varphi_G) + (1 - \alpha) I_{comm}(\varphi_G) \rightarrow \max,$$

где $\alpha \in [0,1]$ – весовой коэффициент, $I_{comp}(\varphi_G)$ – оценка эффективности использования вычислительных ресурсов, на которые назначены микросервисы приложения G , $I_{comm}(\varphi_G)$ – оценка использования сети в результате назначения всех дуг $e \in E$ на маршруты передачи данных в облачном ЦОД.

Должны выполняться следующие ограничения:

а) ресурсные требования v_i соответствуют свободным ресурсам VM_i , т.е.

$$m_{v_i} \leq RAM_{VM_i} - m_{VM_i}(t),$$

$$d_{v_i} \leq HDD_{VM_i} - d_{VM_i}(t),$$

$$u_{v_i} \leq Cores_{VM_i} - u_{VM_i}(t),$$

где m_{v_i} и d_{v_i} – соответственно запрашиваемые размеры оперативной и дисковой памяти, необходимой для функционирования микросервиса v_i ; u_{v_i} – доля запрашиваемых микросервисом вычислительных ядер; RAM_{VM_i} и HDD_{VM_i} – соответственно размеры оперативной и дисковой памяти виртуальной машины VM_i ; $Cores_{VM_i}$ – количество вычислительных ядер у VM_i , $m_{VM_i}(t)$ и $d_{VM_i}(t)$ – соответственно размеры занятой оперативной и дисковой памяти внутри виртуальной машины VM_i в текущий момент времени t , $u_{VM_i}(t)$ – доля использования вычислительных ядер виртуальной машины VM_i в момент времени t .

б) также должны выполняться сетевые ограничения.

В качестве $I_{comp}(\varphi_G)$ предлагается использовать функцию следующего вида:

$$I_{comp}(\varphi_G) = \frac{1}{n(G)} \sum_{i=1}^{n(G)} \bar{U}_{VM,i},$$

где $\bar{U}_{VM,i}$ – оценка средней загруженности i -й виртуальной машины.

Задачу оптимизации функции $I(\varphi_G)$ будем решать с помощью генетического алгоритма, вычисляющего оптимальное назначение φ_G и вложенного алгоритма маршрутизации потоков данных, который прокладывает маршруты передачи данных между вершинами облачного приложения G с учетом φ_G . Для оценки эффективности проложенных маршрутов используется величина $I_{comm}(\varphi_G)$.

Хромосома в генетическом алгоритме будет представлять собой вектор φ_G , а его компоненты будут являться генами. Опишем основные генетические операторы (см. алгоритм 1): операция скрещивания – обычное одноточечное скрещивание для двух векторов; мутация – случайная замена одной виртуальной машины на другую, удовлетворяющую ресурсным требованиям соответствующего микросервиса, селекция – элитный отбор в сочетании с рулеткой. Критерии окончания работы алгоритма – превышение предельного времени T_{max} и отсутствие улучшений в среднем значении оптимизируемой функции на протяжении нескольких поколений.

Алгоритм 1 – Генетический алгоритм назначения облачных приложений

Шаг 1. Замерить текущий момент времени T_{start} .

Шаг 2. Создать $Population_i$ начальную популяцию размера N путем случайного выбора назначаемых виртуальных машин для микросервисов.

Шаг 3. Положить в качестве номера итерации значение $i := 1$.

Шаг 4. Пока $T_{current} - T_{start} < T_{max}$ и имеются улучшения в среднем значении функции $I(\varphi_G)$ на протяжении K поколений необходимо выполнить следующие шаги:

Шаг 4.1. Над хромосомами $Population_i$ с вероятностью P выполнить операции скрещивания, объединив родительские хромосомы в случайные пары. Получаемые дочерние хромосомы сохранить в $Population'_i$.

Шаг 4.2. Для хромосом $Population'_i$ выполнить операцию мутации с вероятностью Q .

Шаг 4.3. Объединить родительские и дочерние популяции $Population''_i := Population_i \cup Population'_i$

Шаг 4.4. Для каждой хромосомы $\varphi_G \in Population''_i$ запустить алгоритм маршрутизации с целью проактивного вычисления наилучших маршрутов передачи данных и получения оценки $I_{comm}(\varphi_G)$.

Шаг 4.5. Для каждой хромосомы $\varphi_G \in Population''_i$ вычислить оценку $I_{comp}(\varphi_G)$.

Шаг 4.5. Для $Population''_i$ выполнить операцию селекции, используя в качестве функции соответствия функцию $I(\varphi_G)$, выбранные хромосомы сохранить в $Population_{i+1}$.

Шаг 4.6. Увеличить на единицу номер итерации $i := i + 1$ и перейти к шагу 4.

Шаг 5. Выполнить назначение в соответствии с лучшим значением $\varphi_G^{\max}$ последнего поколения, при необходимости запустить новые виртуальные машины и проложить вычисленные маршруты передачи данных для $\varphi_G^{\max}$.

Формализуем задачу реактивной и проактивной маршрутизации потоков данных между серверами и виртуальными машинами, исполняющими облачные сервисы.

Пусть $G_T(t) = (V_T, E_T)$ – ориентированный мультиграф, описывающий текущую топологию сети в некоторый момент времени t . Множество его вершин V_T является объединением множества узлов (серверов, виртуальных машин, контейнеров) и других сетевых устройств (коммутаторов, шлюзов, СХД и т.п.).

Каждая дуга $e_T \in E_T$ соответствует некоторой сетевой связи между вершинами $\text{beg}(e_T) \in V_T$ и $\text{end}(e_T) \in V$. У нее также есть противоположная дуга, т.к. связь дуплексная. Между двумя вершинами может быть несколько параллельных дуг, например, параллельные соединения между маршрутизаторами.

На множестве дуг E_T заданы две функции:

а) $b: E_T \rightarrow \mathbb{R}^+ \cup \{0\}$ – отображение, характеризующее текущую пропускную способность каждой дуги в момент времени t .

б) $s: E_T \rightarrow \mathbb{R}^+ \cup \{0\}$ – задержка на соответствующем выходном порту дуги в момент времени t .

Пусть для каждой дуги $e \in E$ облачного приложения $G(t)$ заданы значения:

а) $\underline{b}(e) = \max_t d(e, t)$ – минимальная гарантированная пропускная способность потоков данных, соответствующих данной дуге.

б) $\bar{s}(e) = s = \text{const}$ – максимальная гарантированная задержка (задается в конфигурации облачного приложения).

в) $\hat{s}(e)$ – оценка средней задержки, которая возникнет при обработке пакетов потоков данных на портах сетевых устройств.

Для вычисления $I_{\text{comm}}(\varphi_G)$ может быть использована функция:

$$\begin{aligned}
I_{\text{comm}}(\varphi_G) = \max_R I_{\text{comm}}(\varphi_G, R) = \\
\sum_{\substack{e_i \in E: \\ \min_{e_T \in r_i} \{b(e_T) - \sum_{c \in \psi(e_T) \setminus \{e_i\}} b(c)\} \geq \underline{b}(e_i) \& \\ \sum_{e_T \in r_i} (s(e_T) + \sum_{c \in \psi(e_T) \setminus \{e_i\}} \hat{s}(c)) \leq \bar{s}(e_i)}} \left[\alpha_b (\min_{e_T \in r_i} \{b(e_T) - \sum_{c \in \psi(e_T) \setminus \{e_i\}} b(c)\} - \underline{b}(e_i)) + \alpha_s (\bar{s}(e_i) - \sum_{e_T \in r_i} s(e_T) - \sum_{c \in \psi(e_T) \setminus \{e_i\}} \hat{s}(c)) \right] + \\
+ \beta_b \cdot \sum_{\substack{e_i \in E: \\ \min_{e_T \in r_i} \{b(e_T) - \sum_{c \in \psi(e_T) \setminus \{e_i\}} b(c)\} < \underline{b}(e_i)}} \left[\min_{e_T \in r_i} \{b(e_T) - \sum_{c \in \psi(e_T) \setminus \{e_i\}} b(c)\} - \underline{b}(e_i) \right] + \\
+ \beta_s \cdot \sum_{\substack{e_i \in E: \\ \sum_{e_T \in r_i} (s(e_T) + \sum_{c \in \psi(e_T) \setminus \{e_i\}} \hat{s}(c)) > \bar{s}(e_i)}} \left| \bar{s}(e_i) - \sum_{e_T \in r_i} s(e_T) - \sum_{c \in \psi(e_T) \setminus \{e_i\}} \hat{s}(c) \right|
\end{aligned}$$

где $R = (r_1, \dots, r_{|E|})$ – вектор, задающий маршруты передачи потоков данных, причем $r_i = \delta(e_i)$ – соответствие между коммуникационной связью $e_i \in E$ облачного приложения $G(t)$ и маршрутом r_i , вдоль которого планируется передача данных; $\psi(e_T) = \{e \in E \mid r = \delta(e) \& e_T \in r\}$ – множество коммуникационных связей облачного приложения, маршруты которых проходят через e_T , $\alpha_b > 0$ и $\alpha_s > 0$ – поощрения за соблюдение соответствующих ограничений по пропускной способности и задержкам, $\beta_b < 0$ и $\beta_s < 0$ – штрафы за их несоблюдение. Функция $I_{\text{comm}}(\varphi_G, R)$ отражает поощрения за соблюдение гибких ограничений по пропускной способности и задержкам, устанавливает штрафы за их нарушения.

Также имеются жесткие ограничения на маршруты $r_i = (e'_{i1}, \dots, e'_{in_i})$:

1. r_i действительно является маршрутом:

$$\forall r_i \quad \forall j = \overline{1, n_i - 1} \quad \text{end}(e'_{ij}) = \text{beg}(e'_{ij+1}).$$

2. r_i должен начинаться в вершине, соответствующей началу дуги e_i и заканчиваться в вершине, соответствующей концу e_i , т.е.:

$$\forall r_i \quad \text{beg}(e_{i1}) = \text{beg}(e_i) \& \text{end}(e_{in_i}) = \text{end}(e_i).$$

3. r_i не должен проходить несколько раз через одну и ту же вершину, т.е.:

$$\forall r_i \quad \forall j, k = \overline{1, n_i} \quad j \neq k \Rightarrow \text{beg}(e_{ij}) \neq \text{beg}(e_{ik}).$$

Для оптимизации функции $I_{\text{comm}}(\varphi_G, R)$ по R в рамках данной работы предлагается использовать генетический алгоритм (см. алгоритм 2). Хромосомой будет являться вектор R . Алгоритм использует генетические операторы, аналогичные алгоритму 1: одноточечное скрещивание, элитный отбор в сочетании с рулеткой. Операция мутации заключается в замене одного проложенного маршрута передачи данных другим альтернативным.

Алгоритм 2 – Генетический алгоритм проактивной маршрутизации потоков данных

Шаг 1. Замерить текущий момент времени T_{start} .

Шаг 2. Создать $Population_i$ начальную популяцию размера M . В качестве одной из хромосом R выбрать маршруты, проложенные с помощью алгоритма Дейкстры, запущенного из каждой вершины V , руководствуясь минимизацией суммарных ограничений по задержкам. Остальные хромосомы сгенерировать случайным образом.

Шаг 3. Положить в качестве номера итерации значение $i := 1$.

Шаг 4. Пока $T_{current} - T_{start} < T_{max}$ и имеются улучшения в среднем значения функции $I_{comm}(\varphi_G, R)$ на протяжении K поколений необходимо выполнить следующие шаги:

Шаг 4.1. Над хромосомами $Population_i$ с вероятностью P' выполнить операции скрещивания, объединив родительские хромосомы в случайные пары. Получаемые дочерние хромосомы сохранить в $Population'_i$.

Шаг 4.2. Для хромосом $Population'_i$ выполнить операцию мутации с вероятностью Q' .

Шаг 4.3. Объединить родительские и дочерние популяции $Population''_i := Population_i \cup Population'_i$

Шаг 4.4. Для $Population''_i$ выполнить операцию селекции, выбранные хромосомы сохранить в $Population_{i+1}$.

Шаг 4.5. Увеличить на единицу номер итерации $i := i + 1$ и перейти к шагу 4.

Шаг 5. Вернуть все маршруты из лучшей хромосомы $Population_i$.

Для реактивной маршрутизации, когда маршрут передачи потока данных в момент его появления в сети, разработан алгоритм 4.

Алгоритм 4 – Реактивная маршрутизация потоков данных

Шаг 1. Прочитать вершины отправителя $u \in V_T$ и получателя $u' \in V_T$ потока данных.

Шаг 2. Используя текущий граф топологии $G_T(t)$ с помощью алгоритма Дейкстры рассчитать маршрут передачи данных от u до u' , используя в качестве весов остаточные пропускные способности дуг.

Шаг 3. С помощью правил OpenFlow [2] установить вычисленный маршрут в коммутаторы.

Для экспериментального оценивания разработанных алгоритмических решений был создан симулятор облачной системы и программно-конфигурируемой сети. В его основе лежит:

а) Симуляция работы облачной системы – системы управления, работы виртуальных машин, дисковых образов, шаблонов, хранилищ данных, контейнеров, серверов и т.п. Симуляция позволила на данном этапе НИР сосредоточиться на разработке алгоритмов, а не на реализации технических задач.

б) Эмуляция работы программно-конфигурируемой сети за счет использования системы Mininet [3], поддерживающей протокол OpenFlow. Использование эмулятора позволило обеспечить детальное моделирование компьютерной сети. В качестве контроллера для программно-конфигурируемой сети был выбран Ryu.

В процессах узлов, имитирующих компоненты облачных приложений, запускаются генераторы трафика с заданными параметрами, которые берутся из компоненты симуляции облачной системы.

Генетические алгоритмы назначения облачных приложений и проактивной маршрутизации потоков данных исследовались совместно, рассматривались сочетания генетического алгоритма назначения с генетическим алгоритмом проактивной маршрутизацией (ГА+ГА) и с проактивным алгоритмом OSPF (ГА+OSPF).

С этой целью генерируется пуассоновский поток заявок на запуск облачных приложений $\sigma_G = \{G_i(t)\}$, интервалы времени между появлением заявок распределены экспоненциально с интенсивностью λ_G . Параметры заявок генерировались с помощью подобранных законов распределения согласно имитационной модели. В качестве физической конфигурации системы была использована топология, ранее нами использованная в работе [4].

На рисунке 1 представлены графики зависимости процента нарушений требований QoS (а) и средней загруженности вычислительных ядер облачной системы (б) от коэффициента загрузки, вычисляемого на основе варьируемой интенсивности λ_G . Каждое значение, отмеченное графике, представляет собой усредненное значение соответствующей метрики на 50 случайно сгенерированных потоках заявок на запуск облачных приложений σ_G .

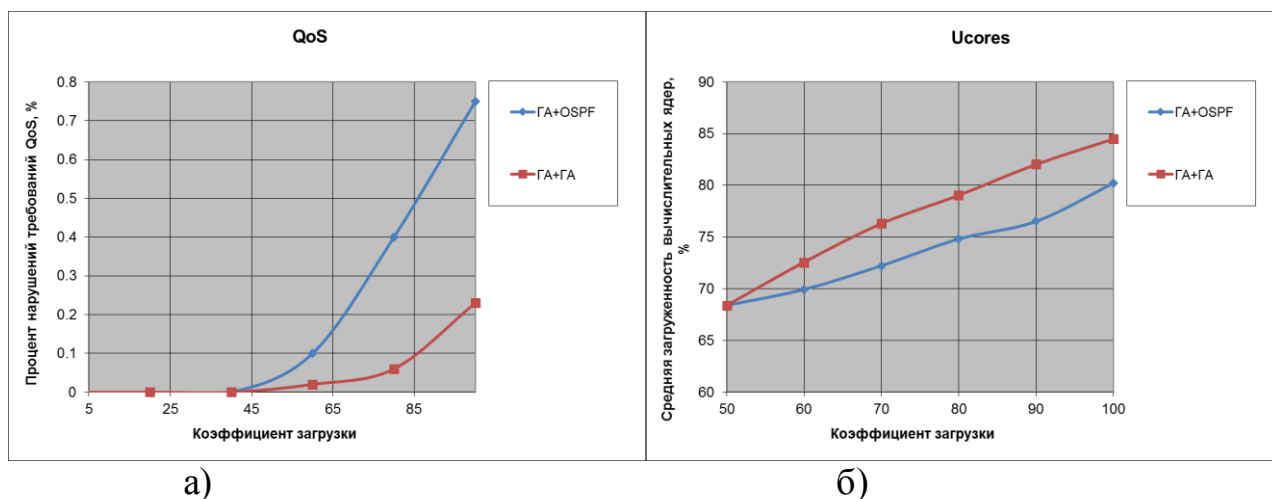


Рисунок 1 – Графики зависимости метрик эффективности от коэффициента загрузки для алгоритмов ГА+ГА и ГА+OSPF: а) процент нарушения требований QoS; б) средняя загруженность вычислительных ядер

Анализ рисунка 1 а) показывает, что сочетания ГА+ГА и ГА+OSPF демонстрирует нулевой процент нарушений требований QoS до тех пор, пока не будет достигнуто значение коэффициента загрузки ~40%. После данного порога сочетание ГА+ГА показывает гораздо лучшие значения данной метрики по сравнению с ГА+OSPF. Рисунок 2 б) демонстрирует преобладание алгоритма ГА+ГА по метрике средней загруженности вычислительных ядер над алгоритмом ГА+OSPF. Улучшения в абсолютном выражении составляют до 6%.

Разработанный реактивный алгоритм маршрутизации потоков данных (РА) исследовался совместно со стандартным реактивным OSPF. Эксперимент проводился на тех же потоках заявок, что и в первом эксперименте. Результаты представлены на рисунке 2.

Анализ графиков показывает рост процента нарушений требований QoS из-за реактивного характера маршрутизации трафика, а также небольшое преимущество предложенного алгоритма реактивной маршрутизации перед OSPF.

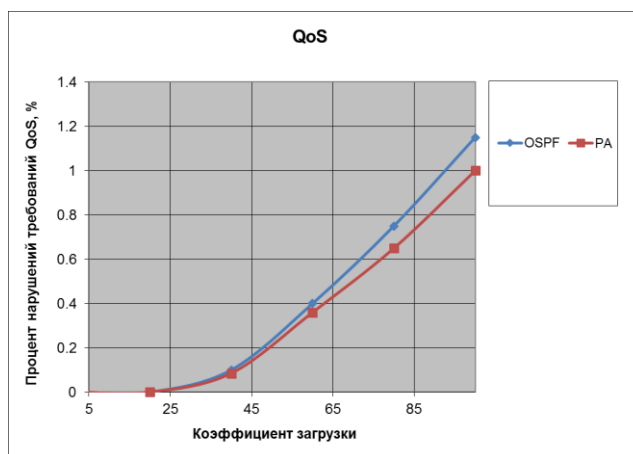


Рисунок 2 – Графики зависимости процента нарушений требований QoS от коэффициента загрузки для реактивных алгоритмов маршрутизации

Исследования проведены при финансовой поддержке РФФИ и Правительства Оренбургской области (проект № 16-47-560335), Президента Российской Федерации, стипендии для молодых ученых и аспирантов (СП-2179.2015.5).

Список литературы

1. Адрова Л.С. Сравнительный анализ существующих технологий контейнеризации / Л.С. Адрова, П.Н. Полежаев // Университетский комплекс как региональный центр образования, науки и культуры [Электронный ресурс]:

материалы Всероссийской научно-методической конференции; Оренбург. гос. ун-т. - Электрон. дан. - Оренбург: ОГУ, 2016. – Загл. с этикетки диска. – С. 2473-2477.

2. OpenFlow - Open Networking Foundation [Электронный ресурс] // Open Networking Foundation. – Электрон. дан. – 2016. Режим доступа: <https://www.opennetworking.org/sdn-resources/openflow>. Загл. с экрана. - (Дата обращения: 25.11.2016).

3. Introduction to Mininet [Электронный ресурс] // Mininet Project. – Электрон. дан. – 2016. Режим доступа: <https://github.com/mininet/mininet/wiki/Introduction-to-Mininet>. Загл. с экрана. – (Дата обращения: 25.11.2016).

4. Polezhaev P. Network Resource Control System for HPC based on SDN / P. Polezhaev, A. Shukhman, Yu. Ushakov // Proceedings of 14th International Conference, NEW2AN 2014 and 7th Conference ruSMART 2014, St. Petersburg, Russia. Lecture Notes in Computer Science. – vol. 8638. – PP. 219-230.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЭМУЛЯТОРОВ КОМПЬЮТЕРНЫХ СЕТЕЙ

Порохненко Ю.С., Полежаев П.Н.

Оренбургский государственный университет, г. Оренбург

В настоящее время всё больше развиваются технологии компьютерных сетей, появляются виртуальные, конвергентные, программно-конфигурируемые сети. Последние предназначены для эффективного управления потоками данных, передаваемых по сети, с единой точки – контроллера. Для реализации подобных сетей используется протокол OpenFlow [1].

Существует следующая классификация методов экспериментального исследования (см. таблицу 1) [2].

Таблица 1. Классификация методов исследования

Процесс	Вычислительная среда	
	Реальная	Модельная
Реальный	Натурное моделирование	Эмуляция
Модельный	Эталонное моделирование	Симуляция

Натурное моделирование представляет собой метод, при котором реальный процесс выполняется в реальной вычислительной среде. В качестве процесса могут выступать сервис, приложение и т.д., а в качестве среды – сервер, операционная система и т.д. При этом собирается информация о работе процесса и состоянии системы, в результате формируется статистика.

Эталонное тестирование – это метод, при котором смоделированный процесс выполняется в реальной среде, при этом оценивается эффективность её функционирования. Процесс должен охватывать следующие характеристики среды: её мощность, скорость обработки и ввода/вывода данных, пропускную способность сети и т.д. В отличие от натурального моделирования, в эталонном тестировании не важен результат выполнения процесса, внимание обращается на функционирование системы в ходе работы.

Симуляция представляет собой подход, при котором смоделированный процесс выполняется в рамках модели вычислительной среды. Такой метод позволяет многократно повторять испытания и достичь большого количества результатов на основе различных условий. В итоге можно оценить поведение системы в различных условиях и создать оптимальную стратегию управления ресурсами.

Эмуляция – это метод, в котором реальный процесс выполняется в модели вычислительной среды. Его идея заключается в том, что создаются синтетические условия для работы реального процесса. Примерами средств эмуляции являются такие проекты, как ModelNet [3], OMNet++ [4], Mininet [5], NS-3 [6].

В ходе исследования необходимо выбрать симулятор, который подходит для моделирования сети при решении следующих задач, связанных с разработкой эффективных алгоритмов планирования и миграции виртуальных машин. Рассмотрим ряд существующих решений.

ModelNet [3] представляет собой платформу для эмуляции сети, которая позволяет экспериментатору запускать реальный код на гипотетической сети с определенной пропускной способностью, задержкой, длиной очереди и другими свойствами. ModelNet может быть развернут на нескольких серверах. Один или несколько из них выделяются для эмуляции трафика, в то время как остальная часть может быть использована для работы в качестве узлов. Когда эти узлы взаимодействуют друг с другом, IP-пакеты посылаются через эмуляторы, чтобы создать иллюзию того, что пакеты приложений следуют по маршруту в реальной сети.

В первую очередь должна быть создана топология виртуальной сети. Для этого могут быть использованы инструменты Modelnet. Зная IP-адреса отправителя и получателя, эмулятор определяет путь и обрабатывает пакеты в соответствии с ним. Каждый хоп на этом пути имеет определенную пропускную способность, организацию очереди, задержку. Эмуляция происходит в режиме реального времени с точностью до миллисекунды.

Во многих распределенных системах серверы имеют гораздо большую мощность процессора и пропускную способность сети, чем требуется. Modelnet использует это, создавая сотни виртуальных узлов на каждом хосте.

OMNeT++ [4] обладает модульной структурой для моделирования сети. Она может использоваться в различных областях:

1. моделирование проводных и беспроводных сетей связи;
2. моделирование протоколов;
3. моделирование сетей массового обслуживания;
4. моделирование многопроцессорных систем и других распределенных аппаратных систем;
5. валидация аппаратных архитектур;
6. оценки аспектов производительности сложных программных систем.

OMNeT++ представляет собой инфраструктуру и инструменты для описания процесса моделирования. Модели собираются из повторно используемых компонентов – модулей. Модули могут быть соединены друг с другом через гейты (порты), а также вкладываться в другие более сложные модули без ограничения глубины вложения. Они связываются посредством передачи сообщений, которые могут содержать произвольные структуры данных. Модули могут передавать сообщения по заранее определенным путям или непосредственно к месту назначения. Последнее полезно для беспроводного моделирования, например. Модули могут иметь параметры, которые могут быть использованы для настройки их поведения или параметризовать топологию сети. Модули, располагающиеся на самом

низком уровне иерархии модулей, называются простыми, и они написаны на C++.

OMNeT++ может работать в графическом режиме и режиме командной строки.

Эмулятор может работать на наиболее распространенных ОС, таких как Linux, Mac OS/X, Windows. OMNeT++ также поддерживает параллельное распределенное моделирование, используя несколько механизмов для связи между распределенными процессами, например, MPI или именованные каналы.

OMNEST [4] – коммерческая версия OMNeT++. Сам OMNeT++ является бесплатным только для учебного и некоммерческого использования.

Mininet [5] – это сетевой эмулятор. Он запускает коллекцию конечных хостов, коммутаторов и маршрутизаторов на одном ядре Linux. Mininet использует облегченную виртуализацию для того, чтобы система выглядела как целая сеть, работающая на том же ядре, системе и под одним пользователем. Хост Mininet ведет себя так же, как настоящий сервер, может запускать произвольные программы (в том числе все, написанные под Linux). Пакеты посылаются с заданной скоростью передачи и задержкой. Они обрабатываются виртуальными программными коммутаторами Ethernet, маршрутизаторами или middlebox согласно заданной топологии. Mininet имитирует работу виртуальных хостов, коммутаторов, контроллеров.

Эмулятор имеет ряд недостатков:

1. ограничения на ресурсы: они должны быть сбалансированы и распределены между виртуальными хостами и коммутаторами;

2. использование ядра Linux для всех виртуальных хостов; это значит, что нельзя запустить программное обеспечение, которое написано для других ОС;

3. Mininet не прописывает правила OpenFlow, если нужны пользовательские настройки маршрутизации или коммутации, необходимо разработать контроллер с необходимыми функциями;

4. по умолчанию сеть Mininet изолирована от локальной сети;

5. хосты Mininet распределяются хост-файлами системы в PID-пространстве, из-за чего есть вероятность завершить системный процесс;

6. Mininet не имеет понятия виртуального времени.

NS-3 [6] представляет собой сетевой эмулятор дискретных событий, который ориентирован в первую очередь для научных исследований и образовательных целей. Он является свободным программным обеспечением.

Проект стремится к созданию цельного ядра моделирования, хорошо документированного, простого в использовании и отладке, который обслуживал бы потребности всего процесса моделирования, от конфигурации сети до сбора и анализа результатов. Ядро моделирования NS-3 поддерживает исследования как IP-сетей, так и сетей, построенных на других протоколах. Подавляющее большинство пользователей фокусируется на беспроводном/IP-моделировании, которые включают модели для Wi-Fi, WiMAX или LTE, а

также различных статических или динамических протоколов маршрутизации, таких как OLSR и AODV.

Кроме того, NS-3 поддерживает планировщик реального времени, что облегчает целый ряд случаев использования "моделирования-в-петле" для взаимодействия с реальными системами. Например, пользователи могут отправлять и принимать пакеты, сгенерированные эмулятором, с помощью реальных сетевых устройств, и NS-3 может служить в качестве основы для соединений между виртуальными машинами.

Эмулятор имеет ряд преимуществ:

1. управление ресурсами; пользователь может соответствующим образом настроить виртуальные машины для каждого конкретного моделирования с требуемыми параметрами, такими как CPU, RAM и т.д.;

2. пользователь может редактировать сценарии моделирования/исходный код и запускать новые симуляции сразу после запуска предыдущей, не опасаясь перегрузки машины;

3. пользователь может запускать большое количество параллельных симуляций на множестве виртуальных машин;

4. процесс сбора результатов централизован, пользователь всегда имеет доступ к результату и соответствующим сценариям моделирования;

5. возможность управления процессом моделирования с помощью любого устройства с подключением к Интернету, а также онлайн редактирование скриптов/исходных файлов;

6. полуавтоматический процесс наладки рабочей среды, знание облачной инфраструктуры не является необходимым;

7. простая миграция рабочей среды между виртуальными машинами с использованием облачных систем, пакетно-массовое обслуживание кластеров, вычислительных сеток Linux/UNIX хостов.

UNetLab [7] – бесплатная многопользовательская платформа для моделирования виртуальных сетей с поддержкой большого списка оборудования. Эмулятор представляет собой виртуальную машину, основанную на Linux Ubuntu. Доступ к управлению происходит через Web-интерфейс,

Сервис обладает рядом преимуществ:

1. практически полноценная поддержка L2;

2. широкая поддержка оборудования Cisco;

3. неограниченное число запускаемых узлов;

4. мультивендорность;

5. многопользовательский функционал с независимыми запусками стенда;

6. низкие требования к ресурсам ПК;

7. полностью графический дизайн топологии сети;

8. неограниченное количество соединений между устройствами.

В таблице 3 представлена сравнительная характеристика рассматриваемых эмуляторов.

У каждого из них имеется документация, они поддерживают возможность моделирования виртуальной сети. OMNet++ и UNetLab могут работать на всех операционных системах, а ModelNet только на ОС Linux. Эмуляторы Mininet и ModelNet не поддерживают установку в распределенном виде на нескольких ПК. Важным преимуществом OMNet++, NS-3, UNetLab является возможность моделирования беспроводных сетей.

Таблица 3 – Сравнительная характеристика эмуляторов

Название	Документация	Виртуальная сеть	Беспроводная сеть	Развертывание на нескольких компьютерах	ОС
ModelNet	+	+	-	+	Linux
OMNet++	+	+	+	-	Linux, Mac, Windows
Mininet	+	+	-	-	Windows, Linux
NS-3	+	+	+	+	Windows, Linux
UNetLab	+	+	+	+	Windows, Linux, Mac

По результатам анализа можно сделать вывод, что NS-3 и UNetLab являются самым многофункциональными эмуляторами, которые подходят для решения поставленных задач по разработке эффективных алгоритмических решений для облачных систем.

Исследования проведены при финансовой поддержке РФФИ и Правительства Оренбургской области (проект № 16-47-560335), Президента Российской Федерации, стипендии для молодых ученых и аспирантов (СП-2179.2015.5).

Список литературы

1. OpenFlow - Open Networking Foundation [Электронный ресурс] // Open Networking Foundation. – Электрон. дан. – 2016. Режим доступа: <https://www.opennetworking.org/sdn-resources/openflow>. Загл. с экрана. - (Дата обращения: 25.11.2016).
2. Gustedt, J. Experimental methodologies for large-scale systems: a survey / J.

Gustedt, E. Jeannot, M. Quinson // *Parallel Process. Lett. World Scientific*. 2009. Vol. 19. – с. 399–418.

3. Vahdat, A. Scalability and accuracy in a large-scale network emulator / A. Vahdat, K. Yocum, K. Walsh, P. Mahadevan, D. Kostid, J. Chase, D. Becker // *ACM SIGOPS Operating Systems Review*. – 2002. – Т. 36. – №. SI. – с. 271-284.

4. OMNet++ Simulation Manual [Электронный ресурс] // OpenSim Ltd. – Электрон. дан. – 2015. Режим доступа: <https://omnetpp.org/doc/omnetpp/manual/>. Загл. с экрана. – (Дата обращения: 25.11.2016).

5. Introduction to Mininet [Электронный ресурс] // Mininet Project. – Электрон. дан. – 2016. Режим доступа: <https://github.com/mininet/mininet/wiki/Introduction-to-Mininet>. Загл. с экрана. – (Дата обращения: 25.11.2016).

6. NS-3 Documentation [Электронный ресурс] // NSNAM. – Электрон. дан. – 2015. Режим доступа: <https://www.nsnam.org/overview/what-is-ns-3>. Загл. с экрана. – (Дата обращения: 25.11.2016).

7. UNetLab Documentation [Электронный ресурс] // EVE-NG. – Электрон. дан. – 2016. Режим доступа: <http://www.unetlab.com/documentation/index.html>. Загл. с экрана. – (Дата обращения: 25.11.2016).

СТРУКТУРА И МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСТАНЦИОННОГО КУРСА ПО МАТЕМАТИКЕ ДЛЯ ШКОЛЬНИКОВ И АБИТУРИЕНТОВ

Руцкова И.Г.

Оренбургский государственный университет, г. Оренбург

Известно, что одним из факторов, способствующим успешному освоению математических дисциплин студентами в вузе, является наличие у них хорошей базовой подготовки [1, 2]. При этом наибольших успехов, как правило, достигают студенты, которые ранее обучались в классах с углубленным изучением математики, информатики и физики, и принимали активное участие в олимпиадах по данным предметам [3, 4].

Однако, к сожалению, не все школьники, проявляющие интерес к математике и информатике, имеют такую возможность. Для помощи таким школьникам (и другим категориям абитуриентов) в Центре довузовской подготовки «Абитуриент» Оренбургского государственного университета уже несколько лет функционируют дистанционные подготовительные курсы по подготовке к ЕГЭ по математике и вступительным экзаменам, проводимым университетом самостоятельно.

Для методической поддержки и контроля за ходом обучения на данных курсах используется электронный курс «Математика». Курс разработан сотрудниками кафедры прикладной математики и размещен на сайте Отдела информационных образовательных технологий ОГУ (<http://ito.osu.ru/>) в разделе «Система электронного обучения Moodle» (<https://moodle.osu.ru/>), в группе «Курсы довузовского образования» (смотрите рисунок 1).



Электронные курсы ОГУ в системе обучения moodle

В начало ► Курсы ► Курсы довузовского образования

Поиск курса: Применить

Категории курсов:

Курсы довузовского образования

Подготовка учащихся к ЕГЭ по физике, математике, информатике Преподаватель: Чакан Александр Афиногенович	Курс разработан Чака А.А., предназначен для учащихся 9-11 классов средних общеобразовательных школ. Форма обучения - очная/заочная
Экология 11 Преподаватель: Гривко Елена Васильевна	Курс разработан Гривко Е.В.
Экология 10 Преподаватель: Гривко Елена Васильевна	Курс разработан Гривко Е.В.
Математика Преподаватель: Руцкова Ирина Геннадьевна	Курс разработан Руцковой И.Г., предназначен для слушателей курсов по подготовке в вуз Центра довузовской подготовки "Абитуриент" ОГУ. Форма обучения - очная(дневная, вечерняя)/заочная/дистанционно-заочная.

Рисунок 1 – Курсы довузовского образования

Данный ресурс содержит все необходимые методические материалы, что позволяет слушателям:

1) рационально организовать работу по повторению, приведению в систему, закреплению и углублению теоретических и практических знаний, умений и навыков по математике необходимых как при решении заданий ЕГЭ и вступительных испытаний в вузы, так и для последующего обучения в вузе;

2) ознакомиться с разделами, алгоритмами и методами (углубление и расширение школьного курса математики) необходимыми для последующего успешного обучения в вузе;

3) проверить уровень усвоения знаний по математике и степень готовности к ЕГЭ и вступительным испытаниям в вузы (тесты, КР, задания для самостоятельной работы);

4) расширить общий кругозор (история математики, обзор ресурсов сети Интернет и др.), приобрести навыки решения нестандартных и олимпиадных задач.

Электронный курс «Математика» четко структурирован. В нем выделены *основная часть*: тематические главы, предназначенные для подготовки к ЕГЭ (или вступительным испытаниям) и последующему обучению в вузе, и *дополнительные материалы* справочного или содержательного характера. Изложение логически последовательное. Использование электронной системы обучения Moodle предоставляет возможность оперативного исправления или дополнения курса необходимыми материалами в зависимости от текущей ситуации: изменения содержания программ по математике общеобразовательных школ, лицеев, гимназий; кодификатора требований к уровню подготовки выпускников образовательных организаций для проведения единого государственного экзамена по математике, кодификатора элементов содержания по математике для составления контрольных измерительных материалов для проведения единого государственного экзамена (<http://fipi.ru/egge-i-gve-11/demoversii-specifikacii-kodifikatory>) или структуры и правил проведения ЕГЭ по математике.

Текущий вариант электронного курса «Математика» содержит 16 тематических глав: «Множества и функции. Свойства числовых множеств», «Степень числа. Тожественные преобразования алгебраических выражений», «Теория многочленов. Рациональные уравнения, неравенства и системы», «Проценты. Задачи на составление уравнений», «Рациональные уравнения и неравенства, содержащие знак абсолютной величины», «Иррациональные уравнения, неравенства и системы», «Тригонометрия», «Логарифм числа. Показательные и логарифмические уравнения, неравенства и системы», «Функции и графики (обобщающее повторение)», «Производная. Приложение производной к исследованию функций», «Первообразная. Неопределенный и определенный интегралы», «Теория вероятностей», «Планиметрия», «Стереометрия», «Векторная алгебра. Применение векторов к решению планиметрических и стереометрических задач». Указанная группировка материала способствует соблюдению непрерывности и логической последовательности изучения (повторения) самой математики и предоставляет

возможность отразить все основные типы заданий, предлагавшихся ранее на ЕГЭ и вступительных испытаниях вузы [5, 6, 7].

Тематические главы, как правило, содержат методические рекомендации по изучению (повторению); тесты проверки усвоения минимального уровня знаний, умений и навыков; примеры решений заданий ЕГЭ и вступительных испытаний в вузе (в порядке возрастания степени сложности); задания для самостоятельного решения (с ответами); дополнительные материалы. На рисунке 2 представлено содержание главы 3 «Теория многочленов. Рациональные уравнения, неравенства и системы».

3 Теория многочленов. Рациональные уравнения, неравенства и системы
Многочлены. Рациональные уравнения
 Методические рекомендации по повторению (изучению) темы "Многочлены. Рациональные уравнения"
 Примеры решений заданий ЕГЭ и вступительных испытаний в вузы по теме "Многочлены. Рациональные уравнения"
 Задания для самостоятельного решения по теме "Многочлены. Рациональные уравнения"
Рациональные неравенства
 Методические рекомендации по повторению (изучению) темы "Рациональные неравенства"
 Примеры решений заданий ЕГЭ и вступительных испытаний в вузы по теме "Рациональные неравенства"
 Задания для самостоятельного решения по теме "Рациональные неравенства"
Задачи с параметром (многочлены, рациональные уравнения и неравенства)
 Примеры решений заданий с параметром по теме "Многочлены. Рациональные уравнения и неравенства"
 Задания с параметрами для самостоятельного решения по теме "Многочлены. Рациональные уравнения и неравенства"
Дополнительная литература
 Курош А.Г. Алгебраические уравнения произвольных степеней
 Шафаревич И.Р. О решении уравнений высших степеней
 Кутужулова М. Квадратичная функция и ее применение к решению заданий с параметрами
 Батуткина Е. История становления методов решения уравнений степени n
 Виртуальная математика. Задачи с параметрами

Рисунок 2 – Содержание главы 3

Методические указания, примеры решений заданий ЕГЭ и вступительных испытаний вузы, задания для самостоятельного решения, как правило, оформлены в виде документов Word, которые открываются по требованию пользователя в отдельном окне. На рисунке 3 представлен фрагмент методических указаний по изучению темы «Тригонометрические уравнения».

Методические указания по изучению (повторению) темы «Тригонометрические уравнения»

Приступать к повторению темы "Тригонометрические уравнения" рекомендуется лишь после того, как Вы усвоили методику проведения тождественных преобразований и изучили свойства обратных тригонометрических функций.

Сначала нужно научиться решать простейшие тригонометрические уравнения: $\sin x = a$, $\cos x = a$, $\operatorname{tg} x = a$, $\operatorname{ctg} x = a$.

Необходимо **выучить все формулы**, в том числе, для частных случаев. Затем приступить к повторению наиболее распространенных методов, желательно в следующей последовательности: уравнения, сводящиеся к простейшим с помощью тождественных преобразований (в том числе, и метод введения вспомогательного аргумента), метод замены переменной (в том числе, и однородные уравнения), метод разложения.

Рисунок 3 – Методические указания по изучению темы «Тригонометрия»
 На рисунке 4 представлен фрагмент параграфа «Примеры решения заданий с параметром по тригонометрии».

Примеры решения заданий с параметром по тригонометрии

В данной главе мы рассмотрим только те задания, где не требуется использование производной.

Пример 1 При каких значениях параметра a уравнение $5\sin 3x - 6\cos x = a$ имеет решение?

Решение.

$$5\sin 3x - 6\cos 3x = a \Leftrightarrow \frac{5}{\sqrt{61}}\sin 3x - \frac{6}{\sqrt{61}}\cos 3x = \frac{a}{\sqrt{61}}.$$

Так как $\left(\frac{5}{\sqrt{61}}\right)^2 + \left(\frac{6}{\sqrt{61}}\right)^2 = 1$, то найдется φ :

$$\begin{cases} \cos \varphi = \frac{5}{\sqrt{61}}, \\ \sin \varphi = \frac{6}{\sqrt{61}}. \end{cases}$$

$$\cos \varphi \cdot \sin 3x - \sin \varphi \cdot \cos 3x = \frac{a}{\sqrt{61}} \Leftrightarrow \sin (3x - \varphi) = \frac{a}{\sqrt{61}}.$$

Следовательно, исходное уравнение может иметь решение тогда и только

Рисунок 4 – Фрагмент параграфа «Примеры решения заданий с параметром по тригонометрии»

Тесты, представленные в курсе, разработаны с помощью соответствующих инструментов системы электронного обучения Moodle, и предназначены для самоконтроля. Их основная цель - проверка усвоения основных понятий, фактов, формул. Результаты тестирования выводятся на экран автоматически, количество попыток - неограниченно. Основные виды используемых тестов: верно/неверно, краткий ответ, множественный выбор, на соответствие и другие. Примеры тестов представлены на рисунках 5 - 7.

Множество всех решений уравнения $|\cos x| = 1$ нельзя представить в виде:
 $x = \pi k$, $k \in \mathbb{Z}$.

Выберите один ответ:

☐ Верно

☐ Неверно

Рисунок 5 – Тест вида верно/неверно.

Упростите выражение

$$\sin 7x \cos 2x + \cos 7x \sin 2x + \sin(180^\circ - 9x)$$

и запишите получившийся ответ без пробелов.

Ответ:

Установите соответствие между левой и правой

$\sin(540^\circ - x) =$	Выберите...
$\sin(180^\circ + x) =$	Выберите...
$\sin(x + 270^\circ) =$	Выберите...
$\sin(450^\circ - x) =$	Выберите...

Рисунок 6 – Тест с вводом ответа

Рисунок 7 – Тест на

соответствие

Дополнительные материалы это - либо материалы справочно-информационного (список рекомендуемой литературы, справочная литература, ссылки на полезные ресурсы сети Интернет, информация об олимпиадах и конкурсах и прочее) или содержательного характера (алгоритмы и методы решения нестандартных и олимпиадных задач, сборники олимпиадных задач и иное). В качестве примеров, на рисунке 8 представлен фрагмент блока, где имеется информация об ОГУ (правила приема, олимпиады для старшеклассников и прочее), а на рисунке 9 представлен фрагмент блока «Материалы для подготовки к олимпиадам и конкурсам».

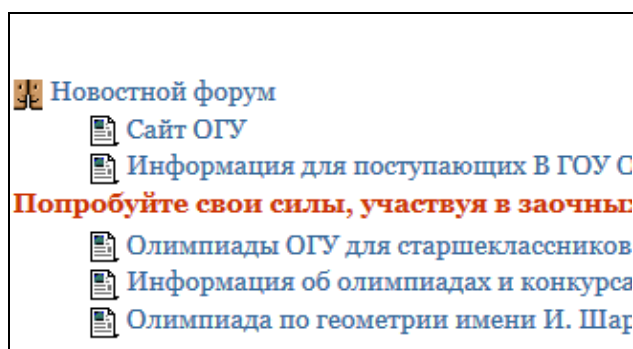


Рисунок 8 – Информация об ОГУ.

Рисунок 9 – Подготовка к олимпиадам

Для проверки уровня усвоения представленного в курсе материала слушателями дистанционных подготовительных курсов используются домашние контрольные работы. Тематика контрольных работ, их количество и график выполнения для каждого слушателя определяются индивидуально, в зависимости от выбранной длительности обучения (одногодичное или двухгодичное), первоначального уровня подготовленности и момента начала обучения. Как правило, в течение учебного года обучающийся выполняет восемь контрольных работ. Каждая из контрольных работ содержит 20 – 40 заданий различной степени сложности, включая как задания уровня В и С

единого государственного по математике, так и нестандартные задания олимпиадного характера. Выполненные задания контрольной работы слушатель отправляет преподавателю на проверку либо по электронной почте, либо используя соответствующие ресурсы электронного курса. Преподаватель, в своей рецензии, не только отмечает допущенные ошибки, но и дает рекомендации по их исправлению или подсказки по выбору алгоритма решения задач. В случае необходимости, работа представляется слушателем курсов на вторичную проверку.

На данный момент доступ к курсу ограничен и осуществляется по логину и паролю, который выдается после заключения с соответствующего договора с Центром «Абитуриент». Для зарегистрированных пользователей доступ к ресурсу возможен в любое удобное для них время, с любого устройства, подключенного к сети Интернет.

В заключение отметим, что электронный курс «Математика» активно используется в практической работе со слушателями центра довузовской подготовки «Абитуриент» с 2012 года. В том числе, он был использован и при работе с молодыми женщинами в возрасте до 23 лет, имеющими одного и более детей. Обучение которых осуществлялось в 2013/14 и 2014/15 учебных годах, согласно постановлению Правительства Российской Федерации от 31.08.2013 года № 756 «О проведении в 2013 - 2015 годах эксперимента по обучению молодых женщин в возрасте до 23 лет, имеющих одного и более детей, на подготовительных отделениях федеральных государственных образовательных организаций высшего образования» (<https://rg.ru/2013/09/06/experiment-dok.html>).

Опыт использования курса показывает, что наибольших успехов достигают мотивированные слушатели, изучающие все предлагаемые ресурсы, соблюдающие график учебного процесса, выполняющие указания преподавателя и прислушивающиеся к его замечаниям и рекомендациям.

Список литературы

1. Руцкова, И.Г. Школьный курс математики с точки зрения вузовского преподавателя /И.Г. Руцкова // Вестник МаГУ: Периодический научный журнал. Вып.5. Естественные науки. - Магнитогорск: МаГУ, 2004. - С.67-71. ISBN 5-86781-333-9
2. Руцкова, И.Г. Основные направления работы кафедры прикладной математики в сфере довузовского образования /И.Г.Руцкова //Вызовы XXI века и образование: материалы всероссийской научно-практической конференции. Секция 8. - Оренбург, 2006. – С.173 -178. ISBN -5-7410-0650-7
3. Руцкова, И.Г. Значение учебно-исследовательской деятельности учащихся в системе профильного обучения математиков и программистов /И.Г. Руцкова //Математика. Информационные технологии. Образование. Сборник научных трудов. - Оренбург: ОГУ, 2008. – С. 268 – 271. ISBN 978-5-7410-0824-93

4. Руцкова, И.Г. Структура, содержание и методическое обеспечение курса математики в лицее-интернате для одаренных детей /И.Г. Руцкова // Развитие университетского комплекса как фактор повышения инновационного и образовательного потенциала региона: материалы всероссийской научно-практической конференции. Секция 13. – Оренбург: ИПК ОГУ, 2007. – С. 307 – 313. ISBN 978-5-7410-0705-1

5. Руцкова, И.Г. Цели и задачи подготовительных курсов по математике на современном этапе /И.Г. Руцкова // Математика. Информационные технологии. Образование: материалы региональной научно-практической конференции в двух частях. Часть 2. - Оренбург: ГОУ ОГУ, 2006. С. 404 -406. ISBN 5-7410-022-6 (Часть 2)

6. Руцкова, И.Г. Подготовительные курсы в системе непрерывного математического образования /И.Г.Руцкова // Проблемы качества образования в современном обществе: сборник статей VI Международной научно-практической конференции. – Пенза: Приволжский Дом знаний, 2010 – С. 192 – 194. ISBN 978-5-8356-1049-5

7. Руцкова, И.Г. Пособие по математике для поступающих в вузы /И.Г. Руцкова. – Оренбург: ОГУ, 2010. – 300 с. Оренбург: ОГУ, 2010. – 300 с. ISBN 978-5-7410-1037-2

ПРИМЕНЕНИЕ ПРИКЛАДНЫХ ПРОГРАММ УЧЕБНОГО НАЗНАЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНЦИЙ БУДУЩЕГО БАКАЛАВРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Рычкова А.А., Гайфулина Д.А., Хакимова Э.Р.
ФГБОУ ВО «Оренбургский государственный университет»,
г. Оренбург**

В соответствии с ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность для формирования профессиональных компетенций (ПК-1, ПК-2) необходимо расширение учебно-методического и материально-технического обеспечений учебного процесса [1].

В процессе изучения дисциплины базового цикла «Криптографические методы защиты информации» на практических и лабораторных занятиях кроме изучения готовых криптографических программных средств будущие бакалавры выполняют исследование и разработку собственных программ.

В статье рассматривается опыт разработки и использования прикладной программы учебного назначения в ходе организации лабораторных работ по разделу «Криптографические протоколы».

Прикладная программа «Исследование криптографических методов формирования электронной подписи» предназначена для проверки подлинности отправляемых сообщений пользователями на основе электронной подписи [2]. Основными направлениями работы являются нахождение хеш-функции от отправляемого сообщения, вычисление электронной цифровой подписи отправителя и получателя на основе различных алгоритмах шифрования, а так же подтверждение или отклонение подлинности сообщения. В основе программы лежат алгоритмы формирования электронной подписи на основе таких алгоритмов шифрования как RSA, El Gamal, алгоритмы Диффи-Хеллмана и Фиата-Шамира, а та же алгоритмы вычисления хеш-функций и основы работы в среде «клиент-сервер». В программе предусмотрено наличие:

- теоретического материала по используемым алгоритмам формирования электронной подписи;
- графического представления происходящего процесса передачи сообщения и всех математических преобразований, происходящих в ходе формирования и передачи электронной подписи, а так же ее проверки;
- последовательность этапов формирования электронной подписи.

Список представленных алгоритмов формирования электронной подписи можно увидеть на левой панели программы или во всплывающем меню перейдя по вкладке «Режимы работы». В данном всплывающем меню имеются теоритические сведения об алгоритмах, а так же можно перейти к реализации, выбрав соответствующий тип алгоритма формирования электронной подписи. Главное окно программы показано на рисунке 1.

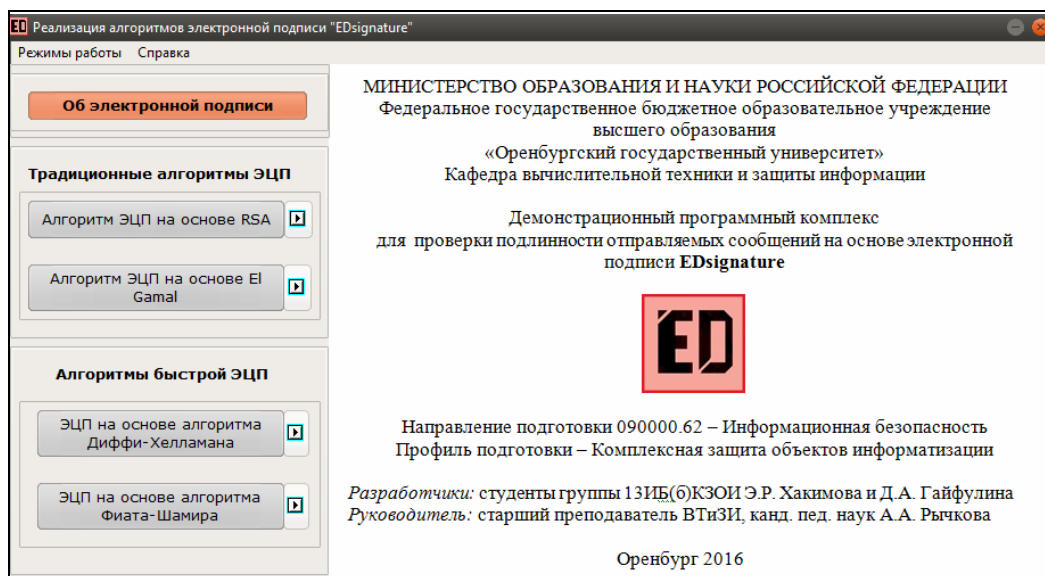


Рисунок 1 – Главное окно программы «EDsignature»

Для выбора определенного алгоритма формирования электронной подписи следует нажать на кнопку на левой панели или на соответствующую строку во всплывающем меню.

При нажатии на кнопку любого алгоритма формирования электронной подписи появляется окно программы, содержащее теорию по данному алгоритму формирования. Данное окно программы для режима формирования электронной подписи на основе алгоритма RSA представлено на рисунке 2.

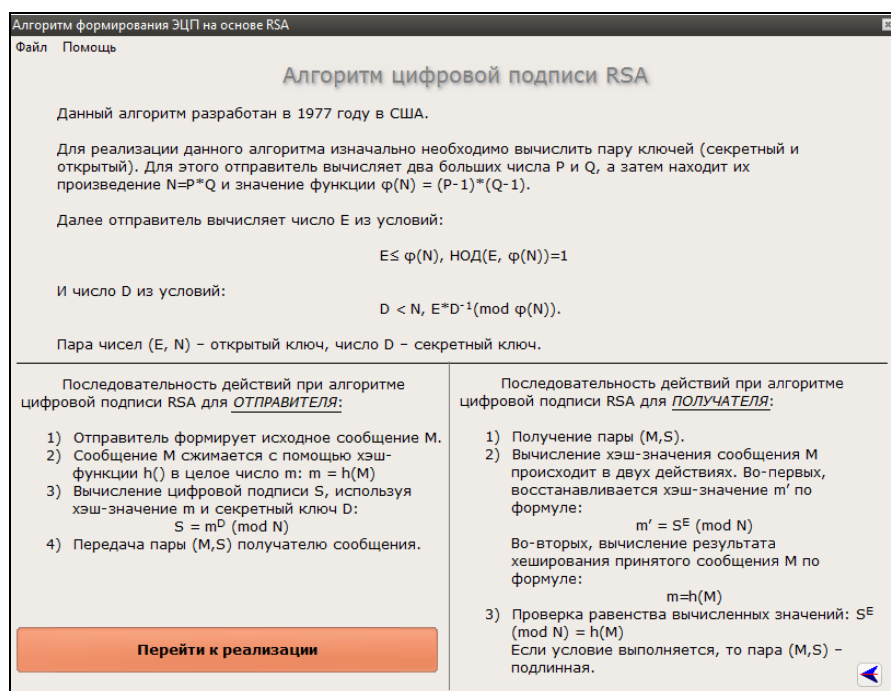


Рисунок 2 – Окно программы «Алгоритм формирования электронной подписи на основе RSA»

Исходными данными для программы являются передаваемое сообщение и криптографический ключ (элементы для формирования ключа).

Для начала работы с программным средством необходимо изначально установить соединение между клиентом и сервером для последующей передачи сообщений и формирования электронной подписи.

Для использования в учебном процессе в программе представлена реализация следующих алгоритмов:

ЭЦП на основе алгоритма RSA. Формирование ключей производится на основе введенных параметров p, q которые должны быть простыми. Пара чисел (e, n) – открытый ключ, число d – секретный ключ. Формирование ЭЦП отправляемого сообщения основано на применении асимметричного метода RSA, где в качестве ключей используются параметры $\{e, n\}$ – являющиеся закрытыми ключами шифрования. На выходе получают ЭЦП, представленную в виде значения чисел $\{M, S\}$, которые передаются получателю. Клиент производит проверку ЭЦП полученного сообщения на основе асимметричного метода RSA, где в качестве ключей используются параметры $\{d, n\}$ – являющиеся открытыми ключами шифрования, переданными клиенту сервером. На выходе получают строку расшифрованного хэша сообщения, который впоследствии сравнивается с вычисляемым хэшем полученного сообщения. По результатам сравнения делается вывод о подлинности отправителя.

ЭЦП на основе алгоритма El Gamal. Для реализации данного алгоритма изначально необходимо вычислить пару ключей с использованием больших простых целых чисел P, G и X . Число Y – закрытый ключ, X – открытый ключ. Сервер производит формирование ЭЦП отправляемого сообщения на основе асимметричного метода Эль Гамаль, с использованием в качестве входных параметров отправляемого сообщения и ключа Y . На выходе получают ЭЦП, представленную в виде значения чисел $\{a, b\}$, которые передаются получателю. Клиент производит проверку ЭЦП полученного сообщения на основе асимметричного метода Эль Гамаль, где в качестве ключей используются параметр X . На выходе получают строку расшифрованного хэша сообщения, который впоследствии сравнивается с вычисляемым хэшем полученного сообщения. По результатам сравнения делается вывод о подлинности отправителя.

Быстрая ЭЦП на основе алгоритма Диффи-Хеллмана. Изначально происходит генерация ключа. Пользователь выбирает случайный секретный ключ x и вычисляет открытый ключ y с использованием генератора абелевой группы G . Сервер производит формирование быстрой ЭЦП отправляемого сообщения на основе алгоритма Диффи-Хеллмана, входными параметрами является отправляемое сообщение и ключ x . На выходе получают быструю ЭЦП, представленную в виде значения чисел $\{M, S\}$, которые передаются получателю. Клиент производит проверку ЭЦП полученного сообщения на основе метода Диффи-Хеллмана, где в качестве ключей используются параметр

у. На выходе по результатам сравнения принимается решение о подлинности отправителя.

Быстрая ЭЦП на основе алгоритма Фиата-Шамира. До начала создания подписи происходит генерация ключей. В качестве секретного ключа выбирается последовательность $s=(s_1, \dots, s_k)$, состоящий из случайных чисел s_i . На основе закрытого ключа считается открытый ключ: формируется последовательность $v = (v_1, \dots, v_k)$. Далее сервер производит формирование быстрой ЭЦП отправляемого сообщения на основе алгоритма Фиата-Шамира, входными параметрами является отправляемое сообщение и ключевая последовательность s . На выходе получают быструю ЭЦП, представленную в виде значения чисел $\{M, S\}$, которые передаются получателю. Клиент производит проверку ЭЦП полученного сообщения на основе метода Фиата-Шамира, где в качестве ключей используется открытая последовательность v . На выходе по результатам сравнения принимается решение о подлинности отправителя [3-7].

При выборе любого из предложенных алгоритмов результатом выполнения программы будет являться вывод сообщения о подтверждении или отклонении подлинности отправителя. На рисунке 3 представлено окно программы при подтверждении подлинности отправителя.

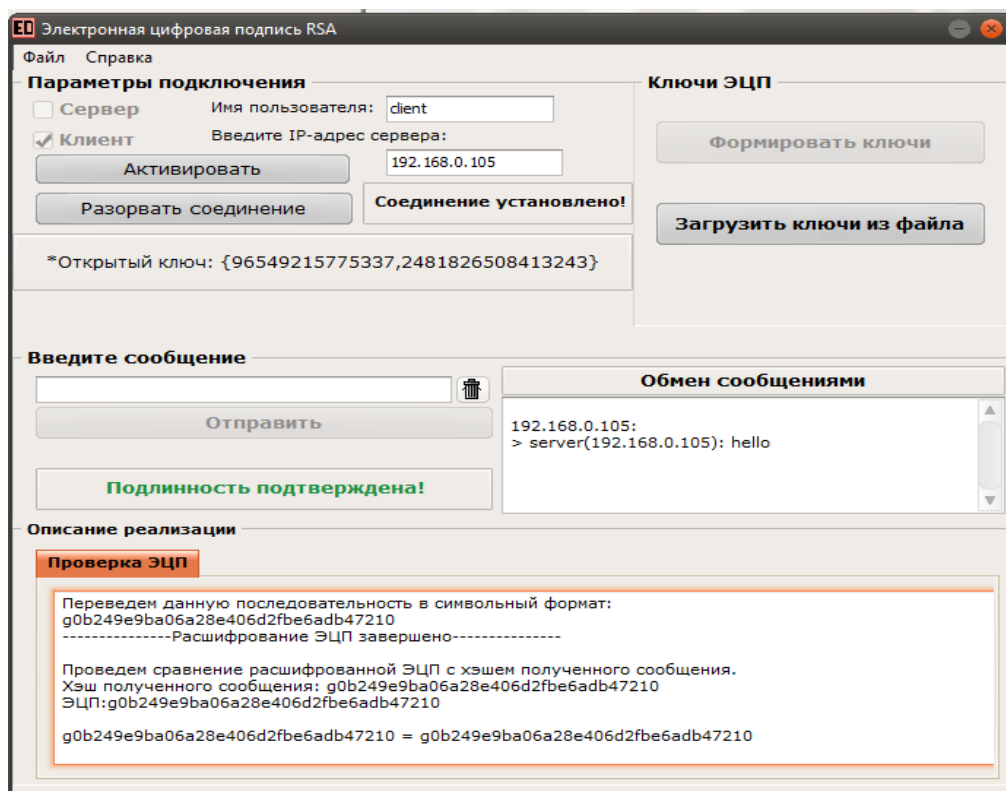


Рисунок 3 – Подтверждение подлинности отправителя сообщения

В результате выполнения лабораторной работы с помощью разработанной прикладной программы «Исследование криптографических

методов формирования электронной подписи» будущие бакалавры по информационной безопасности самостоятельно изучают существующие алгоритмы электронной подписи, проводят сравнительный анализ быстродействия выбранных методов, делают выводы, готовят отчет о проделанной работе. Активное вовлечение студентов в процесс разработки авторских прикладных программ учебного назначения, полученные в ходе выполнения лабораторных работ с применением таких средств, знания и умения способствуют формированию необходимых профессиональных компетенций.

Список литературы

1. Об утверждении федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата): Приказ от 1 декабря 2016 г. № 1515 // Зарегистрирован в Минюсте России 20.12.2016 № 44821/
2. Гайфулина, Д.А. Исследование криптографических методов формирования электронной подписи : прикладная программа / Д.А. Гайфулина, Э.Р. Хакимова, А.А. Рычкова. – Оренбург.: УФЭР. – 2016. - №1332.
3. Ветров, Ю.В. Криптографические методы защиты информации в телекоммуникационных системах: учеб. пособие / Ю.В. Ветров, С.Б. Макаров - Спб.: Изд-во Политехн. ун-та, 2010. - 174 с. - ISBN 978-5-7422-3025-0.
4. Молдовян Н.А. Теоретический минимум и алгоритмы цифровой подписи. / Н.А. Молдовян - СПб.: БХВ-Петербург, 2010. - 304 с. - ISBN 978-5-9775-0585-7.
5. Рычкова, А.А. Разработка и применение прикладных программ учебного назначения для организации самостоятельной работы студентов / А.А. Рычкова : сборник научных статей Всероссийской научно-методической конференции «Университетский комплекс как региональный центр образования, науки и культуры»; Оренбургский гос. ун-т.. – Оренбург: ООО ИПК «Университет», 2014. – С. 3082-3088.
6. Рычкова, А.А. Основы криптографии : мультимедийное учебное пособие / Т.Н. Шалкина, В.В. Запорожко, А.А. Рычкова. - М.: ОФАП. - 2008. - №10602.
7. Тимошин П.А, Перспективы развития и использования систем электронной цифровой подписи / П.А. Тимошин - Прикладная информатика, вып. №2(8) - М.:ЛитРес, 2014. - С.12-26. - ISBN 978-5-4573-8888-8.

ОСОБЕННОСТИ ПОДГОТОВКИ БАКАЛАВРОВ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Сидоров А.В.

**Бузулукский гуманитарно-технологический институт (филиал) ОГУ,
г. Бузулук**

Программные продукты, с которыми приходится работать специалистам, связанным с информационными технологиями периодически меняются. Если раньше такая замена происходила только при значительном изменении требований к самой программе, то в настоящее время изменения в основном касаются интерфейса программного продукта.

При этом изменение версий многих программных продуктов происходит раз в год или даже чаще.

Подготовка специалистов в области информационных технологий должна обеспечивать актуальность получаемых ими знаний. Студенты должны иметь опыт работы с последними версиями программных продуктов, что достаточно сложно обеспечить на практике.

При обучении должны применяться лицензионные программные продукты, стоимость которых достаточно высока. Многие фирмы, выпускающие программные средства, позволяют их использовать в учебных заведениях бесплатно или за незначительную плату. В качестве примера можно привести программные продукты фирмы Autodesk, возможность бесплатного использования которых в образовательном процессе открыта для всех учебных заведений России, в том числе и для домашнего использования студентами. Законодательно в настоящее время организация несет ответственность за незаконное использование нелицензионного программного обеспечения.

По этой причине, ежегодно (или чаще, в зависимости от времени обновления версий программных продуктов) организация должна приобретать лицензии на обновленные версии продуктов.

Вместе с обновлением версий программных средств, необходимо обновление и всей методической документации, сопровождающей данные программные продукты.

Учитывая, что при подготовке бакалавров значительное время отводится на самостоятельное освоение дисциплины, необходимо обеспечить студентов качественными учебными пособиями, учитывающими данные изменения программных продуктов. При подготовке учебно-методической документации значительная доля времени в работе преподавателя будет отводиться не совершенствованию учебно-методического материала, а изменению его содержания, связанного с изменением интерфейса программного продукта.

Подготовка учебно-методической документации является процессом творческим и требует значительных временных затрат. Наличие требований к учебно-методическим комплексам в системе высшего образования приводит к тому, что преподаваемый материал приходится оформлять в сжатые сроки, что может приводить либо к подаче студентам устаревшего материала, либо

снижению качества документирования преподаваемого курса [1]. Последнее является существенным недостатком, так как значительная часть времени студентов приходится на самостоятельное изучение преподаваемого курса (или самостоятельное изучение некоторых вопросов либо разделов курса).

Все указанные проблемы являются решаемыми, несмотря на значительные затраты времени и средств на их устранение.

Другая проблема появляется после окончания учебного заведения.

С одной стороны, знания, получаемые студентами в учебном заведении должны быть актуальными, с другой – должна присутствовать возможность применения получаемых знаний на практике.

Процесс обучения бакалавров информационным технологиям обладает следующей особенностью. Даже если студенты получают актуальный материал в начале обучения, к моменту окончания учебного заведения данный материал может безнадежно устареть. Программные продукты, которые студенты изучали на первом курсе, или же ученики в старших классах средней школы, к концу обучения уже могут быть заменены более актуальными, свежими версиями, то есть другими словами, – устареть.

Еще одной особенностью подготовки бакалавров в области информационных технологий является то, что подготовка специалистов должна осуществляться с применением самых современных программных продуктов. В тоже время в своей дальнейшее работе специалисты могут столкнуться со старыми версиями программ, интерфейс которых претерпел значительные изменения. Применять полученные в учебном заведении знания в этом случае будет достаточно проблематично. Кроме того, работая за ограниченным набором программных продуктов, специалист теряет полученные разнообразные знания в области информационных технологий, превращается в специалиста ограниченной области знаний.

Еще одной проблемой является то, что старые и новые версии программ могут использовать различные несовместимые между собой форматы хранения данных. И, необязательно, что более новая программа обладает возможностью чтения и редактирования устаревших форматов. Во многих случаях форматы хранения данных претерпевают значительные изменения в связи с их низкой эффективностью и обеспечить совместимость устаревших форматов с новыми не представляется возможным. В связи с этим, перед бакалаврами встает необходимость изучения фактически всех форматов хранения данных, что представляется практически невозможной задачей.

Если рассматривать объем информации, накопленный в области информационных технологий за последние годы, то можно увидеть, что он давно превысил некие допустимые пределы осмысления и анализа для одного человека [2].

Невозможно выучить все известные на данный момент языки программирования, разобраться со всеми существующими средами программирования.

Изменение интерфейса программных продуктов, изменение требований к самим продуктам приводит к изменениям в соответствующих языках программирования.

Появление некоторых новых языков приводит к тому, что некоторые из уже известных языков перестают быть актуальными, теряют свою привлекательность, перестают использоваться.

Поэтому еще одной особенностью подготовки современного бакалавра в области информационных технологий является то, что заранее неизвестно, будет ли востребован тот язык программирования, который изучается в курсе информатики к моменту трудоустройства будущего выпускника.

Стремительный темп изменений, происходящих в области информационных технологий, требует столь же быстрых изменений в области получения знаний, что практически не является возможным.

В связи с этим особое внимание следует уделить процессу самоподготовки, эффективно организованному процессу самообразования.

Кроме того, необходимо регулярно проводить исследования в области рынка труда и вносить коррективы в последовательность и объем самоподготовки по тому или иному направлению подготовки. Такая организация деятельности может позволить обладать достаточным уровнем знаний в узкой области и в тоже время достаточной гибкостью, что позволит быстро переориентироваться на другие технологии в случае смены вида деятельности или устаревания используемых информационных продуктов. На рынке труда присутствуют только «сырые», т.е. не владеющие технологиями данного предприятия специалисты. Для того чтобы такой специалист стал полноценным нужны многие месяцы работы на данном предприятии.

Специалисты, проработавшие на конкретном предприятии несколько лет, накапливают огромный опыт. Зачастую они владеют при этом вопросами, выходящими за рамки их непосредственных обязанностей, но чрезвычайно важными для предприятия. Они часто становятся уникальными носителями технологии работы предприятия, однако, в этой части они не всегда достаточно востребованы и оценены, и, поэтому, вынуждены преднамеренно ограничивать область своей деятельности (насколько это возможно) лишь теми вопросами, которыми им заниматься привычно, удобно и за которые они получают заработную плату.

Список литературы

1. Румянцев, С. А. Особенности подготовки специалистов исходя из актуальных данных на рынке труда с использованием времясберегающих психологических технологий [Электронный ресурс] / С. А. Румянцев. // Труды международного симпозиума «Надежность и качество», Т. 2, 2012 г., Пенза / Пензенский гос. ун-т – Электрон. дан. – Пенза, 2012. – С. 441-444.

2. Алахвердов, А. А. Кадровая политика в ИТ подразделениях предприятий и организаций [Электронный ресурс] / А. А. Алахвердов. – Режим доступа: http://www.cfin.ru/management/people/dev_val/it_personnel.shtml (дата обращения: 19.12.2016).

О ПРИМЕНЕНИИ ТЕОРИИ ВЫЧЕТОВ ПРИ РЕШЕНИИ ДИАФАНТОВЫХ УРАВНЕНИЙ

Сикорская Г.А., Косилов Е.А.

Оренбургский государственный университет, г. Оренбург

«Достопочтеннейший Дионисий, зная, что ты ревностно хочешь научиться решению задач, касающихся чисел, я попытался изложить природу их и могущество, начиная с тех оснований, на которых покоится эта наука. Может быть, этот предмет покажется тебе затруднительным, поскольку ты еще с ним незнаком, а начинающие не склонны надеяться на успех. Но он станет тебе удобопонятным благодаря твоему усердию и моим пояснениям, ибо страстная любовь к науке помогает быстро воспринять учение». Таким посвящением открывается «Арифметика» Диофанта Александрийского.

В книге «Арифметика» Диофант (3 век) обобщил накопленный до него опыт решения неопределенных алгебраических уравнений в целых или рациональных числах. Решение в целых числах уравнений с целыми коэффициентами более чем с одним переменным представляет собой одну из интереснейших проблем теории чисел. Некоторые виды таких уравнений были рассмотрены еще до Диофанта знаменитым математиком древности Пифагором (6 в. до н.э.). В средневековой Европе работы Диофанта о решении уравнений в целых числах получили широкое распространение и развитие. Впоследствии, в память о мыслителе, вложившем в исследование неопределенных алгебраических уравнений в целых числах большой вклад, эти уравнения стали называть диофантовыми. Исследованием диофантовых уравнений занимались такие классики математики как П. Ферма (1601-1655), Л. Эйлер (1707- 1783), Ж.Л. Лагранж (1736-1813), К.Ф. Гаусс (1777-1855), П.Л. Чебышев (1821-1894). И в настоящее время многие математики современности работают в области исследования диофантовых уравнений.

И так, диофантовыми уравнениями называют алгебраические уравнения или системы алгебраических уравнений с целыми коэффициентами, для которых надо найти целые или рациональные решения. Диофантовы уравнения имеют, как правило, много решений, поэтому их называют неопределенными уравнениями.

В настоящее время разработано множество методов решения диофантовых уравнений, основанных на свойствах делимости, на разложении на множители, на различных подстановках, на сравнении и т.д. Рассмотрим решение диофантовых уравнений основанное на теории вычетов.

Построим кольцо классов вычетов по $\text{mod } n$. Пусть $Z = \{0; \pm 1; \pm 2; \pm 3; \dots\}$, $N = \{1, 2, 3, \dots\}$

Фиксируем $n \geq 2, n \in N$. Определим остатки от деления целых чисел, например, на число три. Получим три класса вычетов: $\overline{0}$ – класс нуля, $\overline{1}$ – класс единицы, $\overline{2}$ – класс двойки.

Если число принадлежит одному из этих классов, то будем обозначать принадлежность его к этому классу чертой сверху.

Например, $\overline{2} = \overline{-4}$. Эти числа отстоят друг от друга на число, кратное трем: $2 - (-4) = 6 : 3$.

Введем операции над классами

$$1) \quad \overline{a} + \overline{b} = \overline{a + b}$$

$$2) \quad \overline{a} - \overline{b} = \overline{a - b}$$

$$3) \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}, n \geq 2, n \in N$$

Очевидно, что $\overline{a^n} = \overline{a^n}$ (это многократно примененное третье правило).

Пусть $n \in N, n \geq 2$.

Построим множество класса по mod n

$$Z_n = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$$

$$a, b \in Z, \overline{a} = \overline{b} \Leftrightarrow a - b = kn.$$

Теперь перейдем непосредственно к решению диофантовых уравнений.

Задача 1. Доказать, что уравнение $x^2 + y^2 = 2003$ не имеет решения в целых числах.

Решение. «Работаем» по mod4:

x	x ²
0	0
1	1
2	0
3	1

$$\text{Следовательно, } x^2 + y^2 = 2003, \overline{x^2} + \overline{y^2} = \overline{3}$$

Рассмотрим всевозможные варианты:

$$\overline{0} + \overline{0} \neq \overline{3}, \overline{0} + \overline{1} \neq \overline{3}, \overline{1} + \overline{1} \neq \overline{3}$$

Таким образом, уравнение $x^2 + y^2 = 2003$ не имеет решений в целых числах.

Задача 2. Доказать, что уравнение $12x + 5 = y^2$ не имеет решения в целых числах.

Решение. «Работаем» по mod3:

a	a ²
0	0
1	1
2	1

$$12x + 5 = y^2$$

$$\bar{0} + \bar{2} \equiv \bar{y}$$

Класса $\bar{2}$ нет. Получили противоречие.

Ответ: уравнение $12x + 5 = y^2$ не имеет решений в целых числах.

Задача 3. Доказать, что уравнение $12x^2 - 7y^2 = 9$ не имеет решения в целых числах.

Решение. «Работаем» по mod 5:

$$12x^2 - 7y^2 = 9$$

$$\bar{0} - \overline{2y^2} = \bar{4}, \quad \overline{2y^2} = -\bar{4} = \bar{1}$$

y	y ²
0	0
1	1
2	4
-2	4
-1	1

И так, $\overline{2y^2} = \bar{1}$

$$\bar{2} \cdot \bar{0} = \bar{0} \neq \bar{1}, \quad \bar{2} \cdot \bar{1} = \bar{2} \neq \bar{1}, \quad \bar{2} \cdot \bar{4} = \bar{8} = \bar{3} \neq \bar{1}$$

Равенство по mod 5 не возможно, что и требовалось доказать.

Просмотрев уже только эти задачи, можем с уверенностью утверждать, об эффективности поиска решений, или, соответственно, доказательства отсутствия таковых, основанное на использовании теории вычетов. Единственная сложность решения диофантовых уравнений через вычеты это вопрос о выборе mod. Однако вопрос теряет свою остроту в процессе многократного решения подобных задач, то есть правильность выбора модуля нарабатывается с опытом. Теперь более сложные задачи:

Задача 4. Решить в натуральных числах уравнение $3^x + 55 = y^2$,

($x, y \in \mathbb{N}$)

Решение. «Работаем» по mod 4:

y	y ²
0	0
1	1
2	0
3	1

$$3^x + 55 = y^2$$

$$\overline{(-1)^x} + \overline{-1} = \bar{1} \text{ (или } \bar{0})$$

$$\overline{(-1)^x} = \bar{1} \text{ (или } \bar{2})$$

$\overline{(-1)^x} = \bar{1}$ — верно, если x — четный.

$\overline{(-1)^x} = \bar{2}$ — не может быть ни при каком x

$$55 = y^2 - 3^{2x} \Rightarrow 55 = (y - 3^x)(y + 3^x)$$

Проанализируем равенство $55 = (y - 3^x)(y + 3^x)$.

Правая часть равенства есть произведение двух натуральных чисел, причем первый сомножитель меньше второго. Воспользуемся основной теоремой алгебры: любое натуральное число раскладывается в произведение простых единственным образом с точностью до порядка сомножителей. Следовательно, разложить 55 на произведение натуральных можно, либо $1 \cdot 55$, либо $55 \cdot 1$, больше вариантов нет. Таким образом, приходим к совокупности:

$$\begin{cases} y - 3^{x_1} = 1 \\ y + 3^{x_1} = 55 \end{cases} \quad \begin{cases} y - 3^{x_2} = 5 \\ y + 3^{x_2} = 11 \end{cases}$$

Решим каждую из систем.

$$1) \begin{cases} y - 3^{x_1} = 1 \\ y + 3^{x_1} = 55 \end{cases}$$

$$2y = 56 \Rightarrow y = 28$$

$$28 - 3^{x_1} = 1$$

$$-3^{x_1} = -28 + 1$$

$$3^{x_1} = 27$$

$$3^{x_1} = 3^3 \Rightarrow x_1 = 3$$

$$\text{Тогда } x = 6$$

$$2) 2y = 16 \Rightarrow y = 8$$

$$8 - 3^{x_2} = 5$$

$$3^{x_2} = 8 - 5$$

$$3^{x_2} = 3$$

$$3^{x_2} = 3^1 \Rightarrow x_2 = 1$$

$$\text{Тогда } x = 2$$

Ответ: (16; 24), (2; 8).

Задача 5. Решить в натуральных числах уравнение $3^x + 7 = 2^y$

$(x, y \in \mathbb{N})$

Решение. mod3:

$$3^x + 7 = 2^y$$

$$\bar{0} + \bar{1} = \overline{-1}^y; \bar{1} = \overline{(-1)}^y$$

$$\Rightarrow y - \text{четное}$$

$$y = 2y_1$$

$$3^x + 7 = 4^{y_1}$$

mod3:

$$3^x + 7 = 4^{y_1}$$

$$\overline{(-1)}^x + \overline{-1} = \bar{0}; \bar{1} = \overline{(-1)}^x$$

$$\Rightarrow x - \text{четное}$$

$$x = 2x_1$$

Подставим в исходное $x = 2x_1$ и $y = 2y_1$,

$$3^{2x_1} + 7 = 2^{2y_1}.$$

$$7 = 2^{2y_1} - 3^{2x_1}.$$

$$7 = (2^{y_1} - 3^{x_1})(2^{y_1} + 3^{x_1})$$

Раскладываем 7 на множители 1 и 7, так как это число – простое, следовательно

$$\begin{cases} 2^{y_1} - 3^{x_1} = 1 \\ 2^{y_1} + 3^{x_1} = 7 \end{cases}$$

$$2 \cdot 2^{y_1} = 8 \Rightarrow 2^{y_1} = 4 \Rightarrow 2^{y_1} = 2^2 \Rightarrow y_1 = 2$$

$$2^2 - 3^{x_1} = 1 \Rightarrow 4 - 3^{x_1} = 1 \Rightarrow 3^{x_1} = 3 \Rightarrow x_1 = 1$$

$$x_1 = 1 \Rightarrow x = 2$$

$$y_1 = 2 \Rightarrow y = 4$$

Ответ: (2;4).

Предлагаем читателю «поработать» с диафантовыми уравнениями, используя теорию вычетов.

Задача 6. Решите в целых числах уравнение $2x^2 - 5y^2 = z^2$.

Задача 7. Решите в целых числах уравнение $4x^3 - 2y^3 - z^3 = 0$.

Задача 8. Докажите, что уравнение $3x^2 - y^2 = 5$ не имеет решений в целых числах.

Задача 9. Докажите, что уравнение $8x^4 + 4y^4 + 2z^4 = t^4$ не имеет решений в натуральных числах.

Задача 10. Докажите, что уравнение $x^2 + y^2 + z^2 = 2xyz$ не имеет решений в натуральных числах.

Список литературы

1. Борович З.И., Шафаревич И.Р. Теория чисел. - М.: Наука, 1972.
2. Виноградов И.М. Основы теории чисел. - М.: Наука, 1972.
3. Галкин Е. Задачи с целыми числами. - М.: «Математика», 1999 - 2000.
4. Малинин В. Решение уравнений в натуральных и целых числах. - М.: «Математика», 2001, №№ 21 - 22.
5. Молдаванский Д.И. Целые числа. Основы теории делимости. - Иваново: изд-во Ивановского областного института повышения квалификации и переподготовки педагогических кадров, 2001.
6. Хассе Г. Лекции по теории чисел. - М.: ИЛ, 1953.

СИСТЕМАТИЗАЦИЯ КАК СРЕДСТВО ПОВЫШЕНИЯ КАЧЕСТВА МАТЕМАТИЧЕСКОЙ ПОДГОТОВКИ СТУДЕНТА

Смирнова Е.Н., Томина И.П.
ФГБОУ ВО «Оренбургский государственный университет»,
г. Оренбург

В настоящее время в современном обществе происходят значительные социальные и экономические преобразования, общество переходит к демократическому и правовому государству, к рыночной экономике, страна входит в мировую экономическую систему и мировое образовательное пространство, компьютеризация занимает основное место во всех сферах производства, финансов, торговли, снижается административное давление на образовательные учреждения. Образование становится общенациональным преимуществом России.

Образовательный процесс приобретает гуманистическое направление, педагогическая практика приобретает новые технологии обучения, которые способствуют реализовать новую парадигму воспитания и образования. Научно-технический прогресс и увеличивающийся информационный поток во многих сферах человеческой деятельности являются главными в социальной и экономической жизни общества, которое стремительно развивается. Это развитие, в свою очередь, влечет необходимость переработки новой информации и оперативности в управлении, повышая роль быстрого обучения, систематизированных знаний, переучивания с помощью систематизации учебной деятельности, из этого следует актуальность создания новых методов и интенсивных форм обучения в высшей школе.

Современное информационное общество отображает другую важную задачу образования - сформировать новые качества личности - самостоятельность, умение к мировоззренческому выбору и компетентному профессиональному действию, к самообразованию, самоуправлению, самовоспитанию. В связи с этим, отбор средств для развития познавательных творческих способностей в процессе обучения математике остается важным, и это объясняется необходимостью значительных изменений в математической подготовке студентов.

Важное место в современной модели образования занимает образование личности студента с помощью развития усиления проблемности обучения, творческой мыслительной деятельности, воспитания его активности и самостоятельности, устойчивости и гибкости. Развитие и формирование творческой деятельности и активности имеет непосредственную связь с раскрытием способностей и потенциальных возможностей каждого студента [1].

Высшая школа ставит следующие задачи: минимизировать или устранить границы между профессиональным и общим образованием; обучить умению

самосовершенствоваться и учиться; сформировать квалифицированных специалистов процесса деятельности, которые смогли бы взять на себя ответственность за других, и за результаты своей деятельности; сформировать новое, более высокого качества обучение, которое позволит быть конкурентоспособным на рынке труда и повлияет на повышение уровня благополучия граждан; поддержать высокий уровень научных кадров страны.

Программа по высшей математике для высших учебных заведений рассматривает всестороннее развитие личности будущего специалиста, включая творческое воображение, умственные и волевые качества, нравственные черты личности (настойчивость и ответственность, трудолюбие и самостоятельность, честность и дисциплину, целеустремленность и творческую активность) развитие творческих способностей, которые позволили бы аргументированно отстаивать свои убеждения и взгляды [2].

Поэтому необходимо разработать эффективные методики систематизации приемов математической деятельности учеников и студентов, личностно-ориентированного и дифференцированного обучения математике, которые позволят каждому обучающемуся усвоить систематизированное и фундаментальное математическое образование, а у многих сформировать способность к творческой деятельности и творческое математическое мышление, которые смогли бы поставить и решить различные математические, и профессиональные задачи.

Есть реальная возможность качественного усвоения студентами математических дисциплин, а на их основе и профильных специальных предметов, а также, повышения качества математической подготовки студентов технических направлений, если:

- 1) гарантировать плавный поэтапный переход от школьного образования к вузовскому, а также к самостоятельной деятельности студентов, с помощью созданного учебно-методического комплекса по математике;

- 2) создать новые подходы к приобретению студентами учебных математических знаний, основанных на формировании системы приемов учебной и мыслительной деятельности;

- 3) при обучении математике опираться на личностный подход, пользоваться индивидуальными особенностями развития мыслительной деятельности студентов;

- 4) поднимать уровень использования математических знаний при изучении профильных специальных дисциплин;

- 5) проявить интерес к математике и ее пониманию, самостоятельность, стремление к творческой математической деятельности;

- 6) развивать у студентов математическое мышление: абстрактное, логическое, алгоритмическое и убедить их в необходимости и важности математических методов;

- 7) приемы учебной математической деятельности будут зафиксированы и систематизированы чтобы, опираясь на них поставить и решить необходимые в

дальнейшем задачи.

Чтобы это осуществить необходимо решить следующие задачи:

- теоретические задачи: задачи, связанные с разработкой гуманитарной концепции формирования целостной личности в условиях информационного общества в процессе обучения математике;

- методологического задачи: задачи, связанные с разработкой концепции формирования систематизированной совокупности приемов деятельности студентов, развития личности студента при обучении в высшем учебном заведении;

- задачи, затрагивающие реализацию теоретических положений исследования и построение методических основ формирования систематизированной учебной математической деятельности студентов при обучении математике в высшем учебном заведении [3].

Формирование творческого математического мышления и развитие мыслительной деятельности является целенаправленным процессом, надлежащим организовать и проводить в период всего обучения.

Уровень развития математического мышления за последние годы потерпел значительное снижение. Поэтому существует большой разрыв между слабыми знаниями, полученными в школе и вузе, с одной стороны, и высокими требованиями к уровню будущего специалиста - с другой.

В связи с этим возникает необходимость создать целостную научно-методическую концепцию систематизации приемов учебной деятельности студентов, формирования и развития творческой математической деятельности и самостоятельности студентов высших учебных заведений нематематического направления. Необходимо сформировать дифференцированные системы задач по всем разделам элементарной и высшей математики, практические методики и способы их реализации, которые позволили бы повысить уровень и качество математического образования, учитывая интерес к предмету, уровень знаний, индивидуальные способности обучающихся и способствующие активизации процесса обучения, по сравнению с традиционным.

Список литературы

1. Леонтьев, А.Н. *Деятельность. Сознание. Личность* / А.Н. Леонтьев, А.В. Запорожец, П.Я. Гальперин, Д.Б. Эльконин. – Москва: Смысл, 2005. – 352 с. – ISBN 5-89357-153-3.
2. Кудрявцев Л.Д. *Современная математика и её преподавание* / Л.Д. Кудрявцев. - Москва: Наука, 1985. - 176 с.
3. Лунгу, К.Н. *Систематизация приемов учебной деятельности студентов при обучении математике* / К.Н. Лунгу. – Москва: КомКнига, 2007. – 424 с. – ISBN 978-5-484-01010-3.

ПРОБЛЕМЫ РАЗРАБОТКИ МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ ФГОС 4-ГО ПОКОЛЕНИЯ

Сурина Е.Е.

**Орский гуманитарно-технологический институт (филиал) ОГУ,
г. Орск**

Развитие системы высшего образования в России предполагает достаточно скорый переход на ФГОС четвёртого поколения. Основными чертами данного стандарта в отличие от стандартов предыдущих поколений является трансформация образовательных программ ВО в соответствие с требованиями рынка труда. Главной целью образовательного процесса объявляется успешное трудоустройство выпускников. Таким образом, приобретение студентами профессиональных компетенций будет мотивировано именно степенью вхождения конкретного профиля направления подготовки бакалавров или магистрантов в круг потребностей предприятий и отраслей в той или иной профессии с требуемым набором профессиональных функций. Это возможно только при достаточной степени интеграции образовательных и профессиональных стандартов.

В рамках деятельности Министерства труда РФ в настоящее время разрабатывается система профессиональных стандартов во всех отраслях экономики. Одна из целей разработки профессиональных стандартов - удовлетворение запросов работодателей на специалистов определённых профессий соответствующей квалификации. Необходимо отметить, что уже в общих образовательных программах поколения 3+ тем или иным образом учитывались профессиональные стандарты, утвержденные Минюстом. Например, в Орском гуманитарно-технологическом институте (филиале) ОГУ, при разработке ООП направления подготовки 09.03.01 Информатика и вычислительная техника профиль «Программное обеспечение средств вычислительной техники и автоматизированных систем» в качестве нормативных документов рассматриваются Профессиональный стандарт «Программист», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от «17» сентября 2014 г. №679н и Профессиональный стандарт «Технический писатель (специалист по технической документации в области информационных технологий)», утвержденный приказом Минтруда России от 8 сентября 2014г.

Исходя из того, что основным видом профессиональной деятельности выпускника, освоившего ОП ВО по направлению подготовки 09.03.01 Информатика и вычислительная техника, является научно-исследовательская, а Дополнительными видами профессиональной деятельности выступают проектно-конструкторская и проектно-технологическая деятельности, был определен состав обобщенных трудовых функций и трудовых функций,

приведенные в указанных ранее профессиональных стандартах, соответствующие компетенциям ФГОС ВО (таблица 1) .

Таблица 1 Состав обобщенных трудовых функций и трудовых функций, соответствующий компетенциям ФГОС ВО 09.03.01 Информатика и вычислительная техника профиль «Программное обеспечение средств вычислительной техники и автоматизированных систем»

Профессиональный стандарт	Обобщенные трудовые функции (с кодами)	Трудовые функции (с кодами)
ПС ₁ «Программист», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от «17» сентября 2014 г. №679н;	ОТФ ₁ – Разработка и отладка программного кода (А)	ТФ ₁₁ – Формализация и алгоритмизация поставленных задач (А/01.3)
		ТФ ₁₂ – Написание программного кода с использованием языков программирования, определения и манипулирования данными (А/02.3)
		ТФ ₁₃ – Оформление программного кода в соответствии с установленными требованиями (А/03.3)
		ТФ ₁₄ - Работа с системой контроля версий(А/04.3)
		ТФ ₁₅ - Проверка и отладка программного кода (А/05.3)
	ОТФ ₂ – Проверка работоспособности и рефакторинг кода программного обеспечения (В)	ТФ ₂₁ – Разработка процедур проверки работоспособности и измерения характеристик программного обеспечения (В/01.4)
		ТФ ₂₂ – Разработка тестовых наборов данных (В/02.4)
		ТФ ₂₃ – Проверка работоспособности программного обеспечения (В/03.4)

		ТФ ₂₄ – Рефакторинг и оптимизация программного кода (В/04.4)
		ТФ ₂₅ – Исправление дефектов, зафиксированных в базе данных дефектов (В/04.5)
	ОТФ ₃ – Интеграция программных модулей и компонент и верификация выпусков программного продукта (С)	ТФ ₃₁ . Разработка процедур интеграции программных модулей (С/01.5)
		ТФ ₃₂ – Осуществление интеграции программных модулей и компонент и верификации выпусков программного продукта(С/02.5)
	ОТФ ₄ – Разработка требований и проектирование программного обеспечения (D)	ТФ ₄₁ – Анализ требований к программному обеспечению (D/01.6)
		ТФ ₄₂ – Разработка технических спецификаций на программные компоненты и их взаимодействие (D/02.6)
		ТФ ₄₃ – Проектирование программного обеспечения (D/03.6)
ПС ₂ «Технический писатель (специалист по технической документации в области информационных технологий)», утвержденный приказом Минтруда России от 8 сентября 2014 г.	ОТФ ₁ – Оформление и компоновка технических документов	ТФ ₁₁ – Оформление технического документа в соответствии с заданным стандартом
		ТФ ₁₂ – Компоновка технического документа на основе предоставленных источников
		ТФ ₁₃ – Разметка технического документа в соответствии с правилами заданного языка разметки
		ТФ ₁₄ - Подготовка графической схемы по заданному описанию или эскизу

		ТФ ₁₅ - Подготовка снимков экрана компьютерной системы для включения в технический документ в качестве иллюстраций
		ТФ ₁₆ - Разработка несложного технического документа
	ОТФ ₂ – Разработка пользовательских документов, а также стандартных технических документов на основе предоставленного материала	ТФ ₂₁ – Разработка эксплуатационного документа, адресованного конечному пользователю компьютерной системы
		ТФ ₂₂ – Разработка технического документа в соответствии с заданным стандартом на основе предоставленного материала
		ТФ ₂₃ – Создание электронной справки в заданном стандартном формате
		ТФ ₂₄ – Создание демонстрационного или обучающего видеоролика
	ОТФ ₃ – Разработка документов информационно-маркетингового назначения	ТФ ₃₁ – Составление описания продукции или технологии для публикации в рекламном буклете, в каталоге, на веб-сайте
		ТФ ₃₂ – Подготовка рекламной статьи о продукции или технологии для публикации на веб-сайте или в профильных средствах массовой информации
		ТФ ₃₃ – Подготовка слайд-шоу и раздаточных материалов для доклада
	ОТФ ₄ – Разработка технических документов, адресованных специалисту по информационным	ТФ ₄₁ – Описание информационных и математических моделей

	технологиям	ТФ ₄₂ – Описание технических решений с точки зрения специалиста по информационным технологиям
		ТФ ₄₃ – Создание и ведение справочного ресурса для специалистов по информационным технологиям
		ТФ ₄₄ – Подготовка технической статьи о продукции или технологии для размещения на веб-сайте или в профильных средствах массовой информации
		ТФ ₄₅ – Подготовка слайд-шоу и раздаточных материалов для доклада
	ОТФ ₅ –Руководство рабочей группой технических писателей (специалистов по технической документации в ИТ)	ТФ ₅₁ – Проектирование комплекта технической документации
		ТФ ₅₂ – Оценка затрат на разработку комплекта технической документации
		ТФ ₅₃ – Управление разработкой комплекта технической документации

В дальнейшем соответствие формируемых компетенций содержанию той или иной ОТФ или ТФ, отражается в рабочих программах через планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций (знать, уметь, владеть).

Проблемами в построении адекватной и эффективной системы таких взаимосвязей являются, с одной стороны, различие степени обобщенности ОТФ и ТФ в профессиональных стандартах, с другой стороны – состав и содержание дисциплин ООП, ориентированных на устоявшийся комплекс знаний и навыков. Действительно, сравнение ОТФ и ТФ вышеназванных профессиональных стандартов показывает, что ТФ ПС2 «Технический писатель (специалист по технической документации в области информационных технологий)» более детализированы, чем ТФ ПС1 «Программист». Это различие обусловлено как и объективными требованиями профессии, так и

субъективным подходом разработчиков данных стандартов. То же самое влияние субъективных и объективных факторов усиливается при разработке конкретных рабочих программ конкретными преподавателями. С учетом того, что один и тот же профессиональный стандарт в разных направлениях подготовки должен быть реализован формированием различных компетенций ФГОС и задач выбранных основных и дополнительных профессиональных видов деятельности, ситуация становится еще более сложной. Действительно, уже в одной группе направлений подготовки в одном виде деятельности академического бакалавриата существенно различаются формулировки и содержание профессиональных задач (таблица 2)

Таблица 2 Состав задач научно-исследовательской деятельности ФГОС ВО обобщенной группы направлений подготовки 09.00.00 Информатика и вычислительная техника, реализуемых в Орском гуманитарно-технологическом институте (филиал) ОГУ

Направление подготовки	Состав задач профессиональной деятельности
09.03.01 Информатика и вычислительная техника	- изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования; - математическое моделирование процессов и объектов на базе стандартных пакетов автоматизированного проектирования и исследований; - проведение экспериментов по заданной методике и анализа результатов; - проведение измерений и наблюдений, составление описания проводимых исследований, подготовка данных для составления обзоров, отчетов и научных публикаций; - составление отчета по выполненному заданию, участие во внедрении результатов исследований и разработок;
09.03.03 Прикладная информатика	- применение системного подхода к информатизации и автоматизации решения прикладных задач, к построению информационных систем на основе современных информационно-коммуникационных технологий и математических методов; - подготовка обзоров, аннотаций, составление рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе в области прикладной информатики.
09.03.04 Программная инженерия	- участие в проведении научных исследований (экспериментов, наблюдений и количественных измерений), связанных с объектами профессиональной деятельности (программными продуктами, проектами, процессами, методами и инструментами программной инженерии), в соответствии с утвержденными заданиями и методиками; - построение моделей объектов профессиональной деятельности с использованием инструментальных средств компьютерного моделирования; - составление описания проводимых исследований, подготовка данных для составления обзоров и отчетов;

В этой связи возникает вопрос о необходимости определенного уровня унификации связей компетенций ФГОС прежде всего с определенным набором профессиональных стандартов и трудовых функций. При этом необходимо учитывать, что количество утвержденных и введенных в действие профессиональных стандартов увеличивается. Например, в области ИТ в разработке настоящее время находится около 60 новых ПС, каждый из которых может и, безусловно, должен быть отражен в сравнительно небольшой группе направлений подготовки (09).

Решить эту проблему может реализация высокой степени модульности, предполагающую тесную интеграцию различных уровней образовательной системы. Среднее профессиональное, дополнительное профессиональное и высшее образование должны быть гармонично связаны едиными профессиональными стандартами, нацеленными на запросы работодателей. Здесь важна роль программ прикладного бакалавриата — промежуточного звена от среднего профессионального к высшему образованию. При этом актуальным становится включение колледжей в состав вузов. Следующая методическая цель — формирование преемственности между средним профессиональным и дополнительным, а также между высшим и дополнительным образованием. Дополнительные программы переподготовки и образования (ДПП и ДПО) предполагают меньшее количество учебных часов, у вузов и колледжей появляется возможность разрабатывать отдельные модули с тем ли иным кругом формируемых компетенций (а, следовательно и трудовых функций) и выходить с каждым разработанным модулем основных программ на свой сегмент рынка дополнительных образовательных услуг. Так образом, будет реализовываться стратегия непрерывного образования, когда специалист на любом этапе своей карьеры «добирает» необходимые компетенции параллельно со студентами, что особенно актуально в области ИТ, как одной из самых инновационных отраслей экономики. Однако, такая нелинейная схема приобретения новой профессиональной компетентности подразумевает совместное обучение студентов различной степени подготовки, а так же с различными мотивациями, и, возможно, — разных возрастных групп.

Подводя итог вышесказанному, необходимо отметить, что требования к разработке методического обеспечения ФГОС 4-го поколения модульная система потребует от преподавателей не только высокой квалификации по читаемой дисциплине, но и особой гибкости в подготовке и подаче материалов, а также при проверке знаний. Нелинейная схема подразумевает совместное обучение студентов с неодинаковым опытом, «бэкграундом», мотивациями, зачастую — разных возрастных групп.

Список литературы

- 1. Федеральный закон от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации»;*
- 2. Федеральный государственный образовательный стандарт высшего образования (ФГОС ВО) по направлению подготовки 09.03.01 Информатика и вычислительная техника (уровень бакалавр), утвержденный приказом Министерства образования и науки Российской Федерации от «12» января 2016 г. № 5;*
- 3. Профессиональный стандарт «Программист», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от «17» сентября 2014 г. №679н;*
- 4. Профессиональный стандарт «Технический писатель (специалист по технической документации в области информационных технологий)», утвержденный приказом Минтруда России от 8 сентября 2014 г.*
- 5. Федеральный государственный образовательный стандарт высшего образования (ФГОС ВО) по направлению подготовки 09.03.03 Прикладная информатика (уровень бакалавриата), утвержденный приказом Министерства образования и науки Российской Федерации от «12 марта» 2015 г. № 207;*
- 6. Федеральный государственный образовательный стандарт высшего образования (ФГОС ВО) по направлению подготовки 09.03.04 Программная инженерия (уровень бакалавр), утвержденный приказом Министерства образования и науки Российской Федерации от «12» марта 2015 г. № 229;*

ПОПУЛЯРИЗАЦИЯ МАТЕМАТИЧЕСКИХ ЗНАНИЙ И МАТЕМАТИЧЕСКОГО ОБРАЗОВАНИЯ В ПРОЦЕССЕ ОБУЧЕНИЯ ИСТОРИИ РОССИИ

Уткина Т.И., Игнатьева Е.С.

**Орский гуманитарно-технологический институт (филиал)
ФГБОУ ВО «Оренбургский государственный университет», г. Орск**

Проблема популяризации математических знаний и математического образования актуализирована в Концепции развития математического образования в Российской Федерации (распоряжение Правительства РФ от 24.12.2013г.) и в Национальной образовательной инициативе «Наша новая школа» [3]. Указанная проблема выделяется в Концепции как значимая задача развития математического образования России, решение которой обеспечит успех нашей страны в 21 веке [2].

Россия имеет огромный положительный опыт в математическом образовании и науке. Математика занимает значительное место среди других предметов по возможностям развития познавательных способностей человека, в том числе логического мышления и влияния её на преподавание других дисциплин. Качественное математическое образование необходимо каждому для его успешной социализации в современном обществе. Изучение математики играет системообразующую роль в образовании. Но в условиях социальных изменений в России последнего времени обострились проблемы математического образования мотивационного, содержательного, и кадрового характера. В различных научных исследованиях отражены вопросы популяризации математического знания и образования, но в месте с тем вопрос о комплексном использовании средств и возможностей курса истории России в популяризации математических знаний и математического образования остается открытым. Анализ стандартов ФГОС общего образования по истории России и математике, психолого – педагогической и методической литературы, диссертационных исследований по проблеме популяризации математического знания и математического образования позволил выявить противоречия:

- на научно-педагогическом уровне – между необходимостью популяризации математического знания и математического образования в процессе обучения истории России и недостаточной разработанностью теоретических и методических основ популяризации;

- на научно-методическом уровне между дидактическими возможностями курса истории России для популяризации математических знаний и математического образования и недостаточной разработанностью методики использования этих возможностей для популяризации математических знаний и математического образования. Выявленные противоречия обуславливают актуальность темы педагогического исследования «Популяризация математических знаний и математического образования в процессе обучения

истории России». Объектом проводимого исследования является процесс обучения истории России в условиях общеобразовательной школы [2]. Предметом исследования выступает популяризация математических знаний и математического образования на уроках истории России и внеурочных занятиях. Целью исследования является научное обоснование и разработка методики популяризации математических знаний и математического образования в процессе обучения истории России. Для достижения поставленной цели выдвигается следующая рабочая гипотеза: популяризация математических знаний и математического образования в процессе обучения истории России будет обеспечена: если в процессе обучения истории России будут включаться проекты и рефераты по популяризации математических знаний и российского математического образования [4].

В соответствии с целью предметом и гипотезой в проводимом исследовании предполагается решение следующих задач: проведение анализа психолого – педагогической литературы, диссертационных исследований, нормативных документов с целью изучения состояния проблемы популяризации математических знаний и математического образования и определения путей её решения, а также для выявления сущности таких понятий как «популяризация», «популяризация математических знаний», «математического образования»; разработка модели популяризации математических знаний и математического образования в процессе обучения истории России; создание в соответствии с разработанной моделью методики популяризации математических знаний и математического образования в процессе обучения истории России; разработка компьютерного обеспечения методики популяризации математических знаний и математического образования в процессе обучения истории России, экспериментальная проверка эффективности разработанной методики популяризации математических знаний и математического образования в процессе обучения истории России. [2]

Проведенное теоретическое исследование позволило выявить сущностные характеристики таких понятий, как «популяризация», «популяризация математических знаний» [1].

Популяризация науки — процесс распространения научных знаний в современной и доступной форме для широкого круга людей (имеющих определенный уровень подготовленности для получения информации). Популяризация науки, «перевод» специализированных знаний на язык малоподготовленного слушателя, читателя — одна из самых важных задач, стоящих перед популяризаторами науки. Задачей популяризатора науки является превращение скучных научных данных в интересную и понятную большинству информацию. Популяризация науки может быть направлена как на общество в целом, так и на его часть, подрастающее поколение, — талантливых школьников [1].

Важную роль в этом процессе играет научная фантастика, предвосхитившая и вдохновившая множество научных открытий. Существенный вклад в это внёс фантаст Жюль Верн, один из первопроходцев жанра. Приход молодёжи в науку и высокотехнологичные области производства, внимание непосвящённой части общества к научным проблемам зависят от степени популярности науки. Учёные, как носители научных знаний, заинтересованы в их сохранении, развитии и приумножении, чему способствует приток в неё молодёжи. Популяризация науки увеличивает количество людей интересующихся наукой благодаря стимуляции интереса к ней.

Часто бывает, что при популяризации научных знаний она упрощается и постепенно превращается в научный миф. Также бывает, что при популяризации науки возникают такие научно-популярные клише как: тайны мироздания, «учёные открыли», и так далее[1].

Тихо Браге считал, что научные знания должны быть доступны только правителям, умеющим ими пользоваться. Академик РАН Людвиг Фаддеев так высказался о популяризации науки:

«Мы отдаем себе отчёт, что должны все-таки объяснять людям, налогоплательщикам, что мы делаем. Но нужно популяризировать те области науки, которые уже полностью понятны. Современную науку труднее популяризировать. Рассказывать про всякие кварки, струны, поля Янга-Миллса... получается нехорошо — с обманами» [1].

В качестве экспериментальной площадки была выбрана МОАУ «СОШ № 4 г. Орска».. Определены экспериментальные классы (5 по 11) и содержательные модули в курса истории России («Летоисчисление», «Исторические задачи», «От древности до наших дней», «Столетняя война», «Правление Карла великого»; «Отечественная война», «от древности до наших дней», « 900 дней блокады» , «Египет с древности до наших дней»), в рамках изучения которых будет осуществляться популяризация математических знаний и математического образования.

Список литературы

1. Лазаревич, Э. А. *Искусство популяризации науки: 2-е издание, переработанное и дополненное. Ответственный редактор Сикорский, Н.М.: учебник / Э. А. Лазаревич. / Москва: Издательство «Наука», 1978. – 384 с.*

2 *Концепция развития математического образования в Российской Федерации (утверждена распоряжением Правительства РФ от 24.12.13 г., № 2506-р)*

3. *Национальная образовательная инициатива «НАША НОВАЯ ШКОЛА».* [Электронный ресурс]. Режим доступа: http://www.educom.ru/ru/nasha_novaya_shkola/school.php > (дата последнего просмотра 24.11.2011 г.)

4. *Федеральный Государственный Образовательный Стандарт Среднего (полного) Общего Образования (утвержден приказом Минобрнауки России от 17 мая 2012 г. № 413.*

РЕАЛИЗАЦИЯ СИМУЛЯТОРА ИНФРАСТРУКТУРЫ ДЛЯ МНОГОАДРЕСНОЙ ШИРОКОПОЛОСНОЙ ПЕРЕДАЧИ МУЛЬТИМЕДИЙНОГО ТРАФИКА НА БАЗЕ ПРОГРАММНО- КОНФИГУРИРУЕМЫХ СЕТЕЙ

**Ушаков Ю.А., Полежаев П.Н., Шухман А.Е., Бахарева Н.Ф.
Оренбургский государственный университет, г. Оренбург**

1 Введение

Сегодня IPTV является главным конкурентом обычного и цифрового телевидения. IPTV работает по принципу многоадресной передачи – распространения одинакового контента для ограниченного числа абонентских устройств, подключенных к одной и той же группе вещания (каналу).

Основные трудности развертывания IPTV связаны с маршрутизацией широкополосного мультимедийного трафика, которая в современных сетях осуществляется с помощью протоколов IGMP и PIM. Основными недостатками данных протоколов является сложность настройки, дороговизна устройств, которые их поддерживают, и низкая производительность на коммутаторах уровня доступа.

2 Реализация симулятора

Инфраструктура передачи широкополосного мультимедийного трафика может быть представлена в виде ориентированного графа, вершинами которого являются сервера, коммутаторы и маршрутизаторы, а дугами – сетевые связи между ними. Совокупность всех маршрутов передачи данных от вещателя к абонентам группы образует дерево вещания. Формирование оптимального дерева вещания может быть формализовано в виде решения NP-полной проблемы Штейнера для ориентированного графа сетевой инфраструктуры.

Для изучения работы потоков IPTV в сетях второго и третьего уровня, сравнения с традиционными подходами IGMP и PIM, был создан симулятор, описанный в работе [1]. Симулятор построен на базе системы OMNET++ с открытым исходным кодом [2] и возможностью использовать не просто симулируемые структуры, а интегрироваться с эмуляторами и реальными контроллерами (через PCAP интерфейс сетевой карты).

Интерфейс симулятора выполнен на базе IDE Eclipse с интеграцией с OMNET++ (рисунок 1).

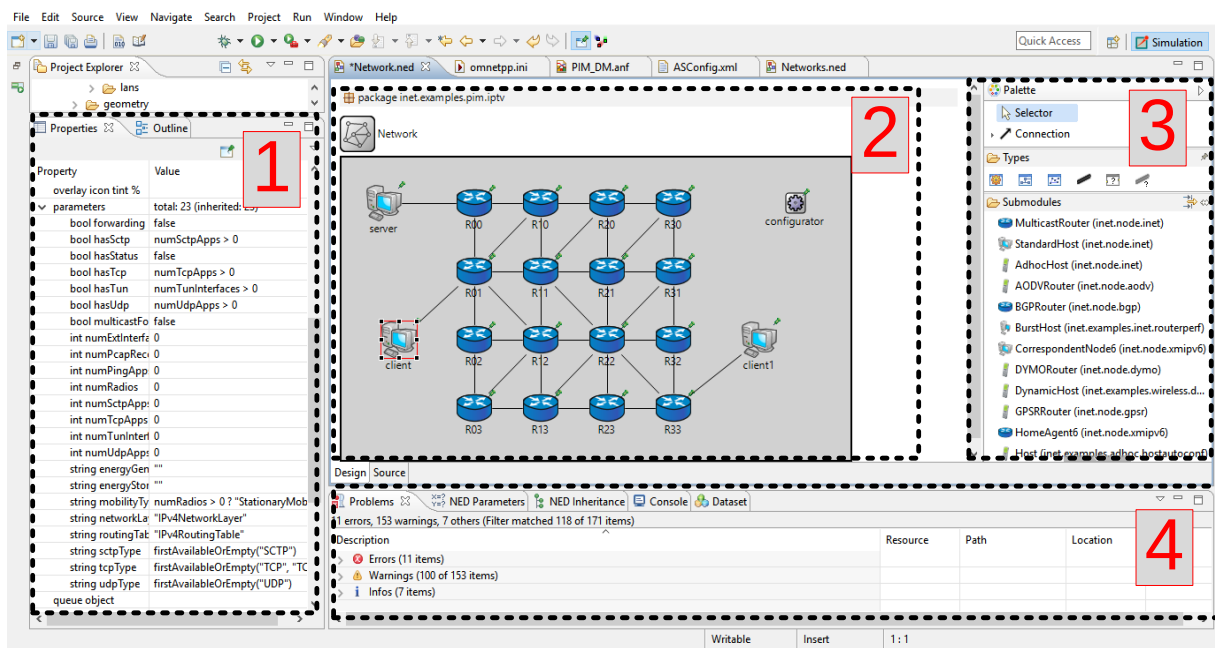


Рисунок 1 – Окно симулятора

Зона 1 предназначена для настройки свойств объектов, например, скорости линии. Зона 2 предназначена для визуального конструирования сети, зона 3 – для добавления новых устройств или связей. В зоне 4 выводятся ошибки и предупреждения от симулятора.

На рисунке 2 показана сеть, на которой исследовались алгоритмы и протоколы многоадресной сети. Топология сети подобрана таким образом, чтобы на ее основе можно было путем отключения интерфейсов симулировать любые топологии, встречающиеся у провайдеров IPTV – звезда, кольцо, кольцо с деревом, вложенные кольца и прочие.

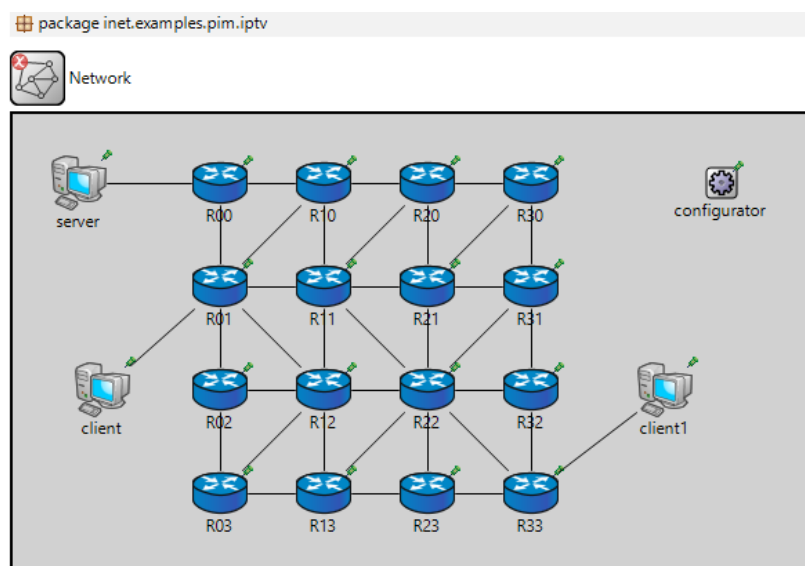


Рисунок 2 – Прототип сети для исследования работы многоадресной рассылки

Также для исследования простых действий каждого протокола был создан модуль визуализации пакетов на основе модуля симуляции OMNET++, дополненный средствами глубокого анализа пакетов, показанный на рисунке 3.

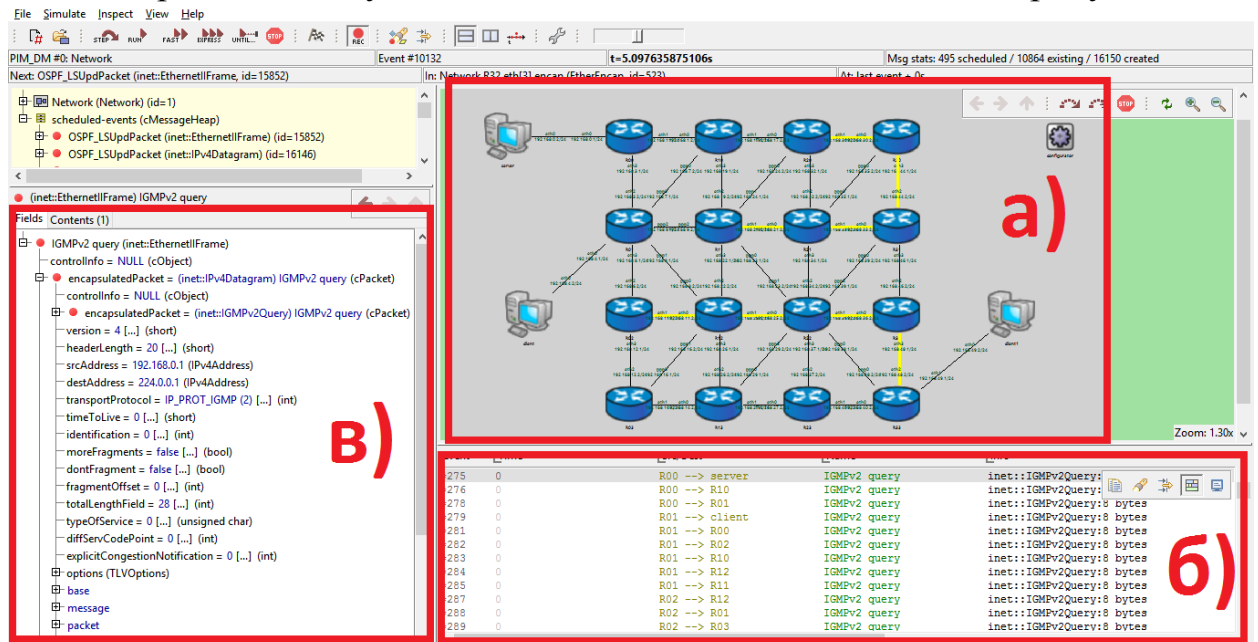


Рисунок 3 – Модуль визуализации пакетов: а) визуализация движения пакетов и нагрузки на линии; б) список пакетов в системе (с фильтром); в) детализация выбранного пакета.

3 Настройка схемы сети симулятора

На схеме отображаются все IP адреса маршрутизаторов и клиентов, пакеты и их содержимое. Для задания параметров используется INI файл и переменные проекта, что делает возможным автоматизацию серии экспериментов с разными входными параметрами. Для задания интенсивности и закона распределения генерации трафика используются параметры приложений, которых может быть несколько на каждом конечном устройстве. Для задания длины пакета используется конструкция:

```
**.server.udpApp[0].messageLength = uniform(500B, 1400B)
```

которая задает на сервере длину UDP пакета случайным образом, распределенным по равномерному распределению в интервале 500-1400 байт. Для задания наиважнейшей характеристики потока – интенсивности и распределения времени между пакетами по экспоненциальному закону распределения используется конструкция:

```
**.server.udpApp[0].sendInterval = exponential(30us)
```

Для задания начала и конца генерации, адреса, порта, типа приложений используется следующие строки

```

**server.udpApp[0].destPort = 5000
**server.udpApp[0].destAddresses = "239.0.0.11"
**server.udpApp[0].startTime = 20s
**server.udpApp[0].stopTime = 100s

```

Адрес назначения должен быть такой же, как и на клиентских приложениях. Начало генерации через 20 секунд сделано для исключения начального влияния процессов обмена таблицами маршрутизации на конечный результат [3].

Для того, чтобы управлять маршрутизацией, в каждом маршрутизаторе есть настройки пириитизации интерфейсов в виде метрик OSPF:

```

<Router name="R00" RFC1583Compatible="true">
  <BroadcastInterface      ifName="eth0"      areaID="0.0.0.0"
interfaceOutputCost="1"/>
  <PointToPointInterface    ifName="eth1"      areaID="0.0.0.0"
interfaceOutputCost="1"/>
  <PointToPointInterface    ifName="eth2"      areaID="0.0.0.0"
interfaceOutputCost="10"/>
  <PointToPointInterface    ifName="eth3"      areaID="0.0.0.0"
interfaceOutputCost="100"/>
</Router>

```

Метрика 1 взята за цену маршрута 10Гбит/с, соответственно 10 и 100 – для 1Гбит/с и 100Мбит/с. При таком способе задания метрики маршрут строится как самый быстрееший по сумме всех каналов следования пакета, как описано в [3].

Для включения OSPF вместо статической маршрутизации необходимо явно это задать:

```

**configurator.addStaticRoutes = false
**R??.hasOSPF = true

```

Для обеспечения корректного симулирования очередей была выбрана очередь DropTail и последующий обработчик WRRQ, как описано в [2]

```

**R??.eth[*].queueType = "DropTailQueue"
**R??.eth[*].queue.frameCapacity = 256

```

Размер очереди 256 пакетов взят из спецификации распространенного маршрутизатора Cisco серии 2900 (2921). Для задания режима Sparse нужно использовать явное указание режима работы и точки RP

```
**.pimConfig = xml("<config><interface mode=\"sparse\"/></config>")  
**.RP = "192.168.3.1"
```

где IP адрес должен совпадать с крайним маршрутизатором, подключенным серверу вещания. Также, в случае Dense маршрутизации явно определяем режим:

```
**.pimConfig = xml("<config><interface mode=\"dense\"/></config>")
```

Для подключения OpenFlow протокола был использован модуль [4], который поддерживает базовую функциональность OpenFlow версии 1.0, которой вполне хватает для реализации маршрутизации. Для работы OpenFlow необходимо добавить в модель поддержку OF и модуля коммутации:

```
import openflow.nodes.*;  
import openflow.utility.SpanningTree;
```

и настроить контроллер

```
**.controller.ofa_controller.port = 6633  
**.open_flow_switch*.sendCompletePacket = false  
**.controller.behavior = "Router"  
**.ofa_switch.connectPort = 6633  
**.ofa_switch.connectAddress = "controller"  
**.buffer.capacity = 10  
**.ofa_switch.flow_timeout = 5s  
**.open_flow_switch*.etherMAC[*].promiscuous = true
```

где «controller» - адрес контроллера, «Router» - место применения OpenFlow. Маршрутизаторы для работы с OpenFlow тоже нужно изменить, добавив в них коммутатор OpenFlow на вход из Ethernet интерфейсов.

4 Апробация симулятора

В результате прогона симулятора в файл записываются все показатели сети, которые можно затем исследовать как в векторном виде, так и в виде гистограмм и абсолютных чисел (рисунок 4)

NetworkMiner

Here you can see all data that come from the files specified in the Inputs page.

runID filter module filter statistic name filter

Folder	File name	Config na...	R	Run id	Module	Name	Value
/inet/ex...	PIM_DM-0.sca	PIM_DM	0	PIM_DM-0-20...	Network.R03.eth[0].queue.dataQueue	queueingTime:histogram...	0.0
/inet/ex...	PIM_DM-0.sca	PIM_DM	0	PIM_DM-0-20...	Network.R03.eth[0].queue.dataQueue	queueingTime:histogram...	0.0
/inet/ex...	PIM_DM-0.sca	PIM_DM	0	PIM_DM-0-20...	Network.R03.eth[0].queue.dataQueue	queueingTime:histogram...	0.0
/inet/ex...	PIM_DM-0.sca	PIM_DM	0	PIM_DM-0-20...	Network.R03.eth[0].queue.dataQueue	dropPkcount	0.0
/inet/ex...	PIM_DM-0.sca	PIM_DM	0	PIM_DM-0-20...	Network.R03.eth[0].queue.dataQueue	dropPksum(packetBytes)	0.0
/inet/ex...	PIM_DM-0.sca	PIM_DM	0	PIM_DM-0-20...	Network.R03.eth[0].queue.dataQueue	rcvdPkcount	4.0
/inet/ex...	PIM_DM-0.sca	PIM_DM	0	PIM_DM-0-20...	Network.R03.eth[0].queue.dataQueue	rcvdPksum(packetBytes)	292.0
/inet/ex...	PIM_DM-0.sca	PIM_DM	0	PIM_DM-0-20...	Network.R03.eth[0].mac	simulated time	20.0037437...
/inet/ex...	PIM_DM-0.sca	PIM_DM	0	PIM_DM-0-20...	Network.R03.eth[0].mac	full-duplex	1.0
/inet/ex...	PIM_DM-0.sca	PIM_DM	0	PIM_DM-0-20...	Network.R03.eth[0].mac	frames/sec sent	0.0
/inet/ex...	PIM_DM-0.sca	PIM_DM	0	PIM_DM-0-20...	Network.R03.eth[0].mac	frames/sec rcvd	0.0
/inet/ex...	PIM_DM-0.sca	PIM_DM	0	PIM_DM-0-20...	Network.R03.eth[0].mac	bits/sec sent	0.0
/inet/ex...	PIM_DM-0.sca	PIM_DM	0	PIM_DM-0-20...	Network.R03.eth[0].mac	bits/sec rcvd	0.0
/inet/ex...	PIM_DM-0.sca	PIM_DM	0	PIM_DM-0-20...	Network.R03.eth[0].mac	rx channel idle (%)	100.0

Inputs Browse Data Datasets

Рисунок—4 Результаты симуляции

Например, для времени ожидания в очереди маршрутизатора R01 и интерфейса eth3 будет выглядеть так:

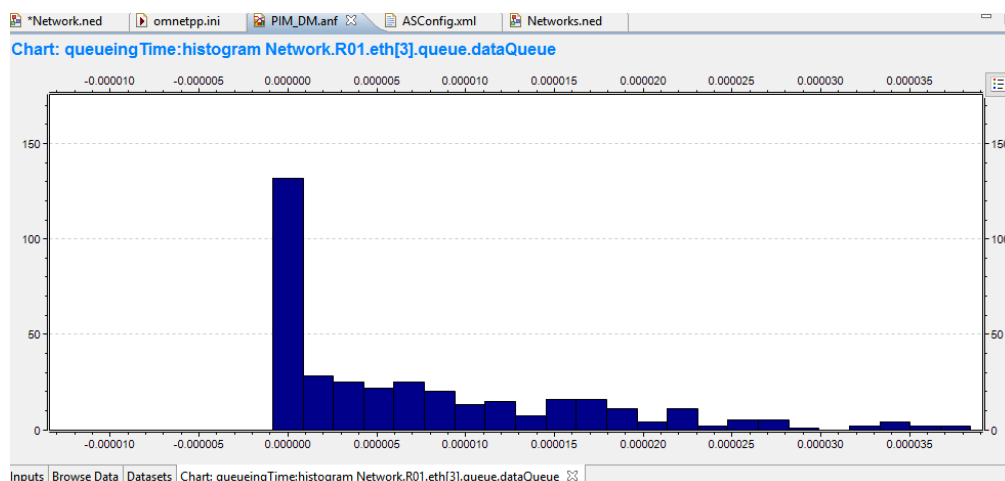


Рисунок 5 – Гистограмма времени ожидания в очереди

В настоящее время провайдер не имеет возможности контролировать деревья мультимедийного трафика на уровне доступа и между L2 коммутаторами. Главный канал может быть перегружен 200–300 IPTV-каналами, и при увеличении числа каналов в HD-разрешении увеличивается и перегрузка.

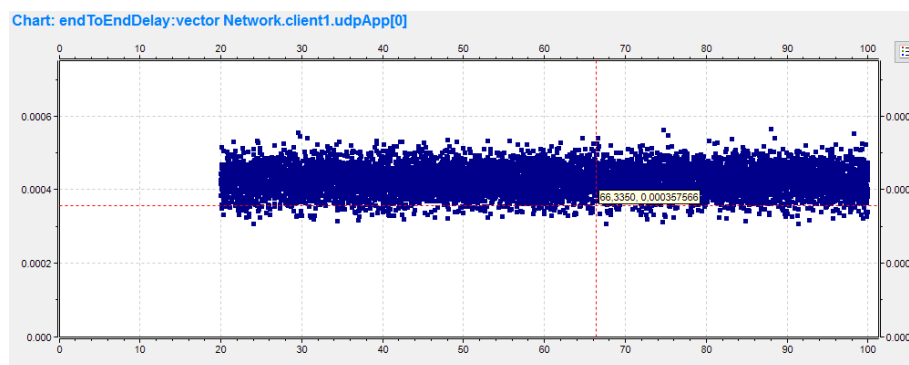


Рисунок 6 – Тестовый прогон симуляции для базового уровня

Но для сравнительного анализа задержек лучше использовать гистограммы: на рисунке 7 показана гистограмма для ненагруженного режима сети при генерации пакетов по экспоненциальному закону с интенсивностью 1000 пакетов, это около 5 FullHD каналов IPTV или 7-8 Мбит/с.

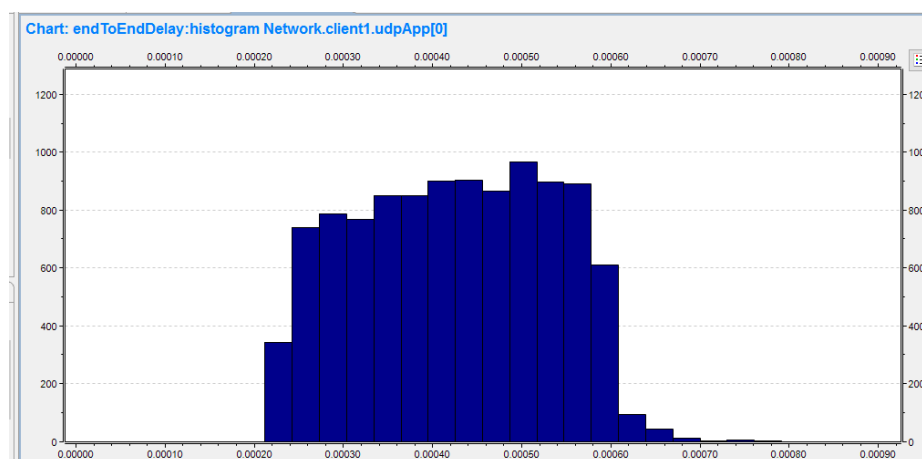


Рисунок 7 - Гистограмма времени отклика

5 Выводы

Разработанный симулятор показал принципиальную работоспособность и гибкость, а также возможность изучать различные аспекты передачи трафика IPTV не вдаваясь в подробности моделирования и не зная основы языков модельных сред. Это позволяет использовать симулятор как в обучении, так и при проектировании новых сетей многоадресной рассылки, в том числе и с использованием других способов маршрутизации и коммутации, например, OpenFlow.

Проект был реализован при финансовой поддержке Российского фонда фундаментальных исследований, проект № 15-07-06071.

Список литературы

1. Ushakov Yu., Polezhaev P., Legashev L., Bolodurina I., Shukhman A., Bakhareva N. Increasing the Efficiency of IPTV by Using Software-Defined Networks // International Conference on Next Generation Wired/Wireless Networking. – Springer International Publishing, 2016. – PP. 550-560.
2. Veselý V., Ryšavý O., Švéda M. Protocol Independent Multicast in OMNeT++. // ICNS 2014: The Tenth International Conference on Networking and Services. – PP. 132-137
3. Ashique M. Simulation-Based Comparative Study of EIGRP and OSPF for Real-Time Applications. Master Thesis Electrical Engineering Thesis no: MEE 10:53 September 2010
4. An OpenFlow Extension for the OMNeT++ INET Framework. Lehrstuhl für Informatik III, Am Hubland. Режум доцмyna: https://www3.informatik.uni-wuerzburg.de/research/ngn/ofomnet/of_omnet.shtml - 20.12.2016.

«САЙТ КОНФЕРЕНЦИИ» КАК ИНФОРМАЦИОННАЯ ПЛОЩАДКА ДЛЯ ПЕДАГОГИЧЕСКОГО СООБЩЕСТВА

Янгичер О.С., Усманов Р.И.

Оренбургский государственный университет, г. Оренбург

С развитием интернет-технологий общение педагогического сообщества перешло на новый интеллектуальный уровень. Географические границы и языковые барьеры с появлением новых программных средств окончательно стираются. Одной из форм обмена опытом, своими наблюдениями и инновациями, достижениями и результатами труда являются конференции. Возможность ознакомиться с актуальными проблемами науки за пределами своего вуза, города, страны как раз и предоставляют системы, с открытым доступом, размещенные в сети Интернет.

Информационная система «Сайт конференции» используется сотрудниками ОГУ для проведения Всероссийской научно-методической конференции «Университетский комплекс как региональный центр образования, науки и культуры» (далее – конференция) 1 раз в год.

Задачи «Сайта конференции»:

- информационное сопровождение конференции (размещение полной информации о направлениях работы, требованиях к оформлению материалов, сроках проведения, условиях участия в конференции);
- онлайн-регистрация участников конференции;
- доступность материалов конференции с любого компьютера, подключенного к локальной сети ОГУ либо Интернет;
- оптимизация и автоматизация процедуры сбора и анализа материалов конференции;
- автоматическое формирование программы секционных заседаний конференции;
- создание архива материалов предыдущих конференций.

При объявлении новой конференции любому пользователю, имеющему доступ к сети Интернет, предоставляется возможность разместить свою заявку на участие с помощью онлайн-регистрации информационной системы «Сайт конференции». В меню главной страницы сайта (рисунок 1) размещается информационное письмо конференции, указывается состав оргкомитета, блок для самостоятельной регистрации личного кабинета, ссылка на архив электронных изданий прошедших конференций, а также располагается форма для авторизации зарегистрировавшихся участников. На рисунке 2 представлен интерфейс страницы онлайн-регистрации личного кабинета участника.

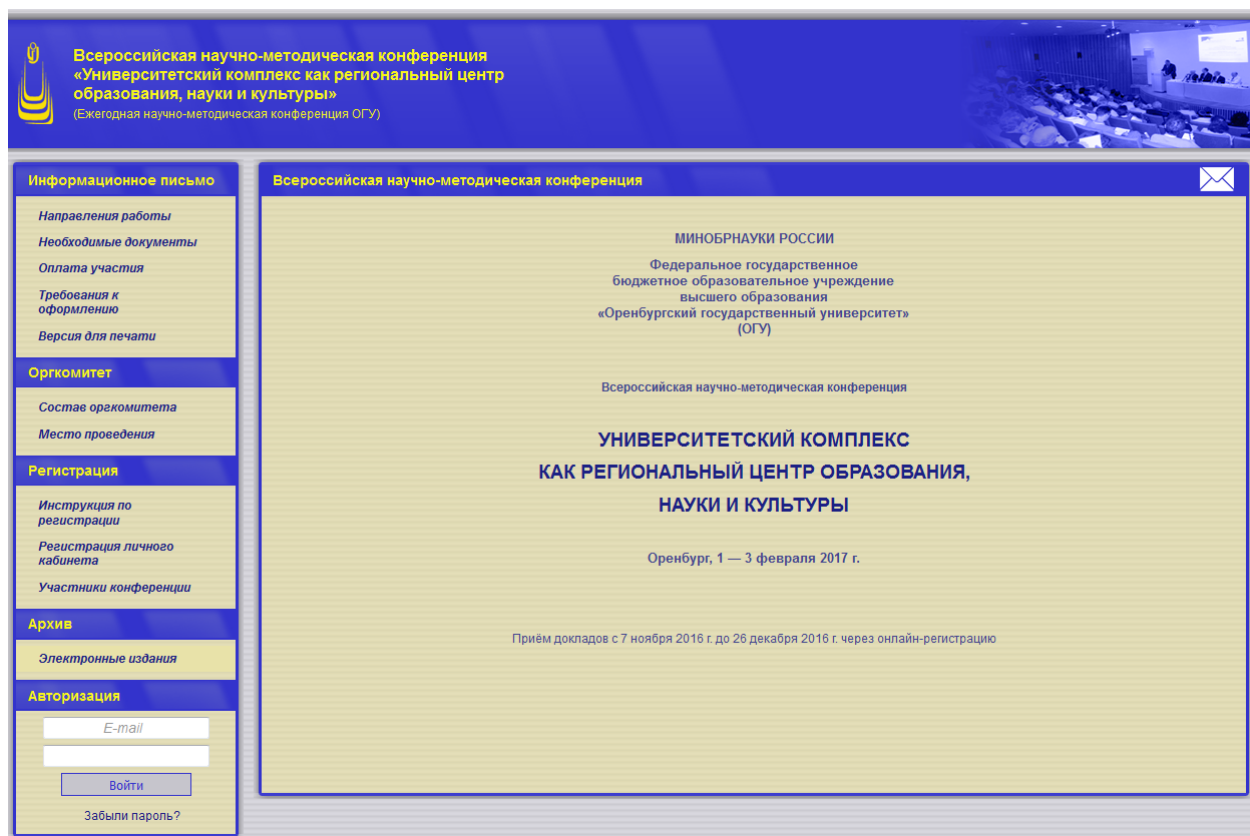


Рисунок 1 – Главная страница информационной системы «Сайт конференции»

Рисунок 2 – Окно онлайн-регистрации личного кабинета участника конференции

После регистрации личного кабинета участникам предоставляется возможность зарегистрировать соавторов доклада, а также прикрепить файлы доклада и скан квитанции об оплате организационного взноса. На рисунке 3 представлена страница личного кабинета участника конференции.

Возможности, предоставленные участнику конференции в личном кабинете:

- просматривать статусы своих докладов (заявка на рассмотрении, заявка принята на рассмотрение, заявка подтверждена председателем секции, заявка отклонена, заявка подтверждена и оплачена, заявка удалена);
- редактировать персональные данные;
- регистрировать соавторов;
- прикреплять файлы докладов;
- автоматическое формирование лицензионного договора о передаче неисключительных прав на использование произведения, а также акта о приеме-передаче Произведения;
- заменять файл доклада (пока он не подтвержден председателем секции);
- осуществлять смену пароля.

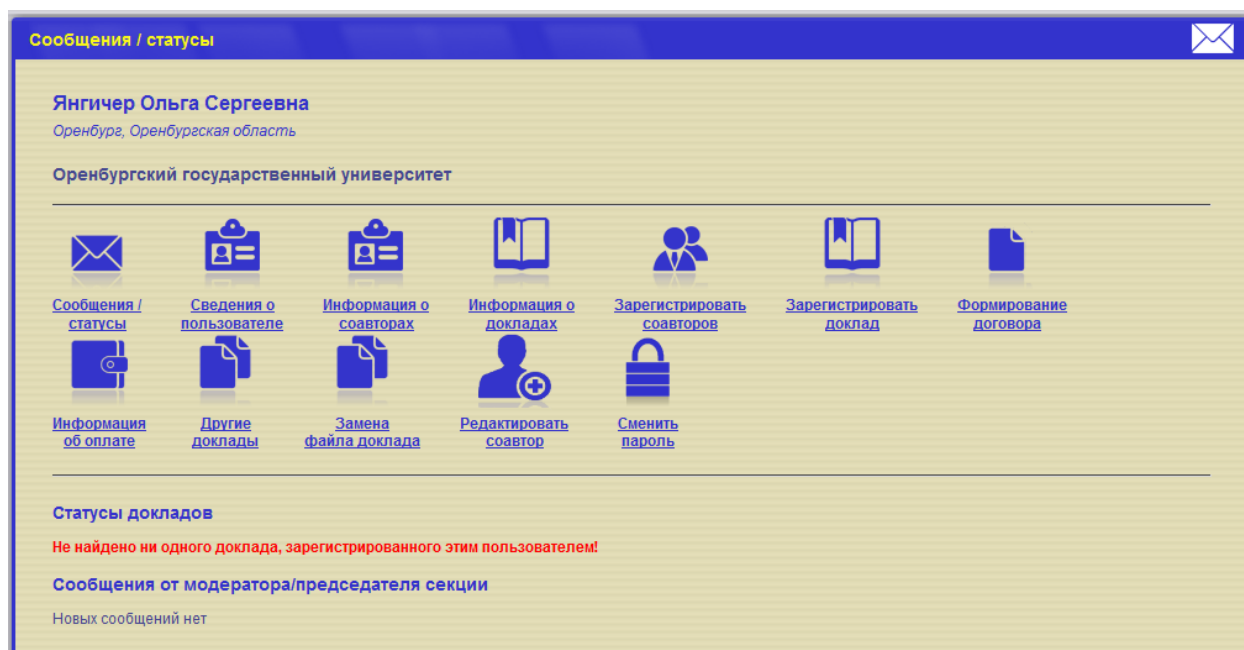


Рисунок 3 – личный кабинет участника конференции

Модератор конференции просматривает поступающие заявки и если вся информация корректна и соответствует указанным в информационном письме требованиям к оформлению, принимает доклад пользователя на рассмотрение (рисунок 4). Информационная система «Сайт конференции» не позволяет владельцу личного кабинета сгенерировать лицензионный договор о передаче неисключительных прав на использование произведения, а также акт о приеме-

передаче Произведения пока модератор не установит для заявки статус «заявка на рассмотрении».

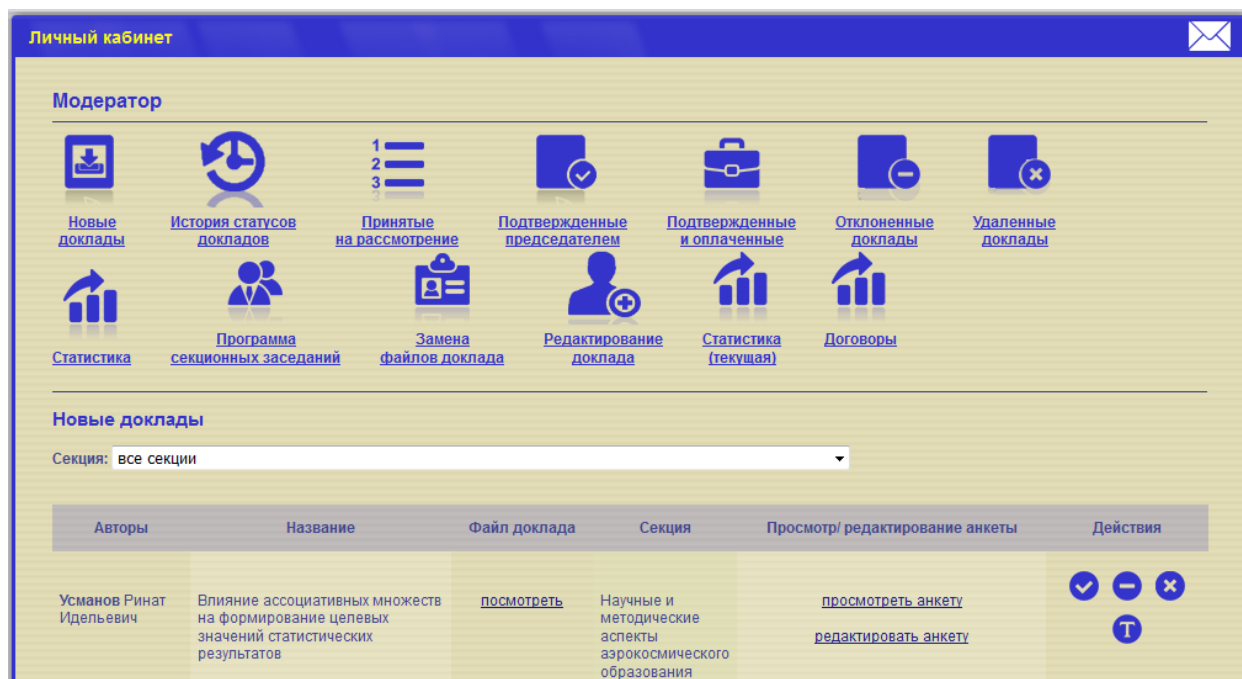


Рисунок 4 – личный кабинет модератора

Принятая на рассмотрение заявка отправляется в кабинет председателя (рисунок 5) указанной секции, который может принять/ отклонить/ отправить заявку на доработку.



Рисунок 5 – личный кабинет председателя

После подтверждения модератором оплаты оргвзноса сведения об участнике конференции появляются в открытом доступе на странице «Участники конференции» (рисунок 6).

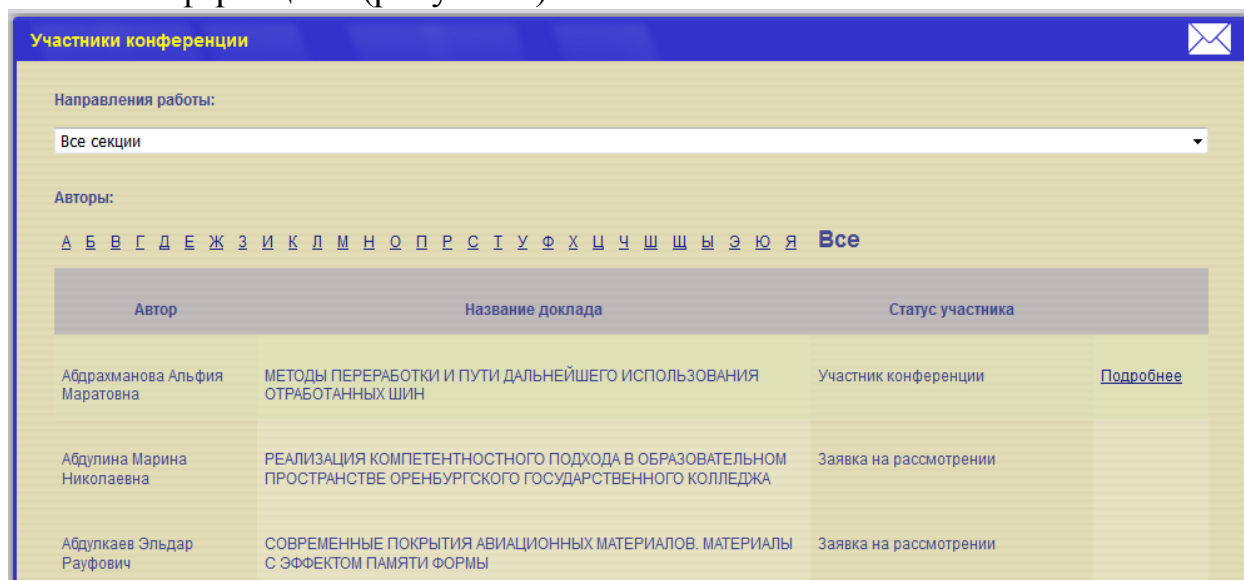


Рисунок 6 – Участники конференции

Участие в конференциях дает шанс начинающим специалистам поделиться своими идеями и познакомиться с разработками опытных практиков и именитых ученых. Работодателям тоже полезно знакомство с исследованиями участников, ведь визуализированное представление работы может помочь сформировать начальное представление о человеке и уровне его профессионализма.

Информационная система «Сайт конференции» зарегистрирована в УФЭР (регистрационный номер №780 от 19.12.12). На данный момент с её помощью была осуществлена технологическая поддержка пяти конференций.